DARK MIRROR - OSSERVATORIO DELLE MINACCE RANSOMWARE

REPORT H2 2024

DARKLAB
RHC INTELLIGENCE LABORATORY

DakLab è un laboratorio di Intelligence all'interno della vasta community di Red Hot Cyber, specializzato nel monitoraggio delle minacce informatiche. nasce con l'obiettivo di diffondere la conoscenza sulle cyber minacce, contribuendo a rafforzare la consapevolezza e le difese digitali del paese.

INTRODUZIONE

Nel panorama odierno della sicurezza informatica, il ransomware si conferma come una delle minacce più pervasive e insidiose. La sua natura è ben nota: attraverso avanzati sistemi di cifratura, i criminal hacker riescono a bloccare l'accesso ai dati e a richiedere un riscatto in cambio della chiave di decrittazione. Questo fenomeno, ormai diffusissimo su scala globale, ha registrato in Italia un decremento rispetto al 2023, anche se questo non è bastato a collocarci al quinto posto per numero di attacchi documentati (149) preceduto solamente da Stati Uniti, Regno Unito, Canada e Germania. Questa seconda edizione del report, si focalizzata sull'intero anno 202evidenziando le nuove tecniche di attacco adottate dagli attori malevoli e i settori maggiormente coinvolti.

Vogliamo offrire un'analisi dettagliata dell'evoluzione di questa minaccia con un duplice obiettivo: da un lato, sensibilizzare i professionisti della sicurezza informatica e i decisori aziendali sulla necessità di rafforzare le proprie strategie difensive; dall'altro, fornire un quadro chiaro sugli impatti economici e reputazionali di questi attacchi, aiutando le organizzazioni a comprendere i rischi concreti e a sviluppare contromisure efficaci.

Nel corso del report esamineremo l'evoluzione dei Threat Actors, approfondendo le loro tecniche, tattiche e procedure (TTPs), le operazioni delle forze dell'ordine e fornendo un punto di vista esclusivo attraverso le nostre interviste dirette ai cybercriminali. Inoltre, analizzeremo le nuove minacce emergenti, come l'integrazione dell'intelligenza artificiale generativa nel cybercrime, e condurremo uno studio approfondito sull'economia del ransomware, con un'analisi delle transazioni sui wallet criminali.

Questo report è il risultato del lavoro congiunto del team Dark Lab, costantemente impegnato nell'esplorazione delle fonti underground e nel monitoraggio delle nuove tendenze della criminalità informatica. Le informazioni e le raccomandazioni qui presentate mirano a fornire un supporto concreto a chi opera nel settore della sicurezza, aiutando aziende e istituzioni a rafforzare le proprie difese e a sviluppare piani di risposta sempre più efficaci.

Pietro Melillo, Direttore del gruppo Dark Lab di Red Hot Cyber

DARKLAB
RHC INTELLIGENCE LABORATORY

INDICE DEI CONTENUTI

"Dark Mirror" è un report realizzato dagli esperti di Dark Lab, un sotto gruppo specializzato in Cyber Threat Intelligence (CTI) di Red Hot Cyber. Grazie al costante monitoraggio delle attività nel mondo underground, abbiamo redatto un'analisi approfondita sul fenomeno ransomware in Italia, per l'anno 2024.

Il nostro obiettivo è informare un pubblico sempre più vasto, contribuendo a rendere l'Italia più resiliente agli attacchi informatici. Attraverso analisi dettagliate e dati raccolti, offriamo una visione chiara delle attuali sfide nella sicurezza cibernetica, promuovendo consapevolezza e misure preventive efficaci.

METODOLOGIA

La nostra metodologia si basa su un approccio multi-strato che integra diverse tecniche di raccolta e analisi dei dati per fornire una comprensione approfondita e aggiornata delle minacce informatiche, con un focus particolare sul ransomware.

1 RACCOLTA DATI

- **Monitoraggio delle Underground:** Utilizziamo strumenti avanzati per monitorare costantemente forum, mercati underground e altre piattaforme clandestine dove avvengono scambi di informazioni e strumenti legati al ransomware;
- **Threat Hunting:** Effettuiamo attività proattive di threat hunting su vasta scala per identificare nuove varianti di ransomware e metodi di attacco emergenti;
- **Partnership e Collaborazioni:** Collaboriamo con altre organizzazioni e enti governativi per condividere informazioni e rafforzare la nostra capacità di rilevamento e di analisi.

2 ANALISI

- **Indicatori di Compromissione (IOC):** Analizziamo gli indicatori di compromissione raccolti durante le attività di monitoraggio e threat hunting per identificare pattern e tendenze;
- **Tecniche, Tattiche e Procedure (TTPs):** Studiamo le tecniche, tattiche e procedure utilizzate dai threat actors per capire le loro strategie e prevedere le loro mosse future. Seguiamo i nuovi Threat Actors per comprendere appieno le nuove TTPs adottate;
- **Analisi Forense:** Siamo in contatto con aziende ed enti che svolgono analisi forensi su campioni di ransomware per capire le modalità di infezione e le misure di evasione adottate dai cyber criminali.

3 REPORTING

- **Dati Aggregati:** Utilizziamo strumenti da noi realizzati per effettuare analisi e tendenze sui dati raccolti e per aggregare e visualizzare le informazioni, facilitando l'interpretazione e la comunicazione dei risultati;
- **Case Studies:** analizziamo i pattern negli attacchi ransomware recenti per fornire esempi concreti delle minacce e delle loro conseguenze. Svolgiamo interviste ai Threat Actors per comprendere appieno le loro TTPs.
- **Tendenze e Previsioni:** Analizziamo le tendenze globali e locali nel campo del ransomware sia a livello di difesa e di attacco. Cerchiamo di offrire consapevolezza del rischio oltre che previsioni sulle future evoluzioni del panorama delle minacce ransomware.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

ANALISI E TENDENZE

TENDENZE GLOBALI, TENDENZE PANORAMA ITALIANO, TRENDS DELLE MINACCE

A cura di Pietro Melillo, Inva Malaj, Luca Galuppi, Andrea Mario Muscarà

ANALISI E TENDENZE

ANALISI GLOBALI – PAESI PIU'COLPITI

Panoramica Generale: Nel corso del 2024, Dark Lab ha documentato un totale di **5333 vittime di attacchi ransomware a livello globale**. Questo numero, sebbene significativo, rappresenta solo una frazione delle vittime reali.

Molti attacchi non vengono riportati nei data leak site (DLS), dove i cybercriminali pubblicano i dati sottratti come parte di una strategia di doppia estorsione. Pertanto, i dati disponibili riflettono esclusivamente gli attacchi confermati.

TOP10 Paesi maggiormente colpiti

5333

Le organizzazioni mondiali che sono state colpite durante l'anno 2024

2748

Le organizzazioni statunitensi che sono state colpite durante l'anno 2024

Panoramica Geografica e Settoriale: Il ransomware continua a colpire indiscriminatamente, interessando sia paesi sviluppati che in via di sviluppo. Gli Stati Uniti guidano la classifica con **2748 vittime documentate**, seguiti da **Canada (283), Regno Unito (277), Germania (168)** e **Italia (149).** Anche Francia, Brasile, India, Spagna e Australia riportano numeri rilevanti, dimostrando che il ransomware è un problema globale che non risparmia nessuna nazione. I settori maggiormente colpiti includono l'industria, i servizi e la tecnologia, confermando l'impatto devastante di questi attacchi sull'economia globale e sulla quotidianità delle persone. La forte concentrazione negli Stati Uniti evidenzia una combinazione di vulnerabilità infrastrutturali e maggiore attività criminale in questa regione.

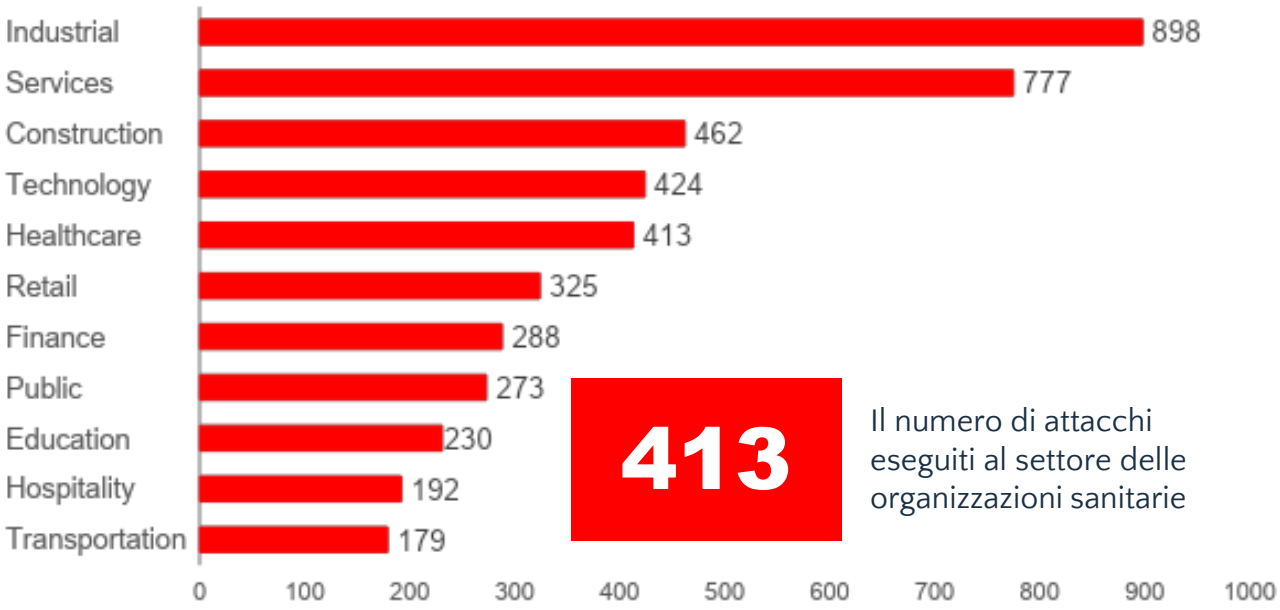
Il 2024 ha dimostrato che **il ransomware rimane una minaccia persistente e in crescita.** L'ampia diffusione geografica e il forte impatto settoriale richiedono risposte coordinate e investimenti in tecnologie di sicurezza avanzate per mitigare i rischi e proteggere le infrastrutture critiche globali.

ANALISI E TENDENZE

ANALISI GLOBALI - SETTORI PIU' COLPITI

Dark Lab ha analizzato i dati relativi ai settori economici colpiti dagli attacchi ransomware nel 2024, identificando quali segmenti dell'economia siano maggiormente esposti a questa minaccia. Principali Evidenze: I settori industriale e dei servizi risultano i più colpiti, con vulnerabilità critiche nelle infrastrutture IT e nella gestione dei dati. Tecnologia e sanità presentano un'elevata esposizione, con rischi significativi per la protezione delle informazioni sensibili. I settori a rischio medio-basso non sono immuni, ma subiscono attacchi con impatti generalmente meno critici.

TOP10 Settori maggiormente colpiti (Worldwide)



413

Il numero di attacchi eseguiti al settore delle organizzazioni sanitarie

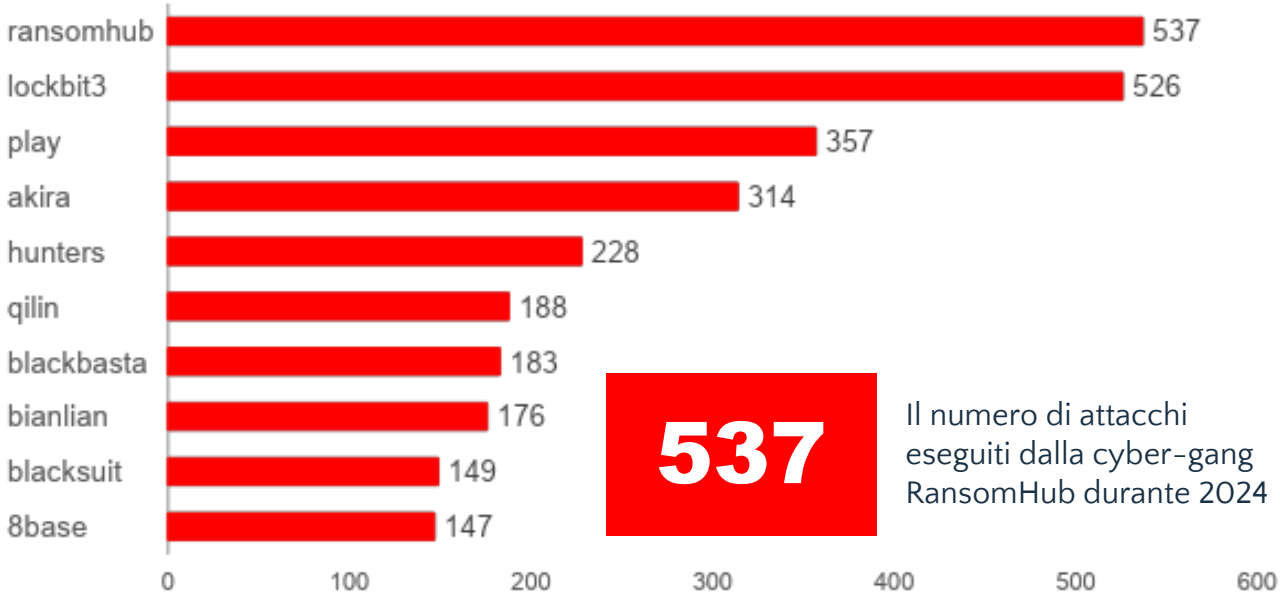
Distribuzione degli Attacchi per Settore: Il settore più colpito dagli attacchi informatici è l'industria, con **898 attacchi registrati**. Questo settore rappresenta il principale bersaglio a causa delle vulnerabilità sistemiche presenti nelle infrastrutture IT. Segue il settore dei servizi, con **777 attacchi**, esposto a elevati rischi nella gestione di dati critici. Il comparto delle costruzioni, con **462 attacchi**, è caratterizzato da sistemi informativi spesso frammentati, il che può portare a un potenziale impatto economico significativo. Il settore tecnologico, con 424 attacchi, risulta altamente esposto per il valore intrinseco dei dati trattati ed è particolarmente attrattivo per i cybercriminali. La sanità, con **413 attacchi**, rappresenta un settore *critico per la continuità operativa e presenta un alto rischio di compromissione dei dati sensibili dei pazienti*. I settori a rischio medio-basso comprendono il retail, con **325 attacchi**, il settore finanziario, con **288 attacchi**, il comparto pubblico, con **273 attacchi**, l'educativo, con **230 attacchi**, e l'ospitalità, con **187 attacchi**.
È quindi essenziale rafforzare la sicurezza nei settori più colpiti, con particolare attenzione alla sanità, dove le vulnerabilità minacciano servizi essenziali. Misure efficaci sono cruciali per mitigare i rischi e garantire la resilienza digitale.

ANALISI E TENDENZE

ANALISI GLOBALI – THREAT ACTORS PIU' ATTIVI

Il grafico evidenzia i gruppi criminali più attivi nella scena del Ransomware-as-a-Service (RaaS) nel corso del 2024. RansomHub, emerso a febbraio 2024, ha totalizzato 537 attacchi nel corso dell'anno, diventando il gruppo RaaS più attivo e pericoloso. Il gruppo utilizza tecniche sofisticate, tra cui backdoor basate su Python e strumenti legittimi come TDSSKiller di Kaspersky, per disabilitare le difese delle vittime.

TOP10 Threat Actors maggiormente attivi (Worldwide)



537

Il numero di attacchi eseguiti dalla cyber-gang RansomHub durante 2024

Il panorama del Ransomware-as-a-Service (RaaS) nel 2024: Nel 2024, il gruppo **RansomHub** si conferma come il più attivo, con 537 attacchi superando **LockBit3**, che con 526 attacchi evidenzia una notevole resilienza. Altri attori rilevanti includono il gruppo **Play**, con 357 attacchi, e i gruppi emergenti **Akira** (314 attacchi) e **Hunters** (228 attacchi), che continuano a crescere e ad adattarsi. Contestualmente, gruppi come **Qilin**, **BlackBasta** e **BianLian** contribuiscono a frammentare ulteriormente il panorama criminale, segnalando un'incrementata diffusione e diversificazione delle minacce. RansomHub continua a dominare il settore con un volume di attacchi senza precedenti, mentre LockBit 3 dimostra una straordinaria capacità di resilienza, malgrado i continui tentativi di smantellamento delle sue operazioni. L'espansione costante di gruppi come Play e Akira è un chiaro indicatore della crescente sofisticazione delle reti criminali, che sono in grado di aggirare sistemi di difesa avanzati e sfruttare le ultime tecnologie per massimizzare i danni. Il 2024 evidenzia, dunque, l'urgenza di risposte coordinate e di investimenti mirati nella cybersecurity, al fine di contrastare un ecosistema criminale in continua evoluzione, popolato da attori sempre più organizzati e pericolosi.

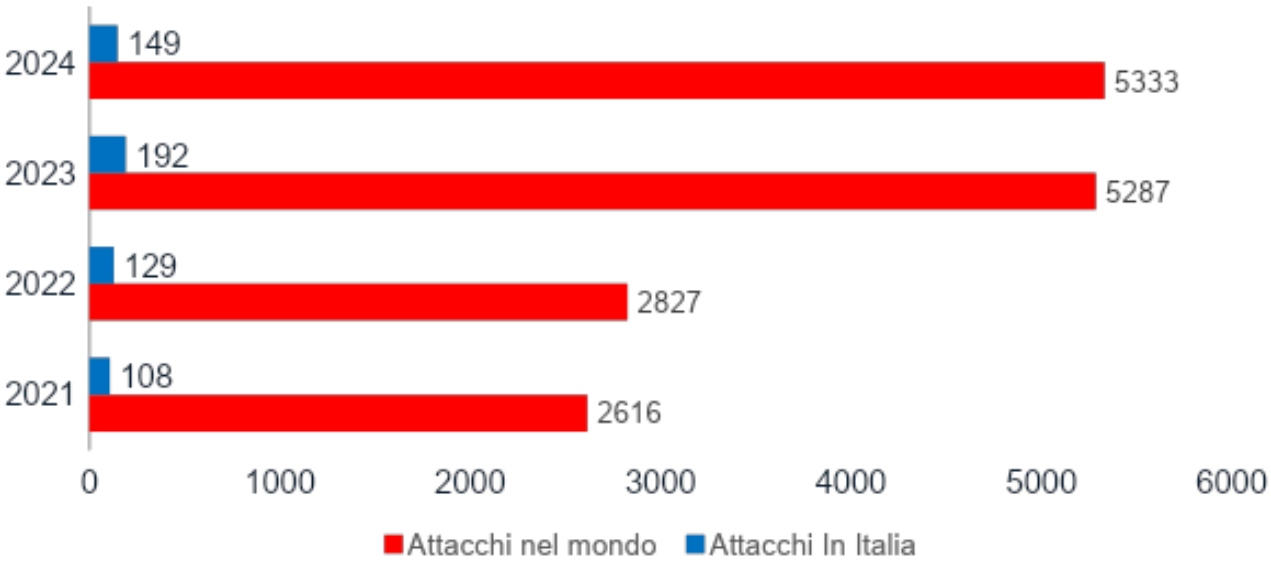
ANALISI E TENDENZE

TENDENZE

I dati relativi agli attacchi ransomware negli ultimi quattro anni rivelano un quadro preoccupante di crescita esponenziale fino al 2023, con un possibile rallentamento nel 2024. Per il comparto Italia rispetto al 2023, c'è stata una importante flessione delle vittime che sono passate dalle 192 del 2023 alle 149 del 2024.

Il grafico presentato mette in evidenza la progressione annuale degli attacchi pubblicati sui data leak site (DLS), distinguendo tra quelli globali e quelli avvenuti in Italia.

TREND Year over Year degli attacchi ransomware in Italia e nel mondo



A livello globale, si osserva una crescita costante degli attacchi ransomware, che passano da **2616** nel 2021 a **5333** nel 2024. Questo rappresenta più del doppio degli attacchi registrati quattro anni prima. Anche in Italia, sebbene con numeri assoluti inferiori, il trend è analogo: gli attacchi sono passati da 108 nel 2021 a 192 nel 2023, con una forte diminuzione nel 2024, in cui si registrano 149 attacchi.

Questa flessione potrebbe essere legata a vari fattori, quali l'adozione di misure di sicurezza più efficaci, un incremento nella consapevolezza delle aziende e dei cittadini, o cambiamenti strategici da parte dei criminali informatici.

È fondamentale sottolineare che questi dati riguardano attacchi riportati nei DLS, che tipicamente rappresentano aziende che hanno rifiutato di pagare il riscatto.
Tuttavia, essi costituiscono solo una porzione degli attacchi effettivi, considerando che molti incidenti non vengono denunciati per motivi reputazionali o di altro tipo. Nonostante la diminuzione relativa degli attacchi in Italia nel 2024, il rischio globale rimane elevato e in continua evoluzione.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

ANALISI E TENDENZE

ANALISI COMPARTO ITALIA

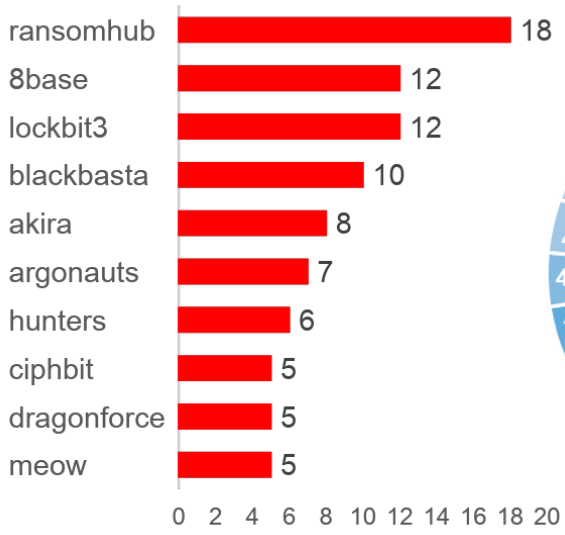
A cura di Luca Galuppi e Marco Mazzola

ANALISI E TENDENZE

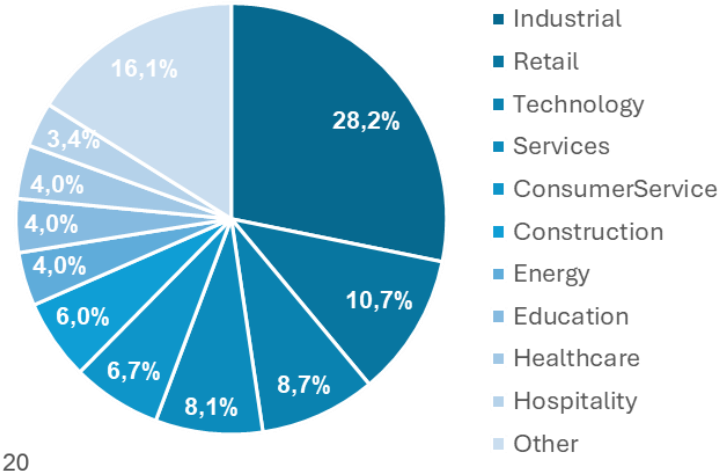
ANALISI COMPARTO ITALIA

L'analisi degli attacchi informatici in Italia nel 2024 mostra una chiara concentrazione delle minacce in alcuni settori chiave: Secondo il grafico sui settori più colpiti, il settore industriale è il principale bersaglio, seguito da retail, tecnologia e servizi. I settori delle infrastrutture critiche (energia e sanità) mostrano percentuali relativamente più basse ma comunque significative, considerando l'impatto potenziale di un attacco riuscito in questi ambiti. Questi dati evidenziano l'elevato rischio per le infrastrutture critiche e i settori strategici dell'economia.

TOP10 Threat Actors maggiormente attivi



TOP10 Settori più colpiti



Osservando i Threat Actors, si nota che il gruppo **RansomHub** è il più attivo, con **18** attacchi documentati, seguito da **8Base** e **LockBit 3**, entrambi con 12 attacchi. Altri gruppi come **BlackBasta** (**10 attacchi**), **Akira** (8 attacchi) e **Argonauts** (7 attacchi) continuano a rappresentare minacce significative.

Sebbene gruppi come **Hunters**, **Ciphbit**, **DragonForce** e **Meow** abbiano un numero inferiore di attacchi (5-6 ciascuno), la loro attività non deve essere sottovalutata. Questi risultati mostrano come la distribuzione degli attacchi sia cambiata negli anni. Il settore dei servizi, ad esempio, mostra una crescita significativa negli attacchi, mentre il settore tecnologico sembra registrare un calo. È evidente, tuttavia, che l'industria rimane il bersaglio principale, richiedendo un'attenzione prioritaria nella definizione di strategie di difesa avanzate per proteggere le infrastrutture più critiche.

ANALISI E TENDENZE

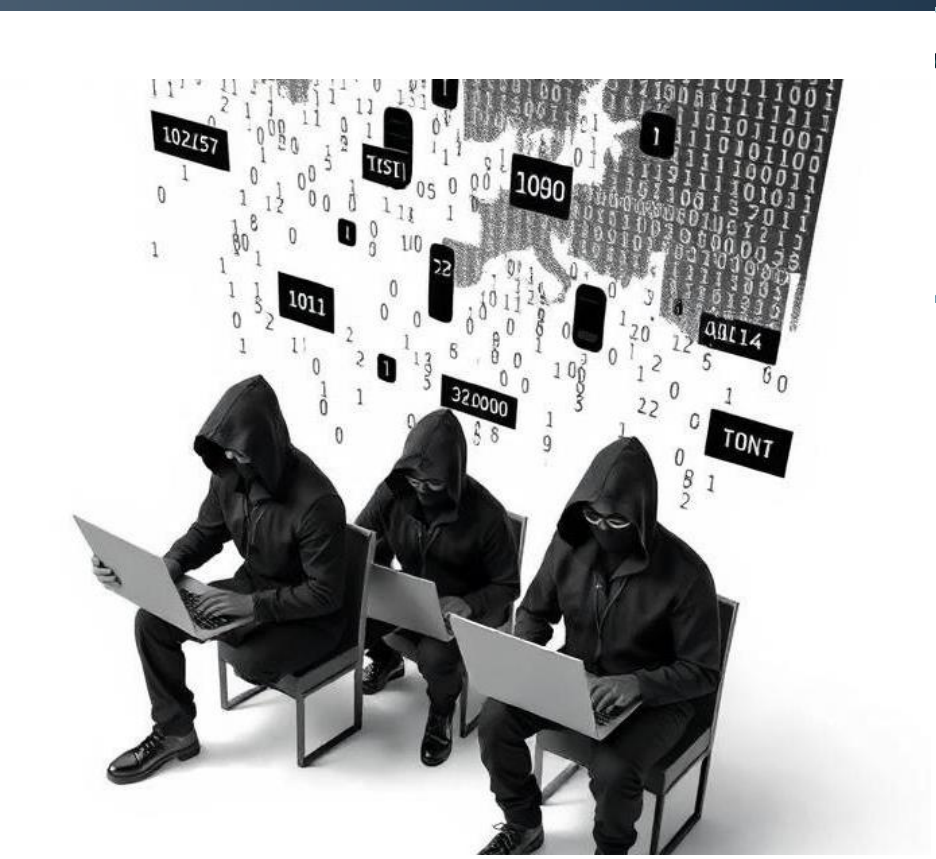
COMPARTO ITALIA

L'analisi dei **76 attacchi documentati in Italia** durante il periodo di osservazione rivela una realtà allarmante: la crescente esposizione dei settori strategici del nostro Paese a **minacce informatiche sempre più sofisticate**. Al primo posto nella lista dei bersagli figura il comparto **Manufacturing**, con circa **13 attacchi registrati**. Questo dato sottolinea la vulnerabilità di un settore fondamentale per l'economia italiana. **Food and Drinks**, con **6 attacchi**, e **Technologies**, con **8 episodi rilevati**, completano il podio, dimostrando che i cybercriminali stanno colpendo aree cruciali della filiera produttiva e tecnologica italiana.

