FLINT.

SEKOIA.IO THREAT **INTEL**LIGENCE **FLASH** REPORT

SEKOIA.IO

TLP:WHITE

2022-039
18/07/2022

Report

Mid-2022 Ransomware Overview

Summary

SEKOIA.IO presents its Ransomware threat landscape for the first semester of 2022, with the following key points:

- Ransomware victimology - Recent evolutions
- A busy first half of the year - Several newcomers in the ransomware neighbourhood
- Cross-platform ransomware features trend
- New extortion techniques
- State-nexus groups carrying out ransomware campaigns
- Ransomware threat groups' Dark Web activities
- A shift towards extortion without encryption?

Ransomware victimology - Recent evolutions

SEKOIA.IO's monitoring service identified 1,350 publicly disclosed ransomware attacks in S1 2022, against 1067 in the same period in 2021. This 26,5% increase is not uniform over the entire period though, as shown on the graph below.

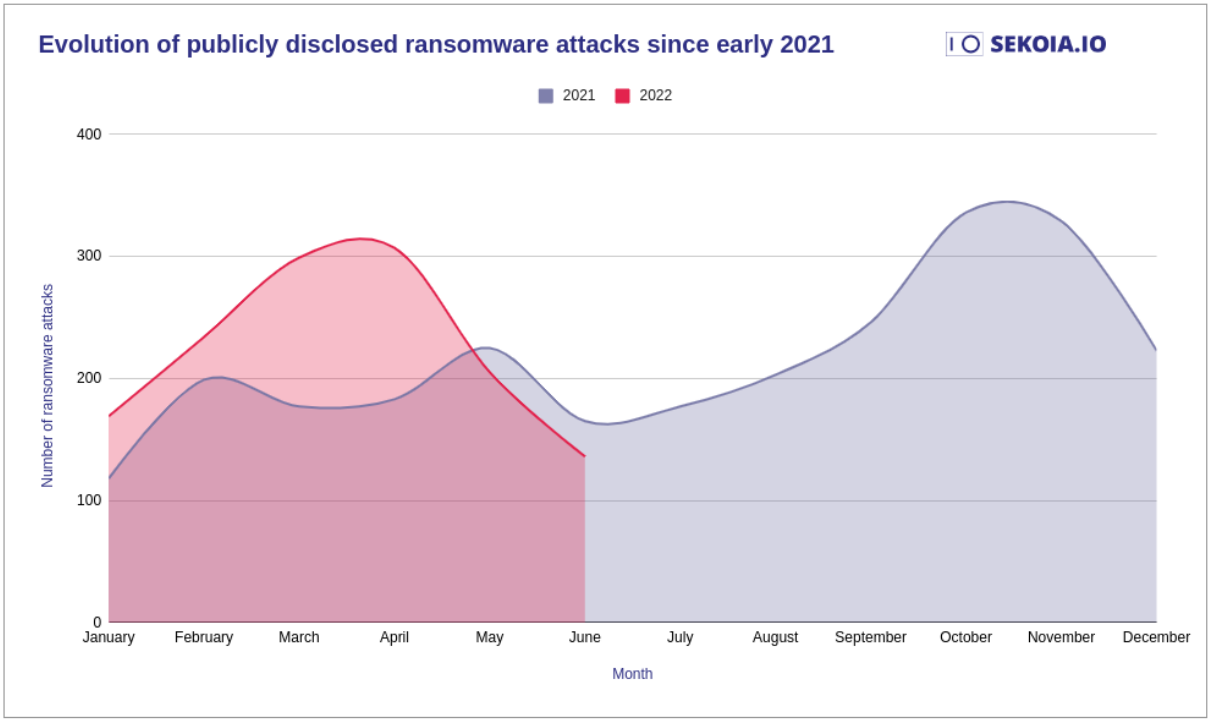

Figure 1. Evolution of publicly disclosed ransomware attacks since early 2021

SEKOIA.IO's monitoring service reported a growing number of ransomware attacks from the beginning of the year until late April 2022. This seems to reflect the natural growth of the threat, following a predominantly ascending curve of the observed number of ransomware attacks, with reduced activity during the holiday seasons twice a year. One exception would have been noted last year, where the decline around March 2021 may have been driven by some of the earlier law enforcement campaigns.

According to the director of cybersecurity at the National Security Agency (NSA), the decrease in observed attacks in May and June 2022 could be explained by the sanctions against Russia following its invasion of Ukraine. Sanctions would contribute to reducing the amount of attacks because "sanctions against Russia are making it harder for cyber criminals to organise attacks and receive ransom payments"[1], forcing them to change their TTPs and temporarily reduce their malicious campaigns' tempo. Since the statement of the NSA's director of cybersecurity is referring to sanctions against Russia, it is likely that this interpretation of decreasing ransomware activity is only valid from those ransomware operations run out of Russia.

There are likely other reasons for these variations - either situational or opportunistic.

For example, the decrease that occurred between May and June 2022 could be due to the fact that only one subset of attacks are disclosed by ransomware groups. This might lead to a significant intelligence gap between the date of the actual attack and the date it became public. For instance, the Black Basta group announced more than twenty victims at once in the beginning of July. Given the possible time gap between the two dates (encryption and start of the extortion campaign), which is different for each ransomware operation, it is likely that those victims' data was encrypted earlier, and thus this drop of the number of attacks since May 2022 has to be relativised.

[1] https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/

Out of the 32 identified active ransomware groups claiming attacks in the first half of 2022, LockBit was the most prolific one. With at least 439 reported victims, it was responsible for 32.52% of known campaigns, while the LockBit - Conti - ALPHV trio registered more than half of the victims (54,67%). Conti's last known victims date from the end of May 2022, as the group took down its attack infrastructure and its members migrated to other ransomware and/or extortion projects, such as BlackCat, AvosLocker, Hive, HelloKitty.

