SEARCHLIGHT. CYBER

RANSOMWARE IN H1 2024

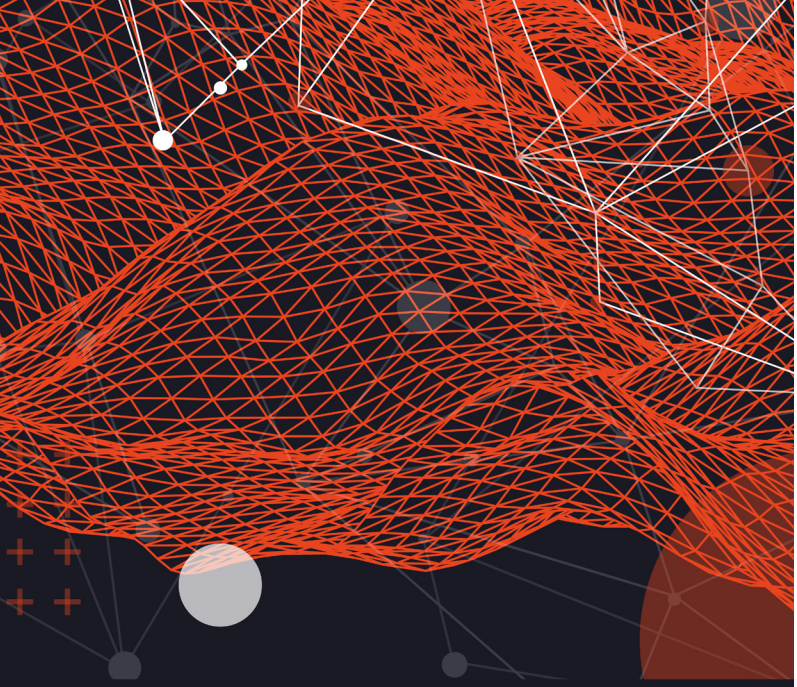
TRENDS FROM THE DARK WEB

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service Supplier



SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service *Supplier*

CONTENTS

INTRODUCTION

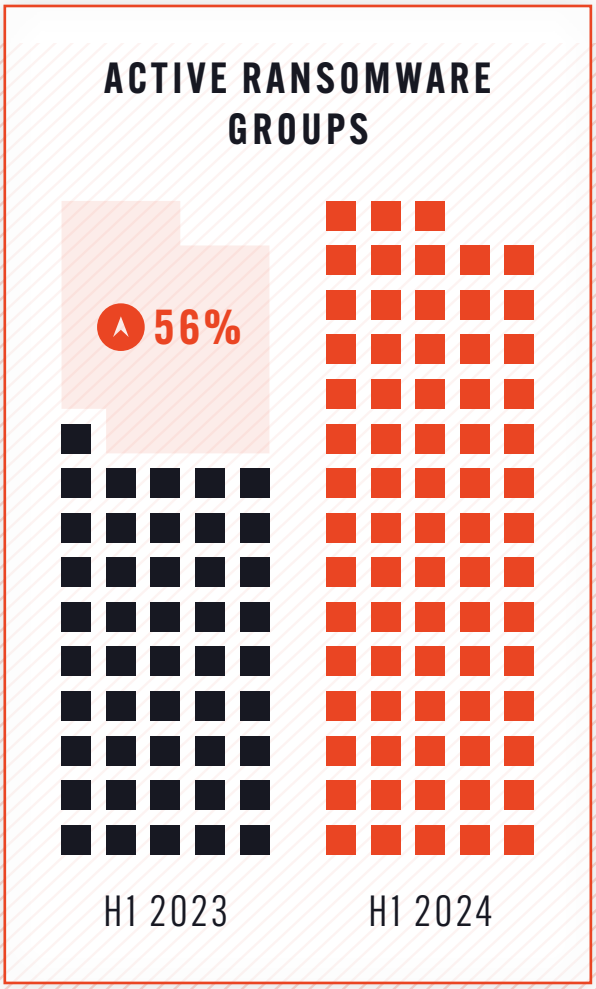
The dark web is anything but static and this is never more evident than when gathering threat intelligence on ransomware groups. Groups emerge, fight for dominance, compete among each other, disappear, and re-appear under new guises on a continual basis.

