DARK MIRROR - OSSERVATORIO DELLE MINACCE RANSOMWARE

REPORT H1 2024

IL COLLETTIVO DARKLAB E' UN SOTTO GRUPPO DELLA COMMUNITY DI RED HOT CYBER SPECIALIZZATO AL MONITORAGGIO DELLE MINACCE INFORMATICHE. Il RHC Dark Lab nasce con l'obiettivo principale di diffondere la conoscenza sulle minacce informatiche per migliorare la consapevolezza e le difese digitali del paese.

INTRODUZIONE

Il ransomware rappresenta una delle minacce più pervasive nel panorama della sicurezza informatica globale. Si tratta di un tipo di malware che, una volta infiltrato nei sistemi informatici, cifra i dati dell'utente o dell'organizzazione, rendendoli inaccessibili. Gli attaccanti richiedono quindi un riscatto per fornire la chiave di decrittazione, con la promessa di restituire l'accesso ai dati. Questo tipo di attacco non solo paralizza il business , ma può anche causare gravi Perdite finanziarie e danni alla reputazione.

L'importanza di studiare il fenomeno del ransomware in Italia è cruciale per comprendere come proteggere meglio le organizzazioni e le infrastrutture critiche del paese. **Con un totale di 72 attacchi documentati da gennaio 2024**, l'Italia si posiziona al quinto posto tra i paesi più colpiti, subito dopo Stati Uniti, Regno Unito, Canada e Germania.

Gli obiettivi di questo report sono molteplici, ma il principale è **sensibilizzare anche i non addetti ai lavori sul fenomeno del ransomware**, evidenziando l'importanza di investire nella sicurezza informatica all'interno delle organizzazioni per ridurne l'incidenza. Il report non solo fornirà contenuti divulgativi, ma presenterà anche una panoramica dettagliata degli attacchi ransomware avvenuti in Italia, analizzando tendenze, settori più colpiti ed evoluzione delle metodologie di attacco. Inoltre, il report offrirà raccomandazioni pratiche per la prevenzione e la gestione del ransomware, proponendo strategie di difesa efficaci e politiche di sicurezza informatica. Attraverso l'esame di dati e casi di studio reali, questo report offre una guida completa per comprendere a fondo il fenomeno del ransomware e le sue implicazioni.

Un ringraziamento speciale va a **Pietro Melillo, ideatore di questo report e custode diligente del gruppo Dark Lab.** Un sentito apprezzamento va anche a tutti i membri del team Dark Lab che ogni giorno esplorano le underground, raccogliendo informazioni di prima mano e redigendo articoli per fornire utili consigli ai nostri lettori, contribuendo così alla protezione delle loro stesse organizzazioni oltre alle infrastrutture del nostro paese.

Massimiliano Brolli, fondatore di Red Hot Cyber

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 sotterraneo digitale, abbiamo redatto un'analisi approfondita sul fenomeno ransomware in Italia, per il periodo H1-2024.

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.

RACCOLTA DATI

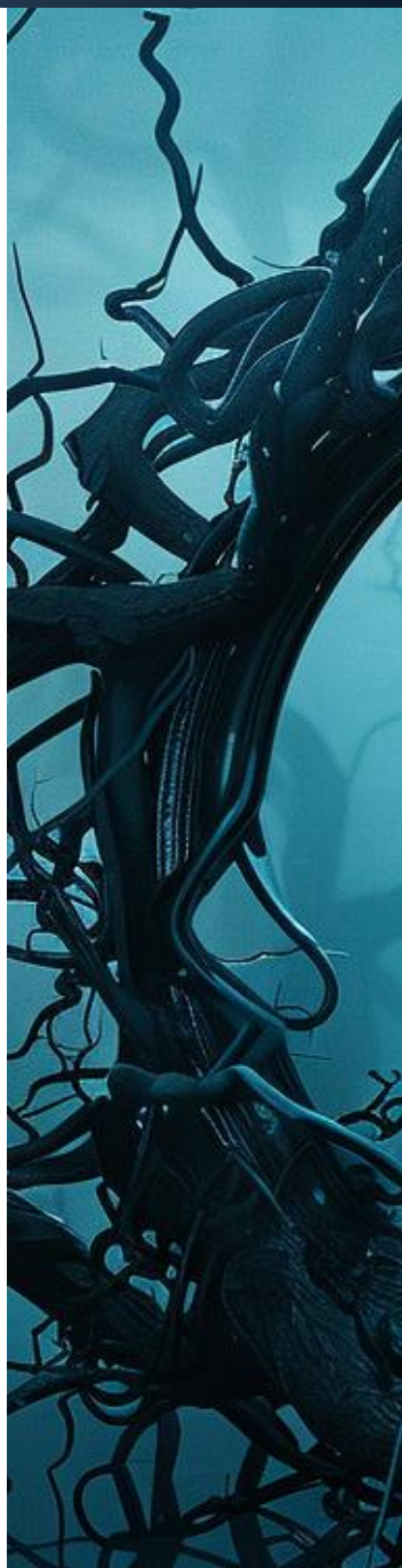
- **Monitoraggio delle Underground:** Utilizziamo strumenti avanzati per monitorare costantemente forum, mercati underground e altre piattaforme clandestine dove avvengono scambi di informazioni e strumenti legati al ransomware;
- **Threat Hunting:** Effettuiamo attività proattive di threat hunting su 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.

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.

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.



RANSOMWARE INSIDE

TASSONOMIA, VETTORI DI INFEZIONE, TECNICHE DI ESTORSIONE E MODELLO RANSOMWARE AS A SERVICE (RAAS)

RANSOMWARE INSIDE

TASSONOMIA

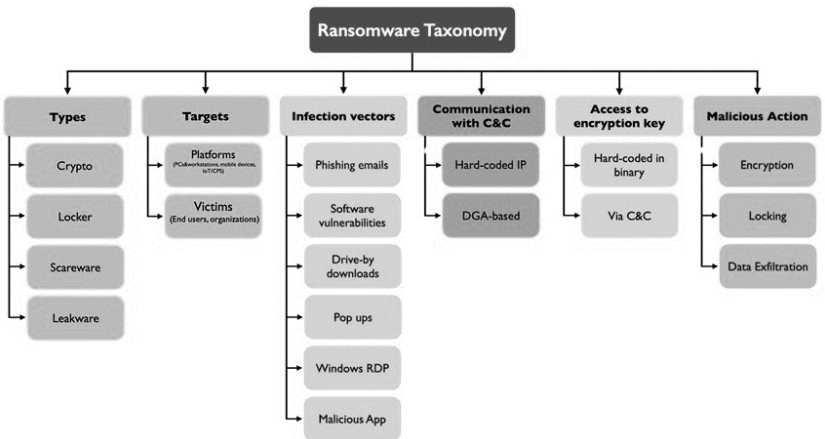
Il ransomware è un tipo di malware che, una volta infiltrato in un sistema, blocca l'accesso ai dati dell'utente o al sistema stesso, richiedendo un riscatto (**ransom**) per ripristinare l'accesso. Gli attacchi ransomware sono progettati per estorcere denaro dalle vittime, che siano privati cittadini, aziende o enti governativi. Gli attaccanti minacciano di mantenere i dati inaccessibili, di cancellarli o di pubblicarli online se il riscatto non viene pagato.

LA TASSONOMIA

La tassonomia è quella disciplina che riguarda la **classificazione e l'organizzazione in categorie strutturate, basata su caratteristiche comuni.**

Quando parliamo di tassonomia del ransomware, ci riferiamo a un sistema organizzato che classifica il fenomeno del ransomware secondo vari criteri, come il tipo di ransomware, i target, i vettori di infezione, i metodi di comunicazione come i server di comando e controllo (C&C), l'accesso alle chiavi di cifratura e le azioni dannose eseguite.

Questa classificazione aiuta gli esperti di sicurezza informatica, aziende e individui a comprendere meglio la minaccia e al tempo stesso sviluppare strategie efficaci per prevenire e rispondere agli attacchi ransomware.



Tipologie di ransomware

Crypto Ransomware: Questo tipo di ransomware cripta i file dell'utente, rendendoli inaccessibili senza una chiave di decrittazione. Gli attaccanti richiedono un riscatto in cambio della chiave. Esempi noti includono CryptoLocker e CryptoWall.

Locker Ransomware: Il locker ransomware blocca l'accesso al sistema o al dispositivo dell'utente, impedendone l'uso fino a quando non viene pagato un riscatto. A differenza del crypto ransomware, non cripta i file, ma limita l'accesso a tutto il sistema operativo. Un esempio famoso è il ransomware Reveton.

Scareware: Questo tipo di ransomware inganna l'utente facendogli credere che il proprio sistema sia stato infettato da un virus o che ci siano problemi di sicurezza gravi. Viene richiesto un pagamento per risolvere questi problemi inesistenti. Sebbene meno dannoso degli altri.

Leakware, o Doxware: Minaccia le vittime di rendere pubblici i loro dati a meno che non paghino un riscatto. Il danno causato da questo tipo di ransomware è irreversibile, poiché una volta che i dati diventano pubblici, chiunque può accedervi. Entità come banche e organizzazioni che gestiscono informazioni confidenziali o sensibili.

RANSOMWARE INSIDE

VETTORI DI INFEZIONE

Il ransomware è una delle minacce informatiche più pervasive e distruttive del nostro tempo. La sua capacità di criptare file essenziali e richiedere un riscatto per il loro ripristino ha paralizzato numerose organizzazioni in tutto il mondo.

Phishing emails : Gli attaccanti inviano email infette a un gran numero di destinatari, sperando che qualcuno apra il link o l'allegato malevolo oppure effettuano un invio mirato ad un gruppo di persone.

Software Vulnerabilities : Gli attaccanti sfruttano vulnerabilità nei software o nei sistemi operativi che non sono stati aggiornati con le ultime patch di sicurezza. Utilizzando strumenti automatizzati, i criminali informatici possono scansionare la rete alla ricerca di sistemi vulnerabili e installare ransomware senza bisogno di interazione umana;

Drive-by Download: Un drive-by download avviene quando un utente visita un sito web compromesso, che automaticamente scarica e installa il ransomware senza che l'utente se ne accorga. Questo metodo sfrutta vulnerabilità nel browser web o nei plugin installati;

Pop Ups: è un vettore di attacco basato sul web che coinvolge pop-up ingannevoli che attirano gli utenti a cliccare su di essi imitando fonti genuine e affidabili. Il ransomware viene quindi scaricato automaticamente sul computer della vittima o porta all'apertura di una nuova finestra contenente collegamenti dannosi

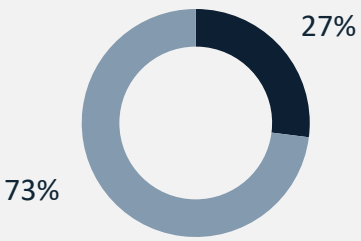
Windows RDP : RDP è uno strumento di amministrazione remota ampiamente utilizzato. Gli attaccanti possono sfruttare credenziali deboli o rubate per accedere a un sistema tramite RDP. Una volta dentro, possono installare ransomware e propagare l'infezione attraverso la rete;

Malicius App : è l'uso di annunci pubblicitari online per distribuire malware. Gli attaccanti inseriscono annunci infetti su siti web legittimi. Quando gli utenti cliccano su questi annunci, vengono reindirizzati a siti malevoli che installano il ransomware sui loro dispositivi;

Statistiche Recenti sul Ransomware:

- Numero di attacchi ransomware nel 2023: **3.2 milioni** *(Fonte SonicWall, McAfee);*
- Costo medio di un riscatto nel 2023: **1.85 milioni di dollari** (*Fonte 2023 Unit 42 Ransomware and Extortion Report" pubblicato da Palo Alto Network);*
- Tempo medio di inattività dopo un attacco ransomware**: 16 giorni** *(Fonte "Global State of the Channel Ransomware Report" di Datto).*

Il 27% delle aziende paga il riscatto ai criminali informatici *(Fonte «State of Ransomware» di Sophos)*



Alcuni consigli Rapidi per Prevenire il Ransomware:

- Formazione: Educare i dipendenti su come riconoscere e segnalare email di phishing.
- Aggiornamenti: Mantenere software e sistemi operativi sempre aggiornati.
- Backup: Eseguire backup regolari dei dati e verificarne l'integrità.
- Autenticazione a Due Fattori (2FA): Implementare l'autenticazione a due fattori per tutti gli accessi critici.
- Monitoraggio: Utilizzare soluzioni di sicurezza avanzate per il monitoraggio continuo delle minacce.
- Gestione degli Accessi: Limitare i privilegi di accesso ai dati e ai sistemi solo a chi ne ha realmente bisogno per il proprio lavoro.
- Segmentazione della Rete: Dividere la rete aziendale in segmenti più piccoli per limitare la propagazione del ransomware in caso di infezione.

RANSOMWARE INSIDE

TECNICHE DI ESTORSIONE

Il ransomware, partendo da Trojan AIDS di Joseph Popp, ritenuto il primo ransomware della storia fino ad arrivare a Wanna Cry e i sofisticati ransomware quali LockBit, Revil e Darkside, hanno subito moltissimi cambiamenti ed innovazioni, sia dal punto di vista tecnico che dal punto di vista dell'estorsione.

Partendo dal presupposto che il cybercrimine da profitto segue la logica del **minimo sforzo per il massimo guadagno**, il ransomware si basa sull'arte dell'estorsione, richiedendo un pagamento in cambio del ripristino di un'infrastruttura IT funzionante. Nel tempo, le modalità di estorsione si sono evolute in quattro specifiche categorie:

1. **Prima estorsione**: implica la richiesta di un riscatto per decifrare i dati criptati all'interno di un sistema informatico.

2. **Seconda estorsione:** se la vittima rifiuta di pagare il riscatto per decifrare i file, i criminali possono ulteriormente ricattare l'organizzazione richiedendo un secondo pagamento per evitare la divulgazione online di informazioni sensibili acquisite durante l'attacco.

3. **Terza estorsione:** qualora l'azienda non vuole pagare il riscatto, i criminali informatici contattano le singole persone violate per richiedere dei soldi per evitare la pubblicazione dei loro dati.

4. **Quarta estorsione:** Le tattiche includono il furto di credenziali dei dipendenti e dei clienti della vittima per rivenderle o utilizzarle illecitamente, l'installazione di software per il mining di criptovalute nella rete della vittima e l'invio di email di phishing dalla rete della vittima per compromettere ulteriori organizzazioni. Gli aggressori comunicano con queste parti, spesso minacciando di divulgare informazioni sensibili a meno che non ricevano il riscatto. Un'altra strategia prevede l'intimidazione di società quotate in borsa offrendo opportunità di vendita allo scoperto a trader non etici.

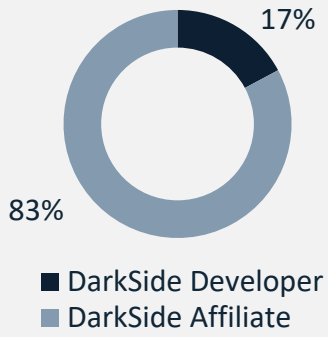
Il Threat Actors DarkSide

DarkSide è una cybergang ad oggi non più attiva, nota per il suo sofisticato ransomware. Nel maggio 2021, ha condotto un attacco contro Colonial Pipeline, una delle più grandi infrastrutture di oleodotti negli Stati Uniti. Questo attacco ha causato un'interruzione delle forniture di carburante negli Stati Uniti D'America,.
In totale, DarkSide è riuscito ad estorcere più di 90 milioni di dollari in pagamenti di riscatto in bitcoin, provenienti da 47 portafogli distinti attraverso le loro operazioni ransomware.

La distribuzione dei guadagni

Qualsiasi pagamento di riscatto effettuato da una vittima viene suddiviso tra l'affiliato e lo sviluppatore del ransomware. Nel caso di DarkSide, lo sviluppatore del malware prendeva il 25% per riscatti inferiori a 500.000 dollari, ma tali provvigioni scendevano al 10% per riscatti superiori a 5 milioni di dollari. Tutto questo viene definito con delle politiche descritte nei blog degli "sviluppatori" o nei forum underground come ad esempio XSS, un forum underground in lingua russa. Questa divisione dei pagamenti dei riscatti risulta chiara sulle blockchain, con le diverse azioni che separano i portafogli Bitcoin controllati dagli affiliati e dallo sviluppatore. Se parliamo di DarkSide, lo sviluppatore ha ricevuto bitcoin per un valore di 15,5 milioni di dollari (17%), con i restanti 74,7 milioni di dollari (83%) destinati ai vari affiliati.

Revenue Share tra affiliati e sviluppatori all'interno del gruppo ransomware DarkSide *(Fonte Elliptic)*



RANSOMWARE INSIDE

TECNICHE DI ESTORSIONE

Oltre alle categorie di estorsione, esistono tre tipologie di forme di negoziazione. Queste modalità, che possono essere di tre tipi, indicano l'approccio che le aziende e i criminali possono adottare, anche ingaggiando specifici negoziatori a supporto:

Negoziazione Aggressiva : è caratterizzata da una negoziazione intensa tra la vittima e i cybercriminali, in cui entrambe le parti cercano di ottenere il massimo vantaggio possibile. La vittima cerca di ridurre il riscatto al minimo, mentre i criminali cercano di ottenere il massimo pagamento. Le caratteristiche principali includono forte pressione per ottenere concessioni, tattiche aggressive, minacce e intimidazioni, e l'obiettivo di sconfiggere l'altra parte. Un esempio è quando la vittima rifiuta di pagare il riscatto iniziale e cerca di negoziare un importo inferiore, mentre i criminali minacciano di distruggere i dati se il pagamento non viene effettuato rapidamente.

Negoziazione Cooperativa : La forma di estorsione "cooperativa" prevede una negoziazione collaborativa tra la vittima e i cybercriminali, mirata a raggiungere un accordo accettabile per entrambe le parti. La vittima mantiene una comunicazione aperta, mentre i criminali mostrano flessibilità. Le caratteristiche principali includono comunicazione rispettosa, concessioni reciproche, ricerca di soluzioni che minimizzino i danni per entrambe le parti e il mantenimento di una relazione di lavoro temporanea. Un esempio è quando la vittima spiega le proprie limitazioni finanziarie.

