Sekoia.io mid-2023 Ransomware Threat Landscape

This blog post aims at presenting an overview of the ransomware-related threat evolution in the first half of 2023. The observations and the analysis shared in this blog post focus on ransomware operations mostly impacting corporate networks in lucrative campaigns.

Overall trends related to the ransomware threat evolution

A significant increase in the ransomware threat volume and intensity

The ransomware threat landscape in the first half of 2023 was notable for its **significant growth** in the number of **active ransomware** operations, the number of **claimed attacks** and the **illicit transactions** volume.

This is highly likely the result of multiple converging factors. First, open sources report on **a record-setting number of ransomware attacks** in S1 2023. Indeed, ReliaQuest reported a number of 1,378 victims claimed on ransomware data-leak websites in the second quarter of 2023, which represents a **64.4% increase** from the record-breaking number of victims named in Q1 2023 (838 organisations), compared to 645 victims reported in Q2 2022. Similar trends were observed by Orange Cyberdefense, Talos, Intrinsec and Dragos. This is highly likely driven by the **mass adoption of the double extortion technique** by a large number of emerging ransomware groups, likely leading to a greater number of ransomware groups publicly disclosing their victims' names.

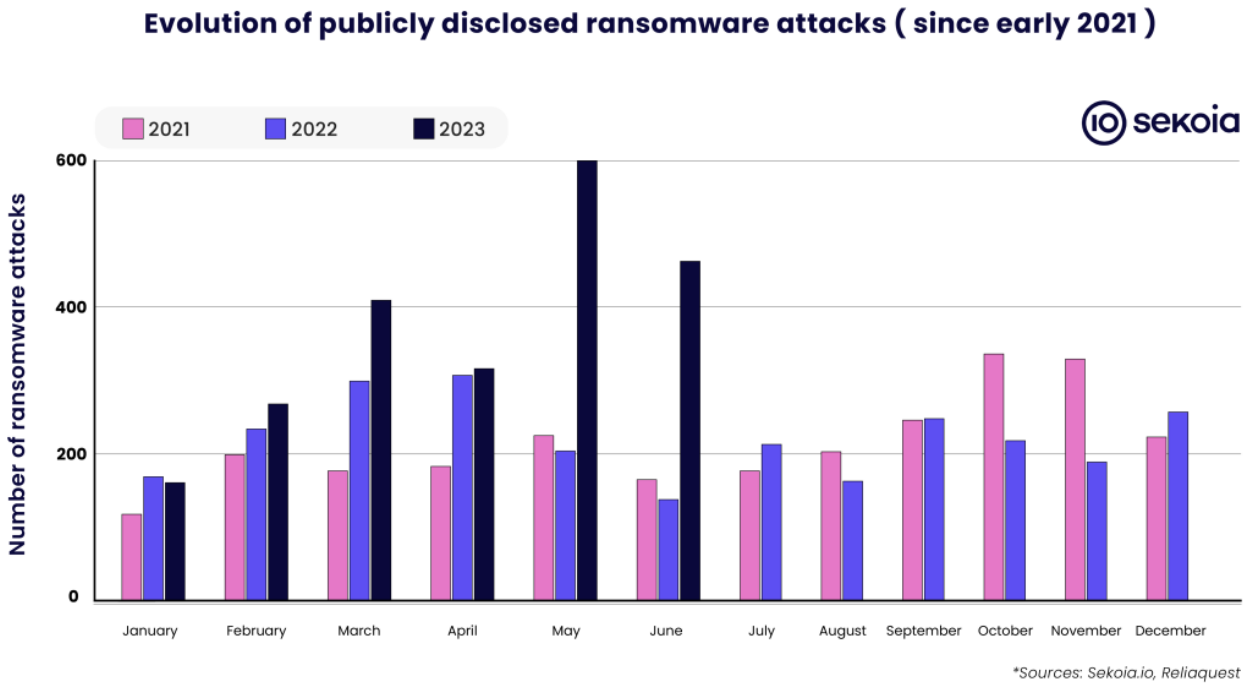

Figure 1. Evolution of publicly disclosed ransomware attacks since early 2021 (Sources: Sekoia.io, Reliaquest)

Second, while Chainalysis observed a significant decrease of 65% concerning the volumes of crypto transactions for the benefit of known illicit entities in S1 2023 compared to 2022, the **ransomware** threat is the **only form of cryptocurrency-related cybercrime to record a significant growth** of extortion revenues in 2023. Chainalysis assess this is due to both the increasing incidence of **Big Game Hunting (BGH) campaigns** with very high initial ransom demands and the proliferation of **successful small attacks**.

