

MORE GROUPS, MORE PROBLEMS

RANSOMWARE IN 2023



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.

METHODOLOGY

The threat intelligence in this report is derived from Searchlight Cyber's Ransomware Search and Insights module, which collates data from the dark web leak sites of ransomware groups. As of January 2024, we track the leak sites of 53 ransomware groups.

The metric we are using 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 groups may choose not to 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 the group is worried 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 correlation with other threat intelligence.

CONTENTS

2	METHODOLOGY
4	CHANGES TO THE RANSOMWARE LANDSCAPE IN 2023
6	THE MOST PROLIFIC RANSOMWARE GROUPS OF 2023
7	LOCKBIT
8	BLACKCAT
9	CLOP
10	WHERE ARE THEY NOW?
10	HIVE
11	VICE SOCIETY
11	AVOSLOCKER
12	GROUPS TO WATCH IN 2024
12	8BASE
12	RHYSIDA
13	AKIRA
14	ABOUT RANSOMWARE SEARCH AND INSIGHTS

CHANGES TO THE RANSOMWARE LANDSCAPE IN 2023

MORE GROUPS, MORE PROBLEMS

The biggest change to the ransomware landscape in 2023 was the increase in operators hosting leak sites on the dark web. While many of the largest groups continued and - in some cases - increased the rate of their output, their share of the overall victims actually decreased.

For example, LockBit remains top dog in terms of having the most victims. But, where its victims accounted for a third of the total posted on the dark web in the last three months of 2022, its share only accounts for 17 percent in the last three months of 2023. Its output hasn't decreased (in fact, it almost doubled its total victim count last year) but the ransomware world has got bigger.

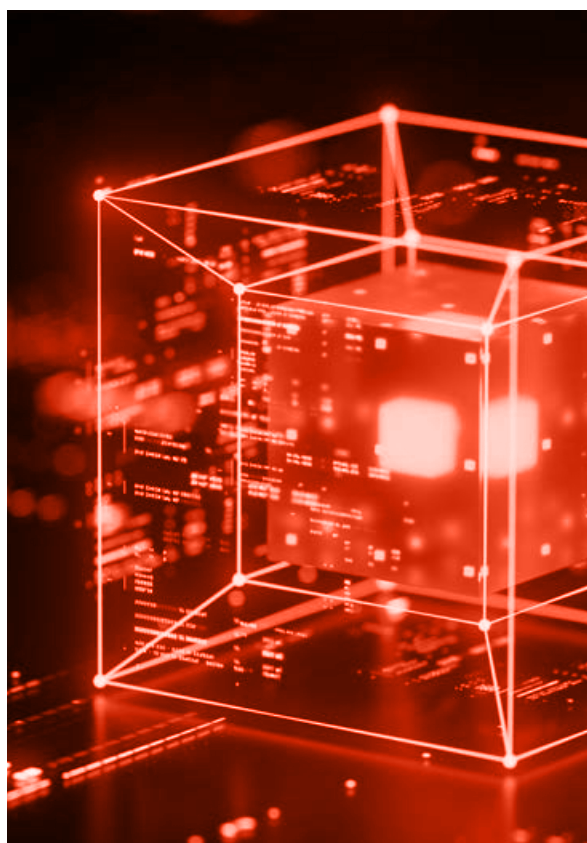
NEW KIDS ON THE BLOCK(?)

New operations spring up every week and, while some are short-lived, others have cemented themselves as being just as prolific - and dangerous - as their predecessors. Notable newcomers that quickly established a reputation in 2023 include 8Base, Akira, and Rhysida (for more information, skip to the "Groups to Watch in 2024" section below).

How "new" the individuals behind these groups truly are is a pertinent question when it comes to ransomware as there is a lot of overlap between operations. This is due to the way that Ransomware-as-a-Service (RaaS) schemes work - affiliates act as independent contractors for different groups, making it difficult to determine where one ends and another begins.