Negoziazione Integrativa : La forma di estorsione "integrativa" prevede una negoziazione in cui entrambe le parti collaborano per trovare una soluzione che massimizzi i benefici per entrambe. Anche se improbabile in un contesto criminale, può includere il recupero parziale dei dati in cambio di un pagamento parziale. Le caratteristiche principali sono la ricerca di una soluzione win-win, massima trasparenza e cooperazione, focus sulla soddisfazione degli interessi di entrambe le parti. Un esempio è un accordo in cui una parte dei dati viene recuperata gratuitamente come gesto di buona fede, con il resto rilasciato dopo il pagamento.

Le aziende, in caso di richiesta di riscatto da parte di un operatore ransomware, possono chiedere supporto a un negoziatore (o mediatore)..

La professione del mediatore nelle attività di estorsione da ransomware è diventata sempre più rilevante e specializzata nel panorama della sicurezza informatica. Questi professionisti agiscono come intermediari tra le vittime del ransomware e i cybercriminali, con l'obiettivo di negoziare il rilascio dei dati sequestrati o il pagamento di un riscatto ridotto. Le loro principali responsabilità includono:

- **Valutazione**: Analizzare l'entità dell'attacco ransomware, identificare i dati compromessi e valutare le conseguenze per l'organizzazione colpita.
- **Comunicazione con i Cybercriminali**: Stabilire un canale di comunicazione con gli estorsori, mantenendo un approccio professionale e rispettoso per evitare ulteriori escalation.
- **Negoziazione** : Lavorare per ridurre l'importo del riscatto richiesto, cercando di ottenere le migliori condizioni possibili per la vittima, come pagamenti rateali o ridotti.
- **Consulenza Strategica**: Fornire alle aziende colpite consigli su come gestire la situazione, comprese le migliori pratiche per evitare futuri attacchi e migliorare la sicurezza informatica.
- **Recupero Dati**: Collaborare con esperti tecnici e con i criminali informatici per tentare il recupero dei dati compromessi dopo il pagamento del riscatto

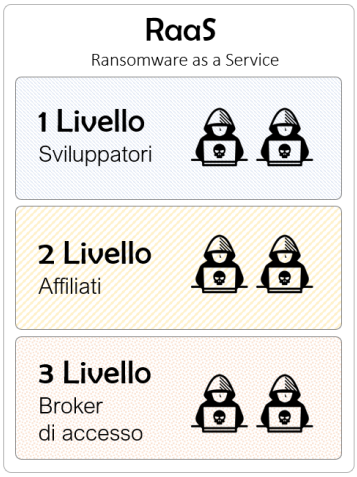
Il mediatore deve possedere competenze approfondite in sicurezza informatica, capacità negoziali eccellenti e una conoscenza aggiornata delle tattiche utilizzate dai cybercriminali. Inoltre, deve operare con discrezione e integrità, garantendo la massima riservatezza delle informazioni trattate durante il processo di negoziazione.

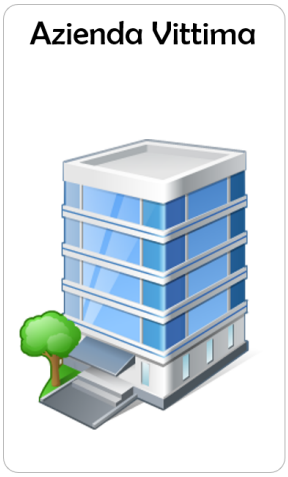
RANSOMWARE INSIDE

MODELLO RANSOMWARE AS A SERVICE (RAAS)

Nell'immaginario popolare, si pensa che la criminalità informatica sia legata a singoli individui con abilità informatiche eccezionali. Ma se vuoi estorcere milioni di dollari a una grande azienda, non puoi fare tutto da solo, hai bisogno di una "squadra" Hai bisogno di *Un gruppo di hacker criminali con competenze informatiche eccezionali, diversificate, e verticali, che frequentano il Dark Web e che con molta probabilità vivono in Russia.*

Infatti, la stragrande maggioranza dei criminali informatici non dispone di tutte le capacità tecniche necessarie per fare da soli e quindi creare malware, estorcere denaro, penetrare le aziende. Ecco appunto che nasce il Ransowmare as a Service (RaaS). Dei gruppi di criminali informatici che collaborano in modo organizzato e strutturati per un unico scopo: *estorcere tanto più denaro possibile ad una ipotetica organizzazione.*





La piramide del RaaS

Per RaaS, come abbiamo detto, si intende "Ransomware as a Service", quindi Ransomware come "servizio", un modello di business criminale dove la violazione viene condotta da un gruppo di criminali informatici militarmente organizzati. Nella barra laterale puoi scoprire come è composta la piramide a tre livelli, per comprendere al meglio il suo funzionamento e la divisione dei compiti tra i criminali informatici.

Gli sviluppatori

Al primo livello troviamo gli "Sviluppatori". Si tratta di esperti nella scrittura dei malware, di crittografia, che li realizzano, li aggiornano continuamente, creano strumenti per poter sviluppate dashboard e sistemi di comando e controllo agli "affiliati", capaci di gestire tutta la fase di infezione, che come vedremo è la fase "attiva" di un attacco ransomware, prima di passare all'estorsione. Gli sviluppatori mettono a disposizione anche degli strumenti di supporto tecnico per gli affiliati, in modo che questi possano avere delle risposte immediate dagli sviluppatori su problematiche tecniche.

Gli Affiliati

Al secondo livello abbiamo gli "Affiliati". Si tratta di altri criminali informatici che affittano il ransomware dagli sviluppatori e conducono la reale attività di attacco e di estorsione, accedendo alle reti della vittima e rimangono al suo interno per molto tempo, esfiltrando quanti più dati sensibili che gli consentiranno un ulteriore livello di persuasione nel caso in cui l'azienda non vorrà pagare la richiesta di riscatto. Gli affiliati, affittano il ransomware dagli sviluppatori, accettando o concordando le loro provvigioni. Gli affiliati, in molti casi, per poter velocizzare le loro attività ed accedere ad una rete di una grande azienda, possono acquistare l'accesso dai broker di accesso.

I broker di accesso

Questi ultimi, sono di fatto dei gruppi di criminali informatici che violano le reti delle azienda per acquisirne persistenza. Sono molto esperti di tecniche di penetration test e, una volta acquisito l'accesso alla rete di una grande organizzazione, la mettono in vendita nei forum underground per poche migliaia di dollari. Gli affiliati, spesso sono clienti dei broker di accesso, in quanto consentono di velocizzare il loro flusso di lavoro.

ANALISI E TENDENZE

TENDENZE GLOBALI, TENDENZE PANORAMA ITALIANO, TRENDS

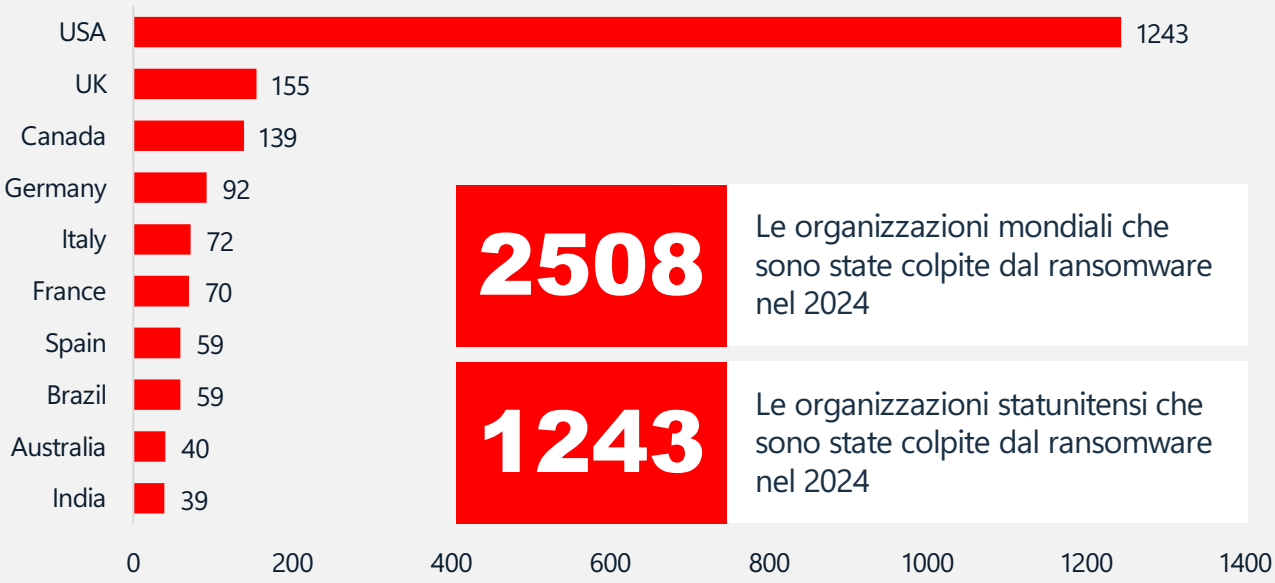
ANALISI E TENDENZE

ANALISI GLOBALI - PAESI PIU'COLPITI

Nel periodo di osservazione che va dal primo gennaio al 30 di giugno 2024, Dark Lab ha rilevato un totale di **2508 vittime documentate** di attacchi ransomware a livello globale. Questo numero, sebbene significativo, rappresenta solo una frazione delle vittime reali.

Molti casi, non vengono riportati nei data leak site (DLS), dove i criminali pubblicano i dati rubati come parte di una strategia di doppia estorsione. Pertanto i numeri riportati sono solo quelli relativi agli attacchi documentati.

TOP10 Paesi maggiormente colpiti



Panoramica Geografica e Settoriale: Le analisi mostrano che il ransomware non conosce confini geografici, colpendo sia paesi sviluppati che in via di sviluppo. I settori maggiormente colpiti includono l'industria, i servizi e la tecnologia, evidenziando l'ampia portata e l'impatto devastante che questi attacchi possono avere sull'economia globale e sulla vita quotidiana delle persone.

Gli Stati Uniti sono chiaramente il paese più colpito, con un totale di 1250 vittime documentate. Questo numero è significativamente più alto rispetto agli altri paesi, indicando una maggiore vulnerabilità o una maggiore attività di attacco in questa regione. Il Regno Unito e il Canada seguono a grande distanza, con rispettivamente **155 e 139 vittime**, seguiti dalla **Germania (92) e dall'Italia (72).** La presenza di paesi come Francia, Spagna, Brasile, Australia e India con numeri relativamente più bassi, ma comunque significativi, dimostra che il ransomware è un problema globale che colpisce una varietà di nazioni, indipendentemente dal loro livello di sviluppo economico.

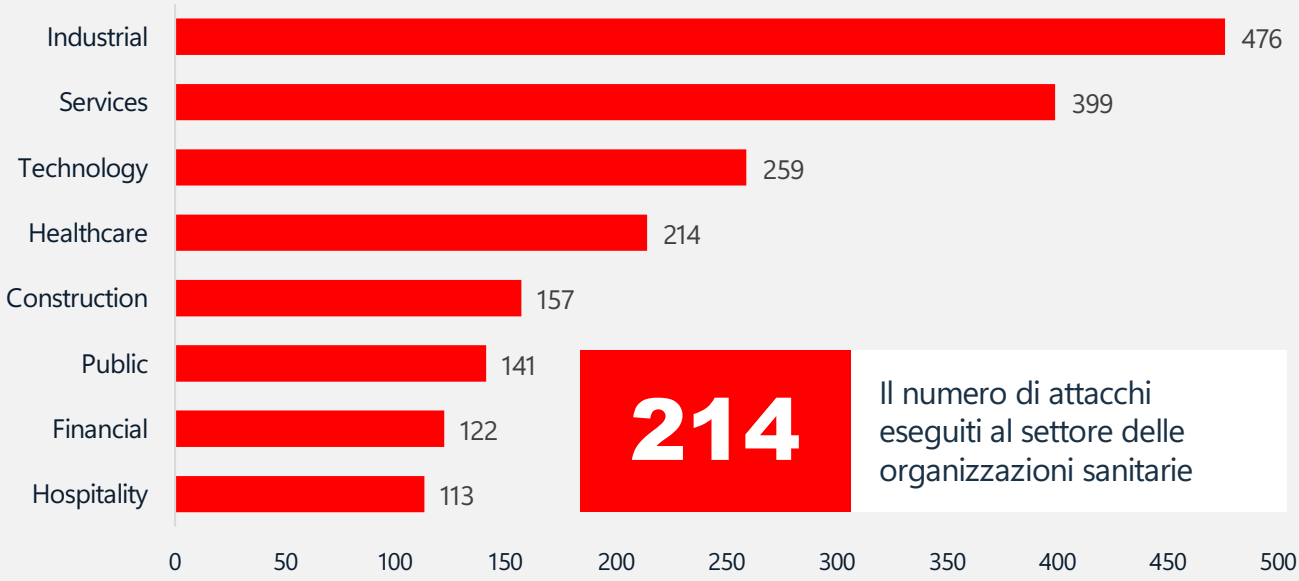
ANALISI E TENDENZE

ANALISI GLOBALI - SETTORI PIU' COLPITI

Le analisi mostrano che il ransomware non conosce confini geografici, colpendo sia paesi sviluppati che in via di sviluppo.

I settori maggiormente colpiti includono l'industria, i servizi e la tecnologia, evidenziando l'ampia portata e l'impatto devastante che questi attacchi possono avere sull'economia globale e sulla vita quotidiana delle persone.

TOP10 Settori maggiormente colpiti (Worldwide)



Settori Maggiormente Colpiti: Dal punto di vista settoriale, il ransomware ha dimostrato una particolare predilezione per il **settore industriale**, seguito dai servizi e dalla tecnologia. Anche la sanità e la costruzione sono tra i settori più colpiti, evidenziando come gli attacchi non risparmino le infrastrutture critiche e i servizi essenziali. Questo porta a una crescente preoccupazione per la sicurezza e la resilienza di questi settori.

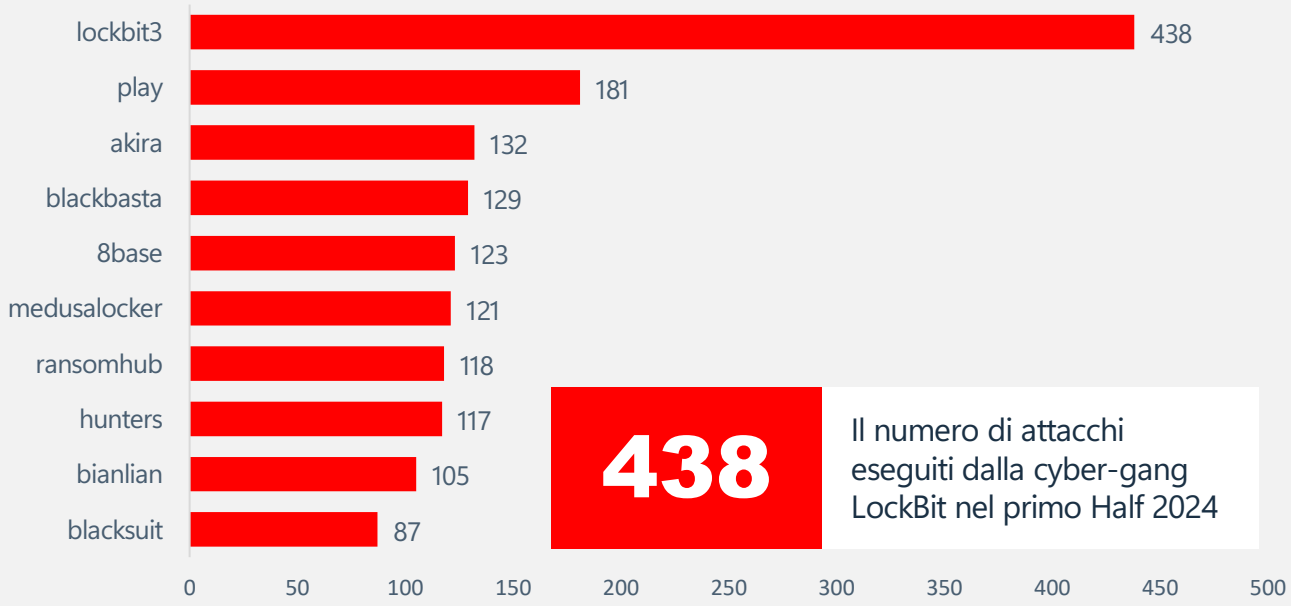
I dati evidenziano come il ransomware colpisce molti settori, data l'importanza economica e la dipendenza tecnologica/digitale degli stessi. Le aziende industriali e dei servizi sono spesso critiche per le infrastrutture nazionali e hanno un'alta probabilità di pagare i riscatti per minimizzare le interruzioni. Il settore tecnologico e quello sanitario sono anche frequentemente presi di mira. Le aziende tecnologiche, essendo al centro dell'innovazione e della gestione dei dati, rappresentano un obiettivo allettante per i criminali informatici.

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 periodo di osservazione. Nonostante due operazioni significative delle forze dell'ordine abbiano colpito LockBit (una a fine febbraio che ha portato alla pubblicazione dei nickname di 192 affiliati e al sequestro del relativo data leak site, e una successiva a maggio che ha rivelato il nome del presunto amministratore Dmitry Khoroshev), il gruppo RaaS non accenna a ridurre i suoi volumi operando con incredibile prolificità e longievità.

TOP10 Threat Actors maggiormente attivi (Worldwide)



Lockbit3, con **438 attacchi a livello mondiale**, è il gruppo più attivo, dimostrando una resistenza sorprendente nonostante le operazioni delle forze dell'ordine. La loro persistenza e il loro successo fanno sì che continuino ad attrarre nuovi affiliati, aumentando la loro visibilità e consolidando la loro reputazione nella comunità criminale.