Third, Sekoia.io assess the reported ransomware threat increase is due to the widespread deployment of ransomware in massive campaigns of **vulnerability exploitation for initial access**, detailed in a dedicated section of this report.

Last, this growth is highly likely due to the emergence of a **growing number of new or rebranded ransomware operations**. In May 2023, Kroll already reported a **56% increase** in the number of **unique ransomware variants** observed, compared to the previous quarter. We assess this is indicative of a **highly lucrative market** and is in line with the naturally upward trend of cybercrime threats at large. Moreover, Chainalysis assess this is complementary to the **reversal of the 2022 downward ransomware trend**notably related to the Russo-Ukrainian war started on 24 February 2022. In a 2022 report, Chainalysis reported on the majority of ransomware revenues being related to threat actors or intrusion sets based in or affiliated with Russia. Thus, the war would “disrupt ransomware operators’ ability to conduct attacks or perhaps even their mandate for such attacks”. An analysis of the relaunched and emerging ransomware operations in 2023 is developed in dedicated sections of this report.

Meanwhile, Avast reported a **decrease in the absolute number of massively distributed ransomware** attacks. Avast assess this is related to ransomware operators of massively distributed malware such as WannaCry and STOP ransomware **switching to targeted attacks**.

A heterogeneous victimology

Based on Sekoia.io observations and open source reporting, **Northern America** (predominantly the United States) was the **most targeted region** in the first half of 2023. It is followed by the **Western European region** (mostly the United Kingdom, Germany, France, Italy), Brazil and Australia.

While most double extortion and BGH ransomware operations avoid conducting campaigns in the Commonwealth of Independent States (CIS) region, a growing number of ransomware campaigns conducted against Russia-based companies was reported. One such example is the MalasLocker double extortion ransomware which emerged in April 2023 asking from victims to donate to a charity instead of paying a ransom, and whose Russian-based victims account for 10,5%.

The **professional, scientific, technical services and manufacturing sectors** were reported to be the most impacted in double extortion ransomware attacks. In Q2 2023, Reliaquest highlights the attackers' **shift from the manufacturing sector** (most targeted previously) to organisations that provide **professional services** to other companies. This concurs with the Kroll reporting in Q1 2023 on a **57% increase** in the overall targeting of the professional services sector from the end of 2022, mostly propelled by ransomware attacks.

An evolving attackers ecosystem

Ransomware operators activities and motivations

Most active double extortion ransomware in S1 2023 were reported to be **LockBit**, **MalasLocker**, **BlackCat** and **8base**. Of them, MalasLocker and 8base are **newcomers** in the ransomware landscape, first reported in early 2023. Sekoia.io observed the **BlackCat** group being in **highly active development** in the first half of 2023, mostly adopting novel TTPs such as the malvertising technique for initial access and the "Bring your own vulnerable driver" (BYOVD) technique.

Besides the double extortion ransomware operations, the **most distributed ransomware in mass campaigns** were reported to be **WannaCry** (18% in Q1 2023 as per Avast) and **STOP** ransomware (15%).

Sekoia.io assess most of these intrusion sets are **financially motivated** and conduct opportunistic attacks. Yet, Microsoft reported on the intrusion set operating the Cuba ransomware continuing to be opportunistic and lucrative-oriented in its ransomware activities, but also being driven by e**spionage-related motivations** in phishing campaigns impacting defense and government entities in Europe and North America notably since late 2022.

Ransomware groups' increasing professionalisation

Since early 2023 and throughout the first half of the year, Sekoia.io observed an **active development** of monitored **ransomware operations' arsenal**. Indeed, our RaaS announcements monitoring routine led us to uncover the release of custom **cryptocurrency mixing** services (MedusaLocker, NoEscape), **DDoS** and **spam** services (Qilin, NoEscape), **call centre** services (NoEscape, Trigona, Qilin), all integrated into the RaaS kits. We assess this highlights the **increasing maturity** of the concerned intrusion sets.