The ransomware landscape is already very different from the one that we described in our annual ransomware report[1] at the beginning of the year and we are releasing this half-year update to keep organizations abreast of the latest trends.

In this report we share our observations of one of the biggest ransomware groups closing up shop for good, a new gang emerging in February and quickly establishing itself as the third most prolific ransomware group, and - of course - some truly devastating attacks executed against organizations in the first half of this year.

While the beginning of 2024 has seen ransomware groups up to their old tricks, it has to be noted that this year has also seen one of the most major law enforcement disruptions of ransomware gangs. Operation Cronos, the huge international law enforcement operation against the LockBit ransomware group saw the utilization of new tactics to discredit the ransomware group among its peers. Although this report shows that LockBit is not out for the count, there is also plenty of evidence to suggest the group was diminished by the global disruption operation (see page 8 for more details).

Of course, these successes have not immediately led to the collapse of the ransomware underground. In fact, our statistics show that there were 73 ransomware groups in operation in H1 2024 compared to 46 in H1 2023, representing a **56 percent increase** in the number of ransomware groups.



[1] https://slcyber.io/whitepapers-reports/ransomware-in-2023/

That said, the number of listed ransomware victims in H1 2024 is down on H2 2023, which may suggest that law enforcement operations are having an effect in protecting organizations. What we could be seeing is the diversification - rather than the growth - of the ransomware scene. This hypothesis would be consistent with the fact that some of the biggest ransomware players have a clearly reduced influence, suggesting that there is no longer the “market dominance” of a small number of highly-prolific ransomware groups that there once was.

While groups and tactics change, what has remained consistent over the past several years is ransomware groups’ use of the dark web - the obfuscated area of the internet where they plan their attacks, buy access and tools, and exploit their victims.

This makes dark web intelligence an invaluable collection source for organizations looking to combat the ransomware threat. If there is one learning from this report, it is that the ransomware landscape is ever-changing. Gathering up-to-date intelligence gives organizations the best chance to identify their adversaries, understand how they conduct their attacks, and prepare their defenses for the more likely threats.

LUKE DONOVAN
Head of Threat Intelligence
Searchlight Cyber

THE MOST PROLIFIC GROUPS OF H1 2024

The first half of 2024 has seen major changes to the "league table" of ransomware groups. Some of the most prolific and established players in the ransomware scene, BlackCat and Cl0p, have exited their positions as the second and third most prolific groups, respectively.

BlackCat (also known as AlphV) retired[2] in March 2024 after executing an especially ambitious attack against the healthcare technology company Change Healthcare[3] (see RansomHub entry on page 10). This sudden retirement came just weeks after law enforcement launched Operation Cronos against LockBit and a few months after BlackCat had suffered its own disruption[4] at the hands of law enforcement, which once again suggests the impact that law enforcement action is having on the ransomware scene.

Cl0p's dark web leak site remains active but the group has not been as prolific as it was in 2023. Unfortunately, this does not mean the group has gone away for good. Cl0p's modus operandi is to use vulnerabilities (often zero days) to exploit several organizations and announce all of its victims in bulk at a later date, most recently demonstrated in its exploitation of the MoveIt vulnerability[5] in June 2023. It is probable that the group is simply conducting monitoring and reconnaissance activities for its next mass-attack.

[2] https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html
[3] https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
[4] https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
[5] https://slcyber.io/cl0p-orchestrates-mass-attack-with-moveit-transfer-zero-day/

While LockBit has retained the top spot that it has consistently owned after the last two years, it too was severely disrupted in the first half of this year by the major law enforcement disruption effort, Operation Cronos. This is reflected in the fact that its victim number has reduced from H1 2023 (see **Figure 1**).

Other groups have of course been quick to take the place of their predecessors. 8Base, BlackBasta, and Play have all been operating since 2022 but, as the ranking shows, increased their output in the first six months of 2024. However, RansomHub is perhaps the most noteworthy group in the top five, having broken into third place despite the fact the group only emerged in February of this year. As we discuss in the profiles below, this may be due to past connections with other ransomware groups.

Although the groups have changed, overarching trends have remained the same. It is noteworthy that all five of these groups are Ransomware-as-a-Service (RaaS) operations, which means that they lease out their ransomware to affiliates to conduct attacks in exchange for a percentage of the takings. This is now a very established model in the ransomware ecosystem and clearly continues to dominate among the most prolific groups.

Read on to find out what we know about the five most prolific ransomware groups of H1 2024.

POSITION	GROUP	NUMBER OF VICTIMS
~ #1 equal to position in H1 2023	LOCKBIT	↓ 434 Down 93 from H1 2023
↑ #2 Up 3 positions from H1 2023	PLAY	↑ 178 Up 59 from H1 2023
↑ #3 Unranked in H1 2023	RANSOMHUB	↑ 171 Up 171 from H1 2023
↑ #4 Up 3 positions from H1 2023	BLACKBASTA	↑ 130 Up 42 from H1 2023
↑ #5 Up 1 position from H1 2023	8BASE	↑ 124 Up 17 from 2023

Figure 1: *The top five most active ransomware groups in the first half of 2024.*

~

#1 LOCKBIT

The LockBit RaaS group was initially launched in September 2019 as "ABCD". Since then its malware has been through several iterations, including LockBit Red, Black, and Green. Its leak site "LockBit 3.0" has become infamous for its countdown timers and options for destroying or downloading stolen victim data.

LockBit has historically been a "noisy" player in the cybercriminal underground, both in its engagement on dark web forums with fans and detractors, and through its prolific output of victims. LockBit was the most active ransomware group by number of listed victims on its dark web leak site in 2022 and 2023, claiming more than a thousand victims last year alone.

This February (2024), LockBit suffered major disruption[6] at the hands of the National Crime Agency (NCA), Federal Bureau of Investigation (FBI), Europol, and other partners in "Operation Cronos". Two individuals were arrested, 28 servers were taken down, 200 crypto accounts frozen, and 1k decryption keys obtained – in addition to the seizure of LockBit's source code, infrastructure for data exfiltration, and a vast amount of intelligence.

Perhaps even more significantly, international law enforcement deployed new tactics aimed at discrediting the ransomware behemoth among its peers and affiliates. For example, defacing its iconic dark web site (**Figure 2**), leaking the usernames of LockBit's affiliates, and ultimately naming the individual they believe to be behind the moniker "LockBitSupp". On Tuesday May 7 the US Department of Justice unsealed charges[7] against Dimitry Yuryevich Khoroshev, who is subject to 26 criminal counts as well as financial and travel sanctions in the US, UK and Australia.

LockBit has proved itself stubbornly resilient in spite of this landmark law enforcement operation. It still tops the list as the most prolific ransomware group in the first half of this year, although its victim count is down on H1 2023 and aspersions have been cast on the credibility of some of its victim listings, with some evidence that the group was re-posting old victims immediately after Operation Cronos in an attempt to salvage its reputation.

[6] https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group/
[7] https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

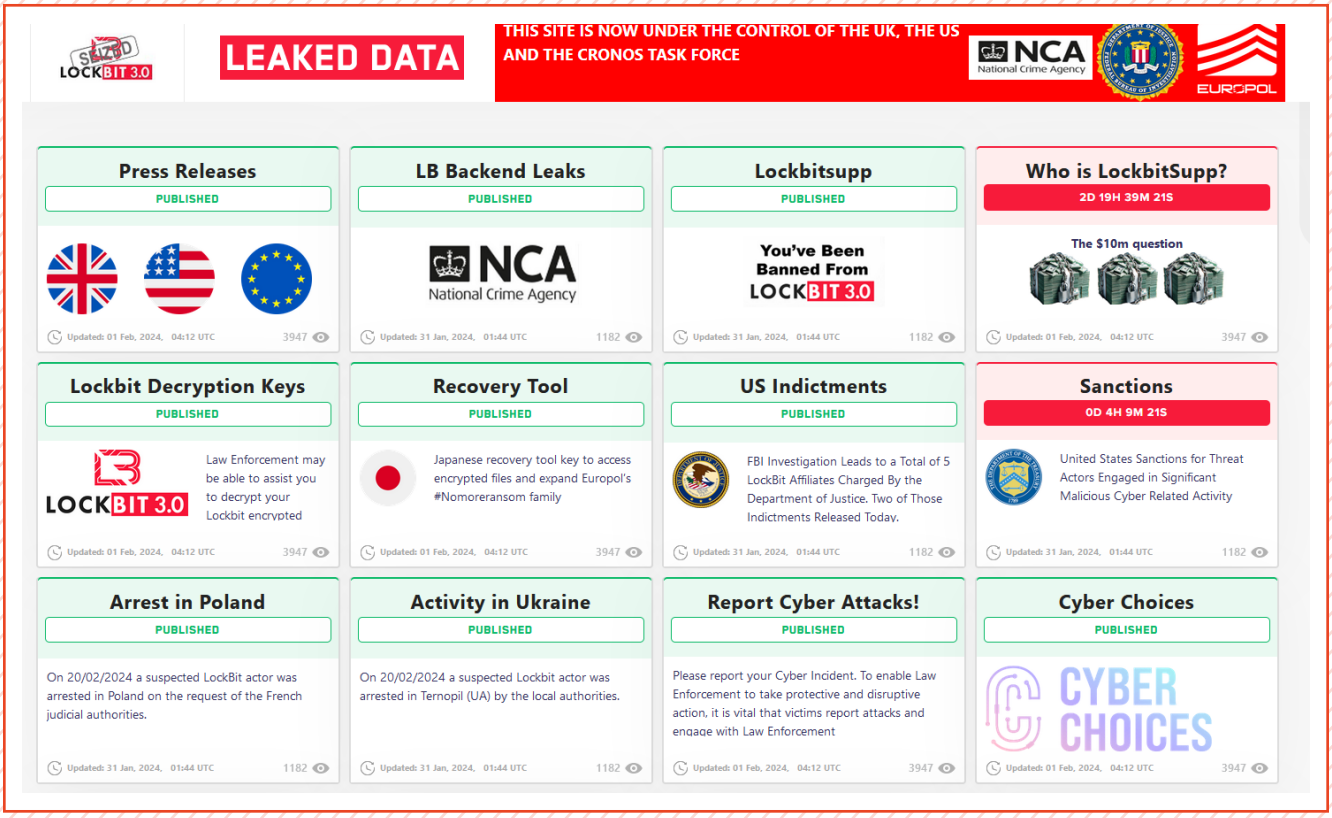


Figure 2: *A screenshot of LockBit's dark web leak site, defaced by law enforcement in February 2024 as part of Operation Cronos.*

#2 PLAY

Play ransomware has been active since June 2022 and is named after the ".play" extension it appends to the files it encrypts. It has been noted that tactics used by Play are shared by fellow ransomware operations Nokoyawa and Hive, suggesting a connection between the operations. There is also evidence that Play ransomware shares some of its infrastructure for staging attacks with the Quantum RaaS group. Play keeps a fairly low profile on the dark web aside from its leak site, not advertising itself on dark web forums. It has even claimed not to be an RaaS gang at all, saying it maintains a closed group to "guarantee the secrecy of deals", in spite of evidence to the contrary.[8]

#3 RANSOMHUB

Despite only emerging in February 2024, RansomHub has quickly become one of the most active RaaS operations we track. Its representatives have been spotted recruiting affiliates on dark web forums, offering a fixed 10 percent fee and the option to collect ransom payments directly from victims before paying the core group.

RansomHub's rapid rise to prominence can potentially be explained by links to BlackCat, an extremely prolific ransomware group that retired earlier this year after attacking the healthcare technology company Change Healthcare. It is suspected that RansomHub could contain former affiliates of the BlackCat ransomware group, especially as the group also listed[9] Change Healthcare as a victim (**Figure 3**).

Its "affiliate-friendly" model could also be seen as a direct response to BlackCat's retirement, where it is believed that the operators of the group perpetrated an "exit scam", taking the entire ransom payment from Change Healthcare without properly compensating the affiliate responsible for the attack. Most of RansomHub's victims are located in the United States.