SEKOIA.IO assesses there is a high probability that former Conti affiliates will return to their malicious activities. This will likely push the trajectory of counted attacks upwards again in the medium term.

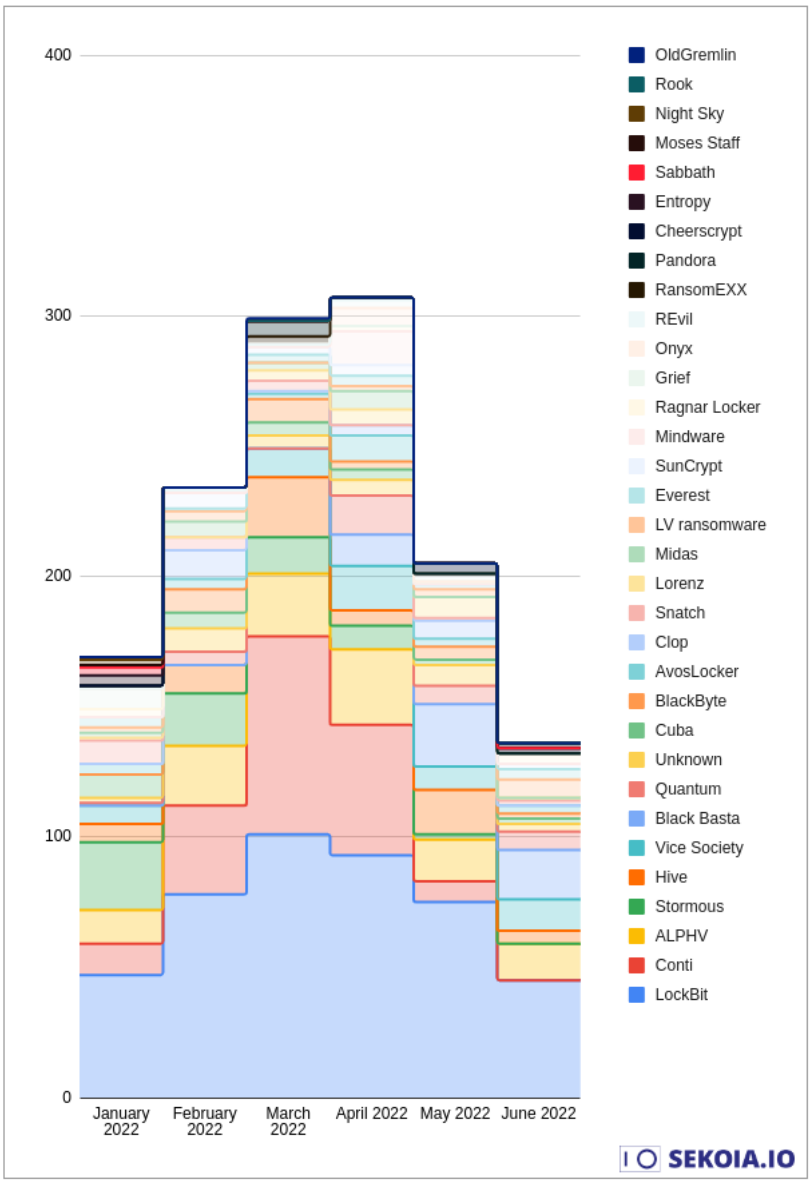

Figure 2. Publicly disclosed ransomware attacks by threat group in the S1 2022

This first semester of 2022 was marked by major events linked to the ransomware activity. Including the declaration of national emergency in Costa Rica on May 11, following a month-long ransomware attack impacting its administration , the most widely reported, and arguably most important of them.s. This campaign, both claimed by and attributed to Conti, was the first to cause such a response from a country. Another victim to experience a major impact, while not on the

same scope, was the Lincoln College in Illinois, U.S. - the first university to shut down following a ransomware attack. While it is not the first private entity to stop its activities following a cyber attack, it was a first in the educational sector, already weakened by a year and a half of Covid pandemic.

