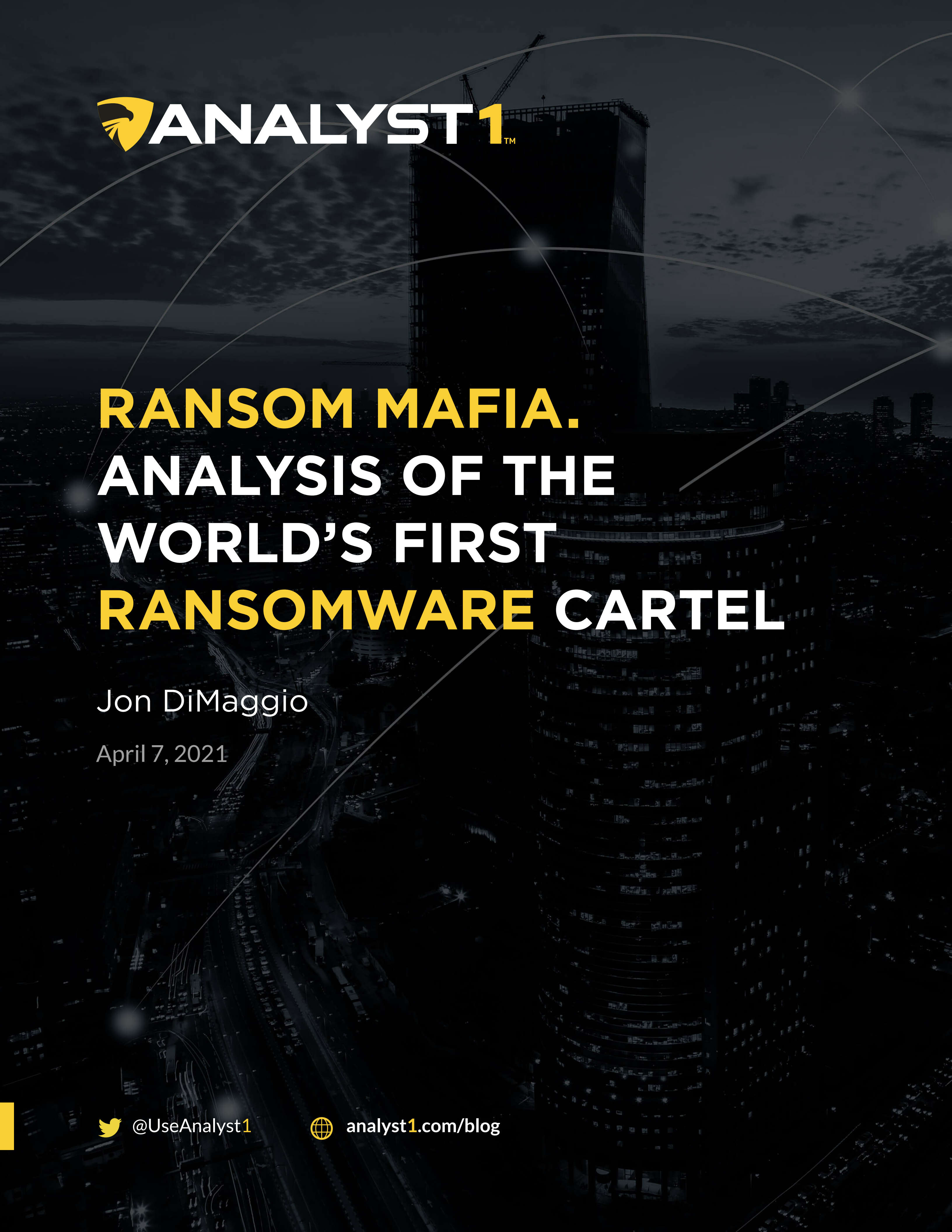


RANSOM MAFIA. ANALYSIS OF THE WORLD'S FIRST RANSOMWARE CARTEL

Jon DiMaggio

April 7, 2021

@UseAnalyst1

analyst1.com/blog

Contents

Introduction

In February 2021, a multinational law enforcement task-force arrested several Ukrainian men for supporting a long-standing ransomware gang known as Twisted Spider. The gang, first seen in May 2019, is behind high-dollar enterprise ransomware attacks. Unfortunately, the arrests had little impact, and several weeks later, in March 2021, Twisted Spider operations continued. Twisted Spider often makes headlines, but it's not only due to their attacks. In June 2020, the gang issued a press release, claiming they joined forces with several other well-known ransomware attackers to create a criminal cartel. If this is true, this collaborative partnership, sharing resources and revenue, would pose a far greater threat to the community than attacks from smaller individual gangs by themselves.

Analyst1 produced this report to address whether or not the Cartel actually exists, as well as to help analysts better understand and defend against advanced ransomware attackers. We conduct research and analysis to address the following goals:

- Research and provide an analytical assessment to determine if the Cartel is real or a fabrication created to distract law enforcement and researchers.
- Profile and assess each gang within the Cartel and determine their relationships with one another.
- Identify the steps behind how each attacker breaches and extorts their victims. Understanding the attacker's behavior and tactics will assist in formulating better defensive and mitigation processes.

Key Findings

Analyst1 spent time digging through criminal marketplaces where Cartel gangs have a presence to research and analyze the criminal entities within the alleged Cartel. We explored the malware and tools the groups use, tracked their bitcoin transactions, and studied relevant reports from other researchers in the field alongside select media outlets.

Our research identified several key findings:

1. Analyst1 observed Cartel affiliated gangs distributing/posting victim data across leak websites belonging to other gangs within the Cartel. In other words, one gang

breached and stole data from a victim and passed it to another gang to post publicly and negotiate with the victim.

2. Analyst1 observed multiple gangs within the Cartel coordinating via Cartel leak websites, including sharing tactics, command and control infrastructure, and sharing/posting victim data.

3. Attackers are moving towards automating their attacks. Multiple gangs have added automated capabilities into their ransom payloads, allowing them to spread and infect their victims without human interaction.

4. Ransom demands continue to increase. Collectively, gangs in the Cartel generated hundreds of millions of dollars from ransomware and data extortion operations.

5. Several Cartel gangs offer Ransomware as a Service (RaaS), hiring hackers to execute attacks while providing them with malware, infrastructure, and ransom negotiation services.

6. Attackers are becoming bolder — they are now conducting PR interviews with reporters, issuing press releases, and leveraging social media ads and call centers to harass and pressure victims into paying.

7. Attackers are reinvesting profits made from ransom operations to advance both tactics and malware to increase their success and revenue. Malware is updated regularly, adding new sophisticated features.

8. One gang, Wizard Spider, developed unique malware geared towards espionage. Analyst1 could not validate how Wizard Spider uses it in attacks. It's existence alone is troubling. We found no other gang in the Cartel that uses or develops espionage malware.

We present other detailed findings and assess the overall Cartel theory in the conclusion of this report.

Cartel Overview

Four ransomware gangs currently exist within the Cartel: Twisted Spider, Viking Spider, Wizard Spider, and the Lockbit Gang as seen in *Figure 1* below.

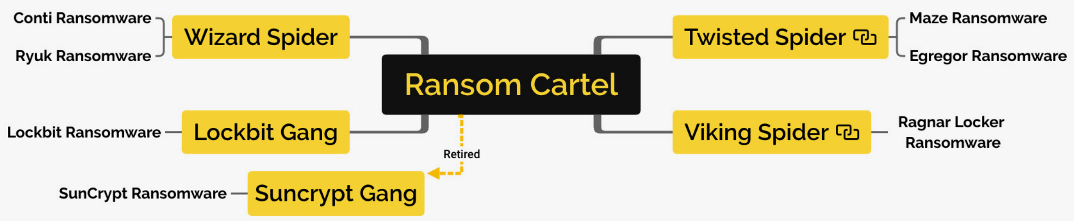


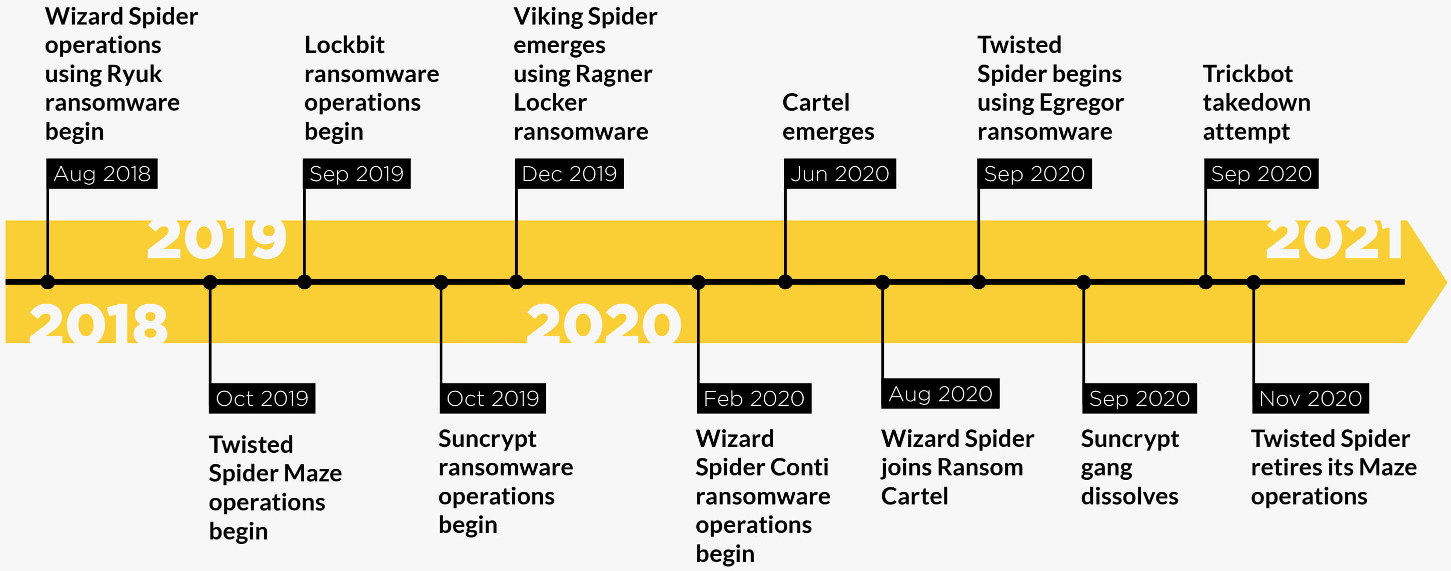
Figure 1: Cartel breakdown

Note: The SunCrypt gang is no longer active, but they previously claimed allegiance to the Cartel and have since retired.

The gangs who make up the Cartel originate from eastern Europe and primarily speak Russian, based on posts made to underground criminal forums. Interestingly, all of the gangs build checks and balances into their ransomware to ensure that the payload does not execute on Russian victims. Here, the malware checks if the system language matches a dialect spoken in the Commonwealth of Independent States (CIS), which formerly made up the Soviet Union. Advanced attackers will often even purposely place false flags into their operations to lead investigators astray. However, the Cartel gangs do little to hide the fact they speak Russian, and they go out of their way not to target victims within affiliated Russian territories.

Timeline

The Cartel emerged in May 2020; however, Twisted Spider began ransomware operations almost a year earlier, in August 2019. The group developed ransomware named Maze to use in its attacks. Twisted Spider is one of the first ransomware gangs to incorporate victim data theft and exposure to pressure victims to pay. Other ransomware gangs soon adopted the tactic, which is now widely used in big game hunting attacks. Several soon-to-be cartel affiliated organizations emerged prior to or during the year between Twisted Spider's appearance and the Cartel's formation. *Figure 2* is a timeline of significant events leading to the Cartel's establishment.



Aug 2018 Wizard Spider operations using Ryuk ransomware begin

Oct 2019 Twisted Spider Maze operations begin

Sep 2019 Lockbit ransomware operations begin

Oct 2019 Suncrypt ransomware operations begin

Dec 2019 Viking Spider emerges using Ragner Locker ransomware

Feb 2020 Wizard Spider Conti ransomware operations begin

Jun 2020 Cartel emerges

Aug 2020 Wizard Spider joins Ransom Cartel

Sep 2020 Twisted Spider begins using Egregor ransomware

Sep 2020 Suncrypt gang dissolves

Sep 2020 Trickbot takedown attempt

Nov 2020 Twisted Spider retires its Maze operations

Figure 2: Ransom Cartel timeline

Twisted Spider

Twisted Spider

During our research into Twisted Spider operations, Analyst1 identified the following key findings associated with the Twisted Spider gang:

- Twisted Spider conducted separate operations using Maze ransomware from May 2019 – November 2020, and they began transitioning to Egregor ransomware from September 2020 to present-day. Each campaign utilized its own malware and infrastructure, primarily separate from one another.
- Twisted Spider created online personas for each campaign, one using Maze and the other Egregor ransomware. The operators who make up the gang use these personas to talk to both the media and security researchers. During media interviews, they discuss their operations and relationships with other ransomware gangs.
- Since its inception, the group has utilized Egregor and Maze ransomware to extort at least $75 million from private sector companies, local governments, and hospitals. We believe this figure to be much more significant, but we can only assess the publicly acknowledged ransom payments. Many victims never publicly report when they pay a ransom.
- Twisted Spider uses a key (string/password) required for the Egregor payload to execute; this makes analysis difficult.
- The gang uses the open-source tool RClone in conjunction with public infrastructure (FTP servers, Dropbox, etc.) to copy and exfiltrate victim data.
- The gang claims to have created a cartel with other well-known ransomware gangs. However, they would later attempt to rescind this claim upon retiring their Maze operations and commencing the attacks using the Egregor payload. However, the evidence we discuss in the Cartel Assessment section of this report supports the theory that Twisted Spider and other gangs do work together. Both their retirement and backtracking on the Cartel affiliation after months of promoting it was likely an attempt to throw off researchers and law enforcement.

Twisted Spider Details

Most criminals try to avoid drawing attention to themselves and their unlawful activities — but not Twisted Spider. The gang talks to the media, provide quotes for articles, and is willing to respond to security researchers. They even have a “Press” section on their data leak website, which they leverage to issue "Press Releases". On more than one occasion, the gang communicated with the cybersecurity media organization *Bleeping Computer.*[1,2]

The first interaction took place after Twisted Spider attacked Canon, U.S.A., stealing and encrypting their data. The attack resulted in a double extortion attempt:

- **Extortion attempt #1:** The gang held Canon's data hostage through ransomware encryption. Only Twisted Spider had the decryption key necessary to restore the data to a usable state. If Canon did not pay the Ransom, the data would remain encrypted.
- **Extortion #2:** Before executing the ransomware, Twisted Spider made a copy of Canon's data, including internal communications and other information not intended for public release.

To pressure Canon into paying the ransom, Twisted Spider threatened to release their data publicly. Afterward, Bleeping Computer reached out to Twisted Spider. Surprisingly enough, Twisted Spider responded to their questions. Bleeping Computer published quotes from the conversation in an article about ransomware attacks.[3] Similar interactions between the publication and Twisted Spider have continued, until the group transitioned to Egregor-based operations in the fall of 2020. Using the new ransom payload, the attacker also obtained new infrastructure for their data leak site and command and control operations. Since then, interview responses have ceased, and the new leak site did not include a "Press" page. This could have been due to the impending law enforcement investigation that led to arrests several months after Egregor operations began. In this moment, Twisted Spider may have realized that they should not be talking to reporters, and that they needed to operate with more discretion.

When Twisted Spider developed Egregor, they built several upgraded capabilities into Egregor's design. For example, the Egregor payload included an option requiring a password to execute the ransomware, unlike in Maze. The password feature provides its developer with an additional level of control. Without the correct password, the payload is rendered useless and will not run. This makes it extremely difficult to analyze and prevents its use by anyone other than Twisted Spider or their affiliates.

While researching Twisted Spider activity, Analyst1 attempted to determine how much revenue the group made through extortion. Unfortunately, while Twisted Spider frequently posts victims' names, they do not post the ransom amount companies pay. However, according to Coveware — a ransomware mediation company — Twisted Spider demanded an average ransom of $693,333 in their operations.[4] During at least one extortion attempt, they attempted to extort 2 million dollars from Allied Universal.[5] If we use the average amount ($693k) and multiply that by the number of victims previously listed on their data leak sites, the group brought in over 75 million dollars. Through our research, Analyst1 found Twisted Spider ransom demands ranging from hundreds of thousands to several million per incident, which corresponds with the average ransom amount Coveware published. You may wonder why a company would pay such a large ransom, but oftentimes the cost of rebuilding after a ransom attack far outweighs the ransom itself. For example, when Twisted Spider attacked Cognizant — an I.T. services company — it cost 50 to 70 million dollars for them to rebuild their systems and restore the affected data.[6] While we never suggest paying an attacker, this example explains why some companies do still choose to pay.

Attack Chain

Figure 3 details the attack chain Twisted Spider uses to breach and extort victims.

