GLOBAL CYBER THREAT INTELLIGENCE

ANNUAL REPORT 2023

WITH FURTHER *2024* PREDICTIONS

Prepared by

Cyberthint Threat Hunters

This report was prepared using Cyberthint Unified CTI Platform, Cyberthint's Dark Monitor, and analysis from Cyberthint threat hunters.

Prepared for

Community

cyberthint

Table of Contents

cyberthint

Unified Cyber Threat Intelligence Platform

We know what information hackers have on you!

Cyberthint is an unified cyber threat intelligence platform that allows you to take precautions against cyber threats that may affect your company and employees in cyberspace.

Be aware of cyber threats targeting your organization in advance with Cyberthint's advanced cyber threat intelligence technology!

Everything you need is on a single platform!

Observe and Prevent to Avoid Being Hunted

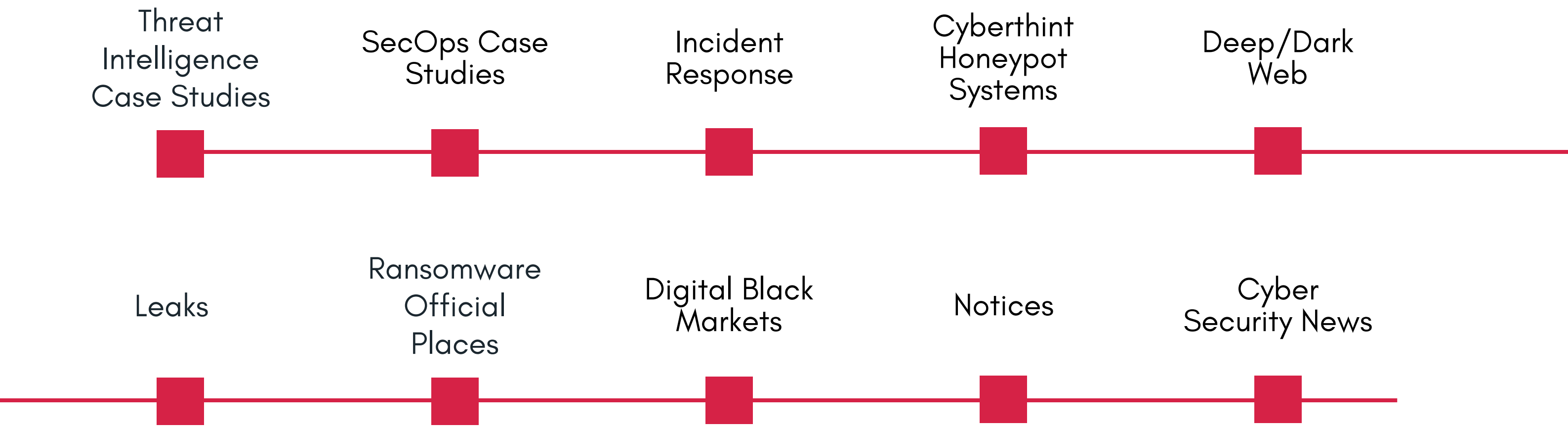
Cyberthint is an organization that protects your assets with an integrated digital vision with more than 15 years of experience in the cyber security world.

Improvised threats that fall outside the foreseen risks in workflows can be overlooked. As cybersecurity professionals, we have ambitiously realized the idea of early detection of behind-the-scenes movements that may pose a risk to organizations with an "automated cyber patrol approach".

Cyberthint provides ideal cyber threat intelligence and security solutions for your organization with its capabilities.
We can help you protect your brands and IT infrastructure with a preventive threat intelligence approach.

About the Report

This cyber threat intelligence report stats prepared by Cyberthint, which includes important cyber events that took place in 2023 at the global level, cases encountered by Cyberthint's & Seccops's teams, observations and analysis, also includes threat predictions for 2024.



Threat Intelligence Case Studies

SecOps Case Studies

Incident Response

Cyberthint Honeypot Systems

Deep/Dark Web

Leaks

Ransomware Official Places

Digital Black Markets

Notices

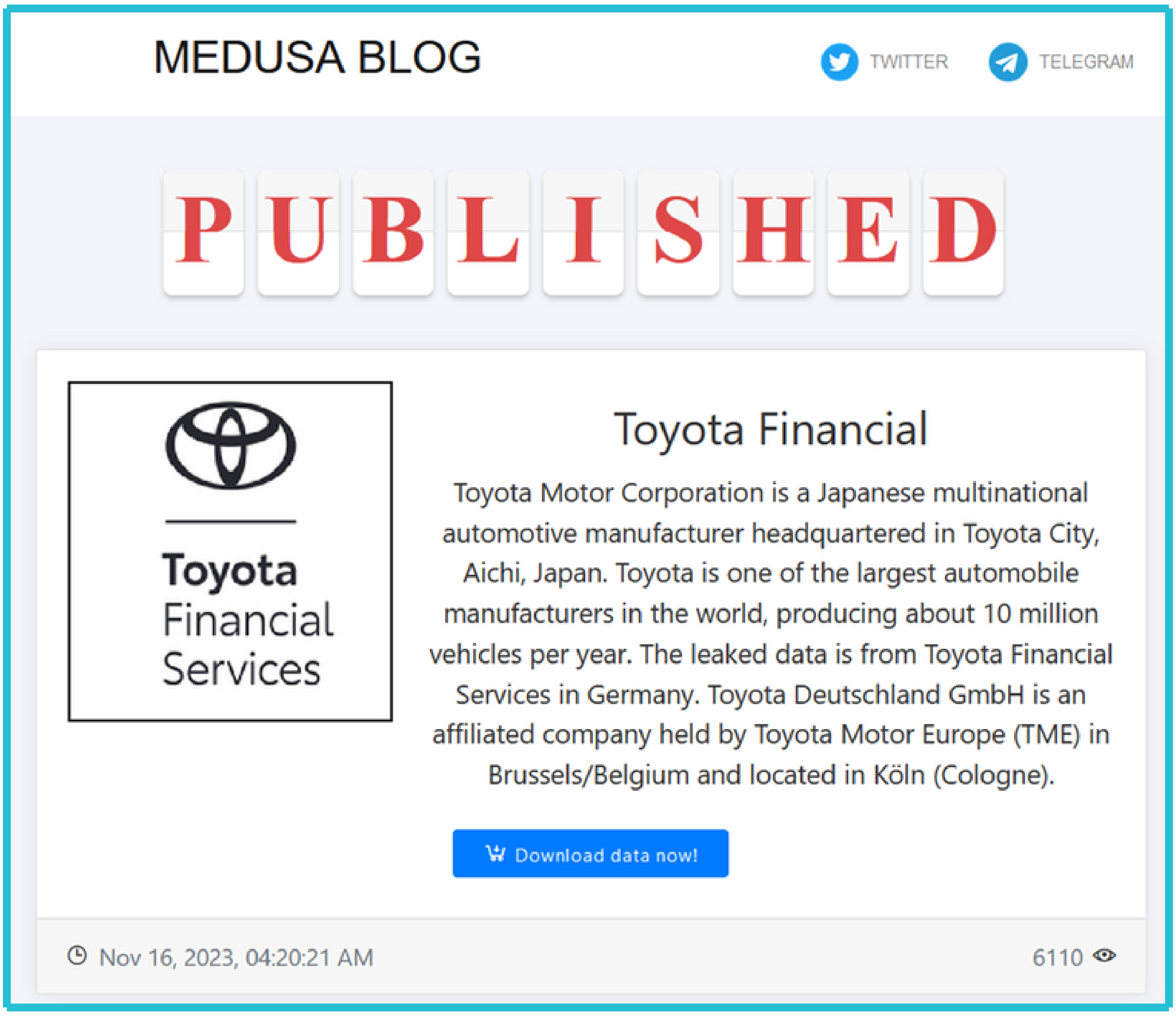
Cyber Security News

Ransomware Attacks/News

Section 1

Toyota

Toyota Financial Services (TFS) was attacked by the Medusa ransomware group in November. Medusa requested a ransom of $8 million to remove the data from their systems and gave Toyota 10 days to contact them.
A Toyota spokesman announced in a statement that unauthorized access was detected on some of the company's systems in Europe and Africa. The company took some systems offline to get the breach which affected customer service under control.
After Toyota refused to pay the demanded ransom, the Medusa ransomware group posted all data related to Toyota on its own leak site on the Tor network.



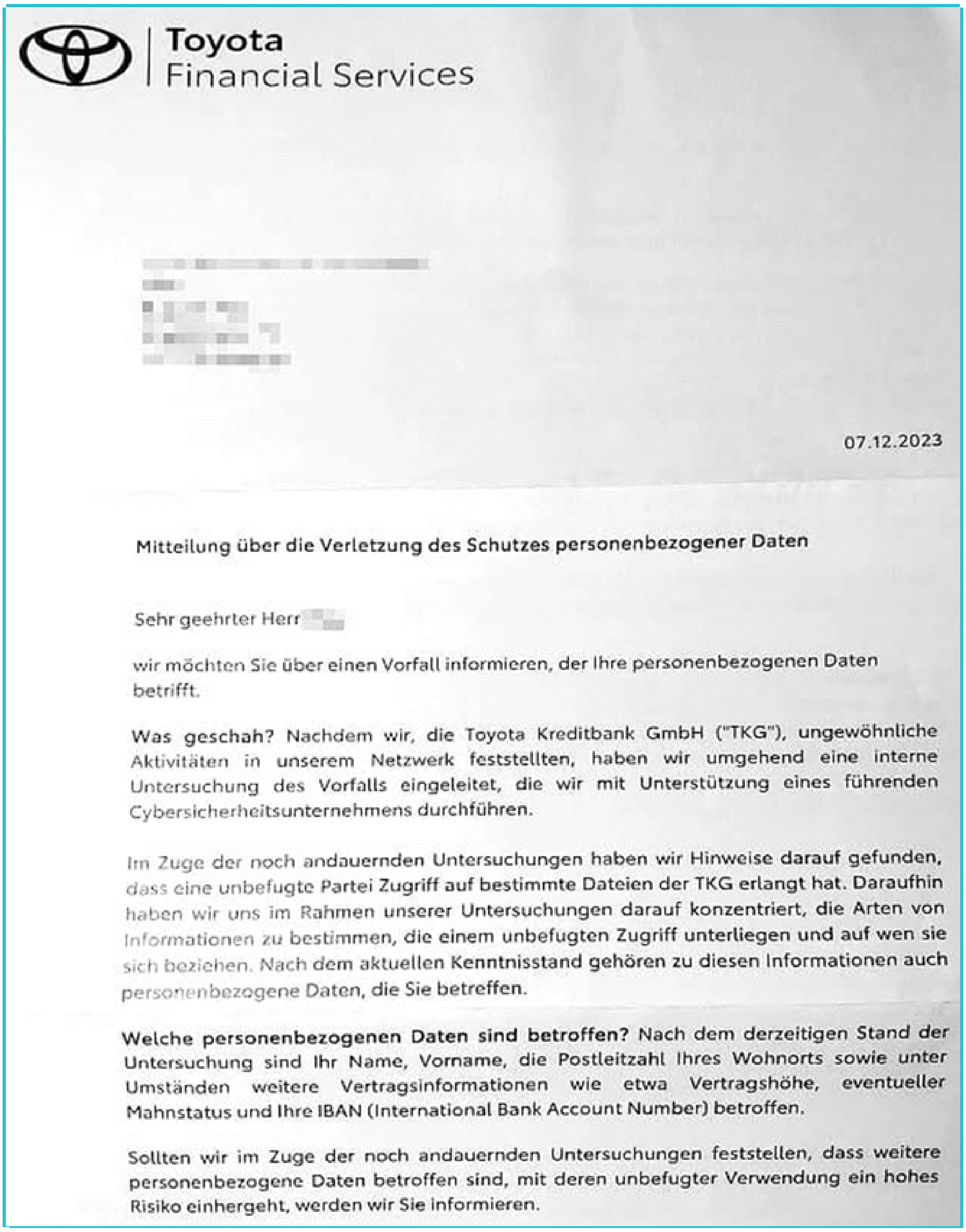
Toyota Financial

Toyota Motor Corporation is a Japanese multinational automotive manufacturer headquartered in Toyota City, Aichi, Japan. Toyota is one of the largest automobile manufacturers in the world, producing about 10 million vehicles per year. The leaked data is from Toyota Financial Services in Germany. Toyota Deutschland GmbH is an affiliated company held by Toyota Motor Europe (TME) in Brussels/Belgium and located in Köln (Cologne).

Nov 16, 2023, 04:20:21 AM

Toyota

In early December, Toyota Kreditbank GmbH, operates in Germany, was identified as one of the affected entities. The company acknowledged that hackers had gained access to customers' personal data and sent a statement to German customers to inform them about the leaked information.



Toyota
Financial Services

[redacted]

07.12.2023

Mitteilung über die Verletzung des Schutzes personenbezogener Daten

Sehr geehrter Herr [redacted]

wir möchten Sie über einen Vorfall informieren, der Ihre personenbezogenen Daten betrifft.

Was geschah? Nachdem wir, die Toyota Kreditbank GmbH ("TKG"), ungewöhnliche Aktivitäten in unserem Netzwerk feststellten, haben wir umgehend eine interne Untersuchung des Vorfalls eingeleitet, die wir mit Unterstützung eines führenden Cybersicherheitsunternehmens durchführen.

Im Zuge der noch andauernden Untersuchungen haben wir Hinweise darauf gefunden, dass eine unbefugte Partei Zugriff auf bestimmte Dateien der TKG erlangt hat. Daraufhin haben wir uns im Rahmen unserer Untersuchungen darauf konzentriert, die Arten von Informationen zu bestimmen, die einem unbefugten Zugriff unterliegen und auf wen sie sich beziehen. Nach dem aktuellen Kenntnisstand gehören zu diesen Informationen auch personenbezogene Daten, die Sie betreffen.

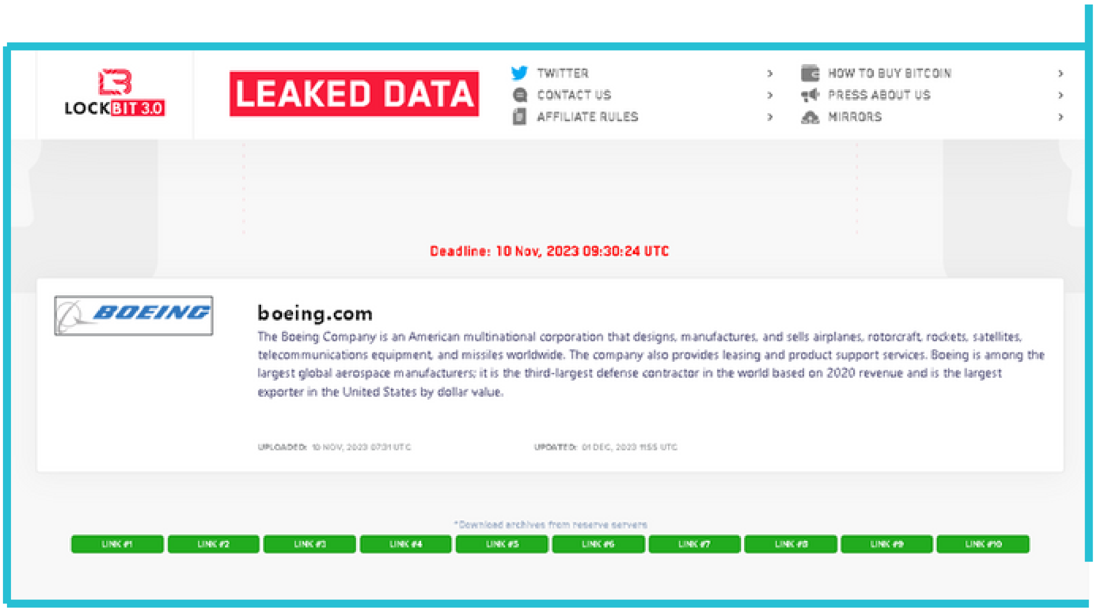
Welche personenbezogenen Daten sind betroffen? Nach dem derzeitigen Stand der Untersuchung sind Ihr Name, Vorname, die Postleitzahl Ihres Wohnorts sowie unter Umständen weitere Vertragsinformationen wie etwa Vertragshöhe, eventueller Mahnstatus und Ihre IBAN (International Bank Account Number) betroffen.