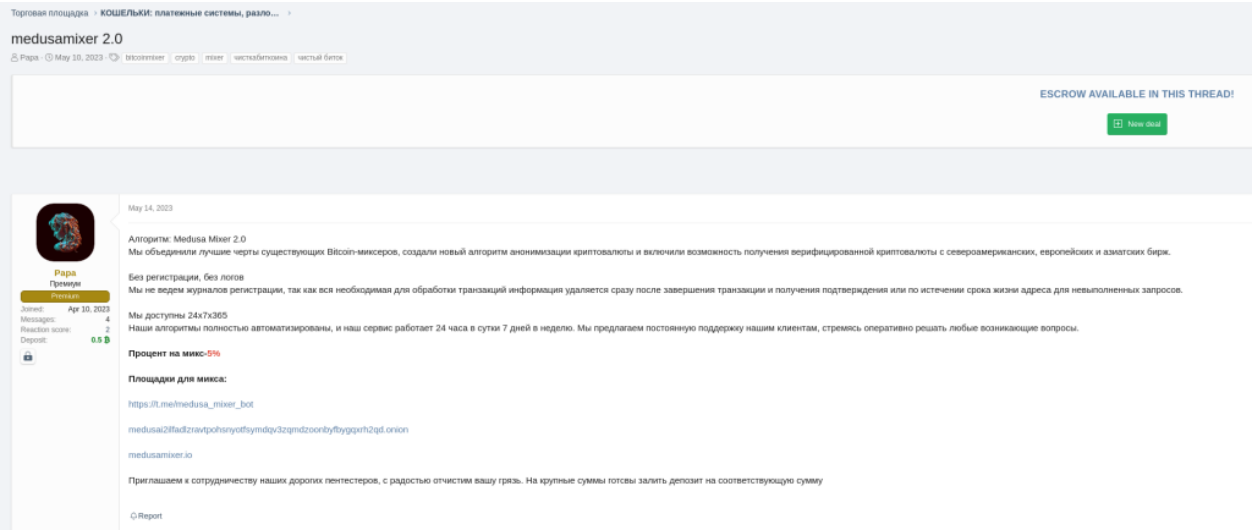

Figure 2. A threat actor that Sekoia.io assess being a MedusaLocker representative advertises the MedusaMixer 2.0 kit on the XSS cybercrime forum

Ransomware operations expanding their attack surface

Over the last few months, open sources reported a significant number of ransomware groups **adding to their attack surface Linux and VMWare ESXi servers** in addition to the traditional Windows operating system. Indeed, the **first Linux variant of Clop** ransomware, active since 2019, was reported being leveraged in a 24 December 2022 campaign. Of note, SentinelLabs released a free decryptor for this variant in February 2023. In February 2023, the **IceFire ransomware also added Linux variants** to its arsenal, one year after its Linux Windows version was first seen, as well as **RTM Locker** and the newly released **Akira** ransomware. This is in addition to the release of **ESXiArgs**, a new ransomware **specifically aimed at targeting VMware ESXi servers**, which conducted a massive encryption campaign in early 2023. This is in line with an ongoing trend established in 2022, when

emerging Linux malware recorded a 50% increase and hit record numbers compared to 2021. In addition, the emergence of numerous new ESXi-based ransomware such as **Cylance** and **Rorschach** is reported to be related to the **adoption of the leaked Babuk ransomware code**.

Sekoia.io assess with high confidence this aims at **extending ransomware's possible attack surface** to consequently expand the scope of potential victims. We assess advanced ransomware groups will increasingly add to their arsenal new variants aimed at targeting Linux operating systems. It is highly likely this trend will also be further increasingly adopted by smaller and relatively less skilled ransomware groups or individual actors, that will notably continue to reuse the leaked Babuk ransomware code. Furthermore, SentinelOne assess ransomware operators will increasingly attempt to **exploit application vulnerabilities for initial access**, as typical vectors such as phishing or drive-by download are less effective in campaigns towards Linux systems.

Ransomware groups' development of custom tooling

According to Sekoia.io observations, ransomware actors show **constant interest** in adding **custom tools and malware** to their arsenal. One such category is the **exfiltration-related** tools and malware stealing sensitive information from compromised networks, in addition to the data encryption. Additionally, Sekoia.io observed **newly launched RaaS** programs such as Cyclops **integrating a custom infostealer to the attack kit** rented to affiliates.

Besides the ransomware operations commonly using commodity infostealers, in recent months, several instances of use of **custom built data exfiltration tools** in ransomware campaigns were reported in open sources. First, the **Vice Society** ransomware group was reported deploying a custom, fully automated, **PowerShell data exfiltration script**. Of note, the technique of using custom-developed PowerShell scripts was already associated with Vice Society in the past. Second, the **Play** ransomware group recently developed [2] two proprietary data theft tools (**Grixba** and **VSS Copying Tool**). Other such examples are **Blacktail** ransomware group, first seen in February 2023, using **[1]** a custom exfiltration tool for delivering the **Buhti** ransomware.

Of note, Sekoia.io observed in the first half of 2023 a **ransomware affiliate using Exmatter** (the BlackMatter's custom data exfiltration tool). The name of victims matched victims claimed on **Lockbit**'s Data Leak Site several days later. We assess this is indicative either of ransomware groups' custom toolkit being shared or rented to other threat actors, or of affiliates distributing ransomware in the name of several groups.