Questa escalation non è casuale, ma riflette un trend globale di intensificazione delle campagne cyber contro infrastrutture critiche. Tra i principali responsabili troviamo gruppi come **RansomHub**, che ha sferrato **10 attacchi** mirati, concentrando le sue offensive nei mesi di luglio e settembre. Segue **Argonauts** con **7 rivendicazioni** tra novembre e dicembre. **BlackBasta** registra **5 attacchi**, mentre **Meow**, **Dragonforce** e **Hunters** si attestano su **4 operazioni** ciascuno. Altri attori come **Akira** e **Medusa** mantengono una presenza costante, pur con un numero di attacchi più contenuto, compreso tra **2 e 3**.

ANALISI E TENDENZE

COMPARTO ITALIA



Nel **secondo semestre del 2024**, l'Italia è diventata terreno fertile per i gruppi **RaaS (Ransomware-as-a-Service)**. Sebbene il numero di attacchi registrati sia inferiore rispetto a giganti come Stati Uniti e Regno Unito, il nostro Paese ha sperimentato **picchi d'attività significativi**, confermando che il panorama cyber italiano è sotto pressione. **Non è solo una questione di numeri**, ma di impatto: ogni attacco ha il potenziale di compromettere filiere produttive, danneggiare l'innovazione tecnologica e mettere a rischio la sicurezza economica nazionale.

È evidente che l'Italia non può permettersi di sottovalutare queste minacce. **Investire in misure di difesa informatica avanzate non è più un'opzione, ma una necessità strategica** per proteggere i settori vitali dell'economia e contrastare

ANALISI E TENDENZE

COMPARTO ITALIA

l'inarrestabile avanzata di cybercriminali sempre più organizzati e spregiudicati.

Nel secondo semestre del 2024, l'Italia ha registrato una crescente attività da parte di cybercriminali, con attacchi documentati in maniera consistente mese dopo mese. Analizzando i dati, emerge un andamento altalenante: luglio ha visto **13 attacchi**, avviando il semestre con un livello di minaccia già elevato. Agosto ha registrato un ulteriore incremento, con **14 attacchi**, il valore più alto nella prima parte del periodo. Settembre ha mostrato una relativa diminuzione, con **9 attacchi**, pur rappresentando un numero rilevante. Ottobre ha ripreso il trend ascendente, con **13 attacchi**, dimostrando la costante pressione esercitata dai cybercriminali. Novembre ha segnato un nuovo massimo con **16 attacchi**, il dato più alto del semestre, indicando un'intensificazione delle attività malevole. Dicembre, pur mostrando un calo rispetto al mese precedente, ha registrato **10 attacchi**, confermando che le festività non sono state un deterrente per i cybercriminali. Questa distribuzione mensile evidenzia una persistenza costante della minaccia, con picchi significativi che richiedono un'attenzione strategica continua.

A luglio, il **Ministero della Cultura** italiano è stato vittima di un attacco ransomware attribuito al gruppo criminale **Mad Liberator**. Il 17 luglio, l'attacco ha comportato l'esfiltrazione e la successiva pubblicazione di dati sensibili, sebbene la quantità precisa delle informazioni rubate non fosse ancora stata determinata. Questo evento evidenzia la crescente minaccia rappresentata da attori malevoli che mirano a colpire istituzioni governative, guadagnando visibilità e applicando pressione strategica.

Ad agosto, è stato il turno dell'**ENEA**, l'Agenzia Nazionale per le Nuove Tecnologie, l'Energia e lo Sviluppo Economico

ANALISI E TENDENZE

COMPARTO ITALIA

Sostenibile, colpita da un attacco ransomware di ampia portata rivendicato dal gruppo **Hunters**. L'attacco ha portato all'esfiltrazione di **219,9 GB** di dati, un incidente che ha messo in evidenza la vulnerabilità crescente delle infrastrutture critiche italiane e l'interesse strategico dei cybercriminali verso enti pubblici e istituzioni scientifiche di rilievo.

A settembre, **l'Università di Genova** è stata presa di mira dal gruppo **RansomHub**, che ha sottratto **18 GB** di dati sensibili. Il tipico modus operandi del ransomware ha comportato la minaccia di diffondere o vendere le informazioni se il riscatto non fosse stato pagato.

Questo attacco sottolinea non solo la crescente minaccia per il settore accademico, ma anche la vulnerabilità delle istituzioni italiane a questi tipi di attacchi, facendo emergere la necessità di proteggere meglio i dati accademici e la proprietà intellettuale.

ANALISI E TENDENZE

COMPARTO ITALIA

Ottobre ha visto l'attacco a **Smeg**, l'azienda di elettrodomestici, che ha subito la compromissione dei suoi sistemi aziendali da parte del gruppo **LockBit**. L'esfiltrazione di dati sensibili è stata seguita da minacce di divulgazione delle informazioni riservate se non fosse stato pagato un riscatto. Questo attacco evidenzia la crescente vulnerabilità di aziende anche in settori non direttamente legati alla tecnologia.

Infine, novembre ha segnato un incremento significativo con l'emergere del gruppo ransomware **Argonauts**, che ha preso di mira l'Italia con una serie di attacchi. In un solo giorno, il gruppo ha rivendicato ben 10 attacchi, sei dei quali localizzati nel nostro Paese. Questo episodio segna una tendenza preoccupante e l'urgenza di rafforzare le difese contro il ransomware, specialmente nei settori più vulnerabili e strategici del paese.

Le statistiche di settore delineano un quadro chiaro delle priorità degli attori malevoli. Il settore **Manufacturing** ha subito **13 attacchi**, confermandosi il comparto più bersagliato. Questo dato sottolinea come i cybercriminali puntino a

ANALISI E TENDENZE

COMPARTO ITALIA

interrompere la filiera produttiva e a sfruttare la dipendenza delle aziende da sistemi altamente digitalizzati. Non meno allarmante è la situazione nel comparto **Food and Drinks Business,** con **6 attacchi registrati**. Spesso percepito come meno protetto, questo settore è in realtà un bersaglio strategico per i criminali, vista la sua importanza critica e la possibilità di richiedere riscatti elevati sfruttando l'urgenza di ripristinare le operazioni. Il settore **Technologies**, con **8 attacchi**, continua a essere un obiettivo redditizio, sia per il valore dei dati che per l'impatto delle loro innovazioni sul mercato.

Questi tre comparti rappresentano la spina dorsale dell'economia italiana e, di conseguenza, il principale interesse per i cybercriminali, che mirano a massimizzare l'impatto delle loro operazioni.

La maggior parte degli attacchi si è concentrata nel nord del Paese, un dato che non sorprende considerando la densità imprenditoriale e il livello di digitalizzazione di queste aree. Regioni come **Lombardia, Veneto ed Emilia-Romagna** si confermano tra i bersagli preferiti, con i cybercriminali che puntano alle infrastrutture critiche e alle aziende leader nei settori industriali e tecnologici. Questa localizzazione geografica riflette anche un paradosso: più una regione è avanzata dal punto di vista tecnologico, più è vulnerabile agli attacchi informatici. Le aziende con un elevato livello di digitalizzazione spesso rappresentano bersagli redditizi per i cybercriminali, che mirano a compromettere dati sensibili, interrompere le attività operative e richiedere riscatti elevati.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

A cura di Carlo Mauceli

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

"*La tecnologia avanzata è l'arma più affilata dello Stato moderno. Se i paesi occidentali sono stati in grado di dominare il mondo in epoca moderna è anche perché detenevano il primato tecnologico*" [Xi Jinping].

Sam Altman, il CEO di OpenAI, la startup americana che il 30 novembre 2022 ha lanciato ChatGPT, il primo Large Language Model (LLM) messo a disposizione del pubblico che in circa due mesi aveva raggiunto cento milioni di utenti, si paragona molto spesso a Robert Oppenheimer, coordinatore del progetto Manhattan, ossia il gruppo di ricerca sulla prima bomba atomica. Altman ne cita spesso una frase diventata famosa, "***Technology happens because it's possible***".

Sam Altman CEO di OpenAI

Letteralmente, "*Una tecnologia esiste perché è possibile*", tanto da arrivare a chiedersi "*Sto facendo qualcosa di molto buono o qualcosa di molto cattivo?*"

Senza ombra di dubbio, come per lo più accade con l'avvento delle nuove tecnologie, in merito all'intelligenza artificiale (AI) è stato sviluppato un marketing della paura, convinti che l'idea di avere all'interno di un dispositivo, che fosse uno smartphone, un tablet o un pc, una sorta di piccola bomba atomica sarebbe stata estremamente attraente per moltissime persone. In realtà, come dimostrato successivamente, molti gruppi di ricerca lavoravano sugli LLM da parecchio tempo e quello di OpenAI è stato il primo caso in cui venne reso pubblico il risultato.

In ogni caso, la campagna divulgativa ha avuto successo, nel senso che l'interesse è esploso, il suo utilizzo è cresciuto in maniera esponenziale così come i suoi utilizzatori e, parallelamente, è cresciuto anche il timore, e, di conseguenza, l'esigenza di una regolamentazione. I sondaggi, al riguardo, sono stati molto interessanti.

Nel **2021**, una ricerca sulla percezione dei rischi legati all'uso dell'AI condotta in 121 paesi del mondo mostrava come in Europa, Asia orientale e sudorientale e Australia prevalesse la

ANALISI E TENDENZE

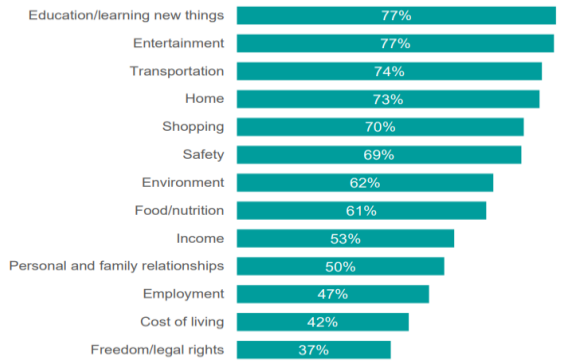
IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

fiducia in un effetto positivo della tecnologia, mentre nelle Americhe, in Africa e nell'Asia meridionale prevaleva il timore. Nel gennaio **2022**, un sondaggio condotto da Ipsos realizzato in 28 paesi del mondo mostrava risultati simili ma con una diminuzione in termini di fiducia che iniziava a prendere piede, soprattutto, in Europa.

	Global Country Average	Argentina	Australia	Belgium	Brazil	Canada	Chile	China	Colombia	Germany	Spain	France	Great Britain	Hungary	India	Italy	Japan	South Korea	Mexico	Malaysia	Netherlands	Peru	Poland	Russia	Saudi Arabia	Sweden	Turkey	United States	South Africa
I have a good understanding of what artificial intelligence is	64%	64%	59%	60%	69%	59%	76%	67%	71%	50%	62%	50%	57%	67%	72%	42%	41%	72%	74%	61%	65%	76%	66%	75%	73%	60%	68%	63%	78%
Products and services using artificial intelligence will profoundly change my daily life in the next 3-5 years	60%	60%	50%	52%	61%	44%	67%	80%	65%	44%	56%	45%	46%	55%	74%	53%	53%	76%	65%	71%	53%	71%	56%	60%	80%	50%	73%	46%	72%
Products and services using artificial intelligence make my life easier	60%	59%	46%	49%	65%	44%	70%	87%	71%	45%	59%	39%	45%	50%	72%	54%	52%	74%	73%	71%	47%	74%	58%	64%	80%	46%	71%	41%	67%
Products and services using artificial intelligence have more benefits than drawbacks	52%	55%	37%	38%	57%	32%	63%	78%	64%	37%	53%	31%	38%	49%	71%	50%	42%	62%	65%	65%	33%	70%	48%	53%	76%	40%	60%	35%	57%
I know which types of products and services use artificial intelligence	50%	47%	38%	37%	58%	36%	59%	76%	62%	37%	46%	34%	37%	38%	69%	45%	32%	60%	62%	61%	41%	63%	52%	57%	69%	37%	60%	39%	57%
I trust companies that use artificial intelligence as much as I trust other companies	50%	55%	36%	40%	50%	34%	56%	76%	57%	42%	50%	34%	35%	48%	68%	48%	39%	46%	60%	61%	38%	60%	51%	52%	73%	39%	63%	35%	56%
Products and services using artificial intelligence have profoundly changed my daily life in the past 3-5 years	49%	53%	37%	37%	51%	32%	58%	73%	58%	31%	49%	32%	33%	38%	67%	41%	30%	62%	62%	65%	40%	65%	45%	50%	72%	30%	60%	36%	56%
Products and services using artificial intelligence make me nervous	39%	33%	51%	42%	35%	49%	36%	30%	39%	37%	48%	32%	50%	31%	53%	26%	20%	32%	38%	48%	36%	35%	30%	28%	51%	37%	48%	52%	52%

Opinioni riguardo l'intelligenza artificiale suddivise per country (fonte Ipsos)

L'autunno del **2023**, dopo il lancio di ChatGPT, ha siglato un deciso cambiamento sia negli Stati Uniti che in Europa nella convinzione che l'industria debba investire di più in misure di sicurezza per proteggere il pubblico ma contemporaneamente nel ritenere che le tecnologie di AI siano sicure ed affidabili e questa percezione, non sempre accomunata dalla comprensione, è risultata più elevata nei Paesi emergenti rispetto ai Paesi ad alto reddito.



Opinioni sulle aree che avranno maggiori vantaggi dalle AI (fonte Ipsos)

Tutto ciò non può che indurci ad una serie di domande. In primo luogo, quanto ne sanno realmente le persone dell'AI? Secondariamente, siamo così certi che il marketing della paura sia un'idea geniale? **E, per finire, quali saranno gli scenari sociali, geopolitici ed economici che l'AI riuscirà a produrre? Una cosa è certa; l'AI ha avuto e sta avendo il "merito" di scuotere le coscienze,** sta creando sia effetti positivi che

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

negativi ad una velocità mai vista prima e sta sempre più creando nuovi equilibri a livello geopolitico ad un ritmo estremamente veloce. Nel corso della storia i progressi tecnologici hanno avuto un'evoluzione tale per cui la loro diffusione, in tutto il mondo, è avvenuta in maniera relativamente lenta. Al contrario, appare chiaro che l'attuale era dell'intelligenza artificiale ha il potenziale per essere dirompente. **L'AI sta già dimostrando il proprio impatto sulla sicurezza nazionale e sulla forza economica.** Col tempo l'AI **sconvolgerà gli equilibri già precari del sistema internazionale.**

Gli Stati capaci di adottare rapidamente e completamente tali tecnologie potrebbero ottenere vantaggi economici e di sicurezza significativi e l'AI potrebbe fornire loro gli strumenti per plasmare il futuro del pianeta. È ovvio, altresì, che non possiamo conoscere gli impatti geopolitici, geoeconomici e sociali che l'intelligenza artificiale e le altre tecnologie emergenti avranno quando si diffonderanno a livello locale, nazionale e mondiale.

Negli ultimi trent'anni, i maggiori progressi globali nel campo dell'intelligenza artificiale hanno avuto origine nel **settore commerciale** ma oggi stiamo assistendo a una rapida evoluzione dell'AI in tutti i settori; non da ultimo, quello cibernetico. L'ingresso e la pervasività dell'AI negli attacchi informatici rappresenta una grave minaccia per il normale funzionamento dello Stato. Si può manifestare attraverso azioni come l'interruzione delle reti elettriche nazionali, lo spegnimento di centrali nucleari, la paralisi dei trasporti nazionali e dei sistemi sanitari, il caos nei mercati finanziari. Non stiamo fantasticando. Non si tratta

Dal mio punto di vista è incredibile come non venga compreso o, forse, non lo voglia essere perché fa comodo a chi detiene il potere, sia esso politico od economico. In questo scenario, non pensare all'Italia e, in misura minore, all'Europa è impossibile. Arrancano entrambe pagando un gap tecnologico di decenni e non è un caso che il numero di regolamentazioni sia cresciuto in maniera esponenziale. La tecnologia o la gestisci o la combatti. Non ci sono molte alternative.

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

INTELLIGENZA ARTIFICIALE E CYBER

In un panorama in cui tecnologia, politica, economia e società sono legate da un filo sempre più stretto, come abbiamo anticipato, l'evoluzione dell'intelligenza artificiale ha anche aperto la strada **a nuove tecniche di attacco nonché alla possibilità di nuove attività malevole**. L'uso crescente dell'intelligenza artificiale negli attacchi informatici è **evolutivo e non rivoluzionario,** il che significa che migliora le minacce esistenti, come il ransomware, ma non trasforma radicalmente il panorama dei rischi nel breve termine.

Attualmente, l'intelligenza artificiale generativa viene utilizzata da attori di tutti i tipi, **statali e non statali, esperti e meno esperti,** per generare un "aumento delle capacità di ricognizione e di social engineering, rendendo entrambi i compiti "più efficaci ed efficienti" ma anche "difficili da rilevare" per la vittima. L'intelligenza artificiale può agevolare "lo sviluppo di malware ed exploit, la ricerca di vulnerabilità e il lateral movement, rendendo più efficienti le tecniche esistenti.

L'AI WormGPT pensata per un uso criminale

Questi usi più sofisticati dell'intelligenza artificiale per migliorare i cyber-attacchi saranno probabilmente disponibili solo per gli attori più dotati ed il limite è rappresentato dalla necessità per gli sviluppatori di avere accesso a dati di alta qualità per addestrare i

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

loro modelli. Attualmente, è solo una possibilità teorica che gli Stati più evoluti in tal senso dispongano di archivi di malware sufficientemente grandi per addestrare efficacemente un modello di intelligenza artificiale a questo scopo ma, man mano che si verificheranno esfiltrazioni di successo, i dati che alimentano l'intelligenza artificiale miglioreranno quasi certamente, consentendo operazioni informatiche più rapide e precise. In fondo, come sempre avviene, più è grande la base dati e maggiore sarà la conoscenza che l'AI avrà a disposizione.

I MALLA

L'impatto dell'intelligenza artificiale sulla minaccia informatica è disomogeneo, sia in termini di utilizzo da parte degli attori delle minacce informatiche sia in termini di aumento delle capacità. L'intelligenza artificiale **offre principalmente ai threat actor un aumento delle capacità nell'ingegneria sociale** e la capacità di riassumere i dati in modo rapido consentirà loro di identificare risorse di alto valore per l'analisi e l'esfiltrazione, migliorando il valore e l'impatto degli attacchi informatici nei prossimi anni. Le sfide della resilienza informatica diventeranno più complesse con lo sviluppo della tecnologia.

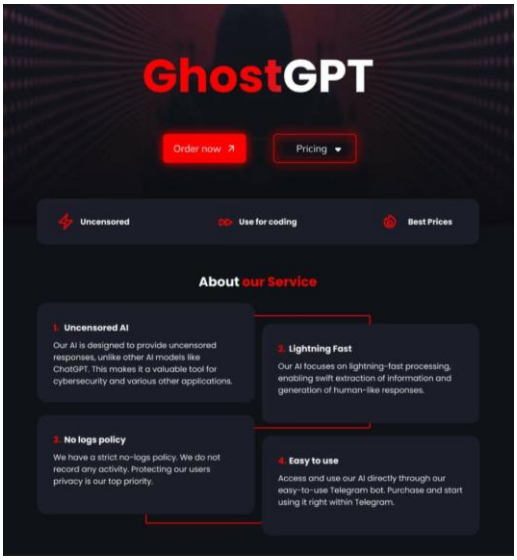
La GenAI e i modelli linguistici di grandi dimensioni renderanno le cose difficili per tutti, indipendentemente dal loro livello di comprensione della sicurezza informatica ed è proprio questo abbassamento del livello di ingresso nel mondo della criminalità informatica che preoccupa maggiormente.

In questo nuovo scenario, i Malla rappresentano una minaccia emergente e sofisticata. Si tratta di **veri e propri servizi che utilizzano modelli linguistici avanzati per automatizzare e potenziare attacchi informatici su larga scala** e sono stati realizzati e sfruttati dai threat actor che per primi hanno

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

compreso quanto l'intelligenza artificiale fosse in grado di offrire loro risorse, velocità e qualità nella generazione di nuove armi informatiche. L'analisi di questo nuovo fenomeno che sta crescendo in modo esponenziale è stata realizzata da alcuni ricercatori dell'Università di Bloomington che hanno descritto il tutto in questo paper: "**Demystifying Large Language Model Integrated Malicious Services**".



L'AI GhostGPT pensata per un uso criminale

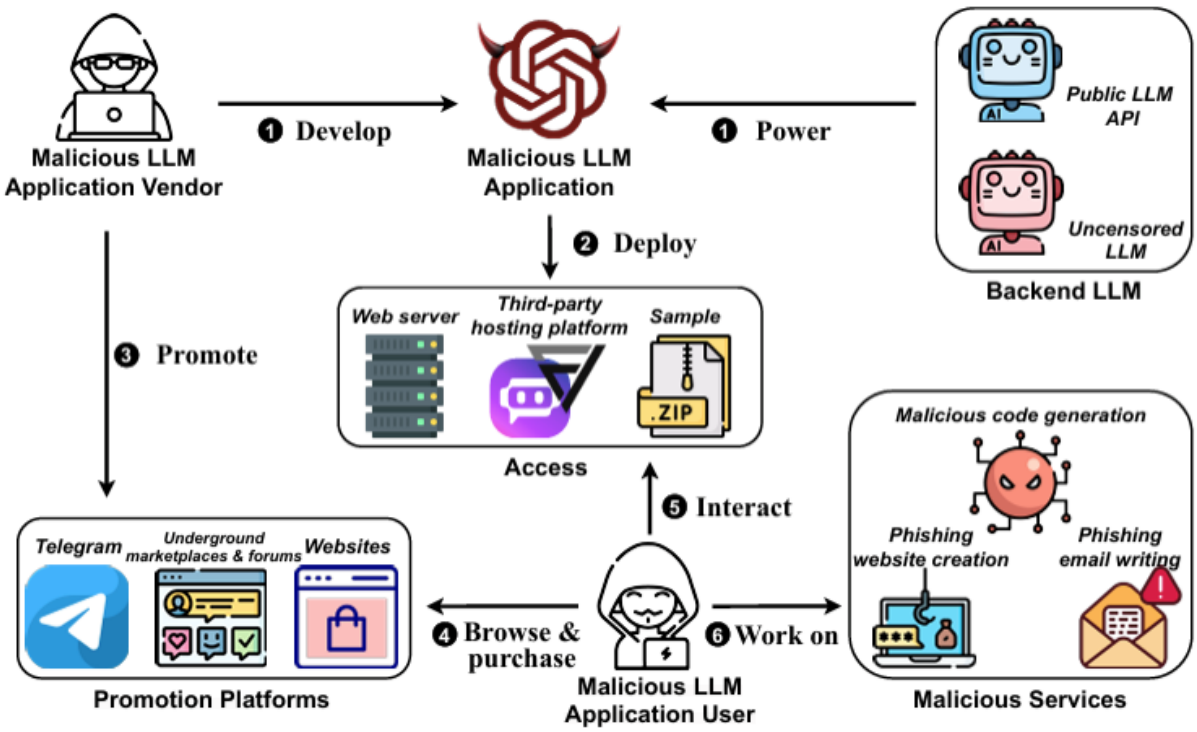
Come detto, i Malla sono servizi malevoli che integrano modelli linguistici di grandi dimensioni per creare strumenti di attacco estremamente efficaci. Si distinguono moltissimo dagli attacchi tradizionali, dal momento che non sono richieste competenze tecniche elevate. Infatti, i Malla permettono ai criminali informatici di sfruttare le capacità di intelligenza artificiale per generare codice malevolo, automatizzare campagne di phishing e costruire infrastrutture di attacco in modo rapido ed efficiente.

Questi servizi sono spesso disponibili su marketplace del dark web, dove vengono venduti a criminali con diverse competenze, dai principianti agli esperti. Pertanto, i Malla garantiscono l'abbassamento delle barriere d'ingresso per il cybercrime, permettendo di sferrare attacchi sofisticati quasi a chiunque con pochissimo sforzo, investimento e risorse.

Il modello è, tutto sommato, molto semplice.

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE



Nell'immagine: Un fornitore di Malla si impegna nell'uso improprio di API LLM pubbliche (ad esempio, OpenAI API, Llama API) o LLM non censurati (ad esempio, Luna AI Llama2 Uncensored, Pygmalion-13B) e li distribuisce per offrire servizi dannosi (❶), come la generazione di codice dannoso.

In genere, Malla viene distribuito come servizio Web o ospitato su una piattaforma di hosting LLMA di terze parti (ad esempio, Poe) (❷).

Dopo l'implementazione, il fornitore Malla lo promuove attraverso vari mercati e forum clandestini (❸).

Gli utenti che cercano strumenti automatizzati per generare codice dannoso o e-mail/siti Web di phishing scoprono questi elenchi Malla.

Una volta identificati, navigano sui siti web delle vetrine associate e procedono all'acquisto dei servizi Malla (❹).

Successivamente, gli utenti interagiscono con il Malla (❺) attraverso un'interfaccia utente grafica (GUI) o un'API, facilitando la generazione di codice dannoso o e-mail/siti di phishing (❻).

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

I Malla, come anticipavamo, sono per tutti e possono essere reperiti sul Darkweb dove vengono venduti sotto forma di abbonamento a prezzi ragionevolissimi.

Name	Price	Functionality			w/wo voucher copy	Infrastructure	Released time (Year/Month)	w. sample
		Malicious code	Phishing email	Scam site				
CodeGPT [11]	10 βytes*	●	○	◐	No	Jailbreak prompts	2023/04	Yes
MakerGPT [49]	10 βytes*	●	○	◐	No	Jailbreak prompts	2023/04	Yes
FraudGPT [30]	€90/month	●	●	●	No	-	2023/07	No
WormGPT [79, 80, 83]	€109/month	●	●	◐	No	-	2023/07	No
XXXGPT [28, 61, 84]	$90/month	●	○	○	Yes	Jailbreak prompts	2023/07	Yes
WolfGPT [77, 78]	$150	●	●	●	No	Uncensored LLM	2023/07	Yes
Evil-GPT [26]	$10	●	●	●	No	Uncensored LLM	2023/08	Yes
DarkBERT [16, 17]	$90/month	●	●	○	No	-	2023/08	No
DarkBARD [14, 15]	$80/month	◐	◐	○	No	-	2023/08	No
BadGPT [2, 3]	$120/month	◐	◐	◐	No	Censored LLM	2023/08	Yes
BLACKHATGPT [4–6]	$199/month	●	○	○	No	-	2023/08	No
EscapeGPT [23]	$64.98/month	●	◐	◐	No	Uncensored LLM	2023/08	Yes
FreedomGPT [32, 33]	$10/100 messages	●	◐	◐	Yes	Uncensored LLM	-	Yes
DarkGPT [18, 19]	$0.78/50 messages	●	◐	◐	Yes	Uncensored LLM	-	Yes

* βytes is the forum token of `hackforums.net`; ◐ indicates implicit mention.

Il loro principale utilizzo e i vari tipi di attacchi informatici che sono in grado di generare possono essere così riassunti:

- **1_Generazione di codice malevolo**. Si tratta di uno degli ambiti più comuni di utilizzo dei Malla. Grazie ad un LLM, i criminali sono in grado di realizzare script e malware ad hoc per sfruttare specifiche vulnerabilità nei sistemi. Questi modelli analizzano e comprendono il contesto e le specifiche tecniche di un determinato sistema target, generando codice in grado di eludere le difese tradizionali. Un esempio reale, peraltro documentato, è quello relativo ad un gruppo di hacker che ha utilizzato un servizio Malla per costruire exploit di tipo 0-day. Ciò ha permesso loro di attaccare sistemi critici senza essere rilevati per mesi. Il codice era così sofisticato che è riuscito ad eludere anche i sistemi di rilevamento avanzati basati su AI.