Segue LockBit, la cyber gang **Play ransomware**. Questo gruppo si posiziona al secondo posto con **181 attacchi** documentati. La loro attività, seppur inferiore rispetto a Lockbit3, mostra comunque una capacità operativa significativa.

Akira e **BlackBasta**, con rispettivamente **132 e 129 attacchi**, hanno dimostrato di essere attori chiave nel panorama del RaaS. La loro continua attività suggerisce una capacità di adattamento e resilienza notevole. Da tenere in considerazione che BlackBasta dal 1 gennaio del 2022 ad oggi ha pubblicato 500 attacchi informatici e ad oggi è il gruppo che ha colpito maggiormente le infrastrutture critiche dei paesi.

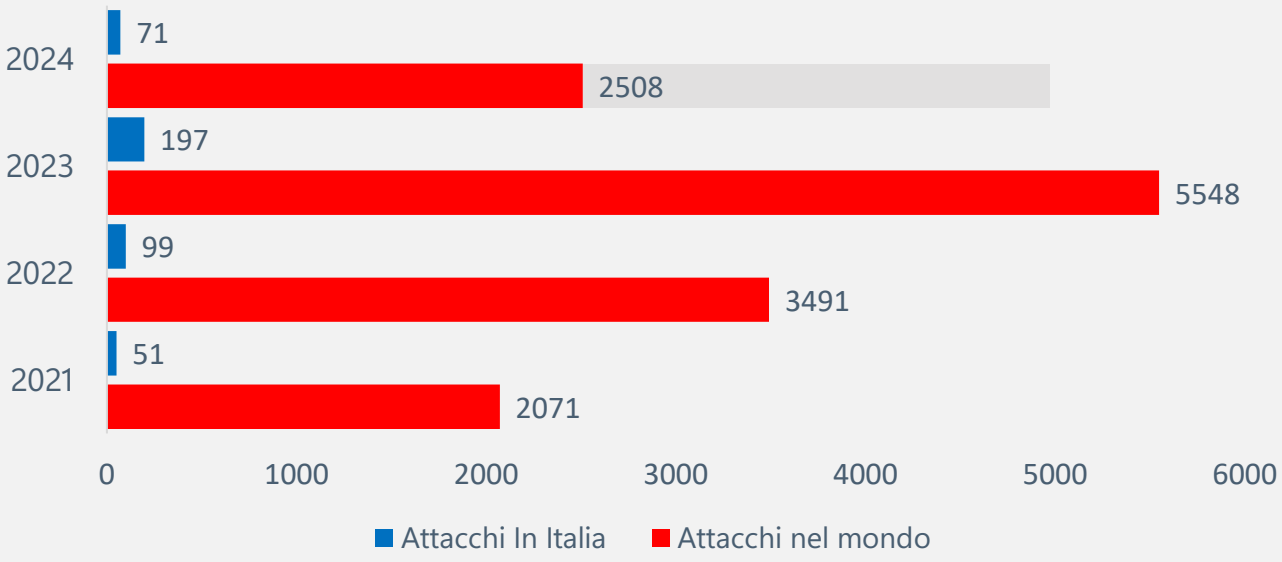
ANALISI E TENDENZE

TENDENZE

I dati afferenti agli attacchi ransomware negli ultimi quattro anni indicano una tendenza preoccupante di aumento costante del numero di attacchi informatici di tipo ransomware. La tabella seguente mostra il numero di attacchi a livello globale e in Italia dal 2021 al 2024.

Anche in Italia, si osserva un trend simile. Gli attacchi ransomware sono aumentati costantemente dal 2021 al 2023, ma sembra cge nel 2024 ci sia una diminuzione interessante.

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



Tenendo in considerazione i dati del primo half 2024, sembrerebbe che ci sia questo anno una diminuzione che potrebbe essere attribuita a diversi fattori, quali miglioramenti nelle misure di sicurezza, maggiore consapevolezza e preparazione contro gli attacchi ransomware, o cambiamenti nelle strategie dei cybercriminali.

È importante considerare che questi numeri riflettono gli attacchi pubblicati sui data leak site (DLS), che solitamente coinvolgono aziende che hanno scelto di non pagare il riscatto. Tuttavia, è noto che rappresentano solo una frazione dei casi effettivi di attacchi riusciti.

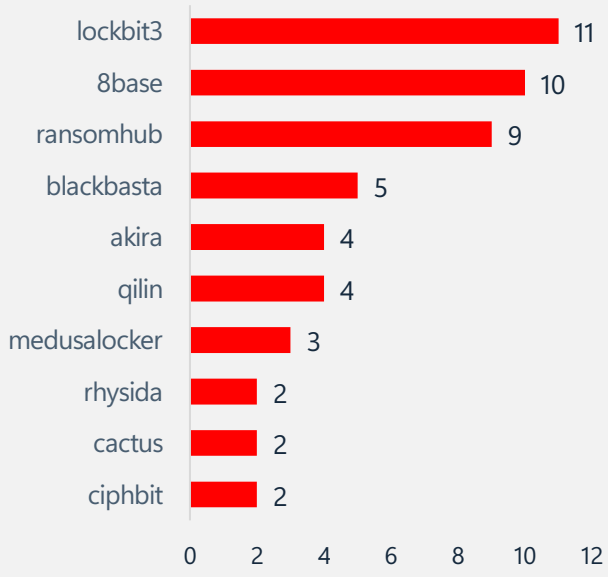
Nonostante il rallentamento, il rischio di attacchi ransomware rimane elevato. Se consideriamo la progressione lineare osservata dal 2021 al 2023, è possibile che i numeri nel 2024 rappresentino un'anomalia temporanea piuttosto che un cambiamento di tendenza a lungo termine.

ANALISI E TENDENZE

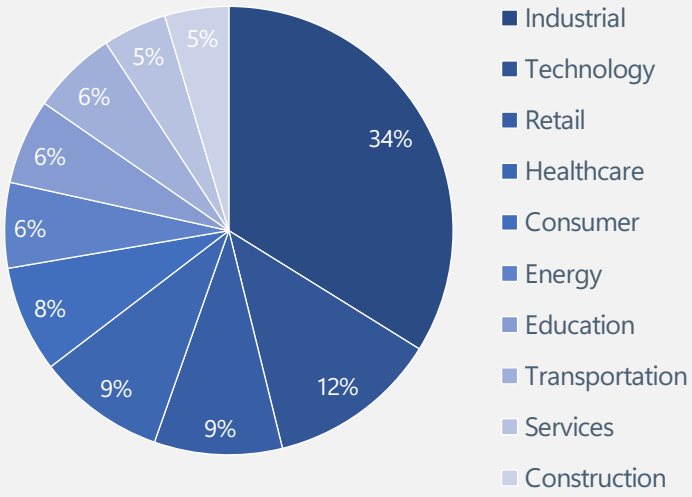
ANALISI COMPARTO ITALIA

Concentrandosi sugli **72 attacchi documentati in Italia** durante il periodo di osservazione, emergono alcuni dati significativi che evidenziano la necessità di rafforzare la sicurezza informatica in specifici settori chiave, come il settore Industriale, Tecnologico, dei servizi e dei trasporti. Al quinto posto il settore sanitario, che pur essendo stato colpito da un numero relativamente inferiore di attacchi rispetto ad altri settori, risulta particolarmente vulnerabile e con **una storia di violazioni di rilievo di organizzazioni sanitarie italiane**.

TOP10 Threat Actors maggiormente attivi



TOP10 Settori più colpiti



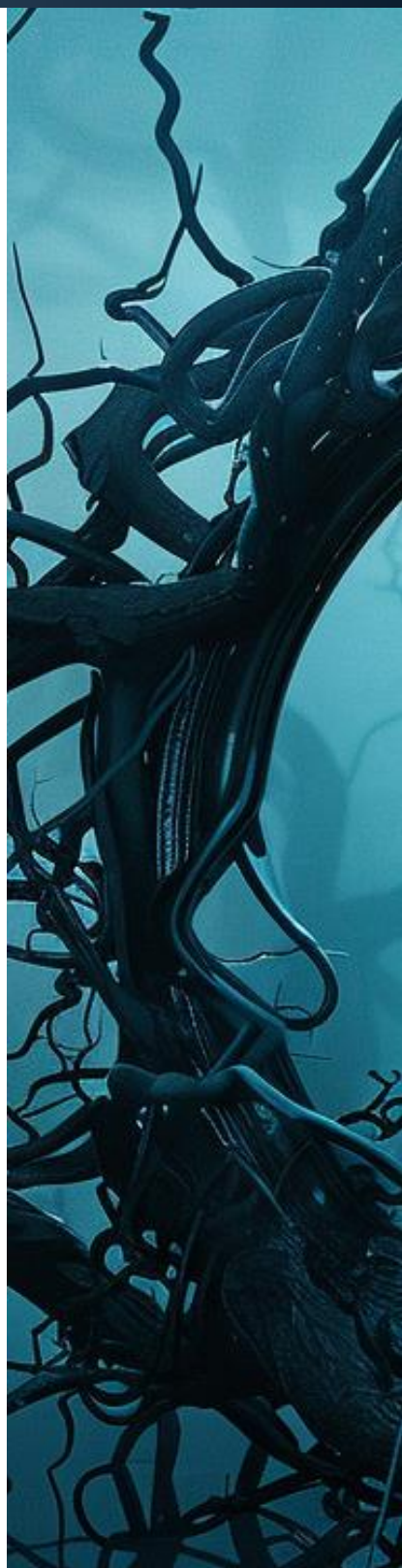
La sua importanza come infrastruttura critica al servizio dello stato lo rende un bersaglio di primaria importanza per i criminali informatici.

Relativamente ai Threat Actors maggiormente attivi, anche in Italia spicca **LockBit** che ha colpito **11 aziende**. Questo gruppo rappresenta la minaccia più significativa per le infrastrutture italiane. Subito dopo abbiamo **8Base** (Intervistati da Red Hot Cyber nel 2023) con **10 attacchi**. Questo gruppo dimostra un'attività significativa nel panorama italiano, suggerendo una capacità operativa robusta e una strategia mirata per colpire il paese. Seguono **RansomHub** con **9 attacchi** seguito da **BlackBasta** con **5 attacchi**. Tutti questi gruppi rappresentano un rischio considerevole che deve essere monitorato con attenzione.

Qilin, Medusa, Ryshida, Cactus e Ciphbit con un numero di attacchi variabile tra 4 e 2 attacchi, mantengono comunque una presenza significativa e continuano a rappresentare una minaccia per le infrastrutture italiane seppur limitata.

ANALISI E TENDENZE

ANALISI COMPARTO ITALIA



L'Italia è stata presa di mira dai gruppi RaaS in maniera rilevante durante il primo semestre 2024, nonostante i valori assoluti siano inferiori ad altri paesi (come USA e UK) il paese ha ricevuto dei picchi non scontati. Nella giornata del 28 Giugno sono stati attaccati nell'arco delle 24 ore ben tre aziende : un data center **[1]** (Roma), una azienda manifatturiera **[2]** (Caserta) e una di spedizione **[3]** (Trieste). Quest'ultimo attacco *(dati amministrativi e finanziari, 150GB)* è stato rivendicato da **RansomHouse** mentre i primi due da **RansomHub** (dati confidenziali di azienda e personale, rispettivamente 541.46 GB e 490 GB). Interessante l'escalation ottenuta dall'attacco a **[1]** dove, oltre ai 70 TB di dati criptati, tramite la compromissione della rete gli attaccanti sono riusciti ad ottenere un accesso diretto a **[2]** evidenziando una mancanza di comunicazione e di protezioni degli asset anche al di fuori della minaccia ransomware. Nessuna delle due aziende ha fatto uno statement pubblico annunciando l'attacco ricevuto al contrario di **[3]** che ha inserito un popup nel loro sito ufficiale.

Nel settore education **[4]** abbiamo vissuto una delle prime vittime di LockBit3 dopo Operation Cronos, con l'exfiltration di ben **514GB** annunciata il 18 Maggio, l'attacco è stato però effettuato il 5 Maggio. L'attacco ransomware ha costretto **[4]** a chiudere parte della sua infrastruttura di rete incluso il portale per le ammissioni studentesche creando problematiche organizzative e rallentamenti logistici. Tra i dati esfiltrati abbiamo *documenti finanziari (budget di spese universitarie e per progetti in fase di operazione)* ed informazioni riservate come contratti per il per eventi del 2024 e investimenti di anni precedenti. Secondo l'ACN, il 13 di Maggio, una settimana esatta dall'attacco, richiedendo 5 giorni di operazioni per poter riavviare gradualmente la rete interna di **[4]**. Non sono state indicate nessun tipo di misura attuata né dei risultati delle prime investigazioni, l'unica nota *"tecnica"* è stata la conferma che il ransomware ha colpito solo una parte della rete rendendo così possibile avviare rapidamente le attività di ripristino.

ANALISI E TENDENZE

ANALISI COMPARTO ITALIA

Il settore dell'Healthcare ha ricevuto 2 attacchi con gravi conseguenze. La sezione italiana di una piattaforma per analisi diagnostiche **[5]** vittima di **BlackBasta** con l'equivalente di **1.5 TB** di dati interni all'azienda e dei suoi clienti, tra i sample pubblicati dal RaaS venivano presentati test medici e documenti di identità generando un grave danno alla privacy degli utenti finali. L'attacco è stato rivendicato il 4 Maggio ma il malware è stato eseguito il 18 Aprile con il recupero graduale della rete a partire dalla giornata del 20 Aprile, per tutto il periodo le attività di business, laboratorio e diagnostiche sono state compromesse in maniera consistente.

[5] ha fin da subito deciso pubblicamente di non voler in alcun modo pagare il riscatto facendo sì che BlackBasta pubblicasse tutti documenti ottenuti al fine del countdown (14 Maggio). Secondo le dichiarazioni della stessa azienda è stato evidenziato come l'uso dei backup abbia permesso di ottenere una copia dei dati cifrati. Venne istituito un canale di comunicazione ad hoc per far si che i pazienti vengano informati se i loro dati siano stati pubblicati ed il *"massimo impegno di **[5]** a gestire le richieste pervenute su altri canali di comunicazione"*. Nel 5 Luglio tutte le persone che hanno contattato **[5]** non hanno ricevuto risposta.

La mole dei dati rubati era sproporzionata per poter contattare ogni singolo paziente, per questo l'azienda ha creato canali di comunicazione appositi, facilitando l'esecuzione dell'articolo 15 del GDPR. Tale comportamento indica difficoltà nel seguire normative in ambito privacy e data protection creando un danno di immagine da non sottovalutare, tutto ciò nonostante l'appoggio delle forze dell'ordine italiane.

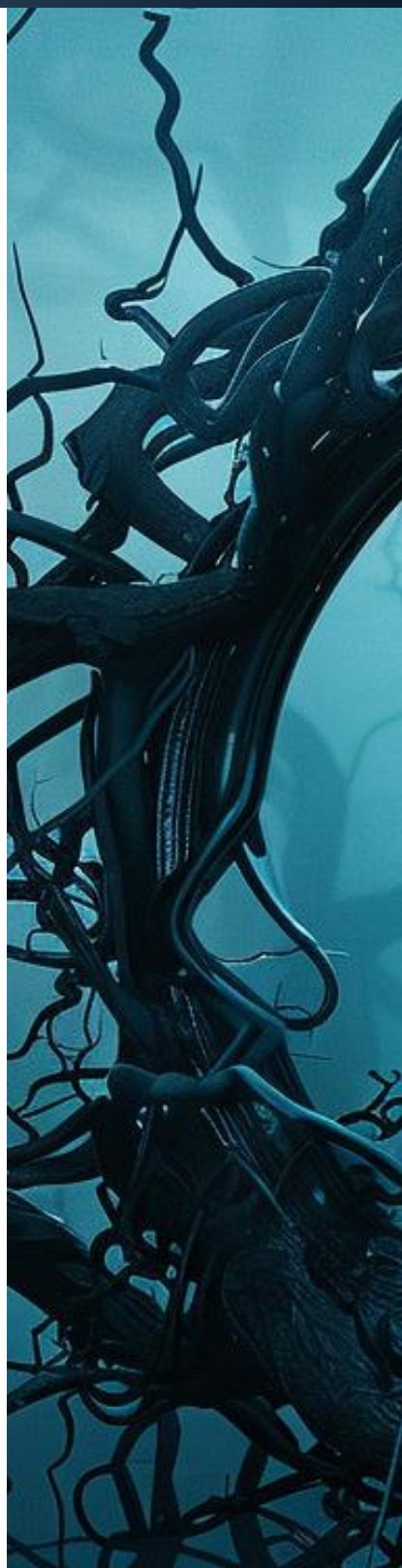
Alla scrittura di questo report non abbiamo nessuna dichiarazione del Garante né piani di sanzioni verso **[5]**, l'ultimo aggiornamento sulla pagina ufficiale di **[5]** risulta essere del 15/05/2024.

ANALISI E TENDENZE

ANALISI COMPARTO ITALIA

Il secondo servizio di healthcare riguarda il RaaS **Cicada 3301**. **[6]** è un insieme di aziende a livello regionale che ha subito l'attacco ransomware nella notte tra il 5 e 6 Giugno creando disagi ai servizi emessi al pubblico. Si tratta del primo attacco rivendicato sul DLS di Cicada, inclusi **1 TB** di dati rubati, è stata emessa una task force di specialisti a livello regionale per il ripristino delle attività.

Gli affiliati di Cicada hanno inizialmente compromesso un appaltatore di **[6]** e solo successivamente sono riusciti ad introdursi nella rete di **[6]** nella quale hanno risieduto per mesi. Durante la fase di negoziazione, i rappresentanti di **[6]** si sono rifiutati di pagare il riscatto e Cicada ha fornito gratuitamente il decryptor pubblicando i dati rubati sul loro DLS il 15 Giugno. i dati comprendono PI e documentazione medica. **[6]** ha ripreso la completa ripresa dei servizi il 27 Giugno per un totale di 20 giorni di disagi.



