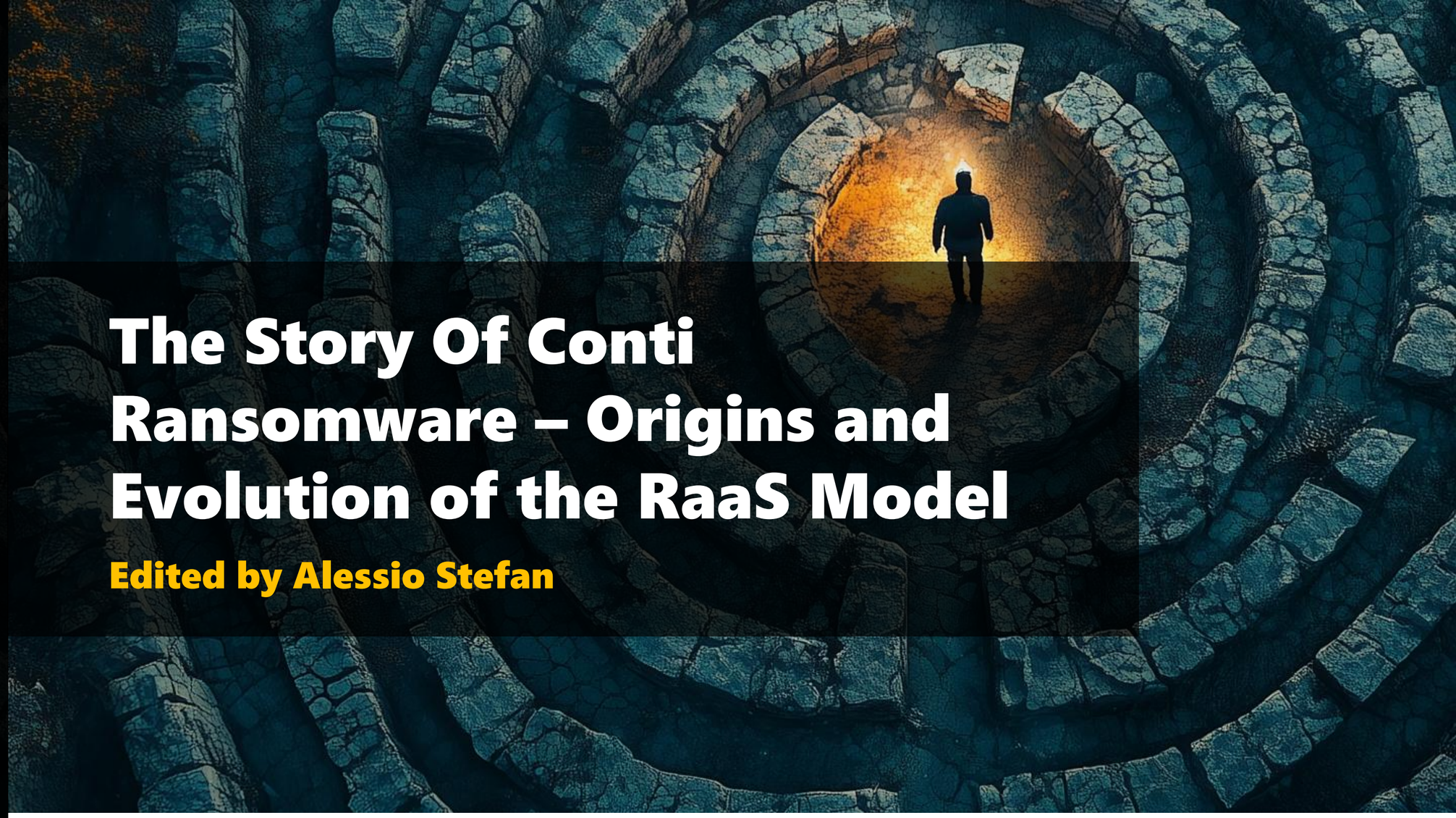
WWW.REDHOTCYBER.COM

La cybersecurity è condivisione.
Riconosci il rischio, combattilo,
condividi le tue esperienze ed
incentiva gli altri a fare meglio di te.



The Story Of Conti Ransomware – Origins and Evolution of the RaaS Model

Edited by Alessio Stefan

IL COLLETTIVO DARKLAB E' UN SOTTO GRUPPO DELLA COMMUNITY DI RED HOT CYBER SPECIALIZZATO AL MONITORAGGIO DELLE MINACCE INFORMATICHE.

Dark Lab nasce con l'obiettivo principale di diffondere la conoscenza sulle minacce informatiche per migliorare la consapevolezza e le difese digitali del paese.

INTRODUCTION

Alessio Stefan

The phrase 'Stereotypes make one story the only story' perfectly captures the limited understanding of digital threats that, for the most part, has always prevailed in the West.

Over the years, the image of the hooded hacker, with extraordinary (almost unmatched) intelligence and destructive intentions, driven by purely economic motives, or the Russian hacker, accused of sabotaging governments and undermining democratic processes with state support, has been consolidated.

These archetypes exist, but they are only one part of a much more complex landscape that evolves independently. Conti, for example, played a key role in the development of the Ransomware-as-a-Service phenomenon, with roots in the Ransom Cartel.After its separation from the cartel, the group launched autonomous operations, evolving as we know it today.

Unlike other groups that tried to keep political motivations and criminal activities separate, Conti mixed the two spheres ambiguously and unscrupulously, affecting victims not only economically but also reputatively, attracting the attention of governments in the United States and Europe.

The breaking point was the Russian invasion of Ukraine, when Conti openly took a political stance. Here, the archetype of the Russian hacker emerges in full force, and this story gives us an opportunity to explore the underlying dynamics, showing how adhering to such stereotypes can become a condemnation.

Conti's story is also linked to numerous law enforcement efforts, both governmental and independent, from which we can learn lessons for dealing with current and future digital threats

INDEX OF CONTENTS

INTRODUCTION

The Evolution of Ransomware: From Floppy Disks to RaaS Ecosystems

Ransomware, a malware designed to encrypt data making them restorable only with the use of a private key. Relatively simple math is all that threat actors out there needs to disrupt networks around the globe, once lock out you can get your plain data back just in one way : cripto payment.

The real first Ransomware ever discovered was made by **Joseph L. Popp Jr.** with his malware called **AIDS**. Isolated in 1989, the program was stored inside a Floppy Disk with the label *"AIDS Information Introductory"*, sent in the email of 20,000 of WHO conference in Stockholm. Once opened the **C:** drive of the victim is fully encrypted, game over. To take your data computer back you had to pay a ransom ($200) sent via envelope to receive anoter floppy used to decrypt files.

That was just a sweet start of a real phenomenon and independent ecosystem with it's own rules and organization. **Ransomware-as-a-Service (RaaS)** provide an affilation model between ransomware developers and attackers, in this way both party can improve attacks efficency with always increasing payments.

In this papers we will unravel the history of one of the most important, aggresive and influent RaaS also known as **Conti**. This group even if (technically) non active anymore left behind both shadows and lights, it's history is the perfect example on how RaaS behave, how they are organized and, more importantly, who is behind online monikers.

We will cover from the really start to the present including everything in the middle, knowing Conti group history is valuable (probably even required) to understand the ransomware phenomenology in the past, present and future.

THE ORIGIN

DARK ROOT

[...] But in case of your refusal to cooperate we will run a great damage to your business, you will lose ten times more in courts due to violation of the laws on the GDPR and yout partner's data leak. We'll inform your employes partners and government about this leak, your data will be pubblished on public blogs and salty competitors. We will inform media about cyberattack to your company and backdoor access to your company data will be sold to other hacker groups and it wil be the last day of your business. We don't want to do that for sure and we will not do that if we negotiate successfully. We are waiting for you in that chat, think about your future and your families. Thank you. Bye

Suncrypt vocal ransome note

Ransom Cartel (named like this by Jon DiMaggio), a pioneer in the RaaS landscap, emerged in 2020 as breeding ground for several now-prominent and well known RaaS. Its members were affiliated with five different groups : **Viking Spider, Suncrypt, Twister Spider, Lockbit Gang** and, our primary focus, **Wizard Spider**.

Prior to delving into Wizard Spider, let's briefly examine Ransom Cartel and the advantages it offered its member groups. Established in June 2020 by **Twister Spider** (active since 2018), the collective was predominantly composed of Russian-speaking individuals from Eastern Europe. **A notable innovation was the introduction of the "no-CIS" rule explicitly in ransomware codes**, preventing encryption of systems located in Commonwealth of Independent States countries.

Analysts discovered that the four groups collaborated to infiltrate networks, culminating in data encryption and exfiltration. These stolen data were then transferred to **Twister Spider**, who managed the data leak site (DLS) and negotiations. Each DLS post included an attribution to the specific group responsible for the breach.

Furthemore the discovery of **Command&Control servers belonging to different groups within the same IP range/address** revealed strong ties between members. This evidences solidified their shared techniques and information exchange in operational and extorsion processes (eg:/ use of DDoS, VM for evasion, double extorsion). While the specific profit share mechanisms and affiliate programs are still unclear, it was evidnt the exceptional efficency and sophistication

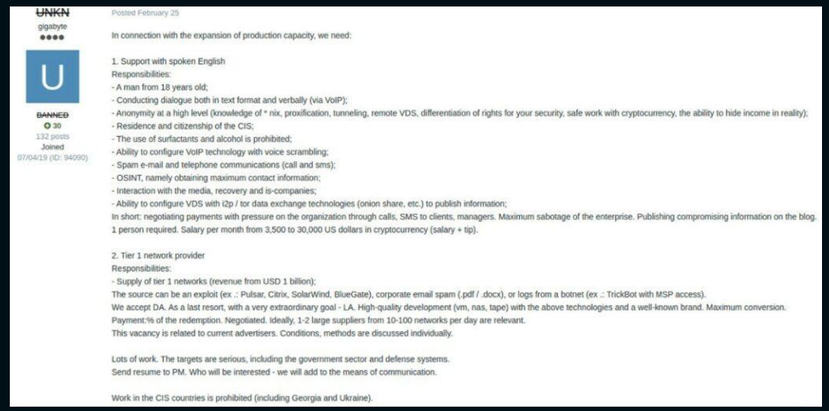
The cartel had undoubtedly dueled the amazing increas in ransomware attack witnessed in 2021 and 2022 as well [1]. The red thread followed by the whole groups was aiming to reputational damage pushing to the limits victims.

Maze explicitly confirmed to BleepingComputer they cooperated with LockBit and "another group will emerge on our website [...]" in June 2020. **November 2020 Twisted Spider retired Maze** trying to masquerade their ties with the other 3 groups, after a year of operations with this specific strain, transition to **Egregor** (started in September 2020). Togheter these operations allowed the group to extort (at least) $75 MLN from victims.

Suncrypt have been interviewed by BleepingComputer as well saying they have joined the cartel because *"They just can't handle all the available field of operations. Our main specialization is ransomware attacks"*. Analysts have speculated that, in the first year of the ransomware era, actors capabilities were highly specialized making collaboration a minimum requirements to monetize their illecit activities. In september 2020 Suncrypt shutdown operations leaving the Cartel after re-emerging with standalone operations.

But who's behind the original *"Ransom Cartel"* concept? Apparently **REvil!** After a series of failures in 2020 the REvil group started to hire new individuals in the underground including **operators** and **negotiators**.

The two groups have huge similarities in ransom notes, ransomware code/techniques and Big Game Hunting strategy. This subset of threat actors has been called **PINCHY SPIDER**....but that's a different story! Is not clear if Twisted Spider is related to REvil directly but the majority of attacks made by the cartel and the post-exploitation activities are close to REvil's ones.