Even in the case of more exclusive, closed-entry ransomware gangs or the inner circles of RaaS programmes, there is a precedent of reshuffling veteran employees into new, rebranded teams. This was perhaps most clearly observed in 2022 when the Conti group dissolved into innumerable descendants including BlackByte, BlackBasta, and Royal. Conti's leaked source code also gave rise to imitator groups, not composed of original members but repurposing the group's malware for their own operations.

These trends continued throughout the 2023 landscape, with the Babuk source code (which was intentionally released) being the most popular blueprint for new groups¹ to build upon, including DarkAngels/Dunghill, Daixin, RA Group and Cyclops/Knight. Meanwhile BlackCat² - a suspected rebrand of the DarkSide/BlackMatter gang of Colonial Pipeline fame - continues to be one of the most formidable forces in the RaaS scene, recently wreaking havoc³ on the networks of two major US casino chains. This report contains more examples of groups "disappearing" but possibly continuing under a different guise.



LAW ENFORCEMENT TAKEDOWNS

While 2022 was dominated by the dramatic bust-up of Conti - in part induced by the leak of the gang's private comms - 2023 also saw its fair share of ransomware disruption.

In January, it was revealed⁴ that the FBI had been infiltrating the network of the prolific Hive ransomware gang for six months, all the while capturing and distributing decryption keys to victim organizations (see the "Where Are They Now" section below for more details).

More recently, RagnarLocker's dark web leak site was replaced⁵ by a notice announcing the page's seizure as part of an international operation led by Europol and Eurojust. In addition to dismantling the group's infrastructure hosted in the Netherlands, Germany, and Sweden, searches were conducted in Czechia, Spain and Latvia. A "key target" of the investigation - thought to be a developer of the RagnarLocker malware - was also arrested in Paris, with five other suspects being interviewed across Europe.

VICTIMOLOGY

In terms of top targeted industries and regions, 2023 follows the trend of previous years. Organizations in the United States are the most targeted by a significant margin, followed by those in the UK, Canada, Germany and France.

Commercial & professional services (encompassing most business-to-business service and supply industries) and capital goods (including aerospace & defense, construction & engineering, and heavy machinery manufacturing) were the top targeted industry groups, with a large share of attacks also hitting software & services, healthcare and education.

WHEN A RANSOMWARE GANG DOESN'T USE RANSOMWARE

As we move into 2024, a new trend that appears to be emerging is threat actors bypassing the use of encryptors altogether, focusing instead on plain data theft and extortion to get their ransoms. This is a major development in the use of double extortion (encryption and exfiltration), which has been the name of the game for several years now.

It is possible that companies' increasing preparedness for encryptors - i.e. with maintenance of up-to-date backups - may have decreased its effectiveness as an incentive to pay ransoms. Meanwhile, greater reputation and regulatory damage from data breaches might increase the incentive to pay to retrieve exfiltrated data. This can be seen in how ransomware gangs present themselves and their "services", with the likes of RansomedVC⁶ explicitly contrasting their ransom fee with the cost of GDPR fines in an attempt to pressure victims into paying.

At the moment, ransomware gangs continue to use a combination of encryptors and data exfiltration, but if the trend continues on this trajectory it is possible that next year's report will have to be named "Ransomware and Data Extortion Gangs".



JIM SIMPSON

Director of Threat Intelligence
Searchlight Cyber

THE MOST PROLIFIC RANSOMWARE GROUPS OF 2023

The background is a dark blue-grey gradient. It features faint, scattered binary code (0s and 1s) and vertical lines of varying heights. A large, semi-transparent orange circle is positioned in the bottom right corner, partially overlapping the text area. The text is white and bold, with a slight shadow effect.



LOCKBIT

GROUP OVERVIEW

LockBit is a Ransomware-as-a-service (RaaS) operation that targets organizations across a broad range of industries and regions. Originally dubbed ABCD, LockBit has developed several versions of its malware, including LockBit Red, Black and Green. On its latest Tor leak site, LockBit 3.0, there are options on some victims' listings to either extend the countdown timer by 24 hours, "destroy" the stolen data, or download the stolen data, for varying price points. LockBit actively engages with its fans and detractors on dark web forums like XSS, promoting its attacks and investing effort into its branding.