The active use of custom exfiltration tools is highly likely due to the **massive adoption of the double extortion technique** by the ransomware groups the last couple of years that continues in 2023, and shows the ransomware actors' persistent interest in leveraging exfiltrated data to **maximise monetisation**. Also, it is highly likely related to the need of

bypassing existing detection solutions and **speeding up the data theft process** before encryption. We assess the development of custom-built exfiltration tools are indicative of the **increasing maturity** of ransomware groups.

Old is the new trend in town

In line with a trend already observed in late 2022, ransomware actors continued to **reuse leaked source code** of known ransomware to launch customised encryption and/or extortion operations. For instance, advanced ransomware operations launched in the first half of 2023 such as **RA Group** and **Buhti** were reported leveraging Babuk ransomware source code which leaked in June 2021.

Additionally, since early 2023, Sekoia.io observed an increasing number of ransomware emerging as variants of LockBit, Babuk or Conti, conducting **encryption-only** attacks and demanding **relatively low ransoms**. We assess with medium confidence these ransomware operators are rather relatively unadvanced **independent actors** that organised groups. While not new, this trend is highly likely indicative of the **continuous democratisation of cybercrime** and of the threat actors' **persistent interest in ransomware**-related activities.

Notable emerging ransomware

Sekoia.io assess with high confidence the increase in successful ransomware attacks mentioned above, both in BGH and in relatively small campaigns, is partly due to the **relaunch** or **emergence of multiple new ransomware operations** since early 2023.

While it is certain that new threat actors continue to join the ransomware ecosystem, a great number of emerging ransomware groups were reported to **regroup affiliates of previously existing groups** since the beginning of 2023. Indeed, **NoEscape** ransomware operation was reported to be a rebrand of Avaddon – a ransomware group that shut down in 2021. Also, **8base** ransomware operation was reported to be linked either to former Dharma and Phobos affiliates or to the RansomHouse group.

This is almost certainly evidence of a quite **closed ransomware ecosystem**, notably that of the relatively advanced intrusion sets targeting corporate assets. This concurs with the Chainalysis' assessment about a great part of known ransomware strains technically active throughout 2022 being **carried out by the same affiliates**.

Cactus

Cactus is an emerging ransomware distributed worldwide since at least March 2023. According to Coveware, Cactus entered the **Top 6 most distributed ransomware in Q1 2023**, which suggests it was actively distributed since its earliest weeks of activity.

According to our observations, the ransomware is leveraged mostly in **Big Game Hunting** (BGH) attacks, since publicly known victims are **large companies** reporting annual revenues from $11.4M to $3.4B. Companies impacted by Cactus ransomware campaigns reported major impacts such as **network outage**, **sensitive data exposure**, **disrupted operations** (delayed and canceled deliveries) and possible **stock market losses**.

The ransomware operators leverage the **double extortion** technique to put greater pressure on victims to pay the ransom, threatening to release the stolen data on the ransomware's dedicated Data Leak Site (DLS) named "Cactus Blog". As of 21 July 2023, Sekoia.io identified 18 victims listed on the "Cactus Blog" DLS. This possibly indicates the number of victims that did not meet the attackers' ransom demand.

Sekoia.io assess Cactus ransomware is an **advanced and growing threat**, due to its **unique encryption routine** and to its **novel technique to avoid detection** which consists in requiring a key to decrypt the binary for execution. In addition, the adoption of the BGH and double extortion techniques by Cactus operators are highly likely indicative of a **well structured lucrative intrusion set**.

8base

The **8base** ransomware group was unveiled in May 2023 and rapidly became one of the most active groups within the cybercrime landscape. Indeed, a significant spike in 8base activity was reported in May and June 2023, when it became the **4th most active group** by number of victims. 8base primarily targets small and medium-sized companies worldwide in double extortion campaigns. Based on claimed victimology, 8base operators highly likley conduct **opportunistic attacks**.

While the ransomware representatives claim they were operating since 2022, the double extortion operation known under the name 8base was launched in the first half of 2023. Indeed, 8base-related resources (Twitter account, Telegram channel and DLS) became active in mid-May 2023.

Sekoia.io assess the spike in the ransomware's activity starting from May 2023 is due to the simultaneous release of numerous victims attacked over a longer period of time.