~~UNKN~~
gigabyte
●●●●

U

BANNED
30
132 posts
Joined
07/04/19 (ID: 94090)

Posted February 25

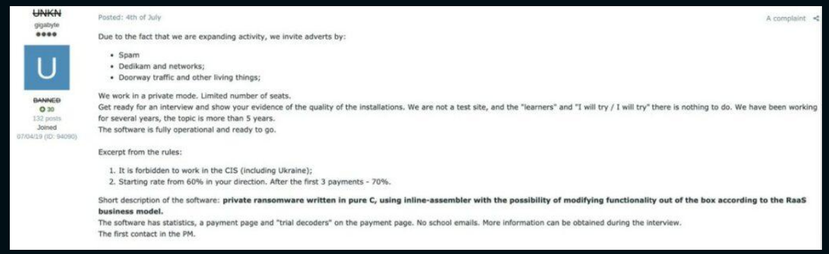
In connection with the expansion of production capacity, we need:

1. Support with spoken English
Responsibilities:
- A man from 18 years old;
- Conducting dialogue both in text format and verbally (via VoIP);
- Anonymity at a high level (knowledge of * nix, proxification, tunneling, remote VDS, differentiation of rights for your security, safe work with cryptocurrency, the ability to hide income in reality);
- Residence and citizenship of the CIS;
- The use of surfactants and alcohol is prohibited;
- Ability to configure VoIP technology with voice scrambling;
- Spam e-mail and telephone communications (call and sms);
- OSINT, namely obtaining maximum contact information;
- Interaction with the media, recovery and is-companies;
- Ability to configure VDS with i2p / tor data exchange technologies (onion share, etc.) to publish information;
In short: negotiating payments with pressure on the organization through calls, SMS to clients, managers. Maximum sabotage of the enterprise. Publishing compromising information on the blog.
1 person required. Salary per month from 3,500 to 30,000 US dollars in cryptocurrency (salary + tip).

2. Tier 1 network provider
Responsibilities:
- Supply of tier 1 networks (revenue from USD 1 billion);
The source can be an exploit (ex .: Pulsar, Citrix, SolarWind, BlueGate), corporate email spam (.pdf / .docx), or logs from a botnet (ex .: TrickBot with MSP access).
We accept DA. As a last resort, with a very extraordinary goal - LA. High-quality development (vm, nas, tape) with the above technologies and a well-known brand. Maximum conversion.
Payment:% of the redemption. Negotiated. Ideally, 1-2 large suppliers from 10-100 networks per day are relevant.
This vacancy is related to current advertisers. Conditions, methods are discussed individually.

Lots of work. The targets are serious, including the government sector and defense systems.
Send resume to PM. Who will be interested - we will add to the means of communication.

Work in the CIS countries is prohibited (including Georgia and Ukraine).



~~UNKN~~
gigabyte
●●●●

U

BANNED
30
132 posts
Joined
07/04/19 (ID: 94090)

Posted: 4th of July

A complaint

Due to the fact that we are expanding activity, we invite adverts by:

- Spam
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: **private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality out of the box according to the RaaS business model.**
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact in the PM.

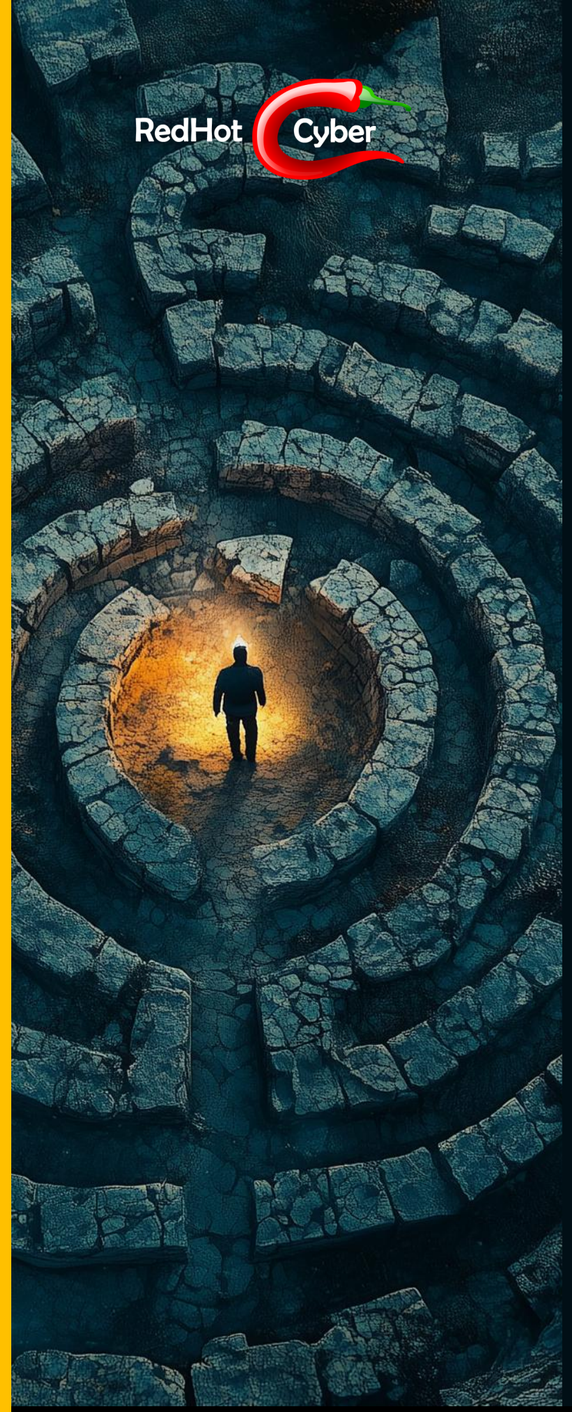
wisted Spider creation last for approximately a year, after the retirement of Maze operations the group slowly degraded. **Pinpointing the exact timeline is challenging, but it's likely that Ransom Cartel's shutdown occurred in early 2021.**The underlying motivations remain obscure and, understandably, undisclosed to the public. Investigations have yielded partial results, revealing the members' long-term aspirations for the cartel. While a large-scale operation might initially intimidate victims, it can also simplify law enforcement's task. **Ransom Cartel was not only large but also highly visible, drawing significant attention** and some members where skeptical about the future of the collective. **Collaboration within Ransom Cartel was often inconsistent and poorly defined**, presenting a significant obstacle that ultimately led to the dissolution of the four groups.

Regarding the end of the *"Ransom Cartel"* the result have been incredibile, amazing and evolution of the RaaS landascape. Every group within the collective had (and some still have!) operated with their own RaaS : **Lockbit Gang founded the (still) well known LockBit RaaS**, Viking Spider continued with **Ragnar Locker** but in October 20 2023 have been affected in a chain of arrests, The last tracks of **Suncrypt** reside in 2022 making them a de-facto veterans in the field and **Wizard Spider** founded the protagonist of our story: **Conti**.

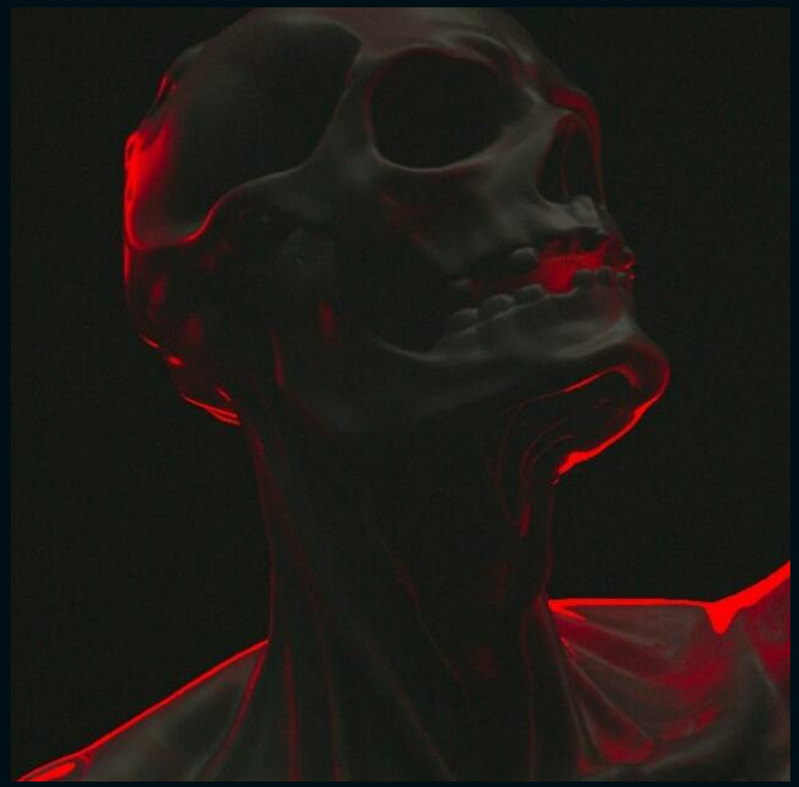
The Ransomware 2.0 Era officially started!

WIZARD SPIDER

НЕ УЧИ́ УЧЁНОГО

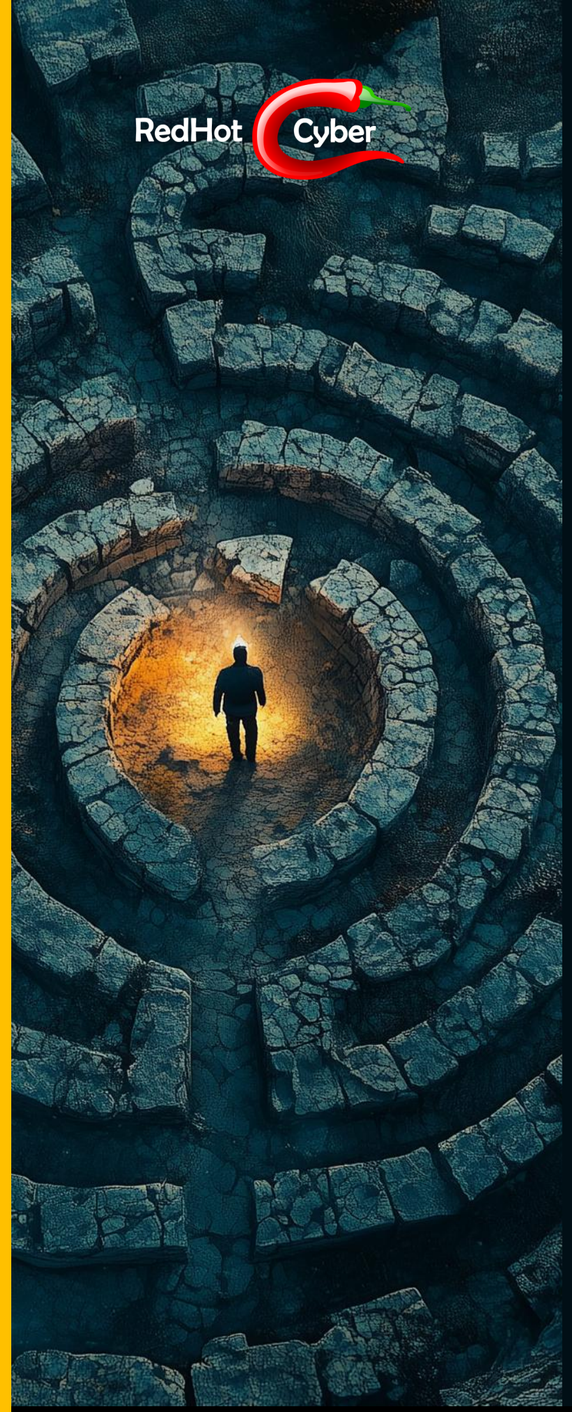


The Ransom Cartel was surely prepared on offensive operation but there was only one group which skills have been far superior by others, **Wizard Spider**. This threath proved sophisticated TTPs and a vast armory. Identified in 2018 using **Ryuk Ransomware** in the wild and joined the Cartel collective in **August 2020** raising the bar significantly.