THREAT ACTORS

NUOVI THREAT ACTORS , INTERVISTE AI THREAT ACTORS E NUOVE TECNICHE TATTICHE E PROCEDURE

I THREAT ACTORS

NUOVI THREAT ACTORS

Questo primo periodo del 2024 vede come protagonisti i 'rookie' nella scena ransomware, seguendo il trend iniziato nella prima metà del 2023. In questo periodo, tre nuovi gruppi, Medusa, AKIRA e 8Base, sono entrati nella top 10 per numero di attacchi. Nonostante il numero complessivo di attacchi sia leggermente diminuito, questi nuovi arrivati hanno distolto l'attenzione dai gruppi più longevi, che nella prima metà del 2024 hanno subito significative perdite reputazionali. La qualità degli attacchi e la scelta delle vittime da parte dei nuovi gruppi sono state determinanti in questo cambiamento.

Inoltre, i nuovi servizi Ransomware as a Service (RaaS) 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.

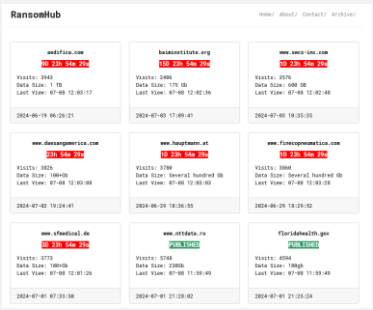
RANSOMHUB

Scoperto a febbraio, questo threat actor si è subito presentato come il più grande gruppo ransomware attualmente attivo. Le analisi hanno rivelato una notevole somiglianza tra RansomHub e Knight, suggerendo un rebranding del precedente malware. Dopo aver annunciato la chiusura delle attività, Knight ha reso pubblico il codice sorgente in Golang, facilitando così la crescita di RansomHub.

La rapida ascesa di RansomHub è dovuta a diversi fattori. Fin dall'inizio, il gruppo ha mirato a settori cruciali come l'healthcare, attaccando healthcare (Change Healthcare) , oltre a colpire la supply chain (come nel caso italiano di Cloud Europe - Mangimi Fusco) e il settore business, con attacchi alla casa d'aste Christie's. Inoltre, RansomHub ha introdotto una strategia innovativa vendendo direttamente i dati sensibili rubati come alternativa alla pubblicazione sul Data Leak Site.Il reclutamento di affiliati di alto profilo come Scattered Spider e Notchy, approfittando del declino di BlackCat/ALPHV, ha ulteriormente consolidato la posizione di RansomHub nel panorama delle minacce informatiche.

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.



Data Leak Site (DLS) del gruppo RansomHub.

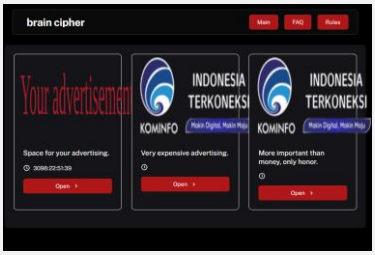
Il gruppo avviato intorno a Febbraio, ha all'attivo ben 92 vittime pubblicate da gennaio 2024 ad oggi. Grazie ad aver approfittato degli affiliati provenienti da altre gang criminali sta scalando la vetta del Ransomware as a Service, raggiungendo Play ransomware che si trova al secondo posto subito dietro a LockBit.

I THREAT ACTORS

NUOVI THREAT ACTORS

BRAIN CIPHER

Ennesima nuova variante di LockBit3.0 che è riuscita a creare danni su tutto il territorio indonesiano. Nella giornata del 20 Giugno il PDN indonesiano (insieme di 2700 datacenter) è caduto vittima di un attacco ransomware con un binario uguale ad un samples di LB3.0, l'attacco ha mandato in crisi più di 210 istituzioni ed applicazioni che si appoggiavano sui servizi del PDN. L'attacco venne in seguito rivendicato dal primo post di Brain Cipher sul loro DLS ufficiale. Dalle chat pubblicate si è evidenziata una richiesta di riscatto di $8 MLN, successivamente rifiutato dal governo indonesiano in uno statement pubblico. Il gruppo offre la possibilità di postare ADV personalizzati alla cifra di 200.000 dollari al mese ed è stato uno dei pochi casi di RaaS ad aver rilasciato gratuitamente il decryptor ad una vittima (in questo caso il PDN).



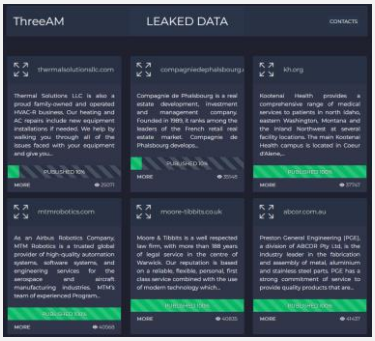
Data Leak Site (DLS) del gruppo Brain Cipher. Il dataleak site è molto minimalista e annovera ad oggi solo tre vittime. E' presente una sezione Min, FAQ e Rules.

3AM

Questo Threat Actor è la prova che il vacillare dei gruppi con una esistente e forte reputazione riesce a far brillare le nuove leve, sfruttando le loro tecniche per potersi pubblicizzare ai potenziali affiliati. Nonostante il gruppo 3AM (o ThreeAM) sia nato nel 2023 il suo uso è stato molto limitato (meno di 30 attacchi con cadenza irregolare) fino all'inizio del 2024.

Un specifico operatore di LockBit (non ancora identificato) sostituisce con 3AM il 'Big Player' quando quest'ultimo viene bloccato da sistemi di protezione. Tale tecnica è stata ripetuta spesso confermando il Threat Actor come un ottimo sostituto e non solo una seconda scelta.

Creato da zero tramite codice Rust, che ne rende difficile le analisi, questa nuova famiglia riesce ad utilizzare tecniche obsolete con successo e offre la gestione dei file in maniera efficente con una sofisticata CLI. Il danno reputazionale recato a LB dopo Operation Cronos, e l'utilizzo di questo sostituto come porto sicuro, può rendere 3AM sempre più presente nella scena ed usato dai ransomware operators.



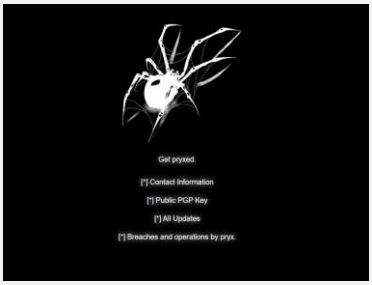
Data Leak Site (DLS) del gruppo 3AM. Data Leak Site molto ben organizzato dove spicca la sezione contatti. Le vittime presenti all'interno del sito sono 30 e viene adottato l'approccio a percentuale di pubblicazione. Questa strategia da modo al gruppo di beneficiare sulla costante pressione verso l'azienda violata per poter ottenere il pagamento del riscatto in cambio della chiave di decifrazione.

I THREAT ACTORS

NUOVI THREAT ACTORS

PRYX RANSOMWARE

Pryx (scoperto da Red Hot Cyber ad inizio Luglio) ha rivendicato il suo primo attacco significativo, annunciando di aver compromesso i sistemi di Rowan College at Burlington County (RCBC.edu) e di aver sottratto 30.000 domande di iscrizione universitaria. Pryx ha affermato di aver violato i sistemi informatici di Rowan College e di essere in possesso di dati sensibili dell'istituto. Questo annuncio è stato fatto sul loro dataleak site (DLS). Il dataleak site di Pryx è una piattaforma dove il gruppo pubblica informazioni sulle vittime che non hanno pagato il riscatto richiesto. Questo sito è accessibile pubblicamente sia tramite internet e, come è consuetudine tra i gruppi ransomware, anche tramite la rete onion.



Data Leak Site (DLS) del gruppo Pryx ransomware. Il dataleak site di Pryx è caratterizzato da un'interfaccia inquietante, dominata dall'immagine di una ragnatela e lo slogan "Get pryxed". La piattaforma fornisce varie sezioni tra cui: Contact Information Public PGP Key, All Updates, Breaches and operations by pryx. L'home page del sito invita i visitatori a "Get pryxed", sottolineando il loro approccio intimidatorio e provocatorio.

Il dataleak site di Pryx è molto elementare e sembra realizzato attraverso html statico ed elenca ad oggi una sola vittima.

SHRINKLOCKER

Scoperto da Kaspersky all'inizio del 2024, ShrinkLocker è stato rilevato in varianti in Messico, Indonesia e Giordania. ShrinkLocker è particolarmente preoccupante perché utilizza una misura di sicurezza, BitLocker, per scopi malevoli.

Una volta ottenuto l'accesso al sistema di destinazione tramite vulnerabilità non corrette, credenziali rubate o servizi esposti su Internet, ShrinkLocker ridimensiona le partizioni del disco non di avvio di 100 MB per creare spazio non allocato. Successivamente, crea nuove partizioni primarie nello spazio non allocato e reinstalla i file di avvio, in modo che il sistema possa essere riavviato con i file crittografati.

Lo script modifica poi le voci del registro di sistema di Windows per disabilitare le connessioni Remote Desktop Protocol e imporre impostazioni di BitLocker come i requisiti PIN. Infine, rinomina le partizioni di avvio con l'email dell'attaccante e sostituisce i protettori di chiavi BitLocker esistenti per impedire il ripristino. Le aziende di produzione di acciaio e vaccini, oltre a un'entità governativa, sono state finora prese di mira da ShrinkLocker. Tuttavia, non sembra limitarsi a settori specifici, colpendo vittime da vari paesi e settori.

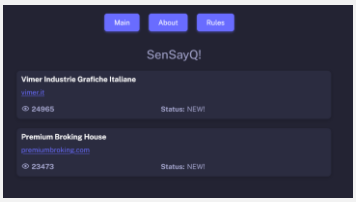
I THREAT ACTORS

NUOVI THREAT ACTORS

SANSAYQ!

SanSayQ! è un nuovo attore emergente nel panorama dei ransomware, individuato di recente. Questo gruppo utilizza tattiche di doppia estorsione, esfiltrando dati sensibili dalle reti aziendali e criptando i file delle vittime. Utilizzano una variante di Lockbit per eseguire la crittografia e rilasciano note di riscatto ([randomID] .README.txt) con il messaggio "---Welcome! You are locked by SenSayQ!---". Le vittime sono minacciate di pubblicazione dei dati rubati sul sito web dell'aggressore se non pagano entro 72 ore.

All'interno della sezione 'about' del loro sito viene riportato che l'obiettivo principale è attirare l'attenzione pubblica sul problema della sicurezza delle informazioni, in particolare sulla sicura conservazione delle informazioni confidenziali. Purtroppo, molti dirigenti fingono di non vedere il problema, finendo poi per trovarsi qui. SenSayQ dà priorità al buon senso. Riportano anche che non desiderano nuocere né rovinare il business. Sono pronti per un dialogo costruttivo e accordi congiunti.

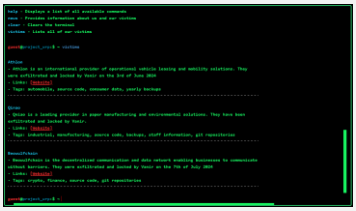


Data Leak Site (DLS) del gruppo SanSayQ! Il dataleak site di SanSayQ! È molto spartano. Contiene tre tasti che conducono alla sezione Main, About e Rulex.
Al momento l'attore malevolo ha annunciato due vittime all'interno del suo sito e una tra tra queste è italiana.

VANIR GROUP

Questo gruppo che ha fatto l'ingresso nel mondo del RaaS a luglio, è stato per la prima volta documentato da Red Hot Cyber. Nel loro sito underground, Vanir Group lascia un messaggio intimidatorio per i loro bersagli, indirizzato ai CEO o agli amministratori di dominio delle aziende colpite. Ecco una parte del messaggio. In breve, il messaggio è una minaccia diretta da parte del Vanir Group, che sostiene di aver compromesso l'infrastruttura interna di un'azienda. Affermano di aver eliminato o criptato tutti i backup e di aver rubato dati cruciali. Invitano il destinatario, presunto amministratore del dominio o CEO, a cooperare per evitare ulteriori danni, implicando che la non collaborazione potrebbe portare alla vendita o distribuzione dei dati rubati. Minacciano conseguenze negative se vengono contattate le forze dell'ordine o esperti di recupero dati.

Data Leak Site (DLS) del gruppo Vanir Group. Il dataleak site si presenta con una grafica vintage con caratteri verdi flourescenti su uno sfondo verde, il che ricorda i vecchi monitor CRT degli anni 80. Al momento il gruppo ha pubblicato solo tre vittime.



I THREAT ACTORS

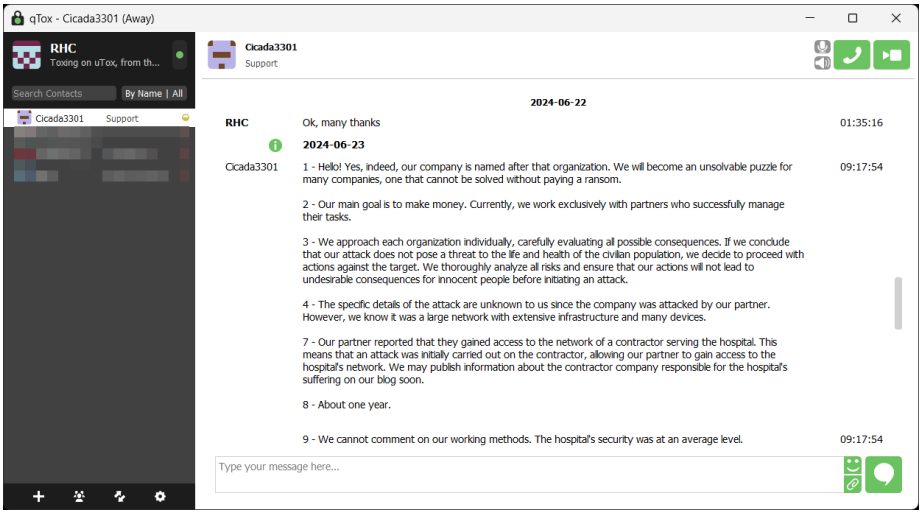
INTERVISTE AI THREAT ACTORS

"Devi conoscere i demoni per imparare a contrastarli." Questa frase, spesso citata da Red Hot Cyber, riassume l'essenza della lotta contro il crimine informatico. Conoscere i "demoni", ovvero comprendere e interpretare come operano i cyber-criminali, non solo ci aiuta a capire le loro motivazioni e i loro metodi (o meglio dire quello che in termini tecnici chiamiamo come Tecniche, Tattiche e Procedure o #TTPs dell'attore malevolo), ma ci consente anche di sviluppare difese informatiche più efficaci, capaci di contrastarli sul loro stesso terreno. Comprendere come ragionano e operano i Threat Actors è essenziale per migliorare le difese cibernetiche e prevenire attacchi futuri, rendendoci sempre più consapevoli delle minacce e del rischio.

INTERVISTA A CICADA6601

Nell'intervista esclusiva con Red Hot Cyber, Cicada6601, il gruppo di black hat hackers responsabile dell'attacco all'ASST Rhodense, ha fornito una visione dettagliata delle loro motivazioni e metodi. Cicada6601 ha rivelato di aver scelto l'ASST Rhodense per la sua vulnerabilità e per l'impatto che avrebbe avuto un attacco su un'istituzione sanitaria critica.

Il gruppo ha discusso le tecniche utilizzate per infiltrarsi nei sistemi, la strategia dietro la scelta delle vittime e come intendono continuare le loro operazioni nel futuro. L'intervista offre uno spaccato inquietante ma illuminante sul mondo dei black hat hackers e le loro tattiche. Cicada6601 ha riportato che le organizzazioni sanitarie in tutto il mondo necessitano di una migliore sicurezza informatica e che la ASST Rhodense aveva una implementazione della sicurezza media. Hanno anche riportato che alla fine hanno rilasciato la chiave di decifratura in modo gratuito.



Schermata del Messenger TOX, dove si è svolta l'intervista a Cicada6601

I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

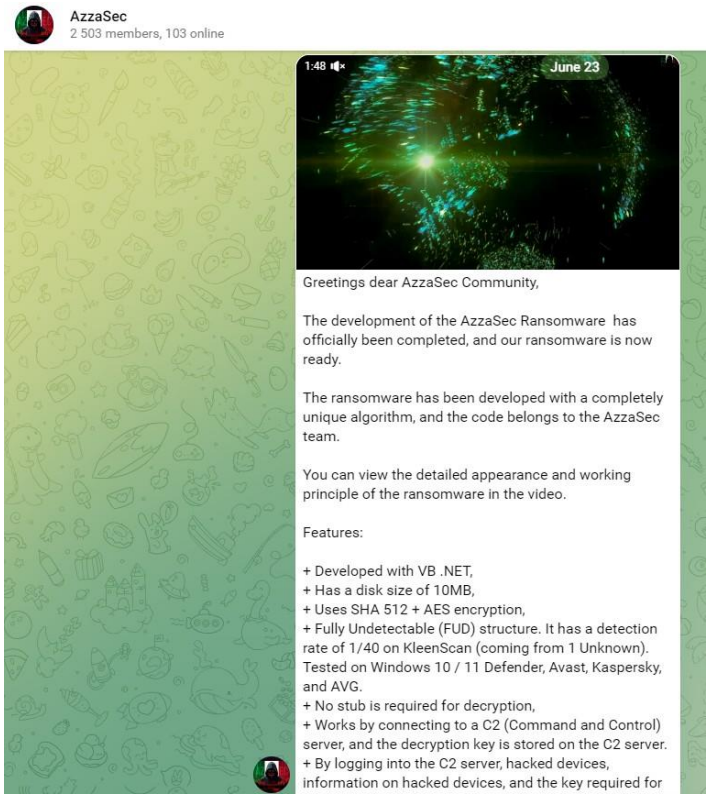
INTERVISTA AD AZZASEC

In un'altra intervista esclusiva, Red Hot Cyber ha parlato con Azzasec, un gruppo di hacktivisti italiani affiliati a Noname05716, noti per il loro supporto a cause pro-Palestina e pro-Russia.