- **2_Creazione di Email di Phishing**. Questo è un ambito in cui i Malla sono estremamente efficaci. Utilizzando la comprensione del linguaggio naturale, i modelli linguistici possono generare email perfette dal punto di vista del social engineer, in grado di imitare perfettamente il tono e lo stile delle comunicazioni aziendali. Risulta chiaro che riconoscere l'inganno diventa estremamente complicato. Nella realtà, è noto il caso di

un'organizzazione finanziaria, vittima di una campagna di phishing altamente sofisticata. Le email generate hanno ingannato diversi dipendenti, compromettendo l'infrastruttura della vittima, esfiltrando informazioni sensibili e arrecando all'istituto una perdita finanziaria significativa. Nessun filtro anti-phishing è stato in grado di rilevare le email a causa del livello di sofisticazione e qualità con cui erano stato realizzate.

- **3_Creazione di Siti di Phishing**. Un altro utilizzo dei Malla è la creazione automatizzata di siti web di phishing. Si tratta di imitazioni di siti legittimi che hanno l'obiettivo di raccogliere dati sensibili quali le credenziali di accesso, le informazioni finanziarie e i dati personali. Anche in questo caso, la qualità dei siti realizzati è altissima il che ne impedisce il riconoscimento anche ai sistemi più esperti. Un caso accaduto è relativo ad un sito di e-commerce falso che è riuscito a truffare migliaia di clienti. Il sito era una copia pressoché identica di un noto rivenditore online, con tanto di certificati SSL ed uno stile molto simile. Gli utenti che hanno inserito le loro informazioni di pagamento sono stati oggetto di successive frodi finanziarie.

- **4_Automazione degli Attacchi di Social Engineering**. I Malla sono anche in grado di automatizzare attacchi di ingegneria sociale. Questi modelli sono in grado di analizzare grandi volumi di dati, identificare vulnerabilità umane e generare script che convincono le vittime a eseguire azioni compromettenti, come cliccare su link malevoli o fornire credenziali di accesso.

Esempio Reale: In una campagna di spear phishing, un Malla è stato utilizzato per creare profili social falsi che hanno interagito con le vittime per settimane, guadagnandosi la loro fiducia. Alla fine, le vittime sono state indotte a trasferire fondi a conti bancari controllati dagli hacker. L'intero processo è stato automatizzato, riducendo al minimo l'intervento umano da parte dei criminali. L'emergere dei **Malla** ha trasformato radicalmente il panorama della sicurezza informatica. Questi servizi non solo aumentano l'efficacia degli attacchi ma rendono anche più difficile la difesa contro di essi. Gli impatti più significativi sono:

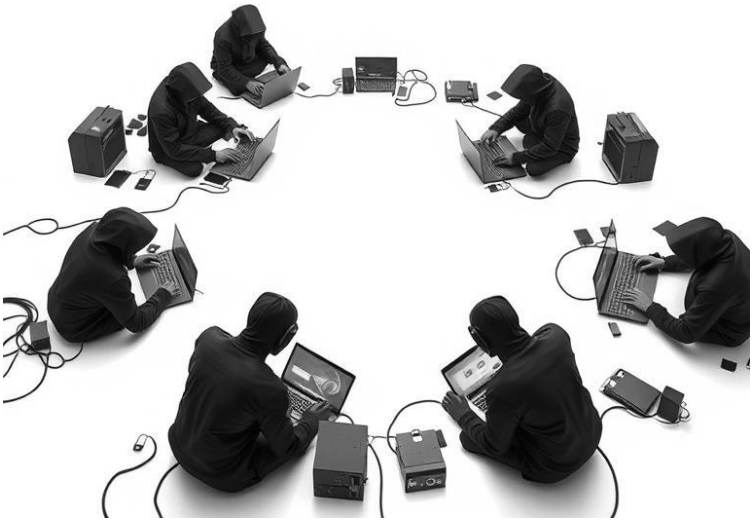
- **Aumento della Frequenza e della Complessità degli Attacchi:** i Malla abbattono il tempo e le risorse necessari per lanciare attacchi complessi aumentandone significativamente il numero.

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

- **Miglioramento della Qualità degli Attacchi:** La capacità dei LLM di generare contenuti realistici e personalizzati fa sì che la rilevazione e l'intercettazione degli attacchi stessi sia sempre più difficile. I sistemi di difesa tradizionali, basati su pattern e firme, spesso falliscono di fronte a queste minacce avanzate.
- **Riduzione della Barriera di Ingresso per il Cybercrime:** I Malla permettono la democratizzazione del cybercrime. Cosa significa? Significa che anche criminali con competenze tecniche limitate sono in grado di lanciare attacchi sofisticati con la conseguenza di un aumento nel numero di potenziali criminali.
- **Impatto Economico e Reputazionale:** Gli attacchi resi più "semplici" dall'utilizzo dei Malla possono causare danni economici significativi alle aziende con un conseguente danno di reputazione che può comportare la sfiducia da parte dei loro clienti.

Per contrastare i **Malla** è necessario avere un approccio avanzato e multi layer quale:



- **1_Sviluppo di AI Difensiva**. È necessario, in primo luogo, combattere ad armi pari e, dunque, bisogna sviluppare sistemi di intelligenza artificiale che siano in grado di rilevare e bloccare gli attacchi generati da questi servizi. L'AI utilizzata in ambito di difesa è in grado di analizzare modelli comportamentali, anomalie nel traffico di rete e altri indicatori di compromissione (IoC) in tempo reale, così da potere rispondere immediatamente alle minacce. Un esempio è quello relativo all'utilizzo di piattaforme AI che siano in grado di identificare tentativi di phishing generati da Malla attraverso l'analisi linguistica delle email. Il concetto è quello di avere un sistema in grado di apprendere continuamente stante la velocità evolutiva delle tecniche di attacco. In questo modo si alimenta la loro capacità di rilevamento, riducendo il rischio di compromissioni.

ANALISI E TENDENZE

IL LATO OSCURO DELL'INTELLIGENZA ARTIFICIALE

- **2_Educazione degli Utenti e Consapevolezza**. Un'altra strategia che è da sempre oggetto ritenuto chiave nell'ambito della prevenzione è l'educazione degli utenti. Rendere gli utenti consapevoli delle nuove metodologie di attacco è la base per poterli mettere nella condizione di riconoscere i segnali di pericolo e adottare comportamenti sicuri. Da questo punto di vista**,** è importante che le aziende definiscano e propongano programmi di formazione continua per i loro dipendenti, con simulazioni di attacchi di phishing e altre esercitazioni pratiche.
- **3_Collaborazione Internazionale**. Oggi, chi ha il potere tecnologico avrà anche quello politico e, dunque, dal momento che il cybercrime è un fenomeno globale, si richiede una cooperazione internazionale per monitorare, identificare e smantellare i Malla.

  Ad esempio, le operazioni condotte congiuntamente da Europol e aziende di cybersecurity hanno portato al sequestro di server utilizzati per operare servizi Malla, smantellando reti criminali e arrestando i responsabili.

- **4_Sviluppo di normative e regolamenti**. È altrettanto importante che l'utilizzo degli LLM venga normato al fine di evitare che possano essere utilizzati per scopi malevoli. Sarebbe utile introdurre normative per regolamentare l'uso e lo sviluppo dei modelli linguistici avanzati.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

A cura di Raffaela Crisci

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

Nel 2024, le forze dell'ordine internazionali hanno intensificato la loro lotta contro il cybercrime, portando avanti operazioni senza precedenti per smantellare le infrastrutture delle principali organizzazioni criminali informatiche. Attraverso azioni coordinate tra agenzie di sicurezza, forze di polizia e unità specializzate in cyber intelligence, le autorità hanno colpito con forza i gruppi ransomware più attivi, compromettendo le loro reti, sequestrando i loro server e arrestando figure chiave del panorama criminale. Queste operazioni non si sono limitate a semplici sequestri, ma hanno incluso anche tattiche di "interferenza massiccia", in cui le forze dell'ordine hanno infiltrato e sabotato i sistemi dei cybercriminali, diffondendo disinformazione al loro interno e minando la loro capacità operativa.

OPERAZIONE CRONOS

Nel 2023, LockBit si è confermato il gruppo RaaS (Ransomware-as-a-Service) più attivo per numero di attacchi, dominando la scena con la versione 3.0 del suo programma. Seguivano a distanza BlackCat e Play, mentre il rilascio della nuova versione 4.0, già annunciato, era atteso per il 2024.

A febbraio 2024, la task force Cronos ha colpito duramente LockBit, sequestrando uno dei suoi domini principali e compromettendo una parte significativa della sua infrastruttura interna. Operation Cronos, condotta da un'alleanza internazionale comprendente FBI, NCA ed Europol, si è protratta per tutto il 2024, caratterizzata da aggiornamenti provocatori rivolti a LockBitSupp, l'amministratore di LockBit. Gli eventi principapli sono stati i seguenti:

- **20 Febbraio 2024** – La task force ristruttura il dominio della quale hanno preso il controllo annunciando di aver smantellato parte dell'infrastruttura interna e di averne ottenuto accesso ai dati . Tra le informazioni ottenute sono incluse chiavi di decription, affiliati e l'identità di LockBit Supp. Il dominio è stato chiuso dopo 2 giorni

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

- **7 Maggio 2024 -** Le forze dell'ordine rivelano ufficialmente l'dentità di LockBit Supp, offrendo una ricompensa fino a 10 milioni di dollari per informazioni che conducano al suo arresto. Nello stesso annuncio, viene pubblicata la lista degli affiliati trovati nel pannello amministrativo, incluse le conversazioni con le vittime, e viene rilasciato un tool pubblico per decriptare i file delle vittime utilizzando le chiavi private sottratte. Viene inoltre smascherata la reale portata dei guadagni di LockBit, ben inferiori a quanto dichiarato.
- **1 Ottobre 2024 -** Il terzo atto di Operation Cronos porta alla luce la collaborazione tra LockBit ed Evil Corp, questi ultimi hanno utilizzato la piattaforma RaaS di LB per poter aggirare le sanzioni internazionali. Viene pubblicato lo schema relazionale del database SQL interno ed annunciate nuove sanzioni contro i responsabili.

Tra le varie fasi delle operazioni appena citate, entrambe le parti hanno avuto modo di esprimersi in maniera più o meno formale spiegando i retroscena di Cronos.

Nei giorni successivi al primo sequestro, LBSupp ha risposto tramite un messaggio sul suo DLS, sostenendo che l'azione della task force fosse motivata dall'attacco ransomware contro la Fulton County,

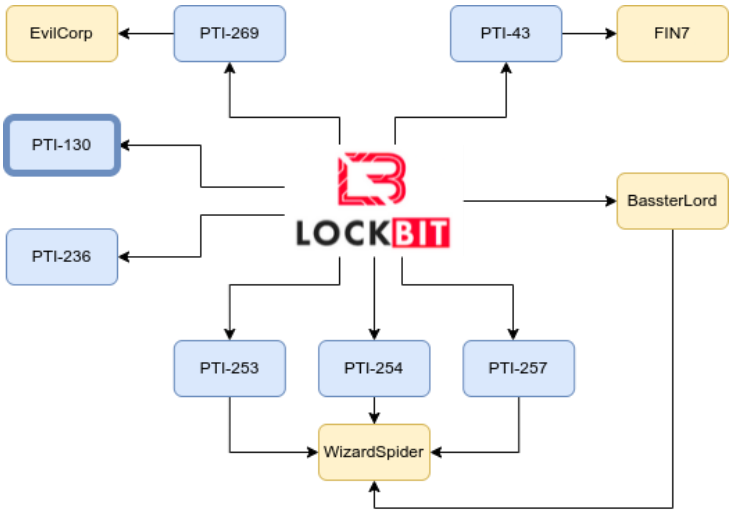
I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

che aveva minacciato di divulgare documenti legali riguardanti Donald Trump. Ha inoltre ipotizzato che l'entry point del dominio è stato causato da una vulnerabilità php Zero-Day.

L'FBI ha risposto all'admin tramite un post sul forum RAMP, attribuendo il successo dell'operazione a una gestione inadeguata del codice sorgente e sottolineando una serie di cattive pratiche tecniche adottate da **LBSupp**. Lungo tutto il 2024, i membri della task force hanno accompagnato le loro azioni con messaggi provocatori rivolti al gruppo LB, rendendo l'operazione anche una campagna psicologica.

Post pubblicato su breach Forums a nome dell'FBI



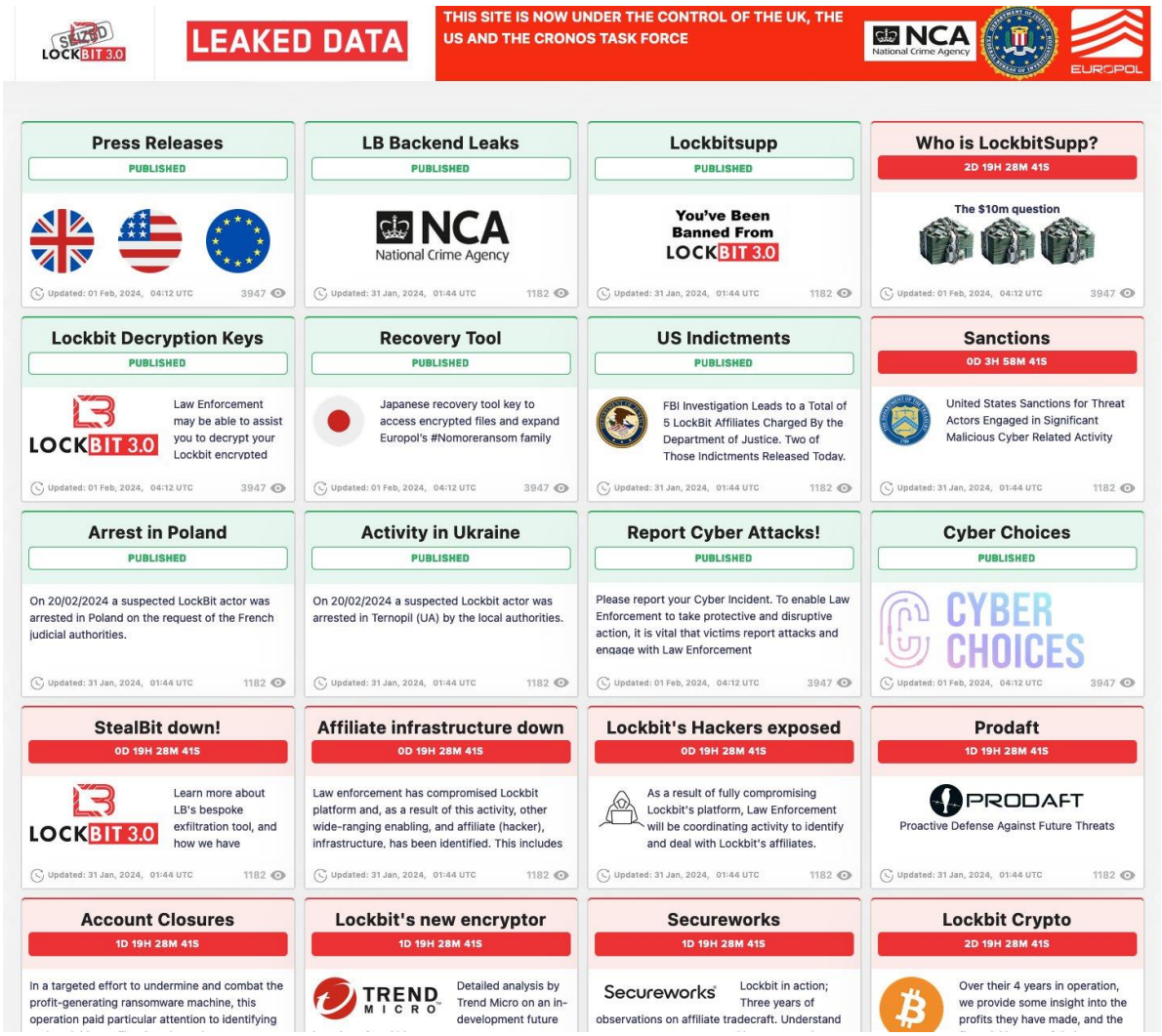
Affiliation del Gruppo Lockbit (Fonte prodaft)

Nel dicembre 2024, viene confermata l'estradizione di Rostislav Panev, uno degli sviluppatori principali di LockBit, arrestato in agosto. Durante il suo arresto sono stati analizzati i suoi device e la loro analisi ha rivelato conversazioni con **Dmitry Khoroshev (alias LBSupp)** e i codici sorgenti di nuove versioni del ransomware ancora in fase di sviluppo.

A pochi giorni dall'inizio del 2025, LockBit ha annunciato ufficialmente il programma 4.0, fissandone il lancio per il 3 febbraio 2025. Tuttavia, non ci sono ulteriori aggiornamenti sul futuro di Operation Cronos o sulle ripercussioni a lungo termine per il gruppo.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT



Data Leak Site (DLS) di Lockbit dopo il deface effettuato dalla coalizione internazionale dell'operazione Cronos

OPERAZIONE ENDGAME

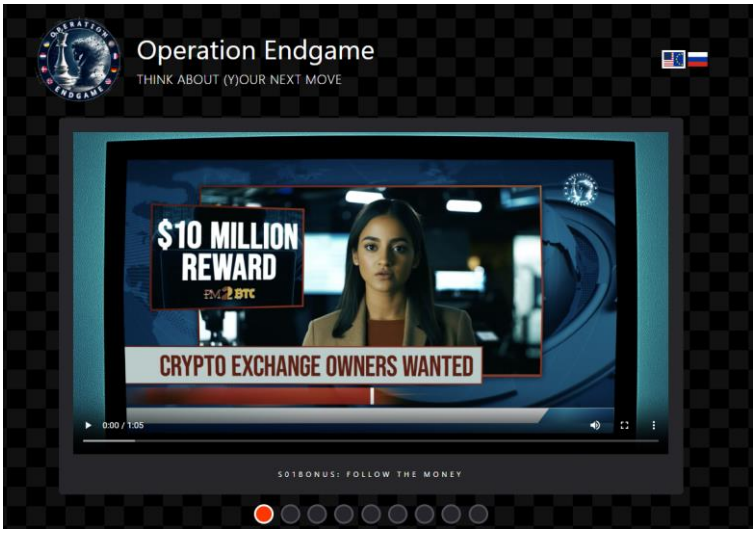
Nel maggio 2024, l'Operazione Endgame ha segnato una delle più grandi offensive contro le botnet e l'ecosistema dei malware dropper. Coordinata dall'Europol e guidata da Francia, Germania e Paesi Bassi, ha coinvolto le forze dell'ordine di vari paesi, tra cui Stati Uniti, Regno Unito, Danimarca, Romania e Ucraina, con il supporto operativo di Eurojust.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

L'operazione si è focalizzata su reti di distribuzione utilizzate per la propagazione di malware avanzati, tra cui IcedID, SystemBC, Smokeloader, Pikabot, Bumblebee e Trickbot. Questi strumenti malevoli erano fondamentali per il rilascio di ransomware e spyware, consentendo ai cybercriminali di superare le difese dei sistemi informatici delle vittime.

Un obiettivo di alto profilo identificato durante l'operazione è stato **Radamir Ramiev**, alias *"Airat Rustemovich Gruber"* , uno dei principali operatori di **SmokeLoader**. Ramiev, noto per la sua lunga carriera nella gestione di botnet e la fornitura di servizi a gruppi di ransomware, è stato tra i cybercriminali esplicitamente citati nei video di Endgame, un chiaro avvertimento ai principali attori del cybercrimine.



Un obiettivo di alto profilo identificato durante l'operazione è stato **Radamir Ramiev**, alias *"Airat Rustemovich Gruber"* , uno dei principali operatori di **SmokeLoader**. Ramiev, noto per la sua lunga carriera nella gestione di botnet e la fornitura di servizi a gruppi di ransomware, è stato tra i cybercriminali esplicitamente citati nei video di Endgame, un chiaro avvertimento ai principali attori del cybercrimine.

27-29 maggio 2024 – L'Operazione Endgame ha smantellato varie infrastrutture critiche e tra queste troviamo:

- Più di **100 server malevoli** utilizzati per il comando e il controllo delle botnet sono stati disabilitati.
- Sequestro di oltre **2.000 domini web** connessi a operazioni illecite.
- **Quattro arresti**, tra cui un operatore in Armenia e tre in Ucraina.
- **Congelamento di criptovalute** per un valore di 69 milioni di euro, derivanti dal noleggio di infrastrutture per la diffusione di ransomware.

31 maggio-10 luglio 2024 – le forze dell'ordine hanno utilizzato il sito web dedicato Operation Endgame per pubblicare un video pilota di 37 secondi, seguito da sette video suddivisi in stagioni ed episodi, ciascuno pensato per rispondere a chi è coinvolto nella criminalità informatica.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

Il messaggio, **"Nessuno è irrintracciabile, nemmeno online"**, ha evidenziato la realtà che i criminali informatici non possono rimanere anonimi nonostante la percepita illusione di ciò. Il primo video dell'Operazione Endgame, intitolato *"GREENHORSE"*, ha mostrato la simulazione di un infiltrato tra i venditori di botnet, culminando con il messaggio di avvertimento: "Pensate alla vostra prossima mossa". Questo ha rafforzato l'idea che l'era della criminalità informatica incontrollata stia giungendo al termine.

Tra i dati sequestrati, sono state identificate comunicazioni tra cybercriminali, chiavi di accesso e dettagli su tecniche avanzate di evasione delle misure di sicurezza. Queste informazioni hanno ampliato il raggio d'azione delle indagini su ulteriori operatori e gruppi affiliati. Il successo di **Endgame** ha temporaneamente paralizzato molte delle infrastrutture che alimentavano attacchi su larga scala, interrompendo la catena di distribuzione di ransomware e altri tipi di software dannoso. Si stima che l'operazione abbia contribuito a prevenire migliaia di nuove infezioni, proteggendo sistemi governativi, aziende e utenti privati in tutto il mondo.

Dopo il primo sequestro dei server, i criminali hanno tentato di ridistribuire parte dell'infrastruttura compromessa. Tuttavia, il rapido coordinamento tra le agenzie ha impedito ulteriori diffusi danni. Alcuni membri delle comunità underground hanno commentato pubblicamente l'operazione, criticando la sicurezza delle botnet smantellate.
Un membro del gruppo dietro **SystemBC** ha affermato che la compromissione iniziale dei loro server è stata facilitata da vulnerabilità note, una lezione che avrebbe dovuto essere imparata dopo operazioni simili. Dall'altra parte, le forze dell'ordine hanno risposto con dettagli sulle debolezze sfruttate, sottolineando la cattiva gestione del codice sorgente come un errore ricorrente nei gruppi colpiti.

La **cooperazione globale** tra Europol, FBI, NCA e altre agenzie ha rappresentato un fattore decisivo per il successo dell'operazione. Nonostante l'importante impatto iniziale, le autorità hanno avvertito che i cybercriminali si riorganizzeranno e che nuove versioni dei dropper smantellati potrebbero emergere in futuro. Tuttavia, le conoscenze acquisite durante l'operazione forniranno un vantaggio nelle prossime azioni di contrasto.
L'Operazione Endgame è stata un chiaro messaggio per l'intero ecosistema del cybercrimine: le botnet e le infrastrutture criminali non sono al sicuro dalla cooperazione internazionale e dalle avanzate tecniche di investigazione.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

OPERAZIONE DESTABILISE

Operation Destabilise è un'operazione globale mirata a destabilizzare le reti di ransomware ancora attive, compromettendo le infrastrutture critiche e colpendone economie nazionali. Promossa dalla **NCA** (UK) l'obbiettivo fu quello che di smantellare le reti di riciclaggio di denaro utilizzate da cybercrime, cartelli della droga in sud america e Irlanda.

L'operazione ha anche incluso missioni contro reti riguardanti il mondo ransomware e spionaggio digitale perpetuato principalmenti da entità Russe ed ha portato a più di 80 arresti dall'inizio delle investigazioni (2021). Solo nel 2024 sono stati portati alla luce i risultati delle forze dell'ordine. La formazione task force internazionale ha compreso CISA, ENISA, FBI e GCHQ con il compito di identificare e neutralizzare la rete di attori coinvolti.

Il Regno Unito ha svolto un ruolo cruciale come hub di queste attività. La **National Crime Agency (NCA)**, collaborando con altre forze dell'ordine britanniche, ha condotto operazioni che hanno rivelato scambi di denaro su larga scala, seguiti quasi immediatamente da movimenti di criptovaluta di pari valore. Il sistema ha contribuito a finanziare ulteriormente attività illecite, alimentando la violenza e il crimine organizzato a livello locale.

o schema finanziario scoperto è stato descritto come complesso dove le reti criminali raccoglievano fondi in un paese per renderli disponibili in un altro spesso convertendo criptovalute in denaro contante. Questo modello offriva un servizio vantaggioso per entrambe le parti: facilitare il riciclaggio di denaro per i gruppi occidentali e permetteva agli attori di utilizzare criptovalute per acquistare droga e armi senza bisogno di movimentare denaro fisico oltre confine. Durante le fasi successive dell'operazione, i responsabili di Destabilise hanno intrapreso una campagna di disinformazione strategica, pubblicando falsi comunicati su forum del dark web per confondere gli investigatori e depistare le indagini.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

Nei messaggi pubblicati, accusavano stati rivali di essere i veri mandanti degli attacchi, cercando di sfruttare le tensioni geopolitiche esistenti per seminare ulteriore caos. Infine le investigazioni hanno scoperto che tale schema veniva utilizzato anche da realtà diverse da quelle del mondo ransomware comprendendo il traffico di droga internazionale e membri dell'élite russa che utilizzano il servizio per poter acquistare proprietà in occidente bypassando le sanzioni in atto dal 2022.

A **Gennaio 2025** è stata dichiarata la continuazione delle indagini, con un focus particolare sul recupero di risorse finanziarie utilizzate per il finanziamento delle operazioni e sulla prevenzione di eventuali nuove ondate di attacchi. Operation Destabilise ha segnato un punto di svolta per la collaborazione internazionale contro le minacce ibride, creando modelli operativi più rapidi e incisivi per il contrasto di campagne di sabotaggio digitale tramite il tracciamento di flussi di denaro.

OPERAZIONE RADAR & DISPOSSSESOR

Nel 2023, Radar & Dispossesor iniziano ad emergere come attori significativi nel panorama delle minacce informatiche, con attacchi mirati principalmente contro infrastrutture critiche e settori finanziari. Entrambi i gruppi hanno mostrato una notevole capacità di evoluzione tecnica, spingendosi oltre i limiti tradizionali del Ransomware-as-a-Service (RaaS).

Nel 2023, Radar & Dispossesor iniziano ad emergere come attori significativi nel panorama delle minacce informatiche, con attacchi mirati principalmente contro infrastrutture critiche e settori finanziari. Entrambi i gruppi hanno mostrato una notevole capacità di evoluzione tecnica, spingendosi oltre i limiti tradizionali del Ransomware-as-a-Service (RaaS).

A partire da gennaio 2024, il gruppo Dispossesor ha attirato l'attenzione internazionale per una serie di attacchi sofisticati contro sistemi di supply chain, utilizzando vettori di attacco che includevano firmware compromesso e attacchi side-channel. L'operazione di controffensiva, denominata Operation Eclipse, è stata lanciata da una coalizione di forze internazionali, tra cui FBI, GCHQ e la Guardia di Finanza, con l'obiettivo di disarticolare le infrastrutture di comando e controllo (C2) del gruppo.