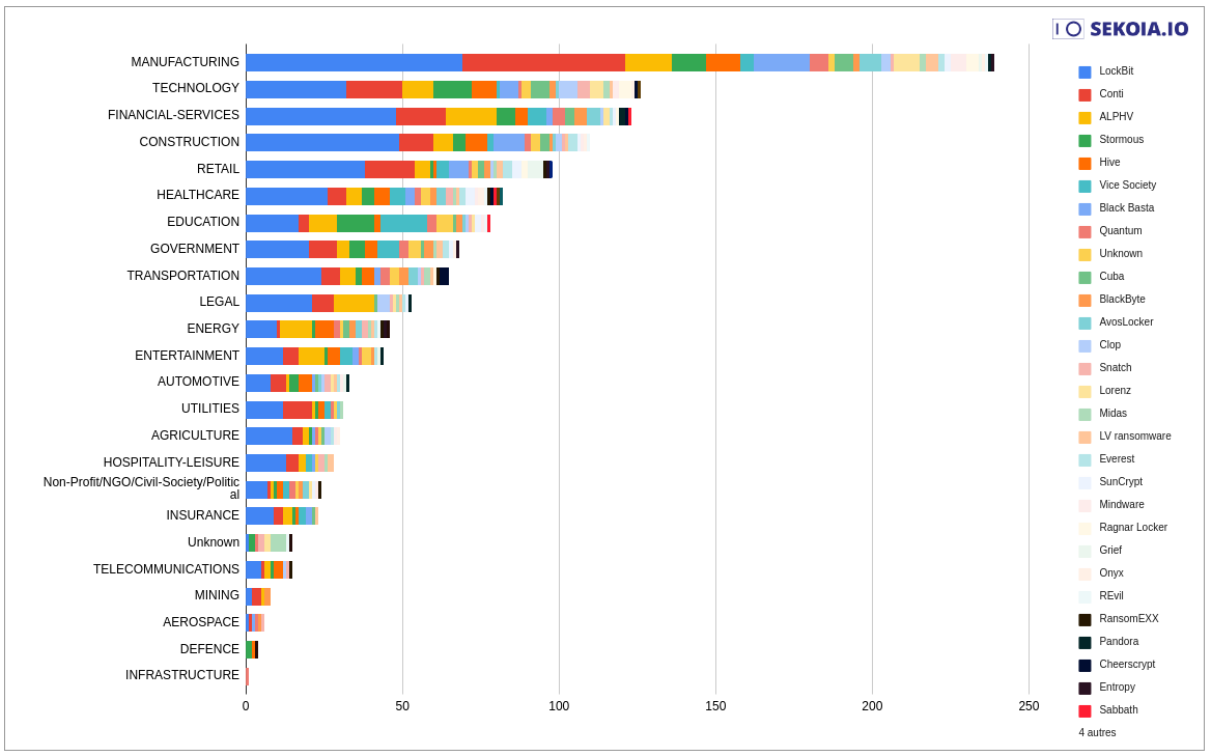

Figure 3. Industries most impacted by ransomware groups in S1 2022

More generally, the manufacturing industry was by far the most affected sector by recent ransomware attacks. Companies in this vertical must deal with multiple systems, including Operational and Information Technology networks and related equipment. By multiplying patch-management complexity and opportunities for misconfigurations, it widens their exposure to cyber threats, hence giving attackers more opportunities for intrusion. Another explanation given by IBM[2] for this higher number of ransomware attacks within this sector could be that disrupting manufacturing of goods will impact their whole customers' chain, adding pressure to quickly fix the issue by paying the ransom rather than going through a potentially lengthy recovery.

Technology and financial sectors complete the ranking of industries most affected by ransomware in 2022 so far. As more actors add extortion to their TTPs, losing innovative edge or customers' trust in their abilities to keep their data private can lead to significant reputational and financial damage.

At least 88 different countries were affected globally, with highest rates in Northern America (including 37% of disclosed victims located in the U.S.), and Europe.

[2] https://www.ibm.com/downloads/cas/ADLMYLAZ

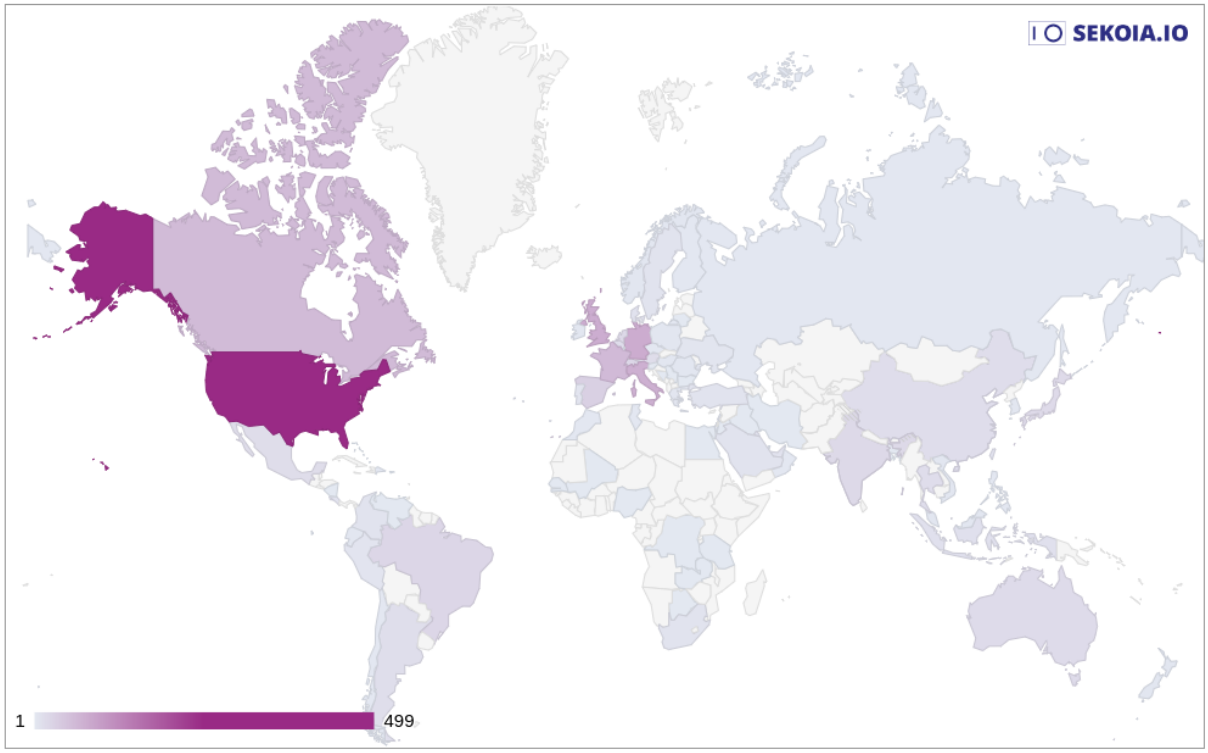

Figure 4. Countries most impacted by ransomware groups in S1 2022, by increasing number of publicly disclosed attacks

A new observation that we were able to make - the war in Ukraine put an end to the pseudo-laxity Russian entities had towards big game hunting ransomware operators. Several ransomware attacks on Russian critical infrastructure were observed in early 2022. Some of them did not demand ransom, but appeared to aim at "simply" compromising the victims' operational activities, such as the attack on Miratorg (Russia's leading meat-producer and supplier) on March 17, 2022. The incident affected at least 18 companies, all subsidiaries of Miratorg Holding. According to a Russian supervision agency, since the victim has not received any ransom note, the objective behind the attack appears to be sabotage and not financial. "It is likely that this incident reflects an information and economic "total war" launched against Russia by the Western coalition", the agency said in a statement which has since been removed from its website. This is in reference to the war between Russia and Ukraine that broke out on February 24, which significantly worsened Russia's economic and diplomatic relations with the West.