Assasec ha riportato recentemente, all'interno del suo profilo telegram che ha realizzato un ransomware che vorrebbe utilizzarlo attraverso degli affiliati.

Ha spiegato come le loro azioni siano guidate da una missione politica e sociale, utilizzando le loro competenze informatiche per sostenere queste cause. L'intervista esplora le motivazioni ideologiche di Azzasec, le loro operazioni recenti e come vedono il futuro dell'hacktivismo. Azzasec ha discusso le difficoltà e i rischi associati alle loro attività, offrendo una prospettiva unica sul ruolo dell'hacktivismo nella geopolitica moderna.

Queste interviste rappresentano un'importante risorsa per chiunque desideri comprendere meglio il panorama delle minacce informatiche. Conoscere i nostri avversari è il primo passo per sviluppare delle strategie efficaci di difesa e mitigazione degli attacchi. E' solo conoscendo a fondo le minacce che risulta possibile trovare modi, anche non convenzionali, per poterle ostacolare.



Post sul canale Telegram di AzzaSec dove viene reclamizzato il nuovo RaaS

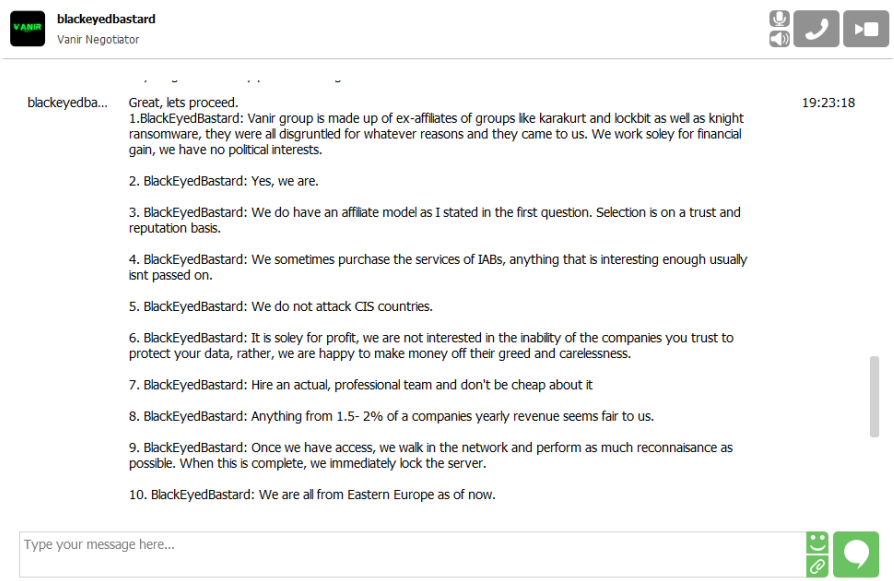
I THREAT ACTORS

INTERVISTE AI THREAT ACTORS

INTERVISTA A VANIR GROUP

Uno dei gruppi emergenti ha catturato l'attenzione degli esperti di sicurezza è il gruppo Vanir. Recentemente, questo gruppo è stato protagonista di un'intervista esclusiva con Red Hot Cyber, dove hanno condiviso dettagli sulle loro operazioni e sulla loro evoluzione. Il gruppo Vanir è noto per essere formato da ex affiliati di noti gruppi di ransomware come Lockbit, Karakurt e Knight, indicando una significativa esperienza e competenza nel campo degli attacchi informatici. Questa esperienza pregressa ha permesso al gruppo di affinare le proprie tattiche e strategie, diventando una minaccia sofisticata e temibile.

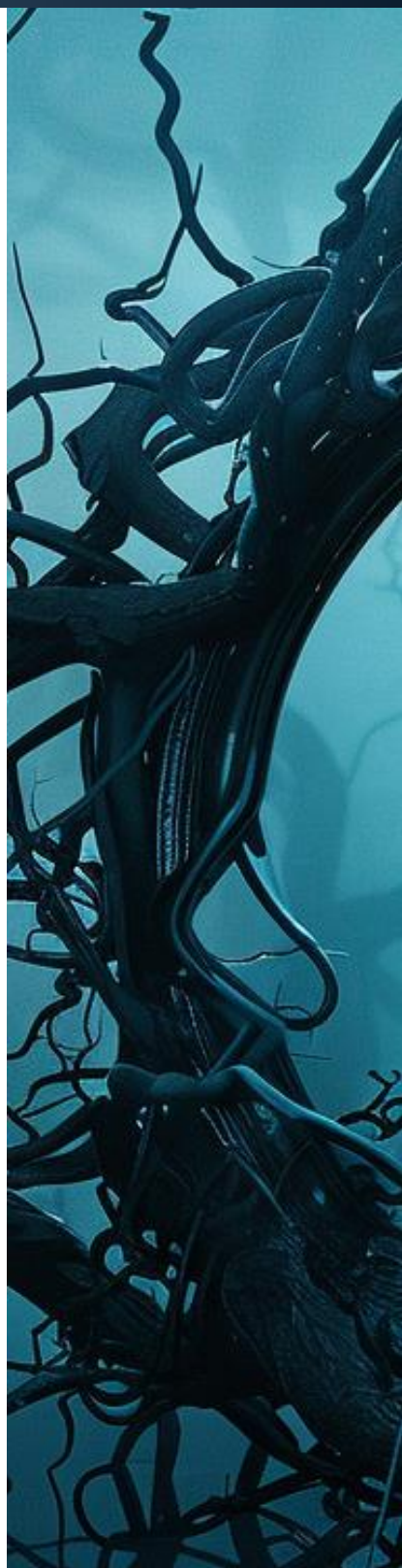
L'intervista ha anche rivelato dettagli su come il gruppo Vanir seleziona i propri obiettivi. I membri hanno dichiarato di preferire le organizzazioni con sistemi di sicurezza obsoleti o mal configurati, ma non escludono di attaccare anche aziende con protezioni più avanzate se il potenziale guadagno è elevato. Questa selettività e adattabilità nelle loro operazioni dimostrano l'alto livello di competenza e flessibilità del gruppo. Alla luce di queste rivelazioni, è chiaro che le organizzazioni devono rafforzare significativamente le loro misure di sicurezza e rimanere costantemente vigili per proteggersi da minacce come quelle rappresentate dal gruppo Vanir.



Schermata del Messenger TOX, dove si è svolta l'intervista con VANIR GROUP

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)



Utilizzando le statistiche del report sono stati identificati i gruppi più attivi in Italia nel primo semestre 2024. Abbiamo scelto 8 gruppi, tra cui **LockBit 3.0, RansomHub, 8Base, Cactus, Akira, Ciphbit, BlackBasta e QLin**, a cui vengono aggiunti nuovi gruppi ransomware, con lo scopo di identificare un certo numero di *tecniche, tattiche e procedure (TTP)* condivise per comprendere come si sono evolute negli attacchi ransomware e quali metodi di intrusione stanno emergendo.

Questa sezione contiene:

- **Accesso iniziale e persistenza**
- **Evasione e controllo**
- **Infezione, esfiltrazione e nuovi metodi di encryption**
- **TTPs somiglianze e differenze**

E' importante sottolineare 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 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 meglio. Per proteggersi al meglio è utile osservare le indicazioni fornite nelle strategie di difesa.

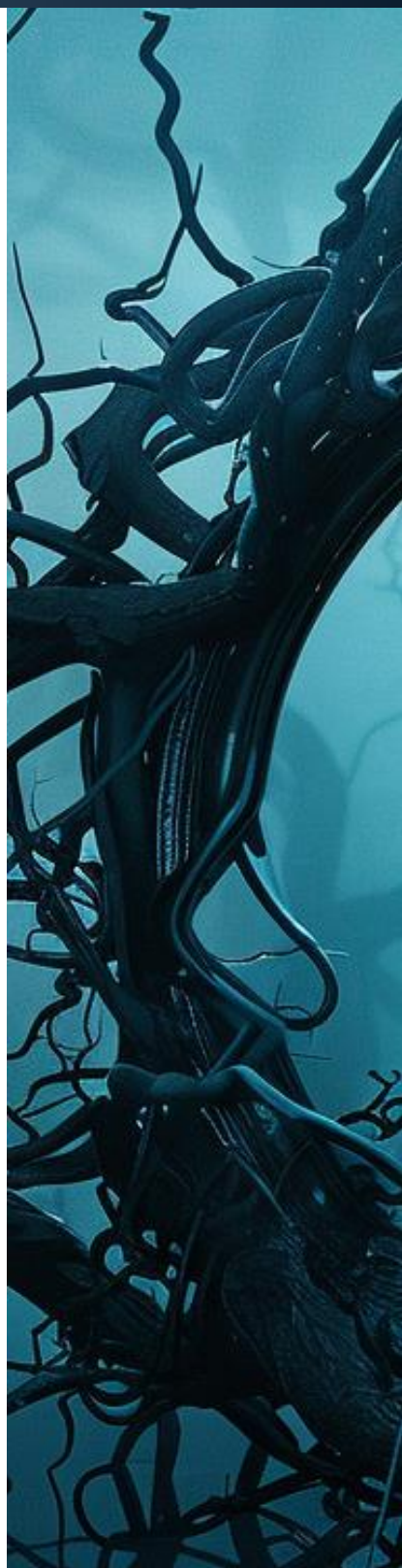
ACCESSO INIZIALE E PERSISTENZA

L'accesso iniziale è ottenuto attraverso vari metodi: tramite **campagne phishing** e **spear phishing**, **rubando le credenziali** (es. Akira, LockBit3.0, QLin, BlackBasta, 8Base, Medusa), **sfruttando il protocollo desktop remoto** (RDP), tramite **l'abuso di credenziali** valide (QLin, LockBit3.0), **siti web compromessi** (drive-by compromise), **configurazioni errate** e impo**stazioni di sicurezza deboli** (QLin, Cactus) o credenziali rubate che vengono acquistate sui forum russi da **Initial Access Brokers (IAB),** intermediari specializzati nell'infiltrazione di sistemi e reti di computer (Lockbit3.0, 8Base, BlackBasta). Infine vengono sfruttate e vulnerabilità zero-day e il software aziendale rimane quindi un obiettivo primario. In particolare:

- **RansomHub** ha ottenuto privilegi di amministratore di dominio, assumendone il controllo sfruttando la vulnerabilità Zero Logon (CVE-2020-1472).
- Vulnerabilità note nei software VPN sono state utilizzate per ottenere (Akira, Cactus) l'accesso iniziale anche attraverso servizi di rete privata virtuale) priva di **autenticazione a più fattori (MFA)** ottenendo l'accesso remoto all'infrastruttura della vittima. All'accesso iniziale viene anche creata una backdooor SSH per la persistenza all'interno della rete compromessa (Cactus).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)



- BlackBasta utilizza estensivamente forum illeciti come Exploit e XSS per reclutare addetti ai lavori all'interno delle organizzazioni target, offrendo significativi incentivi finanziari per l'accesso alla rete, pubblicizzando la sua intenzione.
- Per accedere alle credenziali 8Base utilizza vari tools tra cui password recovery tool *come WebBrowserPassView, PasswordFox o VNCPassView.*
- Akira tenta di abusare delle funzioni dei controller di dominio creando nuovi account di dominio. L'FBI ha anche identificato gli autori delle minacce Akira creando un account amministrativo denominato itadm.
- Dopo aver ottenuto l'accesso agli ambienti target, per ottenere le credenziali necessarie Ransomhub ha sfruttato quelle compromesse sul software di accesso remoto *Citrix* che non aveva l'autenticazione a più fattori abilitata.
- LockBit 3.0 tenta di diffondersi nella rete della vittima utilizzando un elenco preconfigurato di credenziali codificate in fase di compilazione o un account locale compromesso con privilegi elevati. BlackBasta utilizza anche il malware QakBot che esegue azioni brute force per rubare credenziali e raccogliere informazioni (forzatura bruta, iniezioni web, caricamento di altro malware, dumping) .
- Cactus si diffonde sui dispositivi all'interno della rete sfruttando le password deboli o i software senza patch anche attraverso strumenti come *Chisel, Rclone, TotalExec e Scheduled Tasks.* Il ransomware stabilisce la sua persistenza sui sistemi infetti, garantendo che possa continuare le sue operazioni anche dopo il riavvio del sistema.

In prima istanza, le TTPs degli attaccanti si stanno sviluppando su due lati permettendo così di ottenere **accesso ad ogni tipo di rete**, da quelle non protette a quelle costantemente monitorate dai Blue Team: gli **exploit 0-days e 1-days** vengono sviluppati ed adattati alle esigenze dei gruppi in maniera veloce permettendo di sfruttarli ancora prima che la vulnerabilità venga scoperta. Inoltre **il 55% degli attacchi eseguiti su servizi di supply-chain.**

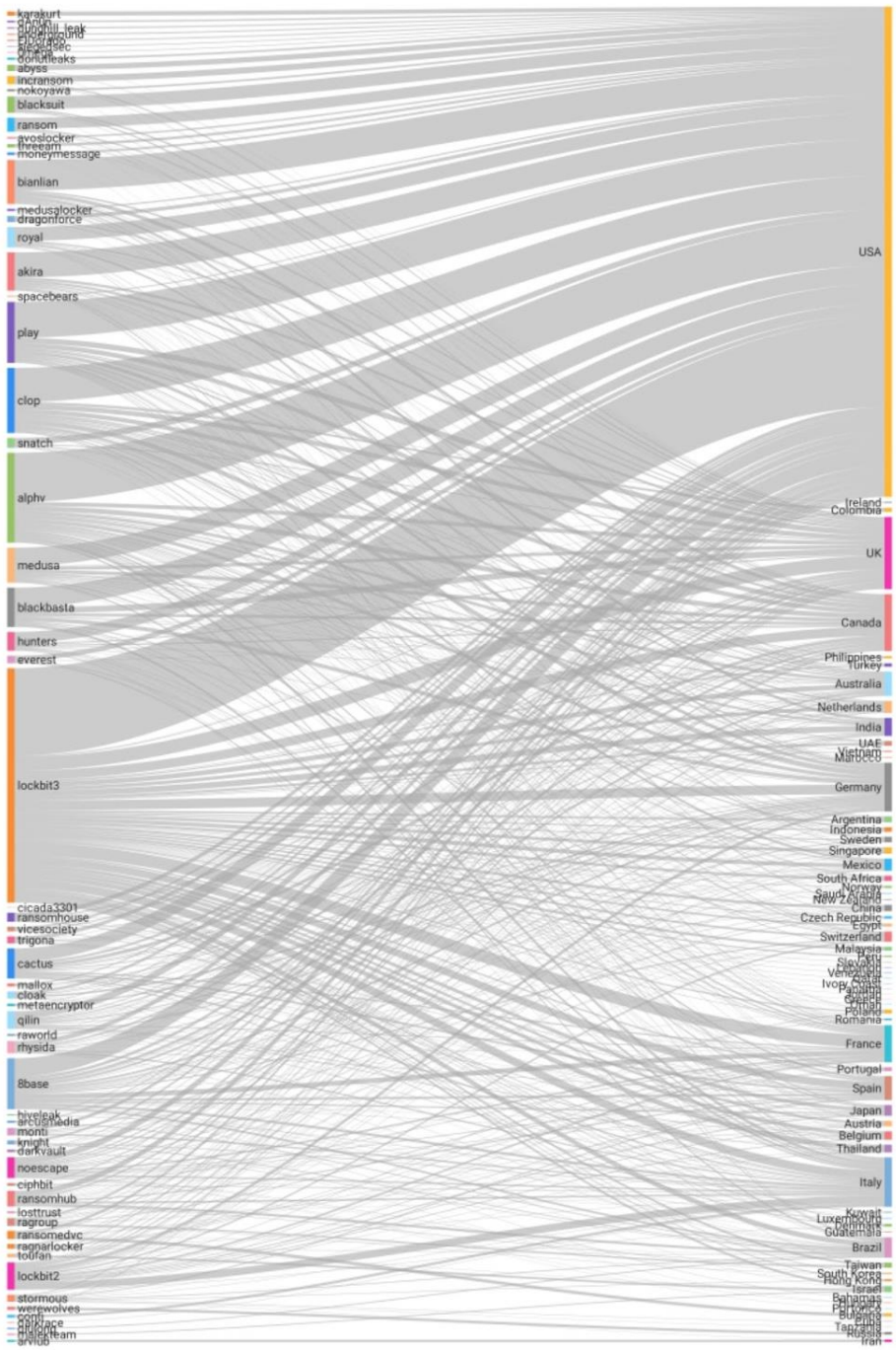
Questo indica come gli attaccanti cerchino sempre di più di ottenere accesso ad aziende di terze parti che possano permettere ulteriori accessi in maniera rapida tramite i servizi forniti dalla vittima e un focus su software/applicazioni enterprise (ex:/ Cloud, security, management di accessi).

In seconda istanza sono state individuate **tattiche, tool ed exploit** outdated anche dai nuovi RaaS come **3AM** che utilizza lo script *PHP Yugeon Web Clicks (2024)* per monitorare il loro DLS. Non è chiara la motivazione di tale scelta ma evidenzia come anche i Threat Actors siano inclini all'utilizzo di vecchi sistemi.

RansomHub ha utilizzato la vulnerabilità ZeroLogon (CVE-2020-1472) in diverse situazioni su server ancora non patchati, **tale exploit consente di ottenere il totale controllo dei domain controller all'interno di reti Active Directory senza la necessità di credenziali**, questo evidenzia come le reti

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)



Flusso degli attacchi gruppi/paese

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)

obsolete (anche quelle di infrastrutture critiche) siano facilmente controllabili. I Threat Actors tentano anche di ottenere credenziali archiviate nel database di Active Directory, con l'obiettivo di compromettere l'intero dominio (Akira) e tentano di raccogliere le credenziali dai browser come Chrome, memorizzate nella cache per diversi utenti.