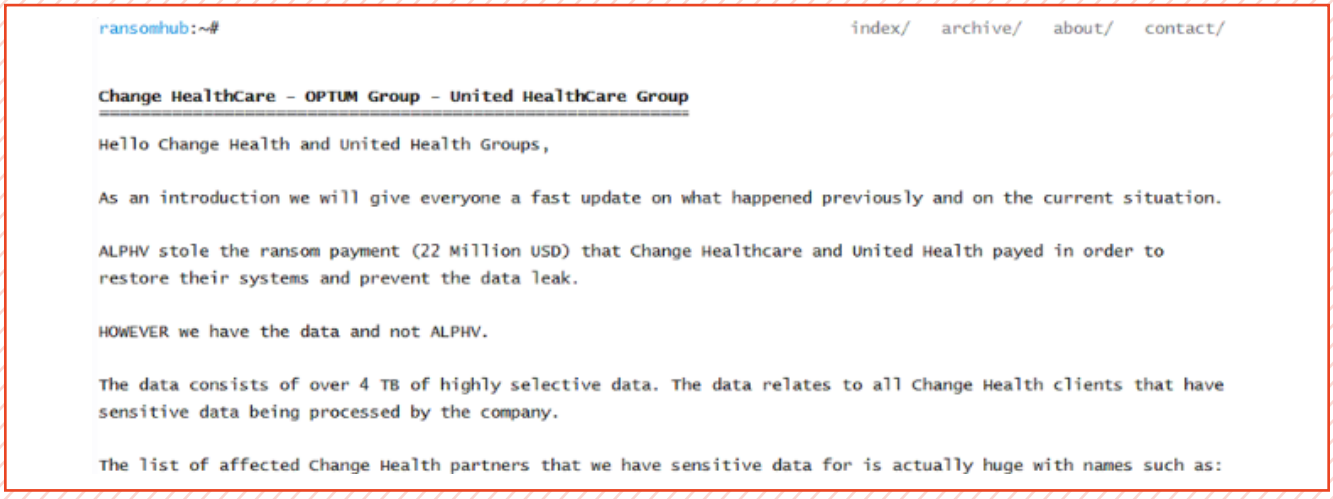


Figure 3: *RansomHub lists Change Healthcare as a victim, months after the healthcare technology company was listed by the BlackCat ransomware group.*

#4 BLACKBASTA

BlackBasta is a RaaS operation that has been active since April 2022 and is notable for its high volume of attacks, use of custom tools, and suspected links to cybercriminal group FIN7. Although it has a consistent output of high-profile victims, BlackBasta takes a relatively muted approach to communication on dark web forums.

In May 2024 the FBI, Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a joint Cybersecurity Advisory[10] (CSA) on BlackBasta, warning that the group has encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors in the US alone.

#5 8BASE

Highlighted as one of Searchlight's "ransomware groups to watch" in our report[11] at the beginning of the year, 8Base has lived up to our expectations that it would become one of the most active RaaS operations in 2024. While the group has been operating since April 2022, its victim output accelerated in the summer of 2023 and has remained consistently high since. 8Base uses a variant of Phobos ransomware in its attacks, modified to append a ".8base" extension onto encrypted files. Researchers have also noted that 8Base's leak site bears many textual similarities to the leak site used by data extortion operation RansomHouse, which might suggest a connection between the two groups.

[8] https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html
[9] https://www.infosecurity-magazine.com/news/change-healthcare-double-cyber/
[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a
[11] https://slcyber.io/whitepapers-reports/ransomware-in-2023/

NEW GROUPS TO WATCH

As discussed in the introduction, one of the most noteworthy trends in the first half of 2024 was the emergence of many new ransomware groups, which suggests a diversification of the ransomware ecosystem. In this section we profile three noteworthy groups who established their dark web leak sites this year but may go on to be the "big players" of the future.

DARKVAULT

Like APT73, DarkVault is also rumored to be a LockBit offshoot. Its appearance in February 2024 coincides with the first actions of Operation Cronos and its branding and leak site bears more than a passing resemblance to LockBit (**Figure 4**). Of course, this could also be a homage to one of the biggest ransomware operations of all time or a cynical attempt to hijack another ransomware group's brand recognition. DarkVault targets organizations across various countries and industries, which suggests it could be a RaaS group, although this is yet to be confirmed by the cybersecurity industry.

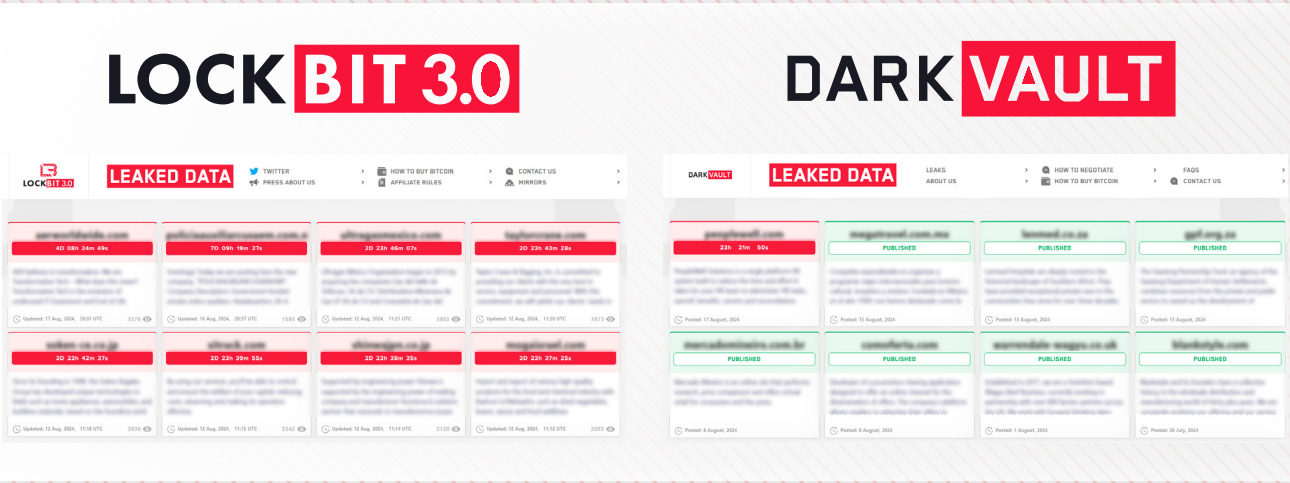


Figure 4: *A side-by-side comparison of the logos and leak sites of DarkVault and LockBit.*

[12] https://www.mandiant.com/resources/insights/apt-groups
[13] https://www.darkreading.com/threat-intelligence/sexi-ransomware-rebrands-maintains-original-methods-of-operation
[14] https://www.computerweekly.com/news/366589583/Qilin-ransomware-gang-publishes-stolen-NHS-data-online

APT73

APT73 appeared in April 2024 and is speculated to be an offshoot of LockBit. There is no conclusive evidence so far that it is a RaaS operation but the group is relatively unique in the ransomware world for having both a dark web and a clear web leak site. While this is not the first time a ransomware group has created a clear web site (both BlackCat and Cl0p have experimented with clear web sites in the past), ransomware operators typically stick to the dark web to reduce the likelihood of law enforcement identifying the actors behind the group. The potential benefit of a clear web site is that the ransomware group can shame its victims more widely, thus applying increased pressure to pay the ransom, although it is a higher-risk strategy.

One interesting aspect of APT73 is its name, which almost certainly refers to the naming convention of Mandiant, a cybersecurity vendor. The acronym "APT" refers to Advanced Persistent Threat Groups[12], sophisticated cybercriminal gangs that Mandiant has determined as being state-backed, with each group classified with a number. By naming itself APT73, which is not an official APT designation, it is possible that the ransomware group is trying to bolster its prestige and suggest a level of sophistication beyond simply being a financially-motivated group. Interestingly, another ransomware group formerly known as SEXi Ransomware has also recently rebranded itself[13] as APT Inc.

QUILONG

The ransomware operation Quilong first emerged in April 2024 and is not a RaaS group. Its status as a closed group is evident in its victimology, which shows clear targeting of organizations in Brazil, primarily in the healthcare industry. RaaS operations rarely have this level of consistency in targeted geographies and industries, as each affiliate will have its own methodologies for selecting victims. Quilong's focus on Brazil suggests the group is also based in the region.

There is also a noteworthy branding quirk with Quilong, who has chosen the name of a Chinese dragon. Like the appropriated use of "APT", the use of Chinese mythical creatures appears to be a current naming trend in the ransomware ecosystem, with the Qilin ransomware group (who made a name for themselves in the June attack[14] on healthcare supplier Synnovis) also being named after a unicorn from Chinese legend.

It is worth noting that at the time of writing this report, the ransomware group's dark web leak site is offline. We have included the group as it was influential in the first half of the year.

CONCLUSION

Dark web intelligence from the first half of this year indicates a growing number of ransomware groups, which means a more complex landscape for cybersecurity professionals to navigate.

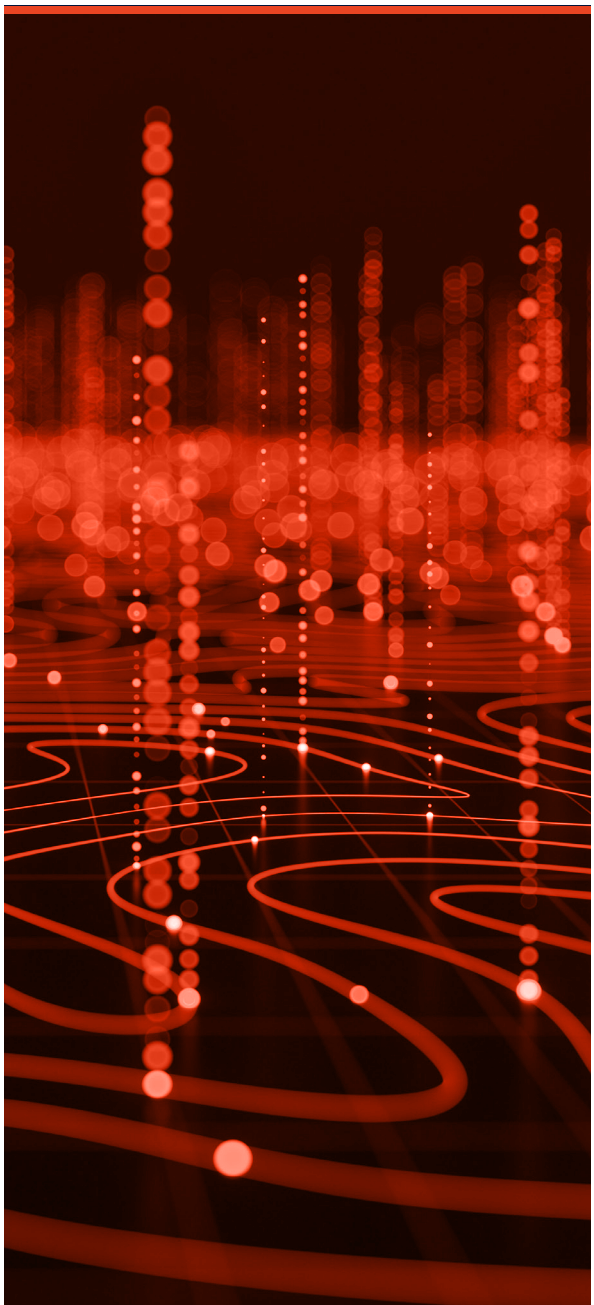
Although some of the big players have been disrupted, we should be under no illusions: ransomware remains a persistent threat. Security professionals therefore need to find ways to continuously monitor the ransomware ecosystem, identify the groups that pose the greatest risk to them, and use threat intelligence to inform their defensive strategies.

Gathering threat intelligence from dark web forums and ransomware leak sites can help organizations to quickly narrow down the ransomware groups that pose the greatest threat to them and - importantly - their suppliers.

If you are an energy company based in the United States, BlackBasta's focus on Critical National Infrastructure warrants further investigation. If you are a healthcare company in Brazil, monitoring Quilong should be considered high priority.

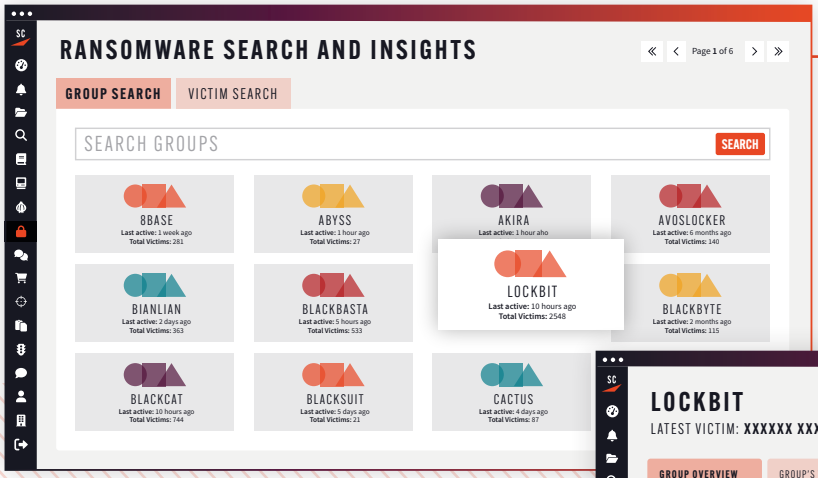
Dark web intelligence can then be used in combination with other sources to understand the tactics, techniques, and procedures of the group, so that defensive decisions can be made accordingly and ransomware groups can be stopped in their tracks.

> **ALTHOUGH SOME OF THE BIG PLAYERS HAVE BEEN DISRUPTED, WE SHOULD BE UNDER NO ILLUSIONS: RANSOMWARE REMAINS A PERSISTENT THREAT.**



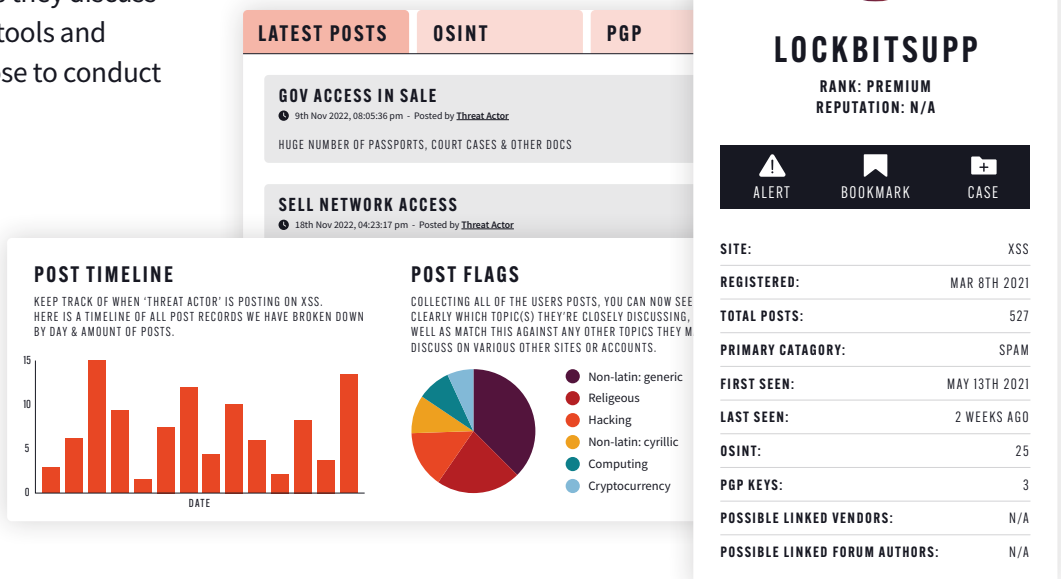
ABOUT RANSOMWARE SEARCH AND INSIGHTS

Our Ransomware Search and Insights module allows security professionals to monitor the dark web activity of more than 50 ransomware groups through one intuitive dashboard.



Select the ransomware group you want to find out more about and interrogate the group's activity with the ability to break down the data by industry and geography.

Pivot on the actors behind the group to view their activity on dark web forums including their connections with other cybercriminals, the tactics they discuss on the dark web, and the tools and vulnerabilities they purpose to conduct their attacks.



VISIT **WWW.SLCYBER.IO** TO FIND
OUT MORE OR BOOK A DEMO NOW.

SEARCHLIGHT CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
200 Massachusetts
Avenue Northwest,
Washington, DC 20001
United States