SEARCHLIGHT CYBER

SAME GAME, NEW PLAYERS

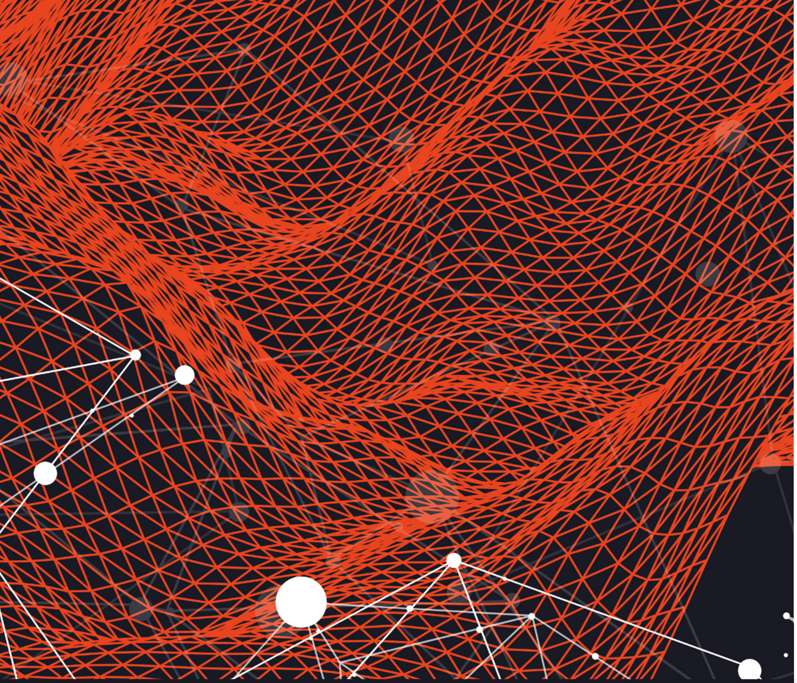
RANSOMWARE IN 2025

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown
Commercial
Service
Supplier



SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable threat intelligence, to help them identify and prevent criminal activity. Originally 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. The company has expanded and evolved, adding external threat management capabilities to create a Continuous Threat Exposure Management platform for organizations. Today we help government and law enforcement, enterprises, and managed security services providers around the world to identify threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM CYBER ESSENTIALS AICPA SOC Crown Commercial Service Supplier

METHODOLOGY

The data in this report is a combination of Searchlight Cyber's dark web telemetry on ransomware groups and open source intelligence.

The metric used to determine the most prolific groups is the number of victims they list on their leak sites. Ransomware operators use leak sites - usually hosted on the dark web - to extort their victims, sell stolen data, and promote their attacks.

However, it is worth noting that this data does not show the total number of ransomware victims because threat actors may not publicize some of their attacks for a number of reasons. For example, if the organization has already paid the ransom, the ransomware operator is engaging in negotiations with the business directly, or there is concern that listing the victim might draw unwanted attention from law enforcement, government, or other parties.

The purpose of this report is to demonstrate what insights can be derived from the dark web, but this data should always be used in conjunction with other threat intelligence.

CONTENTS

INTRODUCTION

This report - Searchlight Cyber's third annual ransomware update - stands out from the previous two because of major developments regarding the "key players" in the ransomware landscape.

LockBit, the number one ransomware group by number of listed victims in 2022[1] and 2023[2], has lost the top spot. BlackCat, also consistently in the top three groups in the last two years, has retired seemingly for good. Meanwhile Cl0p, the third most prolific group of 2023 and claimant of the most infamous hack of that year (using the MOVEit vulnerability), didn't make the top five in 2024.

In this report we'll examine some of the factors behind these changes in the ransomware scene and - as always - take a forensic look at the main players that have emerged as we enter the new year.

While some of the "old guard" of ransomware groups have diminished in stature - or disappeared completely - unfortunately this report shows that this hasn't resulted in a better outlook for organizations. In fact, the victim count in 2024 was up on 2023.