FIRST ACTIVE

September 2019

VICTIMS LISTED IN 2023

1,191

TOTAL LISTED VICTIMS

2,502

KNOWN ALIASES

LockBitSupp
LockBit

ACTIVE FORUM ACCOUNTS

XSS
Exploit

2023 ACTIVITY

LockBit has taken top spot as the most prolific ransomware group for the second year in a row, almost doubling its total listed victim count in the past 12 months. The year arguably started a bit rocky for the group, with LockBit having to issue a "formal apology"⁷ after one of its affiliates attacked Toronto's Hospital for Sick Children, breaking the group's "rules". Another affiliates' attack on the UK's Royal Mail then appeared to leave the group confused, causing them to release a number of conflicting statements⁸ first denying - then confirming - the use of LockBit ransomware in the attack. In one of its statements, the group effectively said it just has too many victims to keep track of.

Indeed, LockBit did claim a long list of high profile victims this year, including (but not limited to) the UK Ministry of Defense⁹, Boeing¹⁰, CDW¹¹, Portuguese water company Aguas do Porto¹², and TSMC¹³, the world's largest contract chipmaker.

In terms of its technical capabilities, in April researchers spotted samples of LockBit (which previously targeted Windows, Linux, and VMware ESXi servers) designed to target macOS¹⁴, a first for major ransomware operations of this scale. In November 2023 a Cybersecurity Advisory¹⁵ was issued warning that LockBit was among many threat actors exploiting the CVE 2023-4966 Citrix Bleed Vulnerability.

BLACKCAT

GROUP OVERVIEW

The RaaS group BlackCat (also known as ALPHV or Noberus) is believed to include developers and money launderers from the former DarkSide ransomware group, most infamous for the Colonial Pipeline attack. BlackCat is also suspected to have recruited former members of the REvil operation. It is noteworthy for being one of the first high-profile ransomware families to be written in Rust, a relatively modern programming language with features that make the malware harder to reverse engineer and defend against. It has also been reported that BlackCat lets its affiliates keep a larger share of the profits than other RaaS platforms. In February 2023 BlackCat announced¹⁶ the latest variant of its ransomware, named Sphynx.

FIRST ACTIVE

November 2021

VICTIMS LISTED IN 2023

454

TOTAL LISTED VICTIMS

731

KNOWN ALIASES

alphy
BlackCat46
ransom

ACTIVE FORUM ACCOUNTS

XSS
Exploit
Ramp

2023 ACTIVITY

BlackCat is another ransomware group that has retained its position as one of the top three most prolific groups for the second year in a row. It has graduated from third to second spot (replacing Conti, which ceased operations in 2022). Indeed, BlackCat has more than tripled its total victim listing count this year, and is fast gaining on the Conti group's final tally of 877 listed victims - although it is still a long way off from achieving LockBit's numbers.

Some of the group's most notable listed victims from this year were Constellation Software¹⁷, Sun Pharmaceuticals¹⁸, Western Digital¹⁹, Five Guys²⁰, and Reddit²¹. BlackCat drew particular attention for its listing of MGM Casinos in September²², which was attacked by its suspected affiliate, Scattered Spider²³.

It looked like the game might be up for BlackCat by the end of 2023, when the U.S. Department of Justice announced²⁴ its disruption of the BlackCat ransomware gang in December, in collaboration with global law enforcement partners. The FBI shared a decryption tool to help victims to restore their systems and a seizure notice was displayed on BlackCat's dark web leak site. However, the ransomware gang soon regained control of the site and down-played the significance of the law enforcement action. It has since added victims to its new dark web leak site.



CLOP

GROUP OVERVIEW

ClOp ransomware is known to be used by the cybercriminal enterprise tracked as TA505 and FIN11. There was a lull in the group's activity for most of 2022, potentially due to the arrest of six ClOp associates in Ukraine in June 2021. However, there was a quick resurgence in attacks and 2023 was by far and away the group's most active year. ClOp is notable for its approach of using vulnerabilities in supply chain software to target multiple organizations, announcing them in a batch at a later date. This was a tactic it used to great effect into 2023.

FIRST ACTIVE

February 2019

VICTIMS LISTED IN 2023

407

TOTAL LISTED VICTIMS

538

KNOWN ALIASES

CL0P

ACTIVE FORUM ACCOUNTS

XSS

2023 ACTIVITY

Hot on BlackCat's heels, ClOp is a new entrant into the top three for 2023. The vast majority of ClOp's victims came from two "mass-hack" attacks it pulled off throughout the year.

In March, ClOp exploited the vulnerability CVE-2023-0669²⁵ in Fortra's GoAnywhere MFT secure file transfer tool to target more than 130 organizations, listing them in quick succession. Then in June, ClOp repeated this approach in one of the biggest and most notable cyberattacks of the year²⁶, exploiting a zero day vulnerability (CVE-2023-34362) in the Progress Software file transfer software tool, MOVEit.

The group had so many victims from the MOVEit breach that it had to explore new ways of leaking data, including using torrents²⁷. While hundreds of companies were listed on its leak site, it is reported²⁸ that there were in fact more than 1,000 organizations impacted by the MOVEit attacks. Noteworthy victims included the BBC, British Airways, Emsisoft, U.S. government services contracting company Maximus, and the French government's unemployment agency, Pôle emploi.

In the aftermath, the U.S. State Department offered a \$10 million bounty for information on ClOp and the group's activity has plateaued significantly since the listing of all of the MOVEit victims. However, the group's "mass-hack" tactic may mean it is conducting activity behind the scenes.

WHERE ARE THEY NOW?

In last year's ransomware report²⁹ we selected AvosLocker, Hive, and Vice Society as three "groups to watch" in 2023. Incidentally, all three of these groups' dark web leak sites have gone offline over the past 12 months! In this section we take a quick look at what became of the alumni of our yearly ransomware report.



HIVE

Hive was a RaaS operation that particularly focused on attacks against the energy and healthcare sectors. In January, it was announced³⁰ that the FBI had infiltrated the ransomware gang's network over a period of several months, all the while capturing and distributing decryption keys to its victims. In the end, the US Justice Department and its law enforcement partners in Germany and the Netherlands seized Hive's servers as well as its dark web leak sites.

While that was the end of the Hive dark web leak site, the group's ransomware lives on - at least in some form. It was noted³¹ that the ransomware code used by HuntersInternational - a relatively new group on the ransomware scene - was very similar to Hive's, leading some to speculate that the Hive operators had returned under a new moniker. Hunters vociferously denied this on its dark web leak site, claiming that it purchased Hive's malware code to serve as an auxiliary capability to its primary business model of data extortion. Since no Hive-adjacent actors appear to have been identified (publicly, at least) or arrested, both explanations are possible.



VICE SOCIETY

ViceSociety was a ransomware/data extortion operation that primarily targeted organizations in the education sector. It gained notoriety for conducting a spree of attacks towards the end of 2022 and beginning of 2023 on institutions in North America and Europe including the Los Angeles Unified School District, University Institute of Technology of Paris, and The University of Duisburg-Essen. In February 2023 we published a report³² on a pattern of dark web traffic to the networks of Vice Society's victims, which we assessed with medium confidence was a precursor to the group's attacks.

ViceSociety stopped posting victims to its dark web leak site in June 2023 and the site went offline in December. However, once again, this doesn't necessarily mean the actors behind the group have left the ransomware scene for good. Some security analysts, including those at Check Point Research³³, have identified similarities in the Tactics, Techniques and Procedures (TTPs) of Vice Society and those used by Rhysida, a ransomware operation that emerged in 2023 (see page 12). Other correlatory factors include temporal crossover - after Rhysida's appearance only two victims were posted on ViceSociety's leak site before it stopped being active - and similarity in victimology, with both Vice Society and Rhysida targeting victims in the education, healthcare and public sector industries.