The group is interesting, they operated in different **teams** enabling different operations concurrently developing their own unique tools including:

- **Sidoh/Ryuk Stealer:** Malware written in C++, after parsing the CLI arguments the stealer start to enumerate the drives within victim host. After this first enumeration **Sidoh** harvest the stored ARP entries attempting to mount the SMB share and subsequently enumerate them avoiding standard Windows paths and DLL. Extensions string have been found inside the different samples analyzed containing **.exe, .sqlite, .msi, .ps1** and even Ryuk Ransomware one. To speed up the exfiltration process the malware skip those files highlighting the **strong tie between Sidoh and Ryuk Ransomware post-exploitation**. The focus was about Word and Excel Documents with proper parsing before exfiltration, interestingly some samples stored keywords that, if presented in filename or contents, trigger the immediate file upload. Some of these words were **NATO, FBI, NSA, tank, military, government** and **securityN-CSR10-SBEDGAR** (EDGAR is a text-search for all SEC documents since 2021) indicating the group was interested in political and governemnt assets as well. The exfiltration occured through FTP.



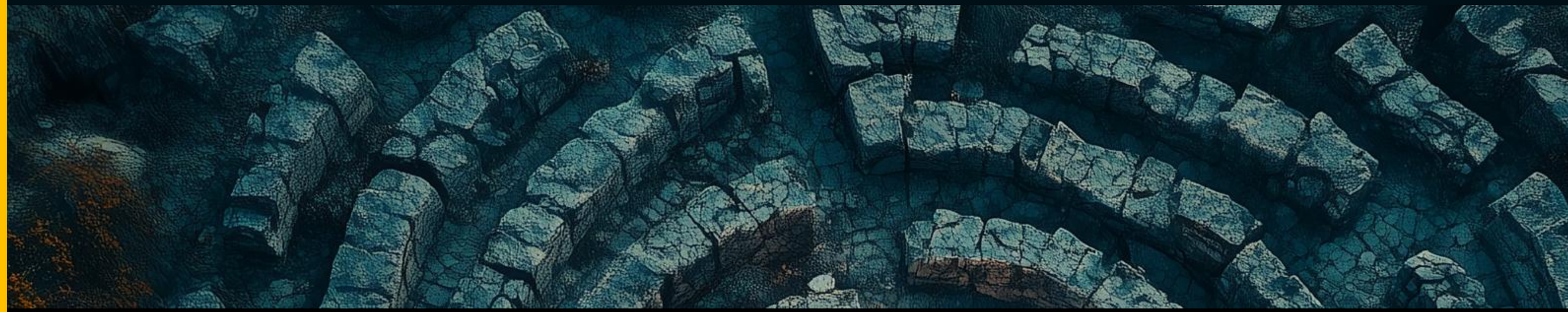
- **Bazar Backdoor:** Used mainly in **TrickBot** operations and delivered via Phishing through Sendgrid email addresses. When Bazar loader is activated (fileless) it triggers a DNS resolution via Emercoin using the domain word *"bazar"* which can be used solely by this specific decentralized service. Connecting on a specific bazar domain (*bestgame.bazar*, *thegame.bazar*, ...) a XOR **Bazar Backdoor** payload is saved into the victim host anf filelessly inject into **svchost** process. Different samples highlights different process injection techniques but often Process Hollowing or Process Doppelganging were preffered. A scheduled task is also configured permitting persistence after system shutdown.
- **TrickBot Trojan:** Probably one of the most sharp and advanced tool creted by Wizard Spider, a modular Trojan born to retrieve banking credentials. With a pretext to ***trick*** the user to click on an image stored in different type of documents, make possible the download of a malign payload decrypted during runtime and injected with different evasion procedures. More than 61 variations have been found in the wild each of them with different purpose like browser data steal, credential theft, criptomining and ransomware as well (especially with **Ryuk Ransomware campaigns**). This tools comes with many hat from man-in-the-middle attacks in user browser to traditional persistence on C2 servers, all of that simplified through the use of modules (usually DLL) which can be loaded into Trickbot making it an highly modular weapon.
- **Anchor:** Another backdoor tool but this time with a focus on PoS devices. Often chained with TrickBot as second stage malware, was designed specifically for Point Of Sales system and sequentially data theft through DNS tunneling.
- **Ryuk Ransomware & Conti Ransomware:** The crown jewels, the whole toolset is designed to coordinate ransomware operations. The two ransomware strain are derived from **Hermes Ransomware** used by North Korean APT to masquarade their operations. These malware are extremely fast in encryption process, especially Conti which run with 32 simultaneus CPU threads. Wizard Spider don't just aim to encryption but also on making recovery as hard as possible shrimming shadow copies, with the combination of evasion and privilege escalation embedded in the code make these 2 ransomware highly efficient. Wizard Spider created other 2 ransomware strains called **MegaCortex** and **GogaLocker** but retired shortly after their use in the wild.

Should be clear enough the huge flexibility and different operations conducted by this team, they are not just smart attacker but professinal developers as well. Wizard Spider performed multiple operations at once highlighting numerous individuals behind the group and extremelysharp skills.

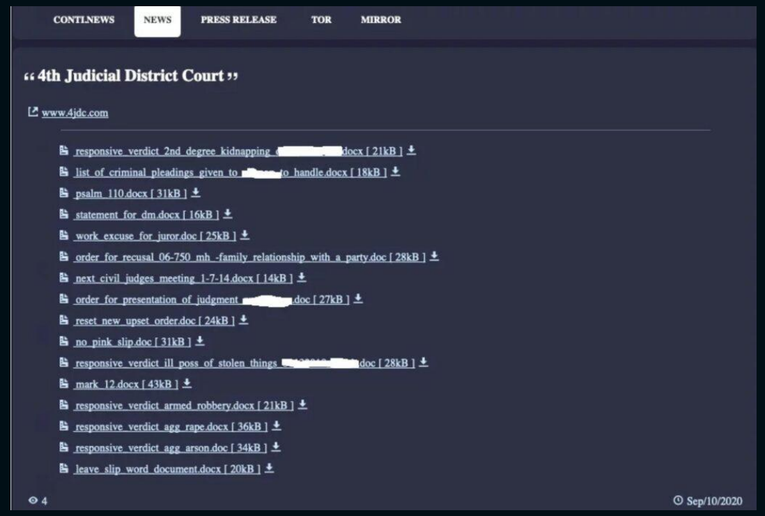
Conti operations would become a new standalone product after leaving the Ransom Cartel and it would dominate the whole environment expanding the Wizard Spider web

CONTI RANSOMWARE

BORN TO LOCK!



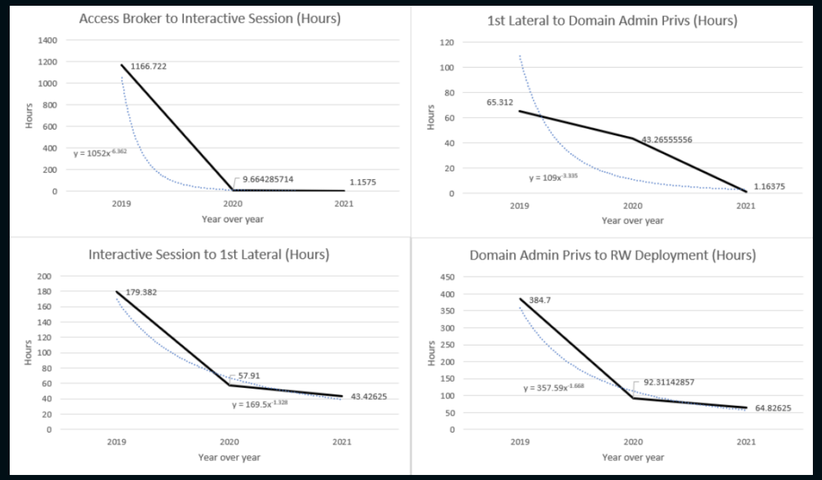
In August 2020 the official DLS of Conti officialy opens to the public.



The vintage look have been quickly changed with an aestethic and professional version in December 2020 presenting **Conti as Ransomware-as-a-service**. From the grand opening of their DLS to the end of 2020 Conti pubblished (approx) 175 victims and was just the start.

The year 2021 has been the golden age of this RaaS with consistent operations over west companies and critical infrastructure. On their prime they have been the second highest RaaS in terms of market share with just REvil above them.

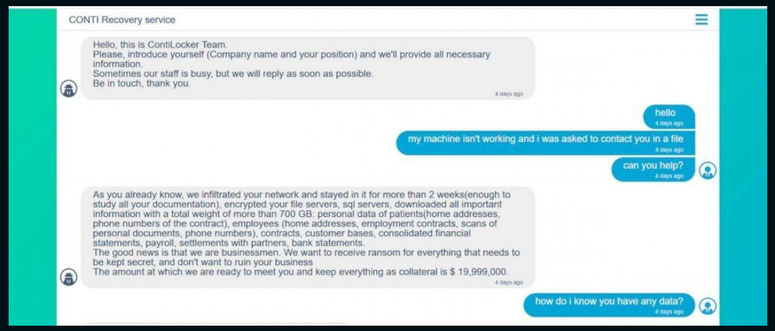
In april 2021 a threat actor was able to encrypt victim network from an inital stage payload in just 2 days and 11 hours. Analysts found wide options of C2, phishing addresses, initial access techniques and malware used in their operations underlying the rang of Conti’s Ransomware Operators TTPs pool which, as result, dropped the average time to damage a victim : from 2 months to 3/4 days.



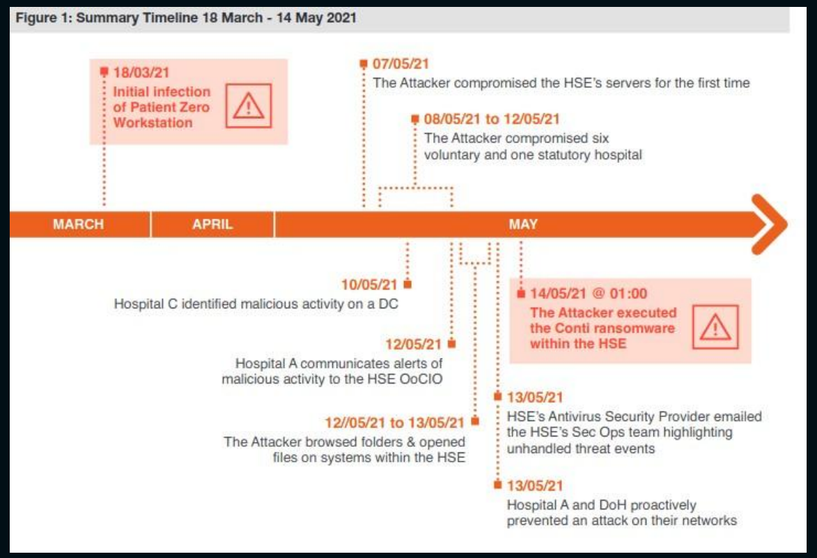
But Conti isn't that famous for their skills, instead their reckless victim selection. Since the 26th October 2020, KrebsonSecurity followed a tip from a *"reliable resources"* that warned the ransomware group behind Ryuk (Wizard Spider) was building a reputation on the Russian underground forums for targetting and damaging healthcare digital assets. The threat became reality shortly after reaching the peak with the **Health Service Executive (HSE)** attack.

HSE is an healthcare system in Ireland public founded founded at the start of 2005. The 14th May 2021 (in the middle of Covid pandemic) Ireland received the biggest cyberattack in the whole country history impacting hospitals appointment systems, COVID testing referral, vaccine registration portal and shutdown of HSE national and local networks.

A full scale disruption made by the Conti ransomware file encryption with several month of recovery as price for the healthcare provider that slowed down the whole country hospitals and medical centers. Encryption was not the only problem Ireland has to face but also stolen data used for double extorsion into the hands of Conti staff.



Conti decided the ransom, in the negiation chat, and set it at $20 MLN with additional samples from the 700GB of stolen data : **27 sensitive files belonging to 12 different individuals.** The total cost of attack including recovery and legal procedure costed about $100 MLN. **HSE** made a public statement highlighting the threat used a 0-day vulnerability and *"there was no experience in how to respond to the attack"* but, during the incident response processes, professionals found tons of outdate workstations (Windows 7 which is not receiving security patches from 2020) around HSE networks that surely helped attackers in the attack procedure.