The number of active ransomware groups is also up year-on-year, creating a more complex landscape for security professionals to monitor. In this increasingly busy landscape, it becomes even more vital for organizations to actively apply threat intelligence to inform their defenses.

> “
> **WITH ALMOST A HUNDRED ACTIVE RANSOMWARE GROUPS LAST YEAR, IT IS NOT ENOUGH FOR ORGANIZATIONS TO SIMPLY BE AWARE OF THE GANGS OUT THERE.**

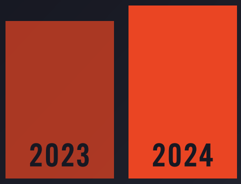
With almost a hundred active ransomware groups last year, it is not enough for organizations to simply be aware of the gangs out there. They need to start to be discerning - narrowing down the groups that are most likely to impact them based on their activity and victimology. They then have to gather intelligence on their capabilities, tactics, techniques, and procedures (TTPs), and tools - and apply these learnings to their defensive measures.

We hope that this report will be an instructive starting point in highlighting the challenge and identifying some of the more prolific groups that organizations should be aware of in 2025.

LUKE DONOVAN
Head of Threat Intelligence
Searchlight Cyber

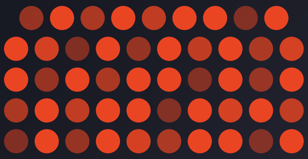
[1] https://slcyber.io/whitepapers-reports/most-prolific-ransomware-groups-of-2022/
[2] https://slcyber.io/whitepapers-reports/ransomware-in-2023/

KEY FINDINGS



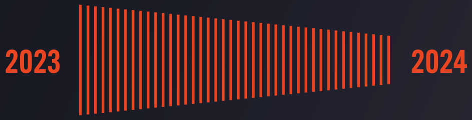
2024 saw an **11% rise** in listed ransomware victims vs 2023.

A total of 94 ransomware groups listed ransomware victims in 2024, a **38% increase** on 2023.



49 new groups were observed posting ransomware victims in 2024.

RansomHub has replaced LockBit as **#1 ransomware group**.



LockBit's victim count in 2024 was less than half of its 2023 victim count, demonstrating clear **impact from Operation Cronos**.

POSITION	GROUP	NUMBER OF VICTIMS	2023 POSITION
#1	RANSOMHUB	611	N/A
#2	LOCKBIT	494	1
#3	PLAY	366	4
#4	AKIRA	315	9
#5	HUNTERS INTERNATIONAL	235	35

CHANGES TO THE RANSOMWARE LANDSCAPE IN 2024

DIVERSIFICATION OF THE RANSOMWARE LANDSCAPE

As outlined in the introduction, 2024 was marked by a major shift in the top ransomware groups. Some of the usual suspects such as BlackCat and Cl0p have dropped out of the top ranking, replaced by newer ransomware operations.

It is noteworthy that, of the five top ransomware groups of the year, only LockBit has been active for more than three years. Incredibly, RansomHub - the most prolific group of the year - only emerged in February 2024.

THE NUMBER OF NEW RANSOMWARE GROUPS INCREASES

While it could be argued that this is part of a long-standing tradition of new groups replacing the old (afterall LockBit itself took the top spot vacated by Conti), another divergence this year is the rate at which new groups are emerging - which vastly outpaces the rate at which old groups are disappearing.

According to our figures, 24 ransomware groups ceased operation between 2023 and 2024. However, 49 new ransomware groups began posting victims for the first time last year. The result is a total of 94 ransomware groups that listed ransomware victims in 2024, a 38 percent increase on 2023 (68 groups).

OVERALL INCREASE IN THE NUMBER OF LISTED VICTIMS

Unsurprisingly, the increase in the number of active ransomware groups has resulted in an 11 percent increase in the number of total victims posted in 2024 (5,728) compared to 2023 (5,081). As ever, it should be remembered that these are only the victims that ransomware groups have elected to list on their leak sites - and is almost certainly far smaller than the total number of organizations impacted by ransomware last year.