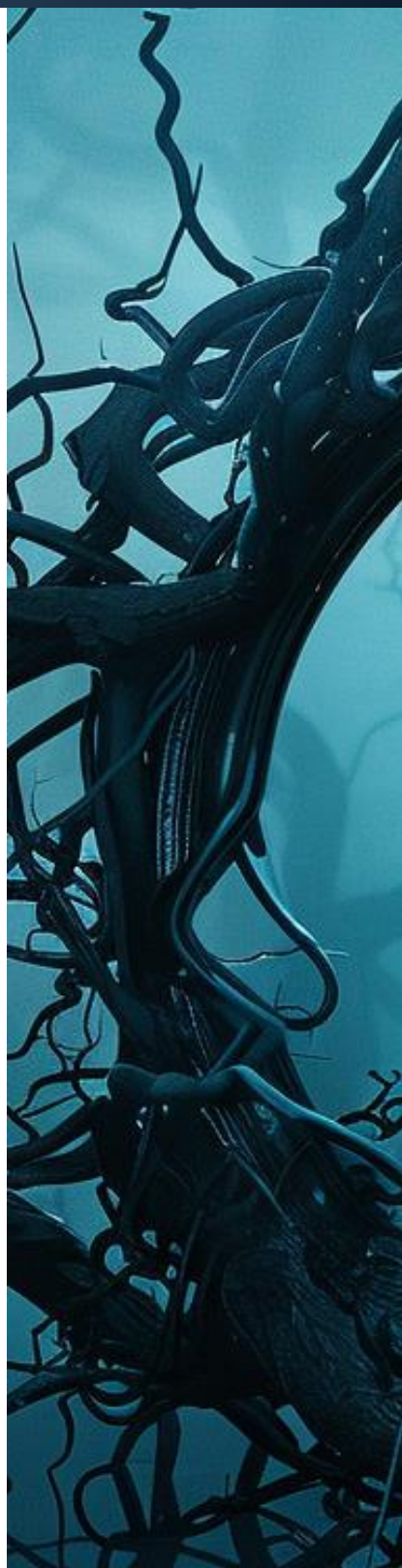
EVASIONE E CONTROLLO

Le gang non solo hanno dimostrato la capacità di penetrare e rimanere all'interno dei sistemi, ma di riuscire ad evadere la difesa, disabilitando i software di sicurezza e terminando i processi relativi agli antivirus (Akira) per evitare il rilevamento. Il fatto di concentrarsi in modo significativo sulle tattiche di evasione della difesa può significare che le gang prendano tempo per comprendere la struttura della rete e aumentare il tempo di permanenza nei sistemi per un processo di esfiltrazione mirato alla doppia estorsione.
Le tattiche comprendono:

- Disabilitazione e la modifica di software di sicurezza come programmi antivirus, soluzioni di rilevamento endpoint o funzionalità di sicurezza nel sistema operativo;
- Offuscamento del software dannoso e Fileless Malware che operano in memoria senza lasciare tracce;
- Modifica del registro di sistema per disabilitare gli avvisi di sicurezza;
- Blocco delle opzioni di ripristino.

Per evadere la difesa dei sistemi Akira manomette gli endpoints, esegue comandi dannosi come differenti utenti e cancella le sue tracce. Cactus riesce ad evadere i sistemi di rilevamento dell'antivirus e utilizza una tecnica di crittografia unica, la quale crittografa il file binario stesso del ransomware, grazie alla quale poi non solo si propaga ma si radica nel sistema con tecniche di offuscamento. QLin utilizza tattiche di offuscamento per eludere il rilevamento (rinomina le funzioni, altera i flussi di controllo, crittografa le stringhe e gli ambienti di debug e sandbox. Per coprire le proprie tracce elimina registri e altri artefatti (TMP) che potrebbero aiutare le indagini forensi (Medusa).

Per stabilire canali di comunicazione e mantenere il controllo sui sistemi compromessi vengono spesso utilizzati strumenti di penetration test. BlackBasta utilizza software commerciali come Cobalt Strike Beacons, SystemBC per nascondere il traffico e comunicare con i sistemi infetti e Rclone per esfiltrare i dati e trasferirli. A questi, per stabilire la persistenza 8base aggiunge strumenti come Chisel, e Scheduled Tasks e, per eludere la difesa, disabilita il Firewall, cancella i registri eventi di Windows e disabilita i componenti di Windows Defender (file batch denominato defoff.bat rilevato come KILLAV). Probabilmente utilizza SystemBC per crittografare il traffico di comando e controllo. Per prendere il controllo sui sistemi compromessi Akira ha utilizzato una backdoor non segnalata (Anydesk.exe / DWAgent.exe) e poi strumenti come AnyDesk e Ngrok.



I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)

INFEZIONE, ESFILTRAZIONE E NUOVI METODI DI ENCRYPTION

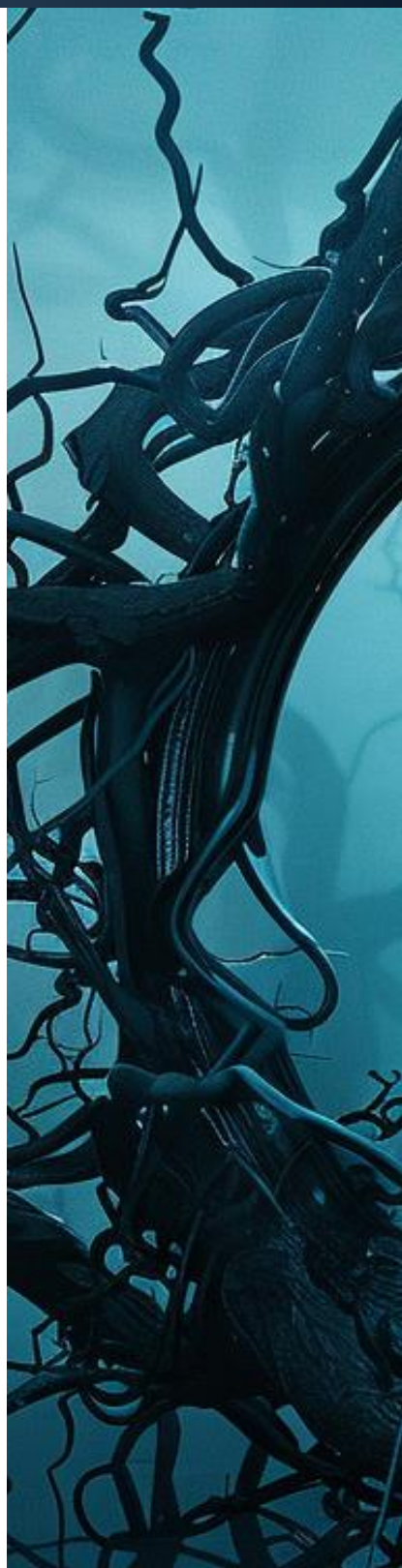
Si stanno osservando tattiche associate ad attacchi ransomware a doppia e tripla estorsione, tra cui l'esfiltrazione, che evitando la distruzione dei dati e potendo generare profitti più elevati, sembra essere diventata uno degli obiettivi preferiti degli aggressori. Per rafforzare la richiesta di riscatto e aumentare la pressione **viene utilizzato l'attacco DDoS come minaccia secondaria dopo l'encryption.** Da notare è che i gruppi di ransomware stanno adottando sempre più strumenti e tecniche associati ad attori sponsorizzati dallo stato con la produzione di malware personalizzati, codici sicuri e sempre più difficili da decodificare.

La catena di attacco delle gang è multiforme. Cactus - secondo l'analisi di SocRadar - che gestisce le operazioni con il software **SuperOps RMM** e simula attacchi con **Cobalt Strike**, crea di canali di comunicazione crittografati con Chisel. Utilizza l'esfiltrazione per aumentare la pressione dell'estorsione. Una volta che i dati sono stati esfiltrati, Cactus crittografa i dispositivi (AES-256-GCM eRSA-4096). La richiesta di riscatto "cAcTuS.readme.txt" viene quindi rilasciata. Tuttavia, una volta che i dati sono stati esfiltrati durante un attacco, i criminali informatici possono continuare a sfruttarli per ulteriori estorsioni molto tempo dopo l'incidente iniziale. Anche se il riscatto viene pagato.

Akira, dopo aver esfiltrato i dati (**FileZilla e WinSCP)** e aver crittografato i sistemi (schema di crittografia ibrido che combina gli algoritmi ChaCha20 e RSA) richiede il pagamento in Bitcoin e per fare pressione sulle vittime seguono le minacce di pubblicare dati sulla rete Tor.

Tra le altre tecniche di esflitrazione, viene usato lo strumento **Stealbit** di Lockbit3.0, utilizzato in precedenza con LockBit2.0 e quella di Qilin, Questo tool combina la crittografia simmetrica per crittografare i file (RSA) con una chiave generata casualmente e asimmetrica per bloccare i file. 8Base utilizza **Smokeloader** per l'offuscamento iniziale e il caricamento del ransomware Phobos.

Le nuove famiglie di ransomware sono riuscite a modernizzarsi includendo nuovi metodi di encryption tra cui **ShrinkLocker** che utilizza la utility **BitLocker** di Windows per criptare i dati tramite il ridimensionamento delle partizione, al momento non si è riuscito ad individuare il RaaS di appartenenza. Gli operatori continuano ad affermarsi creandosi dei tool ad hoc che, pur permettendo di individuare il tipo di operatore nelle indagini di forensics, permettono di adeguarsi alle esigenze di attacco. Scattered Spider è l'esempio cardine, con i tool **Poortry** (driver maligno che permette di terminare processi come EDR e AntiVirus) e **Stonestop** (loader e orchestrator di Poortry) è riuscito a compromettere anche le reti più complesse dal punto di vista degli attaccanti. Medusa ha iniziato a rilasciare ai suoi affiliati una versione personalizzata di **NetScan** facilitando le operazioni di movement e infection del malware.



I THREAT ACTORS

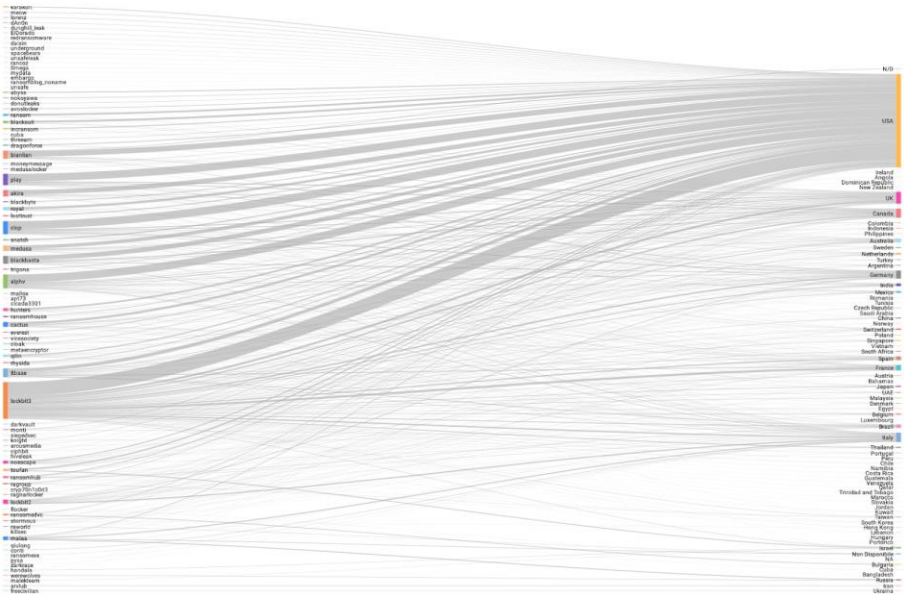
NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)

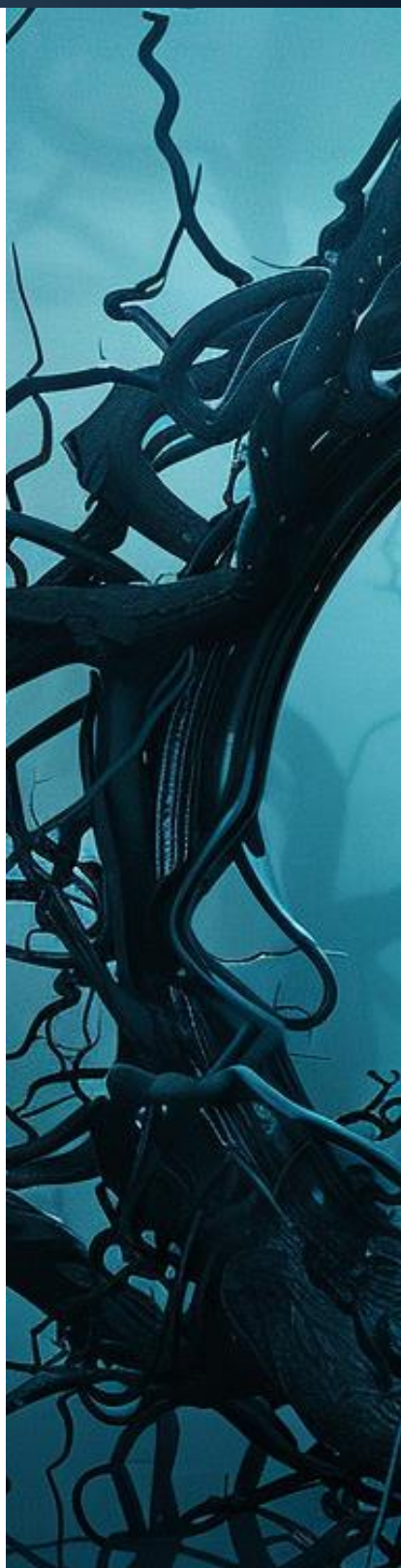
I metodi di estorsioni si stanno muovendo sempre di più al furto di dati rendendolo un metodo prioritario rispetto alla tradizionale encryption alla quale siamo abituati da più di 5 anni. Tutto ciò viene unito ad una specializzazione non tecnica dei RaaS che sono riusciti a comprendere meccanismi legali e di business ed utilizzarli contro le stesse aziende, sta diventando sempre più comune l'aspettare il periodo di tempo (in base alla nazionalità della vittima) entro la quale l'azienda deve avvertire dell'attacco ricevuto e solo dopo pubblicare il post di rivendicazione nel DLS specificando come l'azienda non abbia rispettato la legge in caso di attacchi ed incidenti informatici. Il danno legale alle vittime può creare una maggiore pressione rispetto al tradizionale modus operandi incentivando il pagamento del riscatto, la pubblicazione/vendita di dati sensibili dei clienti non è stata sempre seguita dalle opportune misure delle aziende prevista dalle leggi di data protection.

TTPs SOMIGLIANZE E DIFFERENZE

Nuove tecniche di attacco da vecchie famiglie ransomware

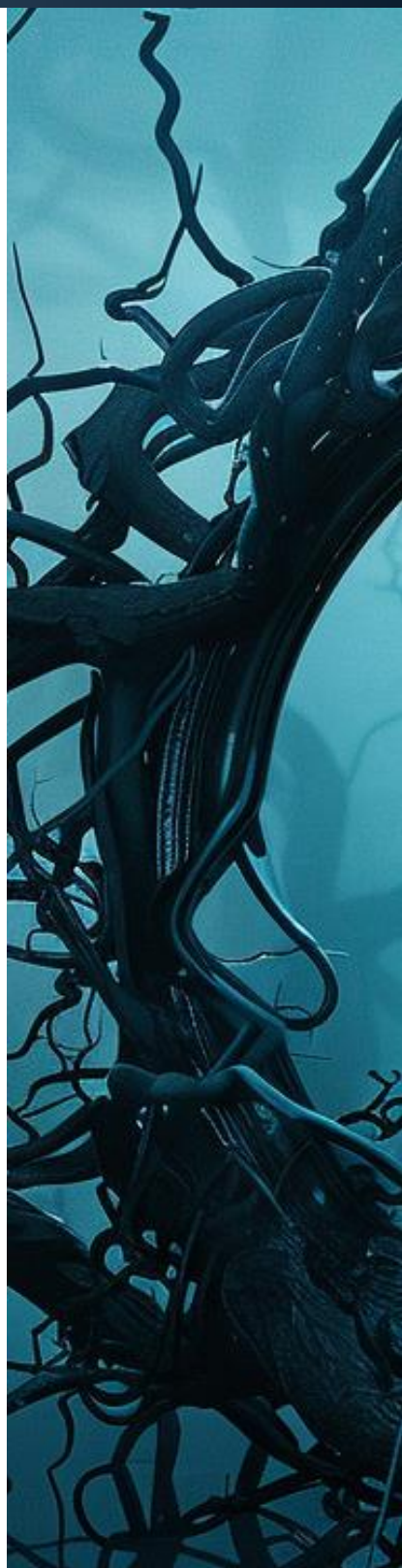
Interessante notare la comparsa di molti gruppi parallelamente al rilascio del codice sorgente del ransomware Babuk (Babyk) - pubblicato dall'utente dyadka0220 'sul forum XSS di lingua russa - che ha generato decine di famiglie ransomware come LockBit, Conti e REvil e sovrapposizioni con locker ESXi ALPHV, Black Basta, Conti, Lockbit, REvil, Play, RansomHouse (White Rabbit e Mario ESXi) a cui si aggiungono gruppi più piccoli. Questo significa che i gruppi ransomware-as-a-service (RaaS) quindi attingono strategicamente ai codici di famiglie di ransomware note e li sviluppano ulteriormente per creare nuove tecniche di attacco.





I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)



Symantec durante l'analisi del RaaS **Ransomhub**, ha rilevato delle interessanti somiglianze con il più vecchio ransomware **Knight** (originariamente noto come **Cyclops**), il cui codice sorgente è stato messo in vendita sui forum clandestini nel febbraio 2024. Se una delle differenze più importanti è l'aggiunta di un comando di sospensione in RansomHub, entrambi i ransomware sono scritti in Go e la maggior parte delle varianti di ciascuna famiglia sono offuscate (Gobfuscate). Hanno inoltre entrambi la possibilità di riavviare un endpoint in modalità provvisoria, prima di avviare la crittografia.

Questa ultima tecnica in un sistema di matrioske - anche se con differenze significative - ci riporta al ransomware **Snatch** (2018/19 Team **Truniger**). Il gruppo hacktivista Snatch è stato collegato al malware nonostante le sue dichiarazioni accertassero che si dedicasse solo sulle fughe di dati. Tuttavia Il membro principale del gruppo Snatch, **Truniger**, è stato affiliato in precedenza al gruppo **GandCrab** (scomparso sulla scena quando è arrivato REvil/Sodinokibi), collegato tra l'altro a una serie di attacchi informatici di alto profilo e operazioni fatte risalire a origini russe. Alcuni gruppi di hacktivisti come quelli citati sviluppano un proprio malware per raggiungere un preciso obiettivo finanziario, che viene poi utilizzato per i loro obiettivi di hacktivismo.

Citiamo quest'ultimo caso per evidenziare come i gruppi hacktivisti si dedichino - a volte in chiaro - a pratiche di estorsione per raggiungere i loro obiettivi. Non ultimo il caso del gruppo GhostSec, che ha rivelato in un video proof-of-concept come il loro malware personalizzato può crittografare i dati ed eludere il rilevamento da parte del software antivirus.

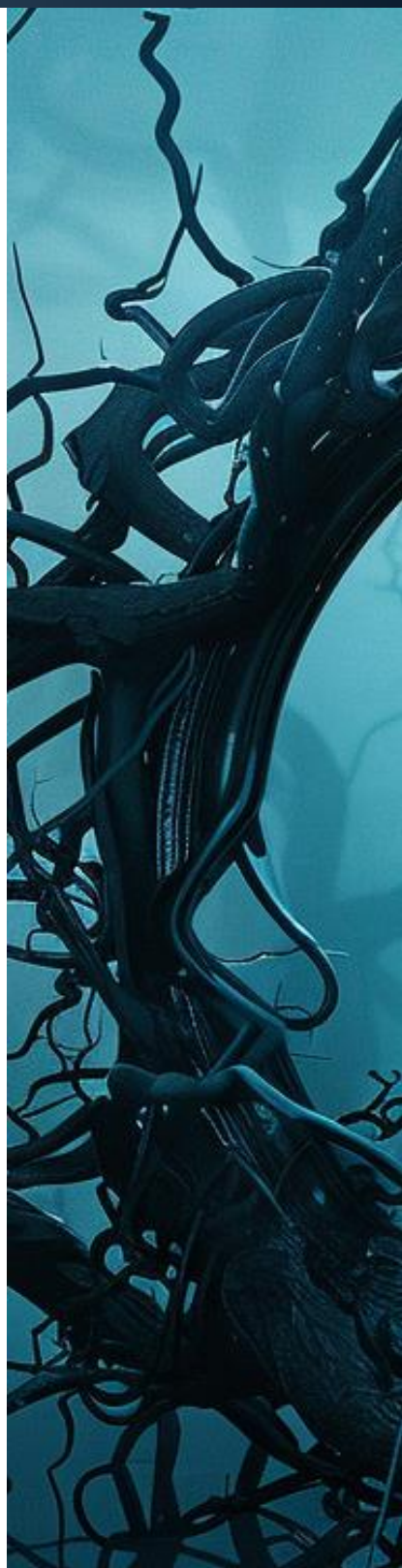
Approcci calcolati

Secondo un'analisi di SOCRadar, gli attori di Snatch **trascorrevano fino a tre mesi sul sistema di una vittima prima di distribuire il ransomware**, indicando "un approccio calcolato, garantendo una massimizzazione del loro eventuale attacco". Quest'ultima è una tendenza che riguarda i gruppi ransomware e non è mai da escludere: i ransomware aumentano al pari dell'aumento delle tensioni dovute ai conflitti e al caos internazionale in corso. Anche se la prima motivazione resta sempre quella economica, non si può escludere che possano venire colpite organizzazioni che possono essere percepite come contrari alle politiche del paese avversario e quindi vittime preferibili ad altre.

Le tattiche vengono affinate con il passare del tempo e si evolvono evitando in molti casi il rischio di rilevamento. In questo caso alcuni gruppi mirano solo all'esfiltrazione dei dati senza implementare il ransomware (Akira, RansomHouse, RansomHub).

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)



Sviluppatori da remoto

E' anche noto che i gruppi ransomware assumano sviluppatori da remoto per progetti specifici: se figura centrale dello sviluppo di Babuk è **Mikhail Matveev (LockBit, Babuk e Hive)**, che utilizza la lingua russa e identificato come partecipante ad almeno tre varianti (LockBit, Babuk e Hive), Brian Krebs, indagando sul gruppo **8base** (attivo dal 2022) ha scoperto che il loro sito darknet ha rivelato inavvertitamente il suo vero indirizzo e si collegava a un server Gitlab privato (gruppo Jcube) - da cui estraeva il codice dalla directory "clients". Krebs è così arrivato al responsabile del codice del gruppo JCube, Andrei Kolev, uno sviluppatore di 36 anni di Chisinau, Moldavia: mentre Krebs lo stava 'intervistando' il collegamento è scomparso restituendo l'errore 405.

•

Stessa nota, stessa comunicazione, famiglie diverse?

8base, che colpisce un'ampia gamma di settori attraverso tattiche di doppia estorsione, ha attirato l'attenzione per delle somiglianze testuali nelle richieste di riscatto con quelle utilizzate da RansomHouse, che acquista dati già trapelati, collabora con siti di fuga di dati e poi estorce denaro alle aziende. Si tratta di gruppi separati o di operazioni coordinate di esfiltrazione di dati? Le analisi di VMware hanno rivelato una corrispondenza al 99% tra le loro richieste di riscatto e la sezione home, termini di utilizzo e domande frequenti dei loro siti.

•

False flag?

Allo stesso tempo, anche se i gruppi ransomware, sembrano essere uniti da caratteristiche comuni, come la lingua russa nel codice sorgente o nei siti di comunicazione dei criminali, questo non identifica in alcun modo chi possa trovarsi dietro.

A volte i criminali fanno uso di vere e proprie **false flag** che agiscono da **dirottatore**. Dopo l'incidente all'ISP ucraino, Serhii Demediuk (vice Segretario del Consiglio di Sicurezza e Difesa Nazionale dell'Ucraina), ha dichiarato che durante l'attacco ransomware all'infrastruttura, l'aggressore è riuscito a danneggiare i server virtuali dell'azienda, compresi i backup situati in diverse sedi: la richiesta di riscatto l'attacco è stata poi eseguita dal gruppo ransomware RansomHub (legato ad ALPHV/Black Cat). Demediuk ipotizza che si sia trattata di un'operazione false flag dei servizi speciali russi volta a interrompere l'attività di un'altra società di telecomunicazioni ucraina, o che i membri del gruppo abbiano utilizzato i loro strumenti e TTP senza la consueta motivazione finanziaria.

RansomHub dome RaaS dà precise indicazioni agli affiliatii che non devono prender di mira specifici paesi (CIS, Cina, Cuba e Corea del Nord) o organizzazioni non-profit, ma non ha altri schemi specifici. Attacca settori come l'industria, l'healthcare, quello dell'educazione o i servizi finanziari e sino ad oggi paesi come: Italia Stati Uniti, Brasile, Indonesia o Vietnam.

I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)

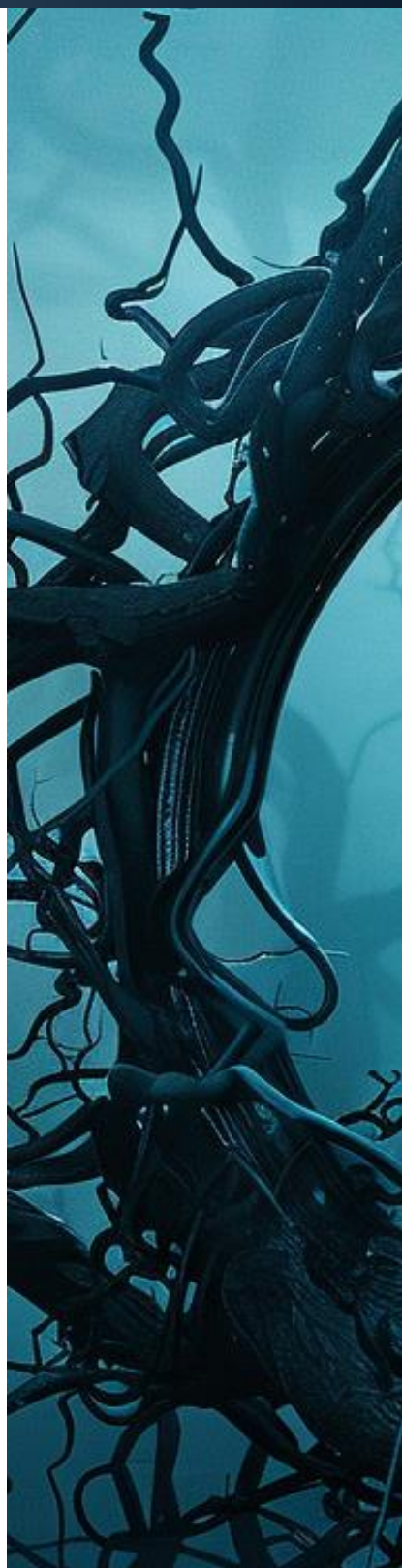
Controversie e rivendicazioni incrociate

Gli affiliati ransomware inoltre si dipanano in tutto il mondo e non sempre lavorano per un solo gruppo, ma spesso per altri e lo possono fare anche in modo parallelo. Ciò genera controversie come le rivendicazioni incrociate (RansomHouse e Alphv/BlackCat, LockBit 3.0) che coinvolgono anche **RansomHouse**. (BianLian, Snatch, Stormous e Abyss).

Allo stesso modo vecchi affiliati ad una gang portano nel nuovo gruppo i loro "strumenti di lavoro" preferiti dando poi luogo ad una sovrapposizione di codici. In questo ultimo caso il tasso di commissione del 90% di **RansomHub (attivo dal 2020),** i bonus come il dcryptor gratuito e la sua capacità di nuovi utenti nell'underground ad esempio, avrebbero portato nella gang ex affiliati come **Scattered Spider** (su base TTP) o **Noberus** (ex ALPHV, Blackcat).

TRENDS

- La proliferazione di attacchi contro settori critici come quello manifatturiero è aumentata.
- Si prevede che in futuro i gruppi ransomware **prenderanno di mira sempre più gli ambienti OT e i loro componenti**, diventando sempre più interessati agli ambienti dei sistemi di controllo industriale (ICS), in particolare quelli con dispositivi Virtual Network Computing (VNC) connessi.
- La **principale fonte di estorsione dei gruppi ransomware è l'esfiltrazione** dei file: contro ciò le soluzioni di backup - efficaci invece contro la crittografia - non sono sufficienti.
- Con le tattiche di double extortion le vittime vengono attaccate una seconda volta, con la **probabilità di essere attaccate a pochi mesi dal primo attacco**.
- Lo sfruttamento delle **vulnerabilità zero-day critiche** è aumentata al pari delle risorse interne dei gruppi.
- la tendenza emergente dei gruppi di ransomware che influenzano i propri affiliati a spostare l'attenzione e **massimizzare l'impatto su settori specifici** solleva preoccupazioni.
- Il periodo di permanenza dei criminali nei sistemi è aumentato assieme ai **metodi di persistenza come backdoor**. In questo modo gli attaccanti possono studiare la rete ed infrastrutture nelle vittime scegliendo con attenzione i dati da rubare e criptare oltre all'accesso ad ulteriori reti sfruttando le prime compromissione in maniera efficace.
- All'aumento delle esposizioni dei dati esposti online e dei rischi legati alla frode finanziaria e al furto di identità, **è probabile che le azioni legali aumentino**, dato che le aziende possono essere ritenute responsabili di una mancata protezione.



I THREAT ACTORS

NUOVE TECNICHE TATTICHE E PROCEDURE (TTPS)

Mappa di diffusione degli attacchi ransomware nel mondo

STRATEGIE DI DIFESA

MISURE PREVENTIVE, CONSAPEVOLEZZA DEL RISCHIO, RACCOMANDAZIONI

STRATEGIE DI DIFESA

MISURE PREVENTIVE

Le minacce informatiche sono in continua evoluzione e i ransomware rappresentano una delle sfide più preoccupanti per le organizzazioni di ogni dimensione. Questi malware prendono in ostaggio i dati e i sistemi IT, chiedendo un riscatto per il loro rilascio. Le conseguenze di un attacco ransomware possono essere devastanti, causando perdite finanziarie, interruzioni del servizio e danni alla reputazione.

Per contrastare questa minaccia, è fondamentale adottare un approccio proattivo e multilivello alla sicurezza informatica.

BACKUP IMMUTABILI E CON VERSIONING

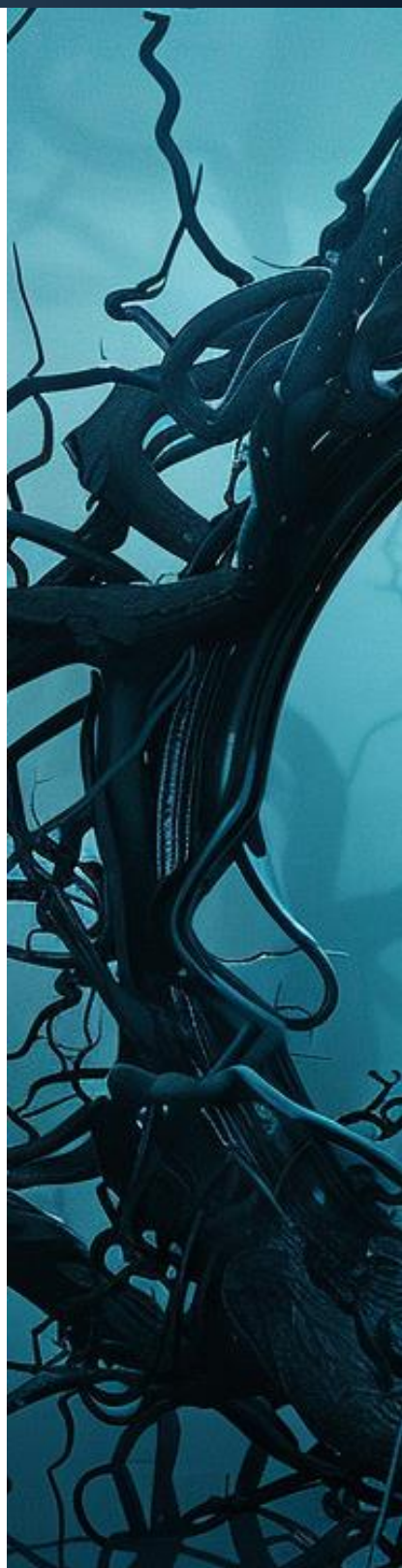
Implementare un sistema di backup che garantisca l'immutabilità e il versioning dei dati. I backup sono un modo semplice ma efficace per mitigare il più possibile il danno ricevuto, nonostante ci siano altri metodi, l'assenza di backup aumenta i tempi di recovery intasando i passi necessari per gestire la minaccia. I backup devono essere condotti in maniera regolare, incrementale e resiliente assieme ad una opportuna infrastruttura per poter ripristinare le reti il più efficientemente possibile.

MINIMIZZARE LA SUPERFICIE DI ATTACCO

Limitare al minimo il numero di software installati su ogni dispositivo e soprattutto su internet, ed utilizzare solo software affidabili e regolarmente aggiornati. Bisogna, inoltre, applicare policy di password robuste e limitare l'accesso ai dati sensibili solo agli utenti autorizzati, adottando il principio del minimo privilegio.

SICUREZZA SU PIU' LIVELLI

Implementare più livelli di sicurezza, tra cui firewall, software antivirus, sistemi di rilevamento delle intrusioni (IDS), e sistemi di prevenzione delle intrusioni (IPS). Questa configurazione offre una difesa robusta contro un'ampia gamma di minacce, inclusi i ransomware. Per rendere più efficace la difesa è consigliabile anche l'utilizzo di Honeypot. Gli honeypot sono sistemi informatici progettati per attirare e ingannare gli hacker, allontanandoli dai sistemi reali e proteggendo i dati aziendali. L'utilizzo di honeypot può aumentare l'efficacia della difesa. Questi sistemi simulano sistemi vulnerabili, attirando gli hacker e allontanandoli dai sistemi reali, proteggendo i dati aziendali.



STRATEGIE DI DIFESA

MISURE PREVENTIVE

Una volta che un hacker entra nell'honeypot, i suoi movimenti vengono registrati e analizzati, consentendo di raccogliere informazioni preziose sulle sue tecniche e sui suoi obiettivi.

MANTENERE SEMPRE IL SOFTWARE AGGIORNATO

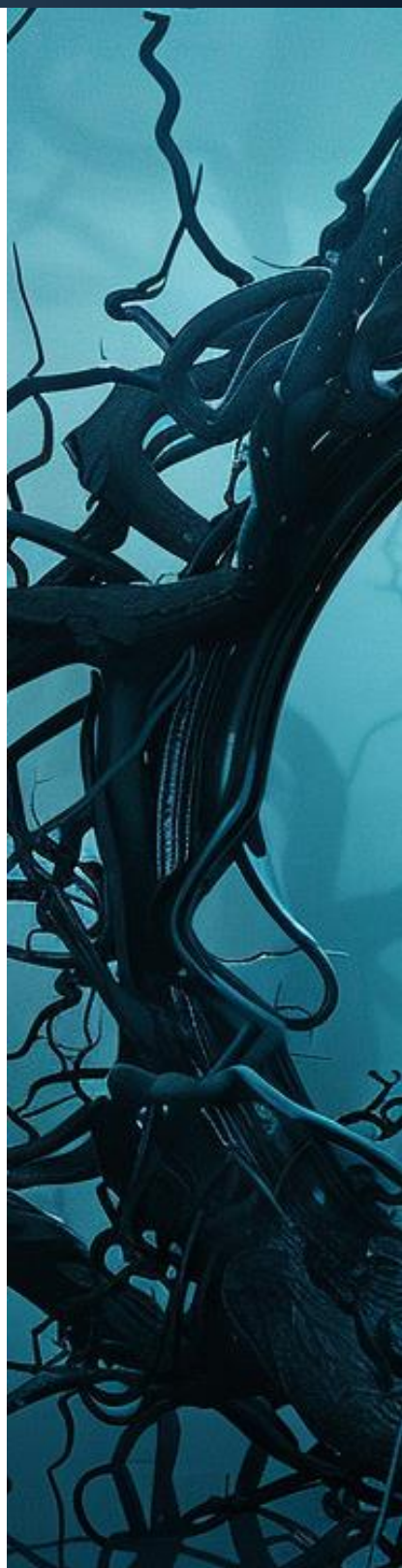
Assicurarsi che tutti i software, compresi i sistemi operativi, browser web e applicazioni siano costantemente aggiornati all'ultima versione. Gli aggiornamenti includono spesso patch di sicurezza che riparano vulnerabilità sfruttate dagli hacker per diffondere ransomware.