We assess with medium confidence the continued high level of 8base ransomware activity in the months following its disclosure is due to the **advancement of its operators**, reportedly former members of other known ransomware groups. For instance, open sources link 8base to the RansomHouse intrusion set. In addition, it was reported that a number of 8base operators are **former affiliates of both Dharma and/or Phobos ransomware**. Coveware assess technically advanced Dharma and/or Phobos ransomware affiliates rebranded and switched to other operations due to the decreasing payment rate of their usual targets: small enterprises. This concurs with the WMare reporting on 8base as a variant of Phobos v2.9.1 ransomware.

Sekoia.io assess the 8base group will **maintain its high level of activity in the short and medium term**. It will highly likely pose an increasing threat to small and medium-sized companies due to the **mass distribution** of either its customised variant of Phobos ransomware or other available ransomware-as-a-service (RaaS).

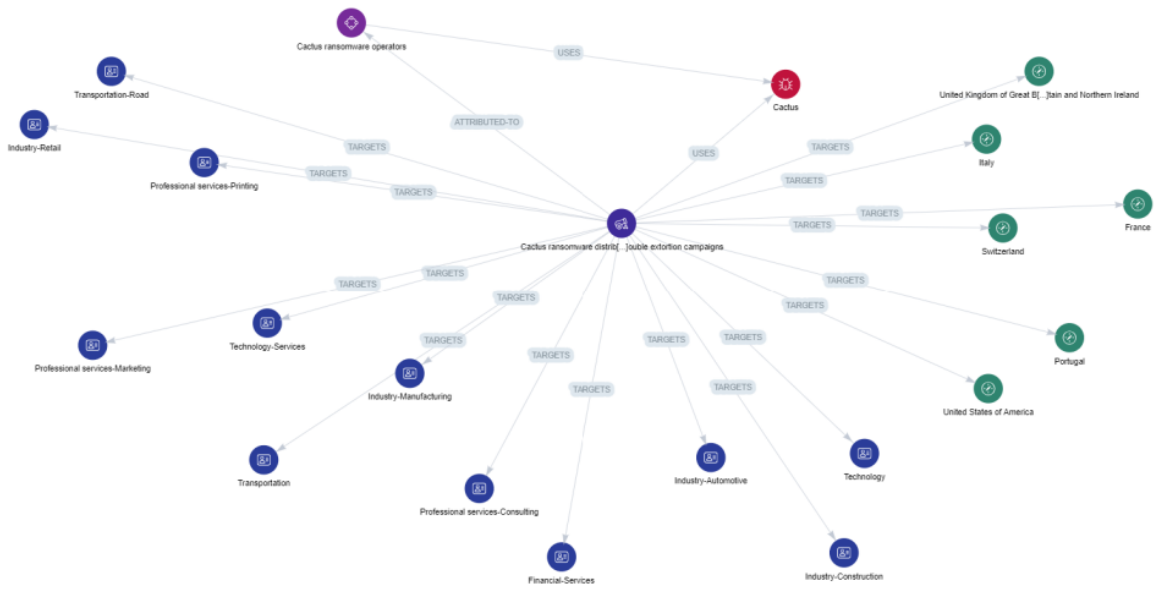

Figure 3. Cactus ransomware known victimology as of 21 July 2023

Akira

As of late June 2023, **Akira** is one of the **most active ransomware groups** since its emergence in April 2023.

The Akira operators use the same-name ransomware to perform **multi-level extortion** during their attacks towards small and medium-sized companies. Indeed, they allegedly **tailor the ransom amount** depending on what the victim intends to retrieve, i.e.:

- ransomware decryptor and full “decryption assistance”;
- evidence of victim’s data removal;
- a “report on vulnerabilities” spotted by the attackers;
- guarantees that attackers will not publish or sell exfiltrated data;
- guarantees that attackers will not attack the victim in the future.

From Sekoia.io observations, the group initially asks for **ransoms from $250,000 to $1,000,000** and then negotiates down the amount. Sekoia.io assess this is evidence of the ever **growing attackers’ interest in collecting the victim’s internal data** when conducting

ransomware attacks, as it provides additional means for maximising the impact of an intrusion and diversifying threat actors' revenues.

The group's activity is particularly busy since 21 April 2023, when Akira representatives started to publicly communicate about its victims on a Tor-based website and to **multiply the number of claimed attacks worldwide**.

Figure 4. Akira ransomware's dedicated DLS

Ransomware-as-a-Service

In Q1 2023, Sekoia.io observed tens of **RaaS recruitment publications** on cybercrime forums such as RAMP, Exploit, XSS and Breached. Ransomware operators leverage these forums mostly to **recruit affiliates** to distribute their custom ransomware, but also to **recruit partners** with specific skills, such as domain privilege escalation, likely to fill a skill gap within the group or for a short-term mission. They usually provide affiliates with an advanced post-compromise kit in exchange for a ransom payment commission.

Here are some of the **most prominent RaaS programs** launched on RAMP and XSS cybercrime forums between January and June 2023:

Ransomware operation (and ransomware representative's username)	Cybercrime forum	Some distinctive benefits for RaaS affiliates	Some distinctive requirements for RaaS affiliates
CryptNet (Shrinbaba)	RAMP	No country restrictions for targeting Provided support for negotiations 90% of every ransom payment	Highly skilled affiliates are needed
Cyclops aka Knight (Cyclops)	RAMP	Custom infostealer No restraints on affiliates' native language Automatic calculation of the ransom amount for each victim A "high commission" from ransom payments (not specified) No-deposit model. If a deposit is made, affiliates can negotiate the ransom amounts by themselves	Highly skilled affiliates are needed
NoEscape (N0_Esc4pe)	RAMP, XSS	Private chats can be created for confidential communication with recovery companies Cryptocurrency mixing service Call service, DDoS and spam services available for ransom amounts exceeding $500,000 90% of every ransom payment for ransoms exceeding $3,000,000 85% of every ransom payment for ransoms under $3,000,000 80% of every ransom payment for ransoms under $1,000,000	
Monti (Garrett)	RAMP	80% of every ransom payment Ransom payments are sent directly to the affiliate's account, by passing any processing by RaaS administrator(s)	4 affiliates only needed
Trigona (Username)	RAMP	Call service worldwide DDoS service "Access to industry journalists"	Deposit of 1 BTC on two top-tier cybercrime forums for over two years
MedusaLocker (Papa)	XSS	RaaS administrators can provide compromised initial access to victim's network if the cooperation proves successful	
Qilin aka Agenda (Haise)	RAMP	Call service, DDoS and spam services Provided support for negotiations	Highly skilled affiliates are needed Contrary to Russian-speaking affiliates, English-speaking ones are required to pay a $5,000 deposit.
Mallox (Mallx aka RansomR)	RAMP	80% of every ransom payment	

Figure 5. Newly launched RaaS in S1 2023. While MedusaLocker, Trigona and Qilin ransomware were first seen in 2019 and 2022 respectively, their RaaS programs were publicly launched in 2023

The majority of known and actively distributed ransomware that we observed launching RaaS programs on cybercrime forums in 2023 (**mostly recruiting on RAMP, XSS and Exploit forums**) are highly likely operated by **advanced intrusion sets**. Indeed, Sekoia.io observed the majority of them conducting operations against **midsize and large companies**, leveraging the double extortion technique and proving continuous evolution of their arsenal and TTPs.

Sekoia.io assess with high confidence the launchment of a public or a private affiliate program on top-tier cybercrime forums is **indicative of a ransomware group's advancement** and suggests possible growth in the number of future attacks. This is highly likely due to the scaling up of campaigns by sharing resources (malware, tools, infrastructure, compromised networks, attack manuals) within a RaaS program.

Additional criteria that could be an **indication of a highly active and expanding RaaS operation** advertised on cybercrime forums are **large forum deposits**, elective membership criteria, solid infrastructure advertised by RaaS administrators, such as extortion kits and highly configurable administration panels, as well as specific indications about the expected victims' geography, field of activity and revenue level.

It is worth mentioning that the actual number of RaaS sold on forums since early 2023 and monitored by Sekoia.io exceeds by a large margin the list above, as **a great number of threat actors advertise their affiliate programs anonymously**.

Such examples are the threat actors rtgtgth and Satana101, active on cybercrime forums in 2023. Sekoia.io assess with medium confidence these threat actors conduct recruitment campaigns of partners providing initial access or leveraging them to distribute ransomware, either for a private RaaS program or a private ransomware group of operators, without identifying themselves as a known ransomware operation representative.

Notable Tactics, Techniques, and Procedures (TTPs)

Mass vulnerability exploitation for ransomware deployment and/or data theft

Ransomware groups were reported to **increasingly exploit known or 0day vulnerabilities** in 2023. The vulnerabilities were mainly observed being exploited for initial access or access to backup/transfer servers. Indeed, we observed several ransomware and extortion groups massively exploiting vulnerabilities with automated exploits such as ESXiArgs (reported to exploit CVE-2021-21974) and TA505.

Related to the **MOVEiT** vulnerability, according to Kroll security researchers, the **TA505** threat actors started working on the creation of a fully automated exploit for more than two years prior to the massive exploitation campaign.

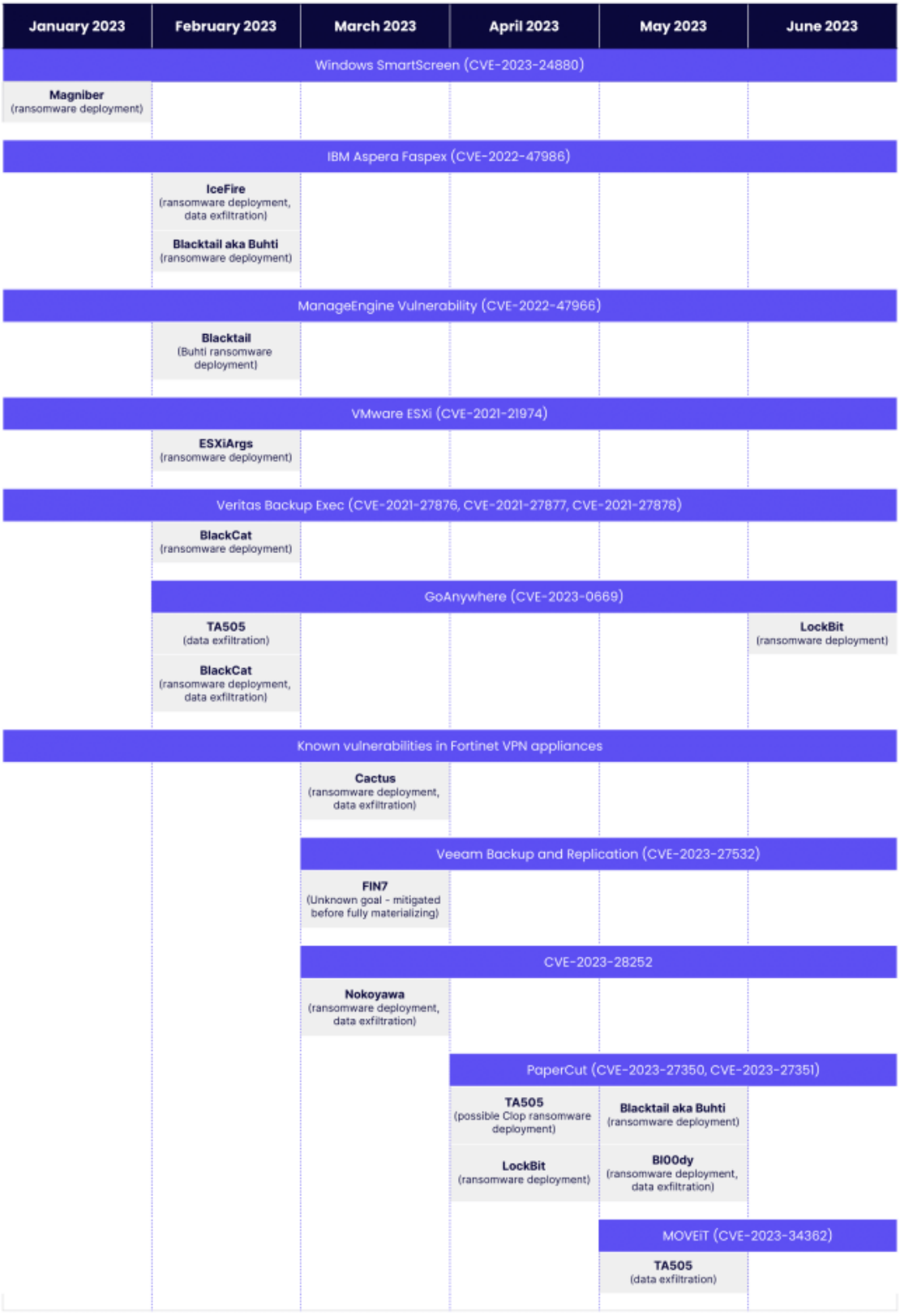

Figure 6. Vulnerabilities exploited for ransomware deployment and data theft between January and June 2023, as reported in open sources

With the opportunity to launch a fully automated exploit, the threat actor switched from the double extortion to the data theft-only extortion technique. Sekoia.io assess this is partly related to the intention to avoid encryption problems at scale. Indeed, most ransomware use symmetric encryption to encrypt files and use an asymmetric key to encrypt the symmetric key and send it to an attacker-controlled server.

Key management for hundreds of victims in a few days can become challenging and encryption problems with files still might happen. Moreover, TA505 seems to be keen on backup/file transfer servers in the first semester of 2023. Encrypting those servers might not be useful if the threat actors don't encrypt the original files, it would only slow the process and might discourage the victims to pay. In a rather contrasting way, the ESXi campaign encrypted the virtual machine files and had over 9000 bitcoin wallet addresses.

Sekoia.io assess ransomware and extortion groups will increasingly attempt to exploit known and 0day vulnerabilities for initial access, partly due to the massive impact on high-profile victims reported above mentioned campaigns.

Malvertising for initial access

In June 2023, a new infection vector was reported being adopted by the BlackCat intrusion set – the **malvertising**. Yet a common distribution method related to infostealers, several ransomware such as **Royal**, **Magniber** and **Revil** were also previously reported to be spread via malvertising.

The goal of malvertising is to promote a lookalike website of a legitimate download page for a specific tool via google/bing ads. The sponsored ads are displayed on top of search results on a search engine. Threat actors hijack this feature to make their fake websites appear before the legitimate ones in the results and increase the number of potential victims for an affordable cost.

The use of search engine ads allows the threat actors to target specific countries or regions. The tools they target to trick their victims into downloading their infected/fake ones are often administration tools, by doing so they hope to get access to enterprise networks this way. They can also look for a referrer when receiving a request to their infrastructure and filter accordingly: allow it if it comes from a google search or redirect it if it doesn't, this means it also becomes harder for security analysts to investigate the threat.

Several intrusions using this initial access vector were reported and attributed to **BlackCat** ransomware affiliates. In this campaign, the BlackCat affiliates used the **SpyBoy** terminator tool to kill security solutions. This tool, which is based on "Bring your own vulnerable driver" (BYOVD), loads a vulnerable driver into the system and use the vulnerability in the driver to get kernel access in order to kill security solutions: anti-virus and Endpoint Detection & Response (EDR) solutions.

Sekoia.io assess with high confidence the malvertising technique will be **increasingly adopted** by ransomware groups in the medium term.

Encryption-based and data theft-based extortion

A great part of newly launched ransomware groups that Sekoia.io monitors leverage the **double extortion** technique by exfiltrating data before encryption and operating a **Data Leak Site**. Of note, 30% of ransomware campaigns where data was encrypted were followed by data exfiltration, based on a survey conducted by Sophos in Q1 2023.

Here are some of the most prominent ransomware operations launching their own DLS since early 2023:

Newly launched DLS in S1 2023

January 2023	February 2023	March 2023	April 2023	May 2023	June 2023
	V is Vendetta	Abyss Locker	Akira	8Base	Cyclops
	Trigona	DarkPower	CrossLock	BlackSuit	Inc. Ransomware
		Money Message	CryptNet	DarkRace	
			RA Group	MalasLocker	
			Dunghill	NoEscape	
				Rancoz	
				Rhysida	
				Shadow	

Figure 7. Newly launched DLS in S1 2023

Of note, Sekoia.io also monitors emerging ransomware operations, such as **ARCrypter**, **RTM Locker** and **DumpLocker**, claimling to exfiltrate victim's data before encryption and threatening to sell it on cybercrime forums or to third parties instead of leaking it on a dedicated DLS.

While a growing number of ransomware groups adopt the double extortion model, another prominent ones such as BianLian were recently reported to **shift to primarily exfiltration-based extortion**. Also, Reliaquest observed a substantial increase (20 occurrences in Q2 2023 compared to only 4 in the previous quarter, but still under the number of 43 in Q4 2022) in the number of victims named on data theft extortion sites. Cisco Talos Incident Response also reported a growing number of data theft extortion campaigns in Q2 2023 that did not involve encrypting files or deploying ransomware. This is **the most-observed threat by Talos** in Q2 2023 and represents a 25% increase compared to Q1 2023.

Conclusion

The ransomware threat registered a **significant growth** in the first half of 2023 associated with the increasing number of **active ransomware operations**, the record-setting number of **claimed attacks** and the highly dynamic **illicit transactions**.

The **escalating ransomware threat** is almost certainly the result of various factors, such as mass adoption of the **double extortion** technique, the increasing incidence of **Big Game Hunting** campaigns, the proliferation of **successful small attacks**, massive campaigns of **vulnerability exploitation** for initial access, as well as to the reversal effect of the 2022 downward ransomware trend, notably related to the Russo-Ukrainian war.

Ransomware operators show **growing interest in collecting the victim's internal data** when conducting encryption. This is stressed by the growing number of emerging ransomware leveraging the double extortion technique, as well as by the increasing use of commodity and custom extortion tools by ransomware operations.

External references :

[1] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buhti-ransomware

[2] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy

Thank you for reading this blogpost. We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io

Feel free to read other TDR analysis here :

Comments are closed.