Cyberint
A Check Point Company

Ransomware Q3 2024 Report

October 2024

Table of Contents

Executive Summary

Although 2024 began with a Q1 decline in the frequency of ransomware attacks, the second quarter was underscored by a return to a much more intimidating world of ransomware attacks globally, and the third quarter continues the trend of the second.
In Q2 2024, the number of attacks stood at 1,277 cases, but Q3 saw a small decrease of 5.5% with 1209 cases.

Although the numbers remain pretty much the same, the dominance of ransomware groups changed, where the RansomHub group is taking the first place crown from LockBit after 2 years.

Interestingly, this quarter, the top 10 ransomware groups were responsible for 58.3% of all attacks. Compared to the previous year, this highlights the significant influence of new ransomware groups and the highest number of active groups on record, indicating a decline in dominance by historically significant groups in the ransomware landscape.

Nevertheless, it is no surprise that the U.S. continues to be the country most targeted by ransomware, while business services is the most targeted sector, similar to last quarter statistics.

There is no doubt that the new faces introduced to the industry, along with ongoing attacks on businesses around the world, claimed many victims. This, combined with the consistency of the industry's leaders – RansomHub, Play, LockBit3.0, Meow, and Hunters - led to devastating results for companies worldwide, such as Young Consulting, Halliburton, and others.

Statistics

As noted, the ransomware sector recorded 1,209 victims this quarter, marking a small decrease of approximately 5.5% compared to the second quarter of 2024.

Top Families

While it was a successful quarter for the entire ransomware industry, three families stood out. The new leader, RansomHub was the most dominant ransomware group, with 195 new victims, 16.1% of all ransomware cases. For the first time since 2022 LockBit are not in first place!

Coming second is the Play ransomware group, which claimed a significant 89 victims, 7.3% of all ransomware cases. As expected, Play continues to be a dominant power in the ransomware landscape.

The third place is saved for the LockBit group, which claimed 85 successful attacks this quarter, marking a new low for the group, with the lowest number of attacks per quarter in a year and a half.

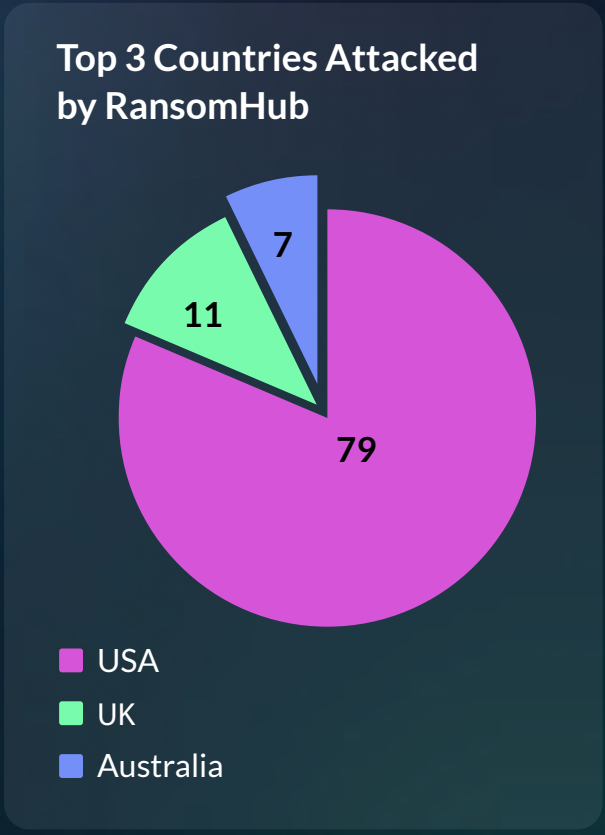
Figure 1

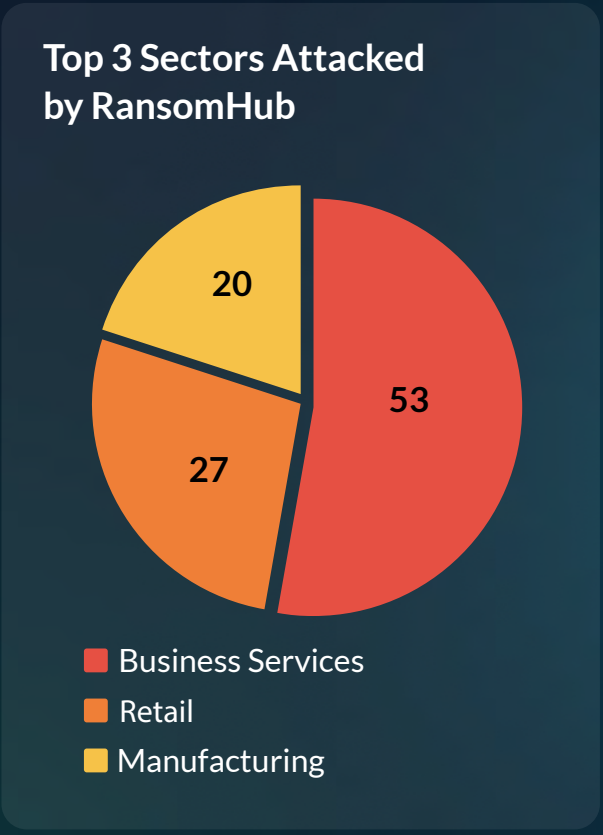
Top 10 Ransomware Families in Q3

RansomHub

RansomHub has quickly risen to prominence in the ransomware landscape, capitalizing on the disruption of major players like ALPHV and LockBit. With its roots likely in Russia and connections to former ALPHV affiliates, the group has established itself as a formidable force by leveraging its Ransomware-as-a-Service (RaaS) model, which offers attractive profit-sharing terms to affiliates. This approach has led to a surge in attacks, particularly in August and September 2024, when over half their attacks took place.