Sollten wir im Zuge der noch andauernden Untersuchungen feststellen, dass weitere personenbezogene Daten betroffen sind, mit deren unbefugter Verwendung ein hohes Risiko einhergeht, werden wir Sie informieren.

Boeing

On October 27, the Lockbit ransomware group announced that they had infiltrated the systems of Boeing, one of the world's largest aerospace companies, via their website on the Tor network and compromised "an enormous amount of sensitive data". The ransomware group gave Boeing some time until November 2 to contact them. While Boeing has not made any statement during this time, the LockBit group shared 4GB of data on November 10, and announced that they would share all information, including databases, if an agreement was not achieved. The shared data included configurations and backups of IT management software. The presence of Citrix backups among this data suggests that the recently discovered Citrix Bleed (CVE-2023-4966) vulnerability may have been exploited.

Following this, LockBit removed the company from its site, stating that negotiations had begun. Boeing was then added back to the LockBit ransomware group's website and the alleged data was leaked. This development shows that the company refused to pay the ransom. Over 40 GB of archive and backup files from Boeing are available for download on the group's website.



Deadline: 10 Nov, 2023 09:30:24 UTC

boeing.com

The Boeing Company is an American multinational corporation that designs, manufactures, and sells airplanes, rotorcraft, rockets, satellites, telecommunications equipment, and missiles worldwide. The company also provides leasing and product support services. Boeing is among the largest global aerospace manufacturers; it is the third-largest defense contractor in the world based on 2020 revenue and is the largest exporter in the United States by dollar value.

UPLOADED: 10 NOV, 2023 07:31 UTC

UPDATED: 01 DEC, 2023 11:55 UTC

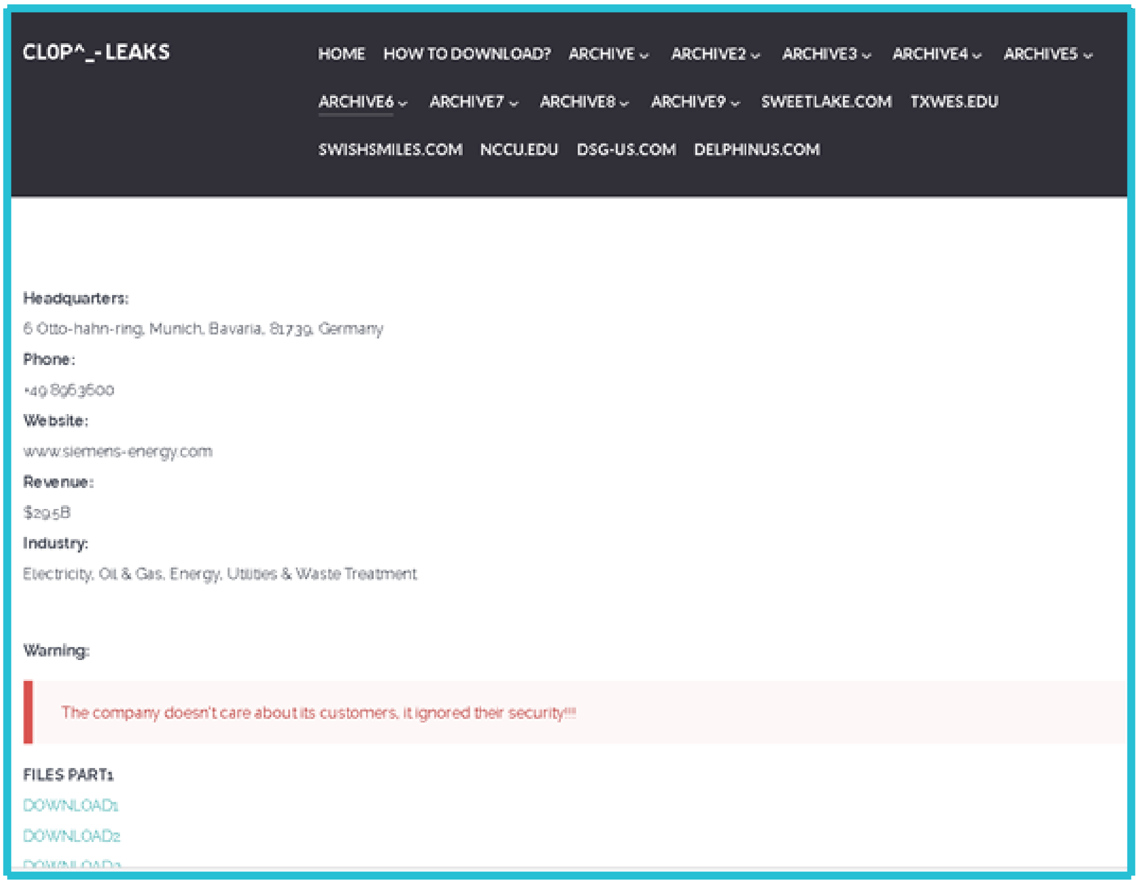
*Download archives from reserve servers

Following these events, Boeing has confirmed that part of its distribution business has experienced a cyberattack. The aerospace giant is aware that a ransomware group has published information allegedly taken from its systems, but has not yet shared any information about the scope of the potential data breach. The company reiterated that the cyber incident does not pose a threat to aircraft or flight safety.

Siemens

A Siemens Energy spokesperson confirmed the data theft carried out by the Cl0p ransomware group. The Cl0p ransomware group is known to have carried out the attack using the zeroday vulnerability identified as CVE-2023-34362 in the MOVEit Transfer platform.

The Cl0p ransomware group shared more than 16GB of data belonging to Siemens on its own leak sharing site on the Tor network. Cl0p ransomware continues to target leading European energy giants such as Siemens Energy.



Headquarters:
6 Otto-hahn-ring, Munich, Bavaria, 81739, Germany
Phone:
+49 8963600
Website:
www.siemens-energy.com
Revenue:
$29.5B
Industry:
Electricity, Oil & Gas, Energy, Utilities & Waste Treatment

Warning:

The company doesn't care about its customers, it ignored their security!!!

FILES PART1
DOWNLOAD1
DOWNLOAD2
DOWNLOAD3

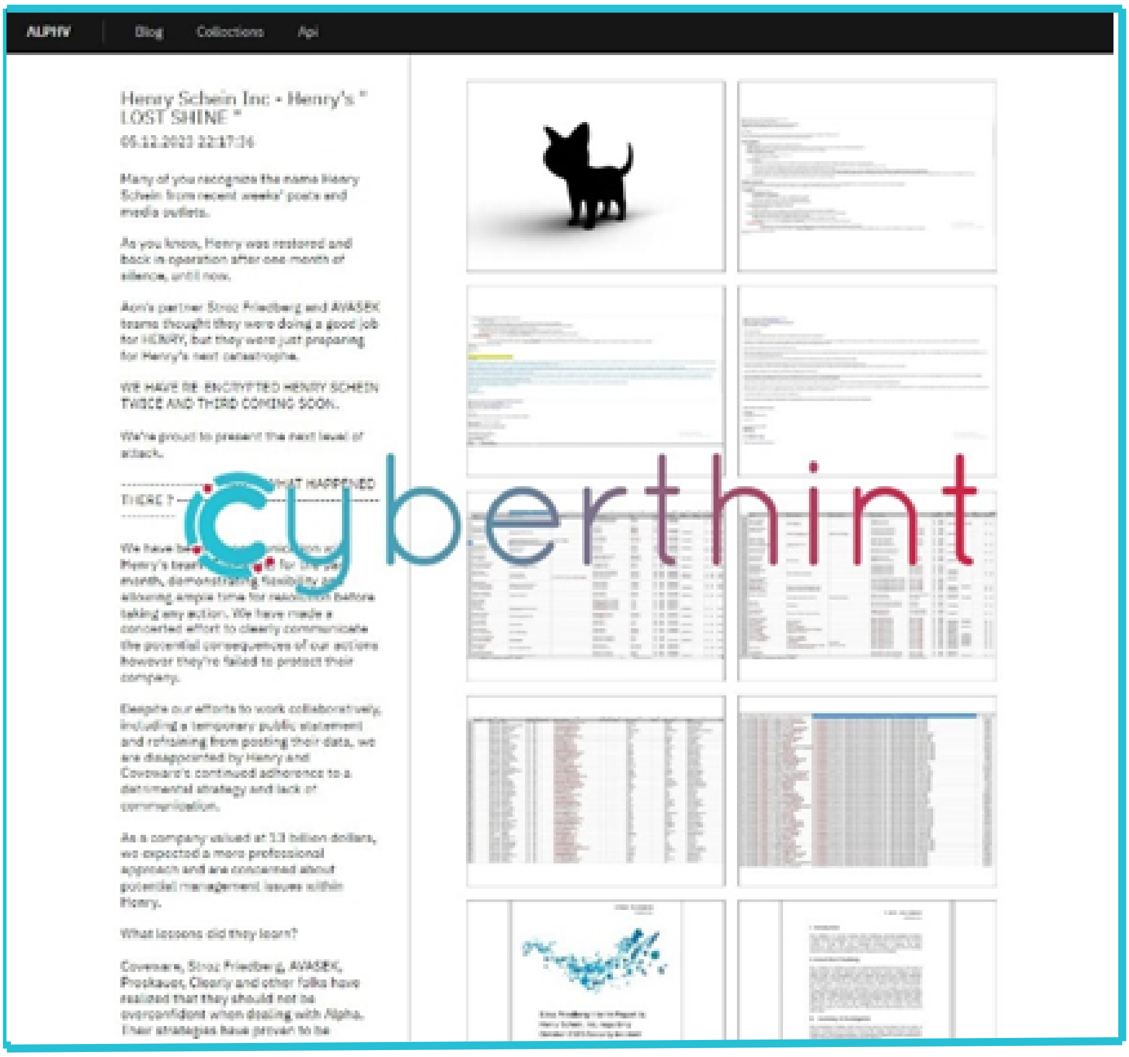
Ransomware Attacks Targeting Azure Cloud Storage Services

The BlackCat (ALPHV) ransomware gang is using the Sphynx encryptor to encrypt targeted Azure cloud storage services using stolen Microsoft accounts. Sophos X-Ops teams discovered that the attackers were using a new variant of Sphynx using stolen credentials. The attackers accessed the Sophos Central account with a stolen one-time password (OTP) to change security policies and encrypt Azure cloud storage services. In total, 39 Azure storage accounts were encrypted and the attackers infiltrated the victim's Azure portal using a stolen Azure key. Remote monitoring and management (RMM) tools such as AnyDesk, Splashtop and Atera were also utilized during the attack. Microsoft found that the Sphynx encryptor used Remcom and Impacket for lateral movement.

Henry Schein

ALPHV/BlackCat hackers have launched a third attack on the website of dental equipment supplier Henry Schein. The company's customer database, financial records and internal communications were compromised in the attack.

On October 15, Henry Schein reported a cyberattack affecting its manufacturing and distribution businesses, and two weeks later the BlackCat/ALPHV ransomware group claimed responsibility, saying they had stolen 35 terabytes of sensitive data by encrypting files.



Henry Schein Inc - Henry's " LOST SHINE "

05.12.2023 22:17:36

Many of you recognize the name Henry Schein from recent weeks' posts and media outlets.

As you know, Henry was restored and back in operation after one month of silence, until now.

Aon's partner Stroz Friedberg and AVASEK teams thought they were doing a good job for HENRY, but they were just preparing for Henry's next catastrophe.

WE HAVE RE-ENCRYPTED HENRY SCHEIN TWICE AND THIRD COMING SOON.

We're proud to present the next level of attack.

---------------- WHAT HAPPENED THERE ? ----------------

We have be[illegible] with Henry's team [illegible] for the past month, demonstrating flexibility and allowing ample time for resolution before taking any action. We have made a concerted effort to clearly communicate the potential consequences of our actions however they're failed to protect their company.

Despite our efforts to work collaboratively, including a temporary public statement and refraining from posting their data, we are disappointed by Henry and Coveware's continued adherence to a detrimental strategy and lack of communication.

As a company valued at 13 billion dollars, we expected a more professional approach and are concerned about potential management issues within Henry.

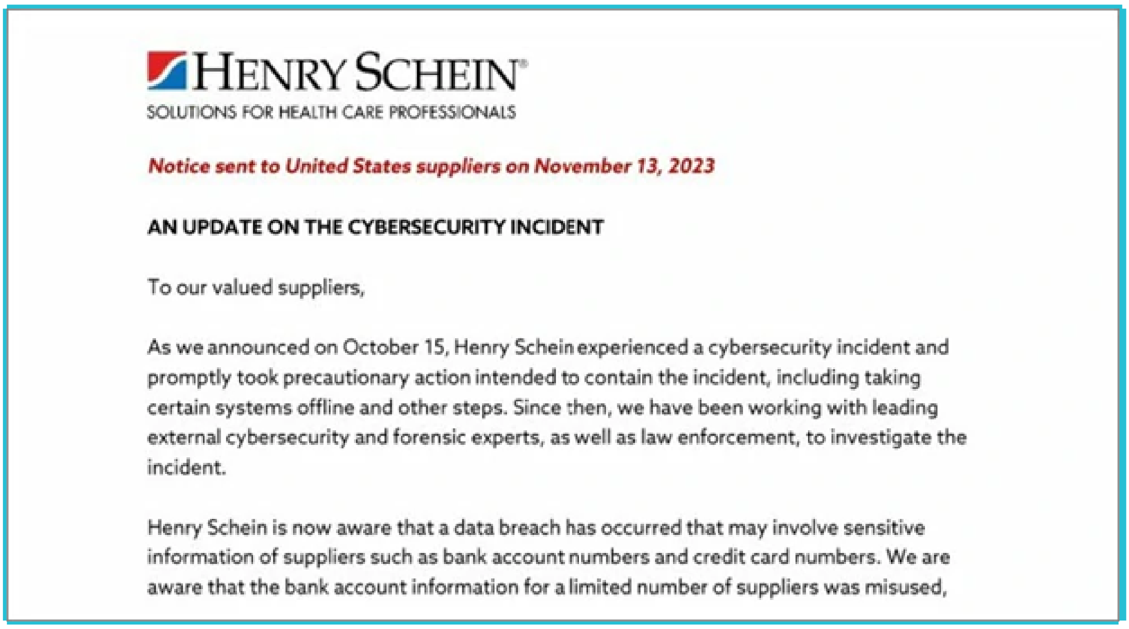
What lessons did they learn?