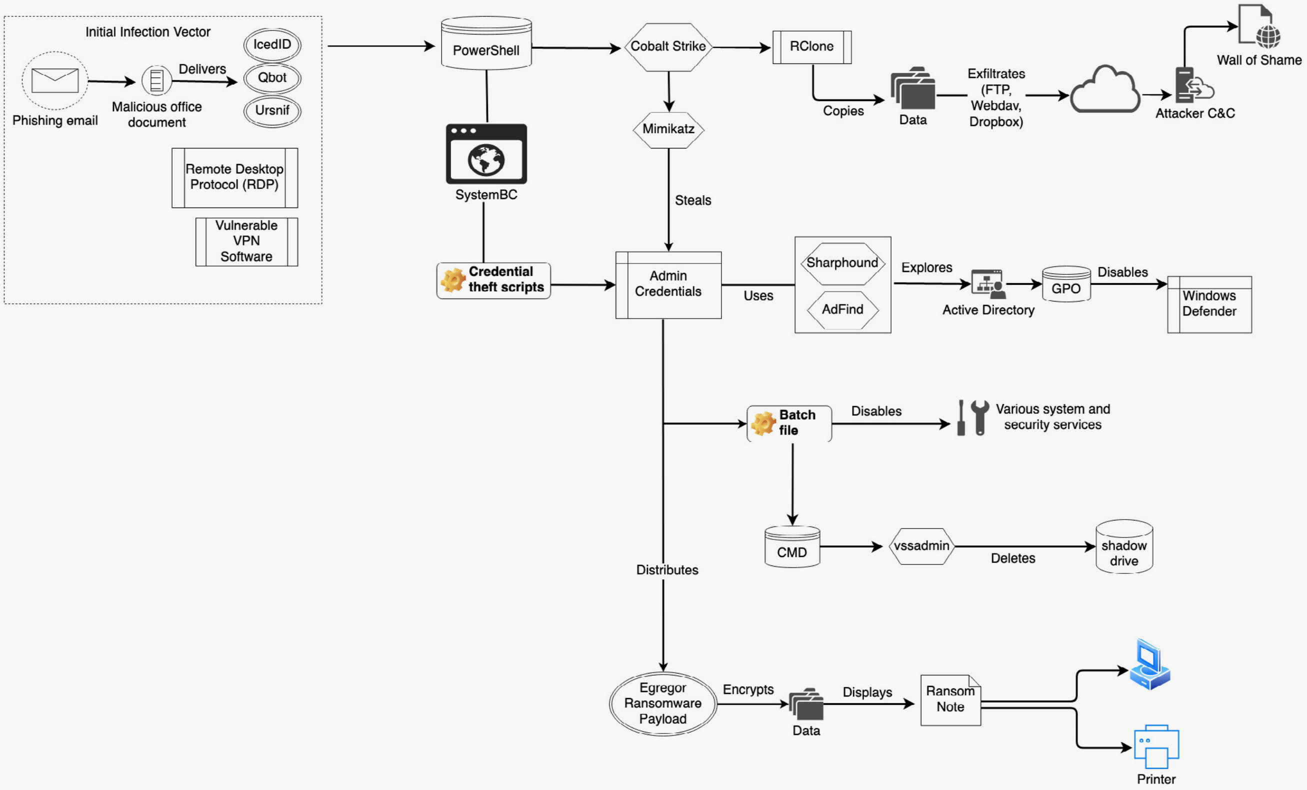
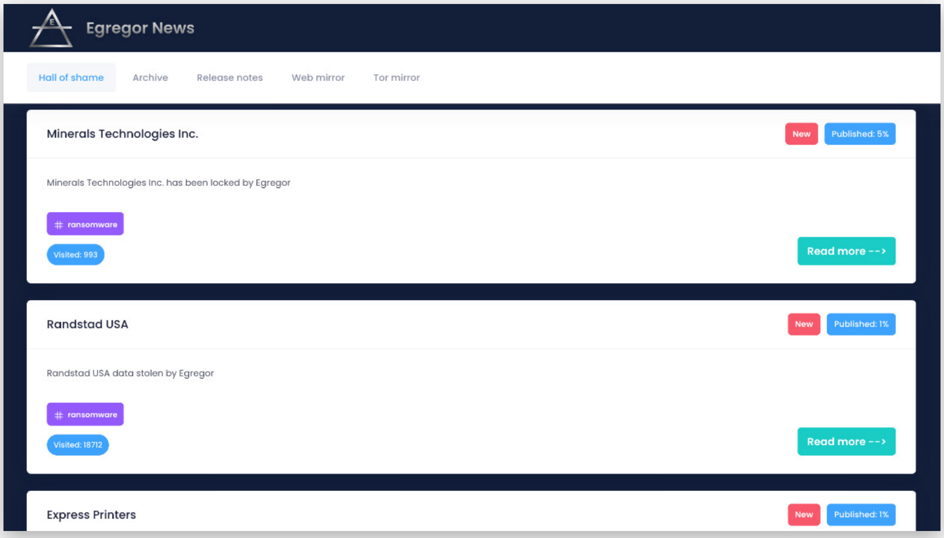


Figure 3: Twisted Spider Attack Chain

1. Initial infection vector varies:
   a. A phishing email delivers a malicious macro-enabled office document that drops commodity malware like IcedID, Qbot, or Ursnif.
   b. In other instances, the attacker uses Brute force tactics to exploit RDP on vulnerable or misconfigured internet-facing devices.
   c. The attacker also gains access by exploiting unpatched, vulnerable VPN software.
2. PowerShell commands are issued to download and compile CobaltStrike.
3. CobaltStrike downloads and installs Mimikatz to collect credentials and gain administrative privileges.
4. In some instances, the hacktool SystemBC manages and executes the rest of the attack. Once installed, the attacker uses the SystemBC control panel to create scheduled tasks. The tasks issue scripts designed to identify and collect administrative credentials necessary for privilege escalation. SystemBC also provides proxy capabilities, encrypting the traffic between the victim environment and the Command and Control (C&C) server.
   A. In situations where the attacker used SystemBC credential theft scripts, they did not use Mimikatz.
5. Next, RClone is downloaded and used to copy victim data, and it is then exfiltrated using attacker-provided scripts.[7] The scripts rely on FTP, WebDAV, or Dropbox to facilitate the exfiltration, which eventually ends up in attacker-controlled infrastructure.
6. Rclone is an open-source command-line tool that manages and syncs local files (data) to a remote site. It is normally associated with syncing cloud data, but the user can still configure any destination, which makes it useful for copying victim data.
7. The attacker uses Sharphound or AdFind to enumerate and identify vulnerable components or misconfigurations of Active Directory.[8]
   A. Sharphound is a tool that profiles Active Directory. It can discover and gather detailed information about group policies, domains, users, computers, and more.
   B. Adfind is an open-source tool which queries and interacts with Active Directory.
8. Using their new administrative privileges alongside the information they've learned about the victim's Active Directory domain, the attacker uses a Group Policy Object to disable Windows Defender.
9. A batch file downloaded via CobaltStrike or SystemBC identifies and disables various system and security services.
10. The script also issues a vssadmin command to delete shadow copies, thereby preventing the victim from using recovery features to restore data.
11. The attacker distributes the Egregor payload throughout the environment.

12. In some attacks, Twisted Spider uses BitsAdmin to distribute the payload.[9]
13. BitsAdmin is a Microsoft command-line tool that manages Windows Background Intelligent Transfer Service (BITS). The service acts at the system level to transfer data asynchronously. The attacker uses BitsAdmin to create jobs that transfer and deliver the ransom payload via the BITS (service) to systems throughout the environment.[10]
14. Once the attacker disperses the payload across all systems, the payload executes, encrypts data, and distributes the ransom note.
15. In some attacks, the ransom note prints repeatedly from all printers within the environment. In at least one attack, it printed tiny ransom notes onto receipt tape from Point of Sale (PoS) systems.[11]

Twisted Spider has encrypted victim data since its inception, but they did not incorporate data theft into their operations until May 2020. At the time, Twisted Spider was one of the few groups who used the double extortion tactic. Not only did Twisted Spider steal the data, but they also established their dedicated leak site (DLS) to "name and shame" the victim. *Figure 4* below is a screenshot of posts Twisted Spider made on their website naming their victims and releasing stolen data.



Minerals Technologies Inc.

Minerals Technologies Inc. has been locked by Egregor

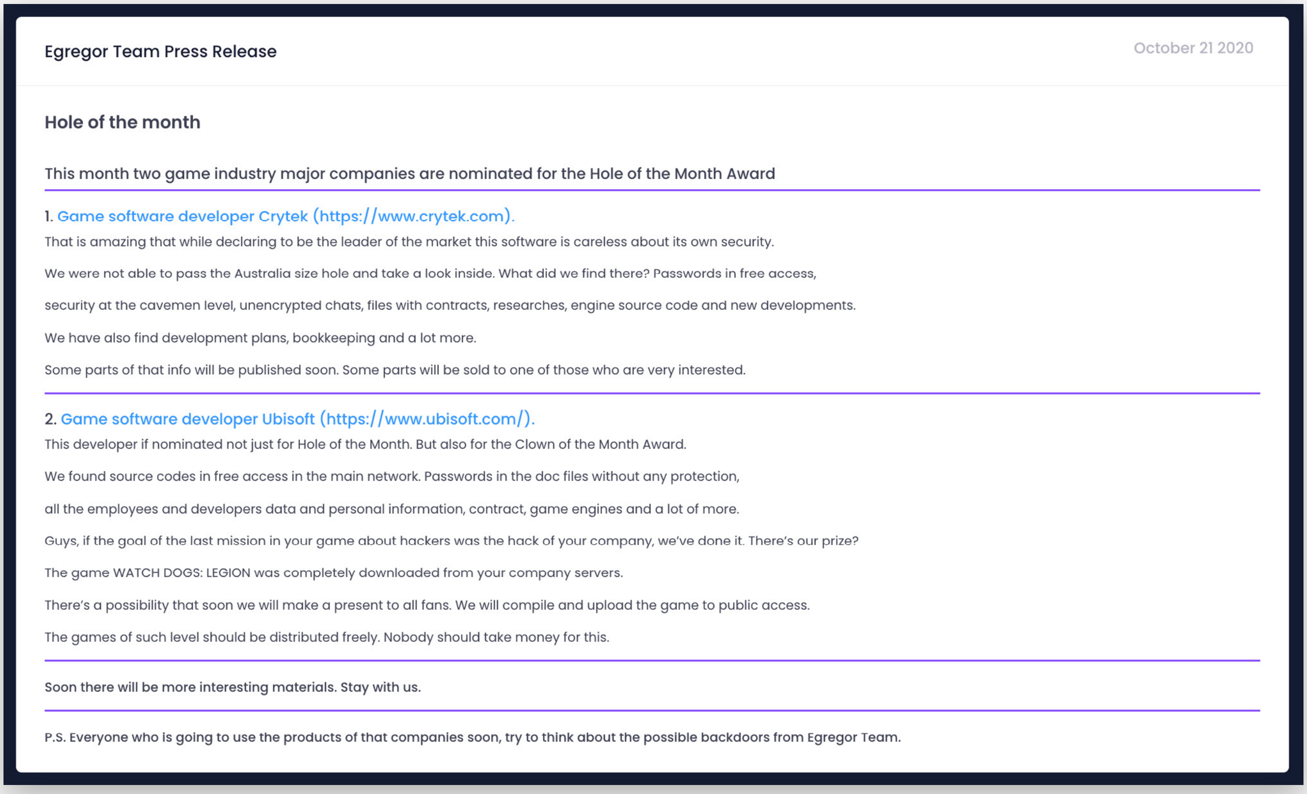
Randstad USA

Randstad USA data stolen by Egregor

Express Printers

Figure 4: Egregor (Twisted Spider) ransomware hall of shame (data leak site).

So far, the attacker is professional even during ransom negotiations in which they directly communicate with the victims. However, perhaps their calm and professional candor is because things have gone their way up to this point. Despite Twisted Spider's attempt to pressure the targeted organizations, not all victims paid. When initial victims did not pay, Twisted Spider calls the victim names in an online tantrum and makes further threats — much like a child who does not get their way. *Figure 5* is an example of Twisted Spider issuing a press release insulting the victim.



Egregor Team Press Release

October 21 2020

Hole of the month

This month two game industry major companies are nominated for the Hole of the Month Award

1. Game software developer Crytek (https://www.crytek.com).

That is amazing that while declaring to be the leader of the market this software is careless about its own security.

We were not able to pass the Australia size hole and take a look inside. What did we find there? Passwords in free access,

security at the cavemen level, unencrypted chats, files with contracts, researches, engine source code and new developments.

We have also find development plans, bookkeeping and a lot more.

Some parts of that info will be published soon. Some parts will be sold to one of those who are very interested.

2. Game software developer Ubisoft (https://www.ubisoft.com/).

This developer if nominated not just for Hole of the Month. But also for the Clown of the Month Award.

We found source codes in free access in the main network. Passwords in the doc files without any protection,

all the employees and developers data and personal information, contract, game engines and a lot of more.

Guys, if the goal of the last mission in your game about hackers was the hack of your company, we've done it. There's our prize?

The game WATCH DOGS: LEGION was completely downloaded from your company servers.

There's a possibility that soon we will make a present to all fans. We will compile and upload the game to public access.

The games of such level should be distributed freely. Nobody should take money for this.

Soon there will be more interesting materials. Stay with us.

P.S. Everyone who is going to use the products of that companies soon, try to think about the possible backdoors from Egregor Team.

Figure 5: Hole of the month press release!

Clearly, the rationale behind nominating a victim for "hole of the month" was to push for a victim to pay the ransom. Then, after being called "hole of the month", the hurtful name-calling intensifies. Twisted Spider then deals the death blow and designates the victim as "clown of the month". For an organized attacker who places time and care into compromising the victim in the first place, it seems odd to handle post-operation tactics and negotiations so childishly. Despite the odd turn of events after the ransom attack, Twisted Spider is still one of the most notorious and dangerous ransomware gangs active today.

Sekhmet Ties

Like its predecessor, Maze, Egregor ransomware shares source code with older ransomware known as Sekhmet. In addition to this, all three variants use the Cha Cha stream cipher and the RSA 2048 encryption algorithm to encrypt victim files. Furthermore, each variant also has similar ransom notes. The developer likely created the original note that remained present across all three as a template — not due to collaboration between the gangs.

However, even without the ransom note connection, the ransomware's shared code and encryption mechanism is a strong technical tie.

While it is unclear if Twisted Spider directly associates with the criminals behind the Sekhmet ransomware attacks, it is clear that they must have access to its source code in order to develop both Maze and Egregor malware variants. Furthermore, attacks involving all three variants also share several tactics. Here, both gangs conduct data extortion in addition to data encryption alongside hosting their websites to name and shame victims. However, these tactics were observed and publicly reported in ransomware attacks beginning in mid-2020. Since then, many enterprise ransomware attackers have adapted these tactics, making them too common to use as evidence for attribution purposes. As of March 2021, attacks involving Maze, Egregor and Sekhmet ransomware are ongoing. Analyst1 tracks the gangs behind the ransomware operation as two separate groups. Additionally, there is no evidence supporting the gang behind Sekhmet has an affiliation with the Cartel.

Twisted Spider Group Facts:

- **First known activity:** September 2020
- **Motivation:** Financial gain
- **Names:** Twisted Spider
- **Historical affiliations:** Twisted Spider previously used Maze ransomware with technical ties to Sekhmet.
- **Spoken language:** Russian
- **DLS websites:** Egreornews[.]com, newsegregor[.]top, wikiegregor[.]top, egregorwiki[.]top, egregor-support[.]com, egregor.top, egregorsup[.]com, egregoranrmzapcv.onion
- **C&C:** amajai-technologies[.]industries (see Appendix for additional IOC's)
- **Malware:** Egregor ransomware, Maze ransomware (Retired), Qakbot, Commodity exploit kits
- **Ransom extension:** 5–6 Random generated characters
- **Ransom note filename:** RECOVER-FILES.txt (Egregor), DECRYPT-FILES.html (Maze)

Viking Spider

Viking Spider

Viking Spider first began ransom operations in December 2019, and they use ransomware known as Ragnar Locker to compromise and extort organizations.[12] Below are key findings identified while researching Viking Spider activity.

- Viking Spider is the first ransomware attacker to install their own virtual machine (VM) into victim environments. They use this VM to evade detection, and they also use it as a launch point to execute the attack.
- The gang is the first to use Facebook ads to pressure victims into paying the ransom.
- Viking Spider outsources call centers in India to contact victims asking them to pay the ransom or risk data exposure.
- Viking Spider uses Managed Service Provider (MSP) software to deliver malware and hacktools as well as provide remote access into victim environments.
- Viking Spider is one of the few gangs who conduct DDoS attacks alongside ransom attacks to pressure victims to pay. Another Cartel gang first used this tactic, but Viking Spider quickly adopted it for their uses as well.
- Viking Spider uses social media such as Twitter to shame non-paying victims publicly.

Viking Spider Details

Viking Spider is the most innovative gang within the ransom Cartel. For instance, the group was the first to use remote MSP software — such as ConnctWise and Kaseya — to gain remote access into target environments.[13] The legitimate use of the tool allows for the MSP to manage their client's environment. During this time, the MSP can take inventory of endpoint systems, upload and download files, remotely access systems, and even more. Here, Viking Spider leveraged its capabilities to deliver malware and tools into the victim environment.

Of course, Viking Spider introduced more novel tactics than simply the use of MSP remote management software. They also used the management software to download a Microsoft installer (MSI) instance of Oracle VirtualBox, a Windows XP virtual machine (VM), and the Ragnar Locker payload.[14] Once up and running, Viking Spider manages the attack from within the VM. No endpoint or antivirus protection runs on the virtual machine; this allows the attacker to hide their malware and hacktools. The attacker uses the Windows XP operating system, given that it does not utilize Windows Defender or other security resources included in current Windows operating systems. Now, the attacker has a hidden enclave within the target's infrastructure wherein they can safely manage and execute the rest of the attack. We detail the attacker's step-by-step process in the Viking Spider Attack Chain later in this report.

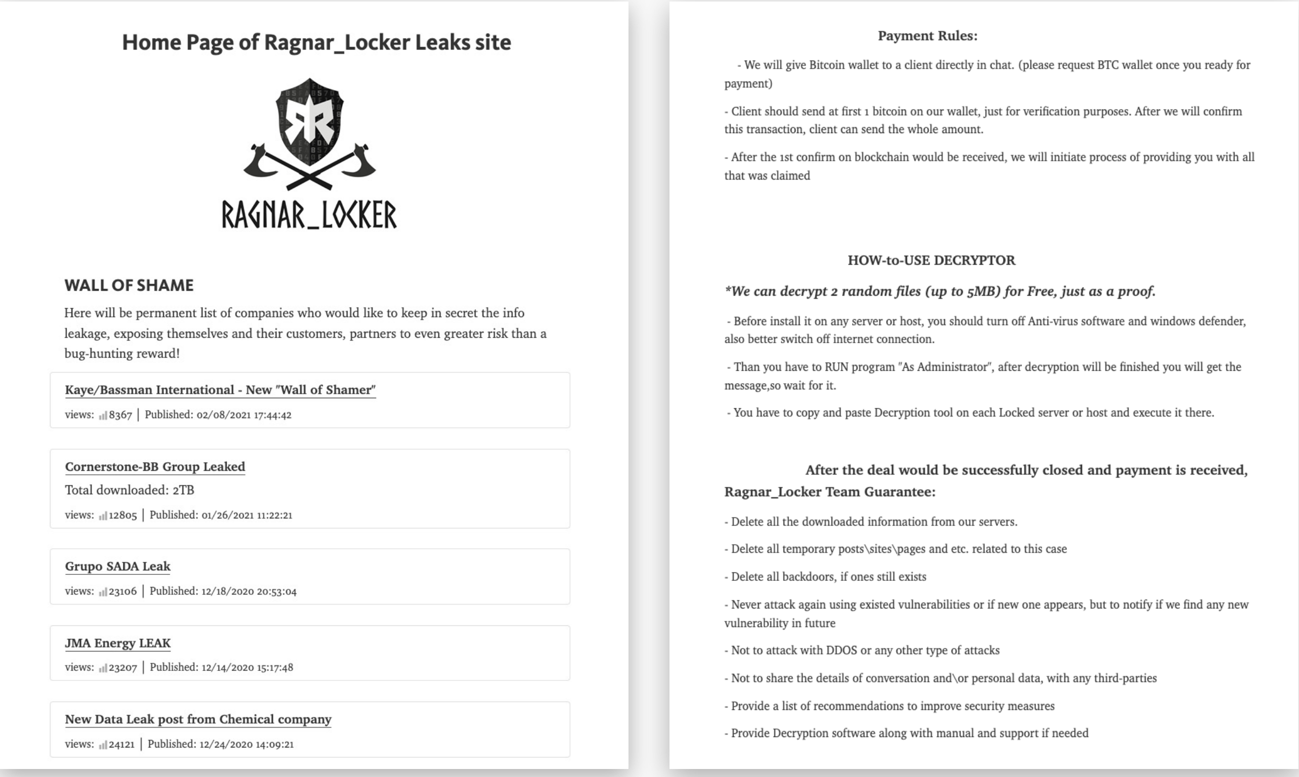
Viking Spider's creativity did not stop here though. Upon completing the ransom and data theft component of the attack, Viking Spider then purchased Facebook ads in order to publicize the breach and pressure victims into paying.[15] The gang hijacked legitimate Facebook accounts to make the purchase, ensuring that neither Facebook nor law enforcement could trace the ads back to the gang. The ads made it clear that Viking Spider would release or sell their sensitive data to other criminals if the victim did not pay.