A busy first half of the year - Many newcomers in the ransomware neighbourhood

The first half of 2022 is no stranger to the appearance of new ransomware groups. No less than 20 new ransomware groups emerged between January and June 2022.

Figure 5. Some of the new S1 2022 ransomware groups and families

A couple of them are only beginning to recruit affiliates on various cybercrime forums, and do not have publicly known victims yet, such as Vandili, RTM and VulcanRansomTeam.

Some ransomware groups are suspected to be rebrands such as Axxes (from Midas, according to Cloudsek) and Pandora (from Rook, according to Cyble), or else newer variants of existing ransomware families such as YourCyanide, Yashma and Onyx. The relatively new Black Basta also raised questions among threat analysts about its potential links to another top-tier ransomware gang, namely Conti. By the way, the group uses a peculiar strategy when announcing a victim: the Black Basta operators are to leak the victim's IP addresses, hostnames, versions of the compromised hosts, as well as a list of usernames and passwords they might have used.

Several of them are modified versions from previously released source code (NB65 ransomware would be a modified version of Conti, and Nokoyawa has code similarities with both Babuk and Karma ransomware).

The newly created ransomware groups also try new ways to pressure the victims into paying: for example, LokiLocker added to its techniques the destruction of the MBR (Master Boot Record) if the victims don't pay. By doing so, the machines won't be able to start on the next boot. On another hand, the GoodWill ransomware doesn't even try to get paid and requires its victims to act for social causes while filming, recording themselves, taking photos and publishing them on social media with a dedicated description in order to receive the decryption key.

Cross platform features trend

The shift toward targeted operating systems other than Microsoft Windows increased in 2022, and could be seen as a confirmed trend that already started in previous years.

Besides Microsoft Windows, it is the Linux based operating system and especially VMware ESXi system that became increasingly targeted by ransomware actors. The RansomEXX group, for instance, acquired this capability as early as 2020[3]. Some other groups such as REvil, Conti, Black Basta, LockBit, The Hive, ALPHV developed Linux support first and then more recently the specific prerequisites for VMware ESXi. New 2022 groups such as Cheerscrypt are only focusing on the Linux environment[4].

When carrying out an attack, ransomware groups try to focus on the most valuable information in a given company: such data is frequently centralised on file servers, databases and applications servers. Some of them were reachable through the encryption of workstations and their network related connections but this could be seen as a very ineffective way of doing it. VMWare ESXi is largely used in corporate environments to virtualise these servers, and therefore became one of the most valuable targets for these groups aiming to steal or encrypt the data.

Alongside these virtualized oriented systems used in large organisations, some groups target more midsized companies (or even individuals with large scale effect) where Network Attached Storage (NAS) is the central equipment for the information. Qlocker has exploited a vulnerability on QNAP devices since 2021, and eCh0raix[5] / Qnapcrypt targets QNAP and Synology equipment as well.

Another interesting move with these ransomware malware (that could also be observed with other malware categories), for the Linux versions but not only, is the change of programming languages. Usually developed in C or C++, recent ransomwares are coded using the Go or Rust languages (ALPHV[6], The Hive[7]). Some advantages of these languages are their ease of use to build cross platform versions[8], their good performance, and secure memory management. From a code protection perspective, the defenders' capabilities (in terms of reverse engineering) are currently more limited and could increase the time spent on analysing this code and understanding the encryption mechanisms.

SEKOIA.IO confirms the observed trend of ransomware groups trying to leverage every technology increasing and protecting their attack impact wherever it is for a small or big company.

[3] https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/
[4] https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
[5] https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/
[6] https://www.digitalshadows.com/blog-and-research/alphv-the-first-rust-based-ransomware/
[7] https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/
[8] https://securelist.com/new-ransomware-trends-in-2022/106457/

New extortion techniques

Ransomware groups are constantly improving their techniques to add pressure and make the victim pay the ransom.

ALPHV/BlackCat started publishing the data they stole from a company not only on their onion leak website but also on a specifically crafted website on the clearweb, with a domain named according to the victim's name. The ransomware included a searchable form in the website, making it possible for employees or clients to directly search whether they appear in the leak. Hence, using the company name as a domain and making the website easily reachable on the internet without requiring TOR would allow anyone (employee, clients, competitor) to get the information, which can be a very efficient way to add pressure on victims.