Coveware, Stroz Friedberg, AVASEK, Proskauer, Clearly and other folks have realized that they should not be overconfident when dealing with Alpha. Their strategies have proven to be

Henry Schein

ALPHV/BlackCat had previously has launched two attacks on Henry Schein. The first attack took place in April 2022 and the second in January 2023. In both attacks, the company's website was brought down and data was encrypted. The attackers demanded a ransom to decrypt the data, but Henry Schein refused to pay the ransom.

In their latest attack, ALPHV/BlackCat again demanded a ransom and threatened to leak the company's data. The company said it would not pay the ransom and publicized the attack.



HENRY SCHEIN®
SOLUTIONS FOR HEALTH CARE PROFESSIONALS

Notice sent to United States suppliers on November 13, 2023

AN UPDATE ON THE CYBERSECURITY INCIDENT

To our valued suppliers,

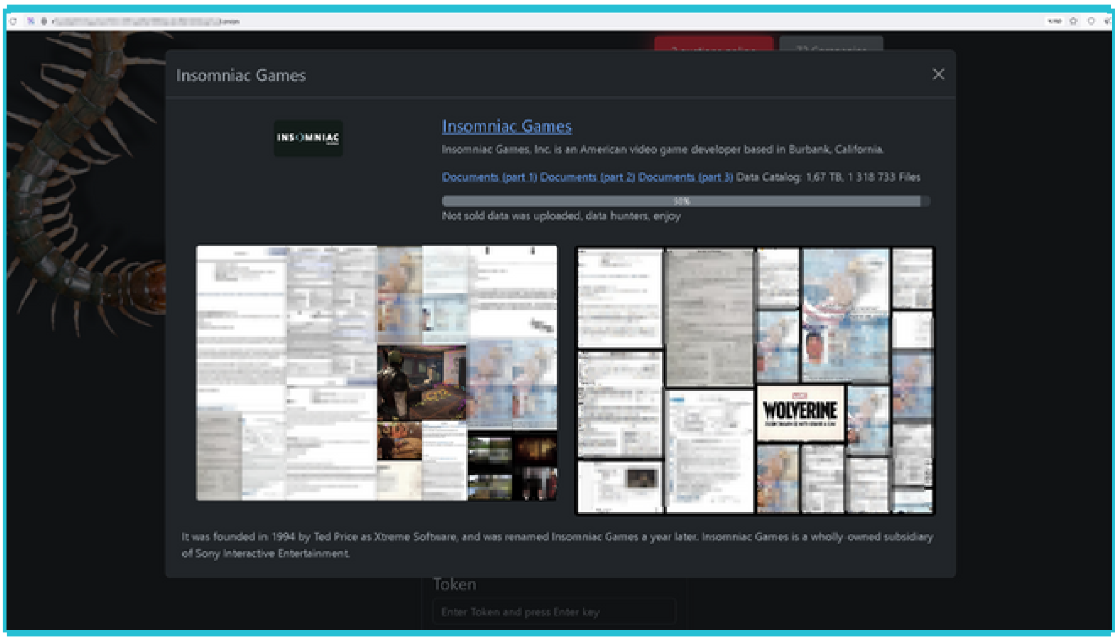
As we announced on October 15, Henry Schein experienced a cybersecurity incident and promptly took precautionary action intended to contain the incident, including taking certain systems offline and other steps. Since then, we have been working with leading external cybersecurity and forensic experts, as well as law enforcement, to investigate the incident.

Henry Schein is now aware that a data breach has occurred that may involve sensitive information of suppliers such as bank account numbers and credit card numbers. We are aware that the bank account information for a limited number of suppliers was misused,

Insomniac Games

On December 11th, the Rhysida ransomware group launched an attack on Insomniac, claiming to have captured a variety of "private, unique and impactful data". Rhysida initially offered a ransom of $2 million for this data and gave Insomniac a 7-day time period to pay.

After the company failed to pay the demanded ransom, the Rhysida ransomware group posted the stolen data on the leak website hosted on Darkweb. The 1.6TB of leaked data includes PowerPoint presentations, game information, HR documents, credit card numbers, detailed information on C-Suite executives and the board of directors, as well as reports covering Insomniac's internal plans.



Insomniac Games

Insomniac Games

Insomniac Games, Inc. is an American video game developer based in Burbank, California.

Documents (part 1) Documents (part 2) Documents (part 3) Data Catalog: 1,67 TB, 1 318 733 Files

Not sold data was uploaded, data hunters, enjoy

It was founded in 1994 by Ted Price as Xtreme Software, and was renamed Insomniac Games a year later. Insomniac Games is a wholly owned subsidiary of Sony Interactive Entertainment.

Token

Enter Token and press Enter key

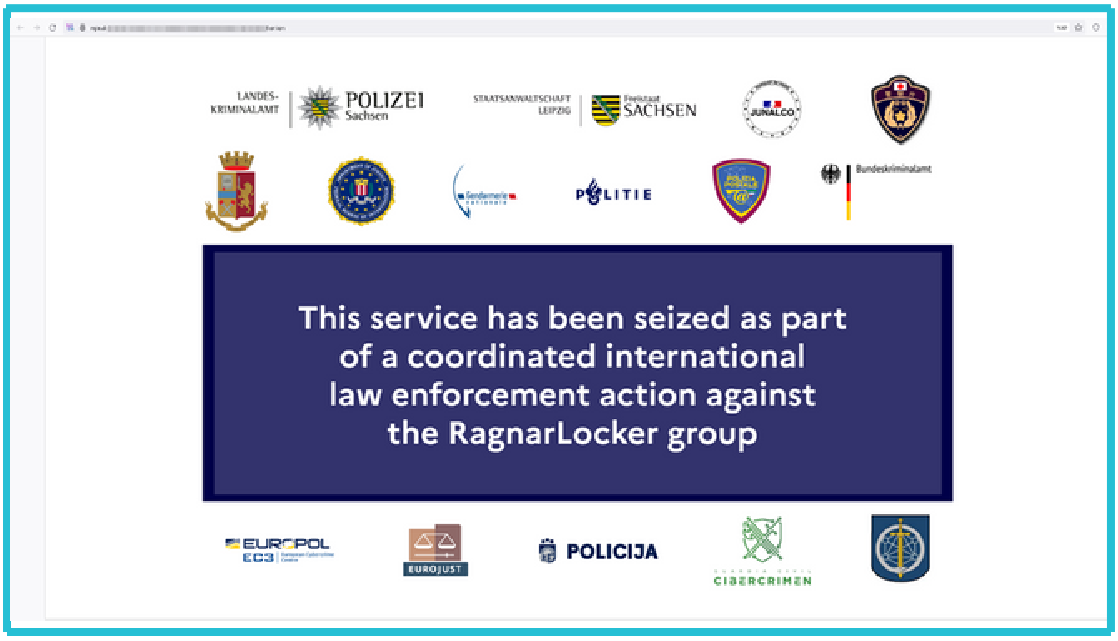
Screenshots and game plans of the "Wolverine" game stand out among the shared data. When the leak is analyzed, it is seen that Sony is preparing to release several more Marvel-based games such as "Spider-Man 3".

Sony Group has been targeted by ransomware gangs such as Cl0p and RansomedVC in the past. The company, which has been subjected to various cyberattacks, including a DDoS attack organized by Anonymous in 2011, has faced a major cybersecurity incident this time.

RagnarLocker Ransomware Gang Collapsed

The RagnarLocker ransomware gang, a high-level ransomware criminal group that has been actively targeting many critical infrastructures since December 2019, has been taken down in an international operation organized by Eurojust and Europol. On October 19, 2023, the group's Tor data leak site was captured in an international operation.

After the company failed to pay the demanded ransom, the Rhysida ransomware group posted the stolen data on the leak website hosted on Darkweb. The 1.6TB of leaked data includes PowerPoint presentations, game information, HR documents, credit card numbers, detailed information on C-Suite executives and the board of directors, as well as reports covering Insomniac's internal plans.



This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group

In recent years, RagnarLocker has attracted attention with their attacks on critical infrastructures around the world. In particular, they attracted a lot of attention with their attack on TAP Air, Portugal's largest airline company.

Searches were conducted in Spain, Czechia and Latvia on October 16-20. The leader of the RagnarLocker ransomware group was arrested on October 16 in Paris, France, and his home in the Czech Republic was searched. In the following days, five suspects were questioned in Spain and Latvia. At the end of the week of activity, the perpetrator, believed to be the group's leader, was brought before the coroners of the Paris Judicial Court.

RagnarLocker Ransomware Gang Collapsed

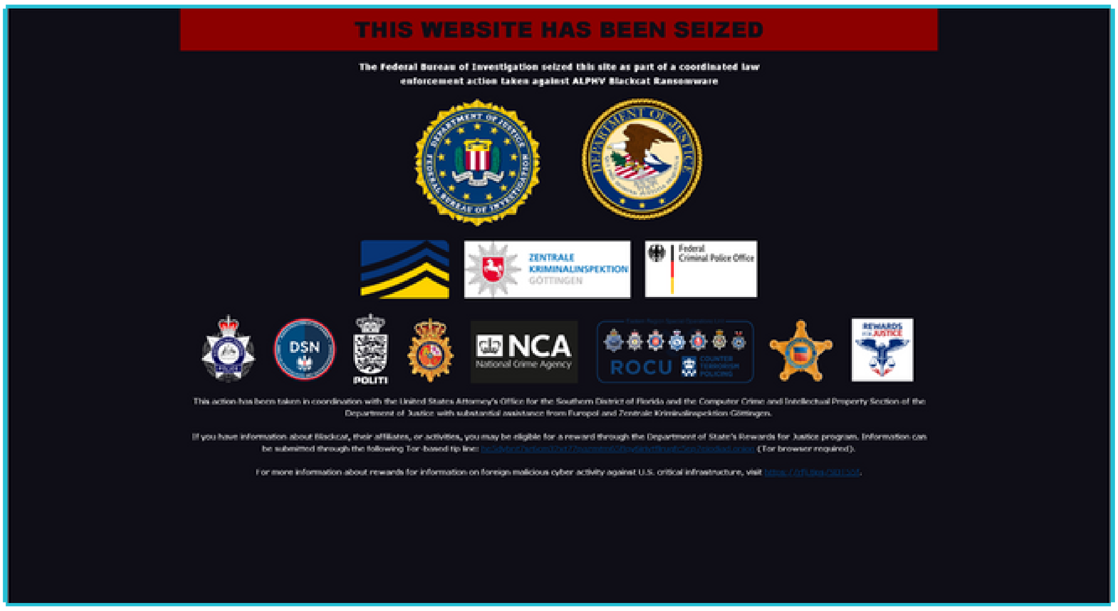
Ransomware infrastructure was also confiscated in the Netherlands, Germany and Sweden. The Tor data leak website was shut down in Sweden.

This international probe follows a complex investigation by the French National Gendarmerie, together with law enforcement agencies in the Czech Republic, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine and the United States.

BlackCat Ransomware Operation

In early December, the BlackCat/ALPHV ransomware operation suffered a Tor data leak and a five-day downtime on negotiation sites, which the group attributed to a hardware issue.

Later, the FBI announced that they had hacked the BlackCat/ALPHV ransomware operation, which by September 2023 had collected $300 million in ransoms from more than 1,000 victims worldwide. Law enforcement, who had been quietly spying on the ransomware ring, obtained the decryption and Tor private keys.


THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

ZENTRALE KRIMINALINSPEKTION GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA National Crime Agency
ROCU
COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: [illegible] (Tor browser required).

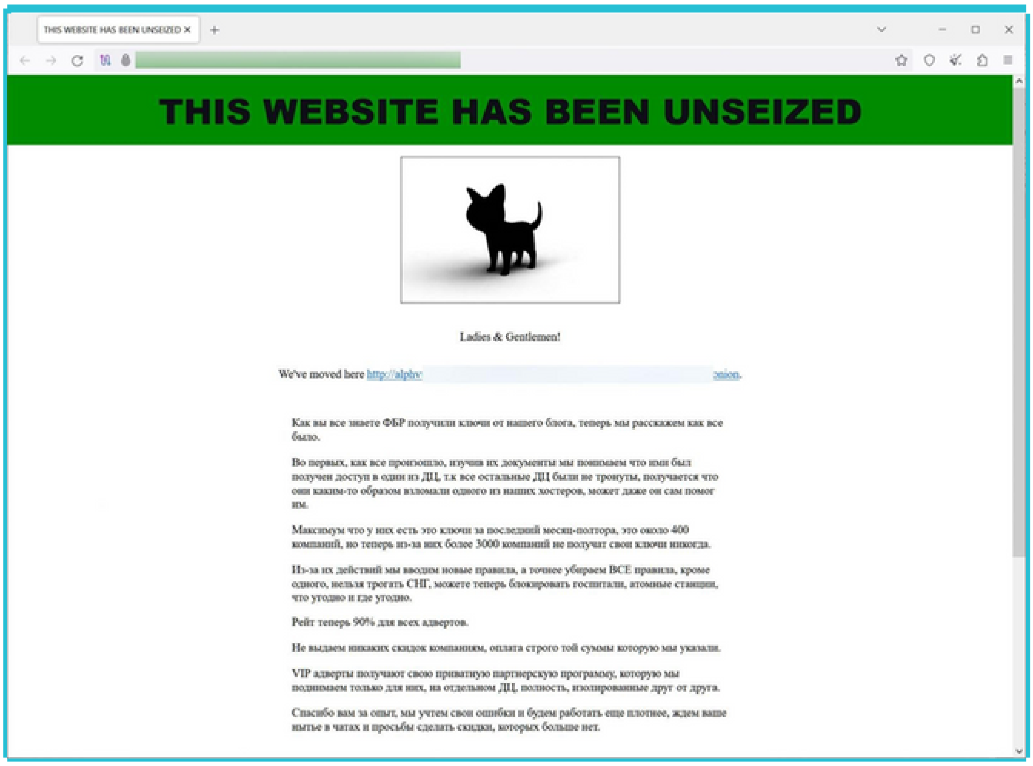
For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit [illegible].

The FBI also obtained decryption keys it issued for victims, helping 400 affected organizations regain control of their data and protect 68 million from ransom demands.

The Ministry of Justice confirmed that the FBI gained access to the network of the BlackCat/ALPHV ransomware cybercrime group, which monitored its activities for months and compromised its websites in December.

When creating a website on the Tor anonymization network, pairs of private and public keys associated with the .onion URL are uniquely generated and then saved on the Tor network. These keys provide control of the website and organize access to it. So, in this case, there was a constant struggle over URL control between threat actors and the FBI, who had the same keys.

During the time the team took back control of the leak site: "THIS WEBSITE HAS BEEN UNSEIZED". In it, the gang announced that it had launched a new Tor URL for data leak sites that the FBI did not have the private keys to and therefore could not seize.



THIS WEBSITE HAS BEEN UNSEIZED

Ladies & Gentlemen!

We've moved here http://alphv[redacted]onion.

Как вы все знаете ФБР получили ключи от нашего блога, теперь мы расскажем как все было.

Во первых, как все произошло, изучив их документы мы понимаем что ими был получен доступ в один из ДЦ, т.к все остальные ДЦ были не тронуты, получается что они каким-то образом взломали одного из наших хостеров, может даже он сам помог им.

Максимум что у них есть это ключи за последний месяц-полтора, это около 400 компаний, но теперь из-за них более 3000 компаний не получат свои ключи никогда.

Из-за их действий мы вводим новые правила, а точнее убираем ВСЕ правила, кроме одного, нельзя трогать СНГ, можете теперь блокировать госпитали, атомные станции, что угодно и где угодно.

Рейт теперь 90% для всех адвертов.

Не выдаем никаких скидок компаниям, оплата строго той суммы которую мы указали.

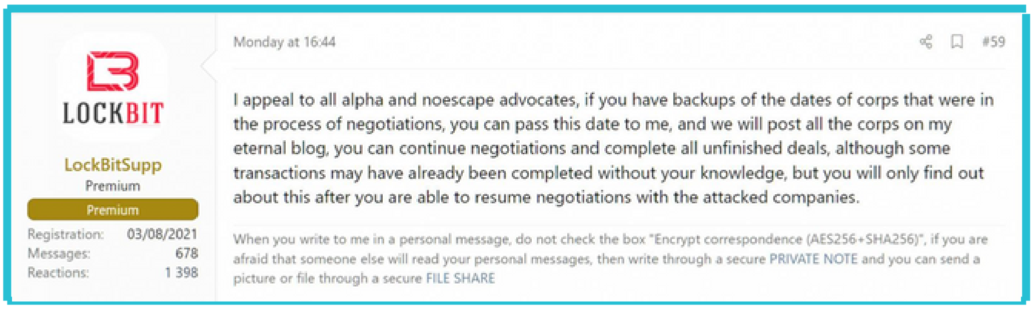
VIP адверты получают свою приватную партнерскую программу, которую мы поднимаем только для них, на отдельном ДЦ, полность, изолированные друг от друга.

Спасибо вам за опыт, мы учтем свои ошибки и будем работать еще плотнее, ждем ваше нытье в чатах и просьбы сделать скидки, которых больше нет.

The group claimed that the FBI had only gained access to decryption keys for the last month and a half, which was about 400 companies. However, they said they would never get the keys for the other 3,000 victims. They said that because of the operation, they had lifted all restrictions on their affiliates, allowing them to target any organization they wanted, including critical infrastructure. Affiliates are still restricted from attacking Commonwealth of Independent States (CIS) countries that were previously part of the Soviet Union. Finally, they said that they will no longer offer any discounts to companies and that payments will be strictly in the amount they specify.

BlackCat Ransomware Operation

After these events, the administrator of the Lockbit ransomware group posted a message on a Russian-speaking forum stating that they could support the ALPHV and NoEscape ransomware group partners in the ongoing ransom negotiations/extortions.



LOCKBIT

LockBitSupp

Premium

Premium

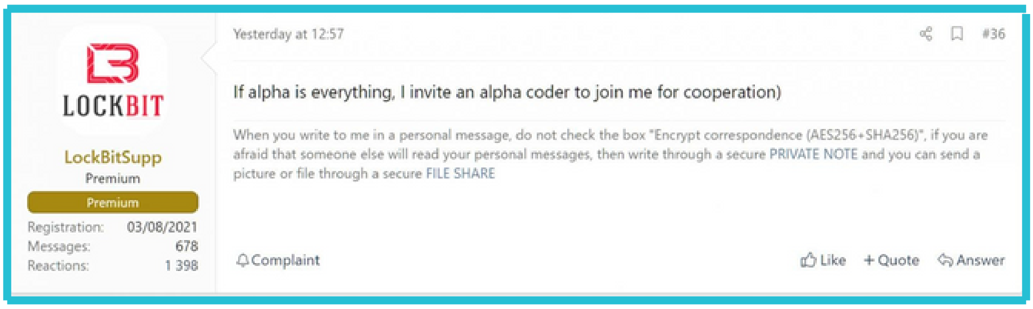
Registration: 03/08/2021
Messages: 678
Reactions: 1 398

Monday at 16:44 #59

I appeal to all alpha and noescape advocates, if you have backups of the dates of corps that were in the process of negotiations, you can pass this date to me, and we will post all the corps on my eternal blog, you can continue negotiations and complete all unfinished deals, although some transactions may have already been completed without your knowledge, but you will only find out about this after you are able to resume negotiations with the attacked companies.

When you write to me in a personal message, do not check the box "Encrypt correspondence (AES256+SHA256)", if you are afraid that someone else will read your personal messages, then write through a secure PRIVATE NOTE and you can send a picture or file through a secure FILE SHARE

Then, in another message, ALPHV ransomware invited developers to join its team.



LOCKBIT

LockBitSupp

Premium

Premium

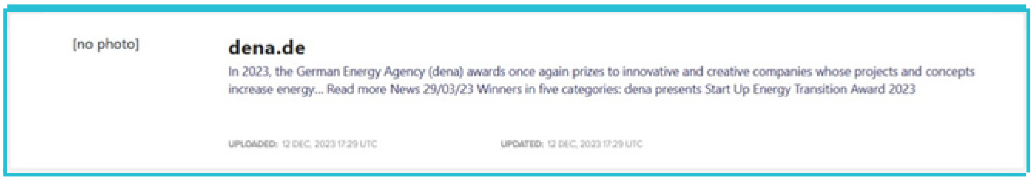
Registration: 03/08/2021
Messages: 678
Reactions: 1 398

Yesterday at 12:57 #36

If alpha is everything, I invite an alpha coder to join me for cooperation)

When you write to me in a personal message, do not check the box "Encrypt correspondence (AES256+SHA256)", if you are afraid that someone else will read your personal messages, then write through a secure PRIVATE NOTE and you can send a picture or file through a secure FILE SHARE

The LockBit ransomware group added the German energy agency Dena, previously attacked by the BlackCat ransomware group, to its list of victims, raising question marks about whether members of the group had joined Lockbit.



[no photo]

dena.de

In 2023, the German Energy Agency (dena) awards once again prizes to innovative and creative companies whose projects and concepts increase energy... Read more News 29/03/23 Winners in five categories: dena presents Start Up Energy Transition Award 2023

UPLOADED: 12 DEC, 2023 17:29 UTC UPDATED: 12 DEC, 2023 17:29 UTC

Cyberthint threat hunters asked Lockbit whether any of the BlackCat/NoEscape developers had joined them, but Lockbit chose to remain silent on the matter for now.

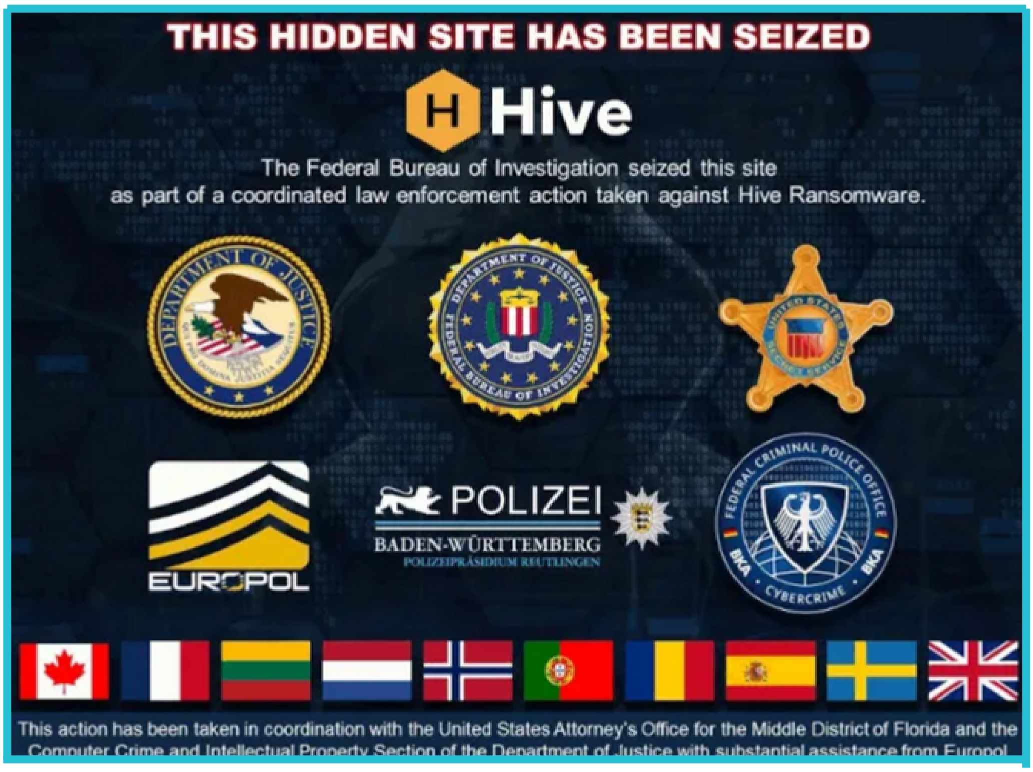
Arrest in Connection with Hive Ransomware Group

French authorities arrested a Russian citizen in Paris suspected of involvement in money laundering on behalf of the Hive ransomware group. After analyzing the suspect's phone, it was discovered that s/he had crypto assets worth €570,000.

Christophe Durand, head of the cyber investigations division of the new French Anti-Cybercrime Office (OFAC), said the suspect, who is "in his/her forties and resides in Cyprus," was arrested on December 5 while in Paris. The arrest resulted in the seizure of €570,000 from the suspect's crypto accounts.

In addition, thanks to the cooperation of Europol, Eurojust and Cypriot authorities, searches of the suspect's home in the seaside resort yielded important evidence for the investigation.

After penetrating the gang's infrastructure in late July 2022, the FBI secretly monitored operations for six months. In this way, detailed information was obtained before the group carried out attacks and targeted organizations were warned. In January 2023, an international law enforcement operation seized the group's Tor network leak website.



THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

DEPARTMENT OF JUSTICE
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
EUROPOL
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE
BKA
CYBERCRIME

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

Arrest in Connection with Hive Ransomware Group

The FBI also obtained more than 1,300 decrypt keys and distributed them to the victims. In this way, payment of a ransom of 130 million dollars was prevented.

In addition to decryption keys, the FBI and Dutch law enforcement officials seized the group's communication logs, malware file hashes, and information on 250 Hive members from servers hosted in California and backup servers hosted in the Netherlands.

In November, the FBI announced that the Hive group had extorted nearly $100 million by blackmailing more than 1,500 companies since June 2021.

MGM Resorts

Casino giant MGM Resorts confirmed that customers' personal information was compromised as a result of a cyber attack in September. This attack caused MGM Resorts a loss of 100 million dollars. The attack was carried out by Scattered Spider, a subgroup of the ALPHV ransomware group, and caused widespread disruption to a number of MGM's systems.

According to MGM's statement, the attack was a cyberattack that resulted in access to the personal information of customers who transacted with MGM before March 2019. The information obtained by the attackers included names, contact details, gender, dates of birth and driver's licence numbers. For some customers, social security numbers and passport details were also leaked.

The attack may have started when threat actors carried out a social engineering attack on the company's IT helpdesk via Vishing (Voice Phishing) method with the information they obtained on LinkedIn belonging to an employee of MGM. The Scattered Spider group stated through a representative that it had encrypted MGM's data and demanded a ransom.

MGM's competitor Caesars Entertainment had also suffered a similar cyber attack and met the ransom demand. However, MGM's rejection of this request is considered as a decision to comply with the FBI's guidelines.

These incidents show that hackers using the right attack vector, as well as large casino chains, can harm any organisation. Social engineering attacks via phone calls, known as vishing, reveal many organisations that do not take enough precautions to ensure cybersecurity as a weak link. To better protect against such attacks, it is important for companies to provide training to their employees and strengthen their verification processes that they are effective. After such a security breach, affected customers should be informed quickly and necessary measures should be taken. MGM committed to providing free credit monitoring services to its customers, but did not disclose the number of people affected by the data leak. Customers should check their bank transactions, report suspicious activity and take measures such as credit freezes when necessary.

These incidents show that businesses of all sizes need to be cautious and proactive against cyber threats. Creating a more aware community and strengthening security measures against social engineering attacks such as vishing can make us more resilient to future attacks.

Ransomware Statistics

Section 2

Ransomware Statistics

Ransomware has undoubtedly become one of the most feared cyber-attack methods for enterprises. This year, many companies, no matter how big or small, have been hit by ransomware attacks and blackmailed into paying ransoms. Operators have evolved to become increasingly sophisticated, improving their hacking methods and encryption algorithms.

Cyberthint threat hunters have been closely monitoring ransomware incidents this year, meticulously collecting different types of data. This data was provided by Cyberthint's Dark Monitor and Cyberthint threat hunters. This data was collected for the purpose of monitoring and analyzing cyber threats.

Summary

- In 2023 compared to 2022, ransomware attacks increased by 137%.
- There were more than 5700 number of ransomware attacks in 2023.
- 18 new ransomware groups were detected in 2023.
- Lockbit has become the ransomware group with the highest number of attacks in 2023 and retained the title of "Most aggressive ransomware group".
- In 2023, USA was the country with the most ransomware attacks.

Ransomware groups emerging in 2023:

- Akira
- MoneyMessage
- Cactus
- LostTrust
- Abyss Locker
- RA Group
- Dunghill_leak
- Rhysida
- NoEscape
- BlackSuit
- RansomedVC
- INC Ransom
- Knight
- ChipBit
- 3AM
- Malekteam
- Hunters International
- WereWolves

New Ransomware Groups

Akira

Akira ransomware operations were launched in March 2023. The group is known to demand exorbitant ransom payments of hundreds of millions of dollars. The Akira ransomware group often targets large-scale businesses. Educational institutions, as well as organizations in the finance, manufacturing, real estate and healthcare sectors are among the sectors targeted by the Akira ransomware group. It is a cross-platform ransomware that can run on both Linux and Windows operating systems.

Money Message

Money Message appeared in March 2023. Its activity can be traced by the presence of a file named "money_message.log" that appears in the root folder of the compromised server. It is a cross-platform ransomware that can run on both Linux and Windows operating systems. It has features such as encrypting network shares. The group has mainly targeted American companies.

Cactus

Cactus has been active since March 2023 and is also a RaaS (Ransomware as a Service) platform. The Cactus ransomware group gains first access to target networks by exploiting known vulnerabilities in the products used by companies (usually Fortinet VPN). The most interesting feature of this software is that it encrypts itself to protect the ransomware, making it difficult to detect by antivirus and network monitoring tools.