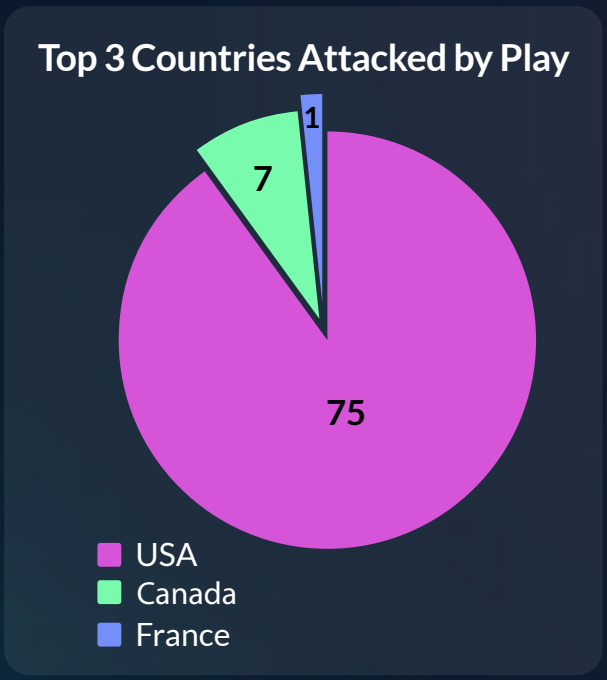
Another interesting fact is that the attack count of those two months represents more than 10% of all ransomware attacks we tracked this quarter!





Play

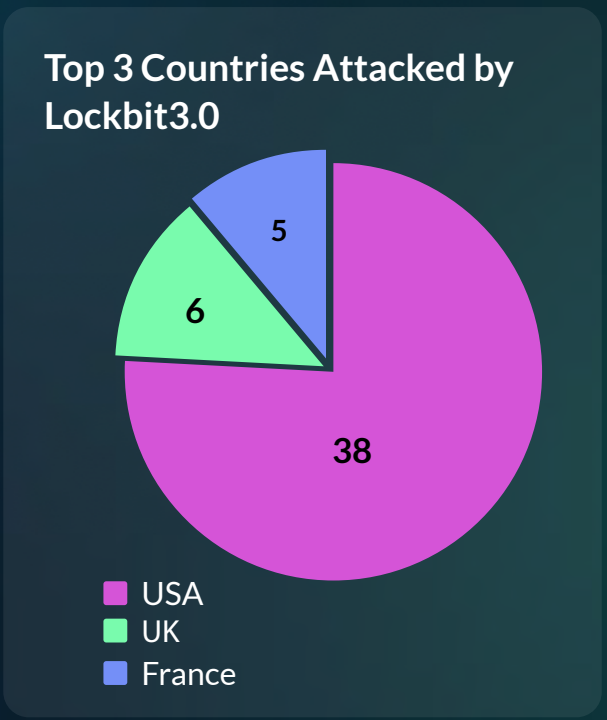
The ransomware syndicate responsible for numerous destructive assaults on significant American municipalities has purportedly executed over 560 successful attacks since June 2022. Researchers uncovered a Linux variant of the Play ransomware that only encrypts files when running in a VMWare ESXi environment, which assists them in wider operations. If not hindered, Play is going to break its own record of yearly victims in 2024 (301).

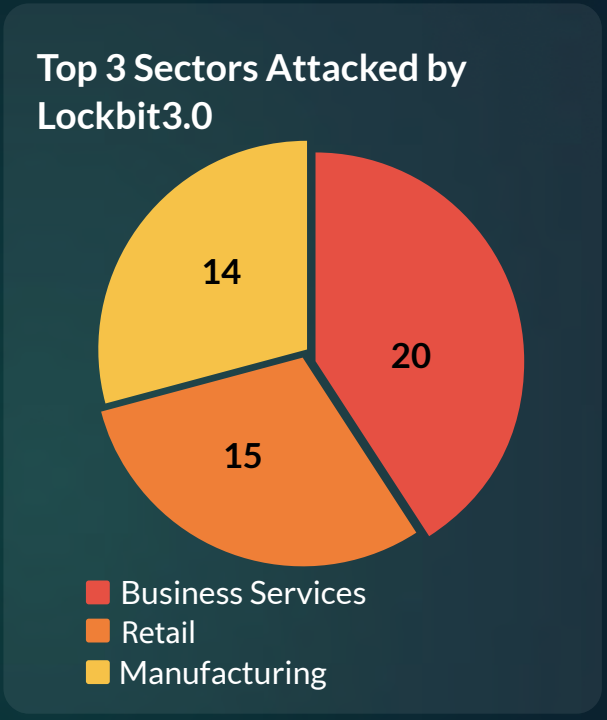


LockBit3.0

Since Operation Cronos, which disrupted LockBit's affiliate program and exposed one of its leaders, Dmitry Khoroshev (known as 'LockBitSupp'), the group's operations have significantly declined. For the first time in two years, LockBit has fallen to third place among ransomware groups this quarter. This marks a notable shift in their activity level following these law enforcement actions.
In Q3, LockBit attacked almost 60% less companies than Q2, showing the massive impact of law enforcement operations.

Despite these major operations against the group, LockBit continued its global onslaught against organizations, maintaining its position in the top 3 ransomware groups as long as possible.





Top Countries

Regarding the most targeted countries (Figure 2), the U.S. remains the number one targeted country globally, with good reason. 50% of the total ransomware attacks targeted the world's number one economy i.e. 599 cases.

The second most targeted country this quarter was the Canada, with 73 cases, lagging far behind the U.S.

Finally, United Kingdom was in third place with 59 ransomware cases this quarter.
Even when focusing on the top three countries, there is no doubt that the U.S. is the most profitable country for threat actors.

Figure 2

Top 10 Targeted Countries by Ransomware - Q3 2024

USA	Canada	UK	Italy	Brazil
50%	6%	5%	3%	3%

Germany	Spain	Australia	France	Israel
2%	2%	2%	2%	2%

Top Sectors

As expected, the business services sector was the most targeted in Q3, with 27% of the ransomware cases, followed by the retail and manufacturing sectors, with 18% and 11%, respectively (Figure 3).