HSE attack timeline

"The opportunity for error is massive. I mean things like people getting the wrong blood transfusions, samples being sent under the wrong patient's name [...] I reviewed one patient and needed to make a decision about whether to change medication. He didn't know what he was on, and I couldn't verify that information"

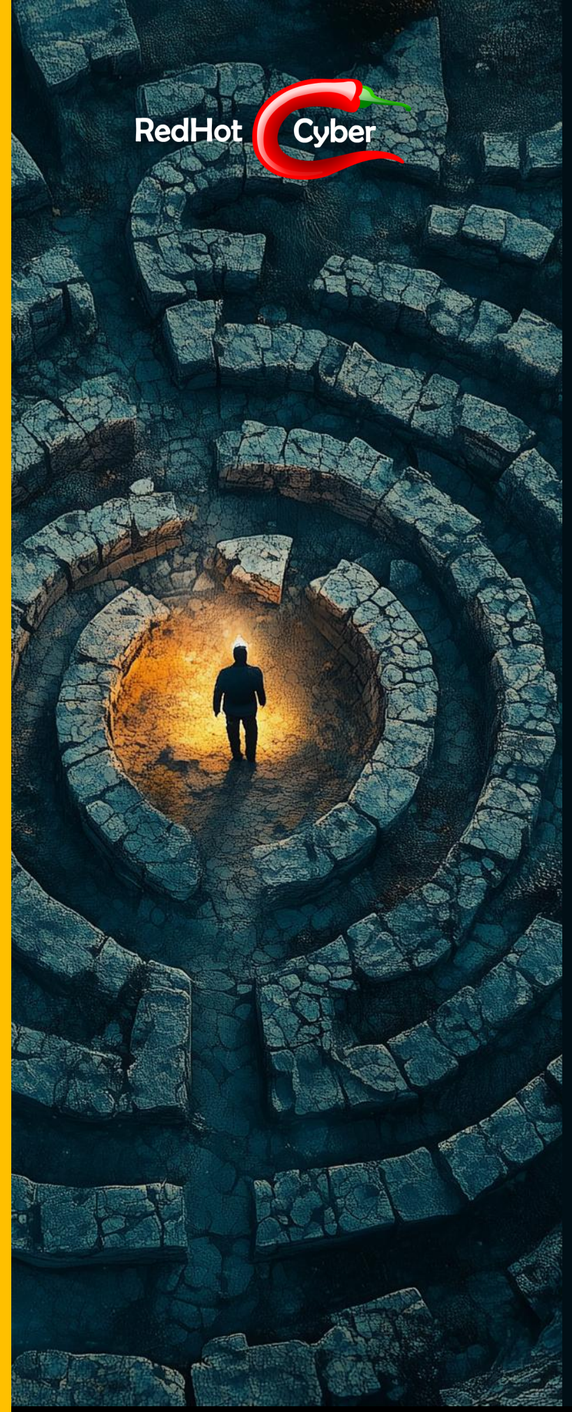
Medic in Dublin after the HSE shutdown

Conti decided to give the decryptor for free (which was slow and *"bad"* standing with security professionals words) while still threating to release the data collected, Irish government decided to refuse the payment meaning all health data have been sold for the RaaS profit.

Was this an isolated attack to the healthcare sector? No! The Irish NCSC (National Cyber Security Center) notified attack attempts to the Ireland Department of Health. NCSC forces isolated the systems and found **Cobalt Strike** (widely used by the group, we would cover this in the next episode) payloads and digital artifacts similar to the ones retrieved in the **HSE** network but we cannot state at 100% Conti was behind this (attempt of) attack as well.

The core of the Conti attack was not just disruption of a public service but ruining the reputation of HSE, legal actions and dense cost between fines and cybersecurity renovations have been made. We cannot state how much money they have made selling the healthcare data (actually, we are not aware if the data have been sold in first instance) but what we can conclude is that HSE image has been deeply ruined while Conti ones stands strong, an "amateur" offensive group brought Ireland hospitals to their knees with a single malware.

NO REST FOR THE WICKED



In 2021 Conti outranked the other groups in the scene in terms of money making. Their formula worked, Conti RaaS operation alone is still the best in terms of (documented) profit. In 2021 their extornions worked for $180 MLN since the creation of the RaaS, which was the double of DarkMatter responsible of the Colonial Pipe Ransomware Attack which changed the vision of cybersecurity (at least) in US.

The United State Department of Justice offered help to Ireland during the HSE meltdown, apparently they took the opportunity to get in touch (indirectly) with the threath. USA pubblished 2 documents regarding Conti and their operations the Joint Cybersecurity Advisory : Conti Ransomware (September 2021) and an FBI Flash (May 2021). The latter is a description of the threat with IoC and TTPs while the former state the FBI locate 16 different attacks made by the RaaS affecting critical infrastructure.

Within this 16 attacks (globaly Conti collected 400 victims in just a year, 290 only in the USA) we have not just healtcare but also **911 dispatcher centers** and with the higher ransom being of $25 MLN. Enough is enough, from now on Conti is officially an enemy of the US goverment.

For instance in August 2021 Conti successfully attacked Nokia subsidiary (SAC wireless) headquarters in Chicago, in April 2021 Broward County Public School, Florida (demanding $40 MLN) and between Septmeber and October 2021 the compnay JVC Kenwood (1.7 TB data stolen plus $7 MLN ransom).

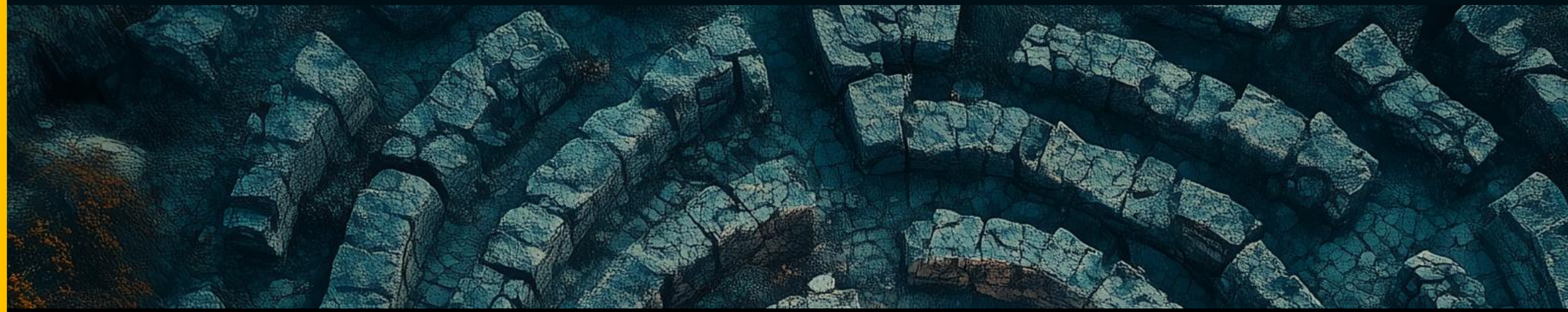
.

Regardless of Conti, Ryuk and **Trickbot** (which became a malware-as-a-service product) operations didn't stop and the group is looking more like a company than a simple criminal gang. They are organized, they have dense internal communication and huge payrolls. In particular Trickbot is becoming wide popular between threat actors outside Conti and Wizard Spider with persistence maintenance and features addition (especially evasion techniques).

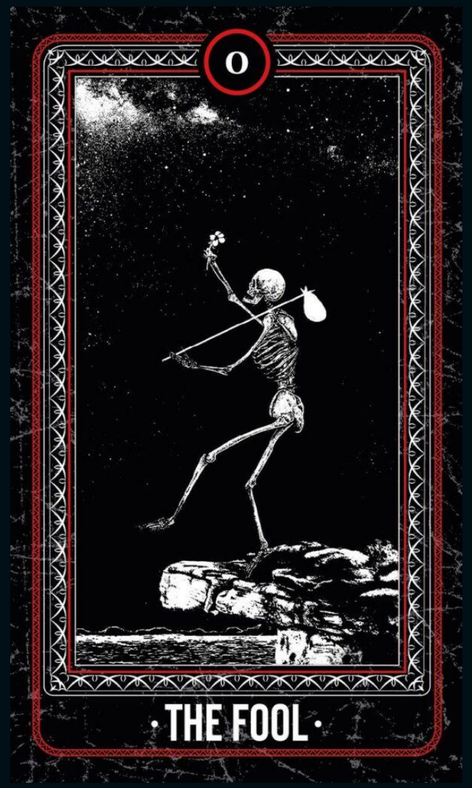
Every interesting story needs some obstacles in the protagonist way and The Wizard Spider empire is near to encounter a lot of them. In the next episode of this small saga we would cover the first arrests, leaks and insight that affected Conti and it's enviroment. We have talked about 2019,2020 and 2021 but a lot more needs to be written. In Febbruary 2022 the world has to deal with a new war in east europe, Russia-Ukraine ware, and this event would uncover the whole Conti background.

THE FOOL

TRICK OR TREAT



Mid-2021, **Conti** is dominating the headlines with consistent attacks and gaining ransoms from victims. The **RaaS operation** has been a big deal in the ecosystem, attracting the attention of everyone involved, including victims, affiliates, and law enforcement corps. But that's just a piece of the whole puzzle.

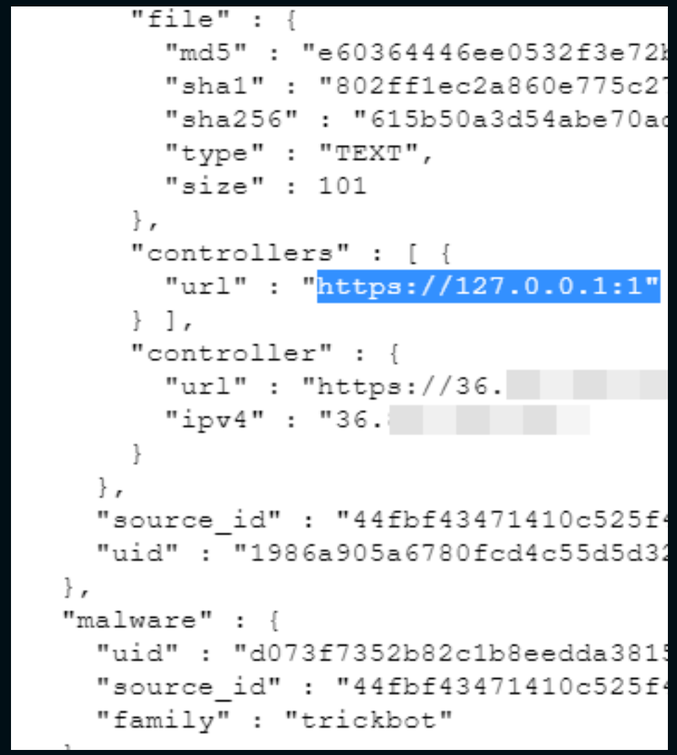


Trickbot operations never stopped and actually continue to evolve. As written in the previous article, Trickbot became a popular tool even outside Conti operations thanks to the transition to a **Malware-as-a-Service (MaaS) model**. With a monthly fee, anyone could use the infamous modular Trojan, which received constant development (in this CyberInt article you can find some of the modules and deliver methods).

The US federal government needed to contrast ransomware and digital attacks, which received a huge boost thanks to this new underground environment that exploded after **Ransom Cartel.** A small step back to 2020, US elections are planned to take place on November 20th. When we described **Wizard Spider/Conti Toolset** in the previous article, we also covered the capabilities of **Ryuk Stealer**. Some of the features included the automatic exfiltration of files that contained specific keywords (names and contents) highly related to Western government assets.

All of this highlighted how the group behind Ryuk, TrickBot, and Conti RaaS had **particular political interests beyond mere business or economic purposes.** Obviously the origin of attacks has been described as **Russian nature**. The United States was concerned about potential influence or sabotage regarding the upcoming elections, which motivated law enforcement to launch **offensive operations against the TrickBot botnet**.

The US Cyber Command (never confirmed by the agency itself), headed by NSA director Paul M. Nakasone, made a disruption operation on the whole TrickBot botnet infrastructure in 2020. On September the botnet was flooded by intentional bogus configuration files which setted the communication with the C2 server to the localhost IP address.