New Ransomware Groups

LostTrust

LostTrust was a ransomware group that started their activities in March 2023 but was little known until it started using the data leak site on the Tor network in September. The LostTrust ransomware is considered to be a variation of MetaEncryptor, which uses almost identical data leak sites and encryptors. The ransomware group is known to have had more than 50 victims, mostly companies in the US.

Abyss Locker

The Abyss Locker ransomware group emerged in March 2023. They commonly target VMware ESXi environments. Abyss Locker ransomware campaigns have targeted numerous industries, including finance, manufacturing, information technology and healthcare. According to postings on the group's website, the primary target is the US, with healthcare, manufacturing and technology sectors being the most frequently targeted.

Ra Group

Ra Group emerged in April 2023. The group's encryptor is known to have been created from the leaked source code of the Babuk ransomware group. Other ransomware groups such as Rook, Night Sky, Pandora, Cheerscrypt, AstraLocker, EXSiArgs, Rorschach, RTM Locker are also known to have used the leaked source code of Babuk ransomware. Ra Group has carried out more than 30 attacks so far.

New Ransomware Groups

Dunghill Leak

The Dunghill Leak emerged in April 2023. Telegram pages were set up in January 2023 and broadcast their victims on Telegram before announcing them on the leak website on the Tor network. Dunghill Leak, a group operated by the Dark Angels Team, is part of the previous Dark Angels data leak site. They used the code of the leaked Babuk encryptor as the encryptor, but have also been observed using the ESXI version of Ragnar Locker.

Rhysida

They emerged on May 2023. The Rhysida ransomware group describes itself as a "cybersecurity team" that offers to help victims identify security weaknesses in their networks and systems. Rhysida ransomware typically gains initial access to a victim's machine through phishing and then uses Cobalt Strike to spread within the system. They are thought to be a Russian-speaking ransomware group. They are also speculated that the Rhysida ransomware group has links to the Vice Society ransomware group.

NoEscape

NoEscape ransomware emerged in May 2023. The developers of NoEscape claim that they developed the ransomware from scratch. The group prefers not to include source code and leaks from other known ransomware families in their ransomware. It is a cross-platform ransomware that can run on both Linux and Windows operating systems. The NoEscape ransomware group is thought to have ties to the Avaddon ransomware group, which shut down in June 2021 after recommendations from the FBI and Australian law enforcement.

New Ransomware Groups

BlackSuit

Blacksuit was launched in May 2023. They bears striking similarities to Royal, a direct continuation of the famous Russian-linked Conti group. Their operators are experienced and may have ties to the Royal ransomware group. Both Royal and the former Conti groups are known for their organizational systems, business models and skilled operators. They have carried out more than 20 attacks since May. Their victims include government agencies, healthcare organizations and educational institutions.

RansomedVC

RansomedVc emerged as an underground forum on August 4, 2023 and has been operating under the ransomware-as-a-service (RaaS) business model for the last few months. This group made a name for itself with the Sony attacks. RansomedVc has listed more than 40 victims on its leak sites on the DarkWeb. It is known to demand ransom payments of up to 1 million dollars, depending on the size of the victim.

INC Ransom

Inc Ransom ransomware emerged in July 2023. Their operators describe themselves as a service for their victims. Victims can then pay the ransom to save their reputation and show the methods used by threat actors. As a result, the victim's systems become more secure. Initial Access methods include sending phishing emails as well as targeting vulnerable services.

New Ransomware Groups

Knight

Knight ransomware operations emerged in August 2023 as an evolution of Cyclops ransomware. Knight was actively promoted and sold on the RAMP (Russian Anonymous Market Place) forum. Knight ransomware first reaches its victims through phishing campaigns. Some of the first phishers sent appear to be messages from TripAdvisor. The encryptor is a cross-platform encryptor that can run on Windows, Linux and macOS operating systems.

CiphBit

CiphBit appeared in September 2023. An interesting feature of its encryptor is encrypting files on the victim's system by appending a unique random four-character identification code. The CiphBit ransomware group has 10 victims so far.

3AM

3AM ransomware cropped up in September 2023. It is developed in Rust language and runs on 64-bit architecture. 3AM ransomware stops various applications and services before encryption, disabling the encryption process and mechanisms to prevent data exfiltration. It also disables backup mechanisms, making data recovery more complicated. One other 3AM's notable feature is that it uses Yugeon Web Clicks software to monitor activities on web pages.

New Ransomware Groups

Malek Team

Malekteam emerged in October 2023. It is thought to be linked to Iran. MalekTeam has carried out 5 attacks so far.

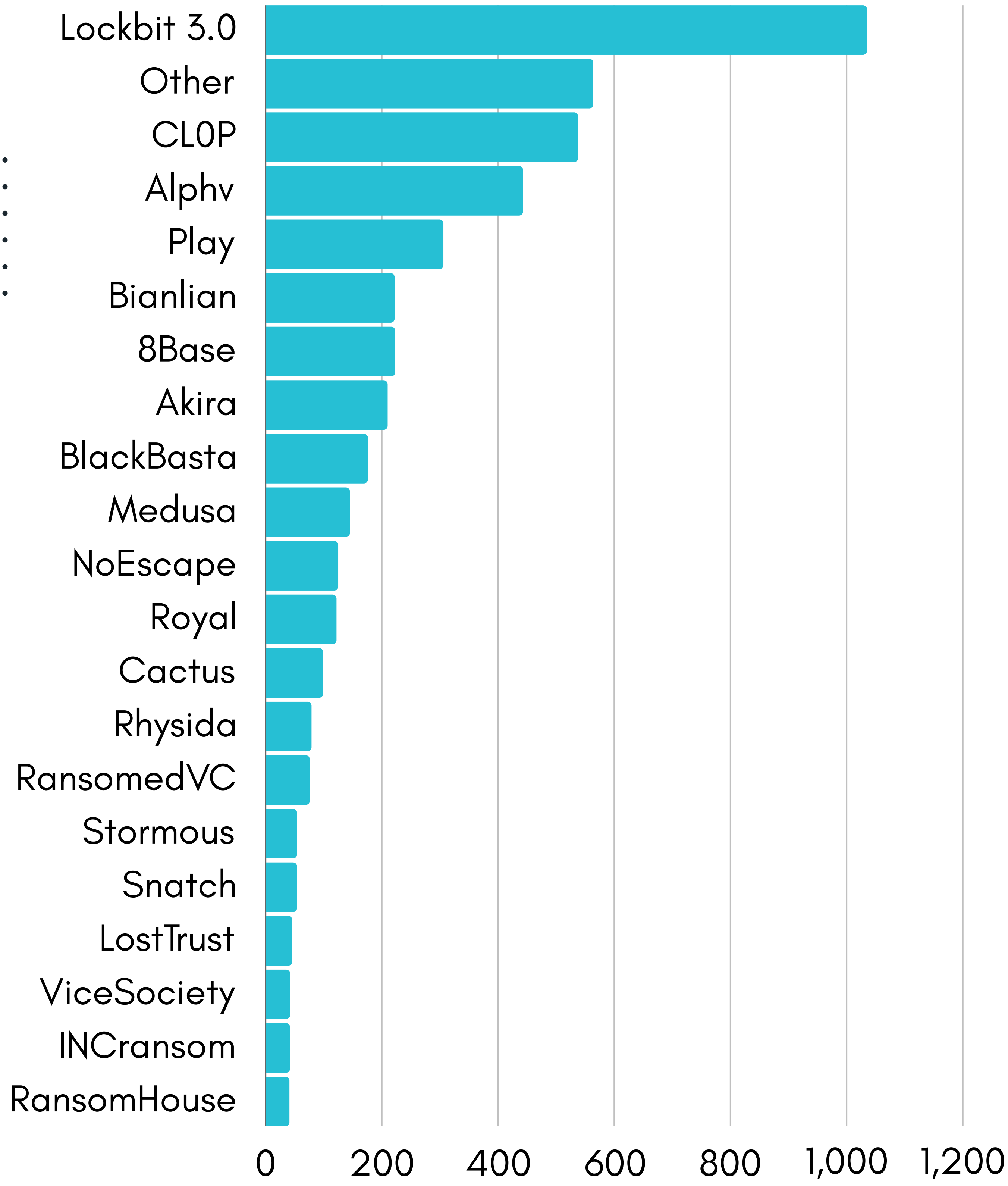
Hunters International

Hunters International is a RaaS service that emerged in Q3 2023. It is thought to be a continuation of the Hive ransomware group due to its 60% similarity to the Hive ransomware code. The Hunters International ransomware group claims to have no connection to the Hive operation.

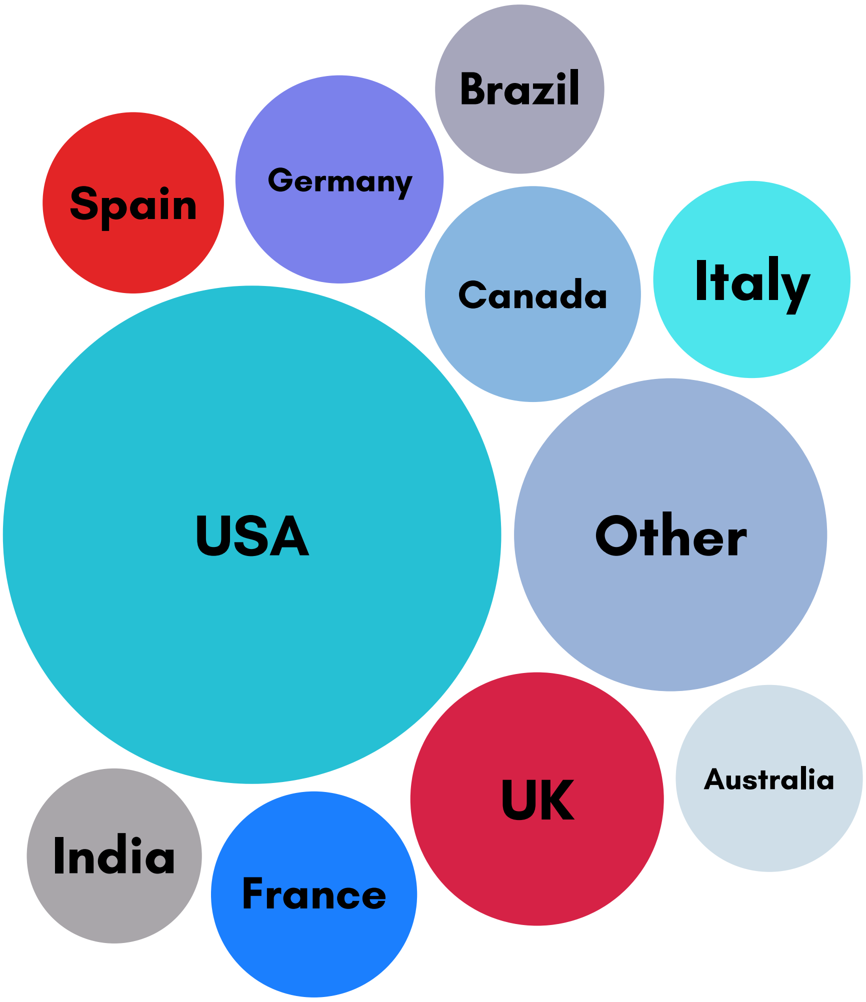
Werewolves

Werewolves is a ransomware group that emerged in the fall of 2023. They chooses its victims mainly from Russia and the US. The group has a mission that emphasizes its dedication to strengthening the cyber immunity of global companies. Furthermore, this group conducts a large-scale recruitment process targeting individuals with hacker skills. The group promises flexibility, regular salary and training to these individuals. So far, more than 24 attacks have been carried out by the group.

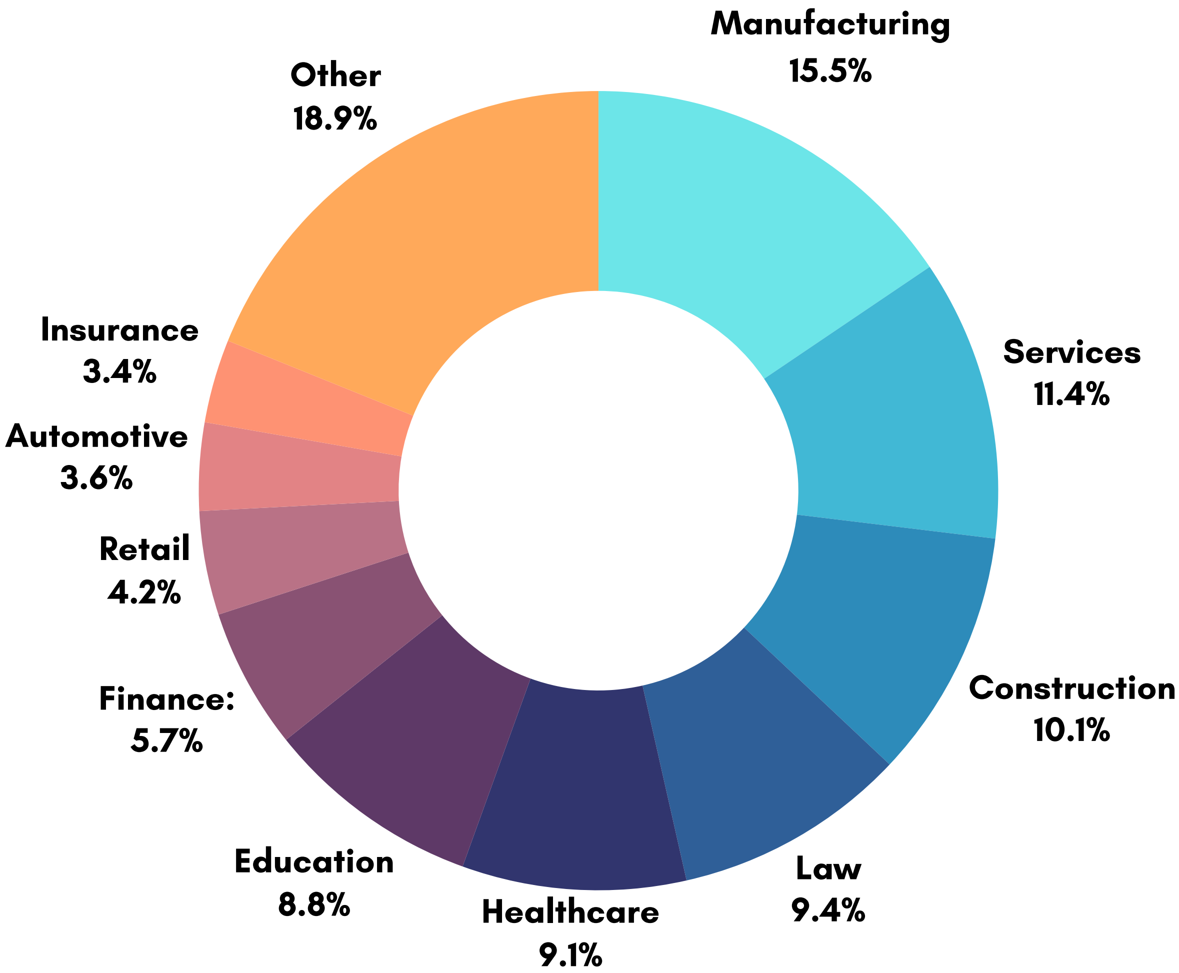
Top Ransomware Groups



Top Affected Countries by Ransomware Attacks



Top Affected Industries by Ransomware Attacks



Resounding Hacking Incidents

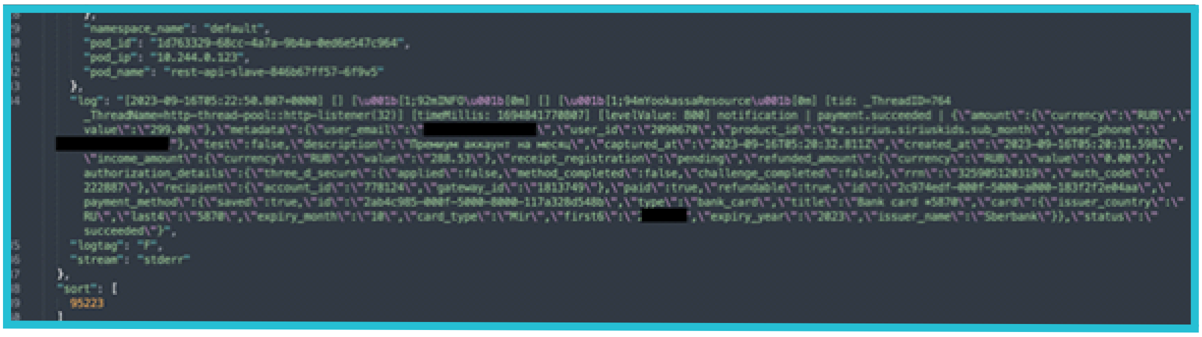
Data Breaches

Section 3

KidSecurity Data Breach

KidSecurity, a popular parental control app used to control and monitor children, has exposed activity logs, and allowed it to fall into the hands of threat actors.
With more than a million downloads on Google Play, KidSecurity is an app that offers parents the ability to follow their children's location, listen to their children's voices and surroundings, and set play limits to keep them safe.