Figure 3

Top 10 Targeted Industies by Ransomware - Q3 2024

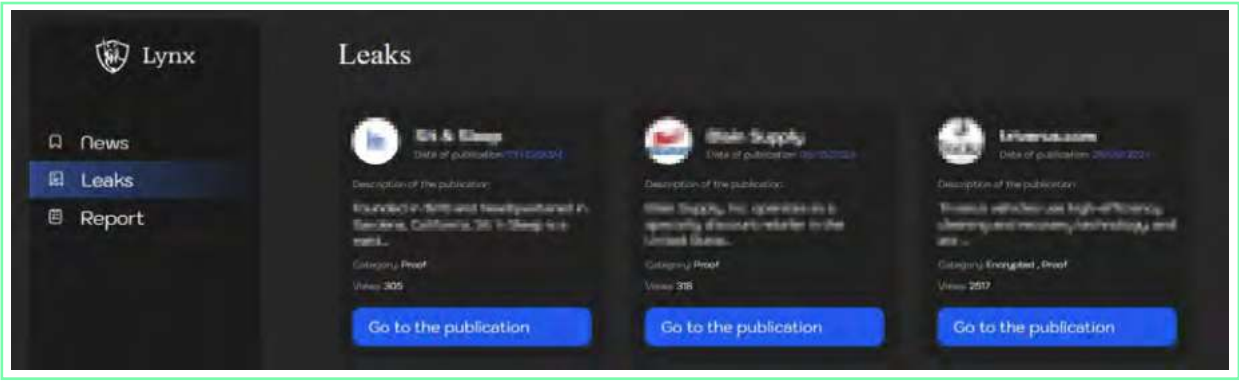
Business Services	Retail	Manufacturing	Finance	Construction
27%	18%	11%	6%	6%

Healthcare	Government	Education	Automotive	Technology
6%	5%	5%	3%	3%

Newcomers

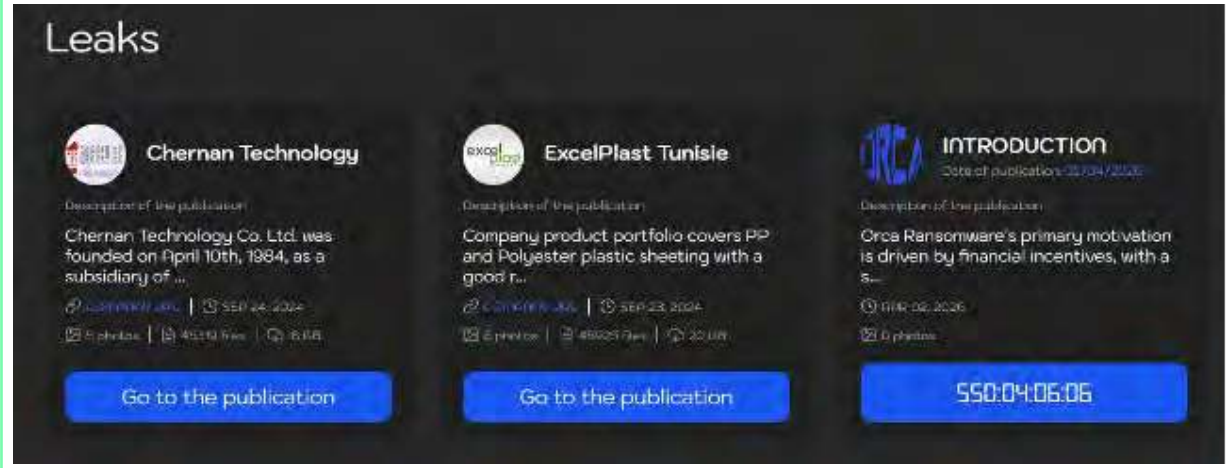
Lynx

Lynx, a double-extortion ransomware group, has been highly active recently, listing numerous companies as victims on their site. However, the group claims to avoid targeting government entities, hospitals, non-profits, and other socially crucial sectors. Once inside a system, Lynx encrypts files, adds the .LYNX extension, and leaves a ransom note titled "README.txt" in multiple directories. At the time of this report, Lynx had claimed over 28 victims, highlighting their ongoing activity in the ransomware landscape.



Orca

Orca Ransomware hit 2 victims in September 2024, Chernan Technology from Taiwan, and ExcelPlast Tunisie from Tunisia. According to them (taken from their DLS 'introduction'): "Orca Ransomware's primary motivation is driven by financial incentives, with a strong commitment to avoiding unnecessary harm to organizations. We understand the importance of ethical considerations in the quest for financial success and adhere to a strict policy against targeting government institutions, hospitals, or non-profit organizations, as these sectors are crucial to society."



The ransomware leak page pertaining to Chernan Technology contains limited information, primarily focused on the company's name. There are no specified compromise dates, nor any significant content extracted from the site such as paragraphs or descriptions. The presence of images is also absent, indicating a streamlined leak with minimal visual components.

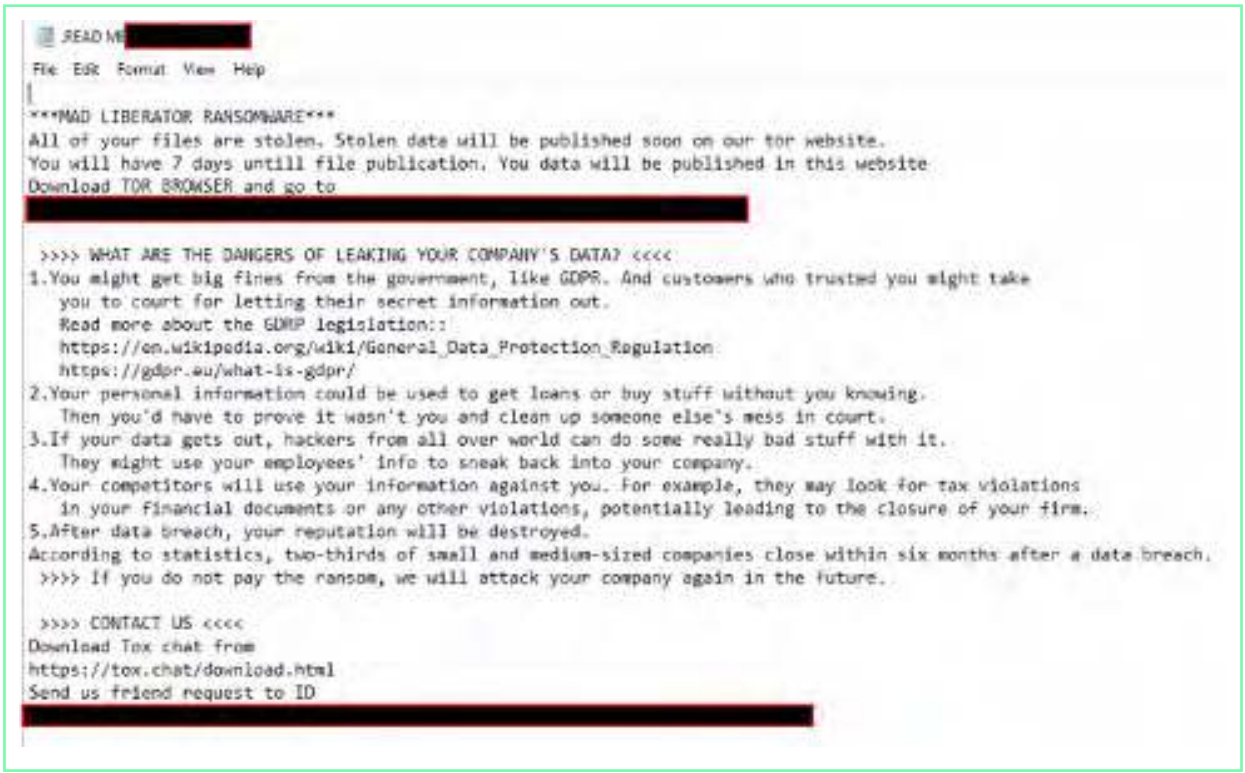
No download links are provided on the page, which suggests that the data disclosure may not have involved direct access to sensitive files or documents typically associated with ransomware incidents. The nature of the leak remains unspecified, and further details about Chernan Technology's activities or the implications of the ransomware attack are not available in the current summary.