The ads had two effects: targeting victims and pressuring them further. First, Facebook ads can be marketed to a specific demographic, helping the attacker ensure the correct target audience viewed the ad. This guaranteed the media and general public would be aware that the company and their data were at risk of public exposure. Second, it encouraged secondary victims to pressure the compromised organization to pay the ransom. Secondary victims are the clients of the breached company whose data is now in Viking Spider's control. According to Brian Krebs, a security blogger, the group even outsourced the task of threatening victims to an Indian call center on at least one occasion.[16] Employees at the call center placed calls to victims, encouraging them to pay or face having their data made public. It is hard to believe any legitimate company would take on this work, but in November 2020, this exact thing took place.

If this was not enough, Viking Spider used Twitter to further name and shame victims. Previously, no ransomware attacker used Facebook ads — let alone hire a call center — to harass and pressure victims into paying. Eventually, Facebook shut the ads down, forcing the gang to use their DLS website to shame and pressure victims.

Viking Spider recently began incorporating distributed denial of service (DDoS) attacks into their operations. The SunCrypt Gang — also a part of the Cartel — was the first to implement the tactic which both Viking Spider and Twisted Spider adapted. Viking Spider even updated their "Rules" page, stating DDoS attacks will cease as long as the victim pays the ransom. Here, they spin this as a support effort to help breached companies discover and mediate the very same flaws in which Viking Spider used to compromise them in the first place.

Figure 6 displays Viking Spiders wall of shame website and their "Rules" page:



Home Page of Ragnar_Locker Leaks site

RAGNAR_LOCKER

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

Kaye/Bassman International - New "Wall of Shamer"
views: 8367 | Published: 02/08/2021 17:44:42

Cornerstone-BB Group Leaked
Total downloaded: 2TB
views: 12805 | Published: 01/26/2021 11:22:21

Grupo SADA Leak
views: 23106 | Published: 12/18/2020 20:53:04

JMA Energy LEAK
views: 23207 | Published: 12/14/2020 15:17:48

New Data Leak post from Chemical company
views: 24121 | Published: 12/24/2020 14:09:21

Payment Rules:

- We will give Bitcoin wallet to a client directly in chat. (please request BTC wallet once you ready for payment)

- Client should send at first 1 bitcoin on our wallet, just for verification purposes. After we will confirm this transaction, client can send the whole amount.

- After the 1st confirm on blockchain would be received, we will initiate process of providing you with all that was claimed

HOW-to-USE DECRYPTOR

We can decrypt 2 random files (up to 5MB) for Free, just as a proof.

- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.

- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.

- You have to copy and paste Decryption tool on each Locked server or host and execute it there.

After the deal would be successfully closed and payment is received, Ragnar_Locker Team Guarantee:

- Delete all the downloaded information from our servers.
- Delete all temporary posts\sites\pages and etc. related to this case
- Delete all backdoors, if ones still exists
- Never attack again using existed vulnerabilities or if new one appears, but to notify if we find any new vulnerability in future
- Not to attack with DDOS or any other type of attacks
- Not to share the details of conversation and\or personal data, with any third-parties
- Provide a list of recommendations to improve security measures
- Provide Decryption software along with manual and support if needed

Figure 6: Viking Spider "Wall of Shame" and "Rules" web pages as of Feb 2021

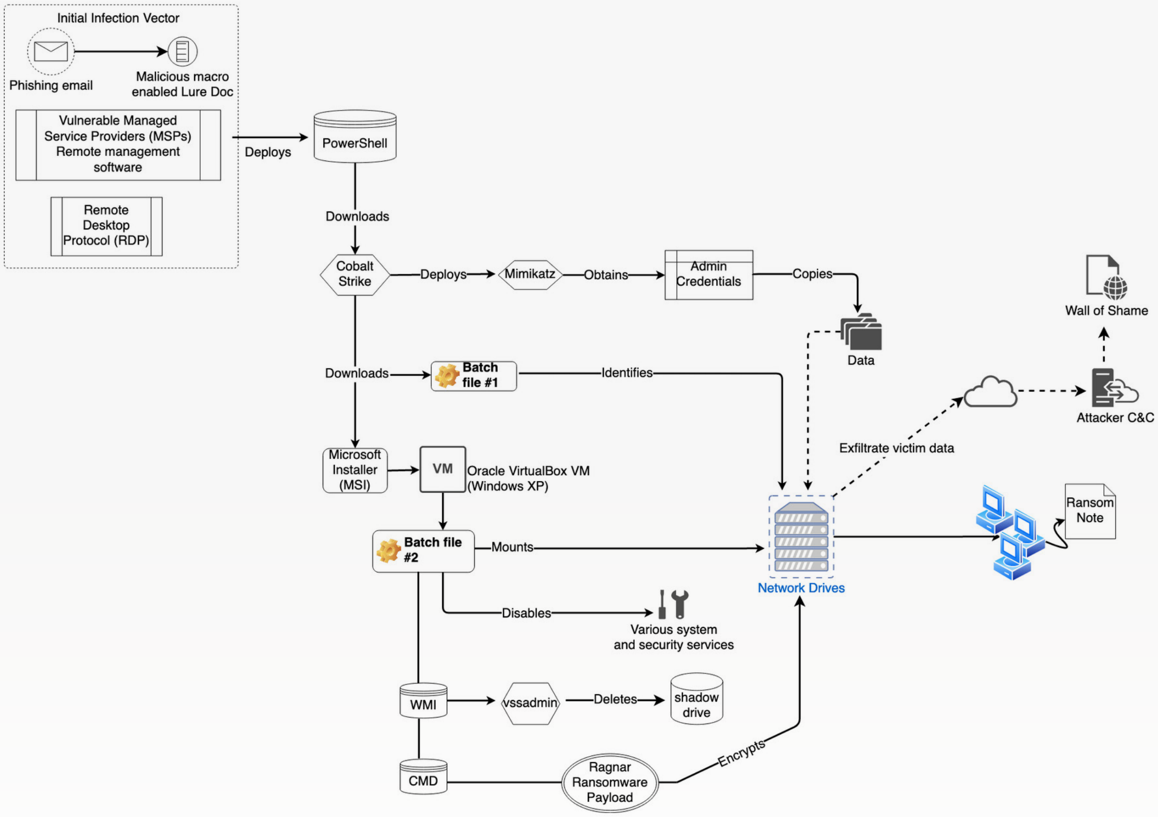


Figure 7: Viking Spider Attack Chain

Attack Chain

Figure 7 above displays the attack chain that Viking Spider used to compromise its targets.

1. The attacker sends a phishing email to deliver a malicious macro-enabled office document.
    a. Viking Spider uses brute force tactics to exploit vulnerable or misconfigured internet-facing devices running the remote desktop protocol (RDP) leading to initial access.
    b. Another initial access tactic Viking Spider used was to exploit vulnerable remote IT management tools such as ConnectWise and Kaseya to gain access, deliver malware and steal victim data from the MSP customer's environment.
2. Using a PowerShell command, Viking Spider downloads and compiles CobaltStrike, which is compiled in the victim system's memory. This allows the attacker to avoid detection.
3. Next, Cobalt Strike downloads Mimikatz. Mimikatz collects/obtains account credentials and escalates privileges. Here, Viking Spider needs the credentials to obtain administrative privileges necessary to execute the attack further.
4. Cobalt Strike downloads and runs a batch file which identifies network drives.
5. A Microsoft installer (.msi) downloads and installs within the victim environment.
6. The MSI installs an Oracle VirtualBox hypervisor and a Windows XP-based virtual machine, including the ransomware payload.[17]
7. The virtual machine maps and connects to the network drives identified earlier in the attack.
8. The attacker copies data from the victim environment and exfiltrates it to attacker-controlled infrastructure.
9. The attack now continues and operates from the VM within the victim environment.
10. The attacker uses another Batch, dispersed throughout the environment designed to disable various security and system services.
11. Using the Windows Management Instrumentation (WMI), the attacker deletes the local shadow copies via the Windows Volume Shadow Copy Service (VSS), preventing the victim from restoring data.
12. The Ragnar ransomware payload disperses to systems throughout the environment and executes.
13. Ransom note appears to the victim for payment.

While analyzing Viking Spider's data leak site, Analyst1 noticed the gang's posts onto their "Wall of Shame" increased significantly in December 2020 and decreased in January and February 2021, as seen in *Figure 8*:

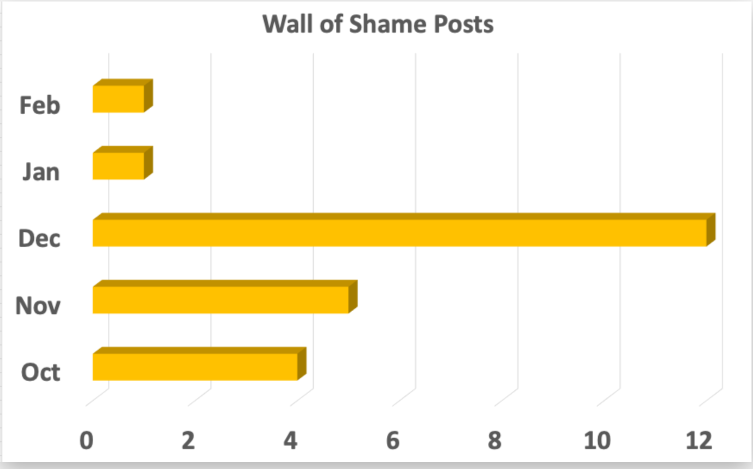


Figure 8: Wall of shame posts by month (Oct 2020 – Feb 2021)

Of course, this could simply indicate Viking Spider is having success, and that victims are paying the ransom without elevating the need for "shaming" them. Keep in mind the gang claims to only "name and shame" victims who do not respond or pay within the allotted time given after ransom execution. However, it could also indicate a decrease in attacks for a re-tooling period, similar to how Twisted Spider attacks using the Maze payload decreased as they prepared to introduce the Egregor payload into their attack flow. A third scenario, it is also possible that Viking Spider could be supporting other Cartel operations, in which their actual attack volume would remain consistent. Regardless, there is no reason to believe Viking Spider is going away anytime soon.

Viking Spider Group Facts:

- **First known activity:** December 2019
- **Motivation:** Financial gain
- **Names:** Ragnar Group, Viking Spider
- **Spoken language:** Russian
- **DLS Websites:** ragnarleaks[.]top, rgleak7op734elep.onion, rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd[.]onion, p6o7m73ujalhgkiv[.]onion
- **Malware:** Ragnar Locker
- **Ransom extension:** .RGNR
- **Ransom note filename:** .ragnar_[Unique_ID]

Wizard Spider

Wizard Spider

Wizard Spider is the most experienced attacker. The gang began ransom operations in August 2018, and they connected to other criminal operations as early as 2016. Analyst1 identified the below key findings during our research into Wizard Spider:

- Wizard Spider has conducted ransom operations previously, using Gogalocker and MegaCortex ransomware variants, both of which are now retired. They currently perform attacks with Ryuk and Conti Ransomware.
- The gang works in multiple teams, conducting simultaneous operations with different ransom payloads. Additionally, they have more malware and hacktools than any other gang associated with the Cartel.
- Wizard Spider developed unique malware known as Sidoh, which was geared towards espionage. Analyst1 could not validate how Wizard Spider uses Sidoh in attacks; however, its existence alone is troubling. We found no other gang in the Cartel that uses or develops espionage malware.
- Conti Ransomware uses 32 CPU threads at once to defeat defenses and encrypt data much faster than any other variant.
- As of February 2021, Ryuk Ransomware includes a new "wake-on-LAN" capability, which allows it to automatically discover and spread to victim systems in the target environment.

Wizard Spider Details

Wizard Spider uses more malware than any other gang associated with the Cartel. *Figure 9* displays the malware used by the gang since their inception.

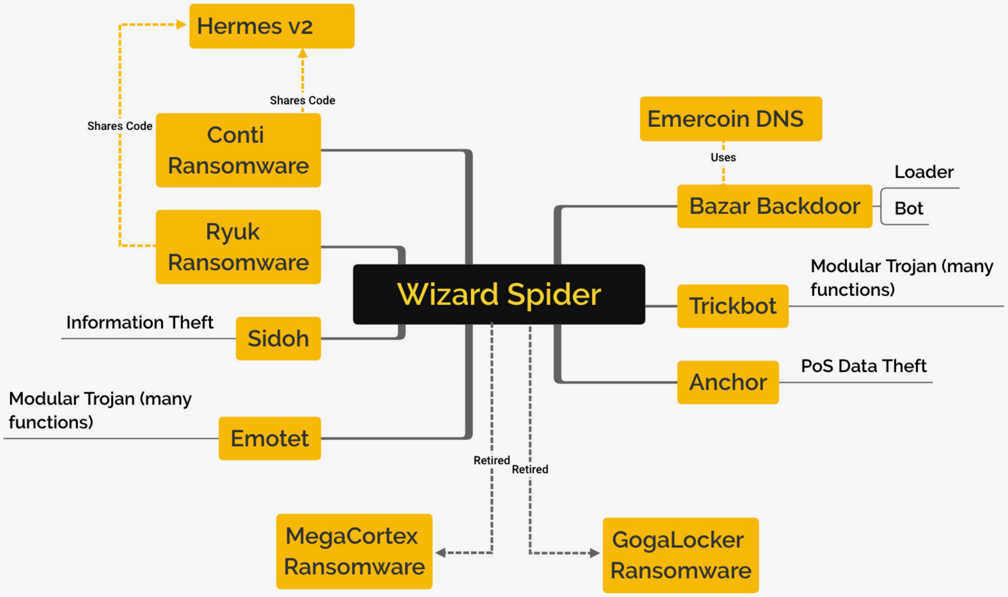


Figure 9: Wizard Spider malware

Trickbot

In the early activity, criminals conducted financial attacks using spam campaigns to deliver Trickbot, which was then purposed as banking malware. Wizard Spider has only taken responsibility for its ransomware attacks, making it unclear if they were the original gang behind the banking malware operations or if they acquired access to Trickbot after the fact. Regardless, Trickbot is one of Wizard Spider's go to resources used in Ransom operations.

One of the advantages Trickbot provides comes from its distribution method. For years, Trickbot spread through high volume mass "spray and pray" spam campaigns, making it extremely prevalent and infecting many systems globally. In 2018, Wizard Spider had no interest in banking-related attacks, but they realized that they could leverage the access Trickbot provides as an entry point to launch ransomware operations. With Trickbot's prevalence in the wild, Wizard Spider did not need to spend time and resources on the initial compromise. Instead, they could cherry-pick victims already infected with Trickbot.

Ransomware Payloads

Using Trickbot's access into victim environments, Wizard Spider first began conducting ransom operations with Ryuk ransomware. Ryuk originates from Hermes ransomware and shares code with both GogaLocker and MegaCortex ransomware families. Additionally, Ryuk, GogaLocker, and MegaCortex have all shared C&C infrastructure. Attacks involving all three payloads continued until late 2019 and into early 2020, when

Gogalocker and MegaCortex operations ceased. Based on analysis of the attacks and the ties discussed, Wizard Spider is behind attacks involving each of the ransomware variants, and they are one of the few gangs that conduct attacks using more than one ransom payload concurrently.

Then in August 2020, Wizard Spider joined the Ransom Cartel. Beyond their experience alone, Wizard Spider has more tools, malware, and sophisticated capabilities than any other Cartel gangs. For example, Conti ransomware uses 32 CPU threads to defeat defenses and encrypt victim data faster than any other variant to date. It also has other unique capabilities, and it can even selectively encrypt files. For instance, it can identify data stored locally vs shared over a network. This allows Wizard Spider to focus on network shares, which typically hold valuable data while providing the attacker the option to leave non-essential data on local systems alone. Focusing on "high value data" instead of "all data" increases operational efficiency and decreases encryption time. Another interesting feature Conti ransomware has is that it utilizes the Windows restart manager, thereby allowing Conti to open and close programs to encrypt their data. There have been several variants of Conti ransomware since its introduction, each adding features and capabilities.

> Wizard Spider has more tools, malware, and sophisticated capabilities than any other Cartel gangs.

Wizard Spider developers worked on more than Conti ransomware alone, though. In Feb 2021, the gang upgraded their Ryuk variant by adding a self-spreading, worm-like capability to the payload. Wizard Spider used a legitimate "wake-on-LAN" technology to identify and infect other hosts on the network with the Ryuk payload. The feature further allowed the attacker to power-on offline systems connected to the victim network. This ensured Wizard Spider could access all victim systems, thereby maximizing ransom encryption throughout the environment.

When Wizard Spider first began using Conti ransomware, Ryuk infections declined. Due to this, it looked as though Wizard Spider might be transitioning away from Ryuk. However, as discussed, gangs often make a public statement when they retire an operation, such as when Twisted Spider announced they intended to retire Maze operations. Several other known ransomware gangs outside the Cartel have done the same when transitioning and retooling their malware and infrastructure. Again, attackers likely do this as a ploy to throw off law enforcement and researchers. If the gang retires, they may believe we would not continue to investigate. Fortunately for the good guys, it usually does not take long to connect the dots when a new operation begins.

As time passed though, Wizard Spider made no announcement, and Ryuk operations continued at a diminished rate. The new Conti operation explains the decrease in Ryuk activity, but the recent payload update is evidence that Ryuk operations are not going away any time soon. In October 2020, Wizard Spider stopped using Trickbot in their attacks. This is likely due to multiple take-down attempts from Microsoft and the U.S. government. Unfortunately, the take-down attempts did not disrupt attacks for long, and Trickbot activity still continues. Regardless, at the time of this report Trickbot has not been seen used in conjunction with new Wizard Spider ransomware attacks.

Further evidence of Wizard Spider conducting concurrent operations involving both Conti and Ryuk payloads surfaced in Jan 2021 . According to a report produced by the cyber security company ClearSky, a Bitcoin wallet used by Wizard Spider received payments from other wallets used in victim extortion attacks involving both Conti and Ryuk ransomware attacks.[18]

- *Address #1:* 1NhNuPogvydJWfTGVp41Rgghqw8MNMjTh3
- *Address #2:* bc1qtaqrv6eeh83vk2hz9myns9lysrzmm4j4366mmw
- *Address #3:* bc1qff0xgtxm6ansnd7dpt9ptc5n0deh3zpw5f9s58

The wallets made it easy to validate ClearSky's findings and provides us with evidence that Wizard Spider is behind both operations.

The Bazar Backdoor

Like Trickbot, attackers use phishing emails to spread the Bazar backdoor. However, Bazar uses the Emercoin — a decentralized DNS resolution service — to provide the malware with the address to command-and-control infrastructure. The Emercoin service uses the .bazar domain (website-name.bazar), which no other provider can use. According to Emercoin's website, due to the design being based on a decentralized model and built on block chain technology, the infrastructure cannot be revoked or suspended, thus making it attractive to cybercriminals:

> *"Because of Emercoin's secure and distributed blockchain the domain name records are completely decentralized and uncensorable and cannot be altered, revoked or suspended by any authority. Only a record's owner can modify or transfer it to another owner, and a record's owner is determined by whoever controls the private key to the associated payment address."*
>
> *— Emercoin*[19]

The Anchor Backdoor

Another resource in Wizard Spider's toolbox is the Anchor backdoor. Wizard Spider uses Anchor to compromise Point of Sale (PoS) systems and steal related financial data such as credit card information. Unlike some of the other malware discussed, Anchor is second stage malware, which attackers introduce after the initial compromise of environments believed to have PoS data. Furthermore, it does not appear in each attack. Upon collecting the data, Anchor obfuscation techniques then combine with DNS tunneling to exfiltrate data.

Sidoh Malware

One of the least-used but most interesting binaries in Wizard Spider's arsenal is Sidoh malware.[20] According to CrowdStrike, Sidoh is not designed for financial gain, unlike the other resources discussed thus far. Instead, its developer designed Sidoh for information theft. Interestingly, CrowdStrike identified strings the tool uses to search for data with the terms "military, secret, clandestine, and government". This type of tool is typically associated with nation-state attacks geared towards espionage. Naturally, this raises many questions about why Wizard Spider uses it. As an analyst, you have to ask yourself: why would a ransomware gang need espionage malware? Analyst1 intends to find out more in upcoming research, but based on Wizard Spider's history of attacks, it does not add up. Additionally, based on initial analysis, Sidoh shares code with Ryuk ransomware. Here, this further supports the theory that Wizard Spider created it.

Attack Chain

Analyst1 believes that the Wizard Spider gang is broken up into several teams. Each of these teams facilitates its ransom operation involving Ryuk and Conti ransomware. Based on this, we believe the Wizard Spider gang is larger than other ransomware attackers, given that other attackers only execute one ransom operation at a time. Utilizing multiple teams would also explain why Wizard Spider uses several attack chains. While we document the two most recently observed with Ryuk and Conti payloads, Wizard Spider has at least five different attack chains in their playbook.

Ryuk Ransomware Attack Chain

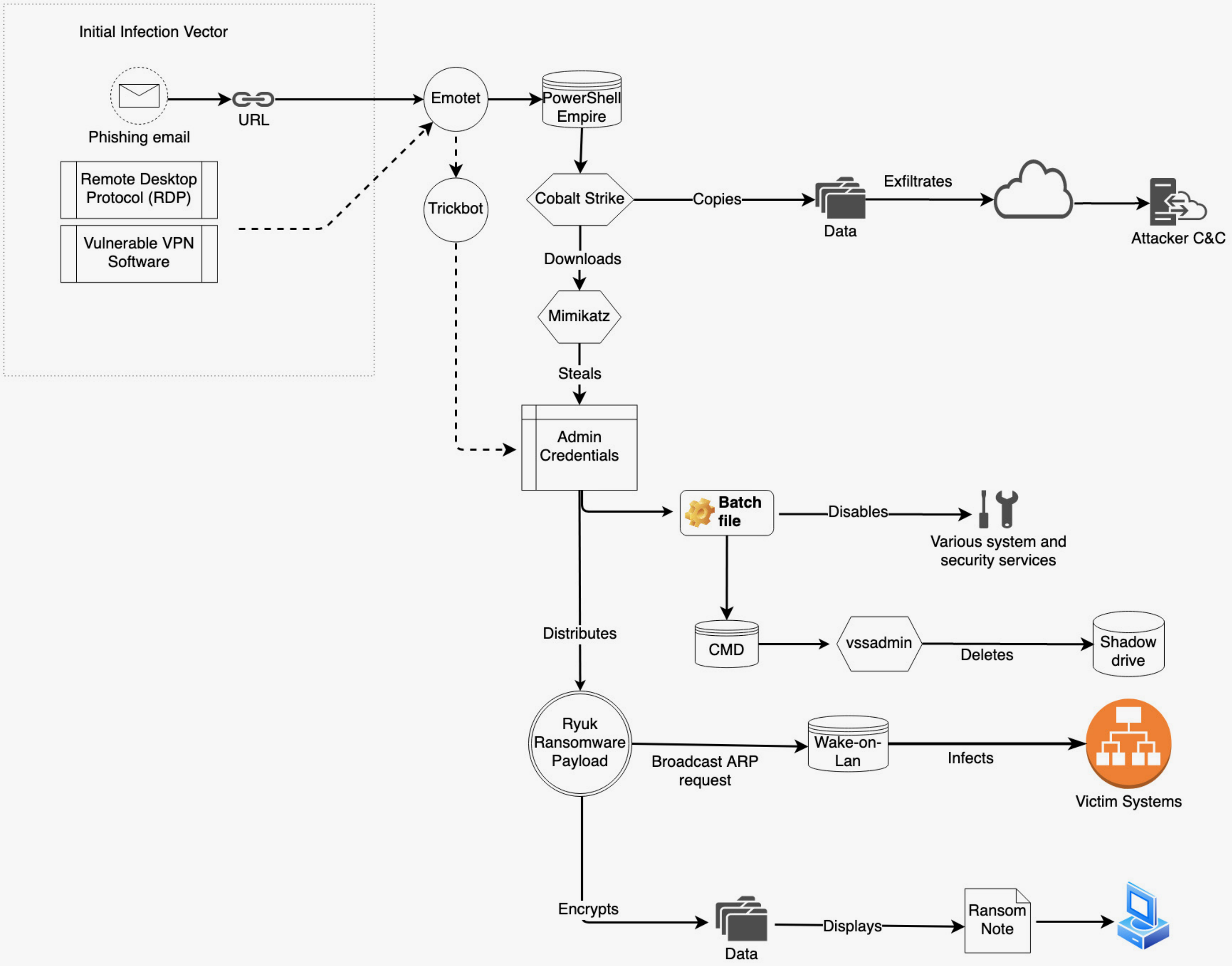


Figure 10: Wizard Spider attack chain using Ryuk Ransomware

1. Wizard Spider utilizes a spear phishing email with a malicious URL to gain initial entry into victim environments.
2. The lure doc executes PowerShell commands on the victim system.
    a. The PowerShell command downloads Emotet onto the victim system.
    b. In some instances, compromised RDP servers provide the initial access into the environment, and PowerShell runs afterward to download CobaltStrike.
3. Emotet then conducts system profiling (recon) and collects information such as computer & usernames, operating system version, network, and other active directory domain information. All of this is sent to the attacker's C&C server.
4. Next, Emotet downloads and drops Trickbot – which runs in memory – and injects into legitimate processes to avoid detection.
5. Trickbot then creates a scheduled task to run, ensuring persistence.

6. The attacker obtains account credentials through Trickbot's credential theft module, or alternatively, through the use of Mimikatz to acquire domain admin credentials.

7. In some instances, the attacker uses the domain controllers via their admin access to spread ransomware across the network.

8. Trickbot then collects email associated files/messages and sends them back to the C&C.

9. Trickbot or CobaltStrike downloads batch files.

    a. The batch files purposed to identify and disable attacker-selected services.

    b. The attacker deletes the local shadow copies via the Windows Volume Shadow Copy Service (VSS), preventing the victim from restoring data.

10. Trickbot downloads the Ryuk payload.

11. The Ryuk ransomware payload uses a wake-on-LAN capability to identify other hosts, wake offline systems, and deliver the ransomware to all systems.

12. Finally, by executing the ransom payload, the victim's data is encrypted throughout the environment.

13. The ransom note appears on systems across the victim's environment.

Conti Ransomware Attack Chain

1. Wizard Spider sends a phishing email targeting the soon-to-be victim.

2. Unlike phishing attempts from other gangs in the Cartel, Wizard Spider often uses legitimate Google docs in the form of a URL present in the email body.

    a. The phishing email encourages the user to click the URL, which then downloads a malicious document. This delivers the Bazar backdoor onto the victim system.

3. Using Bazar malware's capabilities, Wizard Spider downloads CobaltStrike and several other hacktools into the environment.

4. Bazar creates a scheduled task to run, thus ensuring its persistence.

5. Cobalt Strike downloads and executes Mimikatz in the memory of the victim system to elude detection.

6. The attacker uses Mimikatz to steal victim credentials.

    a. The Bazar malware can also steal credential information from victim browsers, but it is unclear if Wizard Spider fully relied on this capability, since Mimikatz also steals credentials.

7. Victim data and Email associated files/messages are collected and sent back to C&C.

8. Cobalt Strike downloads and runs attacker-provided batch files.

    a. Batch files which identify and disable attacker selected services are distributed throughout the environment and ran on each system.

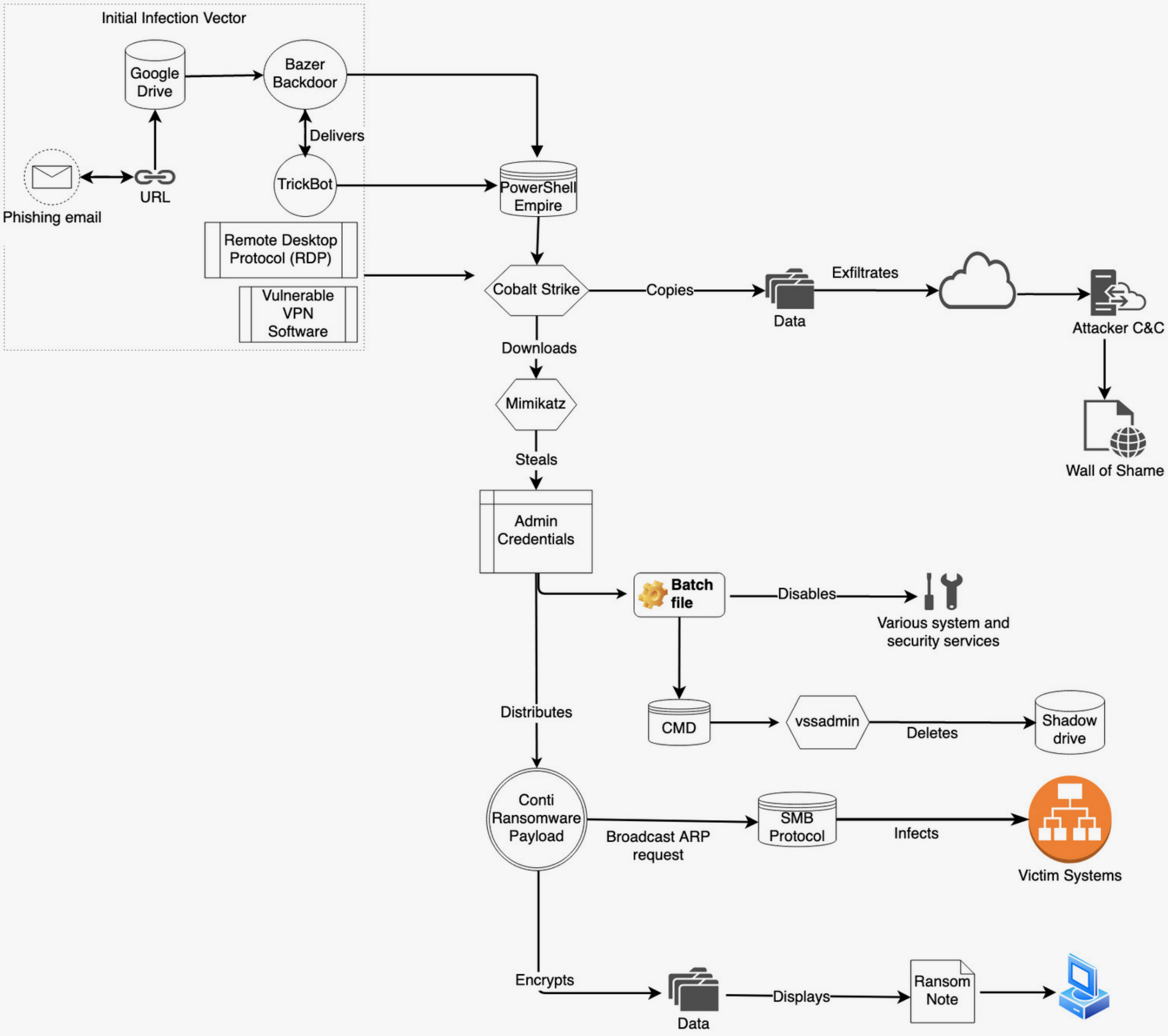
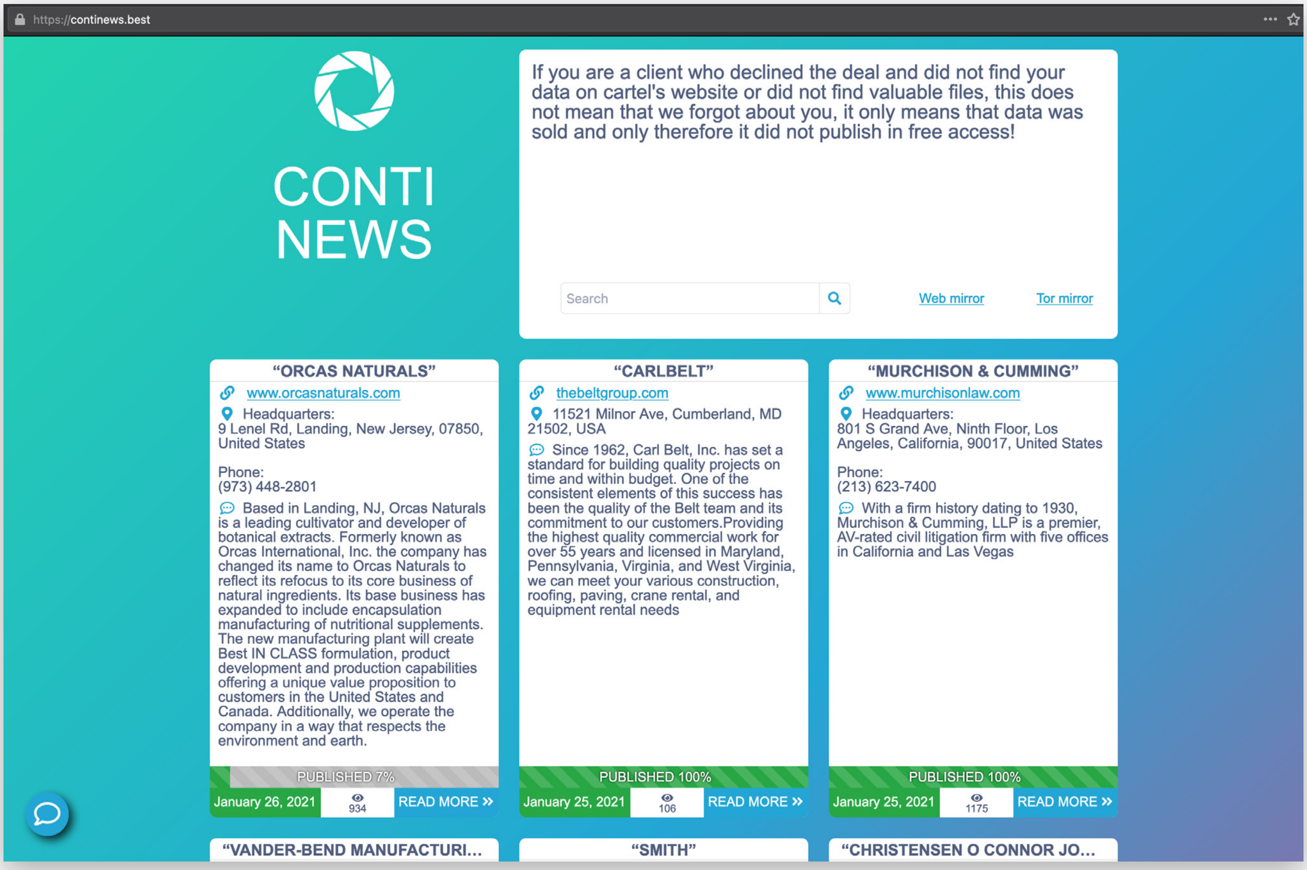


Figure 11: Wizard Spider attack chain using Conti ransomware

9. The attacker deletes the local shadow copies via the Windows Volume Shadow Copy Service (VSS), preventing the victim from restoring data.
10. CobaltStrike and PSExec distribute Conti ransomware payload throughout the environment.
    a. In some instances, the attacker uses the domain controllers via their admin access to spread ransomware across the network.
11. After the ransomware executes, the ransom note presented to the victim.

While specific to their operations involving Conti ransomware, Wizard Spider uses data leak websites similar to other Cartel gangs to “name and shame” and leak victim data.