I THREAT ACTORS

OPERAZIONI LAW ENFORCEMENT

Gli eventi principali di Operation Eclipse sono stati i seguenti:

- **14 Marzo 2024** – La task force ha preso il controllo di uno dei principali server di gestione C2 di Dispossesor, sequestrando una vasta quantità di dati sensibili, tra cui chiavi di cifratura, liste di vittime e conversazioni interne tra gli operatori del gruppo. Il server compromesso ha permesso la distribuzione di un tool di decifratura per le vittime colpite fino a quel momento.
- **20 Giugno 2024** – Una vulnerabilità critica scoperta nel codice di Radar ha permesso agli investigatori di sfruttare una backdoor nascosta per monitorare le attività in tempo reale. Questo ha portato alla scoperta di una collaborazione con gruppi affiliati specializzati in attacchi alla catena di approvvigionamento.
- **5 Settembre 2024** – La conferma dell'identità di uno degli amministratori di Radar, noto con lo pseudonimo di *"ShadeHunter"*, ha dato inizio a una serie di arresti coordinati in Europa orientale. Tra le prove sequestrate, sono emersi piani dettagliati per attacchi coordinati contro sistemi **SCADA/ICS**.

Nel corso delle operazioni, *Radar* ha rilasciato aggiornamenti pubblici tramite forum underground, negando il coinvolgimento diretto in alcuni attacchi e accusando le autorità di manipolazione dei dati sottratti. *Dispossesor*, invece, ha cercato di sfruttare l'attenzione mediatica lanciando una nuova versione del loro ransomware, integrata con capacità di esfiltrazione dati più rapide e avanzate funzioni di evasione degli strumenti di rilevamento.
Il 12 dicembre 2024, un annuncio congiunto delle forze dell'ordine ha rivelato che Operation Eclipse aveva causato danni irreparabili alle infrastrutture dei due gruppi, bloccandone l'accesso a fondi cripto per un valore stimato di **$75 MLN**. Tuttavia, entrambe le entità hanno mantenuto una presenza residuale in alcuni canali del dark web, suggerendo possibili nuove evoluzioni nel 2025.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE

A cura di Olivia Terragni, Alessio Stefan, Pietro Melillo

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

Proseguono nel secondo semestre 2024 complesse intrusioni multifase: a livello globale e nella scala operazionale si può notare sia il 'declino' di Lockbit sia una frammentazione, con l'emergere di nuovi ceppi ransomware in un'intensificazione di minacce significative distinte da pratiche sempre più intimidatorie e tecniche di attacco avanzate (utilizzate anche dal gruppi ATP) sempre più efficienti nell'eludere le difese.

Tra i gruppi con il maggior numero di attacchi: RansomHub (precedentemente noto anche come Cyclops o Knight), Play, Akira, Hunters International, Meow, Killesec, Qilin, Medusa, KillSec e nuovi gruppi come Sarcoma, Funseck, Arcusmedia, Argonauts, Interlock, Lynx, Dragonforce, Ciphbit o ancora Helldown, le cui metodologie di attacco mostrano sia notevoli distinzioni che incroci, con un continuo affinamento dei ransomware e capitalizzazione delle vulnerabilità, contemporaneamente alla minaccia significativa rappresentata dalla capacità di eludere i sistemi di difesa e di attaccare settori critici e dall'utilizzo dell'esfiltrazione dei dati per massimizzare l'estorsione.

Tra le gang da tenere d'occhio: Ransomhub, Cicada3301, 8BASE, ClOP, Sarcoma, Fog, KillSec, BlackBasta, Meow e Sarcoma, emerso dell'ottobre 2024.

E' importante sottolineare - come abbiamo fatto nel report H1 - che definire un insieme di tattiche, tecniche e procedure dei gruppi criminali o analizzarne le somiglianze non è sufficiente per mitigare il rischio e quindi conoscere da dove arriverà il ransomware, quando arriverà e in che modo. I criminali infatti trovano sempre nuovi modi di

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

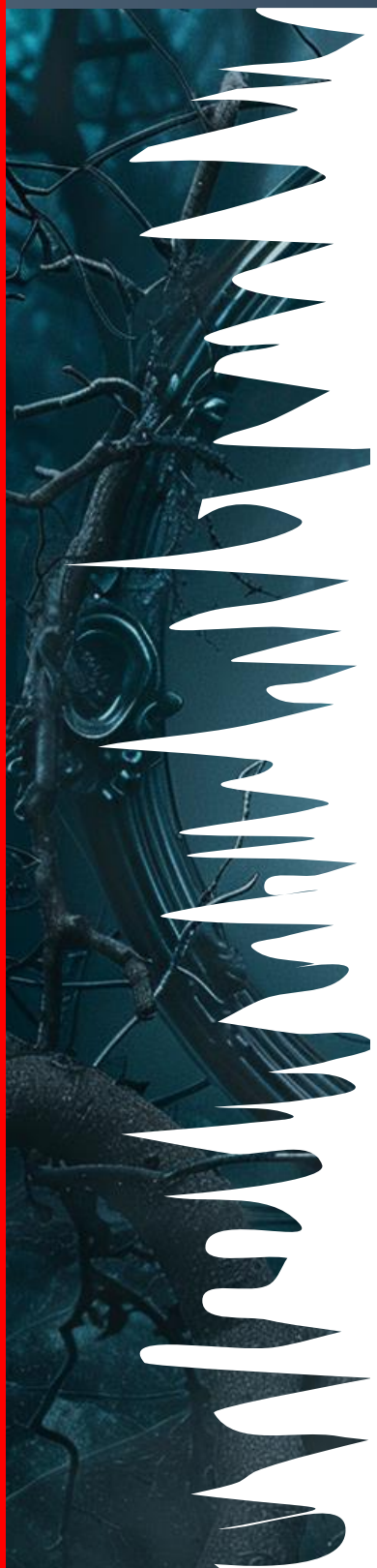
eludere la sicurezza e aggiornare le proprie infrastrutture. Tuttavia data la tendenza delle gang a riutilizzare molti degli stessi strumenti, conoscere comportamenti e strategie abituali di attacco possono fornire informazioni sul loro comportamento e per identificarli. Per proteggersi al meglio è utile osservare le indicazioni fornite nelle strategie di difesa.

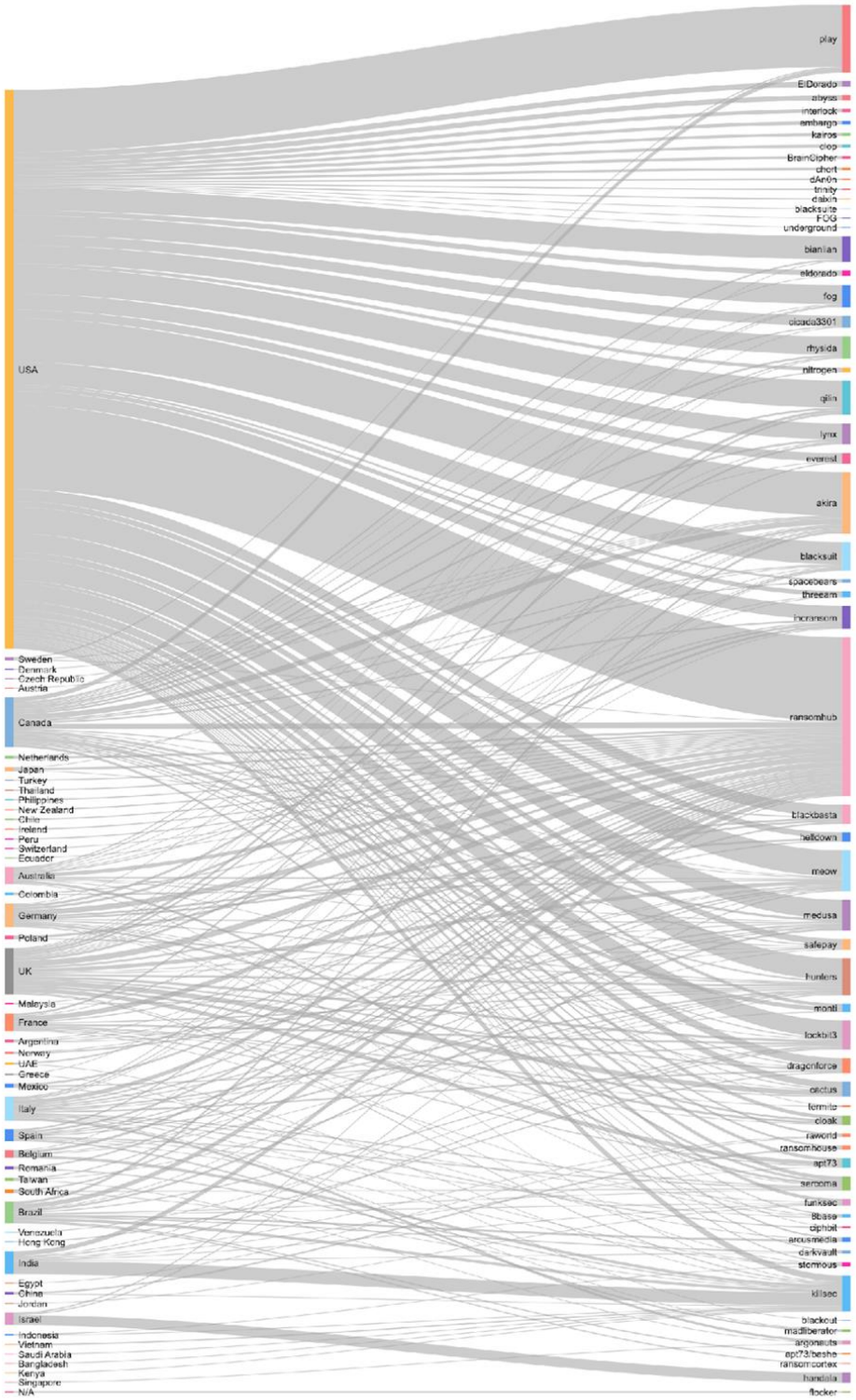
Questa sezione contiene:

1. **ACCESSO INIZIALE E PERSISTENZA**
2. **EVASIONE E CONTROLLO**
3. **INFEZIONE, ESFILTRAZIONE ED ENCRYPTION**
4. **TTP SOMIGLIANZE E DIFFERENZE**

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)





Gruppi per paese target – Periodo di riferimento 2° semestre 2024

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

ACCESSO INIZIALE E PERSISTENZA

Gli aggressori mirano ad attaccare l'infrastruttura e bypassare l'autenticazione tramite lo sfruttamento di tecniche comuni come e-mail di phishing e spear-phishing (che spesso imitano le eMail legittime), ingegneria sociale, malvertising, a cui si aggiungono lo sfruttamento di vulnerabilità note o appena divulgate, applicazioni pubbliche vulnerabili, debolezze nei sistemi (bug del software), un problema temporaneo o una configurazione errata. Come rileva Microsoft, mentre la Multi Factor Authentication (MFA) riesce a bloccare la maggior parte degli attacchi basati su password, **molte tecniche si sono dimostrate efficaci per aggirarla** attraverso il **furto dei token di autenticazione** tramite malware (es.Meduza Stealer consente di acquisire dati da numerose applicazioni software) e attacchi di phishing Adversary-in-the-Middle (AiTM).

L'accesso iniziale è ottenuto inoltre tramite: 'utilizzo di credenziali valide - acquisite tramite broker di accesso iniziale (IAB), altre gang, credenziali rubate durante una violazione che portano a ulteriori infiltrazioni o malware infostealer - come anche credenziali Remote Desktop Protocol (RDP) e Virtual Private Network (VPN) o framework di terze parti. **Diventa sempre più importante proteggere gli "shadow data" esposti tramite il Cloud storage** che sono stati oggetto di una percentuale importante delle violazioni e credenziali rubate o compromesse.

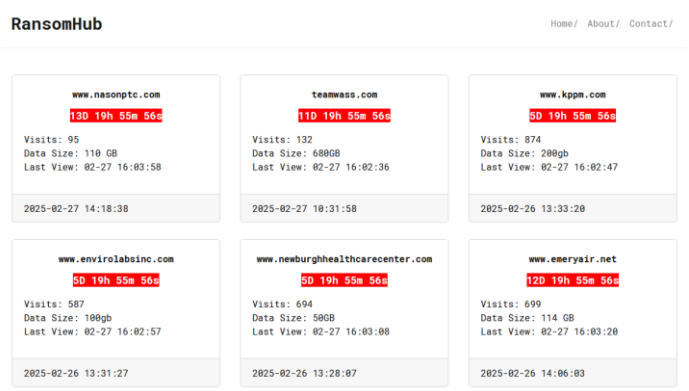
Vengono presi di mira account con privilegi elevati, credenziali e configurazioni deboli dei sistemi remoti (RDP) che permettono di ottenere il pieno controllo sui sistemi per sferrare ulteriori attacchi (es. Sarcoma, RanosmHub, Blacksuit). In special modo botnet e strumenti di automazione consentono un'analisi automatizzata di molteplici indirizzi IP per istanze RDP esposte per poi tentare in modo sistematico migliaia di combinazioni di password con strumenti brute-force (vd. Hydra, Medusa).
Per ottenere l'accesso iniziale e la distribuzione dei dati vengono utilizzate varie piattaforme e market underground tra

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

cui Breach Forums, Exploit Forum, altre minori come Xss, LeakBase, Ramp, Dark Forums, Nulled e Onniforums.

- **Ransomhub** ha sfruttato servizi remoti esposti pubblicamente (RDP/VPN) e ottenuto accessi non autorizzati ai sistemi sfruttando le debolezze dei sistemi operativi o del software (id. Medusa, Hunters). Il gruppo mappa la rete (AngryIPScanner/Nmap) e usa tools (s. Mimikatz) per la raccolta delle credenziali. Ha utilizzato il malware SocGolish, che viene distribuito tramite '**avvelenamento SEO**' dei motori di ricerca e sfruttato la vulnerabilità del SonicWall firewall (CVE-2024-40766) per l'accesso non autorizzato alle risorse (vd. Akira, Fog).



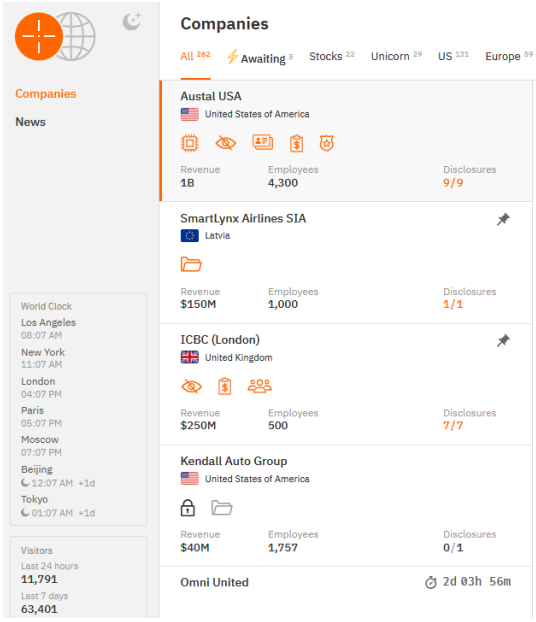
Data leak Site (DLS) del gruppo ransomware **RansomHub**

- **Akira** ha utilizzato credenziali VPN compromesse (senza MFA), estratte dalla memoria di processo del LSASS o attraverso lo scraping (Mimikatz/LaZagnee). Nell'ottobre 2024 ha iniziato sfruttare degli **account Sonic Wall SSL VPN** (Artic Wolf, probabile CVE-2024-40766). Akira e Fog hanno utilizzato gli stessi indirizzi IP VPS per le intrusioni (AS64236 - UnReal Servers, LLC e AS32613 - Leaseweb Canada Inc.) e hanno sfruttato una vulnerabilità nota in Veeam (CVE-2024-40711) che ha consentito loro di eseguire un'esecuzione di codice remoto (RCE) sui server Veeam Backup and Replications.

Data leak Site (DLS) del gruppo ransomware **Akira**

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)



Data leak Site (DLS) del gruppo ransomware **Hunters International**

Data leak Site (DLS) del gruppo ransomware **Interlock**

- Tra le tecniche più recenti di **Blackbasta** l'email bombing, con cui ha **preso di mira le piattaforme di Microsoft Teams** impersonando il supporto IT per indurre le vittime a fornire l'accesso iniziale tramite strumenti di monitoraggio e gestione remoti (RMM). E' stato utilizzato **Qakbot** (Qbot, Quackbot, Pinkslipbot e TA570) durante l'accesso iniziale e ha sfruttato vulnerabilità come ConnectWise CVE-2024-1709.

- **Hunters Int. crea falsi siti web** per impersonare strumenti di scansione di rete open source, per poi sfruttare account con privilegi elevati e utilizza un nuovo trojan di accesso remoto (RAT) C# denominato **SharpRhino** (Quorum Cyber) per infiltrarsi nelle reti aziendali e per modificare il registro di Windows per la persistenza.

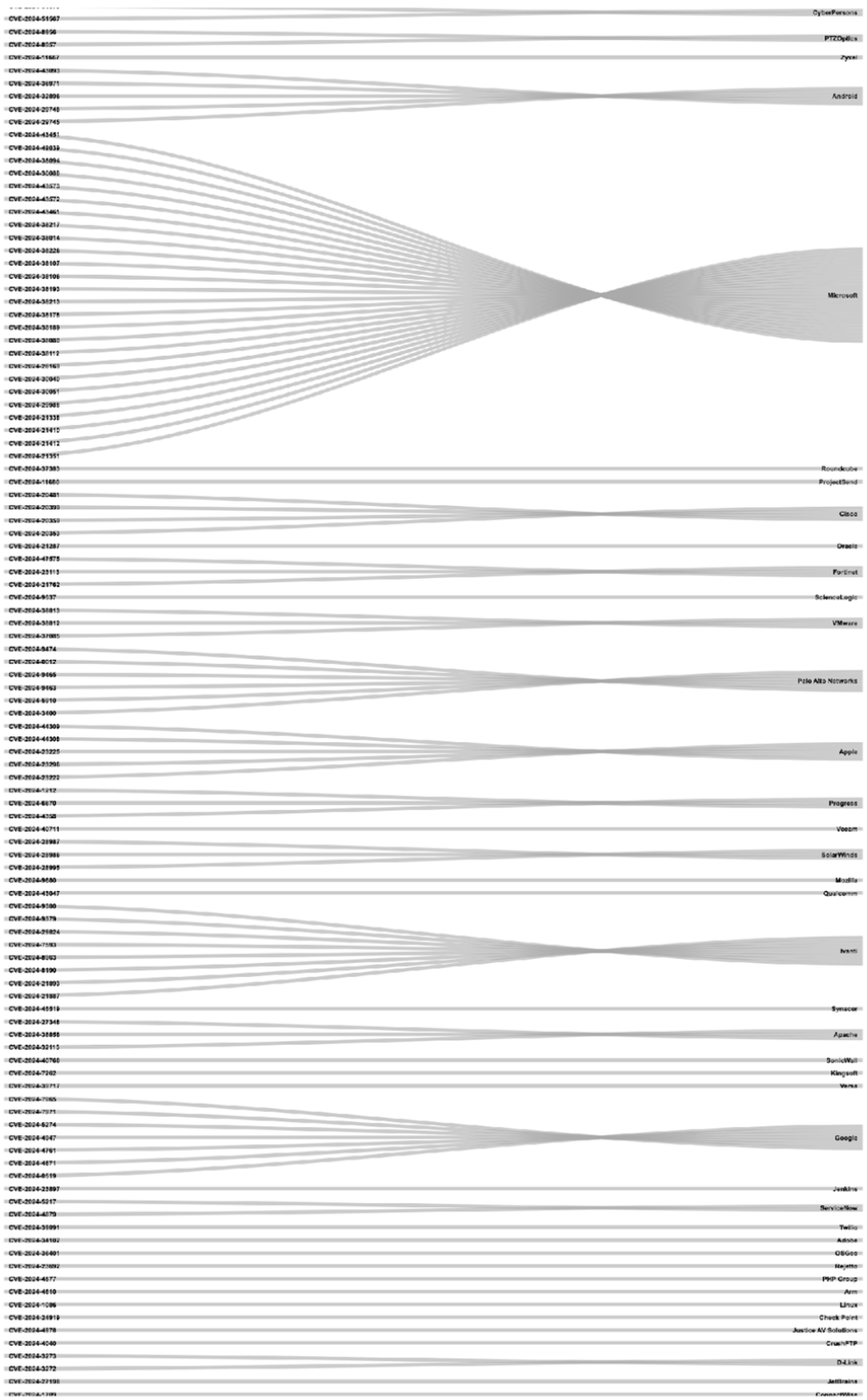
- **Medusa,** fa una ricognizione approfondita della rete (es. Netscan) per identificare obiettivi di valore e procede all'escalation dei privilegi sfruttando strumenti come **PsExec** per garantire una presa più profonda all'interno del sistema compromesso.

- **Interlock** accede inizialmente tramite un falso eseguibile di aggiornamento del browser Google Chrome scaricabile da un sito web legittimo compromesso (Cisco Talos): l'eseguibile è uno strumento di accesso remoto (RAT) che esegue automaticamente uno script PowerShell incorporato quando scaricato ed eseguito.

- **Helldwon** ha ottenuto l'accesso iniziale tramite firewall Zyxel tramite exploit o SSL-VPN (TrueSec).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)



CVE 2024 per fornitore – CISA

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

EVASIONE E CONTROLLO

Una volta ottenuto l'accesso iniziale gli aggressori mappano la rete per identificare le risorse critiche: la persistenza viene stabilita tentando l'abuso delle funzioni dei controller di dominio, vengono attivate tecniche di attacco post-sfruttamento (protocollo di identificazione) - vengono spesso riabilitati account disabilitati ed estratte nuove credenziali con tools come Mimikatz/LaZagne (Akira, BlackBasta, RansomHub),

Ogni dispositivo utente, diventa vulnerabile alla raccolta di ulteriori credenziali, che a loro volta portano ad ulteriori attacchi. Gli infostealer continuano a rappresentare una sfida.

In particolare:

- **Akira** estrae nuove credenziali archiviate nella memoria di processo del Local Security Authority Subsystem Service (LSASS), raccoglie informazioni sulle relazioni di trust del dominio e ha usato SoftPerfect e Advanced IP Scanner per scoprire i dispositivi di rete e utilizzato i comandi net di Windows per identificare e abusare dei controller di dominio. Per aumentare i privilegi prende di mira il **protocollo di autenticazione Kerberos** per rubare le credenziali AD e usa **tecniche di cracking delle passwords (utilizzata** dall'attore di spionaggio **APT 40** o da **Vice Spider** (o Vice tempest, DEV-0832, Vanilla Tempest)

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

specializzato in intrusioni, esfiltrazioni ed estorsioni e collegato all'utilizzo di **Inc Ransomware**. Usa spesso SoftPerfect e Advanced IP Scanner per scopi di ricognizione dei dispositivi di rete e i comandi net Windows per identificare i controller di dominio e raccogliere informazioni sulle relazioni di trust del dominio Alcuni account amministrativi creati da **Akira** erano **denominati "itadm"**.

- **RansomHub** raccoglie credenziali tramite lo scraping, crea account utente, riattiva account disabilitati e utilizza strumenti come Ngrok per il proxy inverso e Anydesk e EDRKillShifter per la persistenza.

- **Dragonforce** utilizza – oltre ad altri strumenti – Mimikatz e Cobalt Strike per la raccolta delle credenziali e il movimento laterale, la backdoor SystemBC per la persistenza e strumenti di scansione di rete per mappare degli ambienti compromessi.

- **Interlocker** utilizza uno stealer di credenziali compilato in Golang: secondo Cisco Talos utilizza query SQL per raccogliere le informazioni di accesso degli account online delle vittime insieme agli URL degli account associati. Infine, i dati vengono scritti in un file "chrgetpdsi.txt" nella cartella temporanea del profilo utente.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- **Qilin** come osservato da Sophos X-Ops,manipola gli oggetti Criteri di gruppo (GPO) per controllare le impostazioni utente e le distribuzioni software e modifica i GPO per eseguire uno script di PowerShell denominato "IPScanner.ps1" su tutte le macchine che hanno effettuato l'accesso alla rete di dominio per r**accogliere dati di credenziali memorizzati nel browser Chrome** che vengono inviate al server di comando e controllo di Qilin.
- **Medusa**, esegue un dump delle credenziali del database Active Directory (AD) e delle credenziali in memoria e tentano di abusare delle funzioni dei controller di dominio creando nuovi account di dominio: eseguono una ricognizione approfondita della rete (Netscan) per identificare obiettivi di valore e mappare la topologia della rete, e utilizza strumenti come PsExec per l'escalation dei privilegi.
- **BlackSuit** utilizza software di monitoraggio e gestione remota (RMM).

EVASIONE E CONTROLLO

I gruppi ransomware continuano a perfezionare le loro tattiche per aggirare la difesa dei sistemi, come le **tecniche di aggiramento degli Endpoint Detection and Response (EDR)**.

> La capacità di compromettere ed eludere i sistemi di difesa permette un movimento silenzioso e mirato all'interno delle reti: ciò rende gli attacchi efficaci e spesso difficili da contrastare e sempre più necessaria una difesa più strutturata.

Sempre più gruppi utilizzano **strumenti (**(vd. EDRSilencer, *EDRSandBlast*, EDRKillShifter, Killer Ultra, Kill AV, AVNeutralizer/AuKill, Brute Ratel etc.) e **tecniche di bypass dell'EDR per aggirare le difese perimetrali.** La Cybersecurity and Infrastructure Security Agency (CISA) ne ha rilevati sino **ad oggi circa 12**: RansomHub, Blacksuit, Blackbasta, Akira, Phobos, ALPH Black, Play, Rhysida, AvosLocker, Snatch, Lockbit 3.0, BianLian.

Secondo alcuni ricercatori (Intel471) a rendere disponibile sul "mercato" (vendita) strumenti come AVNeutralizer ci sarebbe il gruppo **FIN7**, collegato a ceppi di ransomware tra cui REvil, DarkSide, BlackMatter, ALPHV, Black Basta, Maze e Ryuk (vd tendenze).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

Gli EDR killers vengono venduti o acquistati anche come servizi in abbonamento nei "Black Markets" (anche a partire 300$ per un singolo bypass). Tra le **strategie più utilizzate: Living Off The Land (LOTL), software di monitoraggio e gestione remota (RMM) e software open source: tra quelli più utilizzati: AnyDesk, Cobalt Strike, Viper, BloodHound e Impacket.**

Tra le diverse strategie utilizzate (vd. MITRE ATT&CK: T1562.001 Impair Defenses: Disable or Modify Tools): tecniche di evasione avanzate (AET) per aggirare la sicurezza di rete, i sistemi di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS). Vengono arrestati i processi del software di sicurezza (Windows Management Instrumentation (WMI), modificati i file di configurazione o interrotti gli aggiornamenti per impedire l'applicazione delle patch più recenti, viene aggirata la verifica del firmware sui dispositivi di rete, vengono disabilitati gli strumenti di monitoraggio del cloud, con l'obiettivo di spostarsi lateralmente all'interno della rete per poi esfiltrare e crittografare i dati. La tecnica **BYOVD** inoltre - utilizzata dagli aggressori - sfrutta le vulnerabilità nei driver legittimi e firmati, per poi ottenere uno sfruttamento kernel-mode. **Nello specifico**:

- **Ransomhub** cerca di inibire una potenziale risposta agli incidenti cancellando i registri di sistema (Windows e Linux), può disabilitare i sistemi antivirus utilizzando Windows Management Instrumentation. Utilizza strumenti (EDRKillShifter), per disabilitare i sistemi EDR: Trend Micro ha rivelato come il gruppo utilizzi due strumenti noti: TDSSKiller di Kaspersky, per disattivare i sistemi EDR e LaZagne per raccogliere le credenziali nel database per prendere di mira account con alti livelli di privilegi. Usa la tecnica Living off the Land (LotL) nota come Bring Your Own Vulnerable Driver (BYOVD). Secondo ThreatDown/MalwareBytes similmente a Lockbit utilizza anche il flag "-dcsvc" per eliminare i servizi e rimuovere le chiavi di registro relative alla sicurezza).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- **Play** utilizza infostealer per raccogliere informazioni di rete ed eseguire la scansione per il software antivirus. Disattiva il software EDR (es. ProcessHacker, GMER, IOBit, PowerTool, rimuove i file di registro e disattiva Microsoft Deefender tramite script di PowerShell. similmente **Lockbit3.0**, disabilita i processi EDR (vd. Backstab, Defender Control, Terminator GMER, PCHunter, PowerTool, ProcessHacker e TDSSKiller), Utilizzando Bat Armor invece aggira i criteri di esecuzione di PowerShell codificando lo script ps nel file bat, disabilitando e disinstallando il software anti-malware.