MISURE DI ENDPOINT PROTECTION

Come dimostrato da recenti ricerche, i malware sofisticati possono eludere i tradizionali strumenti di difesa basati sulla firma, come gli antivirus. Per contrastare ciò, è necessario implementare misure di Endpoint Protection che monitorino l'intera attività del dispositivo, non solo il traffico di rete. L'Endpoint Protection offre una visione completa dell'attività del dispositivo, consentendo di rilevare in tempo reale modifiche sospette delle registry key, attività anomale nei log di sistema, connessioni di rete non autorizzate ed altri indicatori di compromissione. Questo approccio completo permette di individuare non solo l'esecuzione di malware, ma anche tentativi di persistenza e escalation dei privilegi, che spesso sfuggono agli antivirus tradizionali.

LEAST PRIVILEGE PRINCIPLE

Il principio del privilegio minimo (LPP) stabilisce che ogni utente o sistema dovrebbe avere accesso solo alle risorse e ai dati necessari per svolgere le proprie mansioni. Limitare i privilegi superflui riduce il rischio di danni in caso di attacchi. Le reti Active Directory, spesso sottovalutate, sono un bersaglio primario per gli hacker. Per questo motivo, è fondamentale analizzarne le configurazioni per individuare e correggere eventuali vulnerabilità. L'implementazione di una struttura a Tier, in collaborazione con gli amministratori di rete, può aiutare a migliorare la sicurezza complessiva della rete, bilanciando le esigenze di sicurezza con quelle di usabilità. Concedere agli utenti solo i permessi necessari limita l'impatto potenziale di un attacco e rende più facile individuare eventuali attività sospette.



STRATEGIE DI DIFESA

MISURE PREVENTIVE

MONITORAGGIO E SEGMENTAZIONE DELLE RETI

Monitorare regolarmente le reti e i sistemi alla ricerca di attività sospette o intrusioni, rispondendo prontamente agli avvisi o incidenti. Implementare strumenti di SIEM (Security Information and Event Management) per automatizzare il monitoraggio e il rilevamento rapido delle minacce. Per lanciare un attacco e raggiungere i loro obiettivi gli attaccanti necessitano di muoversi all'interno della rete prima di eseguire il ransomware (o qualsiasi tipo di malware). Segmentare quindi la rete in VLAN (Virtual Local Area Network) per isolare logicamente le diverse reti (ad esempio, IT, segreteria, dipendenti) aiuta a limitare la propagazione di malware. La segmentazione offre vari vantaggi come la gestione della rete, la riduzione della superficie d'attacco e facilita il rilevamento e la risposta agli incidenti.

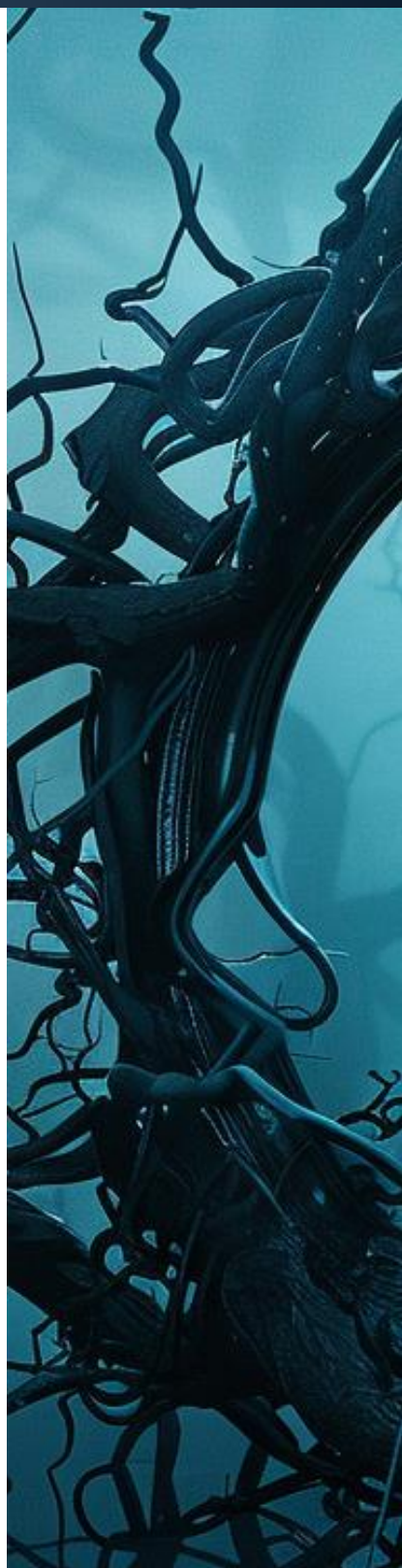
KILL SWITCH

Un kill switch è un meccanismo di sicurezza che può essere utilizzato per disconnettere o isolare un sistema informatico in caso di attacco grave. I kill switch possono essere implementati a livello software o hardware. Un kill switch software può essere attivato manualmente da un amministratore di sistema o automaticamente da un sistema di rilevamento delle intrusioni. Un kill switch hardware interrompe l'alimentazione del sistema, rendendolo inutilizzabile.

E NON DIMENTICARE MAI CHE ...

La sicurezza informatica è una disciplina tecnica in cui l'efficacia si misura contrastando i criminali informatici sul loro stesso terreno. Le attività di assessment tecnico, come il vulnerability assessment e il penetration test, sono fondamentali per una correttaadozione di un efficace processo di ICT Risk Management.

Queste simulazioni di attacchi reali forniscono indicazioni preziose su come migliorare le infrastrutture IT, prevenendo così eventuali compromissioni future.



STRATEGIE DI DIFESA

CONSAPEVOLEZZA DEL RISCHIO

La consapevolezza del rischio è un concetto fondamentale nella gestione aziendale, che implica la comprensione e l'identificazione delle potenziali minacce che possono compromettere il raggiungimento degli obiettivi strategici. In ambito generale, il rischio rappresenta la possibilità che un evento avverso possa influenzare negativamente un'organizzazione, richiedendo pertanto un'adeguata valutazione e gestione.

Adottare un approccio sistematico per identificare e valutare i potenziali rischi informatici che l'organizzazione potrebbe affrontare. Questo include l'analisi delle minacce interne ed esterne, delle vulnerabilità dei sistemi e dei potenziali impatti di un data breach. Sulla base della valutazione dei rischi, implementare controlli di sicurezza adeguati per mitigare i rischi identificati. Questi controlli possono includere misure tecniche, organizzative e procedurali.

- **Formazione e sensibilizzazione utenti:** Gli utenti finali sono la linea di demarcazione tra un attacco concluso con successo ed uno fallito prima ancora di essere attivato. Fornire loro una formazione regolare sulla sicurezza informatica è fondamentale per aiutarli a riconoscere ed evitare potenziali minacce, come le truffe di phishing o le email sospette.
- **Comunicazione e trasparenza:** È importante comunicare in modo chiaro e trasparente ai dipendenti i rischi associati ai cyber attacchi e le procedure da seguire in caso di incidenti.
- **Esercitazioni di simulazione:** Le esercitazioni di simulazione di attacchi ransomware permettono di testare le capacità di risposta dell'organizzazione e di identificare eventuali aree di miglioramento.
- **Adottare un piano di risposta agli incidenti:** Un piano dettagliato ben definito è fondamentale per contenere i danni e minimizzare il tempo di inattività in caso di attacco ransomware. Il piano dovrebbe includere procedure chiare per l'identificazione, il contenimento, l'eradicazione e il recupero.
- **Stipulare un'assicurazione contro i cyber attacchi**: Un'assicurazione può fornire copertura finanziaria per le perdite derivanti da un attacco ransomware, inclusi i costi di ripristino dei dati, la perdita di profitti e le spese legali.
- **Collaborare con le autorità**: In caso di attacco ransomware, è importante collaborare con le autorità competenti per denunciare l'incidente e ottenere assistenza nelle indagini.

La consapevolezza del rischio è un concetto fondamentale nella gestione aziendale, che implica la comprensione e l'identificazione delle potenziali minacce che possono compromettere il raggiungimento degli obiettivi strategici. In ambito generale, il rischio rappresenta la possibilità che un evento avverso possa influenzare negativamente un'organizzazione, richiedendo pertanto un'adeguata valutazione e gestione.

Sebbene il «rischio zero» non sia una dimensione reale, è possibile ridurlo fino a che possa divenire accettabile per una organizzazione. Nel contesto cyber, il rischio assume connotazioni specifiche legate alla sicurezza delle informazioni e alla protezione dei dati. La crescente dipendenza dalle tecnologie digitali espone le organizzazioni a una varietà di minacce informatiche, tra cui il ransomware, che possono causare danni significativi in termini di **perdita di dati, interruzione delle attività e impatti finanziari**.

Per sviluppare una consapevolezza più profonda del rischio cyber, le organizzazioni devono adottare processi e approcci specifici. La **risk analysis (analisi del rischio)** è essenziale per identificare, valutare e prioritizzare i rischi, consentendo alle aziende di allocare le risorse in modo efficace e di implementare le misure di sicurezza più adeguate.

Un approccio efficace alla gestione del rischio cyber deve essere improntato alla protezione della **Confidentiality (Riservatezza), Integrity (Integrità) e Availability (Disponibilità) dei dati,** noti come il modello **CIA**. La riservatezza garantisce che i dati siano accessibili solo a chi è autorizzato, prevenendo accessi non autorizzati e proteggendo la privacy delle informazioni. Parallelamente, la **Business Impact Analysis (BIA)** gioca un ruolo cruciale nel determinare le conseguenze di un'interruzione delle operazioni aziendali, aiutando a comprendere l'importanza di ogni funzione critica e a sviluppare piani di continuità operativa robusti.

STRATEGIE DI DIFESA

LA TRASPARENZA PRIMA DI TUTTO

Non appena si scopre di essere stati colpiti da un attacco ransomware, è fondamentale mantenere la calma.

Per prima cosa contattare immediatamente le forze dell'ordine e fare tutto il possibile per arginare la diffusione dell'attacco. È importante non farsi prendere dal panico per un incidente informatico.

LA TRASPARENZA È AL PRIMO POSTO

In Italia, molte aziende temono che rivelare un attacco possa danneggiare la loro reputazione e immagine. Tuttavia, non comunicare apertamente ma lasciare che la notizia si diffonda tramite altre fonti può essere dannoso per la fiducia dei propri stakeholder. Un incidente informatico può capitare a chiunque, anche alle aziende della lista Fortune 500.

Per questo motivo, è cruciale avere una buona strategia di comunicazione e fornire ai clienti tutte le informazioni necessarie sull'evoluzione dell'attacco, senza preoccuparsi eccessivamente della reputazione. Una volta terminato l'incidente, è opportuno che le aziende spieghino la loro esperienza, come i criminali informatici sono entrati nelle loro infrastrutture IT e cosa hanno fatto per arginare l'attacco.

PIU' LESSON LEARNED E MENO PAURE

Questo processo di condivisione chiamate anche «lesson learned» è fondamentale per dare un vantaggio ad altre aziende, aiutandole a evitare che un attacco simile si verifichi nelle loro infrastrutture.

In sintesi, affrontare un attacco ransomware con trasparenza e comunicazione proattiva non solo rafforza la fiducia degli stakeholder, ma contribuisce anche alla sicurezza complessiva del settore, creando una comunità più resiliente e informata.

A scuola di Crisis Management

In ambito aziendale e pubblico, spesso ci dimentichiamo della responsabilità fondamentale di gestire le crisi in modo efficace e trasparente. Mentre le aziende private devono rispondere ai propri clienti, le pubbliche amministrazioni sono tenute a rendere conto ai cittadini e agli elettori.

Questo principio dovrebbe precedere qualsiasi considerazione rivolta al consiglio di amministrazione, al top management o alle dinamiche interne. Nel contesto italiano, l'incapacità di gestire adeguatamente le crisi in ambito di sicurezza informatica è evidente.

Dobbiamo imparare da chi riesce a farlo meglio di noi, trarne insegnamenti senza necessariamente inventare qualcosa di nuovo o trascendentale. In fondo, si tratta di osservare come altri possano uscire più forti da una crisi e applicare tali lezioni nella nostra realtà. Non dobbiamo illuderci che non subiremo mai un incidente informatico, o che i nostri dati non siano interessanti per qualcuno.

Oggi, ogni organizzazione è potenzialmente destinata a sperimentare un incidente di sicurezza informatica. Quello che varia è soltanto il momento in cui accadrà.

Perciò è essenziale acquisire competenze solide nel "crisis management". Questa disciplina è cruciale non solo per rispondere agli incidenti informatici, ma soprattutto per affrontare efficacemente minacce come il ransomware. Prima o poi, saremo chiamati ad applicarla.

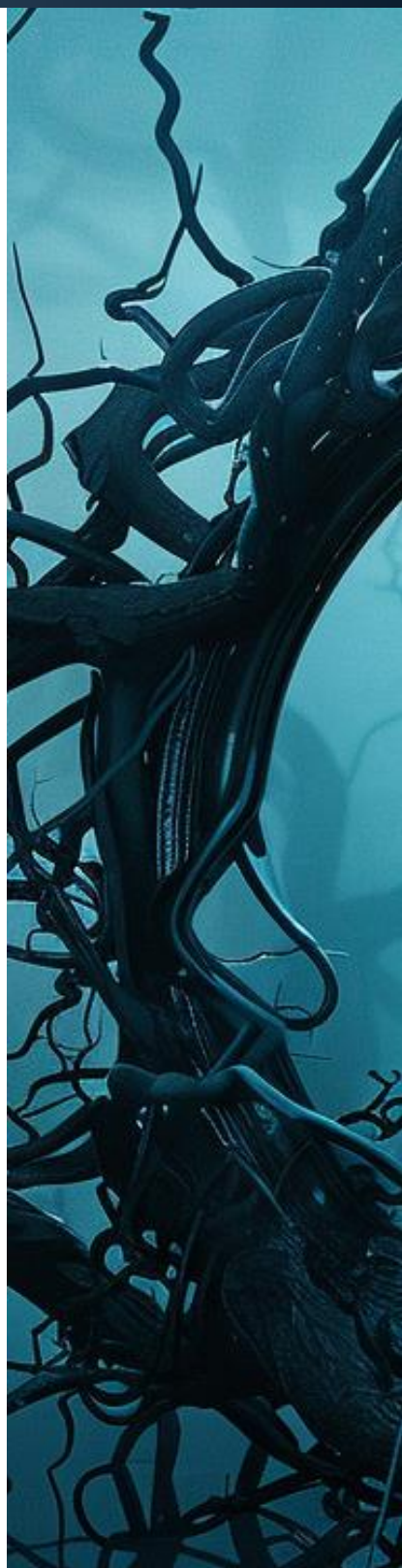
STRATEGIE DI DIFESA

CYBER THREAT INTELLIGENCE

Per conoscere le minacce e prevenire eventuali attacchi, un programma cyber deve includere la **Cyber Threat Intelligence (CTI).** La Cyber Threat Intelligence è un insieme di informazioni analitiche e contestuali sulle minacce cibernetiche che aiutano le organizzazioni. Le fonti di CTI includono dati provenienti da sensori di rete, log di sistema, fonti open-source, e comunità di scambio di informazioni tra aziende e governi. La CTI consente di accedere a informazioni strategiche di prima mano, fornendo una comprensione approfondita dell'evoluzione delle minacce nel dark web. Questo permette di prendere decisioni informate su come contrastarle efficacemente.

Investire nella CTI porta a numerosi benefici per la sicurezza informatica di un'organizzazione. Migliora la sicurezza proattiva, permettendo di adottare misure preventive basate su informazioni aggiornate e precise. I benefici della CTI Possono essere sintetizzati in:

- **Sicurezza Proattiva:** Permette di adottare misure preventive basate su informazioni aggiornate e precise.
- **Rilevamento in Tempo Reale**: Facilita l'identificazione tempestiva di comportamenti anomali e potenziali attacchi.
- **Risposta Rapida e Mirata:** Consente di sviluppare piani di risposta agli incidenti ben informati, riducendo i tempi di inattività e l'impatto degli attacchi.
- **Riduzione dei Costi:** Prevenire gli attacchi ransomware tramite l'uso efficace della CTI può ridurre i costi associati alla risposta agli incidenti e alla perdita di dati.
- **Miglioramento della Formazione e Consapevolezza:** Aumenta la formazione e la consapevolezza all'interno dell'organizzazione, riducendo il rischio di errori umani.
- **Creazione di Firme di Rilevamento Specifiche:** Fornisce dettagli sui pattern di attacco, permettendo la creazione di firme di rilevamento specifiche.
- **Identificazione delle Varianti di Ransomware:** Facilita l'uso di strumenti di decrittazione specifici per recuperare i dati senza pagare il riscatto.
- **Vantaggio Competitivo***:* Migliora la sicurezza informatica complessiva, rappresentando un vantaggio competitivo in un panorama digitale minaccioso.



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.

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

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

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

Alessio Stefan
Studente magistrale di AI & Cybersecurity e CTF player

Sandro Sana
Esperto IT dal 1990, specializzato in Cybersecurity dal 2014, docente e relatore SMAU

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