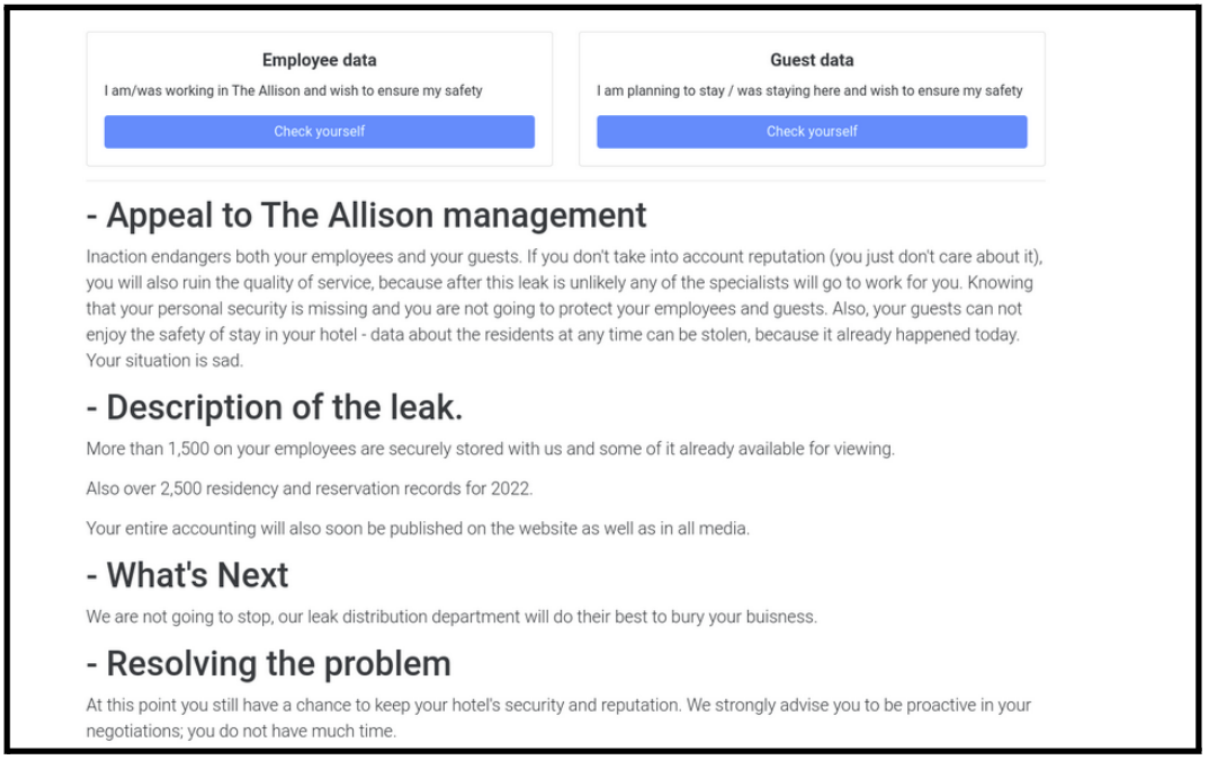

Figure 6. Home page of a website specifically crafted by ALPHV/BlackCat for one of its victim

Industrial Spy rather chose to deface the business website of its victim, thus displaying a ransom note in the website home page. This kind of defacement would have obvious consequences on the company business and reputation.

Figure 7. Industrial Spy ransom note published on the defaced website of its victim

Other observed techniques aimed at pressuring the victim's company consist in directly contacting its impacted customers, by phoning or emailing them, thus giving no chance for the impacted structures or individuals to remain in the dark regarding the leak.

This also highlights that victims have to manage crises in an absolute transparency, while ensuring a quick execution.

In the meantime, other groups, such as Lorenz and Cheerscrypt, follow a more subtle approach consisting in hiding the victim's name on their Data Leak Site[9]. This strategy aims at saving some time for the victim so it can save its reputation before it is leaked.

Figure 8. Unnamed companies displayed on Cheerscrypt's leak site

[9] https://www.bleepingcomputer.com/news/security/ransomware-gangs-now-give-victims-time-to-save-their-reputation/

State-nexus groups carrying out ransomware campaigns

Since 2020, we have observed malicious activities associated with State-nexus threat groups increasingly incorporating ransomware in their toolkit. In the first semester of 2022, state-nexus groups used ransomware in their campaigns, reminding us that traditional cybercrime actors are not the only ones to leverage it.
For example, the Bronze Starlight aka Dev-0401 China-nexus APT group, whose main motivation would be intellectual property theft or espionnage, recently added new ransomware to its arsenal. The ransomware deployed during their campaigns could be the cherry on top, disrupting their victims' IT systems, hiding the data theft as extortion and earning money.

Over time, Dev-0401 was seen deploying Lockfile, Pandora, NightSky, AtomSilo and Rook[10] ransomware after Cobalt Strike was used on the compromised hosts. The HuiLoader loaded the Cobalt Strike beacons on the compromised hosts. Each ransomware was only used in a narrow time-span, accumulating few targets. The latest ransomware to be used by the group - Pandora - mentioned at least 7 victims on its Data Leak Site in March 2022.

On another side, an Iranian APT group which Secureworks researchers refer to as COBALT MIRAGE was seen[11] conducting opportunistic ransomware for both financial gain and intelligence collection.

State-sponsored groups can disguise their data exfiltration and espionage campaigns as ransomware operations, hence exfiltrating data before encryption in order to threaten their victims with double extortion.

We can expect state-nexus groups to continue following emerging models and trends in the future, trying to hide in the masses as stealthily as possible.

Ransomware dark web related activities

Cybercrime forums and marketplaces, hosted both on the regular internet and on the dark web, are invariably a refuge for cybercriminals and other threat actors. When it comes to ransomware, the developers traditionally casted around those platforms to recruit affiliates to their RaaS (Ransomware-as-a-Service) scheme. Those cybercrime platforms also serve to sell or rent ransomware toolkits, share information, ask for support, give user reviews and so on. Multiple ransomware groups operate in collaboration with other threat actors (both individuals and organized groups) such as IABs (Initial Access Brokers), paid "pentester" affiliates and others.

Ransomware families selling RaaS to other threat actors

RaaS representatives seeking partners for their ransomware programs on the Dark Web is a pretty common and widely shared practice.

However, there was one turning point that made ransomware groups put such practice on hold and search for alternative solutions. This was the banishment in mid-2021 of ransomware-related activity on several top-tier hacking forums that used to host some of the largest ransomware gangs. The shift occurred because of the increasing and unwanted media and law enforcement attention

[10] https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
[11] https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us

on the ransomware activity in the aftermath of the Colonial Pipeline ransomware attack in May 2021, and because the different forum administrators worried about potential follow-ups reaching them too (such as major law-enforcement actions).

And yet, ransomware business renewed with this technique in 2022, and is again actively recruiting members in the classiest of ways - by launching and advertising affiliate programs on cybercriminal forums.

A very representative forum of this kind is actually RAMP (Russian Anonymous Marketplace) - founded in 2021 as a forum dedicated to ransomware activity and counting around 2500 members in July 2022. In its section called “Partners Program RaaS”, at least 10 ransomware projects were advertised since early 2022, in order to recruit members, including Monster, RTM, Luna, Avos Locker and other private RaaS groups.

Generally, such forum publications describe the functionalities of the ransomware, and also the terms and conditions of the affiliate program (especially the distribution of revenues between affiliates and ransomware developers, who are keeping between 15 and 30%). Thereafter, discussions continue through private messages on the forum or via Tox - a widely preferred instant messaging platform among ransomware actors lately.

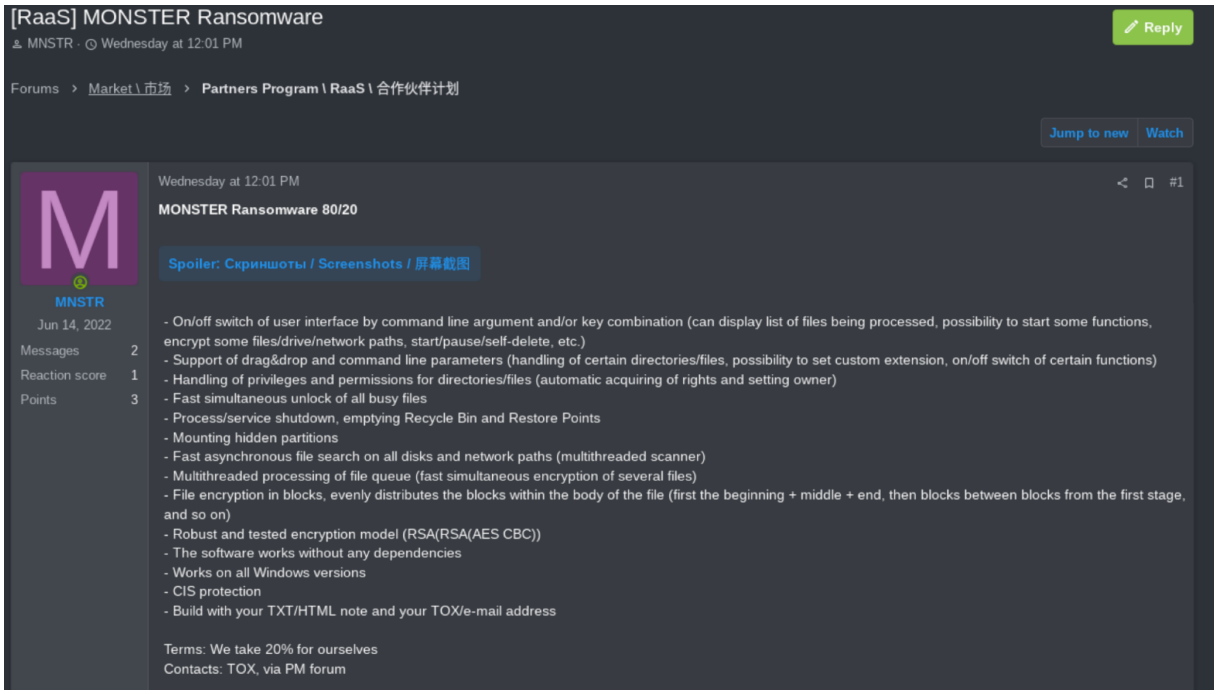

Figure 9. Example of an affiliate program advertised by the MONSTER ransomware group in June 2022

Among the various ransomware being promoted on RAMP since early 2022, the majority are prohibited from being deployed in the countries of the Commonwealth of Independent States (CIS) and are meant for Russian-speaking affiliates only (MONSTER, RTM, Conti, Luna and others).