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

"ORCAS NATURALS"

www.orcasnaturals.com

Headquarters:
9 Lenel Rd, Landing, New Jersey, 07850, United States

Phone:
(973) 448-2801

Based in Landing, NJ, Orcas Naturals is a leading cultivator and developer of botanical extracts. Formerly known as Orcas International, Inc. the company has changed its name to Orcas Naturals to reflect its refocus to its core business of natural ingredients. Its base business has expanded to include encapsulation manufacturing of nutritional supplements. The new manufacturing plant will create Best IN CLASS formulation, product development and production capabilities offering a unique value proposition to customers in the United States and Canada. Additionally, we operate the company in a way that respects the environment and earth.

PUBLISHED 7%
January 26, 2021 | 934 | READ MORE »

"CARLBELT"

thebeltgroup.com

11521 Milnor Ave, Cumberland, MD 21502, USA

Since 1962, Carl Belt, Inc. has set a standard for building quality projects on time and within budget. One of the consistent elements of this success has been the quality of the Belt team and its commitment to our customers.Providing the highest quality commercial work for over 55 years and licensed in Maryland, Pennsylvania, Virginia, and West Virginia, we can meet your various construction, roofing, paving, crane rental, and equipment rental needs

PUBLISHED 100%
January 25, 2021 | 106 | READ MORE »

"MURCHISON & CUMMING"

www.murchisonlaw.com

Headquarters:
801 S Grand Ave, Ninth Floor, Los Angeles, California, 90017, United States

Phone:
(213) 623-7400

With a firm history dating to 1930, Murchison & Cumming, LLP is a premier, AV-rated civil litigation firm with five offices in California and Las Vegas

PUBLISHED 100%
January 25, 2021 | 1175 | READ MORE »

"VANDER-BEND MANUFACTURI...

"SMITH"

"CHRISTENSEN O CONNOR JO...

Figure 12: Wizard Spider data leak site, continews[.]best.

Of note, at the time of this report, we could not identify a data leak site that attackers have used in conjunction with Ryuk operations. It is unclear why Wizard Spider uses the tactic with Conti ransomware but not the Ryuk payload. Also, as a direct result of poor attribution practices, many security vendors and the media claim that Conti replaces Ryuk, which based on the evidence present at this time, is simply not correct.

Wizard Spider Group Facts

- **First known activity:** August 2018
- **Motivation:** Financial gain
- **Names:** Ryuk, Conti, GogaLocker, MegaCortex and Wizard Spider
- **Spoken language:** Russian
- **Website:** Continews[.]best, Conti[.]news, Contirecovery.news
- **Malware:** Ryuk Ransomware, Conti Ransomware, Gogalocker Ransomware (Retired), MegaCortex Ransomware (Retired), Trickbot, Emotet, Bazar, Sidoh, and Anchor malware
- **Ransomware extension:** .CONTI, .RYK (MegaCortex and Gogalocker ransomware families excluded intentionally)
- **Ransom note name:** CONTI_README.txt, RyukReadMe.txt

Lockbit Gang

Lockbit Gang

The Lockbit Gang first came onto the enterprise ransomware scene in September 2020. Much like the other gangs discussed so far, Lockbit brings its own unique tactics to the ransomware game. Analyst1 found the following key findings while researching the Lockbit Gang:

- The Lockbit Gang was the first to automate attacks, and they remain as the most efficient Cartel attacker.
- Lockbit ransomware uses a self-propagation technique. Upon execution, it issues an ARP request to identify devices within the environment, and it then connects using the SMB protocol to spread. Once connected to a live host, it executes a PowerShell command that connects to attacker C&C infrastructure. At this point, it proceeds to download the ransom payload (often disguised as an image file).
- At least once, the attacker overwrote the Master Boot Record (MBR), requiring a password to boot. The Lockbit Gang achieved this through the use of the open-source tool BCDedit. BCDedit is a command-line tool that can edit the boot configuration in M.S. Windows operating systems.
- The Lockbit Gang conducts interviews about their attacks with news media.

Lockbit Gang Details

We mentioned the Lockbit Gang is the most efficient ransomware attacker to date. Most attackers spend days to weeks actively working in a victim's network before executing the ransom payload. However, the Lockbit Gang has compromised victims and automates their attacks, allowing them to move from initial access to ransom execution in just a few hours. While their attacks are far more efficient, they require the Lockbit Gang to gain administrative access early in the attack.

One such example of Lockbit's efficiency comes from Darktrace. Darktrace is a leading AI cyber defense company, and in a February 2021 they identified a Lockbit attack. During this attack, the gang moved from initial breach to payload execution within two hours.[21] Fortunately, in this occurrence, Dark Trace's technology allowed the victim to mitigate the attack, but this is not always the case. Again, this efficiency is significant, as it gives defenders far less time to identify when an attacker is present on their network. In regards to their methodology, the Lockbit Gang uses the ransomware, tools present in the environment, and a commodity keylogger in their attacks.

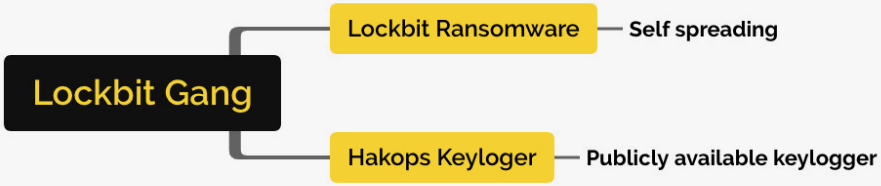


Figure 13: Lockbit Gang malware overview

The attacker also appears to be learning from mistakes in previous attacks, growing in sophistication. In early operations, the group used the file transfer protocol (FTP) to exfiltrate victim data. The problem with this tactic is that FTP transmits data in clear text. Moving large amounts of data from the victim environment could very easily draw attention to the attacker. In recent attacks however, the Lockbit Gang has changed tactics and switched to using an IPSEC tunnel to create an encrypted channel to exfiltrate victim data, eluding detection.

The operational efficiency seen across attacks is not an afterthought with the Lockbit gang, but a primary focus. The streamlined capabilities seen in attacks began in the development phase of Lockbit ransomware. For example, its developer devised many features into its code design, automating portions of the attack chain using a worm-like capability to spread throughout the environment. Specifically, it leverages the Server Message Protocol (SMB) to identify other hosts and network shares within the target environment. Then, using batch files, Lockbit issues PowerShell commands from each discovered host, having them download, execute, and infect themselves with Lockbit's ransom payload. Of course, there is more to the attack, which we discuss next in the Lockbit Attack Chain.

Attack Chain

1. The attacker uses brute force techniques to exploit un-patched vulnerable VPN software.
   a. In the attack observed, the victim's VPN software flaw resulted in the attacker gaining access to a domain admin account.
2. Unlike all other attacks discussed, Lockbit attacks are automated. After gaining initial access, the malware identifies a single host and delivers the ransomware payload.
3. Using their administrative access, security services are disabled on the infected host, such as Windows Defender and the system firewall.
4. A keylogger/screen capture tool (HAKOPS Keylogger) is also dropped on the infected system that captures the victim's keystrokes, takes screenshots, and

transmits data once per day to an FTP server located in Ukraine.

5. The malware instructs the victim system to delete local shadow copies via the Windows Volume Shadow Copy Service (VSSADMIN) to prevent data restoration.
6. Next, the ransomware instructs the victim system to transmit a broadcast ARP request to all hosts in order to identify other systems present in the environment.
7. Now that the network is enumerated and systems and the servers have been identified, the malware issues a PowerShell command instructing each of the hosts to establish a connection with attacker-controlled infrastructure and download an image (.PNG file) that drops a malicious PE.
8. In other occurrences, the attacker downloads additional hacktools in order to lock the user out of their desktop. This prevents the user from interfering with the ransom encryption process once initiated.
9. Upon execution, the downloaded binary installs Lockbit ransomware onto each system identified in the previous discovery step.
10. Finally, the ransomware encrypts the victim’s files and delivers the ransom note.
11. In one at least one attack, MBR is also encrypted on victim systems.

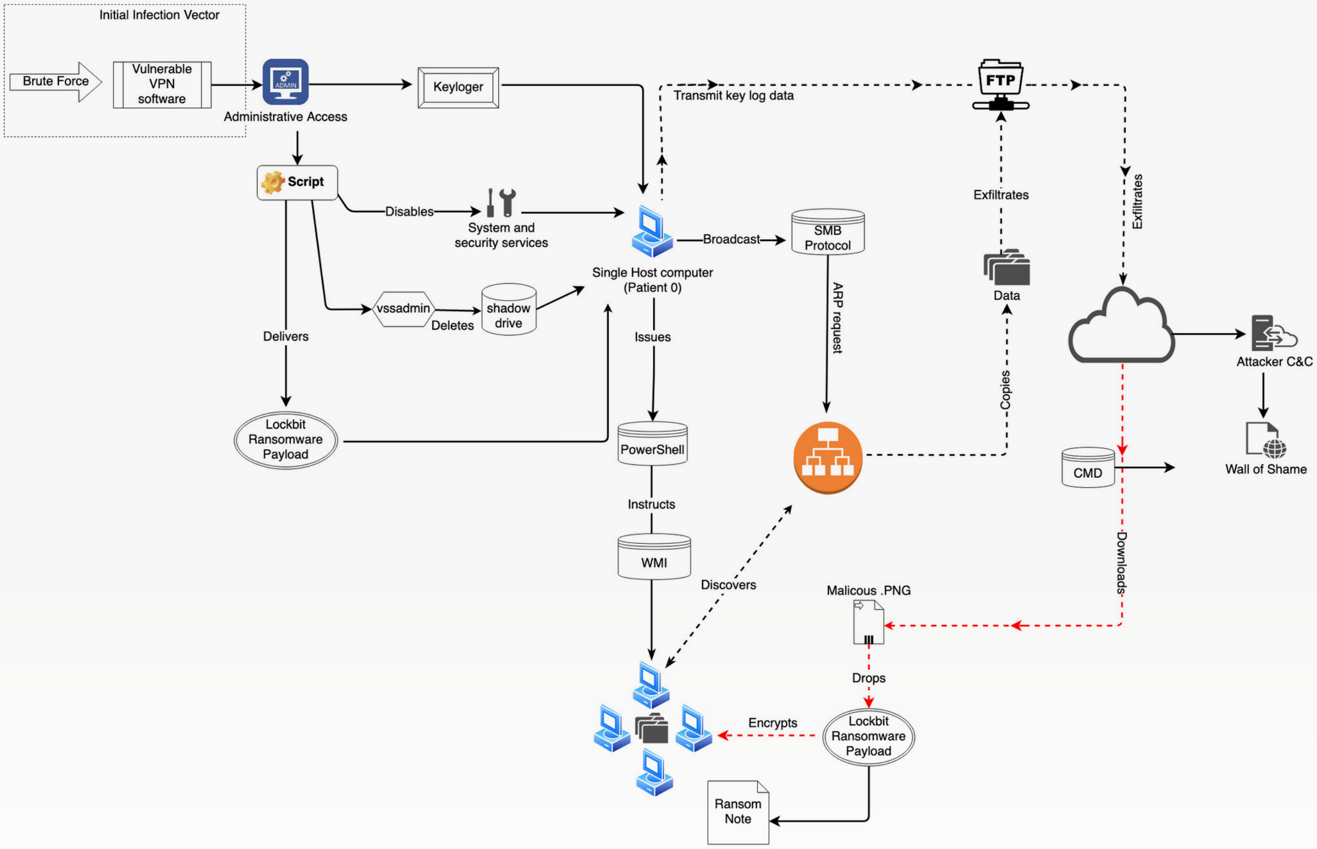


Figure 14: Lockbit attack chain

Attack Chain Two

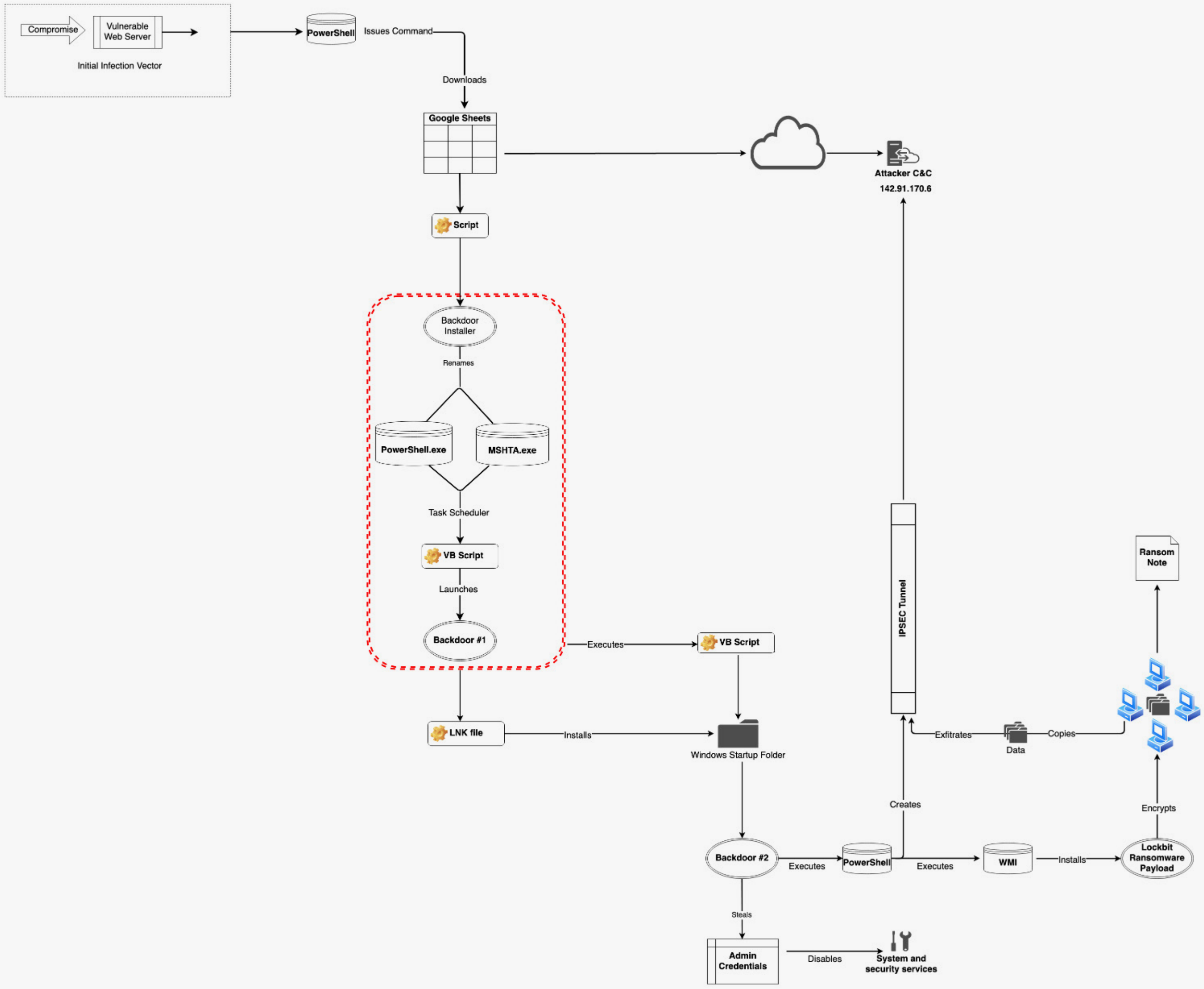


Figure 15: Lockbit Attack Chain two (Derived from research first published by Sophos Security)[22]

1. The specifics of the initial compromise with this particular attack chain are unknown, but Lockbit likely uses other common vectors such as phishing emails that deliver malicious lure docs. Interestingly, according to Sophos, the victims they observed had no public (Internet) facing systems, but many of their internal systems had poor security hygiene.

    a. Similar to the first Lockbit attack chain discussed, Lockbit manages and initiates the attack from one central victim within the target environment.

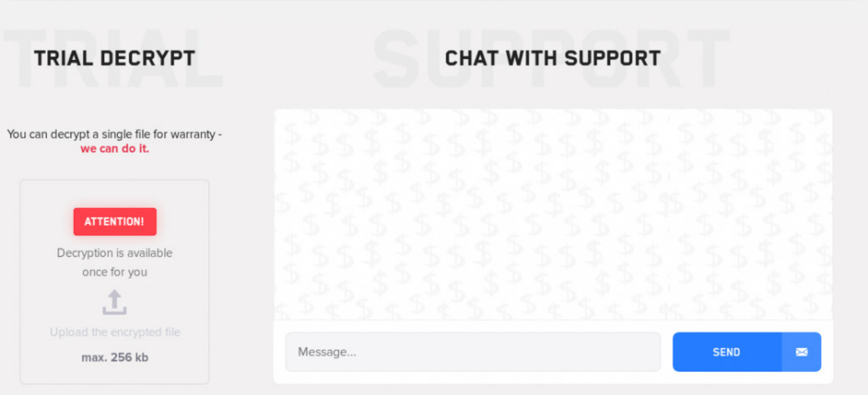
2. Upon initial access, a PowerShell command downloads a Google Doc spreadsheet with Base64 encoded commands in the sheet's cells. This is also evidence that a phishing email is likely the initial infection vector.

3. The victim systems execute the command found within one of the spreadsheet cells, instructing the system to download additional scripts.

4. The next script instructs the victim to connect to Lockbit's C&C server and download yet another script. This script then copies and renames PowerShell.exe and Microsoft Scripting Host, MSHTA.exe.
5. Next, using the resources copied in the previous step, the attacker instructs the system to create a task which uses Visual Basic to "invoke" a secondary backdoor to ensure persistence.
   a. Lockbit also uses a .LNK file, which is placed into the Windows startup directory.
   b. The .LNK file essentially downloads and compiles another backdoor onto the victim system at startup.
6. Several other downloaded modules check and disable security services and applications, delete backup services, and conduct other attack related functions.
7. The backdoors communicate with Lockbit C&C servers, and depending on the response, they will create an IPsec tunnel to copy and exfiltrate victim data.
8. Finally, a PowerShell script invokes WMI to download and distribute the Lockbit payload onto systems throughout the environment.

a. Ransom payload executes, displaying the ransom across the victim systems.

After Lockbit completes the operation's data theft and encryption phase, the double extortion stage begins. Like most other gangs in the Cartel, the Lockbit Gang hosts their own data leak site to name and shame the victim. Additionally, Lockbit adds a secure chat room on their website for victims to communicate during ransom negotiations. Historically, ransomware attackers used publicly available and free email accounts like Proton mail — a legitimate email service based on encryption and secure communications — to negotiate with victims. By using their own secure chat infrastructure to host negotiations, they leave no email trail for law enforcement to investigate. Essentially, this removed one more piece of evidence that could lead back to the individuals behind the gang.