AVOSLOCKER

AvosLocker is a RaaS operation that favors targeting smaller organizations in North America. Its dark web leak site went offline in May, however the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a new advisory³⁴ on the ransomware group's tactics in October 2023. This suggests that AvosLocker may still be active even if they are not advertising their attacks on the dark web.

GROUPS TO WATCH IN 2024

As our predictions from last year demonstrate, the tumultuous nature of the ransomware scene makes it difficult to prognosticate the groups that will even still be active this time next year, let alone which will be the most influential. This is why we advocate continuous monitoring of ransomware group activity, to stay informed of trends in a busy and fast-moving landscape. Never-the-less, we have selected three groups that we believe cybersecurity professionals would do well to take note of as we move into 2024.

8BASE

The 8Base dark web leak site appeared in June 2023 but the group is reported³⁵ to have been active since March 2022. Its activity accelerated in the summer of 2023 and since then it has been consistent in posting victims, quickly becoming one of the most active groups we track (with more than 260 total victims at the time of publication). Its top three targeted industries are commercial & professional services, capital goods, and healthcare equipment & services. 8Base uses double extortion tactics - as well as encrypting an organization's data it also exfiltrates data and threatens to leak it on its dark web leak site.

8Base uses a variant of Phobos ransomware in its attacks, modified to append a ".8base" extension onto encrypted files. Researchers have also noted³⁶ 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. In September 2023, the cybersecurity researcher Brian Krebs demonstrated³⁷ that at least some of the 8Base leak site code was written by a 36-year-old programmer residing in the capital city of Moldova.

RHYSIDA

Rhysida began posting victims on its dark web leak site in June 2023 and already has more than 75 to its name. It rose to notoriety in November for its attack on the British Library³⁸, which took the cherished UK institution's website, systems, and some on-site services offline. Just weeks later, the gang took aim at another British institution - the royal family³⁹ - threatening to leak data from a private London hospital, which it claimed contained sensitive information on the royals.

The group is noteworthy for its focus on organizations in the education industry, who make up 35 percent of its victims, followed by those in health care equipment & services, and the public sector. As discussed in the "Where are they now" section above (see page 11), some cybersecurity analysts have connected⁴⁰ Rhysida with the ViceSociety ransomware group, which ceased operations at about the same time that Rhysida emerged.

The logo for the Akira ransomware group, featuring the word "AKIRA" in a stylized, blocky, white font with a black outline, set against a black rectangular background.

AKIRA

First observed in March 2023, Akira appears to be a novel ransomware strain, written in C++, with versions targeted both at Windows machines and Linux operating systems. Akira is seen⁴¹ 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. Noteworthy victims among the more than 180 it has already amassed include Stanford University, Nissan Australia and the US consulting firm Frost & Sullivan.

CONCLUSION

Intelligence from the dark web demonstrates a clear trend emerging over the past 12 months: a ransomware landscape that has become larger and more diverse. Small, specialized groups have emerged at pace and quickly amassed dozens of victims. Meanwhile, the large, established ransomware operations have also increased their output. Overall, it is more active threat landscape than it was this time last year.

The expansion of the ransomware ecosystem means that organizations need the most up-to-date information on the specific ransomware threats facing their industry and their peers.

Ransomware groups use the dark web to share their tactics, buy their initial access, and recruit affiliates. Visibility into this activity allows security teams to track the emergence of new groups, identify the most likely threats that could impact them, and prepare their defenses based on a better understanding of the tools and techniques their adversaries use. Security teams concerned about ransomware should monitor the dark web activity of actors to understand and prepare for the latest threats.