Mad liberator

The Mad Liberator ransomware group, active since July 2024, focuses on data exfiltration rather than data encryption. Like other extortion groups, they maintain a leak site where they publicly list their victims.

Mad Liberator relies on social engineering to infiltrate its targets, specifically those using remote access tools such as Anydesk. The group deploys malware that mimics a Windows Update screen to make it appear as though the system is updating. This decoy screen, which performs no real updates, is likely designed to evade detection by most antivirus software. To prevent users from exiting the fake update screen using the "Esc" key, the attacker disables keyboard and mouse input through Anydesk, keeping the deception in place.

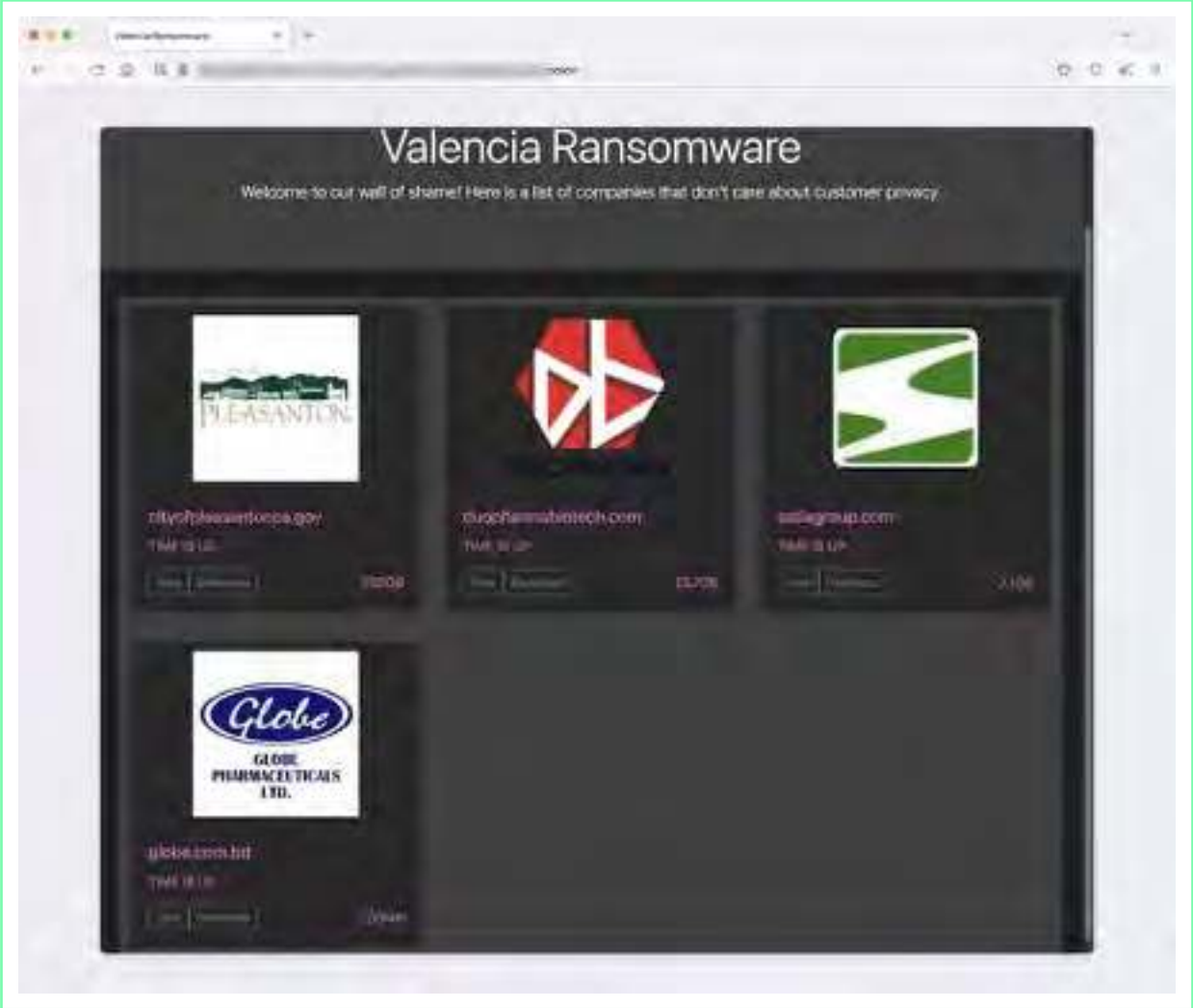
Once inside, the attacker uses Anydesk to access the victim's OneDrive account and files on a central server through a mapped network share, transferring data using Anydesk's FileTransfer feature. Afterwards they run an Advanced IP Scanner to identify other vulnerable devices but do not attempt lateral movement. Instead, they create ransom notes across multiple locations on a shared network, without leaving them on the victim's device.



Researchers highlighted this attack chain as a reminder of the importance of continuous staff training and clearly defined IT policies for remote access sessions. They also recommend that administrators use Anydesk Access Control Lists to restrict connections to trusted devices only.

Valencia Leaks

A new ransomware group has begun leaking data it claims to have stolen from five organizations across the globe. Recently, Valencia Ransomware has added links to its DLS, offering gigabytes of allegedly exfiltrated data for download. The victims appear to include a California municipality, a pharmaceutical company, and a paper manufacturer.