TRIAL DECRYPT

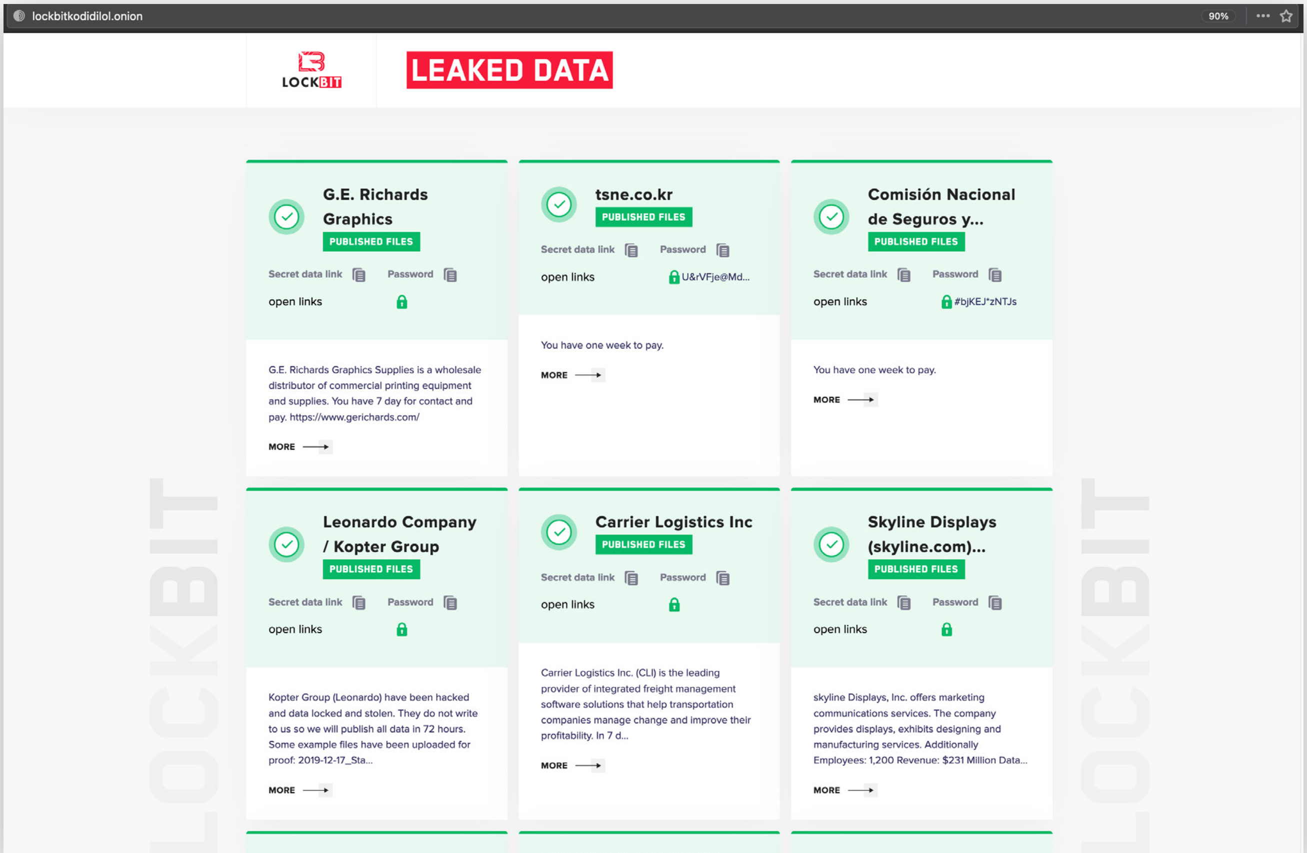
CHAT WITH SUPPORT

You can decrypt a single file for warranty - we can do it.

Decryption is available once for you

Figure 16: Trial decrypt and chat function on Lockbit's data leak site.

Amusingly, Lockbit presents themselves as a “support” service that, for a fee — AKA the ransom payment — will help the victim restore their data and even harden their security posture by disclosing the vulnerabilities discovered in the initial breach. *Figure 17* displays Lockbit’s data leak website.



LEAKED DATA

G.E. Richards Graphics
PUBLISHED FILES
Secret data link Password
open links
G.E. Richards Graphics Supplies is a wholesale distributor of commercial printing equipment and supplies. You have 7 day for contact and pay. https://www.gerichards.com/
MORE →

tsne.co.kr
PUBLISHED FILES
Secret data link Password
open links U&rVFje@Md...
You have one week to pay.
MORE →

Comisión Nacional de Seguros y...
PUBLISHED FILES
Secret data link Password
open links #bjKEJ*zNTJs
You have one week to pay.
MORE →

Leonardo Company / Kopter Group
PUBLISHED FILES
Secret data link Password
open links
Kopter Group (Leonardo) have been hacked and data locked and stolen. They do not write to us so we will publish all data in 72 hours. Some example files have been uploaded for proof: 2019-12-17_Sta...
MORE →

Carrier Logistics Inc
PUBLISHED FILES
Secret data link Password
open links
Carrier Logistics Inc. (CLI) is the leading provider of integrated freight management software solutions that help transportation companies manage change and improve their profitability. In 7 d...
MORE →

Skyline Displays (skyline.com)...
PUBLISHED FILES
Secret data link Password
open links
skyline Displays, Inc. offers marketing communications services. The company provides displays, exhibits designing and manufacturing services. Additionally Employees: 1,200 Revenue: $231 Million Data...
MORE →

Figure 17: Lockbit’s data leak and wall of shame website.

Unlike some of the other Cartel gangs discussed, the Lockbit Gang has not resorted to name-calling in their DLS, and they have remained professional regardless of payment.

Despite these advanced tactics discussed, the Lockbit Gang struggled in early operations to establish itself amongst its peers before they joined the Cartel. A cybercriminal claiming to be a Lockbit affiliate — one who supported four months of ransom operations — claimed problems existed in the attack.[23] According to the affiliate, the problems surrounded the ransomware’s encryption method, and Lockbit Gang could not decrypt victim files. It is standard operating procedure across most enterprise ransomware attacks to decrypt a small number of files as proof that the encryption key will work once the victim pays. If the Lockbit Gang could not decrypt the victim files as proof, it is unlikely a victim would pay the ransom. Naturally, these problems resulted in a loss of profit. The affiliate did their part in the attack, and despite that they never got paid for their work. As an affiliate working for a RaaS provider, this is a big issue. Now, the Lockbit leak site provides a file decryption service, shown in *Figure 16*. Since the gang built the feature into their website they likely resolved the file decryption problem.

Lockbit Gang Group Facts

- **First known activity:** September 2019
- **Names:** Lockbit gang
- **Motivation:** Financial gain
- **Spoken language:** Russian
- **Website:** lockbitkodidilol[.]onion, Lockbit-decryptor[.]com, Lockbit-decryptor[.]top, lockbitks2tvnmwk[.]onion
- **C&C:** https://espet[.]se/images/rs35[.]png, https://espet[.]se/images/rs40.png, 142.91.170.6
- **Malware:** Lockbit Ransomware, Hakops Keylogger
- **Ransom extension:** .lockbit, .ABCD (legacy)
- **Ransom filename:** Restore-My-Files.txt

ANALYST1™

The SunCrypt Gang

The SunCrypt Gang

The SunCrypt Gang began conducting ransomware attacks in October 2019. Analyst1 researched the attacks and progression of SunCrypt operations up to present day and found the following key findings:

- SunCrypt is the first gang to introduce DDoS as an extortion tactic used in conjunction with enterprise ransomware attacks.
- The SunCrypt Gang claimed affiliation with both Twisted Spider and the Cartel. Twisted Spider disputed both claims in an interview with Bleeping Computer.
- SunCrypt ransomware uses the ChaCha20 stream cipher found in Twisted Spider's Maze and Egregor ransomware payloads.
- The SunCrypt gang's ransomware communicated with two C&C IP addresses that Twisted Spider used and controlled in their Maze ransomware operations. These findings are significant, since Twisted Spider disputes the SunCrypt Gang's Cartel affiliation claim.
- Operations ceased in October 2020, but transfers from victims' bitcoin wallets continued until November 2020.

SunCrypt Details

Much like any good reality TV show, drama ensued between the SunCrypt Gang and Twisted Spider after the gang publicly claimed affiliation to the Cartel. In late August 2020, Bleeping Computer publicly released the conversation between the two gangs, wherein each party told their side of the story. Bleeping Computer first reported that the SunCrypt Gang emailed them directly, detailing their new affiliation with the Ransom Cartel. Even stranger, six days after the publication, Twisted Spider contacted Bleeping Computer disputing the claims:

> *"We do not have any connections with SunCrypt, it is a lie."*
>
> *"We do not know why SunCrypt does it, but we believe it is a PR strategy, to send links to companies in chat that they are working us as a pressure."*
>
> *— Reported by Bleeping Computer*[24]

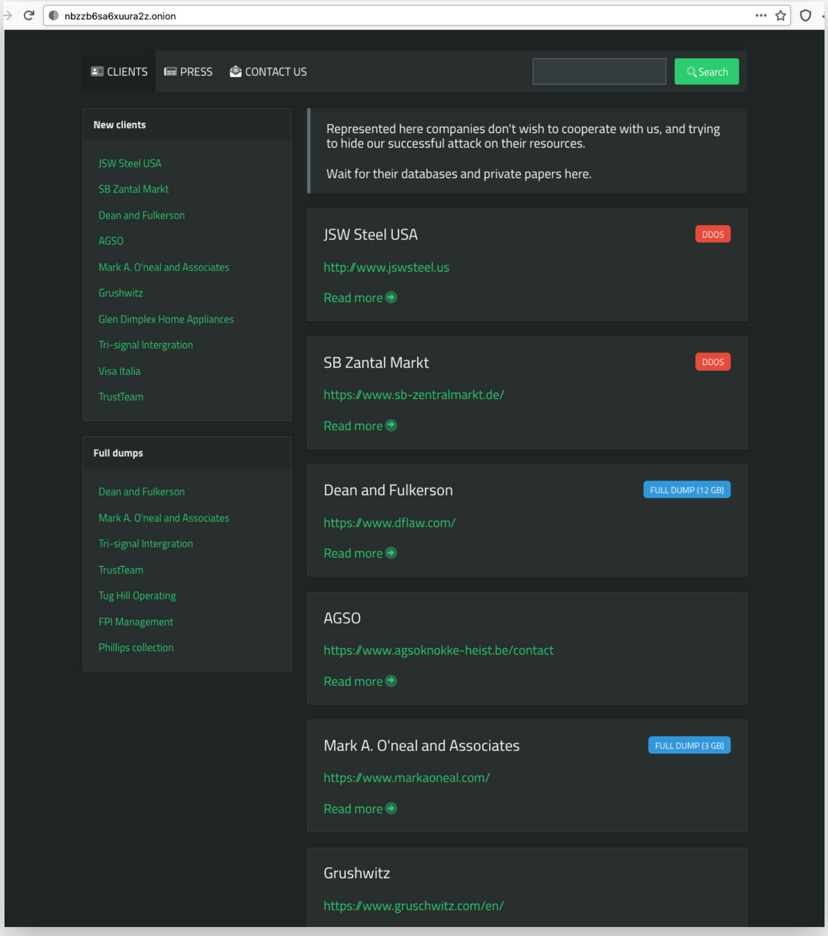
While Twisted Spider disputed SunCrypt's claim, their story did not line up with the facts. Despite claiming that the two groups had no affiliation, SunCrypt and Twisted Spider actually shared C&C infrastructure. Advanced Intel's Vitali Kremez first identified that both attackers leveraged IP addresses 91.218.114[.]30 and 91.218.114[.]31 for C&C in their attacks.[25] Further, Maze, Egregor (Twisted Spider), and SunCrypt (SunCrypt gang) payloads each use the Cha Cha stream cipher to encrypt victim data.

SunCrypt is the first ransomware gang to use DDoS attacks in conjunction with ransomware in its operations

Just after the public dispute with Twisted Spider in early September, the SunCrypt gang began to deploy DDoS attacks in conjunction with ransomware in its operations. As previously mentioned, SunCrypt is the first ransomware gang to use this tactic, and other gangs within the Cartel quickly adopted the strategy. Interestingly, despite claiming no affiliation with SunCrypt, Twisted Spider was the first to adopt the tactic. If having data encrypted and stolen was not enough, now victims had to deal with business loss due to their websites and services being unavailable to their customers. The downed services and unreachable websites may tip off victim clients and draw attention publicly; this of course places additional pressure on the victim to pay the ransom quickly.

Strangely, the SunCrypt Gang disappeared shortly after the addition of the DDoS tactic and their public dispute with Twisted Spider. The gang appears to have abandoned operations, but oddly, their data leak sites remain up. Coincidentally, Twisted Spider terminated Maze ransomware operations around the same timeframe. However, in its closure, Twisted Spider took down their data leak site infrastructure. Let's examine this idea a bit further: suppose a gang is closing down operations, or perhaps they are retooling for the next phase of its criminal activities. In that case, it only makes sense to remove any trace of their previous attacks and infrastructure. If for no other reason, taking down the infrastructure would prevent it from later being used as evidence against the gang. Similarly, this could prevent law enforcement from tracing the infrastructure back to the attacker. While affiliate hackers claim the SunCrypt Gang retired, the sudden departure after their dispute with Twisted Spider remains suspicious.

Furthermore, Twisted Spiders and the SunCrypt Gang's data leak sites have press release pages to communicate and make announcements. Why did the SunCrypt Gang not use their press release page to announce their retirement as other attackers have done? *Figure 18* shows the last update to the press section of SunCrypt's site.



New clients

JSW Steel USA
SB Zantal Markt
Dean and Fulkerson
AGSO
Mark A. O'neal and Associates
Grushwitz
Glen Dimplex Home Appliances
Tri-signal Intergration
Visa Italia
TrustTeam

Full dumps

Dean and Fulkerson
Mark A. O'neal and Associates
Tri-signal Intergration
TrustTeam
Tug Hill Operating
FPI Management
Phillips collection

Represented here companies don't wish to cooperate with us, and trying to hide our successful attack on their resources.

Wait for their databases and private papers here.

JSW Steel USA DDOS
http://www.jswsteel.us
Read more

SB Zantal Markt DDOS
https://www.sb-zentralmarkt.de/
Read more

Dean and Fulkerson FULL DUMP (12 GB)
https://www.dflaw.com/
Read more

AGSO
https://www.agsoknokke-heist.be/contact
Read more

Mark A. O'neal and Associates FULL DUMP (3 GB)
https://www.markaoneal.com/
Read more

Grushwitz
https://www.gruschwitz.com/en/

Figure 18: SunCrypt Press release webpage on their data leak site

Historically, both groups have reputations for talking to the media. When Twisted Spider retired Maze operations, they posted a press release to their website announcing their intention. In addition to not making a press release, the gang never reached out to the media or used social media to announce retiring operations in any way. Instead, they just disappeared in their prime. The only information about their retirement comes from Kela — an Israeli cyberthreat intelligence monitoring firm — who found SunCrypt affiliates (not the core gang) who commented on an underground forum, explaining that the SunCrypt program was closing.[26]

Notwithstanding, the information comes secondhand from criminals and not the SunCrypt Gang themselves, making it hold little weight. Keep in mind; allegedly, organized crime runs the Cartel and the gangs within it. Did the gang retire, or did something else happen to lead to their sudden disappearance? Why did they not make a statement on their website's press section, as others have in the past? Why is their infrastructure live but abandoned? We will likely never know, but there is usually a reason when things don't add up.

Attack Chain

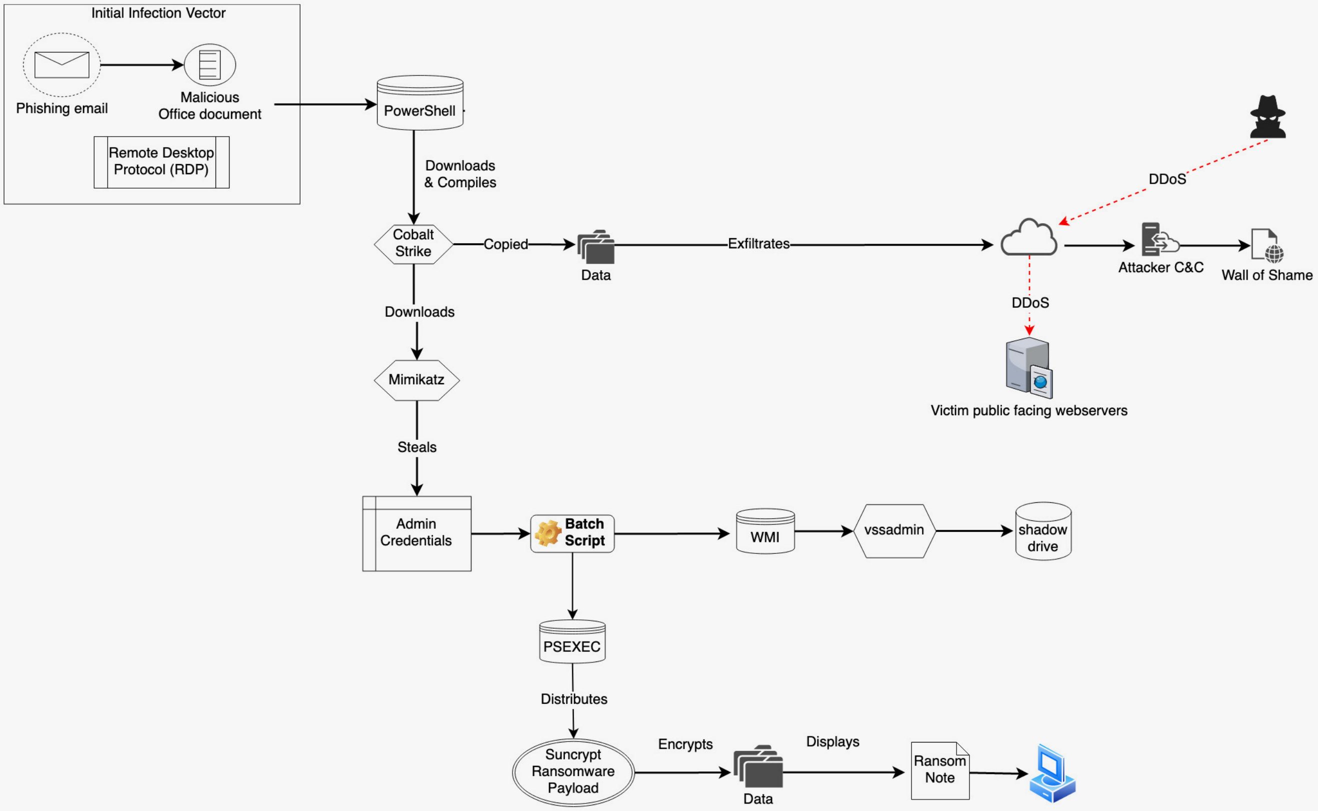
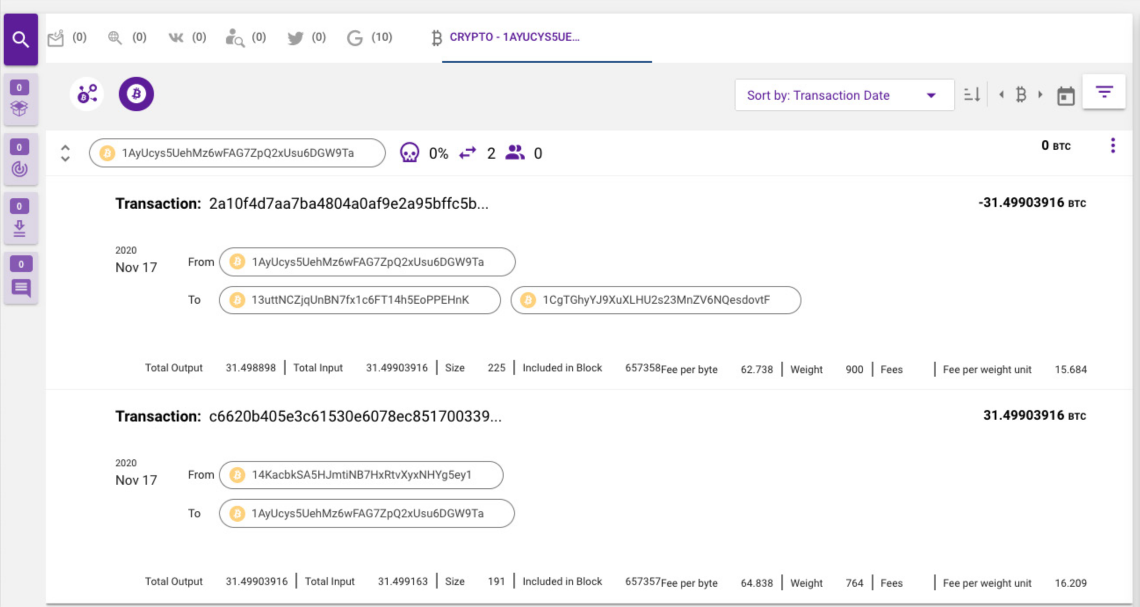