Readers of our half year ransomware update[3] may recall that this is a reverse of the trend that we observed mid-year, where we recorded an increase in ransomware groups but fewer victims. Unfortunately, while there was a decrease in ransomware activity in the first half of 2024 (likely caused by major law enforcement action against LockBit) the total victim count more than rebounded in the second half of the year (**Figure 1**).

That is not to say that law enforcement action is futile. LockBit's 2024 victim count (less than half that of 2023) shows that Operation Cronos had an unquestionable impact on its output. It is also very likely that BlackCat's retirement was at least partly motivated by the coordinated disruption[4] it experienced in late 2023 and the public example law enforcement made of LockBit. LockBit and BlackCat were the first and second most active ransomware groups of 2023, which shows an impressive drive by international law enforcement to go after the biggest players.

[3] https://slcyber.io/whitepapers-reports/ransomware-in-h1-2024-trends-from-the-dark-web/
[4] https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
[5] https://cyberint.com/blog/threat-intelligence/handala-hack-what-we-know-about-the-rising-threat-actor/
[6] https://www.halcyon.ai/attacks/handala-ransomware-attack-elfi-tech-breach-data-compromise
[7] https://www.halcyon.ai/attacks/ransomware-attack-hits-israeli-industrial-batteries-by-handala-hack-group