- **Rhysida** esegue uno script PowerShell noto come SilentKill per terminare i processi dell'antivirus e bypassa il livello di difesa in tempo reale dell'Endpoint Protection.

- **Bianlian** disabilita gli antivirus utilizzando tecniche LotL sfruttando PowerShell e Windows Command Shell: in particolare ha preso di mira Windows Defender e Anti-Malware Scan Interface (AMSI). Modifica i registri di sistema e disattiva la protezione antimanomissione Sophos.

- **Cicada3301** ha utilizzato EDRSandBlast per manomettere i sistemi EDR.

- **Medusa** può disabilitare centinaia di processi relazionati alla sicurezza e impiega una sofisticata tecnica di elusione anti-malware che prevede l'installazione di un agente RMM dannoso e il caricamento di driver vulnerabili. Disabilita gli strumenti di sicurezza utilizzando script di PowerShell e regola le impostazioni del registro per eludere il rilevamento e tecniche di crittografia delle stringhe per offuscare il codice dannoso.

- **Dragonforce**, per bypassare la sicurezza, eludere la difesa e criptare i sistemi usa la tecnica "Bring Your Own Vulnerable Driver" (BYOVD), inclusa nella loro variante Conti del ransomware (utilizzata anche da Cuba ransomware): questo rende i loro attacchi altamente efficaci e difficili da contrastare.

- **Qilin** disabilita servizi chiave come Veeam, database SQL e strumenti antivirus e per terminare i processi EDR/A e prendere di mira le difese (Symantec, Microsoft e Sentinel One) utilizza Killer Ultra che sfrutta un driver Zemana (**CVE-2024-1853**) e ottiene le autorizzazioni a livello di kernel.

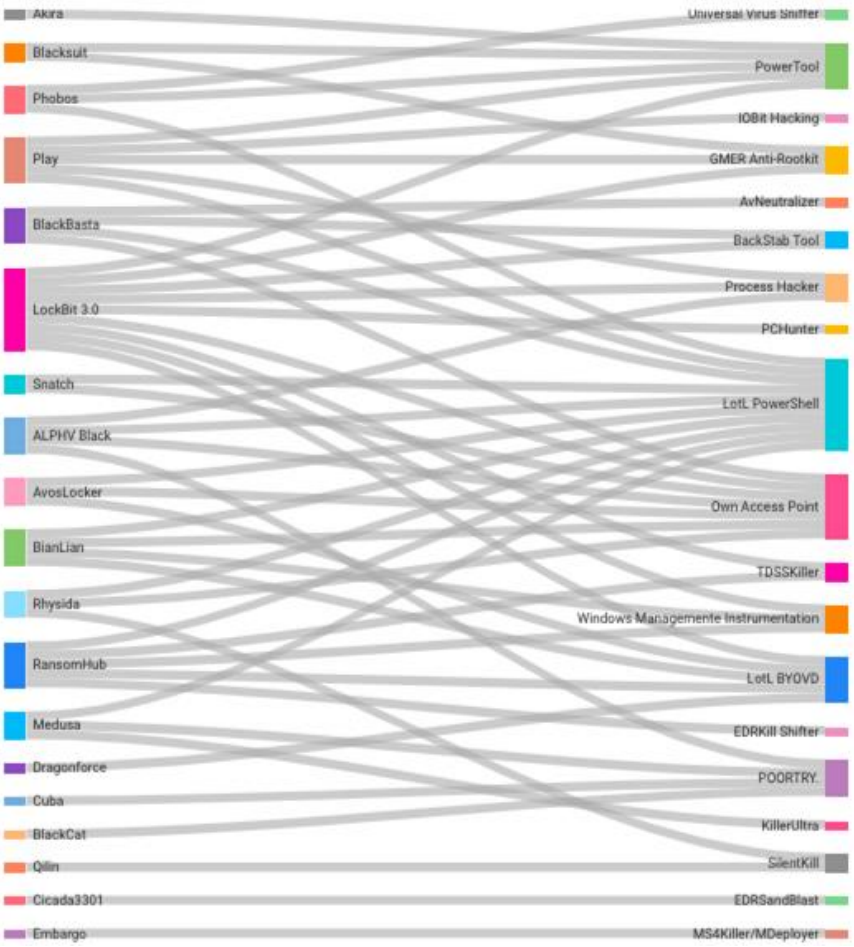
- **Helldown** ha disabilitato manualmente la protezione antivirus in tempo reale tramite PowerShell e tramite un secondo metodo ha utilizzato hrsword.exe per disabilitare il software di protezione degli endpoint su una determinata macchina (TrueSec).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

Gli attaccanti non solo cercano di disabilitare i sistemi di difesa e ogni potenziale loro risposta agli incidenti: **per oscurare le tracce** ed ostacolare le indagini forensi **viene cancellato il registro di sistema** (Linux/Windows). (Ransomhub, Dragonforce, Meow). I **valori di registro** (HKLM e HKCU) **possono essere modificati** per garantire che i payload vengano caricati all'avvio (Medusa).

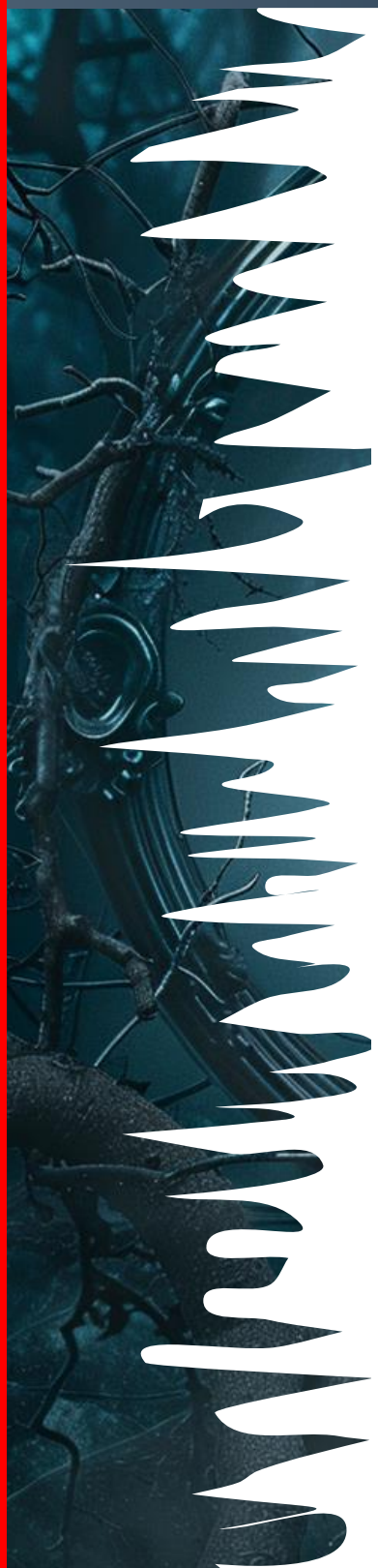
Tra gli strumenti o altri metodi di comando controllo: Remote Desktop Protocol (RDP), PsExec, Cobalt Strike, Connectwise, N-Able, Metasploit, AnyDesk, Radmin, Cloudflare Tunnel, MobaXterm, RustDesk and Ngrok.



Alcuni metodi per gruppo per evadere gli EDR

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)



INFEZIONE, ESFILTRAZIONE ED ENCRYPTION

Nonostante i gruppi sviluppino continuamente nuovi metodi di encryption, molti hanno iniziato a preferire tattiche di doppia estorsione o di sola esfiltrazione che consumano meno tempo e risorse (Akira, Hunters International, BianLian, Meow o Inc Ransom). Altri come Blackbasta usano tecniche di esfiltrazione prima dell'encryption. I file presi di mira nell'esfiltrazione solitamente vengono visualizzati in anteprima (BlackCat, INC ransomware) e hanno le seguenti estensioni: .doc, .xls, .ppt, file di testo e dati .txt, .csv o file di database .sql. Per trasferire i dati ai server o ai cloud RaaSStrumenti sono utilizzati strumenti come ExByte, ExMatter, and StealBit.

Sekoia evidenzia script personalizzati per l'infiltrazione automatizzata:

- lo script utilizzato da **Vice Society** si connette al server Web del set di intrusione tramite una richiesta HTTP,
- lo script shell di **Mallox** che consegna ed esegue il payload ed esfiltra i dati su due server.
- Grixab, utilizzato da **Play** e progettato per elencare tutti gli utenti e i computer all'interno di un dominio, per enumerare software e servizi e raccogliere informazioni su soluzioni di sicurezza e software di backup, raggruppandole in un file ZIP. Attribuito a Play è anche VSS Copying Tool, per enumerare file e cartelle in snapshot VSS e copiare i file in una destinazione scelta, prima della crittografia,
- ExMatter di BlackMatter enumera file specifici e li invia al server prima della crittografia e può corrompere i file.

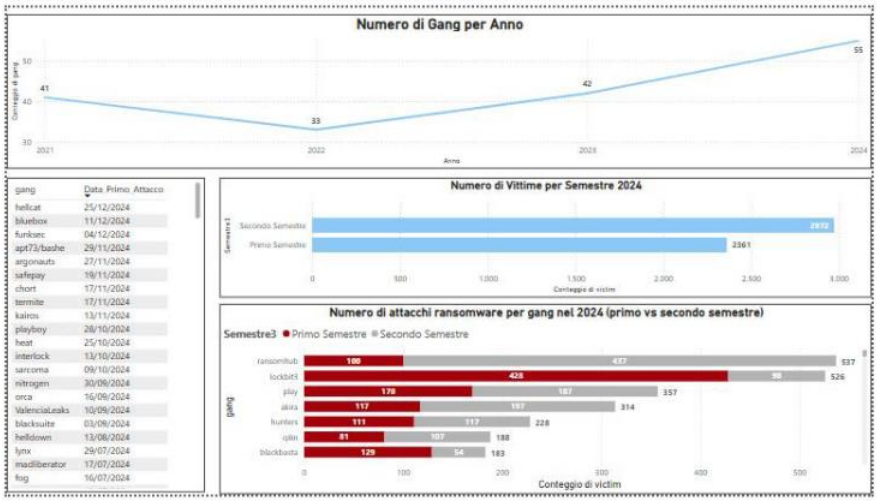
Tra i ransomware che hanno ultimamente destato attenzione:

- **Doubleface** - utilizzato per colpire l'aeroporto di Donetsk - scritto in C/C++ con algoritmi di crittografia AES-128 e RSA-4096, aggira i sistemi di sicurezza e non viene rilevato dai maggiori software di antivirus: l'utilizzo della chiave sbagliata di decrittazione porta alla distruzione dei dati.
- **Interlock**, disponibile nelle versioni Windows e FreeBSD: :il vettore di infezione è ad oggi sconosciuto (Fortinet ha

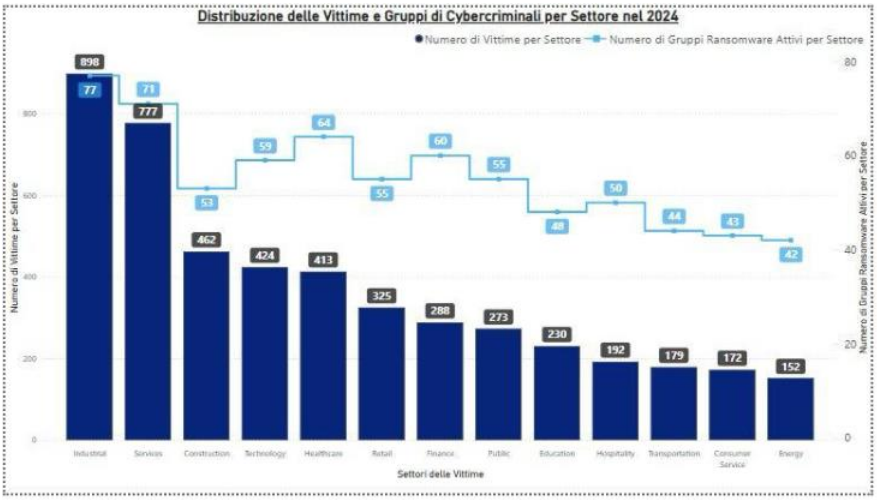
I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

ipotizzato una backdoor di entrata). Il ransomware può essere abiltato alla sua autoliminazione utilizzando una DLL tramite rundll32.exe. I file crittografati ricevono l'estensione .interlock e la nota di riscatto '!__README__!.txt'.



Numero di gang attive per anno, numero di attacchi nel 2024 e numero di vittime.



Distribuzione delle vittime e dei gruppi nei per settore nel 2024

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

Tra gli altri attori:

- **Medusa** esfiltra i dati sui suoi server e impiega la crittografia RSA asimmetrica per codificare file e directory di destinazione, che contengono anche una copia della richiesta di riscatto. I file crittografati hanno in genere estensioni come .medusa o .mylock.

- Il ransomware **Akira** è basato sulla crittografia ibrida (ChaCha20 e RSA): i file crittografati hanno spesso l'estensione ".akira" o ".powerranges". Nella variante Linux ESXi può essere utilizzata l'estensione file ".akiranew" con la nota di riscatto denominata "akiranew.txt". Per l'esfiltrazione utilizza strumenti come WinSCP, RClone o FileZilla, per faciltarla utilizza anche AnyDesk, MobaXterm, RustDesk, Ngrok e Cloudflare Tunnel.

- **Qilin** usa tattiche di doppia estorsione e il ransomware Agenda impiega la crittografia AES-256 per i file e RSA-2048 per la crittografia delle chiavi e rilascia una DLL dannosa (pwndll.dll) che camuffata da WICloader.dll, viene iniettata in svchost.exe per garantire l'esecuzione persistente del file binario del ransomware. **Halcyon ha rilevato una nuova variante Rust del ransomware Qilin**: Qilin.B. ha tecniche di evasione migliorate, impiega la crittografia AES-256-CTR con supporto AESNI per prestazioni più rapide sulle CPU moderne, mentre utilizza ChaCha20 per i sistemi più vecchi. Utilizza anche RSA-4096 per proteggere le chiavi di crittografia, rendendo la decrittazione quasi impossibile senza la chiave privata.

- **Dragonforce**, ha due varianti di ransomware, la prima basata su LockBit Ransomware e la seconda sulla variante Conti Ransomware che personalizza. I file vengono criptati in modo completo, parzialmente o solo i primi byte [header_encrypt_size] e vengono rinominati con l'estensione ".dragonforce_encrypted", anche se ogni affiliato la può personalizzare.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- **Hunters International** esfiltra i dati prima di crittografare i file di cui poi viene modificata l'estensione in .locked con una nota README. Il crittografo è codificato in Rust.

- **Sarcoma** - noto per le sue tattiche aggressive - esfiltra i file prima della crittografia poi utilizzati come leva di estorsione: il malware utilizza algoritmi di crittografia avanzati e rende i file inaccessibili, impossibile decrittografarli senza la chiave e anche quando viene pagato il riscatto è accaduto che non sia stata fornita.

- **Lynx** crittografa i file utilizzando AES-128 in modalità CTR e algoritmi di crittografia Curve25519. Unit 42 ha segnalato inoltre che utilizza l'API Restart Manager "RstrtMgr" per abilitare la crittografia dei file in uso o bloccati da altre applicazioni, e ai file crittografati viene assegnata l'estensione .lynx.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

TTPs SOMIGLIANZE E DIFFERENZE

Tra le caratteristiche comuni dei gruppi in azione l'aumento dell'utilizzo del ransomware basato su **Rust** (es. Akira, **Hive o Hunters Internationa)** con il potenziale sviluppo di varianti sempre più difficili da rilevare**.** Tattiche di doppia estorsione, tecniche ibride crittografiche, pratiche di esflitrazione, miglioramento nell'elusione delle difese fanno parte di **un cambio anche comportamentale**, che mira a trarre il massimo beneficio dall'attacco.

Attraverso il confronto delle tecniche utilizzate le analisi dei ricercatori si trovano le seguenti coerenze:

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- Il ricercatore Rakesh Krishnan ha rilevato come il gruppo APT73 (Bashe) non solo potrebbe essere uno spin-off di Lockbit, ma analizzando il suo vecchio DLS e la sua infrastruttura (basata in Cechia) ha notato che l'ASN (**AS9009) è stato associato in precedenza ai gruppi DarkAngels, Vice Society e PYSA/Mespinoza** e utilizzato da malware come TrickBot, Meduza Stealer o Rimasuta. Sul suo nuovo DLS sono stati pubblicati dei leak precedentemente pubblicati da **BlackBasta**: questo potrebbe dirci solamente che i vecchi affiliati di BlackBasta si sono spostati a Bashe. Osservare gli stessi comportamenti non significa necessariamente che questi attacchi siano stati tutti eseguiti dagli stessi individui.
- Sophos, analizzando 4 diversi attacchi ransomware (**Hive**, **Royal Black Basta)** ha rilevato un copione simile, anche se con alcune devianze significative: sono stati creati account di livello amministratore sui server Domain Controller dirottati utilizzando gli **stessi nomi utente e password specifiche,** sono stati utilizzati meccanismi di persistenza con gli stessi nomi, identici script batch di pre-distribuzione per gettare le basi della distribuzione del ransomware hanno distribuito il payload finale del

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

ransomware utilizzando lo stesso sistema: rilasciando un archivio .7z, denominato con il nome dell'organizzazione presa di mira, che conteneva un eseguibile anch'esso denominato con il nome dell'organizzazione presa di mira. L'archivio .7z era protetto da password con la stessa password e distribuito con lo stesso comando shell.

- In **Royal** TrendMicro ha rilevato come Royal abbia sviluppato una nuova variante di Blacksuit (98% delle somiglianze) il che li ha portati a pensare ad un copy cat o ad una scissione di Royal: argomenti della riga di comando con funzione simili, stringhe di argomenti anche se con nomi leggermente diverso hanno lo stesso scopo, tecniche simili per accelerare la crittografia dei file della vittima, stesse estensioni di file evitate.

Tra i gruppi più recenti:

- **Lynx**, gruppo più recente, è stato associato a **Inc Ransom** (collegamenti tracciati da Rapid7 e Unit 42) con una somiglianza del 48% tra le due versioni e del 70,8% nelle funzioni: ciò potrebbe semplicemente significare che Lynx ha preso una parte considerevole di codice da Inc Ransom, messo in vendita a 300mila dollari a maggio e che includeva sia le versioni Windows che Linux/ESXi del ransomware.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- **TrueSec** ha rilevato somiglianze del gruppo **Cicada3301** con **ALPHV/BlackCat.** suggerendo un ipotetico rebranding: entrambi sono scritti in Rust, usano ChaCha20 per la crittografia, simili comandi per arrestare la VM e rimuovere gli snapshot, la stessa convenzione per nominare i file, metodologie simili per l'eliminazione e la manomissione delle copie shadow e la cronologia suggerisce che la scomparsa di BlackCat e l'emergere prima della botnet Brutus e poi dell'operazione ransomware Cicada3301. Da notare che il codice sorgente del ransomware BlackCat è stato messo in vendita per 5 milioni di dollari.
- Anche il gruppo **BrainCipher** è stato correlato sia a **Lockbit** e al gruppo ransomware **SenSayQ** correlato a sua volt al gruppo RebornRansomware **(GroupIb)**, come lo stesso link TOR della pagina di supporto, le stesse regola utilizzate sul DLS e lo stesso indirizzo email qn.support[@]cyberfear.com (stesso indirizzo email di contatto con un gruppo ransomware **Noname e a sua volta condivisa con EstateRansomware.**) trovato nella nota di riscatto del gruppo ransomware SenSayQ. Simile è anche il formato dell'ID della crittografia usata.
- Per quanto riguarda Akira: oltre ad una sovrapposizione di codice del ransomware Conti (trapelato) ArticWolf ha rilevato tramite blockchain un mescolamento dei fondi tra gli indirizzi wallet degli affiliati. In ultimo l'APT73 (Bashe) ha ottenuto il suo spin-off da LockBit: le sue pagine sembrano una replica del DLS LockBit.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

A complicare maggiormente il panorama è la potenziale collaborazione tra gruppi ransomware e APT, questi ultimi camuffano inoltre le loro attività attraverso il ransomware, mascherando le loro operazioni e coprendo le loro tracce. FBI e CISA hanno rilevato:

- lo sfruttamento del ransomware con capacità di esfiltrazione per **mascherare attività di spionaggio**: il gruppo sponsorizzato dallo stato nordcoreano Andariel è stato osservato in una campagna correlata al ransomware **Play**, suggerendo il suo coinvolgimento nella raccolta e possibile esfiltrazione di dati e nel set di intrusione che gestisce la backdoor RomCom, che è anche associata al ransomware di **Cuba**, ripetutamente segnalato per aver condotto operazioni di ransomware ed esfiltrazione opportunistiche, nonché attacchi a supporto di operazioni di intelligence.
- un autore di minacce – potenzialmente iraniano – noto come Lemon Sandstorm sta conducendo attacchi ransomware in collaborazione con gruppi russi specializzati in RaaS come **BlackCat, NoEscape e Ransomhouse.**

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPs)

- membri dell'**APT Pioneer Kitten** si pongano come IAB per i gruppi di ransomware di lingua russa ad **accedere alle loro vittime in cambio di una parte dei profitti** e sono stati osservati mentre utilizzavano Shodan per identificare indirizzi IP che ospitavano Check Point Security Gateway vulnerabili a CVE-2024-24919, ma è anche noto che ha sfruttato CVE-2024-3400 in Palo Alto Networks PAN-OS e GlobalProtect VPN, nonché vecchie vulnerabilità in Citrix e F5 BIG-IP.

Non ultima è stata la scoperta sul gruppo **FIN7** (id. Carbon Spider, ELBRUS, or Sangria Tempest): collegato a malware bancari come Carbanak, che da tempo sarebbe passato l ransomware e i ricercatori lo hanno collegato a ceppi di ransomware tra cui REvil, DarkSide, BlackMatter, ALPHV, Black Basta, Maze e Ryuk e che continua a sviluppare lo strumento **AvNeutralizer** progettato per interrompere il software EDR. FIN7 e Black Basta avrebbero contribuito secondo SentinelOne, a trasformare gli strumenti di evasione EDR in “armi informatiche” vendute, o in abbonamento, con prezzi che si aggirano dai 300 sino ai 10.000 dollari.

Questo tipo di collaborazioni o quelle tra gruppi ransomware rappresenta un problema non indifferente : da una parte i gruppi avranno sempre più strumenti efficaci e miglioreranno le loro tattiche, dall’altra gli stati beneficeranno di gruppi redditizi.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

THREAT ACTORS

INTERVISTE AI THREAT ACTORS

A cura di Massimiliano Brolli e Alessio Stefan

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

Questo periodo del 2024 vede come protagonisti delle nostre interviste, gruppi ransomware vecchi e nuovi della scena del cybercrime. Dopo aver intervistato cyber gang del calibro di ***LockBit 3, Cicada 3301, 8base, Everest e gli italiani di ALPHA Group, Anonymous italia, ADHD e AzzaSec,*** ecco le nuove interviste condotte nel periodo che va da Luglio a Dicembre del 2024.

In questo caso si tratta di tutte cyber gang ransomware con programmi Ransomware as a Service (RaaS) che mirano a costruirsi una solida immagine sin dai primi attacchi, adattandosi all'intero ecosistema.

Questi gruppi comprendono le dinamiche delle vittime, degli operatori di ransomware e non discriminano nella scelta delle vittime, lasciando agli operatori la libertà di utilizzare l'infrastruttura malware fornita a loro discrezione.

Un mercato democratico
L'interesse dei criminali informatici per il mercato del ransomware è alimentato non solo dalla possibilità di guadagni sostanziosi, ma anche dalla relativa facilità di accesso rispetto ad altri tipi di attività criminose. La natura lucrativa del ransomware, supportata dall'uso di criptovalute per i pagamenti e da infrastrutture digitali che consentono un relativo anonimato, rende questo tipo di attività particolarmente attraente per individui e gruppi in cerca di profitti rapidi.

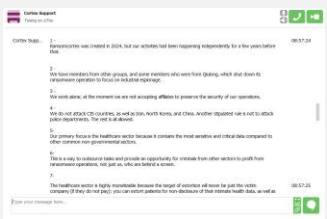
Il fenomeno RaaS ha contribuito a democratizzare ulteriormente l'accesso al ransomware, permettendo a gruppi meno sofisticati di entrare nel mercato con minori risorse e competenze tecniche rispetto ai loro predecessori.

RANSOM CORTEX

Ransomcortex, è una nuova cyber gang ransomware che abbiamo intervistato a luglio del 2024, rivela un gruppo altamente specializzato nel colpire il settore sanitario, recentemente responsabile di attacchi a quattro istituzioni, tra cui **tre in Brasile e una in Canada.** La gang si distingue per la sua efficienza e la strategia mirata, evidenziando la vulnerabilità di un settore già sotto pressione. Le informazioni sanitarie sono particolarmente attraenti per i criminali, poiché offrono opportunità di frodi finanziarie e vendite nel mercato nero.

Questo pone interrogativi sulla sicurezza delle informazioni e sull'impatto sociale degli attacchi ransomware su ospedali e cliniche. Ransomcortex, formatosi nel 2024, **ha un approccio diretto e operativo**. La gang non accetta affiliati per preservare la sicurezza delle proprie operazioni e ha regole precise per non attaccare determinati Paesi e istituzioni.

Data Leak Site (DLS) del gruppo Ransom Cortex.
Il data lake site di Ransom Cortex conteneva 6 vittime alla data della nostra intervista. L'intervista è stata condotta attraverso TOX ransomware, un messanger cifrato molto spesso utilizzato dai criminali informatici.



I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

Si concentrano principalmente sul **settore sanitario** perché considerano le informazioni in esso contenute come le più critiche. Per monetizzare le informazioni rubate, Ransomcortex può ricorrere a più strategie, come *l'estorsione diretta ai pazienti e la vendita dei dati sul mercato nero*. La gang afferma di mantenere un protocollo per garantire che gli attacchi non compromettano direttamente i servizi essenziali degli ospedali.

Durante l'intervista, i membri di Ransomcortex discutono delle loro tecniche di attacco, che includono **vulnerabilità specifiche e ingegneria sociale,** enfatizzando l'importanza della preparazione e dell'aggiornamento continuo delle loro pratiche operative. Affermano di avere un team dedicato alla sicurezza e alla raccolta di informazioni, e si difendono dalle critiche sostenendo che *la gestione delle informazioni sensibili da parte delle istituzioni sanitarie è spesso inadeguata*. Questo approccio mette in evidenza **la necessità urgente per le organizzazioni sanitarie di migliorare le loro misure di sicurezza** per proteggere i dati dei pazienti e mantenere la fiducia pubblica.