Snippet of the configuration files (KrebOnSecurity)

The new configuration broke Trojan's communications effectively stopping part of their operation especially Ransomware attacks. Moreover, **Microsoft** took the turn with a huge **series of legal action in order to shutdown TrickBot machines completely**. In less than 2 weeks the company was able to shutdown 120 out of 128 servers (source Microsoft).

A big hit on TrickBot but not for long…actually shorter than expected. Somehow the *"evil" developers* embedded a fallback mechanism with the objective to recover broken communication channels with TrickBot agents in case the infrastructure was modified. **Resilience sounded like the biggest priority for the TrickBot group.** The operation is not a simple hole in the water just because the quick redemption and adaptability of the threat on the technical side, **it has been a message to everyone showing the position of US government against digital attacks and criminal environments with a proactive approach.**

The directive of **Paul M. Nakasone** under the Trump administration was clear: *"persistent engagement"*, *"defending forward"* and *"hunting forward"* rather than passive prevention and mitigation.

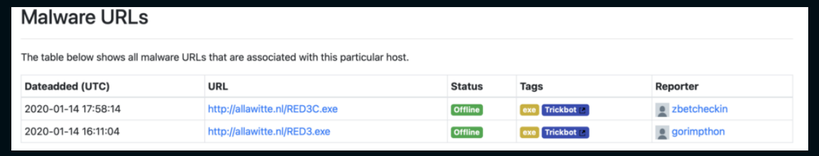
There is no proof of TrickBot used specifically on targets with election sabotage purpose but Ransomware attacks using the Trojan continued even after Biden election with the same pace.

Paul Miki Nakasone (Japanese: 仲宗根ミキ *Nakasone Miki*, born November 19, 1963)[2]: 2 [3][4] is a retired four-star general in the United States Army who served as the commander of United States Cyber Command.

The warrant arrest for TrickBot developers and maintainers was issued in **August 2020**. We had to wait until the start of 2021 before having some of those individuals handcuffed, in Febbruary ***"Max"*** **is the first member of TrickBot that had to face the blinded goddess**.

Ladies and gentelmen, ***Alla Witte*****, 55 years old, in art *"Max"*.**

Before covering the charges she had to faces let's make a small note on how Alla Witte has been (presumably) discovered. First of all take a look at the URL **haus** page about ***"Max"*** personal website. Note the ***"RED"*** keyword.



Malware URLs

The table below shows all malware URLs that are associated with this particular host.

Dateadded (UTC)	URL	Status	Tags	Reporter
2020-01-14 17:58:14	http://allawitte.nl/RED3C.exe	Offline	exe Trickbot	zbetcheckin
2020-01-14 16:11:04	http://allawitte.nl/RED3.exe	Offline	exe Trickbot	gorimpthon

This is not the first time Witte mixed personal life with her underground activities, in December 2019, she infected on of her own devices with TrickBot stealing the data and store everything inside on the C2 server (source Hold Security). **In addition, on social media profiles, Witte cite *"Max"* as someone really close to her**. In short, Operational Security (OPSEC) was not the sharpest skill of Alla Witte creating gaps usefull to law enforcement that were trying to de-anonimize *"Max"*.

She was living in **Suriname** working as web developer freelancer, **the arrest took place in Miami Febbruary 6 2021.** The count on her included :

1. Computer Fraud and (aggravated) Identity Theft
2. TrickBot Development, Administration and Maintenance
3. Deployment of TrickBot
4. Wire and Bank Fraud
5. Money Laundering

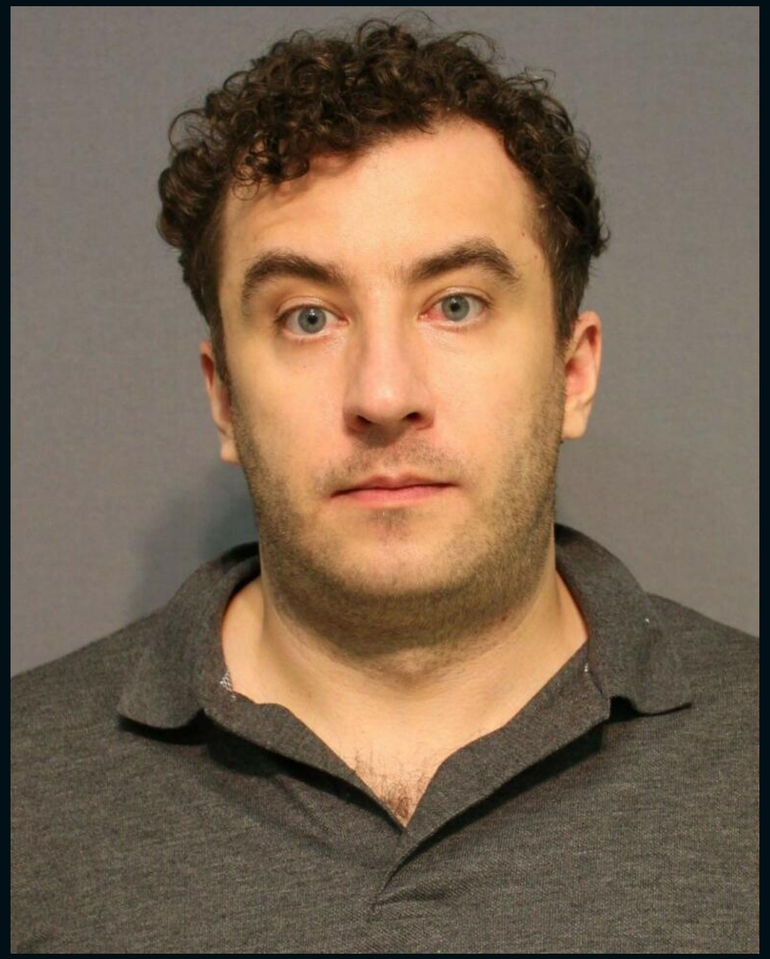
You can find the whole Arrest Warrant on the official USA Justice department website, interesting enough is the reputation within the group. Most of members knew her gender and real name reffering to her like a son would do with his mother.

She had prestige for her technical skills, TrickBot members were really happy to know Witte was in charge of the development process.

CC9	He's capable of everything.
CC9	Such a person is needed.
	I'm afraid that he can tell the firm to go hell, or ask for more money.
	Well that's something for the leadership to decide.
CC9	His assignment is the usual kind.
CC9	There's nothing strange in it.
CC9	:)
	So he's going to develop programs?
CC9	Well, yeah.
	Well, in that case, that's fucking great.

The investigations uncovered the origin of TrickBot reside in **Dyre bank trojan**, in 2023 Alla Witte was senteced to 2 years and 8 months of prison time.

The list was still long and Witte was just the tip of the iceberg. The next individual was **Vladimir Dunaev a.k.a *"FFX"* (38 years old).** Vladimir was resident in **Russia (Yakutsk region)**, in mid-October 2021 he was arrested in **South Korea** (no details on why he moved have been released) and extradited to US. He will face a process with a maximum of 60 years in prison.



Vladimir Dunaev

BleepingComputer, at the time, released a table from the indictment paper showing the activities of Dunaev within the TrickBot group

Dates	Code description
July 2016 - time of the arrest	modifying Firefox web browser
December 2016 - time of the arrest	Machine Query that lets TrickBot determine the description, manufacturer, name, product, serial number, version, and content of the root file directory of an infected machine
August 2016 - December 2018	Code that grabs and saves from the web browser its name, ID, type, configuration files, cookies, history, local storage, Flash Local Shared Objects/LSO (Flash cookies)
October 2016 - time of the arrest	Code that searches for, imports, and loads files in the web browser's 'profile' folders; these contain cookies, storage, history, Flash LSO cookies. It also connects to the browser databases to make queries and to modify them
July 2016 - time of the arrest	An executable app/utility to launch and manage a web browser
July 2016 - time of the arrest	Code that collects and modifies data entries in Google Chrome LevelDB database, browsing history included

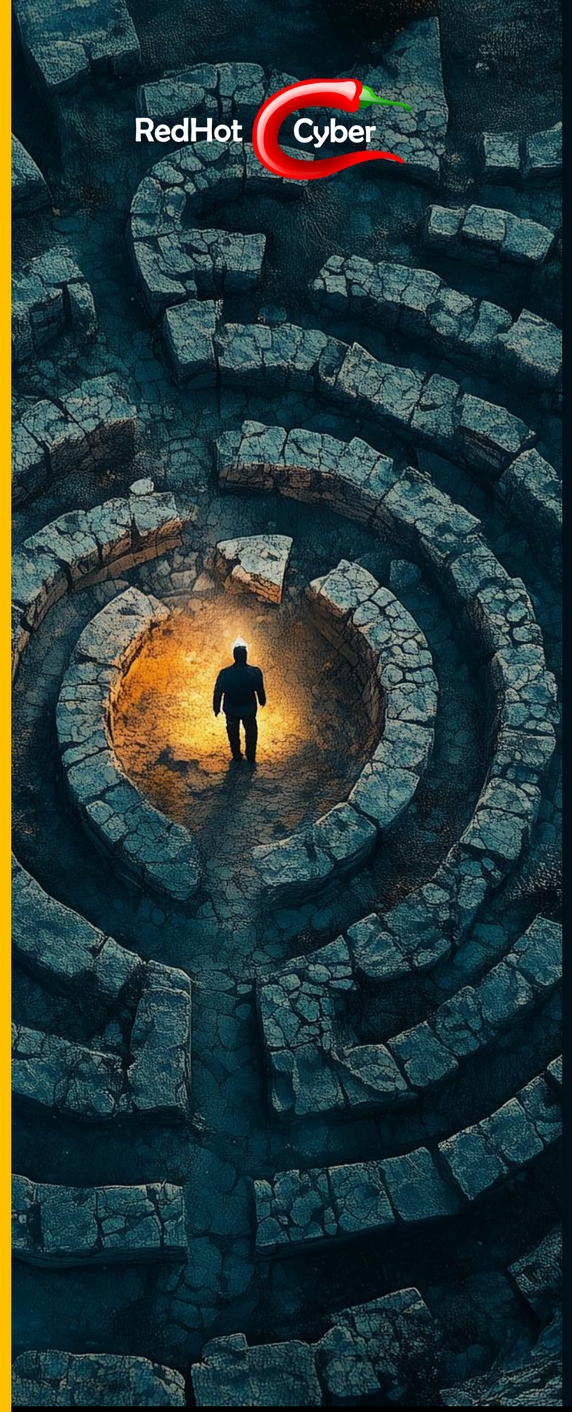
FFX pleaded guilty in 2023 and in March 20th 2024 was sentenced to 5 years and 3 months in prison.

TrickBot developers have been under high pressure with this 2 arrests. US government officials stated to have identified other individuals responsible for deployment, development or money laundering activities related to the modular Trojan group.

TrickBot operations didn't stop but is clear the battleground has changed, **Conti and major western countries governments would prove themselves fighting head to head!**

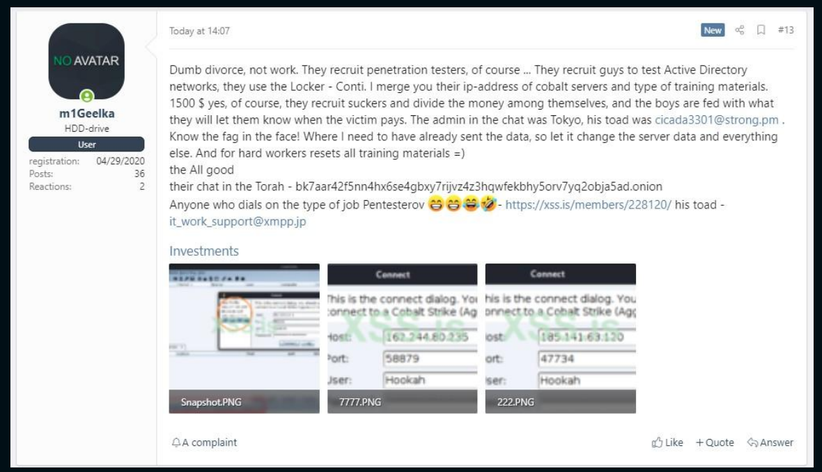
THE HERMIT

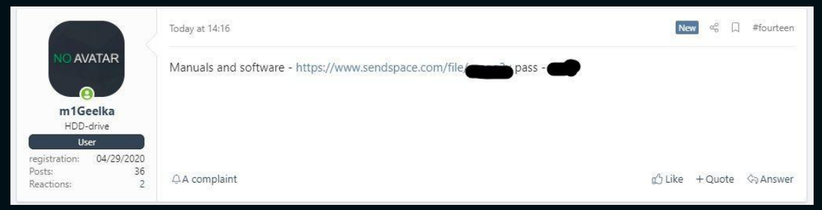
SNATCH & SNITCHES



In August 2021 the ransomware scene transformed from stray cat to urban panther : **LockBit 2.0** was out, **money** flow was bigger than ever, **Colonial Pipeline** attack and **Initial Access Brokers** market became more popular. The ecosystem is now mature with a spice of *"professionalism"* but what happen when *"dark-companies"* lack of transparency and honesty?