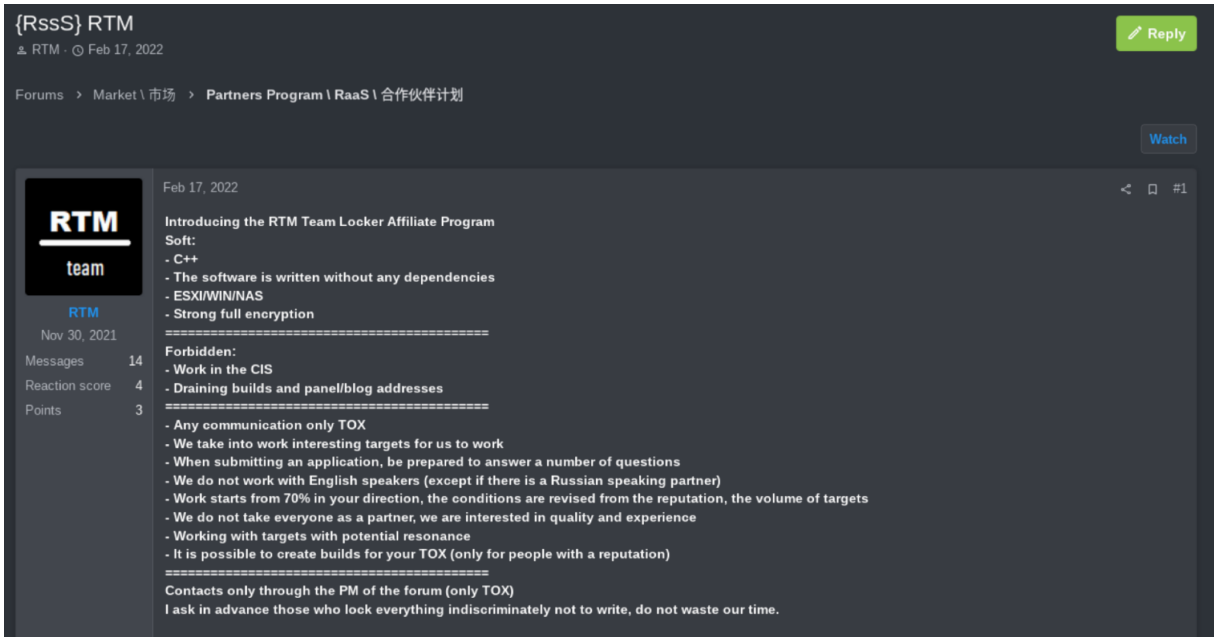

Figure 10. Example of an affiliate program advertised by the MONSTER ransomware group in June 2022

Ransomware groups looking for access

As mentioned above, there was a need in mid-2021 for ransomware groups that used to recruit affiliates via "public" affiliate programs to put that on hold for a while and so they went private (with less but more trustworthy affiliates), switched to other mediums such as websites specially designed for their project (with far less visibility), or strengthened cooperation with other specialised actors, thus reinforcing the professionalisation of the cybercrime world. This is how the behaviour of ransomware gangs on cybercrime forums evolved towards more decentralized forms of cooperation.

In 2022, ransomware groups are more than ever in close cooperation with Initial Access Brokers (IABs). Several cybercrime forums which are the most frequented by threat actors are now a highly attractive environment for matching supply with demand on the initial access market, on which ransomware actors act as access buyers.

Figure 11. (SEKOIA.IO's translation from Russian) Quake3 (a moderator of the XSS group) commenting on the positioning of the forum administration on the ransomware topic (immediate ban of the ransomware-related activities), and on the activity of the IABs ("buying networks is allowed")

Quake3 also introduces the forum member "yanluowang" as a threat actor specialized in buying

access to then deploy ransomware on compromised networks. Indeed, Yanluowang was seen operating targeted ransomware attacks since at least August 2021.

Figure 12. Example of a publication related to remote access buying by Yanluowang (SEKOIA.IO's translation from Russian)

Interaction between ransomware players and Initial Access Brokers is typically initiated through publications on cybercrime forums. Their authors are very often ransomware actors launching campaigns to acquire access by setting a per-access price and then leveraging it internally to deploy ransomware. A second option is to hire IABs as ransomware team members (either for a fixed monthly salary, or for a negotiated share of the group's revenue).

Ransomware groups looking for "pentesters"

The threat actors identified by the ransomware groups as "pentesters" are indeed affiliate partners carrying out a specific phase of the attack.

They are usually in charge of lateral movement and elevation of privileges within the victim's information system. The desired finality of the pentesters' activity would be to open up a way to implement ransomware, which will encrypt and exfiltrate the data of the victim.

These players are intervening after the initial access to a victim machine has already been reached (most often through IABs, as explained above).

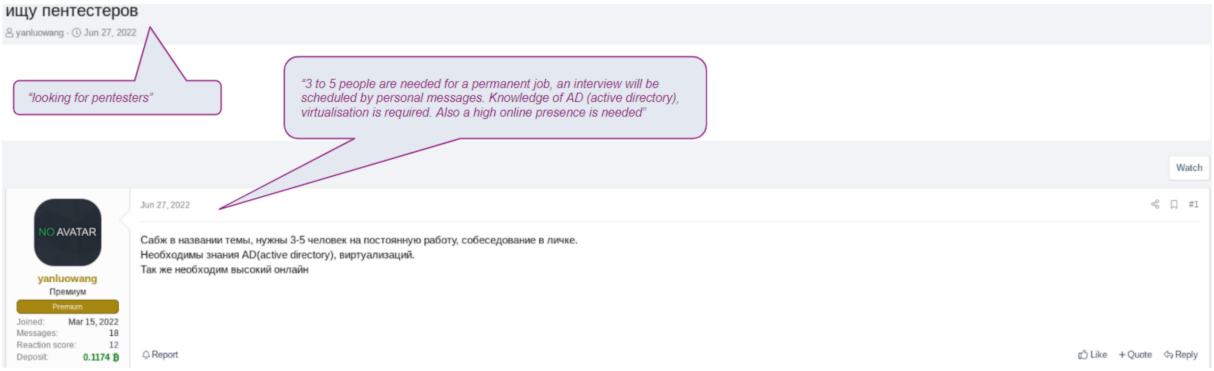

Figure 13. Example of a threat actor looking for "pentesters" to complete its team (SEKOIA.IO's translation from Russian)

On several cybercrime Dark Web forums we observe an increasing number of publications related to "pentesting" - threat actors (both individuals and organizations) providing their services, as well as threat groups aiming to hire them. We expect "pentesters" to become even more present on

underground forums and marketplaces and to be a liaison point between IABs and ransomware players.

A shift towards extortion without encryption

SEKOIA.IO has lately observed a rise of groups conducting data theft attacks without encrypting systems with ransomware, hence asking the victims to pay ransoms for preventing their data to be sold and/or leaked on specialised marketplaces and/or leak sites.

In contrast to the wildly leveraged double extortion technique, actors relying on extortion for data leaking only (rather than for data encryption) expect the data theft to be a sufficient reason prompting the victims to pay, thereby keeping the threat actors away from classical issues related to ransomware development.