RADAR and DISPOSSESSOR

Il gruppo RADAR è emerso nel 2020 come **una costola della nota gang di ransomware LockBit**. Inizialmente, i membri erano coinvolti in operazioni di cybercrime sotto il marchio LockBit, ma hanno successivamente deciso di separarsi per perseguire strategie autonome. RADAR si è specializzato nell'implementazione di attacchi mirati e nel furto di dati sensibili, adottando un approccio che combina sofisticazione e aggressività.

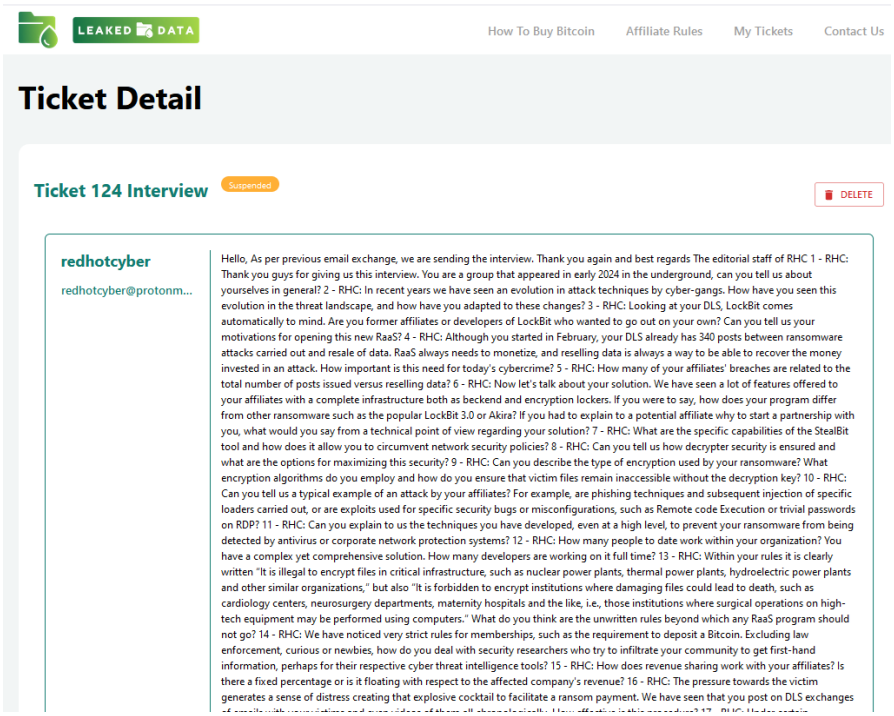
Il gruppo, intervistato a Luglio 2024, era noto per la sua struttura organizzativa e per l'uso di tecniche avanzate per compromettere le reti aziendali. Con un focus sull'estrazione di informazioni riservate e la richiesta di riscatti, RADAR ha rapidamente guadagnato notorietà nel panorama del cybercrime.

Data Leak Site (DLS) del gruppo RADAR and DISPOSSESSOR.
Il data lake site di RADAR and DISPOSSESSOR risulta molto simile a quello di Lockbit Si al a grafica che il modo di rappresentazione delle aziende violate risulta coerente relativamente a quanto riportato nell'intervista, che si tratta di EX affiliati di Lockbit.

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

La loro capacità di adattarsi rapidamente alle misure di sicurezza e di utilizzare strumenti all'avanguardia li ha resi una delle gang più temute nel settore. Nonostante la loro natura criminale, i membri di RADAR hanno mostrato un certo livello di collaborazione con altre gang nel corso delle loro operazioni. Questa rete di alleanze consente loro di **ampliare la portata delle loro attività illecite e di ottimizzare i profitti**. La loro crescente influenza nel panorama del cybercrime continua a rappresentare una *seria minaccia per le organizzazioni a livello globale*, spingendo le aziende a investire in misure di sicurezza sempre più robuste per proteggersi da attacchi sempre più sofisticati.
Ricordiamo che le infrastrutture di RADAR and DISPOSSESSOR sono state sequestrate da una operazione delle forze dell'ordine guidate dall'FBI ad inizio di Agosto del 2024.



Risposte alle domande all'interno del Backend di RADAR and DISPOSSESSOR

Nella sezione "Rules" vengono anche specificati quali target non potranno essere colpiti e viene riportato quanto segue: "È illegale crittografare file in infrastrutture critiche, come centrali nucleari, centrali termiche, centrali idroelettriche e altre organizzazioni simili. Autorizzato a rubare dati senza crittografia. Se non riesci a capire se un'organizzazione è un'infrastruttura critica, chiedi aiuto".

Seizure Wallpaper sul DLS di RADAR & DISPOSESSOR

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

QUILIN

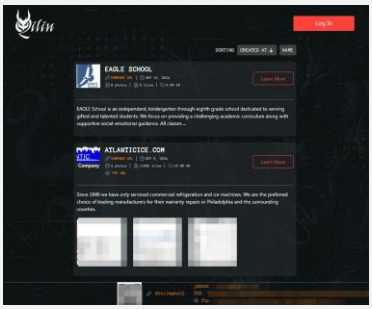
Il gruppo ransomware Qilin, emerso nel 2022, si è rapidamente fatto notare nel panorama della criminalità informatica grazie al suo modello **Ransomware-as-a-Service (RaaS).** Attraverso questo modello, gli affiliati pagano per utilizzare il ransomware e trattenere **l'80-85% dei riscatti estorti**, un incentivo particolarmente alto che ha attratto molti cybercriminali.

Inizialmente, il gruppo ha preferito programmare in Go, ma ha recentemente adottato **Rust**, linguaggio che *rende più complessa l'analisi del loro malware* e permette una maggiore flessibilità operativa.

Nell'intervista, effettuata a Settembre 2024, i membri del gruppo hanno discusso della loro strategia, che *include attacchi tramite doppia estorsione*. Non solo criptano i dati delle vittime, ma rubano anche informazioni sensibili, chiedendo un pagamento sia per il recupero dei file che per non divulgare i dati. Il gruppo sfrutta tecniche di phishing per infiltrarsi nelle reti aziendali e dispone di un data leak site per pubblicare i dati rubati, un elemento comune tra le cyber gang moderne.

Il loro modus operandi, come spiegato nell'intervista, è orientato al guadagno piuttosto che a obiettivi specifici. Qilin è attivamente coinvolto nel mercato del ransomware e opera con un'organizzazione ben strutturata, composta **da sviluppatori, manager e negoziatori.** La crescita del mercato RaaS è una delle ragioni per cui questo tipo di attacchi continua ad aumentare, rendendo la minaccia sempre più pervasiva nel cyberspazio.

Logo di Qulin Network



Data Leak Site (DLS) di QILIN
Il qilin (dal cinese :麒麟) è una leggendaria creatura chimerica ungulata che appare nella mitologia cinese e si dice che appaia con l'imminente arrivo o la scomparsa di un saggio o di un illustre sovrano.

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

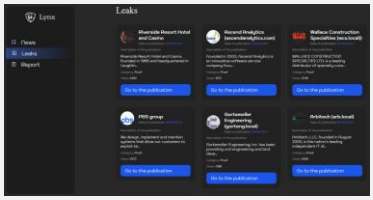
LYNX

Il gruppo Lynx Ransomware è emerso come una cyber gang con **un approccio atipico rispetto alle altre bande di ransomware**. Piuttosto che concentrarsi esclusivamente su attacchi distruttivi, Lynx si propone anche come fornitrice di servizi di penetration testing (pentest), offrendo alle aziende **violazioni "etiche"** per aiutarle a individuare e correggere le proprie vulnerabilità. Questo metodo non convenzionale *cerca di stabilire una linea sottile tra criminalità e consulenza*, dove la gang, pur richiedendo un riscatto per i dati criptati, promette di non rivendere le informazioni ottenute e di fornire alle aziende un rapporto dettagliato sulle falle di sicurezza scoperte.

L'intervista condotta da Red Hot Cyber a Settembre 2024 con Lynx rivela dettagli interessanti sul funzionamento interno del gruppo. Lynx ha sottolineato che, nonostante le apparenze, vedono il loro lavoro come un modo per **migliorare la sicurezza delle aziende,** puntando sulla **trasparenza delle operazioni** e cercando di distanziarsi dall'immagine *classica delle gang ransomware distruttive.*

Un punto di interesse è la loro offerta di report di vulnerabilità alle aziende attaccate, suggerendo soluzioni per rafforzare la sicurezza. Nonostante ciò, continuano a mantenere una posizione ambigua tra hacker etici e criminali.

La discussione ha anche toccato temi come la privacy e la sicurezza nel settore IT, *con Lynx che evidenzia come spesso le aziende non siano preparate a fronteggiare attacchi di questo tipo,* a causa di **amministratori di sistema poco formati e sistemi mal gestiti.** L'intervista si conclude con un tono di riflessione, lasciando intendere che Lynx, pur agendo da criminali, intenda *far luce sulle debolezze strutturali del sistema di cybersecurity aziendale.*



Data Leak Site (DLS) di LYNX
Il gruppo ha attivo (oltre ad un sito nella rete onion raggiungibile con TOR Browser) anche una istanza del data leak site sul clearweb. Al momento dell'intervista, il data leak site presentava un totale di 22 vittime.

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

STORMOUS

L'intervista di Red Hot Cyber al gruppo Stormous fornisce un'interessante panoramica su una delle cyber gang più note nel panorama dei ransomware.

Stormous, conosciuto per la sua **ideologia pro-russa** e la sua attività su piattaforme come Telegram, affonda le radici in un contesto geopolitico teso, sfruttando queste tensioni per *alimentare le sue campagne di attacco*.

La gang ha dichiarato **di essere nata ufficialmente nel 2019**, un periodo in cui il ransomware stava già diventando una minaccia globale, con un aumento esponenziale degli attacchi mirati a infrastrutture critiche e aziende private. Fin dai suoi primi passi, Stormous si è distinta per un approccio *altamente mirato e per la capacità di colpire obiettivi strategici*, dimostrando una sofisticazione tecnica notevole.

Il gruppo si è posizionato come una delle **voci più aggressive nella scena cyber criminale,** sfruttando non solo la potenza del ransomware ma anche **un'efficace propaganda sui social media**. La scelta di focalizzarsi su bersagli ben precisi, spesso legati a *paesi occidentali o aziende di rilevanza internazionale*, riflette una strategia calcolata che va oltre il mero profitto economico.

Uno degli elementi più caratteristici di Stormous è la **sua filosofia apertamente schierata**. La gang non nasconde la propria affiliazione ideologica, che alimenta una retorica di supporto alle cause pro-russe, rendendola **una minaccia non solo tecnica, ma anche politica**. Durante l'intervista, i membri del gruppo hanno sottolineato come *la loro attività sia motivata non solo dalla volontà di guadagno, ma anche da un obiettivo di destabilizzazione geopolitica.* Questo li distingue da molti altri gruppi ransomware, che operano **in modo più opportunistico e meno dichiaratamente ideologico.**

Data Leak Site (DLS) di Stormous
Il gruppo Stormous cambia spesso il proprio data leak site, questo è l'ultimo DLS che è stato realizzato e reso disponibile su telegram. Di seguito l'elenco delle vittime elencate nel DLS.

Canale Telegram di Stormous
Stormous ha dichiarato che monitorano costantemente le politiche di Telegram, e se necessario, migreranno verso piattaforme più sicure in risposta ai cambiamenti nei termini di utilizzo imposti dal gruppo di Pavel Durov. Questo suggerisce che, sebbene Telegram sia stato un canale chiave per le loro comunicazioni, il gruppo è pronto a spostarsi su altre piattaforme qualora le modifiche alle politiche lo rendano necessari

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

INTERLOCK

Tuttavia, dietro le loro dichiarazioni di responsabilità etica, *emergono obiettivi più cinici, come il guadagno economico e la manipolazione delle informazioni*. La loro attività evidenzia come **le vulnerabilità delle infrastrutture digitali rimanga un problema sistemico**, spesso aggravato da **errori umani** e configurazioni deboli. Il gruppo ha attirato l'attenzione non solo per il loro manifesto e le dichiarazioni audaci, ma anche per le *tecniche sofisticate adottate nei loro attacchi.*

La capacità di compromettere piattaforme robuste come **FreeBSD** dimostra una *conoscenza tecnica approfondita e un adattamento costante alle nuove sfide*. Le loro azioni mettono in luce non solo falle tecniche, ma anche una scarsa consapevolezza e preparazione delle aziende nel proteggere dati critici. I commenti di Interlock sui *comportamenti degli* ***amministratori di rete*** *riflettono un mix di osservazioni acute e un intento di umiliazione, che esemplificano la filosofia del gruppo*: sfruttare le **debolezze umane** e **tecniche** per rafforzare il proprio potere e influenza.

Questa intervista non solo permette di comprendere meglio le motivazioni e le tattiche di Interlock, ma sottolinea anche **l'importanza di strategie di sicurezza proattive**. La crescente integrazione dell'intelligenza artificiale e di tecnologie avanzate nella sicurezza rappresenta un'opportunità per contrastare minacce sempre più sofisticate. Tuttavia, come sottolineano gli stessi attori criminali, **nessun sistema può essere considerato invulnerabile**. L'obiettivo è trasformare questa conoscenza in strumenti pratici per la difesa, contribuendo a creare un ecosistema digitale più resiliente.

Data Leak Site (DLS) di Interlock
Il Data leak Site di Interlock è ben strutturato. Leggibile e accattivante tanto che gli abbiamo fatto inostri complimenti durante l'intervista. Il DLS ha un link «Data Leaks»

Interlock riporta nella sezione About As : *«Siamo INTERLOCK, un collettivo implacabile che smaschera la sconsideratezza delle aziende che non proteggono i loro beni più critici: i dati dei clienti e la proprietà intellettuale. Sfruttiamo le vulnerabilità che lasciano aperte, lanciando un duro ma necessario campanello d'allarme a chi pensa di poter tagliare i ponti con la sicurezza. Nel 2024, i numeri parlano da soli: gli attacchi ransomware sono aumentati di oltre il 20% nel solo secondo trimestre, con oltre la metà delle principali violazioni mondiali direttamente collegate alla negligenza aziendale. Le aziende continuano a gestire male le informazioni sensibili e il 60% delle violazioni è riconducibile a falle di sicurezza evitabili. Non si tratta solo di incompetenza, ma di indifferenza. E noi siamo qui per mostrare loro le conseguenze di questa negligenza».*

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

THREAT ACTORS

NUOVI THREAT ACTORS

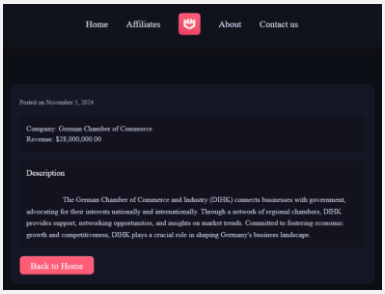
A cura di Alessio Stefan

I THREAT ACTORS

I NUOVI THREAT ACTORS

PLAYBOY

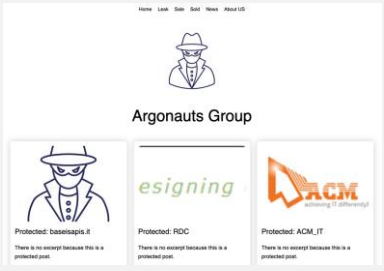
Scoperto a metà Ottobre il gruppo **PlayBoy** ha postato sul suo DLS la ***"German Chamber of Commerce"*** (Camera di Commercio Tedesca). **DarkLab** ha contattato il gruppo che aveva accettato di offrire risposte ad una intervista. Dopo l'invio delle domande, sia il **DLS** che il profilo **TOX** di **PlayBoy** risultano tutt'ora offline od irraggiungibili. L'unico attacco effettuato ha creato danni per diverso tempo facendo sì che si dovesse spegnere l'infrastruttura della Camera di Commercio Tedesca per poi riattivarla la settimana successiva. Ad oggi non si hanno ulteriori notizie a riguardo di questo gruppo.



Data Leak Site (DLS) del gruppo PlayBoy.

ARGONAUTS

Uno degli ultimi gruppi ad apparire nella scena a meno di 40 giorni dal 2025 (27 Novembre 2024), **Argonauts** ha fatto esplodere il suo DLS "vergine" con ben **10 vittime di cui 6 all'interno dei confini dello stivale.** I settori colpiti raccolgono ambienti professionali privati come aziende tranne una vittima (italiana) appartenente al settore **healthcare**. L'unica nuova vittima è stata registrata due giorno dopo (29 Novembre 2024) e si tratta di una azienda di **Taiwan** che si occupa di software e hardware per CCTV. Il DLS è stato designato per poter visionare i dati venduti e attualmente in vendita come secondo modo per monetizzare sulle vittime che rifiutano di collaborare pagando il riscatto richiesto.



Data Leak Site (DLS) del gruppo ransomware Argonauts

PLAYBOY

Dopo l'attacco a **Blue Yonder** nel mese di Novembre 2024, il gruppo **Termite** si è rapidamente guadagnato del prestigio da non sottovalutare. Le origini del gruppo risiedono nella famiglia **Babuk**, leakato interamente nel 2021. Le decine di vittime pubblicate nel DLS risiedono nei

I THREAT ACTORS

I NUOVI THREAT ACTORS

settori industriali e governativi in paesi come Canada, USA e Francia. Durante le indagini è stato evidenziato l'uso della vulnerabilità **CVE-2024-50623,** presente nei prodotti Cleo, che ha permesso l'accesso iniziale degli attaccanti. Presumibilmente il gruppo sarebbe attivo da metà Aprile 2024 ma è stato scoperto solamente nell'ultimo periodo del 2024.

TERMITE

Dopo l'attacco a **Blue Yonder** nel mese di Novembre 2024, il gruppo **Termite** si è rapidamente guadagnato del prestigio da non sottovalutare. Le origini del gruppo risiedono nella famiglia **Babuk**, leakato interamente nel 2021. Le decine di vittime pubblicate nel DLS risiedono nei settori industriali e governativi in paesi come Canada, USA e Francia. Durante le indagini è stato evidenziato l'uso della vulnerabilità **CVE-2024-50623,** presente nei prodotti Cleo, che ha permesso l'accesso iniziale degli attaccanti. Presumibilmente il gruppo sarebbe attivo da metà Aprile 2024 ma è stato scoperto solamente nell'ultimo periodo del 2024.

Ransom Note del gruppo ransomware Termite

CHORT

Chort ransomware è stato scoperto tramite il post su "X" da parte di un utente anonimo che pubblicò una foto del DLS con vittima la **città di Sheboygan (USA)**. Il 10 Novembre la stessa città ha dichiarato di non aver nessuna evidenza riguardo ad una potenziale intrusione sottolineando il monitoraggio della situazione dopo il post pubblicato, il gruppo ha risposto assegnando un riscatto di **$500.000**. Dopo la irruenta rivendicazione del gruppo diversi professionisti hanno assegnato la responsabilità di circa 50 attacchi a **Chort**, tutte le vittime sono appartenenti al settore education e governativo.

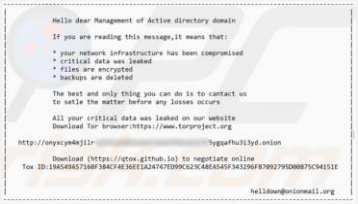
Data Leak Site (DLS) del gruppo ransomware CHORT

I THREAT ACTORS

I NUOVI THREAT ACTORS

HELLDOWN

Questa nuova famiglia Ransomware è da considerarsi tra le più aggressive delle nuove entry di questo secondo periodo del 2024. **Helldown** presenta una cifratura pesante comprendendo RSA, AES e Salsa20 nello stesso malware. Gli operatori di questo RaaS implementano nelle loro operazioni metodi sofisticati e armando vulnerabilità 0-days come quella di **Zyxel (CVE-2024-11667)**. Il codice di **Helldown** condivide la maggior parte di quello di **LockBit 3.0** (leakato nel 2022), recentemente questa nuova famiglia ha addattato il loro ransomware per poter impattare server **ESXi** suggerendo l'interesse nell'attaccare intere infrastrutture virtualizzate. Per poter ottenere informazioni sulla rete della vittima sul lungo periodo gli operatori Helldown creano nuovi account SSL VPN permettendo accesso da remoto che si mischia ad accessi leciti, questa metodologia permette di infiltrarsi in ambienti industriali e non di alto profilo come **Vindix**, **KBO Fire & Security** ed **XPERT Business Solutions.** Nella sola settimana del 12-18 Agosto Helldown ha pubblicato più di 30 vittime.



Helldown Ransom Note

INTERLOCK

Grazie ad un focus su sistemi FreeBSD il gruppo InterLock è stato, tra gli emergenti, il gruppo più svelto a crearsi un nome nel sistema ransomware. Intervistato da RHC Interlock ha fatto parlare di se grazie ad una persistente pubblicazioni di vittime nel loro DLS a partire da **Novembre 2024**. Tra le varie ipotesi emerge principalmente quella di una origine del loro ransomware proveniente da **Rhysida** sia per le TTPs del ransomware che dei tool custom usati dal gruppo stesso come un RAT per collezionare informazioni sulla vittima ed eseguire un keylogger inviando informazioni ad un server C2 controllato dagli attaccanti. L'ipotesi viene rafforzata dal "tema" del gruppo,

Data Leak Site (DLS) di Interlock
Il Data leak Site di Interlock è ben strutturato. Leggibile e accattivante tanto che gli abbiamo fatto inostri complimenti durante l'intervista. Il DLS ha un link «Data Leaks»

I THREAT ACTORS

I NUOVI THREAT ACTORS

presentandosi come professionisti sia nel loro DLS che nella Ransom note create sulle workstation delle vittime e anche dall'utilizzo di **AzCopy** per l'exfiltration dei file. Il gruppo presenta dei programmatori d'eccezione presentando una minaccia con un altissimo grado di adattabilità.

CYBERVOLK

Il collettivo di hacktivisti Russo ha deciso di monetizzare ulteriormente le loro operazioni tramite attacchi ransomware a partire dal periodo **Settembre-Ottobre 2024**. Il codice è basato su quello leakato di **AzzaSec** (gruppo italiano intervistato da RHC e successivamente rinominato **DoubleFace**) e come il suo predecessore è una variante malevola solo per Windows senza nessun tipo di porting o versione per Linux. Il loro servizio RaaS è stato aperto nel Giugno 2024 e sembrerebbe aver incluso altri gruppi di ransom-hacktivist come **HexaLocker** e **Parano**. Non sono presenti rivendicazioni esatte delle vittime ma viene dichiarato nel loro canale telegram di attaccare asset rilevanti per lo scenario geopolitico e un attacco (o serie di attacchi) in Giappone. Le comunicazioni ufficiali del gruppo sono state bloccate dopo i ban di massa perpetrati da telegram in seguito alla vicenda Francia-Durov, non sono disponibili per ciò ulteriori aggiornamenti.

Schermata che presenta l'esecuzione del ransomware CyberVolk su un computer Microsoft Windows

HELLCAT

Responsabile dell'attacco a **Schneider Electric** (Novembre 2024) richiedendo un pagamento di $125.000 in Baguettes, HellCat ha eseguito una formula vincente per far parlare di se attraverso le notizie dei media. Ad oggi le vittime di HellCat ammontano a 3 oltre a Schneider Electric : due vittime government (Israele e Giordania) e una education (Tanzania). Secondo gli analisti il gruppo ha cercato di pubblicizzarsi per una possibile transizione da gruppo autonomo a Ransomware-as-a-Service che potrebbe prendere piede gia a partire dal 2025.

Data Leak Site (DLS) di Hellcat

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

THREAT ACTORS

THREAT ACTORS EVOLUTION

A cura di Alessio Stefan

I THREAT ACTORS

THREAT ACTORS EVOLUTION

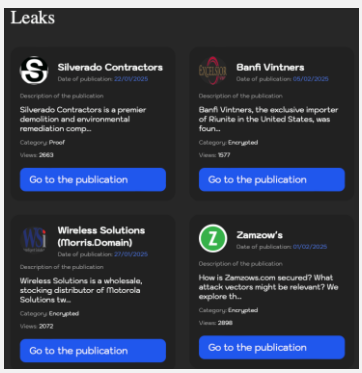
QILIN EVOLUTION

Tra i gruppi di maggior interesse nella seconda metà del 2024 non si può non citare **Qilin**. Il dragone dei RaaS si è dimostrato costante portando a termine dai 5 ai 15 attacchi al mese, in particolare **Settembre** è stato estremamente prolifico con ben **25 post pubblicati sul DLS**. Negli ultimi giorni di **Ottobre** una nuova variante del loro Ransomware è stata trovata ed analizzata sottolineando l'evoluzione del gruppo in termini di **Defense Evasion**. **Qilin.B** è il nome data a questa nuova variante (sempre in **Rust**) che pulisce in maniera continua i Log Eventi di Windows (**ETW**), terminare in maniera autonoma tutti i processi relativi a strumenti **EDR/AV**, **Backup** e di **Virtualizzazione**. In aggiunta, sono state apportate aggiunte lato **encryption**. Ora Qilin Ransomware utilizza l'algoritmo **RSA-4096 con padding OAEP** per rendere ancora piu difficile il recupero dei file lasciando come unica alternativa plausibile l'acquisto del **decryptor**. Il malware controlla se la workstation nella quale viene eseguito supporta **AESNI (**Intel **Advanced Encryption Standard New Instructions)** per poter utilizzare l'algoritmo **AES-256-CTR**, in caso tale feature non sia supportata Qilin.B utilizza il tradizionale **ChaCha20**. L'encryption rimane di tipo intermittente (**intermittent encryption**) dove solo parte dei file viene criptata. **Qilin** si dimostra sempre più violento ed allo innovativo allo stesso tempo, ad oggi la scelta dell'algoritmo da usare per la cifratura dei file in maniera dinamica è una tecnica mai trovata prima in un ransomware.

Logo del gruppo Qilin ransomware

LYNX - READY TO HUNT

Il Threat Intelligence Team di NexTron ha pubblicato la prima analisi del ransomware del gruppo **Lynx**. Queste prime evidenze mostrano una forte somiglianza tra questo ransomware e quello di **INC Ransom**.



Data leak Site (DLS) del gruppo ransomware Lynx

I THREAT ACTORS

THREAT ACTORS EVOLUTION

Tra i flag del malware abbiamo **--kill** per trovare e chiudere i processi/services contenenti le substrings **sql**, **veeam**, **backup**, **exchange**, **java** e **notepad** tramite **Restart Manager Function** (processi) e la funzione **ControlService** (services). Lato encryption viene implementata la architettura Thread di windows chiamata **IO Completion Port (IOCP)** per rendere parallela ed efficiente la fase di cifratura dei file. Il numero di thread creati è uguale al numero di processori, tipica configurazione per architetture **IOCP**. Tramite IOCP vengono passati gli handle dei file da criptare (in una coda tipo FIFO) che vengono poi gestiti in maniera concurrent dai diversi thread creati. Nel caso il processo del ransomware non abbia i permessi necessari per sovrascrivere il contenuto di un file viene eseguita una tecnica di Privilege Escalation con la creazione di un nuovo **SID** e corrispondente **DACL**. La chiava pubblica **ECC (Elliptic Curve Cryptography)** è cifrata ed hardcoded nel codice del malware, dopo essere stata decifrata viene utilizzata con l'algoritmo **Curve25519** ottenendo cosi uno shared secret. Da questo shared secret viene calcolato l'hash **SHA512** ottenendo cosi una chiave **AES**. Tramite la funzione ad-hoc **AESKeyExpansion** vengono generate le round keys. Anche Lynx cifra solo parte dei file aggiungendo un marker in coda al file contenente le chiavi pubbliche (sia **ECC** che **SHA512**). Oltre alle tradizionali tecniche presenti nei ransomware (ex:/ eliminazione di *shadow copies* e del malware stesso), Lynx procede ad enumerare, montare e criptare i file all'interno dei share SMB. Per concludere le ransom note vengono salvate all'interno della vittima e stampate su tutte le stampanti a disposizione.

AKIRA

Il RaaS **Akira** ha avuto dei movimenti interessanti e

I THREAT ACTORS

THREAT ACTORS EVOLUTION

sembrerebbe avere qualcosa in riserbo per il 2025. Dopo che la loro variante ransomware (scritta in C++) descritta come "military grade" è stata totalmente decriptata (nel 2023) il gruppo è apparentemente passato all'utilizzo di linguaggi diversi, specialmente **Rust** sia per la versione **Windows (MegaZord)** che **Linux (Akira_v2)** del ransomware. In questo periodo di transizione il gruppo è abbandonato la **doppia estorsione** occupandosi solamente di exfiltration e leak di dati. Dopo aver costruito la nuova versione del loro malware (Settembre 2024) il gruppo è tornato alla classica doppia estorsione. Nonostante il malware sia scritto (presumibilmente) da zero è interessante notare come le TTP e il flow di queste nuove versioni non si distanziano del tutto dalle versioni precedenti. È stato fatto notare come Akira abbia tratto molti vantaggi dopo **la chiusura di BlackCat** e **l'operazione Cronos contro LockBit** attraendo a sé un alto numero di affiliati. Akira in questo periodo ha sofisticato la sua capacità permettendo ora di attaccare **Server EXSi** con i loro tools. Per quanto concerne l'**initial access** Akira sta privilegiando l'utilizzo di zero-day come la **CVE-2024-40766** (SonicWall SSL VPN) su dispositivi che si affacciano su rete pubblica o tramite VPN della vittima. I processi di **Evasion**, soprattutto per quanto riguardo gli asset EXSi, sono stati rielaborati. Ora Akira crea una **VM** tramite file **VMDK** (usati da VMWare) o **OVA** dalla quale portare avanti altre operazioni senza però il rischio di essere rilevati da EDR o altri meccanismi di difesa. Tra queste operazioni abbiamo la **Privilege Escalation**. Dopo aver chiuso momentaneamente il domain controller della rete Active Directory, Akira copia e comprime (7z) il file **NTDS.dit** (datastore delle Active Directory) per poi trasferirlo all'interno della loro VM. Da li gli attori sono riusciti ad estrarre la chiave di decrypt per ottenere gli hash di tutti gli user (inclusi quelli ad alti privilegi)

Data leak Site (DLS) del gruppo ransomware Akira. L'interfaccia del blog risulta è stata realizzata con uno stile retrò stile anni 80. Sulla base dell'input testuale che gli utenti forniscono al sito è possibile visualizzare specifiche sezioni.

In questa sezione abbiamo digitato «leaks» per visualizzare il contenuto delle violazioni effettuate dal gruppo e dai suoi affiliati.

Schermata della sezione «news»

I THREAT ACTORS

THREAT ACTORS EVOLUTION

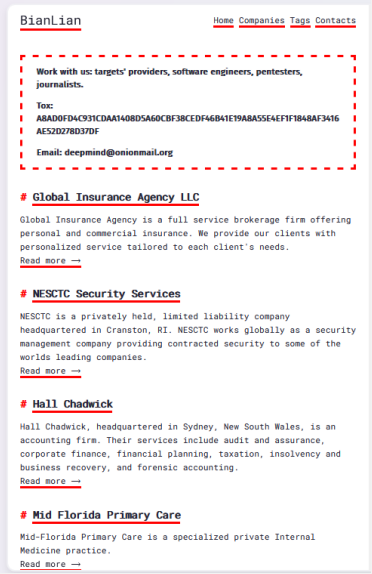
contenuta nell'hive del registro **SYSTEM.** Da qui in poi il gruppo ha effettuato movimenti laterali ed installato agenti RDP per persistenza fino all'exfiltration ed encryption dei dati. Per concludere nelle 24 ore tra **13 Novembre 2024 e 14 Novembre 2024** sono stati pubblicate 30 vittime nel loro DLS superando il loro record di vittime in una singola giornata, Akira sembra abbia preparato tutto il necessario non solo per il loro ritorno alle operazioni ma per superare le performance passate grazie ai cambiamenti nel landscape ransomware.

MEOW & BIANLIAN - NEW BUSINESS

Gruppo nato del 2022 con una solida attività fino ad oggi, il gruppo **Meow** ha deciso di cambiare totalmente modello di business **allontanandosi dal double-extortion model.** Ora **Meow si occupa solamente di furto e rivendita di dati sensibili** (range di prezzo $500-$200,000). Questo nuovo modello permette di effettuare attacchi con n minore livello di detection rispetto all'utilizzo di un ransomware. Il gruppo sembra preferire file contenenti informazioni personali e di tipo industriale. BianLian si sta affidando sempre di più all'utilizzo di strumenti come **Ngrok** e eseguibili UPX-packed. Similmente il RaaS **BianLian** da Gennaio 2024 ha esclusivamente basato le sue operazione nel furto di dati con tanto di minacce legali e/ocommerciali in caso di mancato pagamento. Nel loro caso viene addottato il protocollo **FTP** assieme a **RClone** e **MEGA Upload**.

HUNTERS - FILE SHARING & MANAGEMENT

Durante **Novembre 2024**, due investigazioni su due vittime diverse di **Hunters International** hanno portato alla luce un eseguibile Linux chiamato ***"storage_linux_x64"*** che



Data leak Site (DLS) del gruppo ransomware BIANLIAN. Come è possibile vedere, il gruppo mette subito in evidenza i propri contatti per eventuali collaborazioni.

Data leak Site (DLS) del gruppo ransomware BIANLIAN. Come è possibile vedere, il gruppo mette subito in evidenza i propri contatti per eventuali collaborazioni.

apparentemente non sembra essere maligno. Nella descrizione del eseguibile si capisce che tale programma è usato per gestire i dati rubati, inoltre sembra essere molto di più di un software per file upload permettendo di categorizzare e condividere i dati esfiltrati. Per ora non si hanno ulteriori dettagli a riguardo ma dalle prime investigazioni sembrerebbe che **Hunters International** abbia creato e utilizzi una infrastruttura per un **storage**

CLOAK - DRIVE-BY ATTACK

Halcyon ha rilasciato un report ufficiale riguardo nuovi metodi di persistenza e initial access utilizzati dagli operatori di **Cloak Ransomware**. Il malware viene mascherato come un normale **update di Windows** o altri software comunemente usati dagli utenti permettendo così l'accesso agli operatori. Oltre a ciò viene implementata una nuova variante (basata sul codice di Babuk) ed un disincentivo nell'acquisto dagli Initial Access Broker preferendo exploit kits e social engineering. Nell'arco della seconda metà del 2024 il gruppo ha ottenuto una probabilità (stimata) di pagamento nel range 90%-95%. La nuova variante contiene tecniche sofisticate per quanto concerne la persistenza ed enumerazione dei file da cifrare (potendo selezionare tra cifratura intera o intermittente). Inoltre per bloccare operazioni di shutdown o restart da parte dell'utente vengono modificate delle registry keys pima di iniziare il processo di cifratura dei file. Sempre secondo le analisi di Halcyon, il gruppo sembrerebbe avere una collaborazione attiva con **Good Day** (ex:/

I THREAT ACTORS

THREAT ACTORS EVOLUTION

condivisione di una piattaforma DLS) evidenziando l'aumento della influenza di Cloak sia presente che futura.

PHOBOS - DECLINO

Dopo l'arresto di Evgenii Ptitsyn, responsabile di **Phobos Ransomware,** le operazioni di uno dei RaaS più persistenti di sempre sono vicine al totale declino. Dopo un picco raggiunto nel mese di **Luglio 2024**, con conseguente leak del loro backend e source code, le vittime di Phobos stanno scendendo in picchiata. Phobos era riuscito in un'impresa difficile da attuare, rimanere nascosti ed allo stesso tempo avere un alto numero di vittime, nonostante la loro continuità nell'ambiente l'arresto di Ptitsyn segna un futuro tutt'altro che florido. Molti utenti del forum RAMP stanno già offrendo alternative a Phobos cambiando il codice interno in cambio di denaro, si scoprirà se il 2025 vedrà l'eredità di Phobos in azione oppure se con la fine del 2024 si segna anche quella di uno di RaaS più veterani presenti nella scena.

RHYSIDA - EVIL2

Rhysida è stato uno dei RaaS che ha maggiormente beneficiato da **Operation Cronos** che ha avuto come bersaglio **LockBit** attraendo a se nuovi affiliati e prendendo questa opportunità per potenziare i propri servizi. In questo periodo Rhysida ha eseguito una serie di attacchi sia a **cliniche** (private e pubbliche) che ospedali negli USA ed Europa Centrale con una deadline per il pagamento di una settimana non negoziabile. Il RaaS presenta una nuova minaccia per il **settore healthcare** come lo è stato **Conti** tra il 2020 e 2022, in tutto ciò il rateo delle campagne in settori come manifatturiero e technology rimangono invariati permettendo al gruppo di avere diversi fonti di

Data leak Site (DLS) del gruppo ransomware Rhysida. Il gruppo ransomware generalmente mette all'asta i dati delle aziende violate prima della pubblicazione sul data leak site per poter massimizzare il ritorno economico del gruppo e dei suoi affiliati.

I THREAT ACTORS

THREAT ACTORS EVOLUTION

monetizzazione. Nel settore education Rhysida non ha perso occasione per farsi notare come ad esempio nel caso del **distretto scolastico Tennessee** richiedendo $2 MLN dopo aver impattato la rete il 25 Novembre 2024 (confermato dalla vittima il 1 Dicembre 2024), attacco analogo in Louisiana (**$1.4 MLN**) ed **Henry County Schools** accompagnato da un breach completo di buona parte dei dati inclusi quelli di insegnanti e studenti. Il riscatto medio nel settore education di Rhysida è stimato a circa **$500.00.** Ricordiamo che questo RaaS è lo stesso che ha colpito il **porto di Seattle** ($6 MLN) e **Città di Colombus** con ben 6.5 TB di dati rubati. **Recorded Future ha pubblicato un report unicamente su Rhysida** mostrando come le loro soluzioni siano efficaci per prevenire tale minaccia e mostrando una analisi che collega Rhysida all'ormai scomparso gruppo **Vice Society.**

I THREAT ACTORS

THREAT ACTORS EVOLUTION

HELLDOWN - STEAL DEVOTION

Osint10x ha avuto l'occasione di intervistare l'admin di Hellcat Ransomware che vige sotto il moniker ***"Pryx"***. In questa interessante discussione viene portata alla luce un serie di post pubblicati dallo stesso admin in vari forum riguardo ai ***server-side stealer***, una nuova tecnica che permetterebbe di evadere EDR ed AV in maniera efficiente rispetto ai tradizionali infostealer. Invece di inviare direttamente i dati al server C2, questo nuovo concept di malware estrarebbe tutti i dati necessari come un tradizionale infostealer e li hosterebbe in un sito TOR creato direttamente sulla macchina della vittima. Dopo aver ricevuto l'indirizzo **.onion** gli attori procederebbe ad estrarre i dati con una richiesta do tipo ***GET***. In questa maniera il servizio TOR della vittima si occuperebbere di un semplice file listing che potrà essere raccolto in maniera istantanea tramite script attivati direttamente dal server C2. Per ora, stando alle parola di ***Pryx***, il loro malware

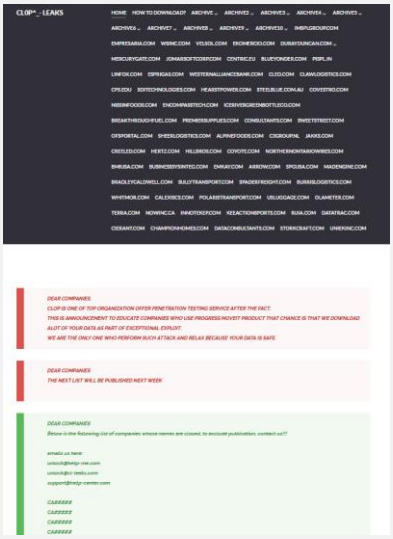
I THREAT ACTORS

THREAT ACTORS EVOLUTION

permette semplicemente di hostare il sito TOR ed inviarne l'indirizzo agli operatori senza nessuna vera e propria attività di ***stealing***. Oltre a ciò, nell'intervista viene evidenziata l'abilità dell'admin di Hellcat nel weaponizare e concatenare più vulnerabilità assieme per ottenere accesso nelle reti delle vittime dando il via alle attività di red teaming ed infine di cifratura in maniera modulare e scalabile. Nonostante il gruppo sia appena affiorato si può notare una alta dedizione e continuità nel espandere le capacità di attacco all'interno del RaaS rendendolo un ottimo candidato da tenere sott'occhio nel 2025.

CLOP - PLEAD GUILTY

Il RaaS **CLoP** si è da sempre reso noto per le sue capacità nello sviluppare e modificare a proprio piacimento vulnerabilità 0-days permettendo di attaccare asset responsabili della supply chain come, ad esempio, l'enorme breach ai danni di **MoveIT** nel 2023**.** Recentemente il gruppo ha dichiarato a [BleepingComputer] di essere responsabili del data breach di **Cleo** tramite la **CVE-2024-55956** che sfruttava una gap di sicurezza non propriamente mitigato dopo la patch per la precedente vulnerabilità **CVE-2024-50623**. Il gruppo ha anche confermato che il loro *"progetto"* contro **Cleo** era stato pianificato ed elaborato da tempo permettendogli di creare un danno massivo a chiunque utilizzasse i software di **Cleo** per condivisione e trasferimento di file. Il governo statunitense ha infine pubblicato una taglia di valore (massimo) **$10 MLN** per chiunque dia informazioni o porti all'arresto di chiunque sia connesso alle attività del gruppo. Il gruppo sta dimostrando da più di un anno di essere altamente specializzato nell'attaccare aziende specializzate nella gestione di file prendendo posizione come minaccia sofisticata capace di impattare su più organizzazioni con un singolo attacco.



Data leak Site (DLS) del gruppo ransomware CL0P. Come si può vedere, a differenza di altri DLS, il sito si presenta con una lista di tutte le violazioni condotte dal gruppo.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Raffaella Crisci, Edoardo Faccioli, Alessio Stefan

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

L'alba illumina i grattacieli di Manhattan, ma dentro l'ufficio di un'importante banca d'investimento regna il caos. Decine di schermi, che normalmente mostrano flussi di dati e numeri in continuo movimento, sono ora spenti o bloccati su un messaggio agghiacciante: "I vostri dati sono criptati. Pagate 10 milioni in Bitcoin entro 72 ore, o li cancelleremo per sempre."

INTRODUZIONE

Nel reparto IT, il direttore osserva i log del sistema con crescente panico. I firewall, apparentemente impenetrabili, sono stati aggirati. Nessuno sa come sia successo, ma una cosa è chiara: l'attacco è devastante. Tutti i backup sono inaccessibili, i clienti sono già al telefono in cerca di risposte e il CEO vuole sapere una cosa sola: *"Chi sono questi criminali?"*

Dietro l'attacco si cela Evil Corp, un'organizzazione di cybercriminali così sofisticata che molti esperti la considerano l'equivalente digitale di un cartello della droga. Ma invece di trafficare cocaina, Evil Corp traffica in qualcosa di molto più prezioso: informazioni e denaro virtuale.

Evil Corp, noto anche come Indrik Spider e Dridex gang, è coinvolto in attività di cybercriminalità dal 2007, inizialmente come affiliato di altre organizzazioni. Le loro attività collegate allo scenario ransomware coinvolgono lo sviluppo di malware ad hoc e l'affiliazione con popolari gruppi RaaS tra cui ***LockBit*** che dopo essere stato obiettivo di **Operation Cronos (2024)** ha permesso alle forze di intelligence di tracciare ulteriormente le attività di Evil Corp. In questa sezione verrà offerta una sintesi comprensiva di tutto ciò che si è scoperto di Evil Corp fino ad oggi grazie alla lunga serie di azioni eseguita principalmente da NCA ed FBI. Evil Corp è un ottimo esempio di come il crimine si stia trasformando passando dalle tradizionali rapine armate in banca a tecniche informatiche sofisticate al fine di estorcere denaro dal settore pubblico e privato esclusivamente da remoto.

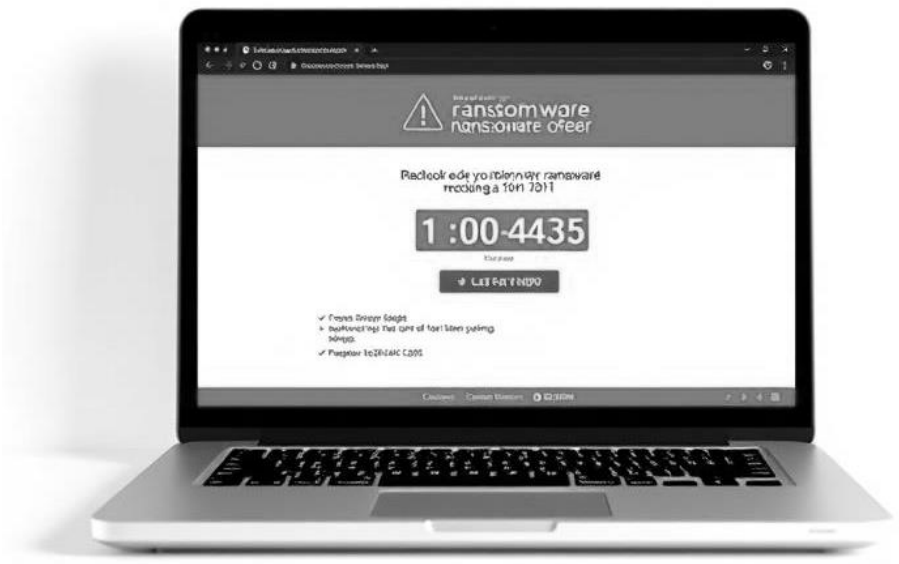
EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

PANORAMICA

Le origini di Evil Corp sono difficili da definire con esattezza a causa della loro rapida evoluzione che avviene dalla sua scoperta nel **2014**. Il gruppo avrebbe iniziato nella scena criminale russofona rinominata ***"The Business Club"*** nel primo periodo del 2007 per poi emergere come gruppo consolidato e a sè stante negli anni successivi. Da quel periodo in poi il gruppo è risultato un ibrido tra operazioni interne e supporto a RaaS esterni con costanza e abilità superiori alla media. Tra le operazioni tracciate abbiamo :

- **Campagne Malware:** ***Dridex*** è stato un trojan bancario diffuso tramite **Macro** di **Microsoft Word.** I primi artefatti furono scoperti nel 2015 con una stima di £20 MLN e $10 MLN rispettivamente in UK e USA. Nei primi mesi del 2016 il trojan è stato sviluppato in nuove versioni che permettevano il furto di chiavi per wallet di criptovalute. Dridex è la fusione di due varianti passate chiamate ***Cridex*** e ***Bugat.*** Tra le vittime di queste operazioni sono incluse ***Penneco Oil Company*** (furto di $3.5 MLN) e ***Franciscan Sisters of Chicago*** ($24.000 da un centro religioso)



EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

- **Phishing:** Le attività di Evil Corp si affidavano a campagne di **spear phishing** per ottenere un primo accesso o infettare la vittima con i loro tools. Il tipo di schemi utilizzate in tale campagne erano estremamente diverse in base al tipo di settore della vittima permettendo persino di ottenere credenziali illudendo l'utente senza la necessità di software esterni.

- **Operazioni Ransomware :** Il business model del gruppo rimane tutt'ora il ransomware. Il gruppo ha sviluppato ed utilizzato le varianti **BitPaymer** e **WastedLocker**, dopo le sanzioni del 2019 Evil Corp ha aderito a diversi programmi affiliazioni RaaS (Hades, PhoenixLocker, Lockbit) per poter mascherare gli autori degli attacchi.

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

CASI DI STUDIO

Di seguito alcuni attacchi che sono stati perpetrati da parte di Evil Corp negli ultimi anni :

- **Ransomware alla città di Baltimore (2019):** Il 7 Maggio 2019 la infrastruttura digitale governativa della città di Baltimora ha dovuto essere spenta a causa del Ransomware **RobinHood.** Questa versione venne descritta come altamente aggressiva che ha bersagliato tutti gli asset presenti nel sistema indipendentemente dal sistema operativo usato. Nella ransom note venivano richiesti 13 BTC per il riscatto (al tempo $76.000) con scadenza di 10 giorni, l'attacco ha evidenziato la mancanza di budget e pianificazioni per quanto concerne la **Information Security** in infrastrutture governative. Lo stesso ransomware è stato usato nel **2018** in **Atlanta.**
- **US Voting Systems (2020) :** Nel periodo COVID, Evil Corp ha adattato le sue campagne malevole alle necessità dei lavoratori di operare in remoto per le loro aziende. Sempre tramite spear-phishing ed il loro armamentario hanno ottenuto accesso in meno di un anno alle reti interne di 31 organizzazioni (8 di queste rientravano tra le **Fortune 500**) in meno di un anno. Tra le vittime erano presenti infrastrutture di supporto al sistema di votazioni online degli USA oltre municipi di città americane (Oregon, Maryland, Texas, Florida e Georgia), parte delle intrusioni sono state bloccate in tempo prima di ulteriori movimenti da parte degli attaccanti.
- **Olympus & Sinclair Broadcast Group (2021) :** Come gia descirtto, dopo le sanzioni del 2019 il gruppo è stato forzato a fare un rebranding del loro encryptor **DoppelPaymer** più volte. Nel 2021 **Sinclair Group** (broadcast TV) e **Olympus** (tecnologie mediche) sono state colpite da una di queste varianti chiamata **Macaw** richiedendo rispettivamente **$40 e $28 MLN.**

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

OPERAZIONI LAW ENFORCEMENT

Maksim Yakubets, noto con i soprannomi ***"aqua"*** e ***"aquamo"***, non è lo stereotipo dell' "hacker" nascosto nell'ombra. Leader di Evil Corp, vive una vita di lusso, guidando auto sportive e frequentando i migliori locali di Mosca. Soprannominato "**il Re del Cybercrime"**, Yakubets è noto per la sua arroganza: le indagini delle autorità hanno provato come abbia trasformato il cybercrimine in una vera e propria azienda, con dipendenti, gerarchie e operazioni strutturate. Yakubets è sospettato anche di aver collaborato con altri gruppi come **Trickbot**, evidenziando una buona dose di esperienza nell'ambiente criminale**.**

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

Maksim Yakubets è noto per il suo stile di vita lussuoso celebrando il suo matrimonio del 2017 con tanto di cerimonia sontuosa, spendendo fino a $600.000. Le immagini e i video confiscati dalle autorità britanniche mostrano Yakubets e altri membri di Evil Corp che guidano supercar e vivono nel lusso. Questo stile di vita ostentato ha attirato l'attenzione delle autorità e dei media, contribuendo a dipingere un quadro chiaro della portata delle loro attività criminali.

EVIL CORPS

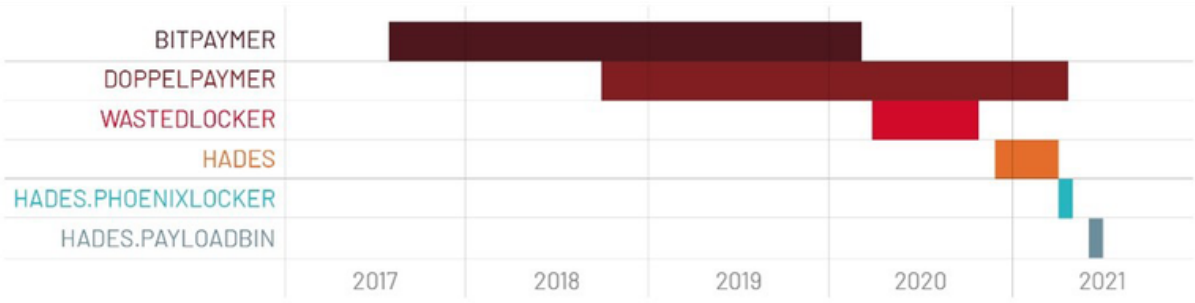
L'ECONOMIA DEL RANSOMWARE

A differenza di molti gruppi di cybercriminali russi che hanno una struttura di leadership distribuita online, Evil Corp è organizzato come un sindacato criminale tradizionale attorno a familiari e amici di Yakubets. Suo padre, Viktor Yakubets, ha un passato nel riciclaggio di denaro assieme ad altri membri della famiglia Yakubets coinvolti nel gruppo. Il gruppo ha operato da luoghi fisici, tra cui il ***Chianti Café*** e lo ***Scenario Café a Mosca***.

SANZIONI E ADATTAMENTO

Le sanzioni imposte dagli Stati Uniti nel 2019 hanno costretto Evil Corp a modificare profondamente le sue tattiche per evitare l'attribuzione. Da allora, il gruppo ha adottato nuove tecniche e strumenti, tra cui il framework **SocGholish** e **Cobalt Strike**, per penetrare e muoversi nelle reti delle vittime. Inoltre, ha sviluppato e utilizzato una serie di varianti di ransomware per rimanere operativo:

- **WastedLocker (2020)**: Un nuovo ransomware che ha mostrato somiglianze con BitPaymer e Dridex utilizzato per attacchi mirati contro le grandi aziende.
- **Hades (2020)**: Una versione compilata a 64 bit di WastedLocker con sovrapposizioni di codice e funzionalità, utilizzata per attacchi più sofisticati.
- **Phoenix Locker (2021)**: Una versione rebrandizzata di Hades con poche modifiche, utilizzata per confondere le autorità e le vittime.
- **PayloadBIN**: Una continuazione di Phoenix Locker con funzioni sovrapposte, utilizzata per attacchi mirati.
- **Macaw Locker (2021)**: Un nuovo ransomware utilizzato per attacchi contro Olympus e Sinclair Broadcast Group, con richieste di riscatto fino a 40 milioni di dollari.



MANDIANT

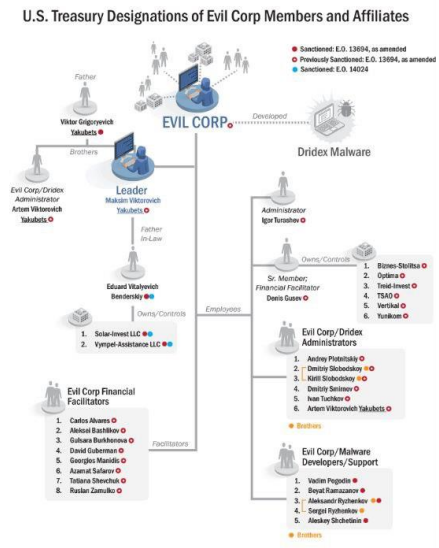
EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Nonostante le sanzioni e le operazioni delle forze dell'ordine, Evil Corp continua a evolversi e adattarsi. Il gruppo ha dimostrato una notevole capacità di cambiare tattiche e strumenti per evitare il rilevamento e mantenere le loro operazioni redditizie. La continua collaborazione tra le forze dell'ordine internazionali e le sanzioni economiche rappresentano una sfida significativa per Evil Corp, ma il gruppo rimane una minaccia persistente nel panorama del cybercrime.

SANZIONI E ADATTAMENTO

Eduard Benderskiy



Struttura di Evil Corp

Molti dei cybercriminali più ricercati dall'FBI sono russofoni. Alcuni lavorano per il governo con stipendi normali, mentre altri accumulano fortune attraverso le operazioni malevole. Se lasciassero la Russia, verrebbero arrestati, ma in patria non sembra esserci interesse ad aprire delle investigazioni.
Le indagini suggeriscono che Evil Corp operi con il tacito consenso delle autorità russe. Alcuni esperti ipotizzano che il gruppo sia persino in contatto con servizi segreti russi (come FSB), utilizzando le loro operazioni per sabotare gli avversari geopolitici di Mosca. **Eduard Benderskiy**, ex alto funzionario **dell'FSB**, ha facilitato le relazioni tra Evil Corp ed i servizi di intelligence russi. Dopo che gli Stati Uniti hanno nominato e incriminato diversi membri di Evil Corp nel 2019, Benderskiy ha utilizzato la sua influenza per proteggere il gruppo, fornendo sicurezza ai membri senior e assicurandosi che non fossero perseguiti dalle autorità interne russe.

DEANON

Gli Stati Uniti hanno coordinato la caccia ad Evil Corp, imponendo sanzioni economiche contro **Yakubets** e i suoi collaboratori. Nel 2019, l'FBI ha emesso un mandato di arresto per **Yakubets**, descrivendolo come uno dei criminali digitali più ricercati al mondo mentre il

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Dipartimento di Giustizia degli Stati Uniti ha offerto una ricompensa fino a $5 MLN per informazioni che portino al suo arresto e condanna. Durante questo periodo le forze di intelligence sono riuscite a ricostruire la struttura del gruppo. Evil Corp opera in un'area grigia del diritto internazionale dove la Russia non concede estradizioni per i propri cittadini e spesso protegge criminali come Yakubets, soprattutto quando le loro attività sembrano coincidere con gli interessi strategici dello Stato. Questo, unito alle tensioni geopolitiche, complica la cooperazione con altri Paesi.

Nonostante ciò, operazioni internazionali recenti hanno preso di mira infrastrutture legate a Evil Corp, come il sequestro di server e portafogli cripto utilizzati per gestire riscatti, infliggendo loro un duro colpo finanziario.

Inoltre, pressioni diplomatiche e un coordinamento più ampio tra le autorità hanno portato ad azioni come il recente arresto di Wazawaka, un criminale legato a gruppi di ransomware collegati indirettamente a Evil Corp. Queste operazioni riflettono un approccio sempre più proattivo nella lotta contro i gruppi di ransomware, considerati non solo una minaccia economica, ma anche un rischio per la sicurezza globale, specialmente quando agiscono sotto il tacito sostegno di regimi autoritari.

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Queste azioni riflettono un approccio sempre più proattivo nella lotta contro i gruppi ransomware, considerati non solo una minaccia economica, ma anche un rischio per la sicurezza nazionale, soprattutto quando agiscono con il tacito sostegno di regimi che sfruttano il cybercrimine come leva geopolitica.

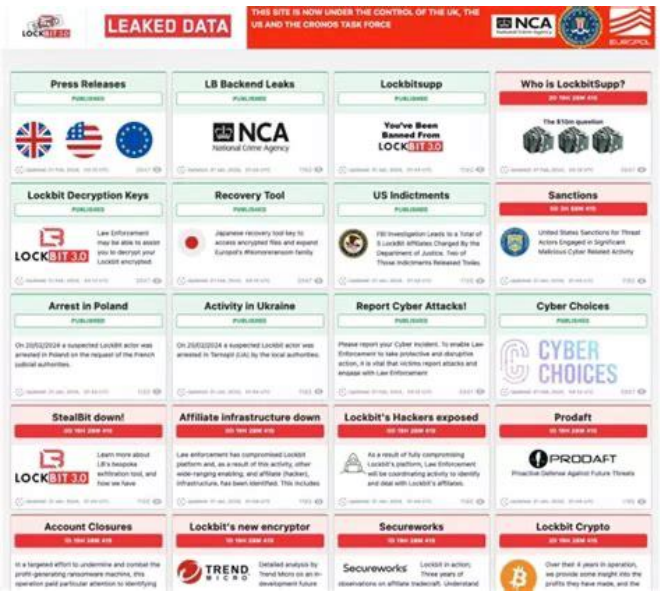
CAT & MOUSE GAME

Aleksandr Ryzhenkov

Evil Corp non è solo un gruppo di persone: è un'idea di una intera struttura atta a sfruttare le vulnerabilità di un mondo sempre più connesso. Le sanzioni del 2019 hanno danneggiato il marchio e le entrate di Evil Corp, costringendo il gruppo a cambiare tattiche e a nascondere meglio le proprie attività. Le tensioni interne hanno portato alla separazione di Igor Turashev, che ha sviluppato il ransomware **DoppelPaymer**. I membri rimanenti hanno abbracciato nuovi tipi di ransomware, con **Yakubets** e **Ryzhenkov** che hanno guidato lo sviluppo di **WastedLocker**.

OPERATION CRONOS

Un'operazione globale ha portato all'arresto di quattro sospetti legati agli attacchi ransomware **LockBit**, fornendo nuove informazioni sulle interconnessioni tra questo gruppo ed Evil Corp. Aleksandr Ryzhenkov, alias "Beverley" e ex vice leader di Evil Corp, è stato identificato come affiliato di LockBit. Si stima che abbia prodotto oltre 60 build di ransomware LockBit**,** tentando di estorcere più di $100 MLN alle vittime. Questi collegamenti tra i due gruppi criminali sono emersi durante la **terza fase dell'Operazione Cronos**, che ha smantellato parte dell'infrastruttura di LockBit nel febbraio 2024 e svelato la collaborazione tra il RaaS ed Evil Corp.



Tale collaborazione fu attuata anche per circumnavigare le sanzioni imposte mascherando i guadagni di Evil Corp sotto il brand di LockBit.

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

EVOLUZIONE E FUTURO

Evil Corp ha dimostrato un'enorme capacità di adattamento, passando dallo sviluppo di ransomware proprietari all'uso di strumenti di terze parti come LockBit per aggirare le restrizioni. Questa resilienza e la continua evoluzione delle tattiche lo rendono uno dei gruppi più pericolosi e complessi nel panorama del cybercrime globale. Nonostante gli arresti e le operazioni delle forze dell'ordine, la minaccia persiste, evidenziando la necessità di uno sforzo globale continuo per contrastare questi gruppi. Le autorità di tutto il mondo continuano a monitorare e perseguire i membri di Evil Corp. La collaborazione internazionale e l'uso di sanzioni economiche sono strumenti chiave nella lotta contro questo gruppo di cybercriminali. Tuttavia, la natura globale e adattabile dell'ecosistema significa che la caccia è tutt'altro che finita.

CRIPTOVALUTE E BLOCKCHAIN

L'economia dietro al mondo ransomware è un ecosistema altamente complesso e strutturato, alimentato dalle ingenti somme di denaro coinvolte e dalle difficoltà legate alla conversione delle principali **criptovalute** in denaro **FIAT** spendibile sul mercato libero. Questi ostacoli rappresentano una sfida importante per i gruppi criminali, desiderosi di condurre vite di lusso e acquisire beni di valore senza attirare l'attenzione delle autorità.
Per affrontare queste sfide, le ransom gang adottano strutture organizzative sofisticate che includono attori specializzati negli attacchi, negoziazione dei riscatti, gestione dei fondi rubati e **riciclaggio**.

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

In questa sezione del report, analizzeremo le tecniche più utilizzate da gruppi come **Evil Corp** e **Lockbit** (recentemente colpito dall'operazione Cronos), concentrandoci sul ruolo fondamentale delle criptovalute e sulle tecniche più comuni utilizzate per bypassare i controlli di identità e tracciabilità imposti dalle agenzie finanziarie globali o dalle forze dell'ordine.

Le criptovalute sono diventate uno strumento chiave nell'ecosistema del ransomware, principalmente per le loro caratteristiche di **anonimato**, **decentralizzazione** e **facilità di trasferimento** globale. I criminali informatici utilizzano le criptovalute, in particolare **Bitcoin** ed altre *"altcoin"* come **Monero** o **ZCash**, per richiedere riscatti alle vittime senza rischiare di essere facilmente identificati o rintracciati dalle forze dell'ordine.

Inoltre, l'utilizzo delle criptovalute permette di gestire meglio i flussi di denaro illeciti e il riciclaggio di questi ultimi grazie ai molteplici sistemi offerti dalla finanza decentralizzata (**DeFi**), come i protocolli di **Mixing**, **CoinJoin** o **AtomicSwap**.

Criptovaluta
E' una valuta digitale o virtuale che utilizza la crittografia e si basa su una rete distribuita e decentralizzata che elimina la necessità di un intermediario come banche o governi.

Blockchain
E' un registro distribuito e immutabile formato da blocchi nel quale vengono inserite tutte le transazioni effettuate che a loro volta vengono convalidati.

DeFi Finanza Decentralizzata
E' l'insieme di funzioni finanziarie basate sulla tecnologia bloackchain e pertanto permette di offrire differenti servizi finanziari senza l'uso di intermediari

Mixing
Servizi che permettono di riversare il bilancio di un wallet su una pool pubblica e poter riottenere la stessa quantità su un wallet diverso. Questi servizi permettono di anonimizzare la sorgente dei fondi ottenuti dove il prelievo, complicando le operazioni delle indagini forensi.

AtomicSwap
Protocollo che permette lo scambio di due criptovalute diverse senza la necessità di appoggiarsi a valuta FIAT o terze parti. Tra le transazioni più comuni abbiamo **BTC > XMR, XMR > BTC** ed **ETH > BTC.** Solo un sottogruppo di criptovalute permette tale operazione.

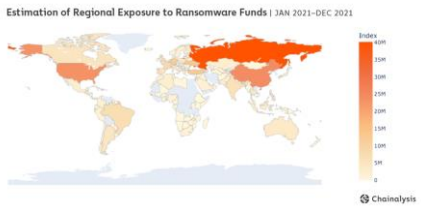
EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

LOCKBIT - EVIL CORP E OPERATION CRONOS

Durante l'ultima operazione congiunta delle forze dell'ordine per smantellare la struttura RaaS (Ransomware as a Service) di Lockbit, è stato sanzionato **Aleksandr Ryzhenkov**, membro di **Evil Corp** e affiliato attivo di **LockBit**. Questo collegamento, insieme alle analisi sui flussi di denaro, ha permesso di identificare un legame tra il gruppo ransomware LockBit e il gruppo criminale Evil Corp.

Federation Tower, Mosca



Densità di fondi illeciti provenienti da ransomware per paese (Chainalysis)

MOSCA EI FLUSSI DI DENARO

Evil Nel 2021, un'analisi condotta da Chainalysis aveva evidenziato come il flusso di denaro proveniente dai pagamenti in criptovalute effettuati dalle vittime ai gruppi ransomware finisse in grandi exchange e fornitori di servizi crypto con sede in Russia, prevalentemente nella città di Mosca. In particolare, la **Federation Tower**, un edificio situato nel cuore della capitale russa, sede di diverse aziende di criptovalute avrebbe ricevuto più di metà del denaro analizzato nella loro analisi. Con un totale di $36 MLN, la Federation Tower non è nuova a scandali riguardanti il riciclaggio di denaro [1][2][3].

OPERAZIONE CRONOS E IL RICICLAGGIO CRIPTO

Con il terzo atto dell'Operazione Cronos, le forze dell'ordine sono riuscite a smantellare parte della vasta infrastruttura di **LockBit**, facendo luce sulle modalità di gestione dei pagamenti ottenuti attraverso i riscatti imposti alle vittime.
Nel corso dell'operazione, l'NCA (National Crime Agency) ha ottenuto accesso a **30.000 wallet Bitcoin**, di cui oltre 500 risultano attivi e hanno ricevuto più di **120 milioni di dollari [4]** tra luglio 2022 e febbraio 2024. Considerando l'intero periodo di attività del gruppo, è probabile che il volume totale del denaro rubato sia molto più elevato.
È importante sottolineare che i fondi rilevati corrispondono

Fonte: **NCA**

ai pagamenti delle vittime a favore di LockBit, ma non includono il 20% che gli affiliati devono cedere agli sviluppatori del malware. Questo implica che il totale delle estorsioni richieste da Lockbit potrebbe essere ancora più elevato.

Il flusso di denaro gestito da LockBit seguiva un percorso complesso per evitare di essere tracciato. Dopo l'attacco, alla vittima veniva indicato dove effettuare il pagamento; da quel momento, il gruppo avviava varie tecniche di **mixaggio** e offuscamento delle transazioni. Tra queste, spiccava l'utilizzo delle tecniche di **CoinJoin** offerte da **Wasabi Wallet**, che consentivano di mescolare i fondi con quelli di altri utenti, rendendo più difficile risalire all'origine.

Oltre al mixaggio, venivano sfruttati metodi di **scambio** tra criptovalute per spostare i fondi su altre blockchain, come **Monero** e **Zcash**, note per le loro funzionalità di privacy avanzata. Questi scambi venivano gestiti tramite piattaforme di exchange come **ChangeNOW** e **SimpleSwap**, che permettevano conversioni rapide e facilitavano il passaggio ad altre criptovalute.

Queste evidenze mettono in luce la limitata efficacia dei controlli KYC (Know Your Customer) e AML (Anti-Money Laundering) richiesti per gli strumenti DeFi perché i gruppi criminali continuano a trovare modi per aggirarli, sfruttando, molto probabilmente identità false, **money mule** oppure strumenti DeFi che hanno sede in paesi dove la normativa antiriciclaggio è meno stringente.

DARK MONEY - TRAILER

"Dark Money: Crimine e Criptovalute"
Un mondo invisibile, fatto di transazioni anonime, mercati sommersi e crimini senza confini.
Cosa unisce ransomware, traffico di droga, corruzione e furti informatici?
Le criptovalute: l'arma preferita dei criminali moderni per riciclare denaro e mascherare le loro operazioni. DarkLab sta lavorando a un prodotto in uscita **nell'anno 2025** che ti porterà nel cuore del lato oscuro della blockchain.
Scoprirai:

- Come il cybercrime utilizza valute digitali per eludere la giustizia.
- I legami tra il dark web e le transazioni anonime.
- Le sfide che investigatori e forze dell'ordine affrontano nel tracciamento del denaro sporco.

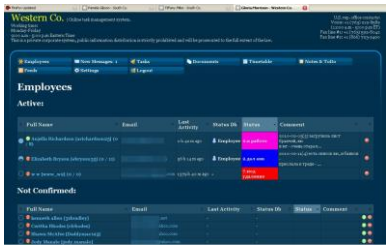
EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Evil Corp era un gruppo ben noto per la sua abilità e struttura organizzativa nel mondo del cybercrime. Le recenti indagini, come l'Operazione Cronos, condotte in collaborazione tra vari paesi come Regno Unito, Stati Uniti, Australia e altre nazioni europee, hanno fatto luce sul loro sistema di gestione e riciclaggio di ingenti somme di denaro e criptovalute. Il gruppo era riuscito a sviluppare un sistema ben strutturato per l'utilizzo dei Money Mules utili a bypassare i controlli di identità (KYC) imposti dai servizi finanziari classici ma anche DeFi.

EVIL CORP E L'USO DEI MONEY MULES

I Money Mule sono individui reclutati dai criminali, non solo informatici, per svolgere operazioni finanziarie finalizzate al trasferimento di denaro ottenuto illecitamente. Questo denaro viene successivamente spostato su diversi conti bancari con l'obiettivo di riciclarlo e renderlo difficilmente tracciabile.
Sebbene i Money Mule vengano utilizzati principalmente in crimini finanziari tradizionali, sempre più gruppi criminali li stanno costringendo a diventare Crypto Money Mule. Questo fenomeno è legato alla necessità di aprire wallet di criptovalute ed effettuare transazioni in monete digitali, al fine di eludere i controlli **KYC (Know-Your-Customer)** e **AML (Anti-Money Laundering).** Tali controlli sono stati introdotti dai governi come parte delle più recenti normative antiriciclaggio, volte a monitorare le identità degli utenti sulle piattaforme finanziarie tradizionali e sui sistemi di finanza decentralizzata (DeFi).



Portale Evil Corp fornito ai money mules

Maksim Viktorovich Yakubets (componente Evil Corp)

RECLUTAMENTO DEI MONEY MULES

Il reclutamento dei Money Mule inizia con la ricerca accurata dei candidati più adatti a questo ruolo. Questi "collaboratori" — a volte ignari delle vere finalità del loro incarico — vengono reclutati tramite campagne di lavoro fittizie che offrono posizioni con le seguenti caratteristiche:

- **Lavoro part-time**
- **Completamente da remoto**
- **Impegno non particolarmente gravoso**

Una volta completata la candidatura e "assunzione" il nuovo collaboratore riceve, da parte del criminali le istruzioni per svolgere il proprio incarico.

EVIL CORPS

L'ECONOMIA DEL RANSOMWARE

Secondo quanto emerso dall'indagine condotta sul gruppo criminale Evil Corp, nei primi mesi un nuovo Money Mule non viene immediatamente coinvolto in operazioni legate al cybercrime. Inizialmente gli vengono assegnate transazioni fittizie o di scarso rilievo, per consentire un periodo di osservazione e valutazione. Solo dopo aver superato questa fase di prova e dimostrato affidabilità, può iniziare a svolgere compiti più rilevanti.
Per comunicare con i **Money Mule**, i criminali possono utilizzare diverse tecniche, come nel caso di Evil Corp, che impiegava portali creati appositamente per la gestione dei loro "dipendenti". Il compenso per i **Money Mule** può essere fisso oppure calcolato in base alle operazioni effettuate, sotto forma di percentuali.
È importante sottolineare che questa pratica rimane molto diffusa, soprattutto nel mondo del cybercrime, dove si stima che circa il 90% delle transazioni finanziarie associate ai **Money Mule** sia legato ad attività criminali online.

PROFILI DI MONEY MULES

Secondo l'FBI, esistono generalmente tre tipi di Money Mule:

- **Inconsapevoli o ignari:** questi individui non sanno di essere coinvolti in uno schema criminale. Vengono reclutati tramite truffe romantiche o false proposte di lavoro.
- **Consapevoli:** questi individui generalmente iniziano come Money Mule inconsapevoli, ma, dopo aver ricevuto vari segnali di avvertimento, comprendono di essere coinvolti in uno schema criminale. Tuttavia, scelgono di continuare a parteciparvi.
- **Complici:** questi individui sono pienamente consapevoli di essere parte di uno schema criminale e decidono deliberatamente di parteciparvi, spesso svolgendo anche attività di reclutamento di personale aggiuntivo.

DARKLAB
RHC INTELLIGENCE LABORATORY

RedHot Cyber

EVIL CORPS

ANALISI DELLE TRANSAZIONI E DEI WALLET CRIMINALI

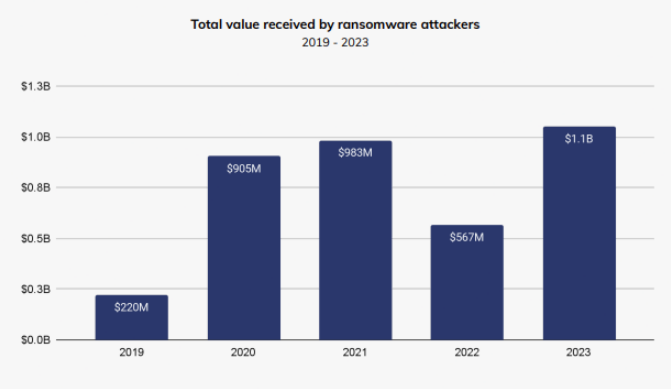
A cura di Alessio Stefan e Edoardo Faccioli

EVIL CORPS

ANALISI DELLE TRANSAZIONI E DEI WALLET CRIMINALI

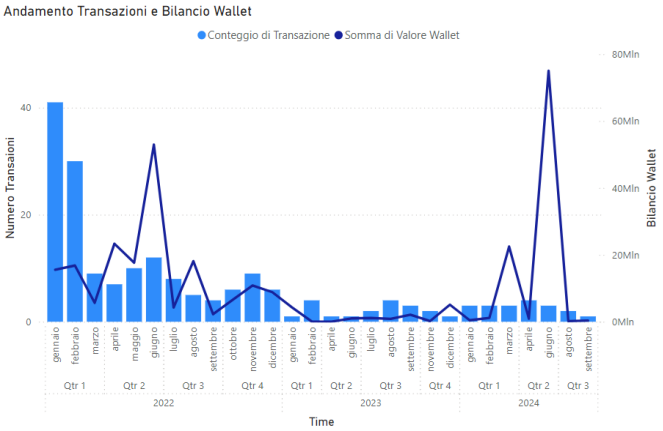
In questa sezione esaminiamo i dati relativi ai pagamenti ransomware, con un focus sul volume generato negli anni precedenti e nel 2024. L'obiettivo è fornire una previsione quanto più realistica possibile. È fondamentale evidenziare che le analisi e le previsioni si basano sui dati raccolti online tramite ransomwhe.re, un portale che monitora i pagamenti segnalati in seguito ad attacchi ransomware. Di conseguenza, i volumi economici analizzati rappresentano solo una frazione del totale generato a livello globale, ma costituiscono comunque una base significativa per individuare e interpretare tendenze a livello monetario

Nonostante il 2022 abbia rappresentato un anno di controtendenza, secondo le analisi di Chainalysis il volume totale degli introiti economici legati ai ransomware è in costante crescita. Questo trend ha portato a generare nel 2023 introiti superiori al miliardo di dollari, con prospettive di un aumento significativo osservando le tendenze attuali.



ANALISI DARKLAB DELLE TENDENZE >= 2024

Le analisi condotte dal team DarkLab di RHC, basandosi sui dati di ransomwhe.re, rivelano un andamento interessante: mentre il numero di transazioni registrate è diminuito nel tempo, il saldo dei wallet collegati ai pagamenti ransomware ha mostrato un incremento significativo. Questo suggerisce che i gruppi ransomware stanno puntando su richieste di riscatto sempre più elevate. Una strategia evidente è quella di proporzionare l'importo richiesto al fatturato delle aziende prese di mira, mirando a massimizzare i profitti con attacchi mirati a realtà più redditizie.

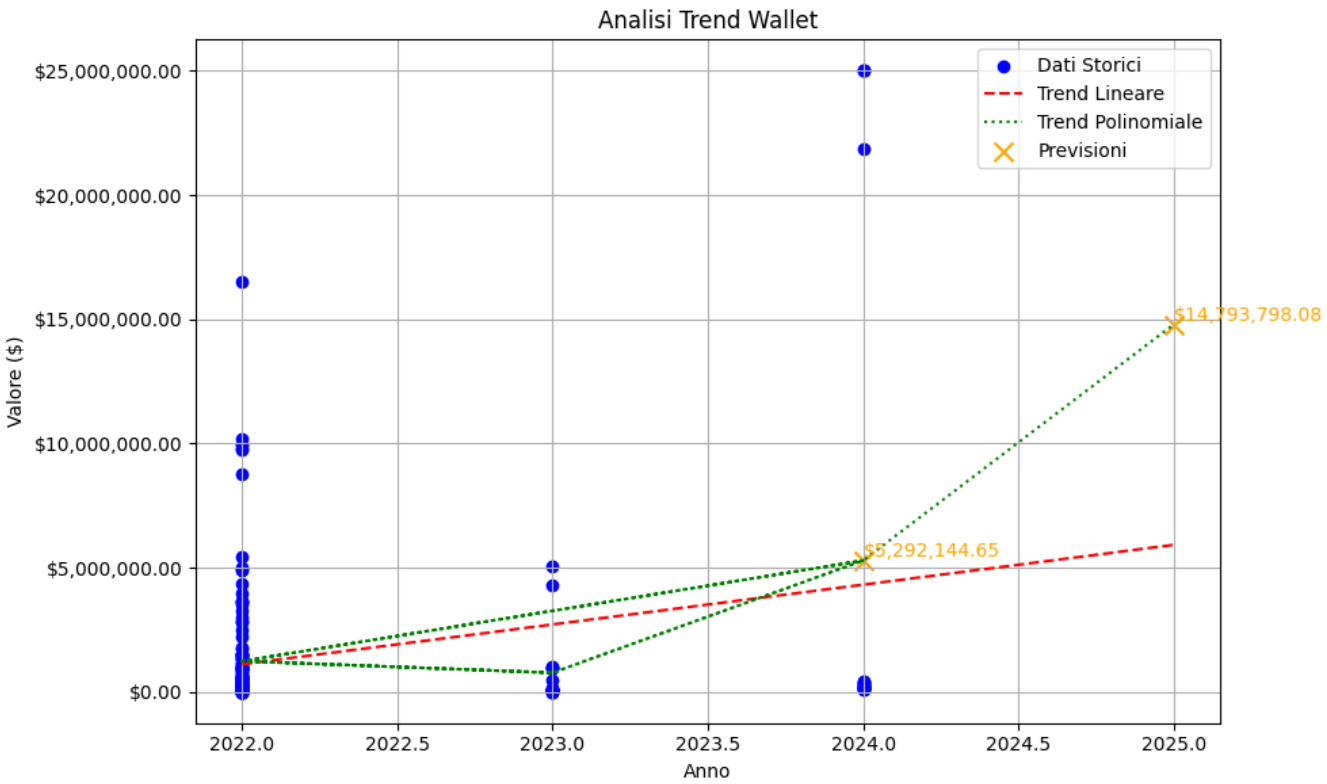


EVIL CORPS

ANALISI DELLE TRANSAZIONI E DEI WALLET CRIMINALI

Grazie ai dati estratti da ransomwhe.re e all'impiego di modelli predittivi, il team DarkLab propone una proiezione sull'andamento dell'economia ransomware per il 2025. È importante sottolineare che questa analisi si basa esclusivamente sui dati attualmente disponibili, raccolti attraverso segnalazioni effettuate sul portale ransomwhe.re. Di conseguenza, l'analisi potrebbe presentare margini di errore e non essere completamente precisa, ma offre comunque una chiara indicazione di un trend di crescita costante, già evidente negli ultimi anni.

Focalizzandoci sulla linea rossa, questa conferma il trend di crescita osservato nel 2023 e analizzato da Chainalysis, suggerendo una possibile ulteriore espansione anche nel 2025. Infine, un'analisi basata su modelli polinomiali evidenzia la possibilità di un incremento ancora più marcato, indicando per il 2025 una crescita particolarmente pronunciata del volume economico generato dai ransomware.



DARKLAB COMMUNITY

La community di Dark Lab è il cuore pulsante dietro il report "Dark Mirror". Composta da esperti di Cyber Threat Intelligence (CTI), professionisti della sicurezza informatica e appassionati del settore, la nostra missione è quella di creare un'Italia più resiliente agli attacchi informatici attraverso la condivisione di conoscenze, risorse e competenze.
Dark Lab è una community eterogenea che unisce talenti da vari settori della cybersecurity. I nostri membri includono analisti di minacce, ricercatori, ethical hackers e consulenti di sicurezza, tutti uniti dalla passione per la difesa contro le minacce informatiche. Grazie alla nostra diversità di background e competenze, siamo in grado di affrontare le sfide della cybersecurity da molteplici prospettive.

Pietro Melillo
Esperto di Cyber Threat Intelligence e professore universitario, è il coordinatore del gruppo Dark Lab

Olivia Terragni
Esperta in Network economy, Information Economics, Digital Forensics e CTI

Carlo Mauceli
Esperto di Cybersecurity, Cyber Threat Intelligence e Appassionato di Geopolitica e Tecnologia

Luca Galuppi
Senior IT Engineer esperto in Firewall, Networking e Architetture IT

Edoardo Faccioli
Esperto di Cyber Threat Intelligence e Cybercrime.
.

Andrea Mario Muscarà
Cybersecurity Analyst & Ethical Hacker

Alessio Stefan
Studente magistrale di AI & Cybersecurity e CTF player

Massimiliano Brolli
Esperto di sicurezza, di ricerca dei bug e del Red Team, è il fondatore di Red Hot Cyber

Inva Malaj
Appassionata di Cyber Security e Cyber Threat Intelligence

Marco Mazzola
Esperto in Network e Cyber Security

Reffaela Crisci
Esperta di Cyber Threat Intelligence, coordina un sotto gruppo di DarkLab