Well we should analyzed what happened with *XSS* user **m1Geelka**





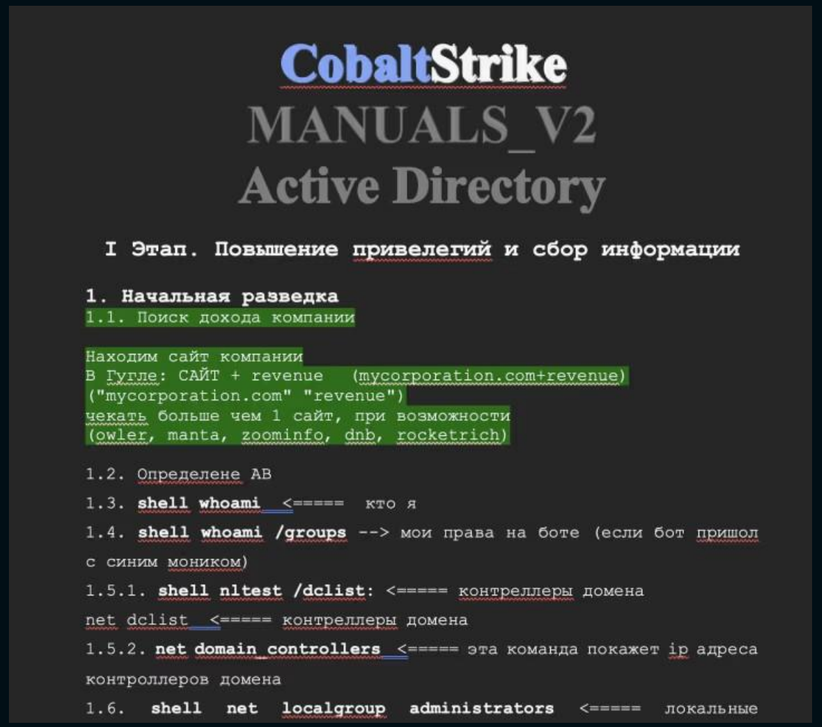
This (really upset) **ex-Conti affiliate** leaked the manuals provided to attackers in order to exfiltrate data and deploy their ransomware. The guides were about **Active Directory** environment, enumeration and common attacks abusing missconfiguration or knwon vulnerabilities (*PrintNightmare*, *EternalBlue* and *ZeroLogon*).

But let's go with a bit of order, why this person was angry? His blogpost is pretty clear the motivation was minor payments based solely on ***"what they [Conti] will let them know the victim pays".*** The affiliate program was 70/30, **70% to the attackers and 30% to the RaaS**, the point is the difference on Conti claim and the real ransom amounts. Unluckly nothing critical has been leaked, no source code, no secrete chat and no identities disclosed. *Wait a lil' bit for that)).*

Some specific used by affiliates have been uncovered : strong use of **Cobalt Strike**, powershell scripts and procedure to exfiltrate data (install RDP agents and upload everything on **MEGA/FileZilla upload**). More technical figures would stand up for moment with surprise expression on their face, **the procedure described is simple, really basic.**

Somehow the **Conti** staff wanted to create documentation for novice and non-expert attackers, probably for 2 reasons : ***easy to fool*** and ***"quantity over quality"*** with standardise attacks. If the words of the affiliate were true it means the total payment for an attack was **$2100**, even without knowing the target is pretty unrealistic given the average ransom were **+$100K.** We can believe the affiliate words with wide range of confidence.

Like legal companies out there do, Conti was taking advantage of some employees just for profit. The guide contained some IP addresses and some minor IOCs that some major vendor added to their solutions and Conti threat profile.



In case you want to get in touch with the leak contents, ForbiddenProgrammer made a public GitHub with everything you need.

FOUR OF SWORDS

OPERATIONAL BRIEFING

Until now we covered a lot regarding Conti in terms of evolution and timeline, before continuing our journey is necessary we stop and mentions some attacks made by Conti RaaS in 2021. We already talk about the **Irish HSE ransomware attack** so let's break down other meaningfull operations.

- **London Graff Jewellers**: At the end of October Conti have successfully exfiltrated and encrypted data of Graff Jewellers, a well known UK brand. Conti posted **61,000 files** on their DLS claiming those have been just the 1% of total exfiltrated files, the files contained billing and shipment information of VIP like David Beckham, Donald Trump and **Arab Royal Families members**. Graff had to shut down their networks and during forensincs investigation they believed **11,000** costumers records have been stolen. Conti requested tens of millions as ransom. The **11th of November** Conti decided to post an update regarding London Graff attack, **claiming they will permanently delete files related to Arab, EAE and Qatar families while releasing data regarding** ***"US-UK-EU Neo-liberal plutocracy"***. Interesting statement, the ***"soul"*** of the group drove them to damage western countries as much as possible on every attack they perform. They also shoutout the **Daily Mail** for the article which made understood the RaaS what type of data have been stolen, sticking with Conti words they didn't analysed exfiltrated contents properly.

"ANNOUNCEMENT"

Hello!

This is an important privacy and confidentiality announcement from the Conti Team.

As some of you may know, two weeks ago, we uploaded data from a company Graff on our blog.

This publishing, however, lead to an in-depth investigation of the sample files by the Daily Mail. Daily Mail is a UK paper (not American Twitter 2-digit-IQ "journalism"), th erefore, their analysis was done with the highest standards of reporting and uncover ed things that we have unfortunately missed.

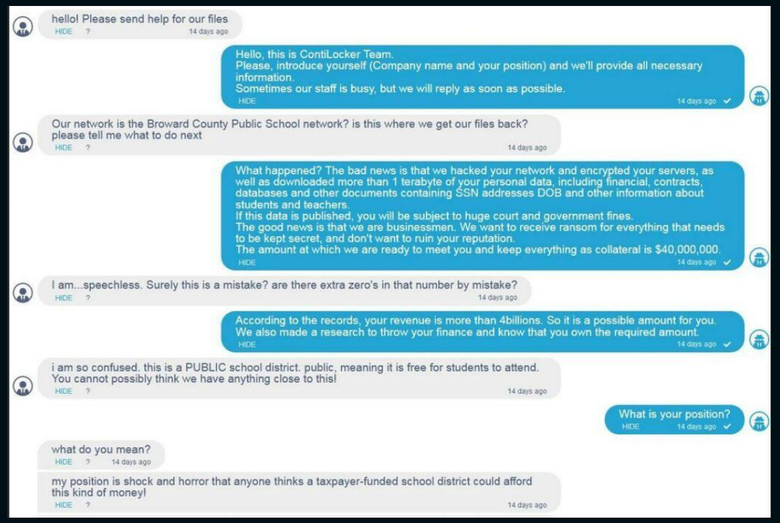
We found out that our sample data was not properly reviewed before being uploade d to the blog.

https://www[.]dailymail[.]co[.]uk/news/article-10148265/Massive-cyber-heist-rocks-high-society-jeweller-Graff.html#comments
As a response to the investigation by Daily Mail, we will delete all Graff's information from the blog, and will clarify our privacy and confidentiality policy.
1. Conti guarantees that any information pertaining to members of Saudi Arabia, UAE, and Qatar families will be deleted without any exposure and review. Our Team apologizes to His Royal Highness Prince Mohammed bin Salman and any other members of the Royal Families whose names were mentioned in the publication for any inconvenience.
2. Conti guarantees that besides the 1% files shared on our blog, there were no instances of exposure or sharing of the Graff Diamonds data. In other words, none of this information was sold on auctions or offered as samples, or revealed in any other capacity to any third party.
3. Conti guarantees to implement a more rigid data review process for any future operations.
We want to thank the Daily Mail for investigative coverage and great journalist work, especially regarding the US and UK individuals in the Graff files. As long as the truth is overt, it prevails! As for the Graff Diamond case, we will conduct our own review that will focus exclusively on US and EU citizens.
Our goal is to publish as much Graff's information a possible regarding the financial declarations made by the US-UK-EU Neo-liberal plutocracy, which engages in obnoxiously expensive purchases when their nations are crumbling under the economic crisis, unemployment, and COVID. While the Nations of America and Europe are chocked by lockdowns and totalitarian surveillance, the neoliberal elites of these states enjoy the luxury of a feast in time of plague.
Along with purchase statements on diamonds and $500,000 USD necklaces, we will publish financial declarations and money orders, so the public knows.
With this publishing, we also hope to raise awareness of the UK and EU governments who have regulations that legally prosecute the companies who can not protect their customer data. We also want to motivate these customers themselves to initiate legal action.
We hope to see more great coverage from Daily Mail!
Stay safe!
Kind Regards,
Conti Team

11/4/2021 1309 0 [0.00 B]

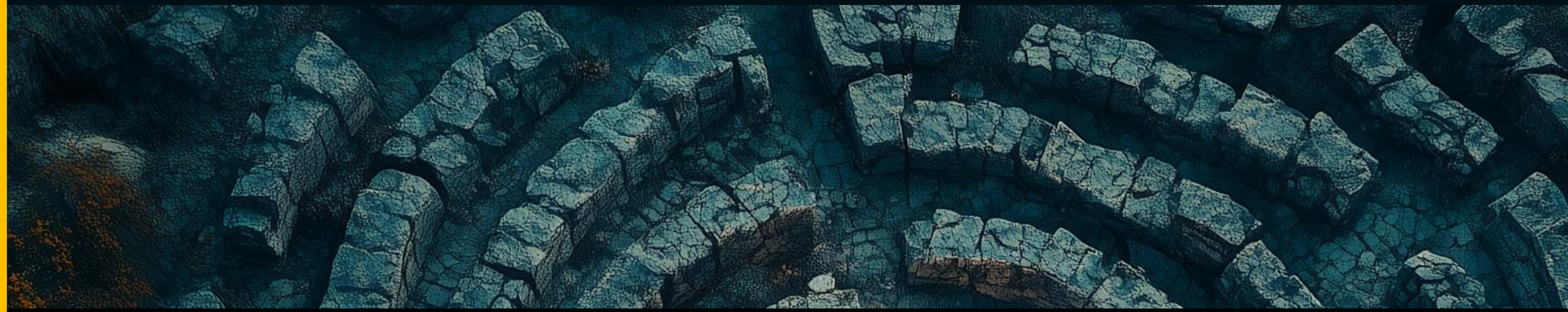
- **JVCKenwood:** The Japanese multinational had the honor to be pubblished on Conti DLS as well. **$7 MLN of ransom** for the decryptor and not publish **1.7 TB of data** which have been stolen, as proof they provided a PDF scan of an employee's passport. The server impacted have been the ones responsible to sales in **Europe.** The company stated the unauthorized access on their servers originated from a subsidary group residing in Europe, professionals hypothesis is Conti bought the access from an **IAB**.
- **Exagrid:** After less than a month from Irish HSE attack a new victim have been forced to deal with Conti disruption, we are talking of **Exagrid** a tiered backup storage company. The group claimed to have encrypted SQL Servers and file servers while stealing 800GB of data. They sticked within the network for a month ***"enough to study all of your documentation"***. The company negotiated until May 13th when a deal have been reached, at first the RaaS offered a **$1 MLN discount** but negotiations concluded with agreement of **$2.6 MLN payment.** A funny detail is that after the decryptor has been sent Exagrid required a new one because the original one have been destroyed by error. This attack was a critical strike to the company prestige since it has been awarded 7 times with industry awards about ***"solution for recovery procedures following ransomware attacks"***.
- **Broward County Schools:** March 7th 2021, Broward County Public Schools district found the infrastructure destroyed and unavailable. It didn't take much before they found a ransom note from ***"ContiLocker Team"*** with negotiation chat link. Here we have some screenshot of the chat which are pretty interesting to read.

Conti asked for a ransom of **$40 MLN** since, as they stated, the District impacted have a revenue of **$2 BLN**. For the RaaS sounded a *"reasonable"* price for the recovery. Broward County is a public school district and not private but **Conti claimed the opposite** when the victim rappresentative asked for a **$500,000** payment, the group responded with ***"Guys, you were hired by the Broward Schools and we know exactly who you are [...] We paid and hired the outsource-company and we know exactly that your recovery-company received a wire transfer from Broward(bankofamerica), that's why we are ready to agree to 10M$"***. The representative stick with his position, Conti decided to drop the negotiations and upload the chat publicly



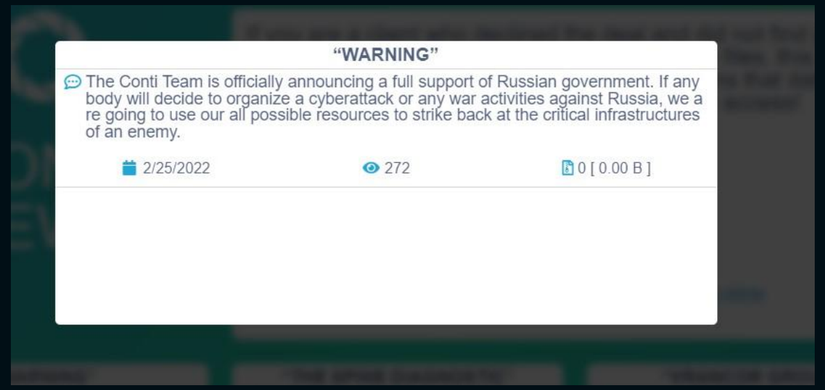
THE WORLD

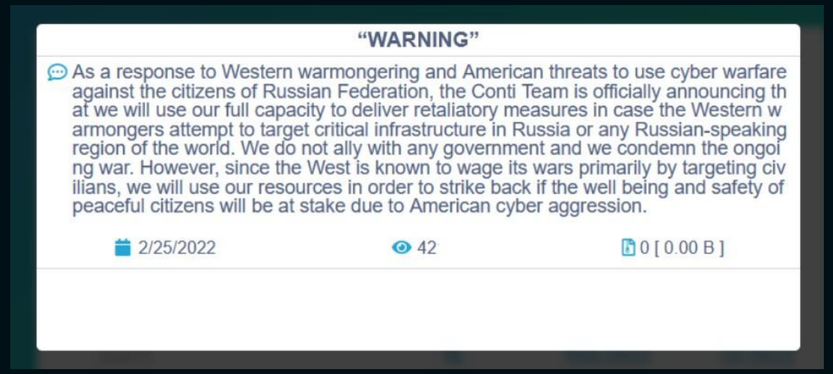
NO ANGELS IN THE GAME, JUST DEMONS



The 2022 started and Conti continued to populate the DLS. Everything was returning to the normal well-being after 2 years of COVID-19 and economic losses, slowly the globe was recovering and ready to stabilize. **On Febbruary 24st, president Putin announced the deployment of Russian troops in Donbass** in order to support separatist corps in **Donetsk** and **Luhansk** regions protecting them from the *"genocide"* caused by Ukraine, minutes later his words tranlsated into reality. The rest is history ready to be written once the war reaches its conclusion.

On that period ransomware groups were not too explicit on their politic positions pubblicly, **is not a good idea to mix politics with businesses. Febbruary 25 Conti pubblished a new post on the DLS**, no new victim this time. **Just a message to the world.**



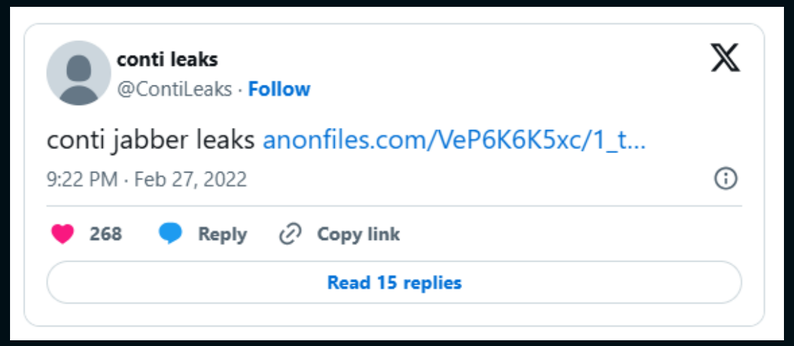


This was something new in the ransomware landscape. Conti is not just picking stating his position but also threatening other countries to not attack with *"any war activities"* against Russia, otherwise **digital retaliation** would occur.

The headlines flooded with their statements while non-technical people were confused, skeptic or scared. Hard to digest when the same group which blocked good part of Irish healthcare system is ready to pull the trigger on your critical infrastructures.

For a while silence and tension were the only things dominating the room. **In less than a week something new was shaking, again, the infosec environment but this time not from Conti.**

Febbruary 27th Conti understood their position and threats came with a price and an **Ukrainian security researcher** was there to make them pay once for all. The account ContiLeaks on Twitter/X announced with a link that **13 months of Conti chat logs have been leaked**



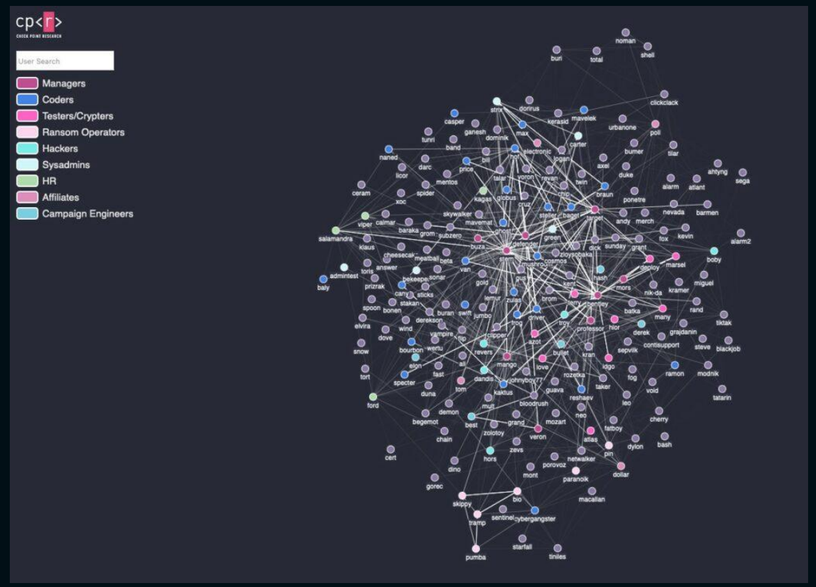
Every messages from **January 29 (2021)** to **February 27 (2022)** is now out for everyone. The messages comes from a Jabber server and Rocket Chat logs. Some usernames are recurrent : **Defender, Stern, Mango** and **Target** (keep in mind this last one) just to name a few. ***"Max"*** (Alla Witte) is also present into the chat logs.


```
{
  "ts": "2020-06-24T20:32:57.402584",
  "from": "braun@q3mcco35auwcstmt.onion",
  "to": "max@q3mcco35auwcstmt.onion",
  "body": "I did auto-clear, I need to check everything now."
}
```

```
{
  "ts": "2020-06-25T19:39:49.044620",
  "from": "braun@q3mcco35auwcstmt.onion",
  "to": "max@q3mcco35auwcstmt.onion",
  "body": "You have updated the column, but you have not migrated to the server:{backslash}nhttp://prntscr.com/t6i8xg"
}
```

```
{
  "ts": "2020-06-26T14:28:52.797338",
  "from": "max@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "I know him a little bit, just had plans to take him seriously. But I know Angular and React, so the base is there."
}
```


Check Point Research made an amazing job with an in-depth analysis of the chat logs, something special is their graph rappresenting the organigram of the group.

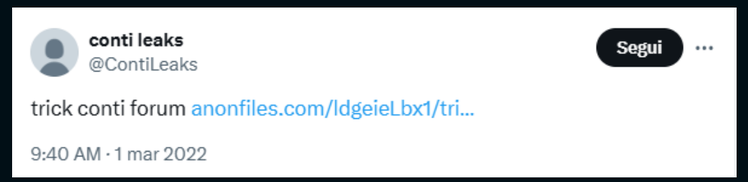


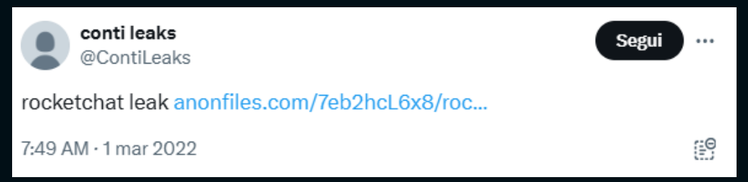
Even if was just a little scratch, what came out with analysis was between brilliant and surprising. The structure of the group is really far from a simple group of computer specialists. **Human Resources, sysadmins, affiliates, negotiator, operators and developers** are well distincted from each others, with timetables and day-off like a regular company. They have also project outside malware like the creation of a social media for blackhats. An ***"employee of the month"*** program was also part of the Conti company structure, individuals with outperforming results would be rewarded with an extra payroll.

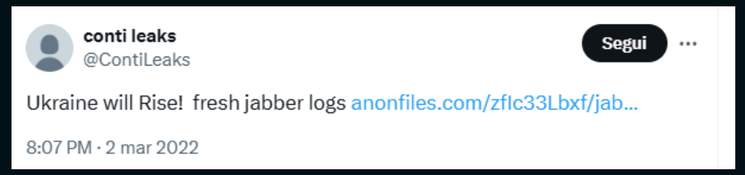
To understand how much professionals those people are take into account that when **Windows 11** was out Conti had a team responsible just of reverse engineering the software seeking for new exploit and abuses.

Chats include recruitment, updates, executable/DLL requests for crypto and relations with other ransomware families like **Ryuk, Maze** and **LockBit** (apparently, LockBitSupp in persons have joined the chat with pseudonym *"Brom"*). A good part of development process was about AV evasion where *"employees"* asked to their *"supervisor"* to buy CarbonBlack AV and other major AV/EDR product. Same thing on **Reverse Engineering** and **testing**, a refurbished **SonicWall** (SMA 410, the new model at the time) have been bought for that.