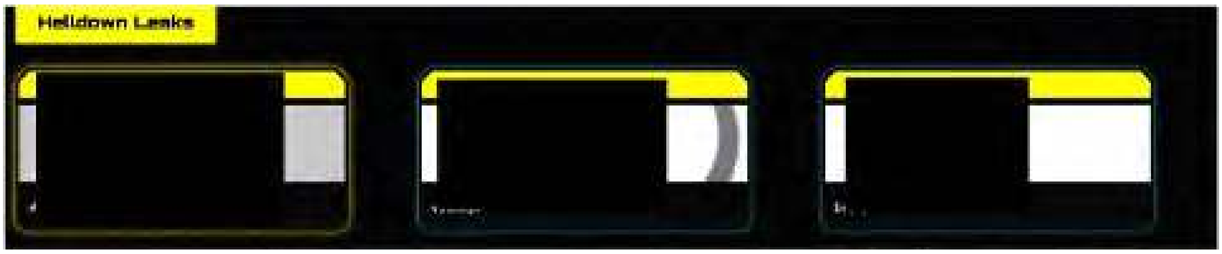


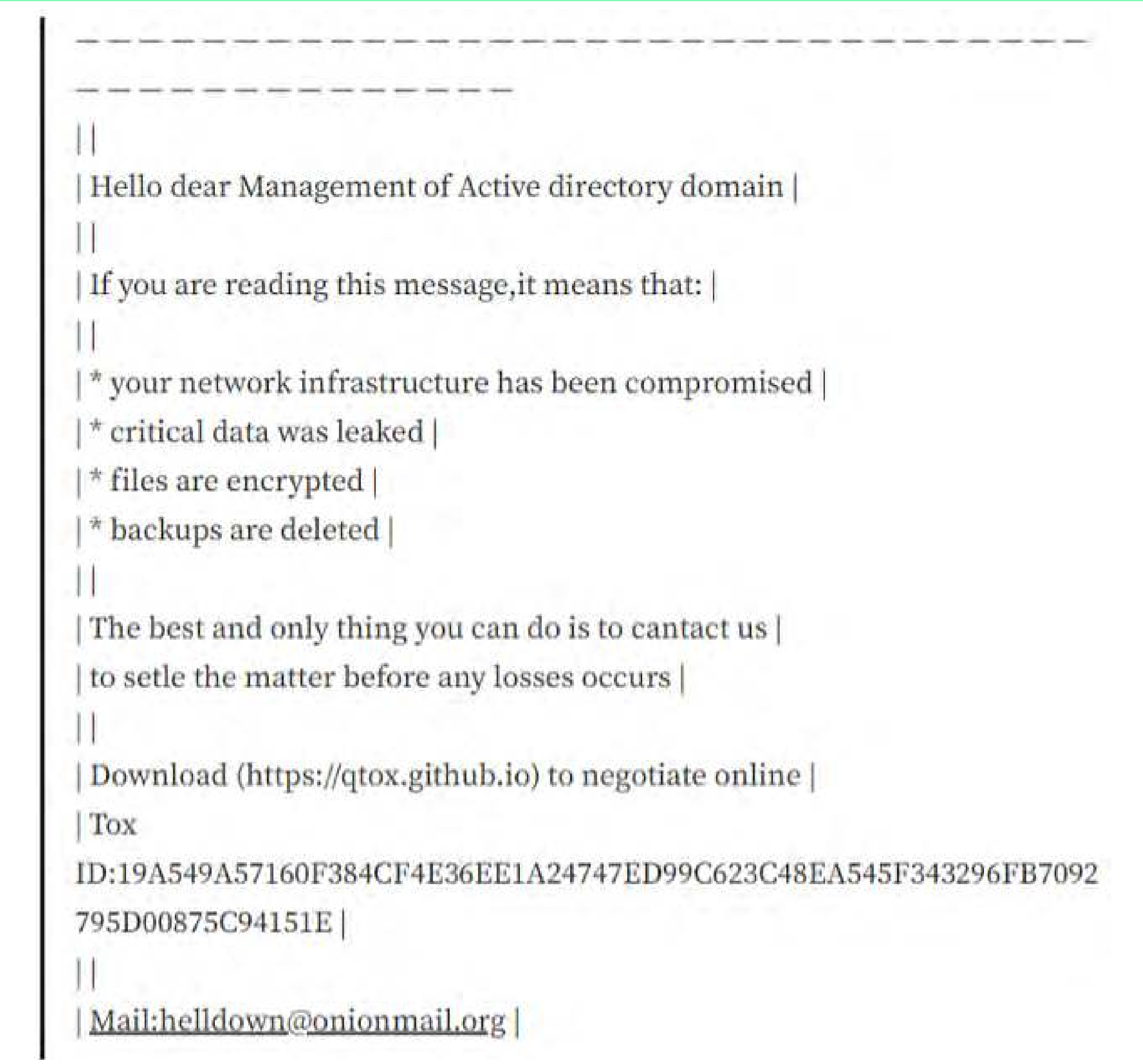
The reported victims are the City of Pleasanton in California, where attackers claim to have taken 283GB of sensitive data; Malaysia's Duopharma Biotech with 25.7GB; Indian paper manufacturer Satia with 7.1GB; and Bangladeshi drug company Globe Pharmaceuticals with 200MB. Additionally, Spanish fashion giant Tendam is also rumored to be a target, which is especially concerning as they were also reportedly struck by Medusa ransomware earlier this month.

There is growing speculation that some Valencia group attacks may be connected to critical vulnerabilities found in the WhatsUp Gold network monitoring software from Progress. These vulnerabilities, that allow attackers to take over admin accounts, were discovered and responsibly disclosed in May, with a proof-of-concept exploit released in late August.

Helldown

Helldown is an emerging ransomware group that listed 17 victims on its leak site last month. Despite being relatively new, Helldown has rapidly gained a reputation in the cybersecurity community for its aggressive tactics. The group uses advanced encryption methods, including AES, Salsa20, and RSA, while maintaining a high level of anonymity through the dark web and cryptocurrency transactions. Known for exploiting vulnerabilities to breach networks and disable security measures, Helldown primarily targets the IT services, telecommunications, and manufacturing sectors. Their approach of exfiltrating sensitive data and threatening to release it publicly unless a ransom is paid has proven both highly effective and destructive.