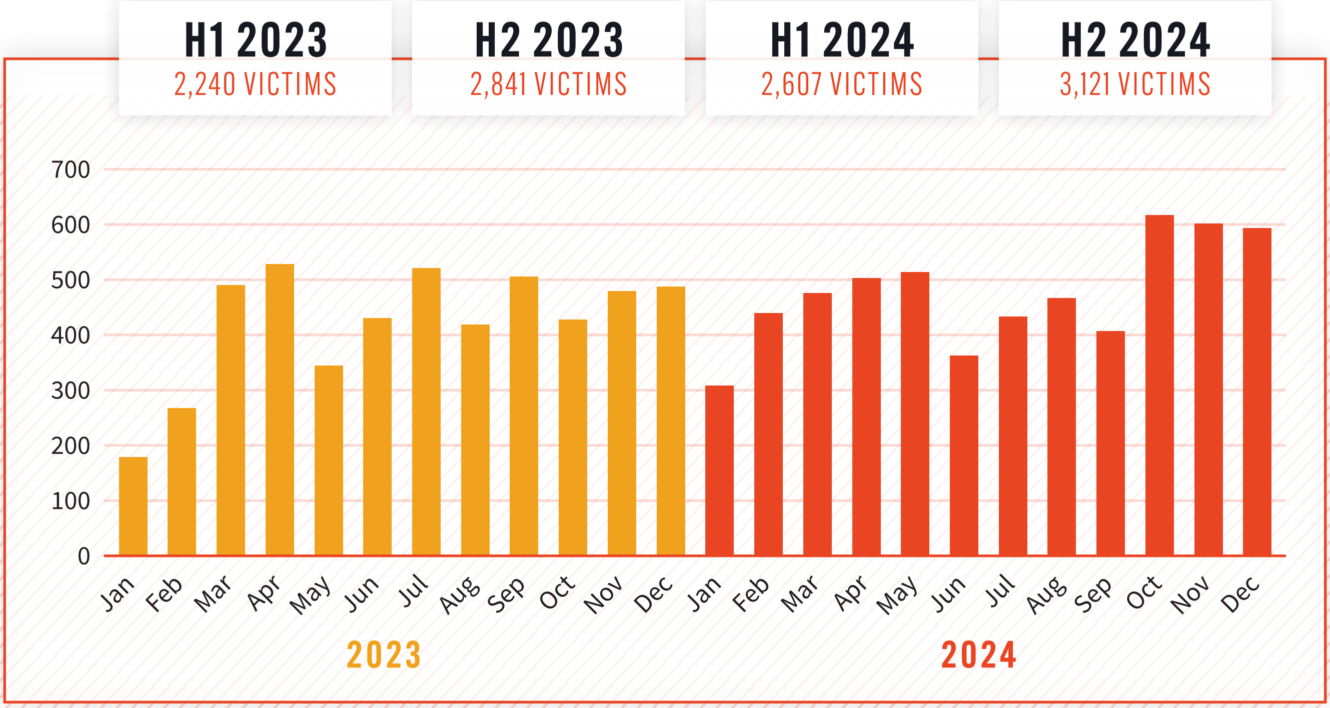


Figure 1: *Total ransomware group victim listings in 2023 and 2024.*

However, what the total results do show us is that ransomware capabilities are becoming more and more accessible in the criminal underground, leading to an increased number of smaller groups in operation. This creates challenges for security professionals, who have a more complex and dynamic ransomware landscape to make sense of and defend against.

POLITICALLY MOTIVATED GROUPS

Another complication in 2024 is the emergence of ransomware attacks that are explicitly motivated by ideology. While politics has influenced the actions of ostensibly financially-motivated groups to some extent in the past (it is no coincidence that Russian-speaking groups tend to target organizations in North America and Western Europe), it is relatively novel to see ransomware being deployed in the furtherance of a political aim.

Hacktivist groups have also been observed deploying ransomware. For example, Handala - a pro-Palestinian hacktivist group that has been active since December 2023 - has added ransomware to its repertoire, alongside it usual tactics of data theft, phishing, defacement, and wiper malware. Its ransomware victims include the Ma'agan Michael Kibbutz[5] in June 2024, the healthcare company Elfi-Tech[6] in June 2024, and Israel Industrial Batteries (IIB)[7] in September 2024.

This new trend speaks to the blurring of lines between cybercrime and cyberwarfare, which requires organizations to consider another dimension in their ransomware threat assessment. Now, in addition to monitoring financially motivated actors, organizations need to expand their list of potential adversaries to include those that may target them for ideological reasons.

In the next section, we profile the most prolific ransomware groups we have observed this year.

#1 RANSOMHUB

ACTIVE SINCE	February 2024
LISTED VICTIMS IN 2024	611

RansomHub took the number one spot by listed victims last year, despite only emerging in February 2024. Its quick rise to prominence can be explained by a number of factors. Firstly, like a number of emerging ransomware groups, it isn't strictly speaking "new". RansomHub has been tied to[8] Knight ransomware, which stopped operating just as RansomHub emerged in February 2024. It is also suspected to have taken on former affiliates of BlackCat and LockBit.

Another potential reason behind RansomHub's success is the perception that it has an "affiliate friendly" Ransomware-as-a-Service (RaaS) model, initially offering a fixed 10 percent fee for those that make attacks using its ransomware and the option to collect ransom payments directly from victims before paying the core group. These elements make it an attractive option for affiliates that are looking for a guaranteed return, where other RaaS operations have been unreliable in paying-out in the past.

Like many of the large ransomware-as-a-service operations, RansomHub's victimology appears to be indiscriminate towards industries, although (as with many ransomware groups) there is a clear concentration of victims in the United States. The ransomware landscape is fickle and - as our stats show - new groups can disappear just as quickly as they emerge. However, RansomHub's pedigree, popularity, and prolificity certainly make it a group that all security professionals should be watching in 2025.

[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

#2 LOCKBIT

ACTIVE SINCE	September 2019
LISTED VICTIMS IN 2024	494

Thanks to the efforts of Operation Cronos, the security industry and law enforcement know considerably more about LockBit now than they did this time last year.[9] As part of the operation, the National Crime Agency claimed[10] that it has accessed LockBit's source code, 1,000 decryption keys, and a "vast amount of intelligence" from its systems.

Law enforcement agencies subsequently published information on LockBit's capabilities and operations, including details of its data exfiltration tool Stealbit, data about its affiliates, and - most dramatically - naming one individual that they believe to be the leader of the LockBit group. Russian national Dmitry Khoroshev has been charged[11] by the U.S. Department of Justice as being the creator, developer, and administrator of LockBit that operates under the dark web aliases of LockBit and LockBitSupp.

In spite of Khoroshev's indictment and the considerable disruptive impact of Operation Cronos on LockBit's infrastructure and reputation, the group has continued to attack victims - although at a much diminished rate. LockBit's total victim count for 2024 was less than half of 2023, demonstrating the effect that coordinated international law enforcement can have in tackling one of the greatest threats impacting businesses.

However, it does have to be recognized that LockBit's inclusion in the top five ransomware groups of last year means that it remains a persistent threat. LockBit continues to list victims, recruit affiliates, and try to reclaim its reputation on dark web forums. At the time of writing, LockBit's dark web leak site has a countdown timer for February 3rd, teasing LockBit 4.0, although it is unclear at this stage whether that entails a brand new ransomware strain or just an update to its dark web leak site. What is clear is that LockBit intends to maintain its position as a major player through 2025.

[9] https://slcyber.io/whitepapers-reports/ransomware-in-2023/
[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

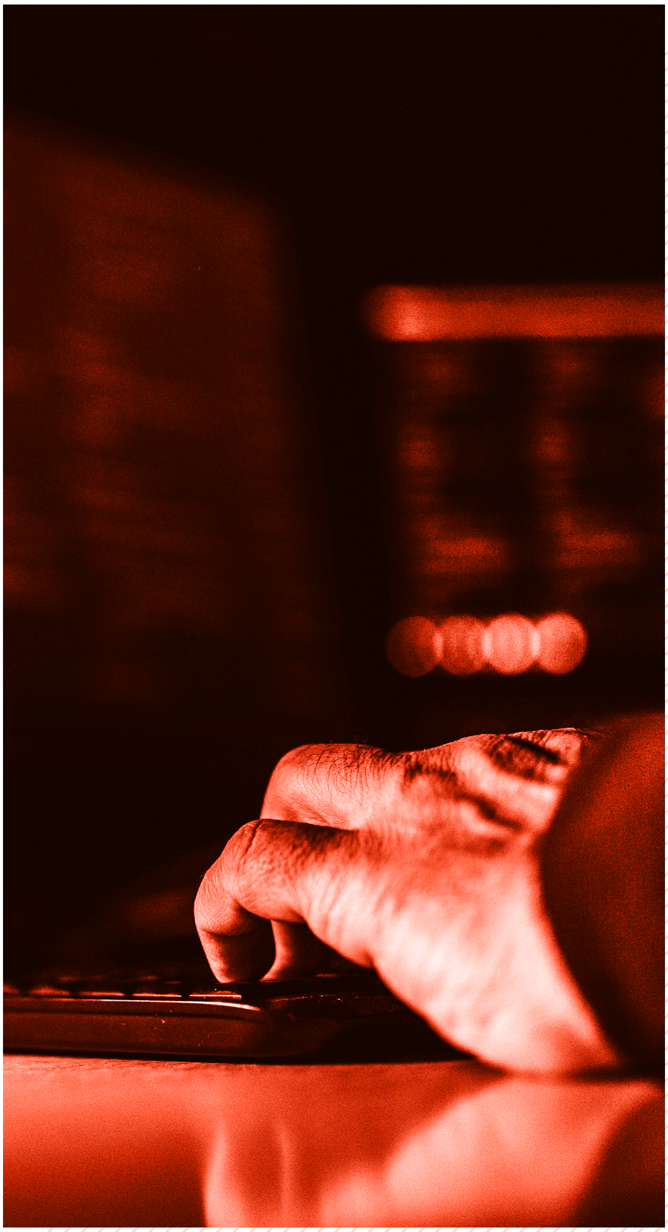
#3 PLAY

ACTIVE SINCE	June 2022
LISTED VICTIMS IN 2024	366

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. In July 2024 Trend Micro researchers observed[12] that the Play ransomware group has introduced a Linux variant of its malware that specifically targets VMWare ESXi environments.

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.

In October 2024, security researchers[13] at Palo Alto's Unit 42 published evidence of a deployment of Play ransomware by a threat actor backed by North Korea, known by a number of aliases including Jumpy Pisces, Andariel, and APT45. The link between this threat actor and Play is unclear, but demonstrates the potential for crossover between state-sponsored cyber activity and ostensibly independent cybercrime networks.



[12] https://www.infosecurity-magazine.com/news/play-ransomware-target-vmware-esxi/
[13] https://thehackernews.com/2024/10/north-korean-group-collaborates-with.html

#4 AKIRA

ACTIVE SINCE	March 2023
LISTED VICTIMS IN 2024	315

Listed as one of our "groups to watch in 2024" in last year's report,[14] Akira has lived up to our expectations in terms of its victim output. The group claimed more than 30 victims on its dark web leak site in one day[15] in November 2024.

First observed in March 2023, Akira originally used a novel ransomware strain, written in C++, with versions targeted both at Windows machines and Linux operating systems. However, a joint cybersecurity advisory issued[16] on Akira in April 2024 noted that the ransomware group had also been observed deploying Megazord, using Rust-based code which encrypts files with a .powerranges extension.

The advisory also warned that Akira has impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia. The group is known to leverage known vulnerabilities in VPN appliances to gain initial access to its target, who typically reside in the commercial & professional services, capital goods, education, and software & services industries.

[14] https://slcyber.io/whitepapers-reports/ransomware-in-2023/
[15] https://www.securityweek.com/akira-ransomware-drops-30-victims-on-leak-site-in-one-day/
[16] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

#5 HUNTERS INTERNATIONAL

ACTIVE SINCE	October 2023
LISTED VICTIMS IN 2024	235

Hunters International has been active since October 2023 but - as with RansomHub - it should be noted that the group did not appear in a vacuum. There are clear code similarities between Hunters International and the ransomware used by Hive, a RaaS group that was dramatically shut down in January 2023[17] after a seven month covert infiltration and disruption campaign executed by law enforcement.

Hunters International has denied being a rebrand of Hive, instead claiming to have acquired the defunct group's source code and infrastructure. Either way, this case once again demonstrates the links between different groups and the difficulty in eradicating any particular ransomware strain for good.

Its first full year in operation, noteworthy victims of the group in 2024 included the London branch of the Industrial and Commercial Bank of China (ICBC),[18] Japanese optics giant Hoya,[19] and Namibia's state-owned telecoms company Telecom Namibia.[20] The group also claimed an attack on the U.S. Marshals Service on its dark web leak site, although this was disputed[21] by the law enforcement agency.

In August 2024, researchers at Quorum Cyber also published research[22] on a Remote Access Trojan (RAT) used by Hunters International to "achieve initial infection, elevate their privileges on compromised systems, execute PowerShell commands, and eventually deploy the ransomware payload."

[17] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[18] https://www.theregister.com/2024/09/11/hunters_ransom_icbc_london/
[19] https://www.cyberdaily.au/security/10422-hunters-international-take-credit-for-hoya-optics-attack-demand-us-10m
[20] https://www.bbc.com/news/articles/ce3l509e6x7o
[21] https://www.bleepingcomputer.com/news/security/us-marshals-service-disputes-ransomware-gangs-breach-claims/
[22] https://www.bleepingcomputer.com/news/security/hunters-international-ransomware-gang-targets-it-workers-with-new-sharprhino-malware/

CONCLUSION

The main takeaway from this report is that the ransomware landscape has become larger and more complex as we move into 2025, necessitating a closer focus on threat intelligence from security teams. There are more groups to monitor and many of them are relatively new.

Of course, this doesn't mean that the "usual suspects" should be discounted. While it is undoubtedly true that LockBit was severely knocked by the law enforcement action (Operation Cronos), it was still the second most active of the year and should by no stretch be dismissed as a threat - especially as the group teases "LockBit 4.0" for February 2025.

Similarly, Cl0p - notorious for its 2023 mass-attack against hundreds of organisations using the MOVEIt software vulnerability - had a relatively muted 2024. However, at the time of writing (January 2025) the group has bulk-listed 60 new victims on its ransomware leak site that it claims it compromised using zero-day vulnerabilities in the Cleo file transfer software. The group may have more surprises in store for 2025.

As the ransomware ecosystem becomes more complex and fragmented, organisations should be using threat intelligence to try and identify the groups that pose the greatest threat to their organisation, and prepare their defenses based on how those groups operate.

Developing an understanding of multiple ransomware groups' tactics, techniques and procedures (TTPs) allows an organisation to determine commonalities between the groups. Where there is significant overlap of TTPs, prioritisation of security within these areas can be resource effective and allow greater protection against multiple groups.

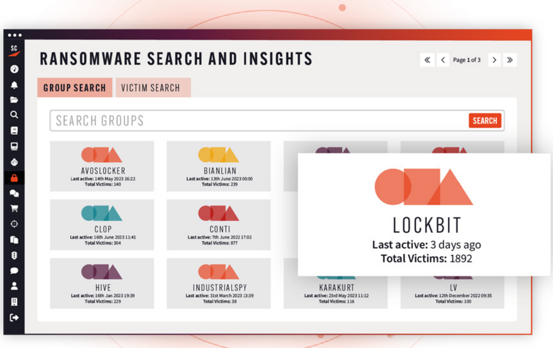
> **“**
>
> **IF SECURITY TEAMS CAN NARROW IT DOWN TO THE FOUR OR FIVE WHO TARGET THEIR INDUSTRY, GEOGRAPHY, OR PEERS, AND REALLY UNDERSTAND HOW THEY LAUNCH THEIR ATTACKS, THEY CAN GET AHEAD OF THOSE WHO ARE MOST LIKELY TO TARGET THEM.**

There are security practices that all organisations should have in place: patching vulnerabilities, applying MFA, and educating employees. However, when preparing for specific threats, security teams need to focus on the most likely adversaries.

It is near impossible to prepare for dozens of ransomware groups at once, but if security teams can narrow it down to the four or five who target their industry, geography, or peers, and really understand how they launch their attacks, they can get ahead of those who are most likely to target them.

ABOUT RANSOMWARE SEARCH AND INSIGHTS

Our Ransomware Search and Insights module allows security professionals to monitor ransomware group activity on the dark web through one intuitive dashboard.



RANSOMWARE SEARCH AND INSIGHTS

« ‹ Page 1 of 3 › »

GROUP SEARCH | VICTIM SEARCH

SEARCH GROUPS — SEARCH

AVOSLOCKER
Last active: 14th May 2023 16:22
Total Victims: 140

BIANLIAN
Last active: 13th June 2023 00:00
Total Victims: 239

CLOP
Last active: 16th June 2023 11:41
Total Victims: 304

CONTI
Last active: 7th June 2022 17:02
Total Victims: 877

HIVE
Last active: 16th Jan 2023 19:39
Total Victims: 229

INDUSTRIALSPY
Last active: 31st March 2023 13:39
Total Victims: 38

KARAKURT
Last active: 23rd May 2023 11:12
Total Victims: 116

LV
Last active: 12th December 2022 09:35
Total Victims: 100

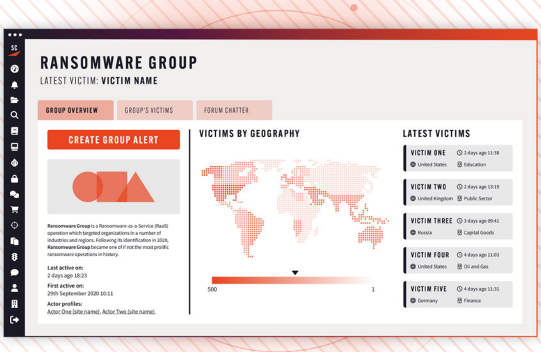
LOCKBIT
Last active: 3 days ago
Total Victims: 1892

GAIN VISIBILITY INTO THE RANSOMWARE LANDSCAPE:

- ➤ See ransomware groups active on the dark web in one place.
- ➤ Get top level trends on which groups are posting the most victims.
- ➤ Analyse ransomware group victimology by industry and geography.

INTERROGATE RANSOMWARE GROUP ACTIVITY:

- ➤ See all of the victim posts on a ransomware leak site, even if a post is deleted by the group.
- ➤ Safely access the dark web leak site directly through our Stealth Browser.
- ➤ Find assets related to a ransomware group including dark web aliases and social media accounts.



RANSOMWARE GROUP
LATEST VICTIM: **VICTIM NAME**

GROUP OVERVIEW | GROUP'S VICTIMS | FORUM CHATTER

CREATE GROUP ALERT

Ransomware Group is a Ransomware-as-a-Service (RaaS) operation which targeted organizations in a number of industries and regions. Following its identification in 2020, **Ransomware Group** became one of if not the most prolific ransomware operations in history.

Last active on:
2 days ago 18:23

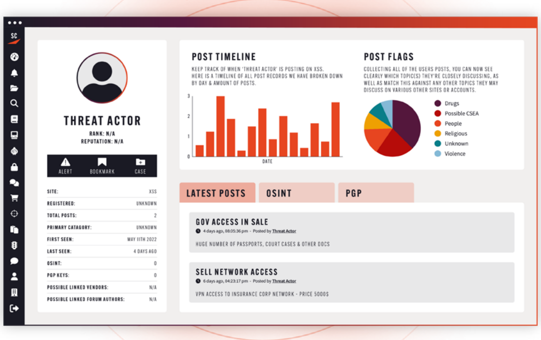
First active on:
29th September 2020 10:11

Actor profiles:
Actor One (site name), Actor Two (site name)

VICTIMS BY GEOGRAPHY

LATEST VICTIMS

VICTIM ONE	United States	Education
	2 days ago 11:38	
VICTIM TWO	United Kingdom	Public Sector
	2 days ago 13:19	
VICTIM THREE	Russia	Capital Goods
	3 days ago 09:41	
VICTIM FOUR	United States	Oil and Gas
	4 days ago 11:03	
VICTIM FIVE	Germany	Finance
	4 days ago 11:31	



THREAT ACTOR
RANK: N/A
REPUTATION: N/A

SITE:	XSS
REGISTERED:	UNKNOWN
TOTAL POSTS:	2
PRIMARY CATAGORY:	UNKNOWN
FIRST SEEN:	MAY 11TH 2022
LAST SEEN:	4 DAYS AGO
OSINT:	0
PGP KEYS:	0
POSSIBLE LINKED VENDORS:	N/A
POSSIBLE LINKED FORUM AUTHORS:	N/A

POST TIMELINE

KEEP TRACK OF WHEN 'THREAT ACTOR' IS POSTING ON XSS. HERE IS A TIMELINE OF ALL POST RECORDS WE HAVE BROKEN DOWN BY DAY & AMOUNT OF POSTS.

POST FLAGS

COLLECTING ALL OF THE USERS POSTS, YOU CAN NOW SEE CLEARLY WHICH TOPIC(S) THEY'RE CLOSELY DISCUSSING, AS WELL AS MATCH THIS AGAINST ANY OTHER TOPICS THEY MAY DISCUSS ON VARIOUS OTHER SITES OR ACCOUNTS.

LATEST POSTS | OSINT | PGP

GOV ACCESS IN SALE
4 days ago, 08:05:36 pm - Posted by Threat Actor
HUGE NUMBER OF PASSPORTS, COURT CASES & OTHER DOCS

SELL NETWORK ACCESS
6 days ago, 04:23:17 pm - Posted by Threat Actor
VPN ACCESS TO INSURANCE CORP NETWORK - PRICE 5000$

PIVOT ON THE ACTORS BEHIND THE GROUP:

- ➤ Monitor actors associated with ransomware groups on dark web forums.
- ➤ Identify connections with other cybercriminals, including Initial Access Brokers.
- ➤ Uncover the tools, tactics, and vulnerabilities they use 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