ContiLeaks was not satisfied enough so March 1st and 2nd released new fresh logs from the jabbers







On those new chats we have a conversation between **Mango** and **JhonyBoy77** where they discuss about **Alexei Navalny**


```
{
  "ts": "2021-04-09T18:13:13.493686",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "so are we even interested in this kind of data?"
}
{
  "ts": "2021-04-09T18:13:24.029087",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "so are we patriots or what?)))"
}
{
  "ts": "2021-04-09T18:13:31.862572",
  "from": "professor@q3mcco35auwcstmt.onion",
  "to": "mango@q3mcco35auwcstmt.onion",
  "body": "we are of course patriots)"
}
{
  "ts": "2021-04-09T18:13:49.854505",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "I got it. I'll let you know if they decode it."
}
```



```
{
  "ts": "2021-04-09T19:17:31.204192",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "yep ocean) the point here is not just to roll out all the files at once, but a little bit at a time."
}
{
  "ts": "2021-04-09T19:17:42.538304",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "that's what I'm getting at)"
}
{
  "ts": "2021-04-09T20:24:01.943505",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "johnyboy77@q3mcco35auwcstmt.onion",
  "body": "don't forget about Navalny, I beeped the chief there - he's waiting for details"
}
```

Moreover the chats included members' opinion about Ukraine, Russia and the war in Donbass

> "**Patrick:** War was inevitable, ukraine made an application for nuclear weapons in their possession
> **Weldon:** monkeys don't explain things, they climb trees
> **Elijah**: @patrick well done and done. Still, no one will ever use it. Yes, just to scare
> **Elijah**: Look, missiles from North Korea periodically arrive in the territorial waters of the Russian Federation. But no one cares. And they have nuclear weapons, by the way. But somehow no one was alarmed
> **Patrick:** old man, you're wrong, there is no doubt about north korea now. No one is happy about the war, brothers, but it is high time to put this neo-Nazi gang of Canaris's foster kids on trial"

Their idea on Zelensky is obviously not soft and they took opportunity to underscore his Jewish origins

> **Weldon**: Zelensky is a jew. Oh fuck
> **Kermit:** Jews. Oh great. My favourites
> **Weldon**: that's right, not Jewish, but a Jew
> **Kermit**: fuck, I wish I was a jew. just be born Jewish and you're considered a member of a secret society and you mess up the Russians' life
> **Weldon:** A tartar was born – a Jew cried
> **Gelmut:** black Crimean Tatar born in Odessa, who received Russian citizenship 😀
> **Weldon:** Obama?
>
> **Gelmut:** A Jewish boy approaches his parents and says – I want to be Russian. To which the parents reply: – If you want to be Russian, you go to the corner and stand there all day without food. Half a day later, his parents ask: "How do you live as a Russian? And the boy answers: – I've only been Russian for two hours, but I already hate you Jews.

Sticking again with the Ukraine, they defined *Holomodor* as a sort of *"fable"*

```
Date: 2022-02-24T10:09:57.223Z
From: angelo
Message: in RU

Date: 2022-02-24T10:09:53.067Z
From: Patrick
Message: where is this?

Date: 2022-02-24T10:09:36.729Z
From: angelo
Message: fuck you

Date: 2022-02-24T10:09:34.600Z
From: angelo
Message: but how many problems are there now

Date: 2022-02-24T10:09:23.527Z
From: angelo
Message: there are problems yes

Date: 2022-02-24T10:09:12.657Z
From: grem
Message: Yes, they are brainwashing children with fables about the Holodomor

Date: 2022-02-24T10:09:02.947Z
From: angelo
Message: yes

Date: 2022-02-24T10:08:58.730Z
From: Patrick
Message: they are all in jail

Date: 2022-02-24T10:08:47.115Z
From: angelo
Message: Judge Khakhlova was covered up and she rotted people

Date: 2022-02-24T10:08:37.893Z
From: angelo
Message: and they were winged
```

A lot of sexist and homofobic messages have been sent into rocket chat without no problem with other members to follow up. What is most disturbing is the black humor about children abuse

> **Angelo:** is it possible to fuck the girls while they are sleeping?
> **Elroy:** No, get enough sleep, then, in the evening ..
> **Angelo:** ok, I'll put the tape back
> **Benny:** iconic movie..

They also share what they are watching with others

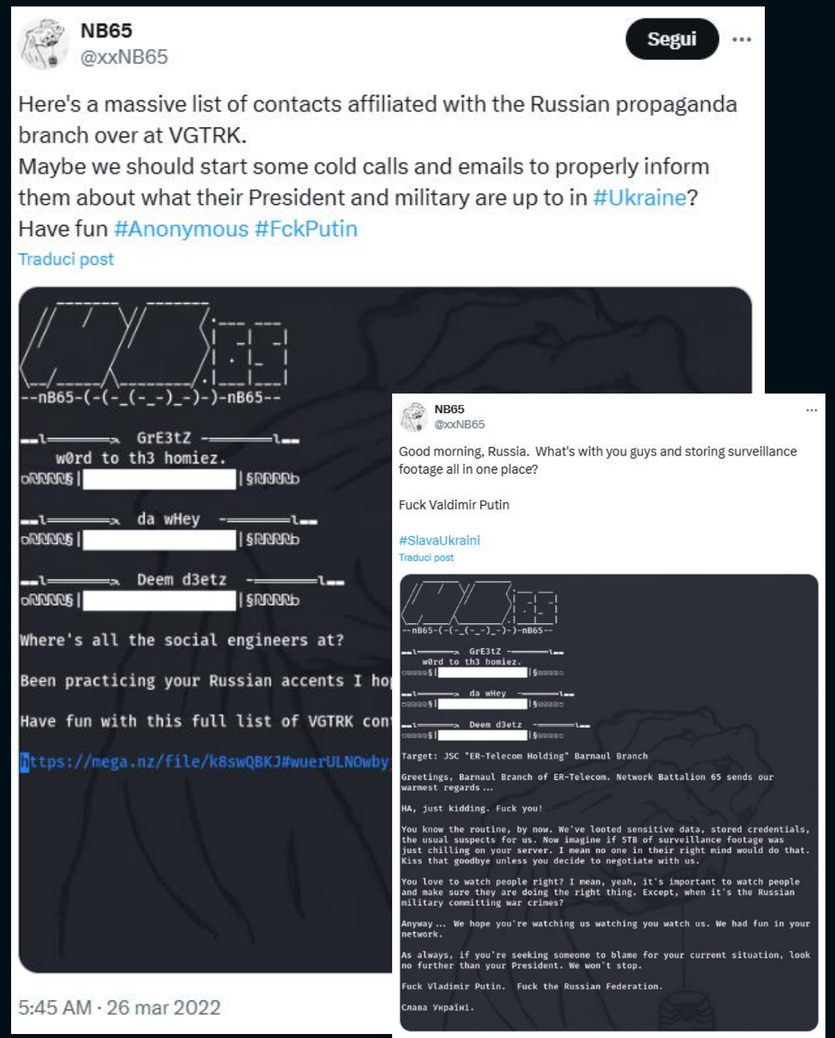
> **Kermit:** although after my link everyone went to try for sure
> **Angelo:** cp what is it?
> **Kermit:** Child Pornography
> **Angelo:** No, even under 17 is no way
> **Kermit:** Come on
> **Angelo:** well, 16
> **Kermit:** There are such lyali at 16

Regarding this problematic and disturbing discussion topics most of the messages show that Conti guys are just normal people with their daily lives, vices and families. Their thesis about Ukraine and other anti-Russian individual stick with the Russian narrative, the decision to explicitly support Russia is no surprise.

Chats was not the only thing that came from the underground, the **source code of Conti ransomware and TrickBot backend have been leaked** as well. The latter have been extremely useful to collect all the IoC and prevent some of the attacks using that infrastructure, good hit since the tool have been heavily used in ransomware operations.

The Conti source code have a total different story, the real backfire is yet to come. A group of hackers named ***NB65*** broke the non-written rules of Ransomware : ***Never. Attack. CIS. Countries***. They took the leaked source code, changed some parts and removed the language safeguards to avoid encryption within CIS countries machine. When everything was ready they started attack on Russian companies and instead of the typical ransom notes requesting a ransom payment they **wrote a textual note warning that the attacks are due to Russia's invasion of Ukraine.**

The well-known companies affected are **Tensor** (document management operator), **Roscosmos** (space industry) and **VGTKR** (radio and television company owned by Russia). VGTKR was affected with a huge exfiltration of data, **786.2 GB**, most of them are emails and files. No DLS this time, everything can be found on Distributed Denial of Secret webpage. **The leaked sensitive documents includes proof of Kremlin influence on the direction of the contents broadcasted and some *"tips"* on how to cover specific events directly from the FSB.**



Conti learned that taunts are not always the best choice, their position about Ukraine probably made angry a lot of persons even within their own group. **ContiLeaks** made an interview with the CNN giving some insight about is own mission.

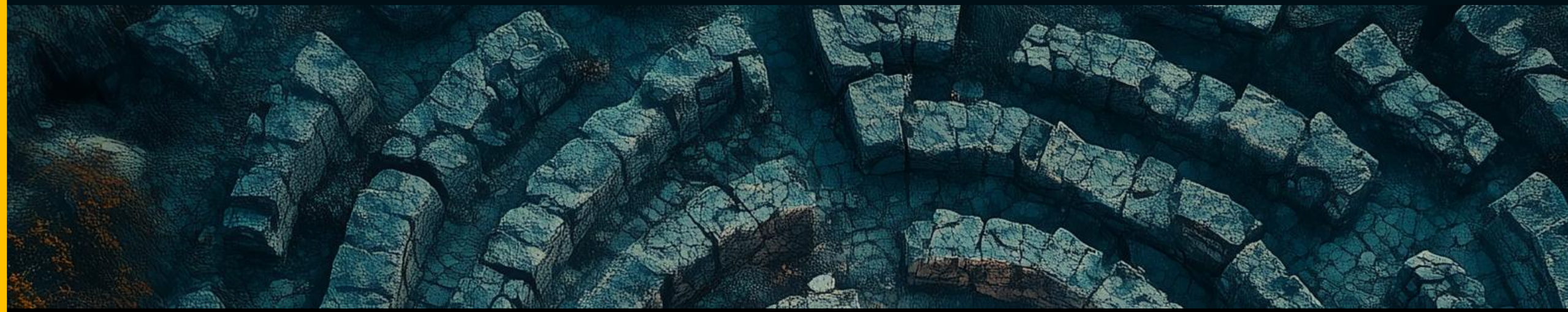
He confirmed to be Ukrainan and motivate the leaks with *"I cannot shoot anything, but I can fight with a keyboard and mouse"*. According to the interview, he was passing the days inside a bunker with his laptop exfiltrating every possible message as possible. He added the FBI contacted him directly asking him to stop so as not to be in the way of their investigation, he stopped for a while but completed the leak regardless the FBI recommendation.

The FBI suggested to remain with a covert access and contribute directly with law enforcement, the reason behind this is (probably) for the tension that was already in play with the war. Biden and Putin had a call in 2021, after that some major REvil members have been arrested in Russia, this was the first sort of collaboration between the two states in terms of digital crime arrests. Probably the actions of **ContiLeaks** have contributed to broke the thin collaboration between the eagle and the bear.

- Conti leaks (original & translated)
- Conti Source Code

ACE OF PENTACLES

406, NOT ACCETTABLE



The Conti leak can be described as the **Panama Papers of the Ransomware-as-a-Service**, they defined themselves and acting as patriots. Showing what's behind the curtains have been sensational, the substance behind the form was highly organized with dense workflow and deadlines. **The *"company"* also helped Alla Witte with processural expenses donating $10.000 to her.**

They had Human Resource, recruitmnet campaigns and everything analogue of a real company. Simply amazing. From now on the CTI community will be really aware of the scale behind every group, a perfect example is LockBit which made professionalism the main attribute of the first and only *ransomware "brand"* ever existed.

The ties with the Russia government was not a misteery but having the proof in front of you will still give you a chill on your spine. **They were not just taking their nationalism deadly seriously, they acted to prove it everytime they had the opportunity to do so.**

The first arrests and the friendly fire put **Conti**, in this part of the story, in a dangerous situation. The use of their own ransomware in the same territory they claimed to protect was a huge hit on the group reputation.

To the readers: Please don't mislead what you read in this article as the norm about every RaaS or digital threat out there. The stereotype of the *"evil Russian hacker"* like every stereotype, has a real baseground but is not enough to generalize the whole landscape.

Most groups don't (at least explicitly) speak about politics and nationalism like Conti did. Obviously, they have only benefits until they respect the *"No CIS" rule*, but this doesn't automatically mean their actions are state-sponsored or motivated by nationalism. Please take care of non-technical headlines and make a distinction between state-sponsored actors and RaaS groups.

The story of Conti is far from its conclusion, there are a lot of surprises worth to be narrated. In the next episode we will discover what happen when the illest RaaS in the scene gets humiliated. Remember the user named *"Target"*? Well, he will be one of the new protagonists of the next episode, enjoy the image below as trailer for the next part.