ABOUT RANSOMWARE SEARCH AND INSIGHTS

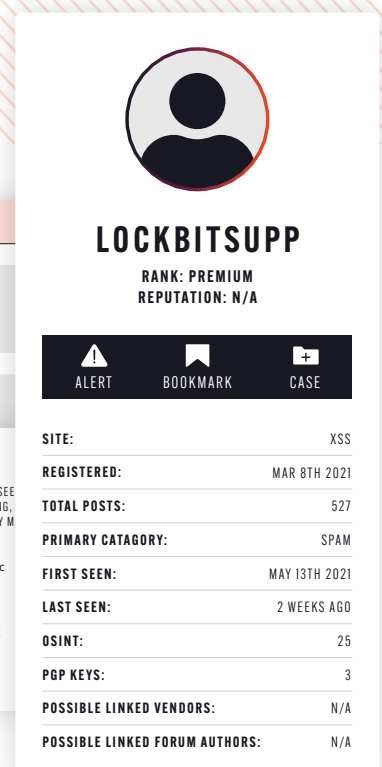
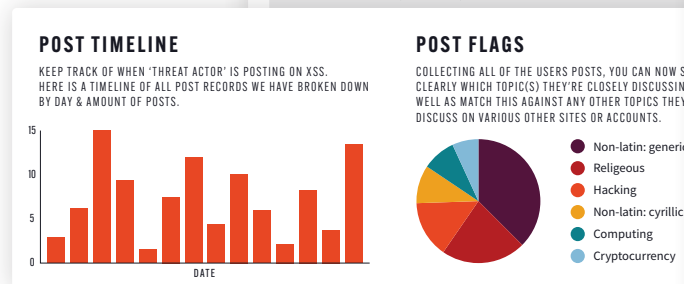
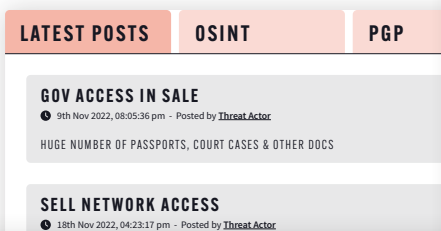
Our Ransomware Search and Insights module allows security professionals to monitor the dark web activity of more than 50 ransomware groups through one intuitive dashboard.



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.



REFERENCES

PAGE 4

- 1 // https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map_v25.pdf
- 2 // <https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/>
- 3 // <https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/>

PAGE 5

- 4 // <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>
- 5 // <https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop>
- 6 // <https://cybernews.com/security/gdpr-abused-ransomware-extortion/>

PAGE 7

- 7 // https://www.theregister.com/2023/01/04/lockbit_sickkids_ransomware/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=67457502&_hsenc=p2ANqtz-_kLL70wzltkosPpw0pAloGeUCSTKkv1Ly7UDYLRWjvH6lmksM3E4dzW-37KWfYZ4a4apj9ppFlkJkxQU6dcQok6yQ&utm_content=67455854&utm_source=hs_email
- 8 // <https://www.slycyber.io/lockbit-claims-then-denies-then-claims-attack-on-royal-mail/>
- 9 // <https://www.computing.co.uk/news/4123967/breaking-uk-mod-attacked-lockbit>
- 10 // <https://www.reuters.com/business/aerospace-defense/boeing-assessing-lockbit-hacking-gang-threat-sensitive-data-leak-2023-10-27/>
- 11 // https://securityaffairs.com/152470/cyber-crime/lockbit-ransomware-gang-hacked-cdw.html#google_vignette
- 12 // <https://securityaffairs.com/142477/cyber-crime/lockbit-water-utility-aguas-do-porto>
- 13 // https://techcrunch.com/2023/06/30/tsmc-confirms-data-breach-after-lockbit-cyberattack-on-third-party-supplier/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=73625306&_hsenc=p2ANqtz-9po71UaXKb6YH3ZwjGL1xn8NqNtRCcxOwNXSnmZ1xkbo76qLDjVR2J5cYDnL_HCT7AAzNqnw3KQeqOI05o3pYPR8c&utm_content=73612237&utm_source=hs_email
- 14 // <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/>
- 15 // <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a>