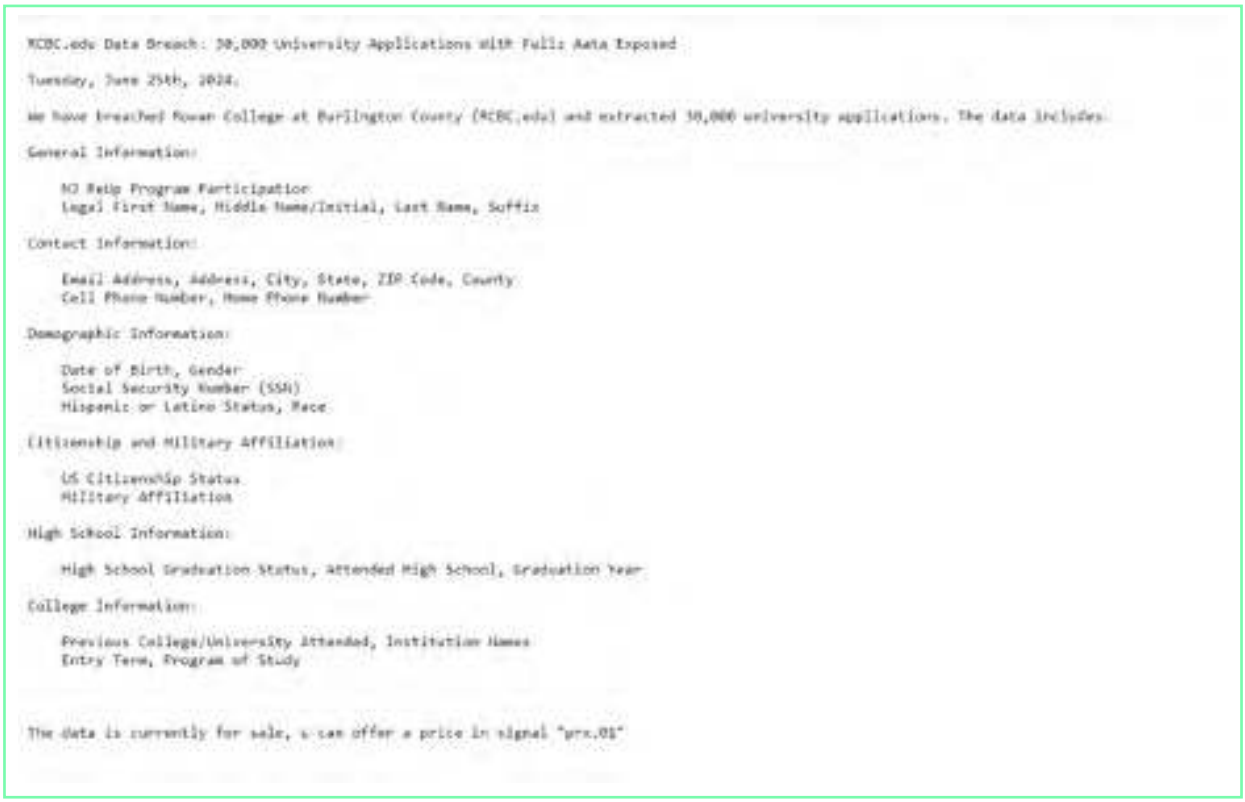



\- -

| |
| Hello dear Management of Active directory domain |
| |
| If you are reading this message,it means that: |
| |
| * your network infrastructure has been compromised |
| * critical data was leaked |
| * files are encrypted |
| * backups are deleted |
| |
| The best and only thing you can do is to cantact us |
| to setle the matter before any losses occurs |
| |
| Download (https://qtox.github.io) to negotiate online |
| Tox ID:19A549A57160F384CF4E36EE1A24747ED99C623C48EA545F343296FB7092795D00875C94151E |
| |
| Mail:helldown@onionmail.org |

Pryx

A new ransomware group, "Pryx," has recently appeared on the cybercrime scene, claiming responsibility for its first major attack. Pryx announced that it compromised the systems of Rowan College in Burlington County (RCBC.edu) and stole 30,000 university applications. According to the group, they successfully breached the college's IT systems and obtained sensitive data from the institution. This disclosure was made via their data leak site, accessible through both the regular internet and the dark web.



RCBC.edu Data Breach: 30,000 University Applications With Full Data Exposed

Tuesday, June 25th, 2024.

We have breached Rowan College at Burlington County (RCBC.edu) and extracted 30,000 university applications. The data includes:

General Information:

NJ Help Program Participation
Legal First Name, Middle Name/Initial, Last Name, Suffix

Contact Information:

Email Address, Address, City, State, ZIP Code, County
Cell Phone Number, Home Phone Number

Demographic Information:

Date of Birth, Gender
Social Security Number (SSN)
Hispanic or Latino Status, Race

Citizenship and Military Affiliation:

US Citizenship Status
Military Affiliation

High School Information:

High School Graduation Status, Attended High School, Graduation Year

College Information:

Previous College/University Attended, Institution Names
Entry Term, Program of Study

The data is currently for sale, u can offer a price in signal "pryx.01"

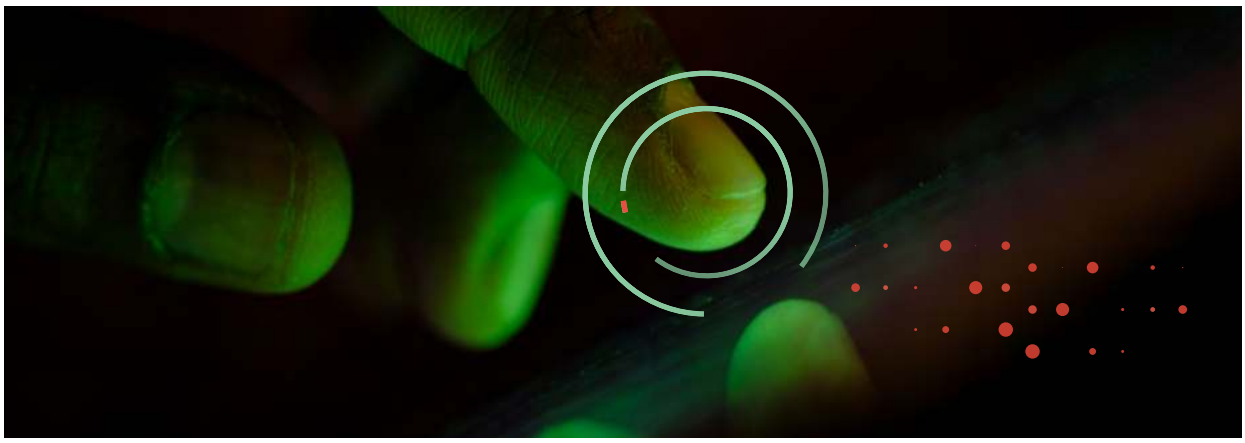
Pryx operates a data leak site where they publicly expose information about victims who refuse to pay the ransom. This platform is accessible to the public on the internet, as well as, like many ransomware groups, through the dark web.