On September 16, security researchers discovered that the app was unable to configure authentication for Elasticsearch and Logstash collections. Without authentication for these collections, unauthorized users could access them and modify, delete or steal data. According to estimates, user activity logs were kept accessible to anyone on the internet for more than a month. According to research, more than 300 million data records were compromised in total, including 21,000 phone numbers and 31,000 email addresses. Some credit card details were also accessible.



```
      },
      "namespace_name": "default",
      "pod_id": "1d763329-68cc-4a7a-9b4a-0ed6e547c964",
      "pod_ip": "10.244.0.123",
      "pod_name": "rest-api-slave-846b67ff57-6f9v5"
    },
    "log": "[2023-09-16T05:22:50.807+0000] [] [\u001b[1;92mINFO\u001b[0m] [] [\u001b[1;94mYookassaResource\u001b[0m] [tid: _ThreadID=764
      _ThreadName=http-thread-pool::http-listener(32)] [timeMillis: 1694841770807] [levelValue: 800] notification | payment.succeeded | {\"amount\":{\"currency\":\"RUB\",\"
      value\":\"299.00\"},\"metadata\":{\"user_email\":\"[redacted]\",\"user_id\":\"2090670\",\"product_id\":\"kz.sirius.siriuskids.sub_month\",\"user_phone\":\"
  [redacted]\"},\"test\":false,\"description\":\"Премиум аккаунт на месяц\",\"captured_at\":\"2023-09-16T05:20:32.811Z\",\"created_at\":\"2023-09-16T05:20:31.598Z\",
      \"income_amount\":{\"currency\":\"RUB\",\"value\":\"288.53\"},\"receipt_registration\":\"pending\",\"refunded_amount\":{\"currency\":\"RUB\",\"value\":\"0.00\"},\"
      authorization_details\":{\"three_d_secure\":{\"applied\":false,\"method_completed\":false,\"challenge_completed\":false},\"rrn\":\"325905120319\",\"auth_code\":\"
      222887\"},\"recipient\":{\"account_id\":\"778124\",\"gateway_id\":\"1813749\"},\"paid\":true,\"refundable\":true,\"id\":\"2c974edf-000f-5000-a000-183f2f2e04aa\",\"
      payment_method\":{\"saved\":true,\"id\":\"2ab4c985-000f-5000-8000-117a328d548b\",\"type\":\"bank_card\",\"title\":\"Bank card *5870\",\"card\":{\"issuer_country\":\"
      RU\",\"last4\":\"5870\",\"expiry_month\":\"10\",\"card_type\":\"Mir\",\"first6\":\"[redacted]\",\"expiry_year\":\"2023\",\"issuer_name\":\"Sberbank\"}},\"status\":\"
      succeeded\"}",
    "logtag": "F",
    "stream": "stderr"
  },
  "sort": [
    95223
  ]
```

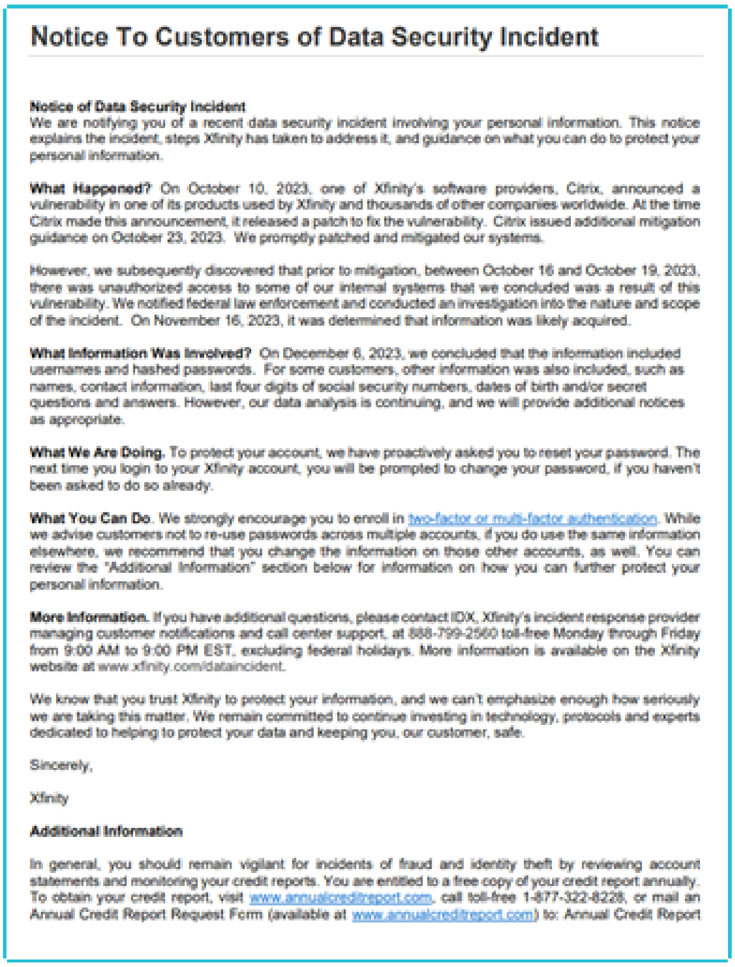
Xfinity Data Leak

Comcast, the parent company of Xfinity, sent a notification to its customers that it had discovered "unauthorized access to its internal systems" using a vulnerability in Citrix.
During routine cybersecurity drills on October 25, cybersecurity teams reported that they detected "suspicious activity" and access to Comcast's internal systems between October 16 and 19, about two weeks after Citrix released a security update for a vulnerability known as Citrix Bleed.

After investigations, Xfinity found that 35 million people were affected by the data leak.

The company announced in a statement that username and password hashes of customers were obtained from the affected systems.

To protect affected accounts, Xfinity urged customers to reset passwords, change answers to security questions and tighten security with two- or multi-factor security measures.



Notice To Customers of Data Security Incident

Notice of Data Security Incident
We are notifying you of a recent data security incident involving your personal information. This notice explains the incident, steps Xfinity has taken to address it, and guidance on what you can do to protect your personal information.

What Happened? On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.

However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.

What Information Was Involved? On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.

What We Are Doing. To protect your account, we have proactively asked you to reset your password. The next time you login to your Xfinity account, you will be prompted to change your password, if you haven't been asked to do so already.

What You Can Do. We strongly encourage you to enroll in two-factor or multi-factor authentication. While we advise customers not to re-use passwords across multiple accounts, if you do use the same information elsewhere, we recommend that you change the information on those other accounts, as well. You can review the "Additional Information" section below for information on how you can further protect your personal information.

More Information. If you have additional questions, please contact IDX, Xfinity's incident response provider managing customer notifications and call center support, at 888-799-2560 toll-free Monday through Friday from 9:00 AM to 9:00 PM EST, excluding federal holidays. More information is available on the Xfinity website at www.xfinity.com/dataincident.

We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter. We remain committed to continue investing in technology, protocols and experts dedicated to helping to protect your data and keeping you, our customer, safe.

Sincerely,

Xfinity

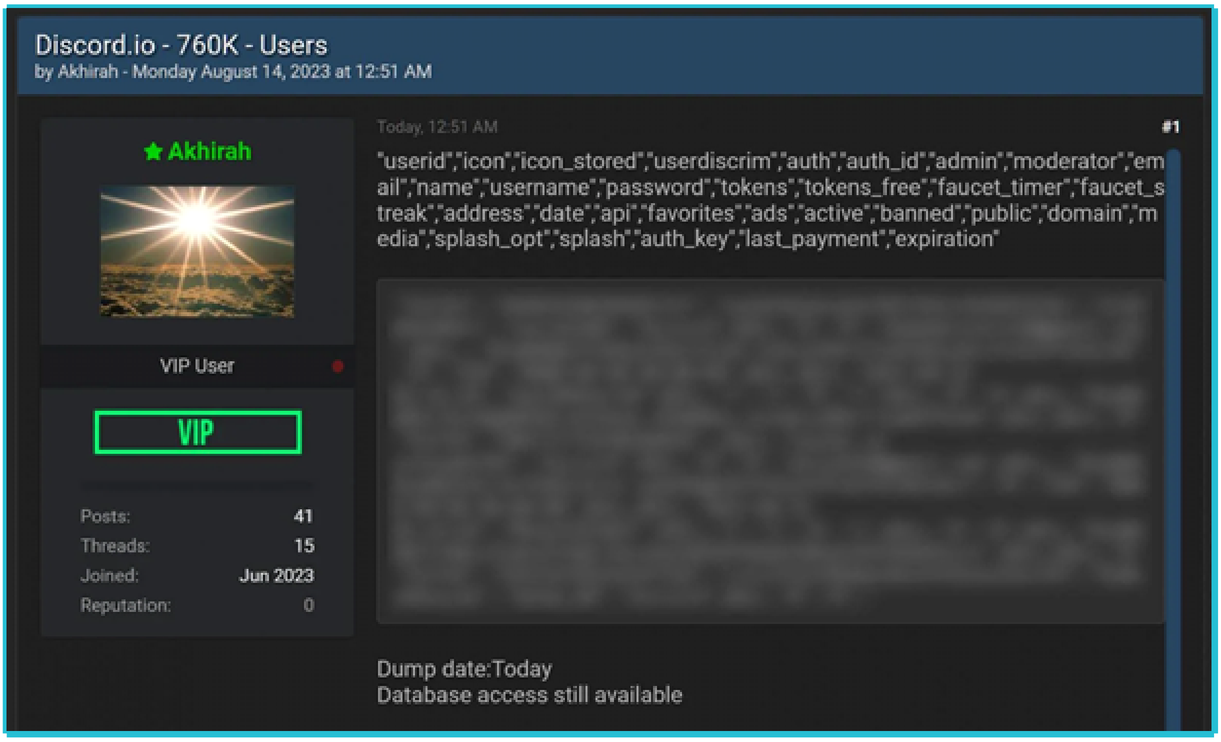
Additional Information

In general, you should remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You are entitled to a free copy of your credit report annually. To obtain your credit report, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or mail an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report

Discord.io Data Leak

Discord.io is a third-party website that allows users to create custom links for their Discord channel. Discord.io suffered a data leak in which the information of 760,000 users was exposed.

On August 14, a threat actor known as 'Akhirah' offered the Discord.io database for sale on a hacker forum. As proof, the threat actor shared the data of four users.



Discord.io - 760K - Users
by Akhirah - Monday August 14, 2023 at 12:51 AM

Posts: 41
Threads: 15
Joined: Jun 2023
Reputation: 0

Today, 12:51 AM #1

```
"userid","icon","icon_stored","userdiscrim","auth","auth_id","admin","moderator","email","name","username","password","tokens","tokens_free","faucet_timer","faucet_streak","address","date","api","favorites","ads","active","banned","public","domain","media","splash_opt","splash","auth_key","last_payment","expiration"
```

[redacted]

Dump date:Today
Database access still available

Discord.io confirmed the leak, which affected 760,000 users, confirming that "Usernames, Discord IDs, Email addresses, Billing addresses, Salted and hashed passwords, Leaked passwords" were compromised. On August 15th, it announced that it had stopped all services.

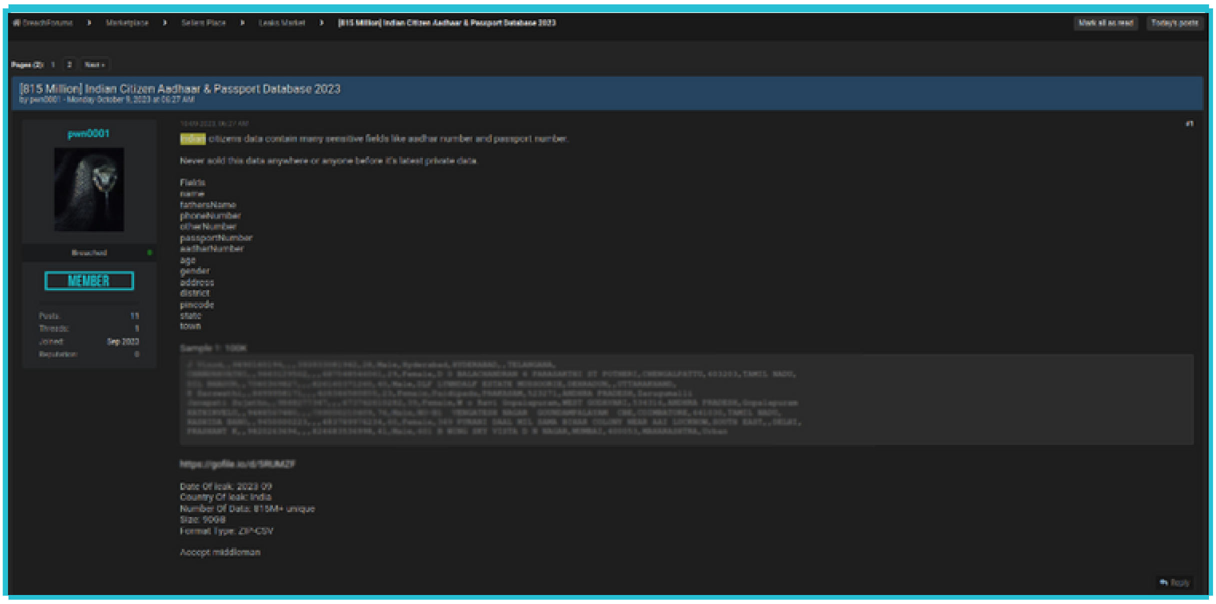
Discord.io canceled all existing subscriptions and refunded all users who had recently purchased premium memberships.

Massive Data Leak from India

The personal information of more than 815 million Indian citizens was allegedly compromised in what is being called the largest data breach in Indian history.

In October, a threat actor named "pwn0001" put up for sale on a dark web forum claiming to have obtained personally identifiable information (PII), including that contained in the Aadhaar ID cards of 815 million Indian citizens.

The threat actor claimed that the data was obtained from the Indian Council of Medical Research (ICMR) COVID-19 test records, but the ICMR denied this, stating that they had not experienced a data leak.



[815 Million] Indian Citizen Aadhaar & Passport Database 2023
by pwn0001 - Monday October 9, 2023 at 06:27 AM

10-09-2023, 06:27 AM

Indian citizens data contain many sensitive fields like aadhar number and passport number.

Never sold this data anywhere or anyone before it's latest private data.

Fields
name
fathersName
phoneNumber
otherNumber
passportNumber
aadharNumber
age
gender
address
district
pincode
state
town

Sample 1: 100K

[redacted]

https://gofile.io/d/5RUMZF

Date Of leak: 2023 09
Country Of leak: India
Number Of Data: 815M+ unique
Size: 90GB
Format Type: ZIP-CSV

Accept middleman

In November, Minister of State for Electronics and Information Technology Rajeev Chandrasekhar told a press conference in Bhopal that "evidence of leakage and investigation is going on, but the data was not stolen".

In the latest development in the case, the Delhi Police's cyber security unit arrested four people on charges of breaching the Indian Council of Medical Research (ICMR) database in early December. Police alleged that the four suspects sold citizens' personal information on the dark web after they managed to leak data from ICMR's database.

If the alleged breach is real, it affects more than half of the country's estimated population of 1.4 billion.

Mr. Cooper Data Leak

Mr. Cooper, a leading US mortgage servicer, suffered a data breach in October. The company announced that approximately 14.7 million people were affected by the data breach, including all current and former customers.

Mr. Cooper notified the Maine Attorney General's Office about the data breach, stating that 14.5 million people were affected. In a notice sent to victims of the breach, they stated that names, addresses, phone numbers, social security numbers, birth dates and bank account numbers were stolen.

The company said that between October 30 and November 1, an unauthorized third party gained access to some of its systems. On October 31, after detecting the intrusion, it was forced to shut down its systems, resulting in a service outage from November 1 to November 4.

In their latest statement, the company said that it is continuing to investigate the latest cyber incident, and to support affected customers, it is providing free identity protection for two years through TransUnion IdentityForce.

Most Important Vulnerabilities in 2023

Section 4

Most Important Vulnerabilities in 2023

CVE-2023-23397 CVSS Score: 9.8

This is a vulnerability affecting Microsoft Outlook and some versions of Microsoft Office. By sending a malicious email, attackers can access a victim's Net-NTLMv2 hash value, which can be used as the basis for an NTLM Relay attack against another service to authenticate as a user. The Microsoft Threat Intelligence team found that Russian state-linked Forest Blizzard (STRONTIUM, APT28, FANCYBEAR) exploited this vulnerability to gain unauthorized access to systems.

CVE-2023-4966 CVSS Score: 9.4

The Citrix Bleed vulnerability is a critical vulnerability in Citrix NetScaler ADC and Gateway. Exploiting this vulnerability allows attackers to gain unauthorized access and poses a serious threat to the confidentiality and integrity of sensitive information. Cybercriminals have been known to exploit this vulnerability to launch attacks targeting sectors such as finance and government.

CVE-2023-37580 CVSS Score: 6.1

CVE-2023-37580 was discovered by Google TAG (Threat Analysis Group) as a zeroday vulnerability affecting Zimbra Collaboration email servers. CVE-2023-37580 is an XSS vulnerability. There have been 4 cyber attack campaigns organized by exploiting this vulnerability.

Most Important Vulnerabilities in 2023

CVE-2023-36553 CVSS Score: 9.8

This is an OS Command Injection vulnerability discovered in FortiSIEM. Attackers can use this vulnerability for exploitation by sending specially crafted requests and execute arbitrary commands on the operating system.

CVE-2023-34362 CVSS Score: 9.8

SQL Injection vulnerability in the MOVEit Transfer web application. It allows attackers to execute SQL queries on the database in an unauthorized manner.

CVE-2023-20867 CVSS Score: 3.9

Improper Access Control vulnerability in Citrix Content Collaboration. When exploited, attackers can gain unauthorized access to the Customer-managed ShareFile Storage Zones Controller.

Most Important Vulnerabilities in 2023

CVE-2023-27350 CVSS Score: 9.8

It is a remote code execution vulnerability in PaperCut MF/NG. It allows attackers to execute unauthorized commands on the targeted system.

CVE-2023-20887 CVSS Score: 9.8

It is a remote code execution vulnerability in VMWare Aria Operations. It allows attackers to execute unauthorized commands on the root user.

CVE-2023-0669 CVSS Score: 7.2

A remote code execution vulnerability in Fortra's GoAnywhere Managed File Transfer software. It allows attackers to execute commands in an unauthorized way.

Malwares in 2023

Section 5

Malwares in 2023

Cyberthint threat hunters conducted research on malware in 2023 to identify the most commonly employed methods by threat actors for malware delivery. These findings were obtained through the Cyberthint Unified Cyber Threat Intelligence Platform and the research efforts of Cyberthint threat hunters.

Summary

- Droppers were the most infected malware type.
- Brazil was the country that suffered the most malware attacks.
- The use of Clipper type software increased in malware attacks.

Malware Infection via Youtube Videos

Threat actors create a video showing the use of a particular software and talking about its benefits, and upload it to YouTube. They put download links to the software in the video description. Viewers with limited knowledge of computer security often – without checking – click on the links in the video descriptions to download and run the malware, thereby infecting their devices with malware. Threat actors used this method to infect many people's devices with malware in 2023.

Malware Infection by Exploiting Vulnerabilities

Threat actors can infect systems with their malware by exploiting vulnerable systems. This method usually targets vulnerable web applications and vulnerable servers to infect them with malware. As a result of their research, Cyberthint threat hunters have found that targets in these attacks are often discovered by scanning systems open to the internet and infected in this way.

Malwares in 2023

Malware Infection via Unsecured Sites

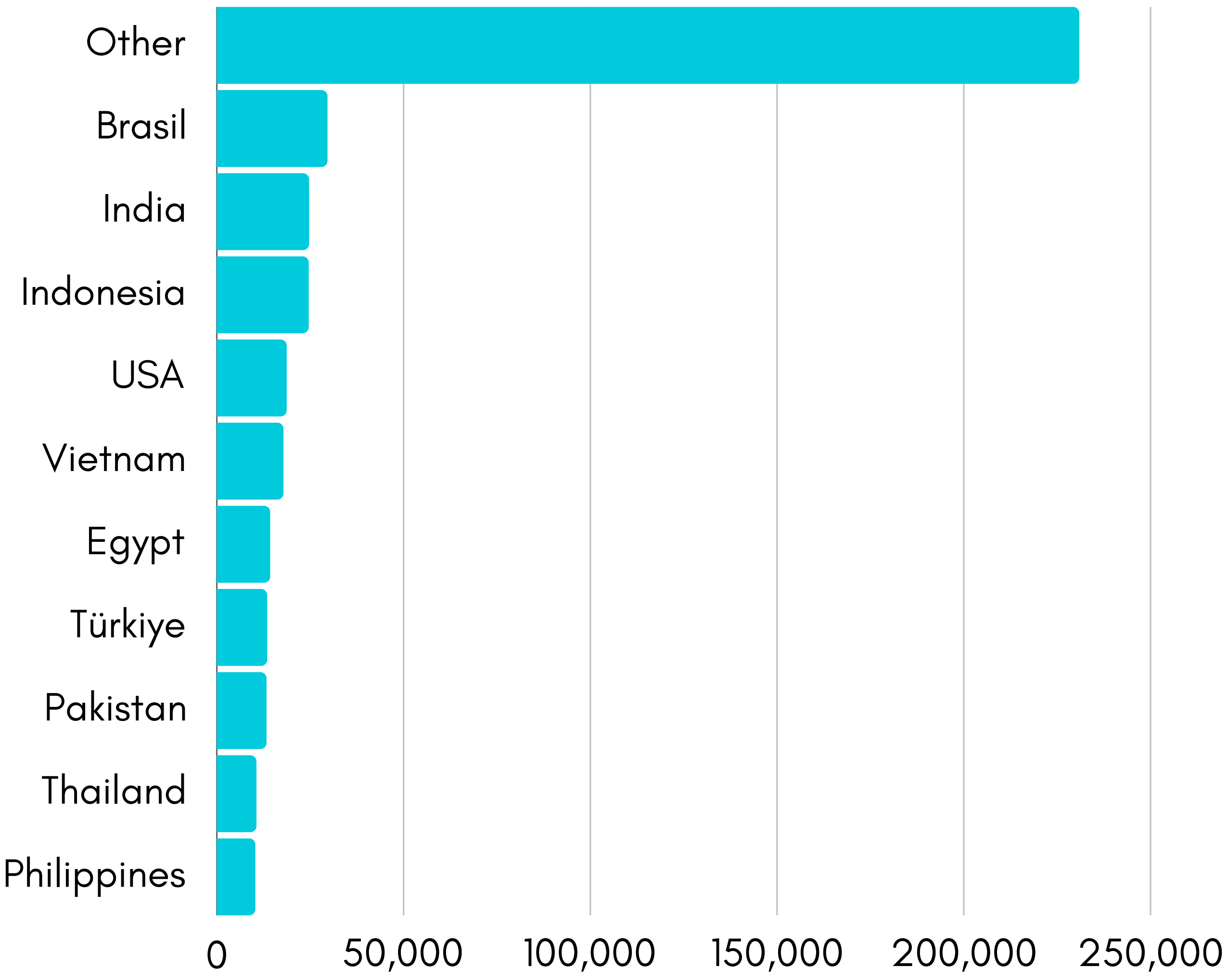
Threat actors create a website that replicates the original websites of popular programs and add a download link to their malware in the download button section of the fake website. They then perform a typosquatting attack to purchase a domain name that is similar to the original domain name and use it to advertise the program as legitimate software so that it appears at the top of the first page of search engine results. People who do not pay attention to the domain name fall into this trap by not realizing the danger when they visit the fake website, as the appearance of the site is identical to the appearance of the official website of the program. In 2023, threat actors infected many inattentive users with malware by spoofing the websites of popular software such as 7-Zip, Blender 3D, Capcut, CCleaner, Notepad++, OBS, Rufus, VirtualBox, VLC Media Player, WinRAR and Putty.

Another drawback of visiting untrusted websites is that malware can be downloaded onto your device without your knowledge through pop-ups that open up from everywhere. Threat actors often do this through sites such as pirated movie streaming sites and pirated game download sites. This can also include more dangerous software such as adware and spyware. It is used to steal users' data, identities, passwords or financial information, hijack their devices, blackmail them with ransomware, or recruit them into botnets.

Malware Infection via Pirated Software

Threat actors target pirated software users by binding their malware to illegally downloaded files such as programs, games and movies. When pirated software users download and run this illegal content, they also run the hidden malware and their systems are infected. Threat actors often try to evade antivirus solutions by asking piracy users to turn off their antivirus systems before running the downloaded content or the downloaded files will not work properly. Cyberthint threat hunters have observed in their research on malware victims that most of them had their Antivirus turned off at the time of infection.

Top Countries Most Affected by Malware Attacks



APT Activities in 2023

Section 6

APT Activities in 2023

Cozy Bear's Global Cyber Attack

In the last quarter of 2023, the Russian APT group Cozy Bear carried out a series of cyberattacks with the TeamCity server authentication vulnerability (CVE-2023-42793) discovered in September. This attack targeted a wide range of organizations, affecting many companies in the US, Europe, Asia and Australia. After gaining initial access using the TeamCity vulnerability, Cozy Bear uses services such as Dropbox to create a backdoor. The compromise of TeamCity servers gave malicious actors access to source code and software deployment processes, jeopardizing companies' operations. Recent observations indicate that there are more than 700 vulnerable TeamCity servers worldwide.

Apt29's Exploitation of WinRAR Vulnerability

The APT29 group was found to be using the WinRAR vulnerability (CVE-2023-38831) discovered in August. Using this vulnerability, APT29 targeted victims with emails containing a malicious ZIP file. The attackers chose to use a free static domain to connect to the command and control server hosted on the Ngrok service. This method allowed APT29 to keep its activities secret. APT29's operation combines traditional and new techniques and uses the WinRAR vulnerability and the Ngrok service as an efficient way to transmit payloads.

Operation BlueNoroff RustBucket

In the last quarter of 2023, BlueNoroff, a subgroup of the North Korean Lazarus Group, launched an operation called "RustBucket" targeting users in the US and Japan. The operation was carried out using the newly discovered Mac malware called "ObjCShellz". When this malware is run on compromised devices, threat actors can gain unauthorized access to the devices via reverse shell. To avoid detection, the malicious payload communicates with the swissborg[.]blog domain, which at first glance looks like a cryptocurrency website. In this operation, BlueNoroff targeted cryptocurrency exchanges and banks.

APT29 Phishing Campaign

Phishing Campaign Against Foreign Embassies in Kiev
The Dukes (APT29) was observed sending phishing emails to various foreign embassies in Kiev after Ukraine launched a counterattack in June 2023. The campaign appears to be aimed at gathering intelligence on Ukraine.

APT Activities in 2023

APT33's Use of Password Spraying Technique

APT33 Targeted Organizations with Password-Spraying Attacks
APT 33 has been observed using password-spraying attacks against a wide range of organizations. With the password-spraying technique, attackers attempt to obtain successful logins by trying a limited number of passwords on a large list of users. Microsoft said it has detected successful intrusions in a small number of cases, and that when APT 33 gains access to networks, it leaks information from victim servers.

APT35 Launches Attacks with New Backdoor

APT35 Targets Organizations with New Backdoor
APT 35 (Charming Kitten) used a new backdoor dubbed "Sponsor" against organizations in Brazil, Israel and the United Arab Emirates. APT 35 appears to have attempted to gain access to a wide range of systems, suggesting that the campaign was aimed at gathering intelligence on a broad scale rather than attacking a specific organization.

APT37 Launches Attacks with New Backdoor

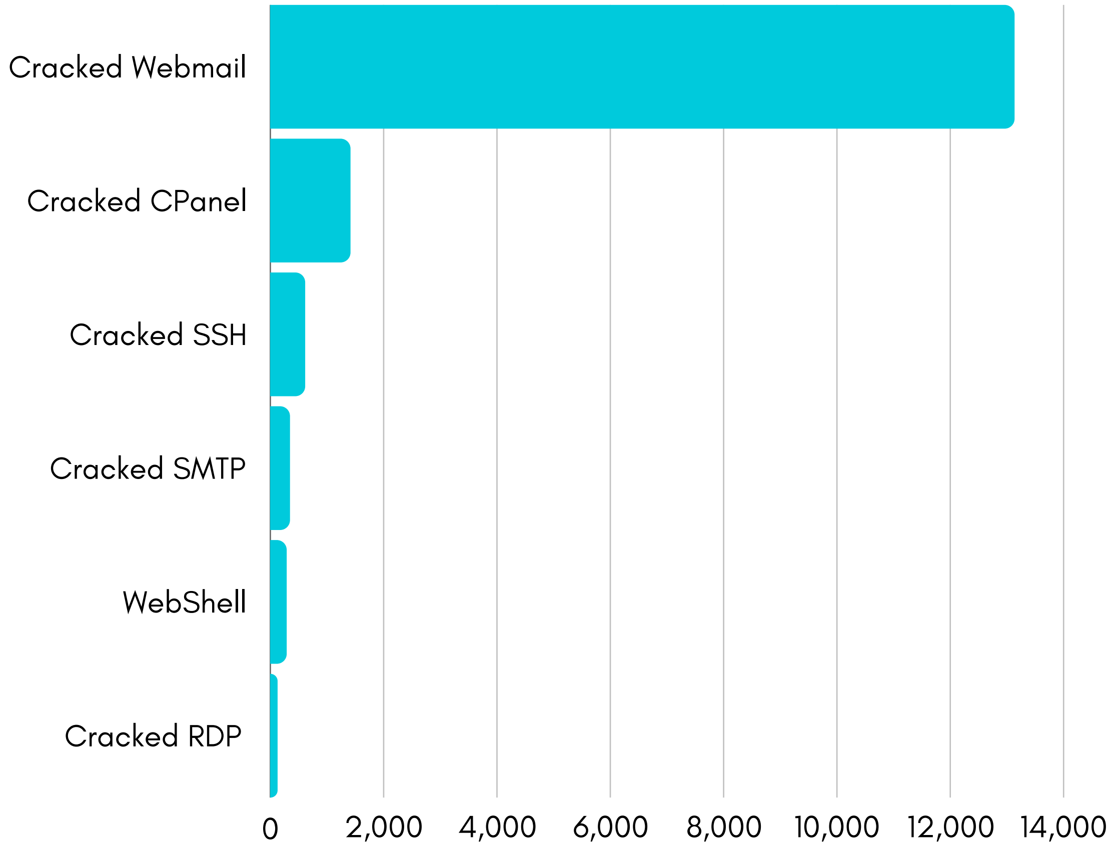
APT37 Hijacks Networks of NPO Mashinostroyeniya
APT 37, a North Korean threat actor, compromised sensitive networks, including the email server of Russian missile design firm NPO Mashinostroyeniya. Analysis revealed that the attackers used a backdoor called "OpenCarrot". NPO Mashinostroyeniya is known as a leading developer of hypersonic missiles, satellite technologies and next-generation ballistic weapons. This incident took place shortly after Russian Defense Minister Sergei Shoigu's visit to Pyongyang. The targeted company could be a valuable target for North Korea as it is one of Russia's key designers and manufacturers of long-range missiles.

Black Markets in 2023

Section 7

Black Markets in 2023

Threat actors can take advantage of compromised information during the "initial access" phase to infiltrate the organizations they target. Threat actors frequently use log black markets to purchase compromised infiltrations. Cyberthint threat hunters analyzed the data in black markets in detail and reached the following conclusions.



Dark Web Trends

Section 8

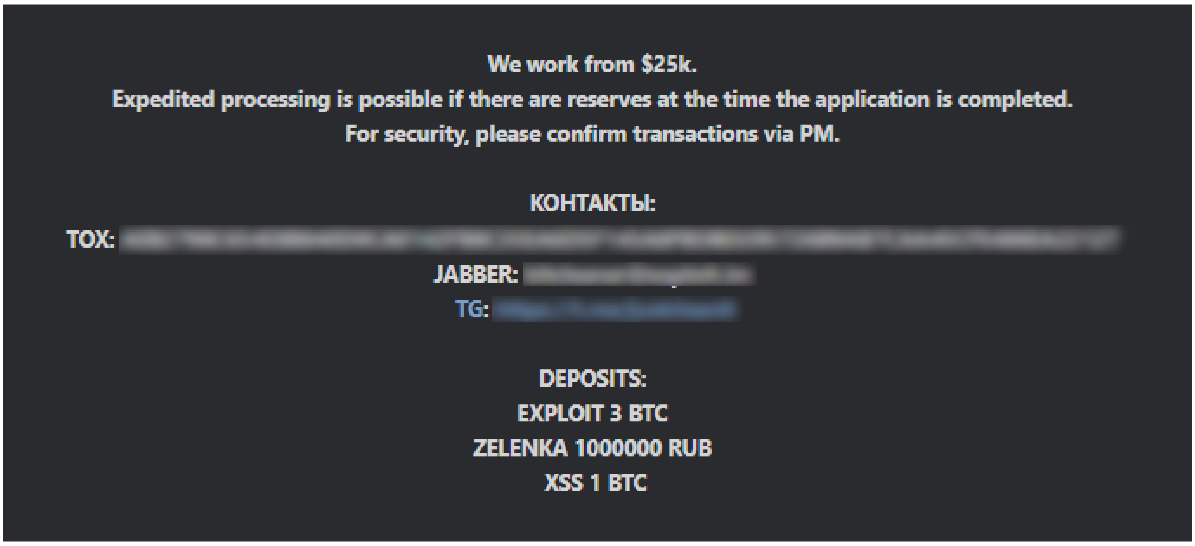
Dark Web Trends

Platforms on the DarkWeb Increase Their Security

Cyberthint threat hunters have detected that threat actors operating on the dark web have increased security measures on their platforms. Regardless of platform type, security measures are now being tightened on many different types of platforms, such as ransomware infiltration sites, blackmarkets and private messaging platforms. In addition to adding DDoS protections and bot verifications, platform owners have tightened authentication across cross-platform accounts for the safety of their users. Undoubtedly, the main reasons for this increase in security and privacy include competition between threat actors and successful operations by law enforcement agencies this year.

CryptoCurrency Mixing

The biggest motivation for independent threat actors on the DarkWeb is unquestionably financial. Threat actors transfer the money they obtain illegally to crypto wallets. Bitcoin and Ethereum, two of the most widely used cryptocurrencies in illicit trade, have a structure that makes all transactions publicly visible. This does not sit well with threat actors in terms of privacy. To improve their anonymity, threat actors use so-called CryptoCurrency "mixer" services. These services take a commission of 0.25% to 3% and transfer the black money from the threat actor between many different wallets with different amounts, making it difficult to trace transactions. In 2023, many threat actors used this method to increase the anonymity of the money laundering process.



We work from $25k.
Expedited processing is possible if there are reserves at the time the application is completed.
For security, please confirm transactions via PM.

КОНТАКТЫ:
TOX: [redacted]
JABBER: [redacted]
TG: [redacted]

DEPOSITS:
EXPLOIT 3 BTC
ZELENKA 1000000 RUB
XSS 1 BTC

2024 Predictions

Section 9

2024 Predictions

Phishing Attacks Evolving

2023 was a very active year in terms of phishing attacks. Threat actors gained access to an organization's systems through phishing attacks while gaining the first unauthorized access. In 2024, the upward trend in phishing attacks is expected to continue. Cybercriminals can carry out more sophisticated and personalized attacks to trick users using social engineering techniques. These attacks, which are carried out via email, text or fake websites, aim to obtain sensitive information from victims.

To protect against phishing attacks, security awareness should be kept high, employees should be regularly trained and effective security measures should be taken. In addition, security measures such as reliable communication channels and multi-factor authentication will become more important.

APT Attacks

Advanced Persistent Threats (APT) refers to long-term, sustained and targeted attacks on target systems. In 2024, APT attacks are expected to increase. Attackers can infiltrate target organizations and work for long-term espionage, data theft or infrastructure disruption. The fact that APT groups are often state-sponsored allows them to carry out much more sophisticated attacks. It is predicted that 2024 will be a challenging year between states and this will be reflected in the cyber world.

To protect against APT attacks, organizations should focus on endpoint security (XDR technology), network security, security awareness trainings, security incident management and the use of up-to-date threat intelligence.

Increasing Trend of Ransomware Attacks

Ransomware attacks are undoubtedly one of the most frightening cyber threats for companies. This type of malware, which is used to infect systems to steal sensitive data and encrypt it, increased significantly in 2023 compared to 2022. It is estimated that there will be a significant increase in ransomware attacks in 2024, considering that ransomware gangs are becoming more professionalized over time and operators are more meticulous in their recruitment.

No matter how much corporate companies try to prevent these attacks with their security products and software, ransomware groups can sometimes get ahead of this situation with more qualified operators and more sophisticated attack methods.

2024 Predictions

Artificial Intelligence Threats

Technological advancements and developments in artificial intelligence are driving dramatic changes across many industries, bringing with them new cybersecurity challenges. In 2024, as AI technology becomes more pervasive and sophisticated, new threats are expected to emerge. In this context, in 2024, it is predicted that AI-powered attacks, deepfake attacks by imitating voice and images through artificial intelligence and deep learning, and attacks on AI infrastructures used in software will increase.
In addition, attack vectors that threaten artificial intelligence (prompt attacks) will also be on the agenda.

Cyber Wars Between Countries

Unlike traditional military conflicts, cyber wars are conflicts that target computer systems and are conducted over the cyber surface. In 2023, the Israeli-Palestinian conflict witnessed significant developments in the field of cyber warfare. This conflict is an example where not only conventional weapons were used, but also cyber weapons.

Cyber warfare involves a country or a group of actors attacking the computer systems of another country with the aim of gaining strategic advantage or weakening the enemy. During the Israeli-Palestinian conflict, both sides played an active role in cyberspace, engaging in cyber espionage and activities aimed at harming the opponent.

Considering the 2023 cyberspace and cyber attacks, it is predicted that state-sponsored and hacktivist (voluntary) attacks will increase in cyber wars.

Attacks on IoT Devices

2023 witnessed a period of accelerating digital transformation on a global scale. Internet of Things (IoT) devices are increasingly present in every aspect of our lives, taking on more and more functions. However, this increased connectivity is also opening new doors for cyber threats.

Cyberthint threat hunters predict that attacks on IoT devices, whose security is often overlooked, in individual/organizational environments will increase in 2024.

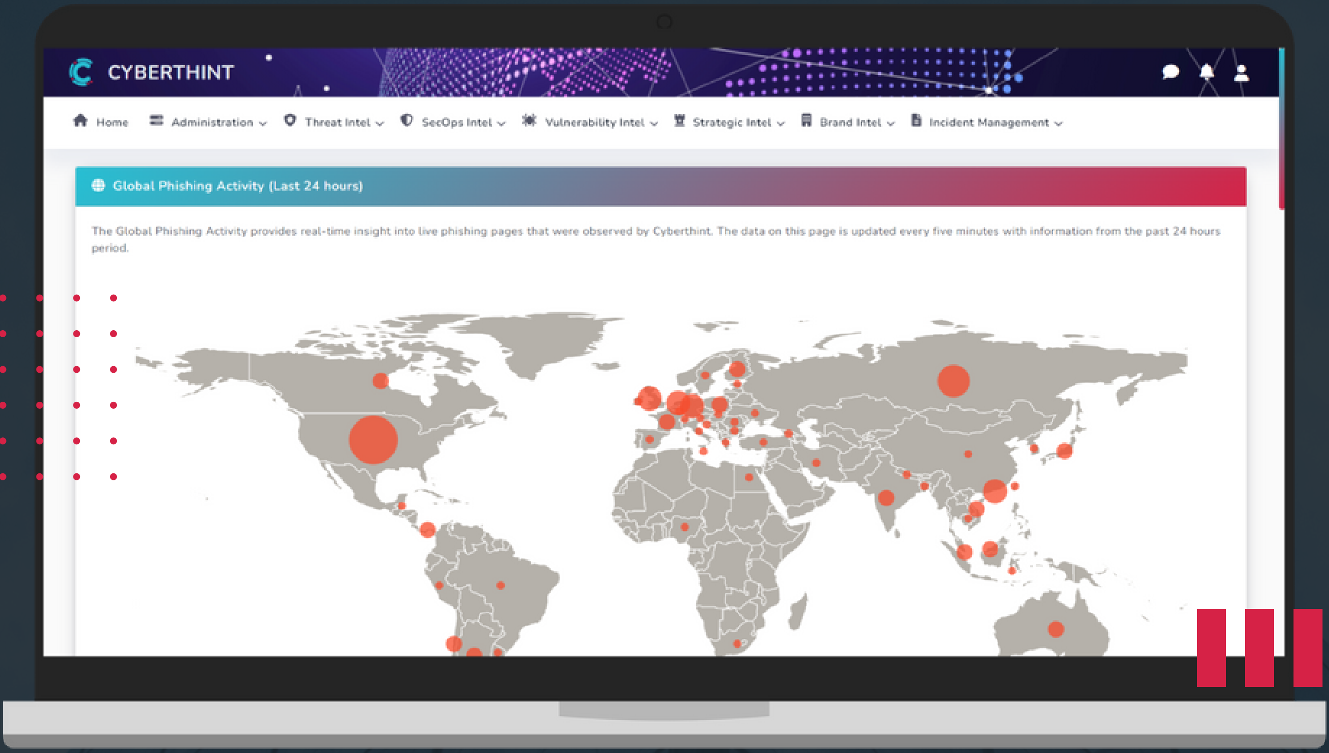
2024 Predictions

Cloud Platforms Attack Trend

With the progress of technology, the use of Kubernetes, Docker, OpenShift and other container platforms is becoming more popular and adopted, and cyber attacks on these platforms are increasing. Aware of this increase, threat actors continue to develop attack techniques to intrude into cloud-based platforms. At the top of these, misconfigurations in these cloud environments are exploited to gain access to systems. Therefore, threat actors are expected to increase their attacks on these platforms, which have an increasing attack surface. Threat actors have already started to produce malware such as ransomware, cryptominers and worms targeting cloud infrastructure systems. In order to protect themselves from these attacks, organizations should keep their cloud infrastructure systems up to date and apply newly released security patches without wasting time.

Volumetric Increase in DDoS Attacks

2023 was an important year for DDoS attacks. For example, in October 2023, Google announced that they had prevented the largest DDoS attack in history, a massive 398 million requests per second. Threat actors are expected to continue to negatively impact organizations in 2024 with large-scale attacks on networks and services. In 2024, DDoS attacks are expected to become more sophisticated and large in volume/scope.



Global Phishing Activity (Last 24 hours)

The Global Phishing Activity provides real-time insight into live phishing pages that were observed by Cyberthint. The data on this page is updated every five minutes with information from the past 24 hours period.

See
Cyberthint Unified Cyber Threat Intelligence Platform
in action

FREE TRIAL REQUEST

Contact Us

Website
www.cyberthint.io

X
@cyberthint

Telegram
t.me/cyberthint

Linkedin
Cyberthint

Email Address
info@cyberthint.io

Address
71-75 Shelton Street, Covent
Garden, London, United
Kingdom, WC2H 9JQ