Figure 19: SunCrypt Gang attack chain

1. The attacker gains initial access by using multiple vectors. The attacker sent spear-phishing emails with malicious attachments or brute-forced RDP connections on victim infrastructure.
2. PowerShell commands issued to download and compile CobaltStrike in the memory of the infected system.
3. Next, CobaltStrike downloads Mimikatz and uses it to obtain administrative credentials.
4. The attacker copies and exfiltrates victim data.
5. A batch script is downloaded and dispersed to systems throughout the environment.
6. Scripts run, executing commands to delete shadow copies necessary for data restoration.
7. Using PSExec, the ransom payload disperses and executes to encrypt victim data
8. The payload distributes the ransom note.
9. After data theft and encryption, the attacker launches a DDoS attack against the victim's infrastructure and services, preventing them from conducting business and pressuring them to pay the ransom.
10. Posts to the the "Wall of Shame" website threaten to leak victim data. The longer the victim takes to pay, the more data the attacker leaks.

Following the payment transactions from SunCrypt operations provides insight into the revenue generated from their attacks. One of the victims made two transactions involving a SunCrypt wallet address. The first was for one bitcoin; this is typically done in attacks to validate the transaction and wallets before sending larger amounts. In the second transaction, the victim paid the SunCrypt Gang over 31 bitcoin for a total of ~$350,000 (based on bitcoin currency value at the time the attack took place).



1AyUcys5UehMz6wFAG7ZpQ2xUsu6DGW9Ta 0% 2 0 0 BTC

Transaction: 2a10f4d7aa7ba4804a0af9e2a95bffc5b... -31.49903916 BTC

2020
Nov 17
From 1AyUcys5UehMz6wFAG7ZpQ2xUsu6DGW9Ta
To 13uttNCZjqUnBN7fx1c6FT14h5EoPPEHnK 1CgTGhyYJ9XuXLHU2s23MnZV6NQesdovtF

Total Output 31.498898 | Total Input 31.49903916 | Size 225 | Included in Block 657358 Fee per byte 62.738 | Weight 900 | Fees | Fee per weight unit 15.684

Transaction: c6620b405e3c61530e6078ec851700339... 31.49903916 BTC

2020
Nov 17
From 14KacbkSA5HJmtiNB7HxRtvXyxNHYg5ey1
To 1AyUcys5UehMz6wFAG7ZpQ2xUsu6DGW9Ta

Total Output 31.49903916 | Total Input 31.499163 | Size 191 | Included in Block 657357 Fee per byte 64.838 | Weight 764 | Fees | Fee per weight unit 16.209

Figure 20: SunCrypt ransom payment in bitcoin (Constella Intelligence Hunter platform)

Of note, the attack involving this bitcoin wallet took place in September 2020, several weeks before SunCrypt ceased operations. However, the money was not moved out of the account until November 17th, almost two months after the gang disappeared. Yet another piece of evidence that does not add up.

SunCrypt Gang Group Facts

- **First known activity:** October 2019
- **Motivation:** Financial gain
- **Spoken language:** Russian
- **Names:** SunCrypt Gang
- **DLS websites:** nbzzb6sa6xuura2z[.]onion, ebwexiymbsib4rmw.onion
- **C&C:** 91.218.114[.]31, 91.218.114[.]31 (also used by Twisted Spider -Maze operations)
- **Malware:** SunCrypt ransomware
- **Ransomware extension:** Random string of characters
- **Ransom note name:** YOUR_FILES_ARE_ENCRYPTED.HTML

ANALYST1™

Cartel Assessment

Cartel Assessment

In November 2020, Twisted Spider — the gang who began the Cartel — announced that they were shutting down operations. In a further twist, they also claimed the Cartel never existed! In their last press release, Twisted Spider stated the Cartel was only real in journalists' minds. Based on the events detailed throughout this paper and the specific ties between the Cartel gangs outlined next, Twisted Spider's claims are untrue.

The initial claim the gang was retiring was misleading. The tactics used in the attacks overlap in infrastructure, and the technical similarities between Egregor and Maze ransomware made for strong attribution. Clearly, Twisted Spider was behind both operations. The second claim stating the Cartel never existed was not as clear-cut.

Twisted Spider, Viking Spider, Wizard Spider, the Lockbit gang, and the SunCrypt gang claimed they were a ransomware Cartel. Why would all of these criminal gangs speak out publicly, stating they had joined together? To further assess, Analyst1 looked to the evidence to make our own assessment.

The first tie we found provided evidence that the groups are working together and sharing resources to extort victims. Several gangs compromised and stole victim data, which they passed on to Twisted Spider. Twisted Spider then posted the victim's data and attempted to negotiate a ransom on their data leak site. This type of collaboration and sharing would not occur unless all three criminal elements had a trusted relationship with one another. *Figure 21* below is a visualization of the Ties A and B which we discuss next.

Tie A: Shared Data Leak Sites

In May 2020, Viking Spider compromised MJ Brunner of brunnerworks.com. After the compromise, Viking Spider posted Brunner's data to their leak site, ragnerleaks[.]top. A few weeks later in June 2020, Twisted Spider posted Brunner data on Viking Spider's behalf along with threatening messages to their data leak site, mazenews[.]top. Not long after, a similar situation took place. This time, the Lockbit Gang breached and attempted to extort a target: the Smith Group. At the time however, the Lockbit Gang did not have a data leak site. In a continued effort to share Cartel resources, Twisted Spider posted the stolen data to their site, mazenews[.]top, on behalf of the Lockbit gang. Furthermore, Twisted Spider referenced both the Cartel and each member gang who originally stole the data on both occasions. *Figure 22* shows the post below.

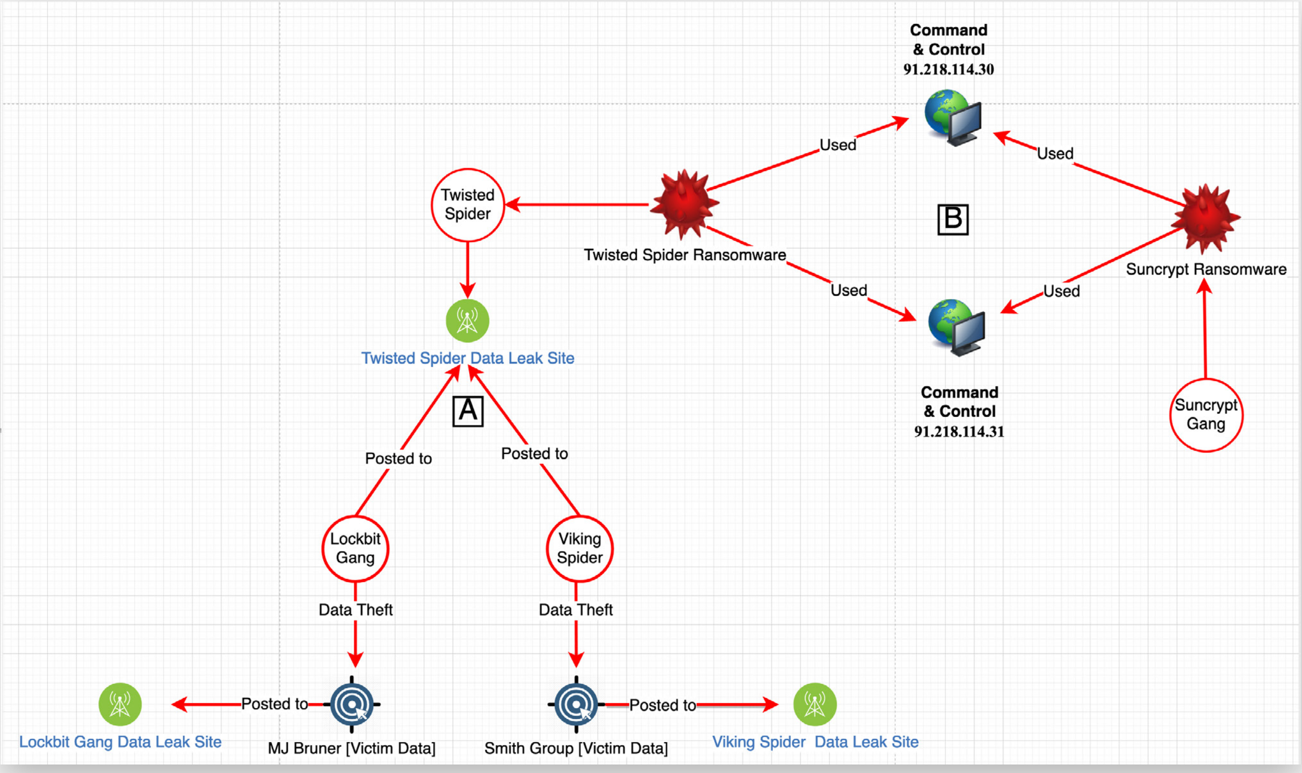
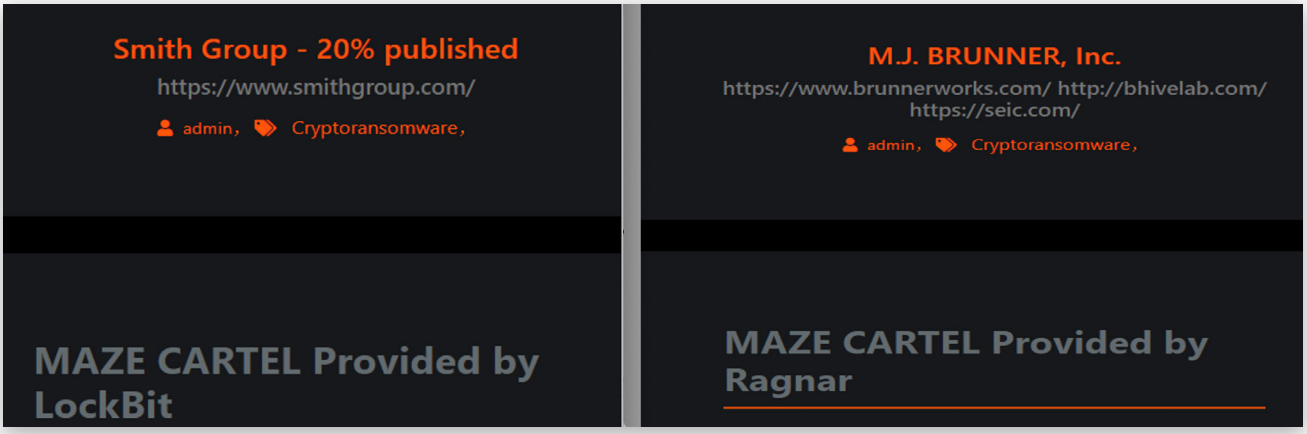


Figure 21: Cartel Ties A & B



Smith Group - 20% published

https://www.smithgroup.com/

admin, Cryptoransomware,

MAZE CARTEL Provided by LockBit

M.J. BRUNNER, Inc.

https://www.brunnerworks.com/ http://bhivelab.com/ https://seic.com/

admin, Cryptoransomware,

MAZE CARTEL Provided by Ragnar

Figure 22: Twisted Spiders data leak site, Mazenews[.]top displaying data stolen by Viking spider (Ragnar) and Lockbit gang.[27,28]

Tie B: Shared Infrastructure

We mentioned previously that the SunCrypt Gang told Bleeping Computer in August 2020 that they joined the Cartel, which Twisted Spider disputed. Yet, beginning in October 2020 in their early operations, Twisted Spider used two IP addresses, 91.218.114[.]30

& 31 for command-and-control infrastructure.[29,30] Ten months later, the SunCrypt Gang used the same IP addresses for command-and-control to deliver ransomware in their attacks. Granted, the tie would be stronger if the IP used in ransom operations took place during the same time frame. However, Twisted Spider used the 91.218.114.3X range for attacks over at least six months. The extended use and address range indicates that this was persistent infrastructure that Twisted Spider frequently used and controlled themselves. It is unlikely that the SunCrypt Gang would have access to the infrastructure if they did not have a trusted relationship with Twisted Spider. *Table 1* below details the evidence supporting Tie B.

Sha2 Hash	Ransomware	Affiliation	Date	C&C
91514e6be3f581a77daa79e2a4905dcb df6bdcc32ee0f713599a94d453a26fc1	Maze	Twisted Spider	10/2019	91.218.114.30, 91.218.114.31
E3DEA10844AEBC7D60AE330F2730 B7ED9D18B5EEC02EF9FD4A394660E82E2219	SunCrypt	SunCrypt gang	08/2020	91.218.114.30, 91.218.114.31

Table 1: Shared IP space used as C&C for both Twisted Spider and the SunCrypt gang

Other Ties:

Several other circumstantial and technical ties exist as well. These are weaker ties, and you should not use them for attribution on their own, but they are worth discussing collectively:

- Maze and Egregor ransomware (Twisted Spider) SunCrypt ransomware (SunCrypt Gang) use the Cha Cha stream cypher to encrypt data.
- All of the gangs build checks and balances into their ransomware to ensure the payload does not execute on Russian victims.
- Gangs in the Cartel share and adapt each other's tactics:
  - Double extortion technique (data theft and data encryption)
  - DDoS in conjunction with data theft and data encryption
  - Use of VM within victim environments to execute attacks and avoid detection
  - Use of data leak websites to name and shame victims
- Additionally, each gang discussed has claimed affiliation to the Cartel. Some made claims to reporters while others posted on leak sites and social media.

Closing

Analyst1 assesses that the Cartel is not an authentic entity, but instead a collective of criminal gangs who, at times, work together in ransom operations. There needs to be more than cooperation, resource, and tactic sharing between gangs for their partnership to qualify as a true Cartel, though. Profit-sharing is the primary element missing in the coalition of ransomware attackers discussed. Cartels are dangerous due to the large financial resources that profit-sharing provides.

Analyst1 researched all known bitcoin wallets and their associated transactions associated with the gangs discussed. We followed the money trail and observed examples of victims paying a gang and gangs paying their affiliates, but we did not find any evidence that the gangs share profits with other gangs in the Cartel.

We believe the gangs created the Cartel facade to appear larger, stronger more powerful to further intimidate victims into paying ransom demands. The illusion and public claims made about the Cartel achieved the desired effect; however, it also brought global attention from law enforcement and government entities. We believe this prompted Twisted Spider to lie about retiring, and this explains why they attempted to retract their Cartel affiliation. For the same reasons, Twisted Spider stopped communicating publicly, and they no longer use social media or press releases to voice their demands.

Moving forward, Analyst1 believes these ransomware gangs will continue to work with one another. The working relationship, however, will likely continue to be done behind the scenes and not on a public level. Groups will continue to share tactics and resources, making them far more dangerous than if they were operating independently. Both ransomware and malware used to gain initial compromise will increase in their levels of sophistication and capability. Specifically, Analyst1 believes ransomware gangs will focus development efforts to automate attacks. The new capabilities gangs are introducing into their ransomware demonstrate that automation is essential. Analyst1 believes this trend will continue making ransomware operations more efficient and dangerous. As automation capabilities increase, the use of affiliate hackers will decrease. This means ransomware gangs do not have to share profits with affiliates, thus increasing the revenue derived from each attack. With the decrease in the timeframe it takes to execute each attack, Analyst1 believes the overall volume of attacks will grow, raising the number of victims extorted.