Pryx's data leak site presents an ominous interface, with a spider web motif and the slogan "Get Pryxed" prominently displayed. The platform is organized into sections like Contact Information, Public PGP Key, All Updates, and Breaches and Operations by Pryx. The homepage boldly invites visitors to "Get Pryxed," reflecting the group's aggressive and provocative style.

Ransomcortex

Recently, On July 2024, the landscape of cyber threats has been enriched by the emergence of a new ransomware group named “Ransomcortex”. This group is distinguished by its specialization in attacking healthcare facilities, having already collected four victims within a few days of its first appearance. Among these, three are Brazilian healthcare facilities and one is Canadian.

Unlike many other ransomware groups, Ransomcortex has concentrated its efforts solely on attacking healthcare facilities. This targeted approach raises concerns about what criminals gain if ransoms are not paid. The answer lies in the intrinsic value of healthcare data, which can be exploited in various ways. Criminals can commit financial fraud by using patients’ personal information to open bank accounts, apply for credit cards, or secure loans. They may also resort to extortion, threatening to release sensitive medical information unless their demands are met. Additionally, stolen medical data can be sold on the black market or used for phishing and online scams. Furthermore, the data can facilitate identity theft, where criminals create false identities using the personal information of patients.



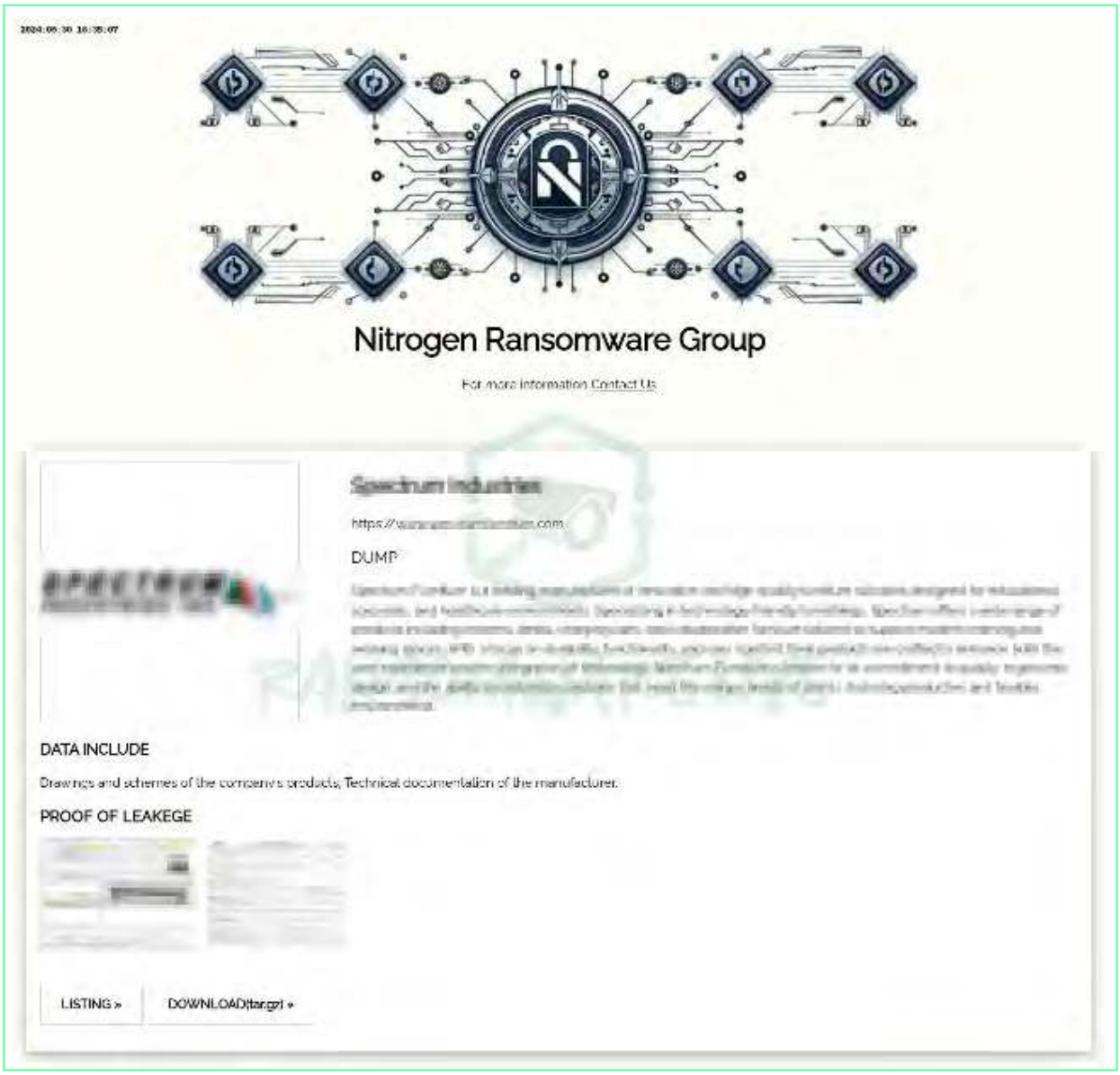
Vanir group

The group emerged on July 2024, hitting 3 victims in a short time and publishing them on their official data leak site. The 3 victims are from United states, China and Netherlands. All 3 of them were posted on the same day – 10/07/2024. The Vanir Group's website features an interactive terminal where users can input commands such as "help" for a list of available commands, "news" for updates about the group and their activities, and "victims" to view a list of all their targets.

However, the group's data leak site was seized by law enforcement, and it's been two months without any sign of their return:

Nitrogen

New ransomware group that published 6 victims on September 30. Currently their blog “Nitroblog” is down. 5 of the victims are from the USA, and one is from Canada.



Arrests

UK Arrests Teen Linked to MGM Resorts Ransomware Attack

UK authorities have arrested a 17-year-old suspected of involvement in the 2023 ransomware attack on MGM Resorts. The individual is thought to be part of the "Scattered Spider" hacking group, notorious for its social engineering tactics and high-profile cyberattacks. The MGM breach led to widespread disruption of its IT systems and compromised customer data. This arrest marks a key step in efforts to dismantle Scattered Spider's operations.