PAGE 8

- 16 // <https://www.scmagazine.com/news/blackcat-ransomware-stealth-speed>
- 17 // https://www.securityweek.com/ransomware-group-claims-attack-on-constellation-software/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=71644635&_hsenc=p2ANqtz-3ZW2Y8jKsSub2YlZAS5KIDvF1qvnHmFjRG5n8W4M09oRZ99uM6EhDgcv_Inse5lr5kMG71WhZOHFWQe8kUqB-cqp0Q&utm_content=71643022&utm_source=hs_email
- 18 // <https://www.scmagazine.com/brief/ransomware-attack-confirmed-by-sun-pharmaceuticals>
- 19 // https://www.bleepingcomputer.com/news/security/hackers-leak-images-to-taunt-western-digital-cyberattack-response/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=71405799&_hsenc=p2ANqtz-bCh4HD_
- 20 // https://cybernews.com/news/five-guys-ransomware/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=68604273&_hsenc=p2ANqtz-8yehKlZWHpU3lVA-AL0xd2HienoDqkFJSCuzbpLeTx-XlzpP7ckTrOUJsiZaVmH3TW6zm884ikAhVLCBPXgAouYq2eog&utm_content=68604060&utm_source=hs_email#:~:text=Attackers%20breached%20Five%20Guys%20servers,incident%20and%20the%20criminals%20demands.
- 21 // https://www.databreaches.net/blackcat-claims-they-hacked-reddit-and-will-leak-the-data/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=73122413&_hsenc=p2ANqtz-CJi9WU6KEvZ-kGhAx3Qjzlp3b1NFzAawsPtlu3lFUY2LDl2B5m_dbkPdazocS0AJpg09wKjWShuTOT6sAaw0wmQ&utm_content=73118939&utm_source=hs_email
- 22 // <https://www.slycyber.io/mgm-and-caesar-casino-hacks-explained/>
- 23 // <https://www.bloomberg.com/news/articles/2023-09-13/mgm-caesars-hacked-by-scattered-spider-in-span-of-few-weeks?sref=y3YMCJ4e>
- 24 // <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphv-blackcat-ransomware-variant>

PAGE 9

- 25 // <https://www.inforisktoday.co.uk/clop-goanywhere-attacks-have-now-hit-130-organizations-a-21526>
- 26 // <https://www.slycyber.io/cl0p-orchestrates-mass-attack-with-moveit-transfer-zero-day/>
- 27 // <https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/>
- 28 // <https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/>

PAGE 10

- 29 // https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_
- 30 // <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>
- 31 // <https://www.bitdefender.com/blog/businessinsights/hive-ransoms-offspring-hunters-international-takes-the-stage/>

PAGE 11

- 32 // <https://www.slycyber.io/threat-intelligence-on-vice-societys-dark-web-footprint/>
- 33 // <https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/>
- 34 // <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a>

PAGE 12

- 35 // https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=73625306&_hsenc=p2ANqtz-8kRD3wjLcq7AEtqrLdiDt7OqWSebt9EhYyTCHVXS4OHQr-aZnnD1bs22TACEGELVqdHA5nhu_J1KTLh8va70KrbajQ&utm_content=73612237&utm_source=hs_email
- 36 // https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=73625306&_hsenc=p2ANqtz-8kRD3wjLcq7AEtqrLdiDt7OqWSebt9EhYyTCHVXS4OHQr-aZnnD1bs22TACEGELVqdHA5nhu_J1KTLh8va70KrbajQ&utm_content=73612237&utm_source=hs_email
- 37 // https://krebsonsecurity.com/2023/09/whos-behind-the-8base-ransomware-website/?utm_campaign=News%20and%20Insights&utm_medium=email&_hsmi=76730525&_hsenc=p2ANqtz-8R3XwhDb-gDeaZL7YpS6paDoSTwAS9DOzcfTldru5bwo7855Shtvnc1qikV75JagHng9t9X744uy27gdo-677xs-aUvQ&utm_content=76730908&utm_source=hs_email
- 38 // <https://www.bbc.com/news/entertainment-arts-67544504>
- 39 // <https://www.computerweekly.com/news/366561917/Rhysida-ransomware-gang-hits-hospital-holding-royal-families-data>
- 40 // <https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/>

PAGE 13

- 41 // <https://stairwell.com/resources/akira-pulling-on-the-chains-of-ransomware/>

VISIT **WWW.SLYCYBER.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

900 16th Street NW,
Suite 450, Washington,
DC 20006
United States