Appendix

Twisted Spider IOCs

004a2dc3ec7b98fa7fe6ae9c23a8b051ec30bcfcd2bc387c440c07ff5180fe9a
0b231d592355bb443dd267b9526332955f7dd8f1bd567cd5aeb2db8628dfc523
14e547bebaa738b8605ba4182c4379317d121e268f846c0ed3da171375e65fe4
1745456c184699bba5c15966a907042c61336e1940d321bb1962e92b5481ae26
28f3f5a3ea270d9b896fe38b9df79a6ca430f5edab0423b3d834cf8d586f13e6
2d01c32d51e4bbb986255e402da4624a61b8ae960532fbb7bb0d3b0080cb9946
3aad14d200887119f316be71d71aec11735dd3698a4fcaa50902fce71bdccb07
3ae02fc1fdb653997eeb9303305f1ec35dbb87eb603b573bd94895f35542f1a8
3e5a6834cf6192a987ca9b0b4c8cb9202660e399ebe387af8c7407b12ae2da63
3fc382ae51ceca3ad6ef5880cdd2d89ef508f368911d3cd41c71a54453004c55
3fd510a3b2e0b0802d57cd5b1cac1e61797d50a08b87d9b5243becd9e2f7073f
4139c96d16875d1c3d12c27086775437b26d3c0ebdcdc258fb012d23b9ef8345
4c9e3ffda0e663217638e6192a093bbc23cd9ebfbdf6d2fc683f331beaee0321
68369e1357be3d515b5a4cd5185f5891b3314f2184ae1ce93ce6501fdc531749
6ad7b3e0873c9ff122c32006fdc3675706a03c4778287085a020d839b74cd780
765327e1dc0888c69c92203d90037c5154db9787f54d3fc8f1097830be8c76ab
7caed5f406445c788543f55af6d98a8bc4f0c104e6a51e2564dd37b6a485cc18
8d5ad342ea9fde48920a926780be432236d074d34f791b5c96ec3a418a1bbbd5
8f1005d38062f183f0d917deca0721f715e86e8ae451467ae68444a1630b582c
9017c070ad6ac9ac52e361286b3ff24a315f721f488b53b7aaf6ac35de477f44
92d72d4c1aaef1983a05bb65ee540236b98fdab4ca382d15a845ab6d07ea1fb8
932778732711cd18d5c4aabc507a65180bf1d4bd2b7d2d4e5506be4b8193596e
967422de1acc14deb7e7ce803d86aff44e2652bfcd550e3a34c2e37abc883dee
9c900078cc6061fb7ba038ee5c065a45112665f214361d433fc3906bf288e0eb
a3214d742b7b35674c549feb5984505da1b0684cbcada6dd8dc292599441430a
a376fd507afe8a1b5d377d18436e5701702109ac9d3e7026d19b65a7d313b332
a9d483c0f021b72a94324562068d8164f8cce0aa8f779faea304669390775436
aee131ba1bfc4b6fa1961a7336e43d667086ebd2c7ff81029e14b2bf47d9f3a7
b2d79fb20a243d3f5dca96fd9e70683f7c0ba1a29668c560b83a14ce4e29d479
c1c4e677b36a2ee6ae858546e727e73cc38c95c9024c724f939178b3c03de906
c3c50adcc0a5cd2b39677f17fb5f2efca52cc4e47ccd2cdbbf38815d426be9e1
ee06c557f1acd5c4948b1df0413e49f3885f8ac96185a9d986b91a1231444541
fcfaaef504de1a48e3d3952b493f154c672db7f41ee1dfc442099e5603d78ad0
49.12.104.241
91.199.212.52
185.238.0.233
217.8.117.148

45.11.19.70
45.153.242.129
49.12.104.241
91.218.114.30
91.218.114.31
amajai-technologies[.]industries
hxxp://185.238.0.233/newsvc.zip
hxxp://185.238.0.233/k071sm.exe
hxxp://185.238.0.233/b.dll
Egreornews[.]com
newsegregor[.]top
wikiegregor[.]top
egregorwiki[.]top
egregor-support[.]com
egregor[.]top
egregorsup[.]com
egregoranrmzapcv[.]onion

Viking Spider IOCs

041fd213326dd5c10a16caf88ff076bb98c68c052284430fba5f601023d39a14
1602d04000a8c7221ed0d97d79f3157303e209d4640d31b8566dd52c2b09d033
30dcc7a8ae98e52ee5547379048ca1fc90925e09a2a81c055021ba225c1d064c
3bc8ce79ee7043c9ad70698e3fc2013806244dc5112c8c8d465e96757b57b1e1
63096f288f49b25d50f4aea52dc1fc00871b3927fa2a81fa0b0d752b261a3059
68eb2d2d7866775d6bf106a914281491d23769a9eda88fc078328150b8432bb3
7af61ce420051640c50b0e73e718dd8c55dddfcb58917a3bead9d3ece2f3e929
9416e5a57e6de00c685560fa9fee761126569d123f62060792bf2049ebba4151
98d91b550f5c6bfc2b7767985071d1dfa2e39780dc41b9d9d07e5117d58a8686
9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376
afab912c41c920c867f1b2ada34114b22dcc9c5f3666edbfc4e9936c29a17a68
b670441066ff868d06c682e5167b9dbc85b5323f3acfbbc044cabc0e5a594186
c2bd70495630ed8279de0713a010e5e55f3da29323b59ef71401b12942ba52f6
ce33096639fb5c51684e9e3a7c7c7161884ecad29e8d6ad602fd8be42076b8d4
cf5ec678a2f836f859eb983eb633d529c25771b3b7505e74aa695b7ca00f9fa8
dd5d4cf9422b6e4514d49a3ec542cffb682be8a24079010cda689afbb44ac0f4
dd79b2abc21e766fe3076038482ded43e5069a1af9e0ad29e06dce387bfae900
e1957024039b0e48a15c27448f19d4df4f0e4666f9ac34e7f4d42dd3c32e15ed
ec35c76ad2c8192f09c02eca1f263b406163470ca8438d054db7adcf5bfc0597
a8ee0fafbd7b84417c0fb31709b2d9c25b2b8a16381b36756ca94609e2a6fcf6
5fc6f4cfb0d11e99c439a13b6c247ec3202a9a343df63576ce9f31cffcdbaf76
1472f5f559f90988f886d515f6d6c52e5d30283141ee2f13f92f7e1f7e6b8e9e

ragnarleaks[.]top
rgleak7op734elep[.]onion
rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd[.]onion
p6o7m73ujalhgkiv[.]onion
5.45.84.171

Wizard Spider IOCs

004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf
040fcbd360c7498756519cb0e687120bd623da80784034ea89178409491b1c44
10647257df71ea293dc1b0ac7eae8d1a50e2305469a6b0e1101a471d455385e6
198667b1eda010a431dfb051a101cc73ead1d45ba8d0f6641ec1c14bca4106f3
19fe977cbefdbffa9f61fcbf81f34177235345a2db87bfc45be62f18e770923f
2fc6d7df9252b1e2c4eb3ad7d0d29c188d87548127c44cebc40db9abe8e5aa35
3995502a85cc12c6962740989c4fb800d514bdf2ec667fdb7e4c8206adca0235
403f71c2f75573f78487e4da0a902d646c945603e7e08a792bc40d056fb01800
456dc28731284188734ef4724d38dca91dcba6c780e6268603365967522cdd6e
4594624a828fe7704559f90a45cf1db38a22ddb5e856a2003f15a3789d75e1ce
5e1cc282194aecc0e1b5841ac4c15f9b0e4fdbc3396a3b53ffdb49d537cf24d7
67abee9b578f57503efd474fe552d7c66320fb1ca45654d68d9c6f631655cd56
6d11b0f83d725b745fc10a5224ce4cb0582c7f4e912347f681f1fbe599bb5c27
8f2c2f88afa0fe046f6d7cebad058a19aa9fd2e4823496c0bc7a111010d49d3c
983c499dd64ba2067a00f8ed032b1b367b2cc191d0ab3573c766efdd656c2cf9
a5751a46768149c5ddf318fd75afc66b3db28a5b76254ee0d6ae27b21712e266
a7bff21d2695168b3f4aad1aa084f3a986d074a363ae52c7545536a98f00fe63
b800bf6f11170ff68cd552484fa144571069513adad2d75ac7462b126b5f0816
c67ba4c6e872dbcd2b1281c33fb033f886d8472ea021cf3974a445c4b804fec2
eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe
0898a80dc248a7931f8e2bf76a22a0a8d54b39a815e3fe810a2a190c50017892
23e95ba67603234352ff2864dc7fa54742f501e5922f01f8c182dbefc116f97f
27725028ff57dddea00ba8f2539b4477125ed873ee8dfde663f77b6c25914f31
330690fd9d001e63f7aa537a28d326e7ffcd61d59ba140a637337ccad1cafb52
350b0d6ae25e81c8394b119f4d569c083df8d17e6241d8efed0858cf91c745d7
41367ad447e3d86176713af7776c1ab22d5fc7fd0fe9584f14d201b9bf071700
52ea54a4b3fb594b4b99f0c209fa6917394c44fb73d4e47f0d997477044107f5
58a0a5646669443e997f88d532219141ff6c9ca8d36cd449c34a1807be919a9d
703ee3222eccd0e355b9ef414be9153fa3a2ad8efb8176fee887d7744a9f632f
7faeb64c50cd15d036ca259a047d6c62ed491fff3729433fefba0b02c059d5ed
808d0052b74dd75c087669f3e93a664e95716a3961fd70b3fd0635768a92f93c
826ab21b35cb73a12a56002c87c492d0192e85f912627e440f49e2d2777942ec
8fe01ec7a48e40dc8292e1ee22db0e59b549c46cb3163447f920a420bfb91cdd
9b4b620b78598d6c560ad5ae92f7c45eb038faae623b31ab77c009b560363c66

9eb7abf2228ad28d8b7f571e0495d4a35da40607f04355307077975e271553b8
ac9b07bd783e52e5997977617d41111849faafcbc3604f9aace2db106bf8b399
b90690767f3379633923f746abb0adf9fda6242f30f113dd23480f870d6eb09c
c96be7b8b38eef75be58ac44e9ba36b5a8dae626ceb7df5b653b1d441a10b407
d083ecc1195602c45d9cb75a08c395ad7d2b0bf73d7e70e2fc76101c780dd38f
eb0106ddaa84ba85fdaba5df923df7ecdc612a90e1268e031923266fa17eef4c
Continews[.]best
Conti[.]news
Contirecovery[.]news

Lockbit Gang IOCs

0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76
1ee1b337b902a0077b4d69f58b8a5c4e3c15e844576883e06e77a0bfdc65703e
1fae469ab79043c62b06379c6e119f602ec4ce511e85145b07f610b794e64524
21aab3925870f8e11cf4c94b9b84d252118278a50206e622b8148001e205213f
23688b5c717697159182523316838f12048fa0800bce6b6cf57b2fa3f2f614a6
2d0b775b997d1232e2d9843d593b4f7c84c3a17d5517e225bcd883968f6483e6
32a950e15ea27afe7ce87c36ea1ba807dc0f0b94712e55b27a0c57bc12c0e043
43929c8548157f399526e8318e42e34f78055b22bb4b3e6e83ab58f63d017f44
5bff8bc1a44b81f89eb5699afeb0625675570e2b6464c524d15f6c643504b0d1
70cb1a8cb4259b72b704e81349c2ad5ac60cd1254a810ef68757f8c9409e3ea6
745a79a2bce5ad44a11a08abaa0b97b6849dd82177cc0dd7365f269078f6fc2d
7ab8c20217d91760beea0884b680446f09811a8564c8b5704242447115e424a8
7d12f939d949d432042c2363e7e2997e78779cf16337a1d66de52b79f943f750
9b4e043249bd16b16f050a23794064e535e661a5514f555abd552faddb3b9f09
b65ab27749a0741982c4bc6a07a9ec24e6f66f2d60a9f9676bfddc68807360bf
b9733c8d049b907e1c3988be7e83c75d22ef060a0bd9250c430139ff0daf0883
cfa35c27600933fbc490ea2d7954f78ba565bef02588907bc16b9cb22e2875d2
e3f236e4aeb73f8f8f0caebe46f53abbb2f71fa4b266a34ab50e01933709e877
e60b8df7cd461eee3778d9f9056b062793a17caf1ab2215498740bf116269dd0
ec88f821d22e5553afb94b4834f91ecdedeb27d9ebfd882a7d8f33b5f12ac38d
f0cdae12fbd486199ce23aed579815dbe4331bd1dd8313fb3f0bc5d08f9aad5c
f36c525fb7000c90c861d52c7e81bc38ccd73adc42d9744527ddd1b05af47ca4
https://espet[.]se/images/rs35[.]png
https://espet[.]se/images/rs40[.]png
lockbit-blog[.]com
lockbitkodidilol[.]onion
Lockbit-decryptor[.]com
Lockbit-decryptor[.]top
lockbitks2tvnmwk[.]onion

Suncrypt Gang IOCs

0d7ed584dd1ae3cc071ad1b2400a5c534d19206be7a98a6046959a7267c063a1

3090bff3d16b0b150444c3bfb196229ba0ab0b6b826fa306803de0192beddb80

4b1f7e3323d797882d6082760592ea1984c29b975c1ae3c1daebf62dfb6a14e7

5bcef50ca8508939c361f0042e264f5e909ce2d8e949aa3db30fc81c1a8765b1

6672c590317da13fa55f02b73ee737091922542ce29fd0514341c7d1f27b8d68

6d39b67805c6c17ab950679e752d9a947de4e911034a1c9c63473d40b5eee21c

763b713938e62c036fa8f010cc3ac5f202be649e32a3ab5a2052da613e61643d

a52a8d8f92438bea70563f51da313f60aabd0fbbe8701a7ed4205f6f38acdf02

a9abb1e3d1060abac6830b591f2f4805b401fc4220b6f85f9ffdc7c26748e4bb

91.218.114.30

91.218.114.31

nbzzb6sa6xuura2z[.]onion

ebwexiymbsib4rmw[.]onion

Endnotes

[1] BleepingComputer. “Canon Publicly Confirms August Ransomware Attack, Data Theft.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/.

[2] BleepingComputer. “SunCrypt Ransomware Sheds Light on the Maze Ransomware Cartel.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/.

[3] BleepingComputer. “Canon Publicly Confirms August Ransomware Attack, Data Theft.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/.

[4] Coveware: Ransomware Recovery First Responders. “Egregor Ransomware.” Accessed March 26, 2021. https://www.coveware.com/egregor-ransomware.

[5] BleepingComputer. “Allied Universal Breached by Maze Ransomware, Stolen Data Leaked.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/.

[6] ComputerWeekly.com. “Maze Ransomware Attack Will Cost Cognizant at Least $50m to $70m.” Accessed March 26, 2021. https://www.computerweekly.com/news/252482950/Maze-ransomware-attack-will-cost-Cognizant-at-least-50m-to-70m.

[7] SentinelLabs. “Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone,” November 25, 2020. https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/.

[8] SentinelOne Inc. “Egregor Ransomware DFIR Analysis Report.” Accessed March 26, 2021. https://assets.sentinelone.com/labs/Egregor.

[9] Nocturnus, Cybereason. “Cybereason vs. Egregor Ransomware.” Accessed March 26, 2021. https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware.

[10] stevewhims. “BITSAdmin Tool - Win32 Apps.” Accessed March 26, 2021. https://docs.microsoft.com/en-us/windows/win32/bits/bitsadmin-tool.

[11] BleepingComputer. “Egregor Ransomware Print Bombs Printers with Ransom Notes.” Accessed March 26, 2021. https://www.bleepingcomputer

[12] Team, The CrowdStrike Intel. “Ransomware + Data Leak Extortion: Origins and Adversaries, Pt. 1,” September 24, 2020. https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/.

[13] BleepingComputer. “Ragnar Locker Ransomware Targets MSP Enterprise Support Tools.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/.

[14] ———. “Ragnar Locker Ransomware Deploys Virtual Machine to Dodge Security.” Sophos News (blog), May 21, 2020. https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/.

[15] “Ransomware Group Turns to Facebook Ads — Krebs on Security.” Accessed March 26, 2021. https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/.

[16] “Ransomware Group Turns to Facebook Ads — Krebs on Security.” Accessed March 26, 2021. https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/.

[17] Loman, Mark. “Ragnar Locker Ransomware Deploys Virtual Machine to Dodge Security.” Sophos News (blog), May 21, 2020. https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-

virtual-machine-to-dodge-security/.

18 “Conti Modus Operndi and Bitcoin Tracking.” Cybersecurity Report. Clearsky Cybersecurity & Whitestream ltd., February 2021. https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf.

19 “EmerDNS Introduction - Emercoin Community Documentation.” Accessed March 26, 2021. https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction.

20 “2020 Global Threat Report.” Cybersecurity Report. Crowdstrike, 2020. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf.

21 “LockBit Ransomware Analysis: Rapid Detonation Using a Single Compromised Credential.” Accessed March 26, 2021. https://www.darktrace.com/en/blog/lock-bit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential.

22 Gallagher, Sean. “LockBit Uses Automated Attack Tools to Identify Tasty Targets.” Sophos News (blog), October 21, 2020. https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/.

23 Gemini Advisory. “‘LockBit’ Launches Ransomware Blog, Blackmails Two Companies,” September 16, 2020. https://geminiadvisory.io/lockbit-launches-ransomware-blog/.

24 BleepingComputer. “SunCrypt Ransomware Sheds Light on the Maze Ransomware Cartel.” Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/.

25 Accessed March 26, 2021. https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/.

26 November 6, Mathew J. Schwartz• and 2020. “Data-Exfiltrating Ransomware Gangs Pedal False Promises.” Accessed March 26, 2021. https://www.databreachtoday.com/blogs/data-exfiltrating-ransomware-gangs-pedal-false-promises-p-2965.

27 Kela. “How Ransomware Gangs Find New Monetization Schemes and Evolve in Marketing,” August 25, 2020. https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/.

28 Security Intelligence. “Maze Ransomware Influenced LockBit’s New Data Leaks Website,” November 24, 2020. https://securityintelligence.com/news/maze-ransomware-influenced-lockbits-new-data-leaks-website/.

29 “Maze Ransomware.” Accessed March 26, 2021. https://www.schneiderdowns.com/our-thoughts-on/maze-ransomware.

30 “VirusTotal.” Accessed March 26, 2021. https://www.virustotal.com/gui/file/3090bff3d16b0b150444c3bfb196229ba0ab0b6b826fa306803de0192beddb80/detection.

ABOUT AUTHOR:

Jon DiMaggio, Chief Security Strategist

Jon DiMaggio is a Senior Threat Intelligence Analyst and has over 14 years of experience. He possesses advanced expertise in identifying, tracking, and analyzing Advanced Persistent Threats (APTs). Additionally, Jon speaks at national level conferences such as RSA and BlackHat. He conducts interviews based on his research with media organizations such as Fox, CNN, Bloomberg, Reuters, Wired magazine, and several others.

ABOUT US:

Analyst1, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

@UseAnalyst1 **analyst1.com/blog**

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.