In fact, many reasons can make threat actors shift to this method:

- More and more companies are realising that backing up the data is absolutely essential. Hence encrypting those systems may now have less impact. Besides, this is why ransomware threat actors actually started in 2019 exfiltrating the data to add more pressure.
- Developing its own ransomware asks for specific human and technical resources. Developers and encryption specialists have to make the encryption process efficient but also the fastest possible. However, RD is time, energy and money consuming.
- Ensuring a rapid and efficient encryption doesn't guarantee the decryption will be effective and the systems will return to an initial state. Indeed, victims reported several times they lost or saw their data being damaged after they paid the ransom and applied the decryption key. Therefore, ransomware groups also have to invest resources in ensuring a proper decryption mechanism, since many of them value the importance of their global reputation, as victims are more willing to pay if they know the group is used to properly decrypt their victim's systems.
- The RaaS system is sometimes too tremendous with multiple actors acting under the same ransomware's banner. In some cases, this led the groups to lose track of the operations that have been conducted or are being conducted. Hence, some victims have experienced being encrypted and ransomed multiple times by the same threat actor, which does not play in favour of their so-called reputation.
- For technical reasons and challenges, some ransomware operations have succeeded in exfiltrating the data, while the encryption process didn't go as expected. This highlighted their need to capitalise on the data theft with another way of asking for ransom.
- Data theft and its public disclosure is a sensitive and serious issue the victims are confronted with, and threat actors are finding more and more ways to add pressure to leverage this concern (e.g. by phoning/emailing victim's clients, defacing websites, etc.).

Therefore, exfiltrating data may ensure threat actors the same profit as both exfiltrating and encrypting the data, while getting rid of encryption challenges.

Those who made that choice tend to let aside hack and leak websites in favour of marketplaces that threat actors may set-up specifically for their groups instead of selling the stolen data in famous

and commonly used marketplaces.

For instance, Industrial Spy is one of the first half of the year's emerging groups, focusing mainly on data theft (a ransomware attack has been reported though). The stolen data is classified according to the interest of the buyers: when advertising the sale of a company's data, it is classified for seven days as premium. The threat actor says he is committed to sell it only to one buyer during this period, while this condition is not fulfilled after seven days. This strategy could pressure/encourage the victims to buy their own data within this short period of time to ensure their data to be exclusively sold back to them. This also can get the full attention of a competitor interested in buying it instead of letting it fall into the hands of other industry actors.

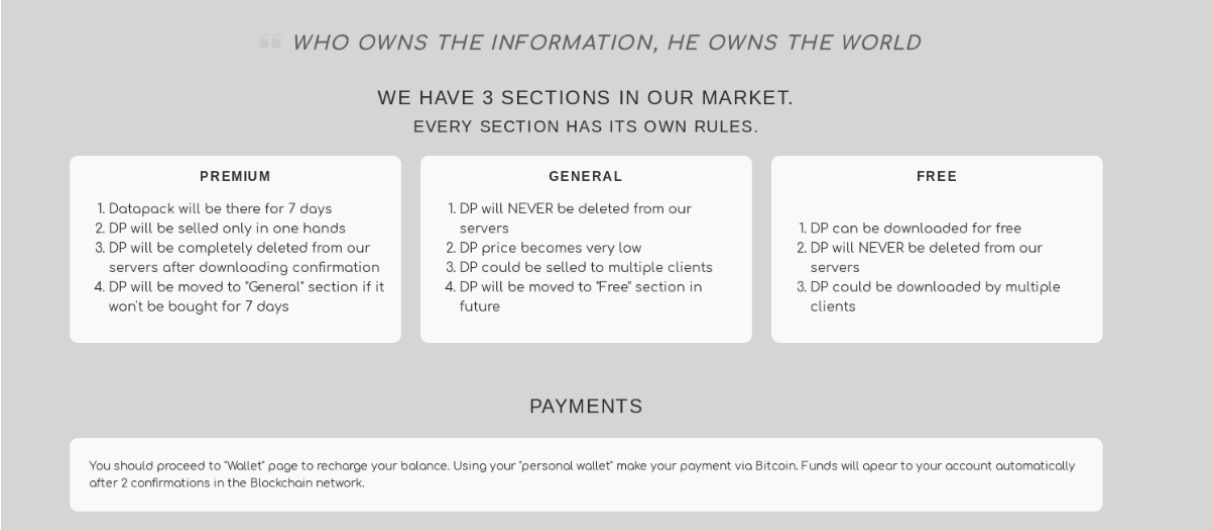

Figure 14. Industrial Spy leaks classification model

Overall, cybercrime in its entirety is constantly investing effort to renew itself by implementing new tactics and techniques to get a better profit from its operations. Hence, each year comes with a new trend that defenders have to keep a close eye on to ensure better protection.

CONFIDENCE
HIGH

REFERENCE

- SEKOIA.IO Cyber Threat Intelligence Investigation
- [ZDNet] Ransomware has gone down because sanctions against Russia are making life harder for attackers
- [IBM Security] X-Force Threat Intelligence Index 2022
- [Kaspersky] RansomEXX Trojan attacks Linux systems
- [Trend Micro] New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code
- [Unit 42] New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices
- [Digital Shadows] ALPHV: The First Rust-Based Ransomware
- [Microsoft] Hive ransomware gets upgrades in Rust
- [Kaspersky] New ransomware trends in 2022
- [Bleeping Computer] Ransomware gangs now give victims time to save their reputation
- [Secureworks] BRONZE STARLIGHT Ransomware Operations Use HUI Loader
- [Secureworks] COBALT MIRAGE Conducts Ransomware Operations in U.S.

You can now access all FLINT reports and associated IOCs
on our SEKOIA.IO Intelligence Center web portal.