FBI Disrupts Dispossessor Ransomware Operation, Seizes Servers

On August 12, 2024, in a significant international collaboration, the FBI successfully disrupted the Radar/Dispossessor ransomware operation. The agency seized servers and websites associated with the group, marking a major victory against the cybercrime network. The takedown follows a thorough investigation involving law enforcement agencies worldwide, as they continue to target organized cybercriminal groups. This operation highlights ongoing efforts to dismantle ransomware organizations that have been responsible for numerous attacks globally.

Germany Seizes 47 Crypto Exchanges Linked to Ransomware Gangs

German authorities have successfully seized 47 cryptocurrency exchanges used by ransomware gangs for laundering illicit gains. This move is part of a larger effort to crack down on cybercriminal networks exploiting digital currencies to obscure their financial activities. These exchanges were found to have facilitated the laundering of funds linked to ransomware attacks, further highlighting the increasing use of cryptocurrencies by threat actors for illicit transactions.

The action comes as part of a coordinated global initiative to target platforms that provide ransomware operators with the financial infrastructure needed to hide their ransoms and profits. This effort demonstrates law enforcement's growing focus on digital currencies as a critical part of disrupting cybercriminal operations.

New Trends

Ransomware Groups Targeting Linux and VMware ESXi Systems and Developing New Capabilities

In recent years, ransomware groups have increasingly shifted their focus towards Linux-based systems and VMware ESXi servers, recognizing them as valuable targets within corporate infrastructures. These systems often host critical virtual machines (VMs) that, if compromised, can cause widespread disruption.

- Play Ransomware developed a Linux variant specifically to attack VMware ESXi servers, a hypervisor that is widely used in enterprise environments .
- Cicada3301 Ransomware followed a similar strategy by launching attacks on VMware ESXi servers, highlighting the growing focus on exploiting Linux-based virtualized environments .
- BlackByte and BlackBasta have also adapted their tactics, with BlackByte using vulnerabilities in VMware ESXi to launch attacks that exploit authentication bypass techniques, allowing them to encrypt virtual machines.

These attacks are part of a broader trend where ransomware operators target Linux systems due to the increasing reliance on these platforms for hosting critical business infrastructure. The growing focus on virtualization environments is also driven by the potential to impact large-scale operations with just one attack, as compromising ESXi servers can lead to encryption of numerous virtualized resources in one go.

Furthermore, ransomware capabilities have evolved considerably over the past year, with attackers developing more sophisticated techniques to evade detection and maximize damage. Black Basta, for instance, has adopted custom malware designed to bypass security tools, making it more evasive and effective against modern defenses. In addition, ransomware groups like RansomHub are leveraging legitimate tools like Kaspersky's TDSSKiller to disable endpoint detection and response (EDR) software, allowing them to operate undetected in compromised environments.

Another significant development is the abuse of cloud-based tools for data theft. For example, ransomware operators, including BianLian and Rhysida, are now using Microsoft's Azure Storage Explorer and AzCopy tools to steal data from victim networks and store it in cloud-based infrastructure, adding a new layer of complexity to their operations.

These developments demonstrate the growing sophistication of ransomware, with groups increasingly targeting more robust systems and leveraging new capabilities to outsmart security measures across various environments.

Major Incidents

Rhysida Ransomware Behind Port of Seattle Cyberattack in August 2024

In August 2024, the Port of Seattle was hit by a ransomware attack attributed to the Rhysida ransomware group. The attack disrupted the U.S. government agency responsible for Seattle's airport and seaport operations. While the exact details of the breach and its full impact are not entirely clear, it is known that the attack caused significant system outages over a span of three weeks.

RansomHub Claims Kawasaki Cyberattack, Threatens to Leak Stolen Data

The RansomHub ransomware group claims to have carried out a cyberattack on Kawasaki, a global manufacturer, threatening to leak stolen data unless a ransom is paid. The threat actors reportedly gained unauthorized access to sensitive company data and have issued an ultimatum, leveraging the potential exposure of this information to press for payment. As with other RansomHub operations, the group engages in double extortion tactics, encrypting files while threatening to expose sensitive information publicly.

Halliburton Confirms Data Stolen in Recent ransomware attack on August 2024

Halliburton, a major oil and gas services company, confirmed that sensitive data was stolen during a cyberattack in August 2024, linked to the RansomHub ransomware gang. The attack, which caused significant operational disruptions, led to systems being taken offline as the company worked with cybersecurity firm Mandiant and law enforcement to address the breach. While Halliburton has not disclosed detailed information about the stolen data, it was revealed that the ransomware group used a new version of their encryptor to carry out the attack, as part of a double extortion scheme aimed at both encrypting data and threatening to leak it unless a ransom is paid.

BlackSuit Compromised Data of Young Consulting Customers

Young Consulting, a prominent US software provider specializing in employer stop-loss insurance, confirmed that the BlackSuit ransomware group compromised the personal data of nearly a million customers.

Occurring in April, the breach involved unauthorized access and subsequent data encryption by the attackers. The compromised data included full names, Social Security numbers (SSNs), birth dates, and insurance claim details of clients, notably affecting Blue Shield of California subscribers.

Moreover, BlackSuit claims to have leaked extensive corporate data on its extortion site, including contracts, financial records, and personal employee information, heightening the risk of further illicit use of the exposed information.

Conclusions

In Q3 2024, the ransomware landscape saw minor changes, with a 5.5% drop in total attacks compared to the previous quarter. RansomHub led with 195 victims, accounting for 16.1% of all ransomware cases, while Play remained stable with 89 victims. LockBit, for the first time in two years, fell to third place with 85 attacks due to law enforcement pressure. The U.S. remained the top target, representing 50% of cases, while Israel entered the top 10, replacing India.

New players like Orca, Lynx, and Mad Liberator introduced different techniques, such as data exfiltration. Although fewer new groups emerged this quarter compared to the last, these developments reflect a constantly evolving ransomware landscape, with both established and newer groups competing for dominance.

Law enforcement actions worldwide continue to put pressure on ransomware groups, leading to the decline of major players like LockBit. As these large operations struggle, it's only a matter of time before other big and small ransomware groups follow the same path. The ongoing crackdown has created a more hostile environment for these groups, signaling that their dominance may not last much longer.

Overall, this quarter followed a similar pattern to the previous one. Aside from LockBit's decline and RansomHub's rise, there were no significant shifts in the ransomware landscape, maintaining consistency with Q2 trends.

Contact Us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm