cyberthint

GLOBAL CYBER THREAT INTELLIGENCE REPORT 2022

WITH FURTHER 2023 PREDICTIONS

Published

February 2023

Prepared by

Cyberthint

TLP

White

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.

News From Us

Telegram Channel

Follow darkweb and cybersecurity agenda with Cyberthint's Dark Monitor: t.me/cyberthint

New Version Released

New UI

20+ Projects

Many of our customers choose us again!

New Partnerships

ADEO CYBER SECURITY

Beyaz Net

EMA Security

intelegon

allincyber

About the Report

This cyber threat intelligence report stats prepared by Cyberthint, which includes important cyber events that took place in 2022 at the global level, cases encountered by **Cyberthint & Seccops teams**, observations and analysis, also includes threat predictions for 2023.

Resources

- 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

Editorial and media support of this report is provided by cloud7

CISCO HIT BY YANLUOWANG RANSOMWARE ATTACK

On Tuesday, August 10, in the evening, the Yanluowang Ransomware gang claimed on their official leak website that they had hacked Cisco and that they had the data and would publish it. Two hours after the allegation, Cisco published a detailed statement about the incident on its blog.

According to the Cisco statement, the leaked information was related to the account of a compromised employee and contained the data of the Box cloud storage folder, which did not contain any data that would compromise the security of its customers.

UBER ALSO SUFFERED MAJOR DATA LEAKS

Uber suffered two data breaches last year. The first incident occurred in mid-September, when a hacker posted a message on the company's Slack community saying "I am a hacker and Uber exposed a data breach". The hacker claimed to have accessed several of Uber's databases, including messaging data.

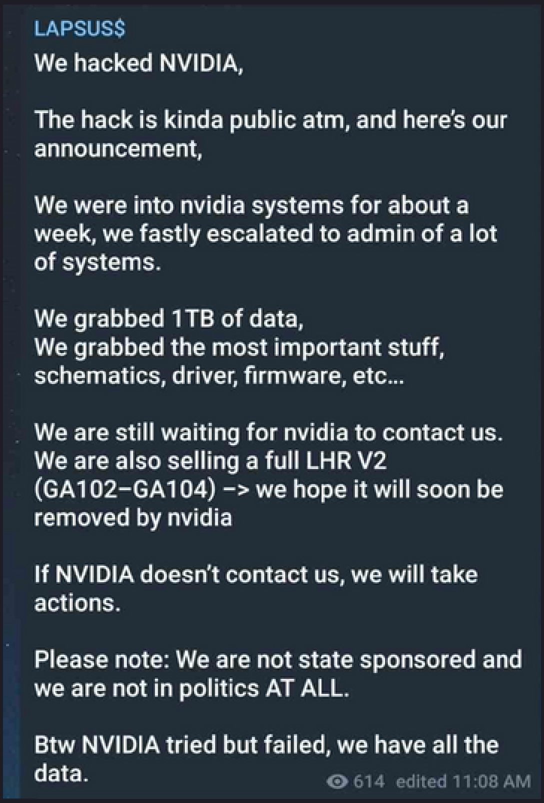
Just three months later, Uber exposed its second data breach when a hacker calling themselves "UberLeaks" accessed the data of more than 70,000 Uber employees.

MEDIBANK HACKED

Medibank, one of Australia's largest private health insurance providers, confronted a massive data breach in October affecting 9.7 million current and former customers. Hackers gained access to the personal data of all Medibank, its health insurance branch ahm and its international customers, as well as a significant number of health declaration data. This personal information included customers' name, address, date of birth and, in some cases, Medicare card numbers. When Medibank did not accept to pay the ransom offered by the REvil gang, the REvil gang began publishing the stolen data on the dark web in November 2022. The leaked data is also understood to include the names of high-profile Medibank customers, such as government MPs in Australia, including prime minister Anthony Albanese, The Guardian reported.

NVIDIA DATA LEAK

LAPSUS$ APT Group targeted Nvidia Company and accessed the data of more than 70 thousand employees.



LAPSUS$

We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

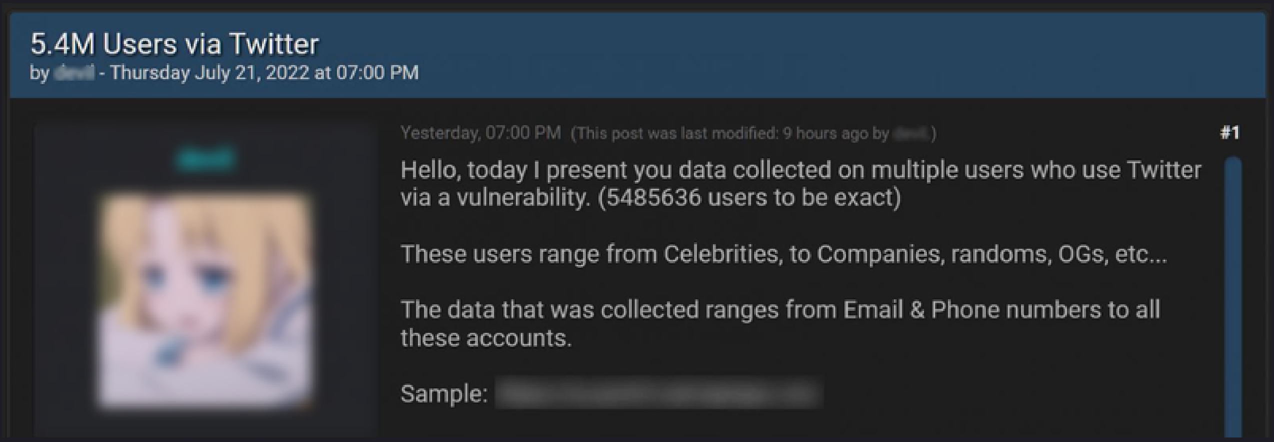
The LAPSUS$ Group, which captured more than 1 TB of company data in total, announced this attack via Telegram. Stating that the Nvidia Company should contact them, the LAPSUS$ Group publicly shared a 20 GB leak from the 1 TB of compromised data. By escalating their demands, LAPSUS$ then asked NVIDIA to share their gpu drivers as open source via Telegram. In the face of all these events, the NVIDIA Company confirmed this attack and announced on March 1, 2022 that they noticed this attack on February 23, strengthened their network, acted together with cyber incident response teams and applied to the necessary legal authorities. The company emphasized the importance of security and stated that they will increase their security measures day by day.

INTERNATIONAL RED CROSS ORGANIZATION DATA LEAK

On January 18, unidentified attackers leaked the data of more than 515,000 global Red Cross staff. According to the Red Cross statement, the attack on them was carried out with specifically designed attack tools that are used by APT groups and are not open to the outside. On December 9, 2021, the Red Cross determined that the attackers carried out this leak and stated that the attack occurred as a result of the CVE-2021-40539 vulnerability with a CVSS 3 score of 9.8. The data leaked from the attack included not only data belonging to the Red Cross, but also data belonging to the Red Crescent. The Red Cross Organization, which announced that it works in partnership with the Red Crescent, advised Red Cross and Red Crescent staff who believe their data has been compromised to contact the relevant local offices in their countries.

TWITTER DATA LEAK

Due to a vulnerability on Twitter, the data of 5.4 million Twitter users went up for sale on dark forums.



5.4M Users via Twitter

by [redacted] - Thursday July 21, 2022 at 07:00 PM

[redacted]

Yesterday, 07:00 PM (This post was last modified: 9 hours ago by [redacted]) #1

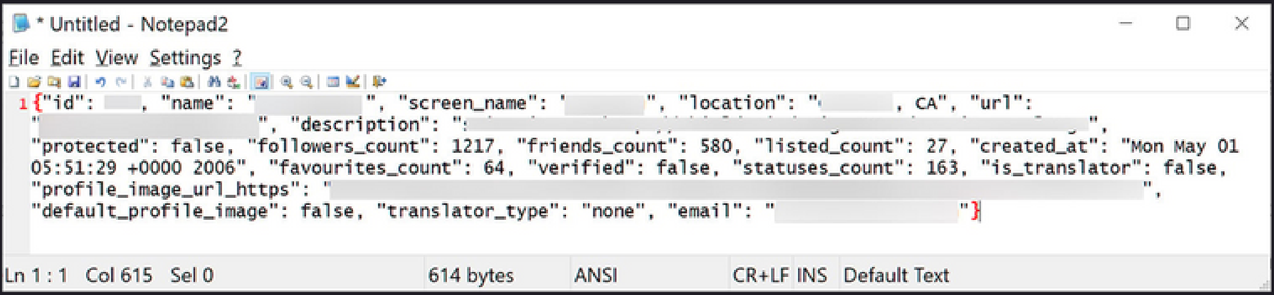
Hello, today I present you data collected on multiple users who use Twitter via a vulnerability. (5485636 users to be exact)

These users range from Celebrities, to Companies, randoms, OGs, etc...

The data that was collected ranges from Email & Phone numbers to all these accounts.

Sample: [redacted]

With this vulnerability, which allows you to find out which account an email or phone used on Twitter is associated with, attackers have obtained the data of many people since December 2021. Although this vulnerability, which had a CVSS3 score of 8.2 reported through HackerOne, a bounty hunting program, and earned the finder $5040, was later closed, malicious actors took advantage of the time until the vulnerability was closed and scraped the data of more than 5.4 million accounts.



```
{"id": [redacted], "name": "[redacted]", "screen_name": "[redacted]", "location": "[redacted], CA", "url":
"[redacted]", "description": "[redacted]",
"protected": false, "followers_count": 1217, "friends_count": 580, "listed_count": 27, "created_at": "Mon May 01
05:51:29 +0000 2006", "favourites_count": 64, "verified": false, "statuses_count": 163, "is_translator": false,
"profile_image_url_https": "[redacted]",
"default_profile_image": false, "translator_type": "none", "email": "[redacted]"}
```

The hacker who offered this data for sale on a hacker forum for 30 thousand dollars sold it twice in total. Stating that he could publish all the data for free in the future, the hacker kept his promise and published all this data for free on December 23, 2022. Although there was no password leak, the emergence of many users' information such as e-mail accounts poses a danger, especially for users who want to use Twitter anonymously.

ROCKSTAR GAMES' NEW GAME AFFECTED BY DATA LEAK

Some data belonging to GTA 6, which has been developed by Rockstar Games, one of the world's largest game companies, for more than 10 years, was leaked by cyber attackers. On September 19, 2022, Rockstar Games announced that many data, including confidential information from the early development process of the game, fell into the hands of attackers. The attackers released more than 90 videos of the in-game and put the game's source code up for sale. Rockstar Games took action in cooperation with the security services and as a result of the investigations, a 17-year-old young hacker who was found to be responsible for this leak was arrested in the UK. The arrested young member was detected to be associated with the Lapsus$ group responsible for cyber attacks on companies such as Nvidia and Uber. In light of all these events, Strauss Zelnick, CEO of Take-Two, the parent company of Rockstar Games, said in a statement that "all of this is disappointing, but the development of the game will not be affected."

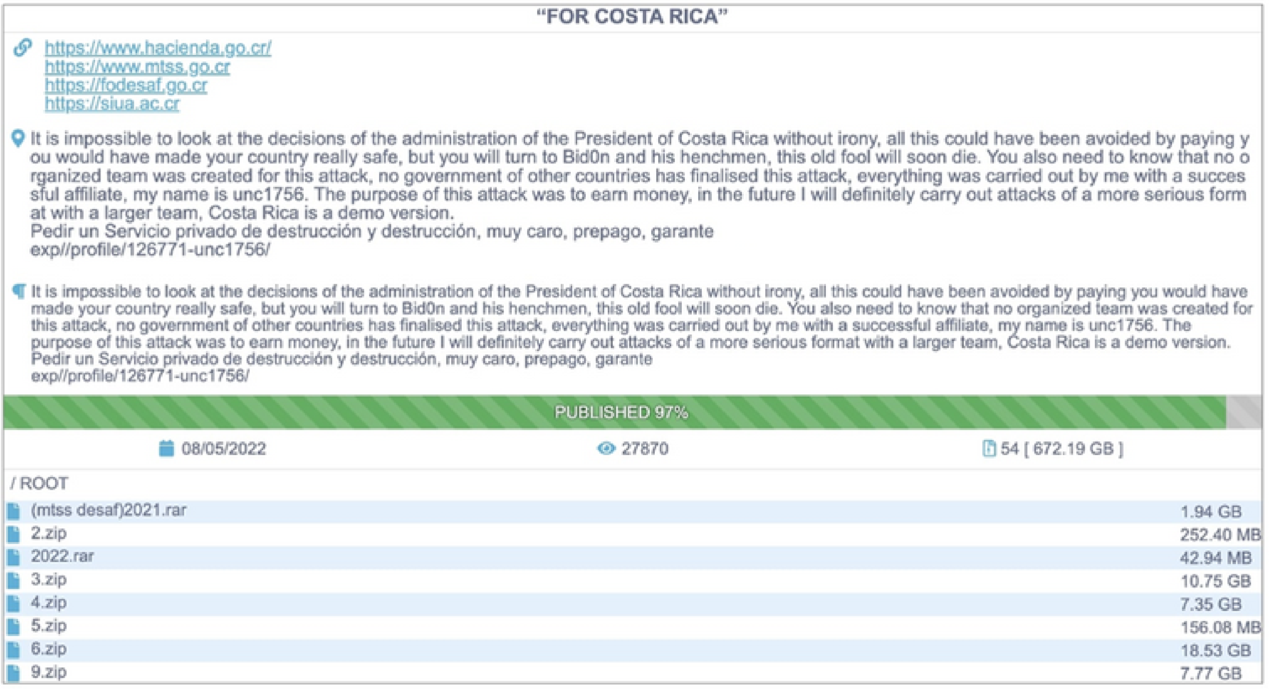
DROPBOX HACKED

In 2022, Dropbox became one another of the victims of phishing attacks. On October 14, the usernames and passwords of the GitHub profiles of some users within the company were captured by the attackers. With this information, threat actors were able to access Dropbox's secret github repos. The attackers accessed about 130 github repos of Dropbox and their connection to these accounts was blocked as soon as the threat was detected. Stating that no Dropbox user data was stolen, the Dropbox company added in a statement that some API keys, information of several hundred company employees, as well as old and current customer information were leaked. Dropbox Company, which was in the process of adopting a more phishing-resistant structure before this incident occurred, said in a statement that all of its environments will soon be secured by WebAuthn with hardware tokens or biometric factors.

MILLION DOLLAR THEFT FROM CRYPTO.COM

Crypto.com, one of the most well-known cryptocurrency trading platforms in the world, being exposed a major attack in January 2022. Approximately $18 million worth of Bitcoin and $15 million worth of Ethereum were stolen in this attack, which targeted the crypto wallets of approximately 500 people. It was determined that the attackers who carried out this attack, whose total net amount stolen was 33.7 million dollars, bypassed two-factor authentication and accessed users' accounts. In light of all these incidents, the company stated that it is working on the possibilities of switching to a new two-factor authentication infrastructure and increasing security in different ways.

COSTA RICA VICTIMIZED BY RANSOMWARE



"FOR COSTA RICA"

https://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying y
ou would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no o
rganized team was created for this attack, no government of other countries has finalised this attack, everything was carried out by me with a succes
sful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious form
at with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying you would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no organized team was created for this attack, no government of other countries has finalised this attack, everything was carried out by me with a successful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

PUBLISHED 97%

08/05/2022 | 27870 | 54 [672.19 GB]

/ ROOT

(mtss desaf)2021.rar	1.94 GB
2.zip	252.40 MB
2022.rar	42.94 MB
3.zip	10.75 GB
4.zip	7.35 GB
5.zip	156.08 MB
6.zip	18.53 GB
9.zip	7.77 GB

The Ransomware attack carried out by the Russia-based Conti Group against Costa Rica in April 2022 caused echo around the world. Costa Rica refused to pay this ransom against the Conti Group, which demanded a ransom of 10 million dollars as a result of the attacks. The Conti Group, which published more than 600 GB of stolen data over the internet, announced that it will continue its attacks. The attacks cost Costa Rica 30 million dollars a day and forced Costa Rica to shut down some of its services.

Rodrigo Chaves Robles and his government, which took charge on May 8 after elections in Costa Rica, declared a state of emergency in the country. Chaves said that his country was officially at war with the attackers and that there was clear evidence that some people in the country were in league with the Conti Group.

2400+ New Ransomware Victims

Ransomwares are undoubtedly one of the most damaging types of cyber attacks.

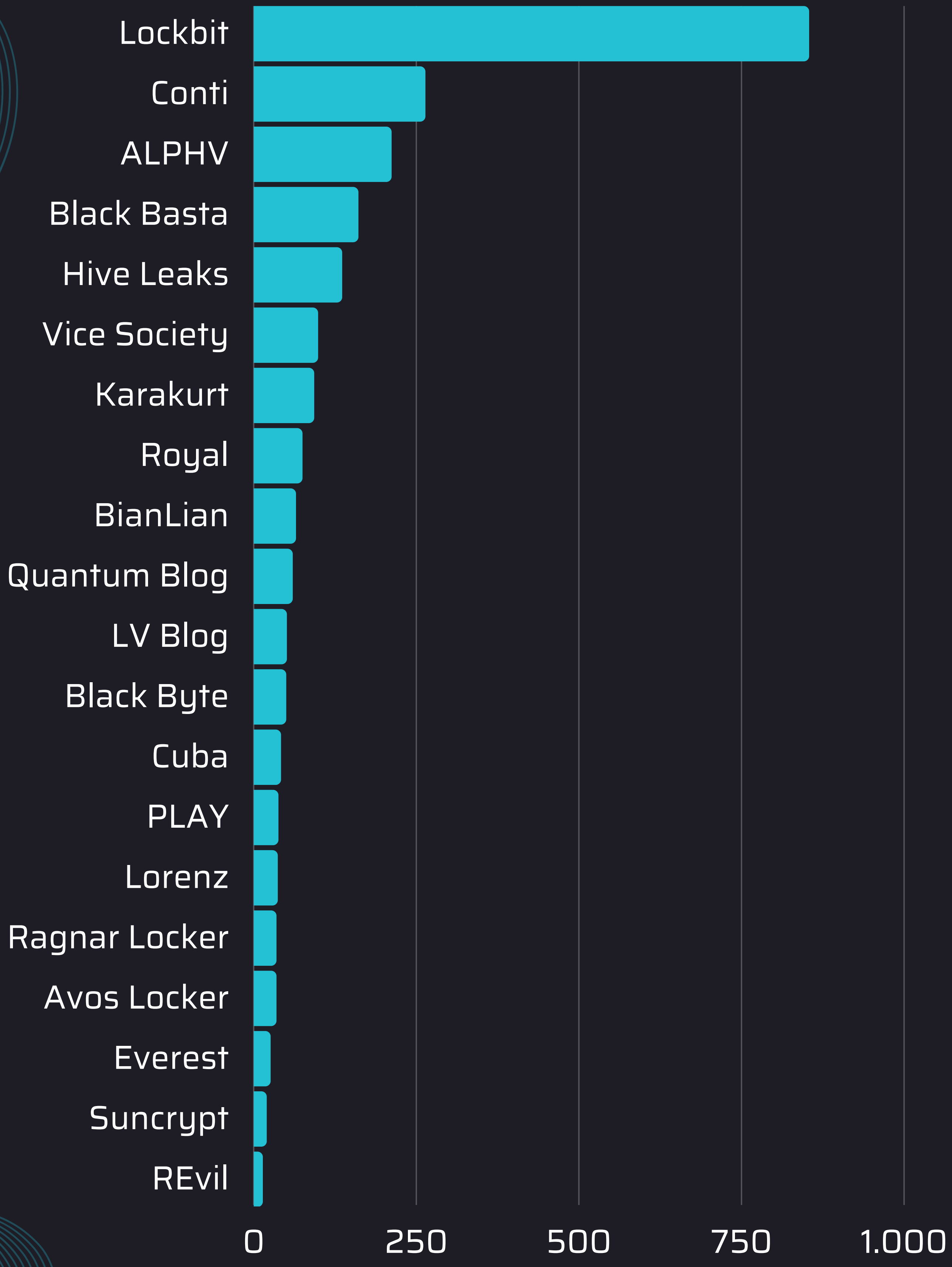
2022 was statistically the worst year for ransomware attacks. Whereas last year hackers focused on critical infrastructure and financial services, this year they focused on organizations where they could do the most damage. With the emergence of new ransomware groups, the techniques and methods used in attacks have become more sophisticated.

- There was an 82% increase in ransomware attacks in 2022.
- More than 2,400 companies have fallen victim to ransomware this year.
- In 2022, 15 new (active) ransomware groups were detected.
- LockBit was the most aggressive ransomware of 2022.
- The United States was the country most exposed to ransomware attacks this year.
- 80% of organizations have encountered an email-based ransomware attack at least once.

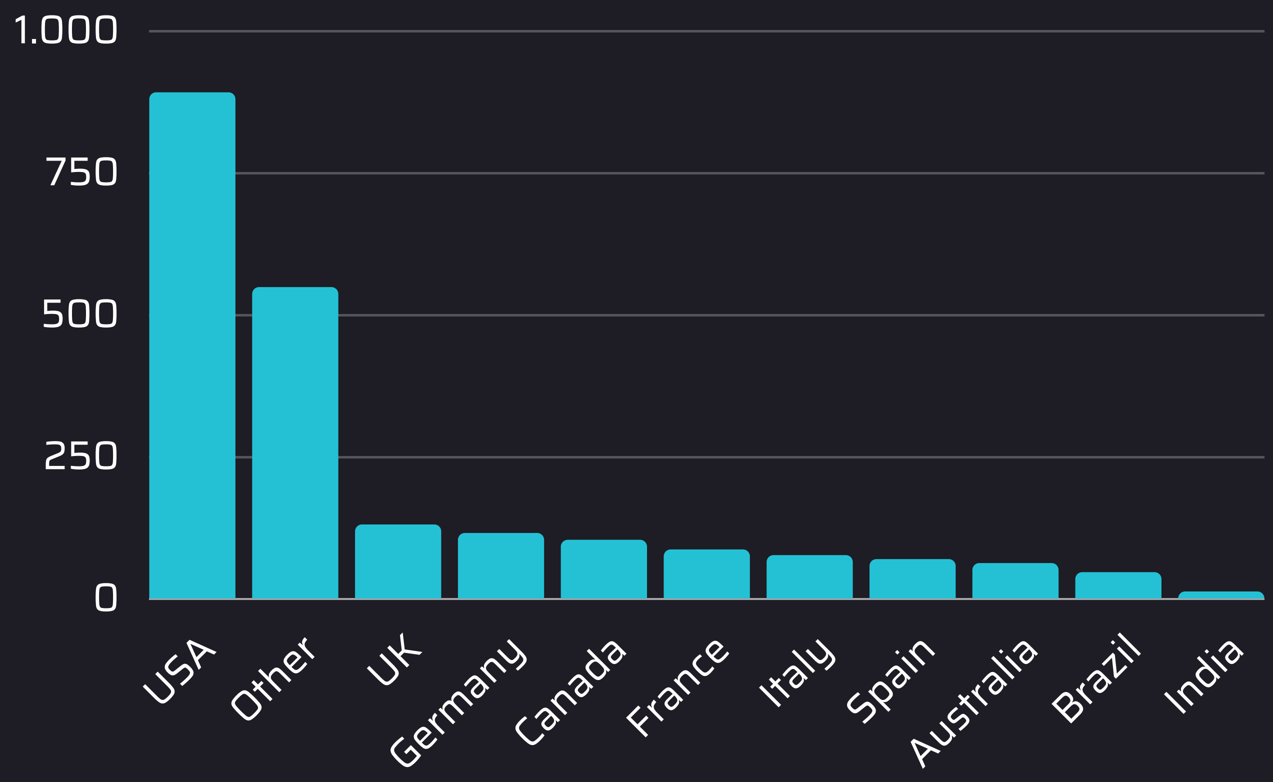
Recent Ransomware Groups

- NOKOYAWA Leaks
- Project Relic
- Medusa Locker
- Royal Ransomware
- Mallox Ransomware
- Free Civilian Ransomware
- DAGON Locker
- DAIXIN Team
- Qilin Ransomware
- Bl00dy Ransomware Gang
- Black Basta Ransomware
- Yanluowang Ransomware
- Play Ransomware
- BianLian Ransomware
- Cheers Ransomware

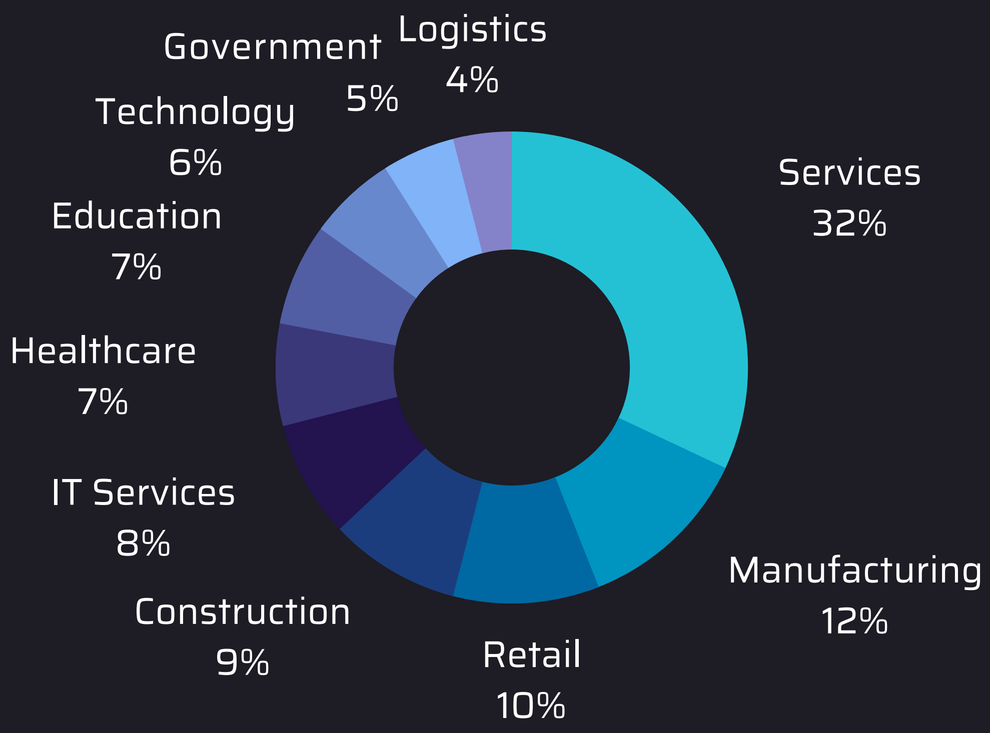
The Most Active Ransomware Crime Groups in 2022



Countries Most Affected by Ransomware Attacks in 2022



Industries Most Affected by Ransomware Attacks in 2022



APT ACTIVITIES

APT (Advanced Persistent Threat) is an advanced/sophisticated cyber attack or malware used in targeted attacks for purposes such as information gathering, espionage, sabotage.

APT Difference from Others

- To infiltrate the target system undetected and stay on the target for as long as possible, basically transmitting sensitive information to the source for its purpose.
- The fact that these attacks are aimed at a specific target, can bypass traditional security mechanisms and operate in target organizations for a long time makes it difficult to detect these attacks.

Newly Emergent APT Groups

- Dark Pink
- Polonium
- Earth Longzhi

Dark Pink

Active since June 2022, the Dark Pink group has so far carried out eight attacks targeting Vietnam, the Philippines, Indonesia, Cambodia and Bosnia and Herzegovina. Targeting primarily government and military organizations, this APT group uses a range of advanced tactics and special tools. The attack group targets its victims with personalized attacks through spear-pishing and aims to trap its victims through a series of attack chains and different scenarios.

Polonium

The Polonium Group, named after an element in the chemical periodic table, is a Lebanon-based group specifically targeting Israeli organizations. Thought to have been active since February 2022, this group was first detected by Microsoft in June 2022. The group, which mainly attacks organizations in sectors such as manufacturing, military defense and information technology, is thought to coordinate its operations with multiple actors in the Iranian Ministry of Intelligence.

Earth Longzhi

Earth Longzhi, a new subgroup of China-based APT41, is targeting several Asian countries and Ukraine. This group, whose existence was not previously known and whose existence was detected in November 2022, is thought to have been active since 2020. This group, which primarily targets sectors such as government, infrastructure, health and defense, carries out its attacks through spear-phishing. Earth Longzhi, which is competent in terms of red team capability, steals sensitive information of its victims thanks to the special methods and hacking tools it has developed.

Important APT Activities That Happened This Year

Cyberattacks in the Russia-Ukraine War

Since February 24, 2022, Russia's invasion of Ukraine has found its counterpart in the cyber world. There was already a cyber war between these two countries due to disagreements since 2014, but the momentum of the cyber war has increased considerably due to this latest war. So much so that experts described the situation as "cyber chaos", not cyber war.

According to the first quarter 2022 report published by STM(Savunma Teknolojileri Muhendislik ve Ticaret A.S.), Russia increased its online attacks against Ukrainian military and state institutions by 196 percent in the first days of the invasion it launched in Ukraine on February 24. Russian military intelligence GRU launched a series of DDoS (Distributed Denial of Service) attacks against Ukrainian websites in early February 2022. The attacks targeted Ukrainian banking and defense websites. Using the malware-as-a-service tool "DanaBot", Russian advocacy groups continued DDOS attacks against Ukrainian Ministry of Defense websites. On February 23, 2022, one day before the actual start of the war, Russia targeted Ukraine with HermeticWiper, a wiper software that corrupts system data and renders the affected system inoperable. The next day, on February 24, 2022, Russia attacked Ukrainian government systems with another wiper software, this time called IsaacWiper.

In the midst of this cyber chaos, Ukraine has attempted to create an army of cybersecurity experts in response to Russia's attacks. The aim was to attack Russia's strategic military and critical infrastructure. At the same time, Ukraine took actions to mobilize international sentiment. The activities bore their first fruit on March 1, when Anonymous officially declared war on Russia. At least 2,500 Russian and Belarusian targets were reportedly hacked by Anonymous. These included more than three hundred websites of Russian government agencies, state media organizations, banks, as well as the websites of leading Belarusian banks such as Belarusbank, Priorbank and Belinvestbank.

On March 14, ESET detected the third wiper software deployed by Russia and named it CaddyWiper. It had no coding similarities to the previously detected HermeticWiper and IsaacWiper, and was wiped all user data and information from infected devices.

Later on, Ukraine continued to attack Russian banks. So much so that on May 6, Russian state-owned bank Sberbank said in a statement that they had never been subjected to such a DDoS attack until now.

The DDoS attack was 450GB per second and aimed to inflict financial losses on Russians. In November, Ukrainian attackers announced that they had gained access to documents of the Russian Central Bank. By publicly sharing 27,000 files, the Ukrainian attackers also affected the Russian public's confidence in the Russian ruble.

With Ukraine's support in the international community throughout the war, Russia has been subjected to an unprecedented chain of cyber attacks. Ukrainian attackers published informational articles urging the Russian public to take part in opposing Putin and the war. Experts expect the cyber war between the two sides to escalate further.

The Breakdown of Diplomatic Relations between Iran and Albania as a Result of Iranian Hacker Attacks against the Albanian Government

A cyber attack on Albania in July, The Albanian government was forced to shut down some of its online services. A new ransomware was discovered during the investigation of this cyberattack and has been dubbed Roadsweep. This ransomware had encrypted files on compromised systems and left a ransom note claiming to be targeted by the Albanian government. Researchers compared Roadsweep ransomware to other malware and concluded that Iran might be behind it, but this was not entirely certain.

In September, the US White House blamed Iran for the cyberattacks on NATO ally Albania and strongly condemned the incidents. A few days after this condemnation, the Albanian government was again subjected to cyberattacks. According to a statement from the Albanian Interior Ministry, the attack forced the Albanian authorities to temporarily disable the Total Information Management System (TIMS), a system used to track data on those entering and leaving people in Albania. Albanian Prime Minister Edi Rama claimed in a tweet that the cyber attack was the work of "the same attackers" who carried out the July attack. In another statement, Prime Minister Edi Rama said that investigations had found "indisputable evidence" that Iran had hired four groups to carry out a cyber attack on Albania in July. In light of all these events, the Albanian government, convinced that the Iranian government was the perpetrator, announced on September 7, 2022 that it officially suspended diplomatic relations with the Iranian government and expelled Iranian diplomats.

Dark Pink Attacks

The Dark Pink Group, which mainly targets Asia-Pacific countries, launches its attacks with social engineering methods. In line with the attacks analyzed so far, Dark Pink initiates the chain of attacks with the spear-pishing method and directs its victims to upload ISO files in different scenarios. This ISO file opened by the victim activates a Dark Pink-specific malware called TelePowerBot. TelePowerBot is a registry construct that is launched via a script at system boot and connects to a Telegram channel where it receives PowerShell commands to execute. In another scenario, DarkPink uses a pest it calls KamiKakaBot. KamiKakaBot is a malware that targets data stored in Chrome-based and Firefox browsers. It can be described as the .NET version of TelePowerBot, which has information-stealing capabilities. As with TelePowerBot, this malware is injected into the ISO file and after the victim interacts with it, the data is leaked via Telegram.

The group is thought to have been active since June 2022, and so far eight attacks have been detected. According to researchers, Dark Pink may have carried out many more attacks.

North Korea's Use of Dolphin Backdoor

Operating since 2012, APT37, also known as ScarCruft, is a dangerous North Korean-backed espionage group that primarily targets South Korea but has also targeted other Asian countries. ScarCruft is mainly interested in government and military organizations, as well as companies in various sectors linked to North Korean interests.

According to ESET researchers, the North Korean-backed ScarCruft APT group targeted South Korea with a previously unknown backdoor "Dolphin". According to Filip Jurčacko, one of the researchers who analyzed the Dolphin backdoor, Dolphin has many espionage capabilities such as stealing credentials, leaking documents, taking screenshots, and keylogging. Dolphin's malicious use of cloud services such as Google Drive for data theft and command and control. Much more sophisticated than its counterparts, Dolphin can detect USB-like removable devices and connected smartphones, and is capable of exfiltrating files such as media files, documents, emails and certificates.

Dolphin weakens the security of its victims' Google and Gmail accounts by modifying their security settings so that threat actors can maintain access to their Gmail account.

APT41 Attacks Hong Kong with Spyder Loader Malware

The Chinese-backed APT41 group is targeting government organizations in Hong Kong as part of the ongoing Operation CuckooBees. This financially motivated threat group, which has been active since 2012, attacked targeted Hong Kong-based networks with SpyderLoader to gather information. Specifically targeting information storage systems, the attack not only gathered information but also executed malicious payloads, gathered information about corrupted devices and executed malicious scripts.

Researchers say APT41 had remained active undetected on some victim networks for more than a year. In addition to these attacks, APT41 continues to evolve the SpyderLoader malware with new features. Symantec Research Group warns companies to take precautions, especially those with valuable information that could be targeted by APT41.

Meta Detects New Android Malware Used by APT Groups

The activities of the South Asia-based Bitter APT and APT36 groups were among the leaders in the cyber threat report published by Meta (Facebook) in the second quarter of 2022. According to Meta's report, Bitter APT targeted New Zealand, India, Pakistan and the United Kingdom, infecting victims with malware. Bitter APT, which has so far made use of link shortening services, third-party server providers and exploited websites, has now added two more weapons to its arsenal: Fake and/or malicious mobile apps targeting iOS and Android users. The iOS version of these apps was a fake messaging app released through Apple's legitimate Testflight service, which was socially engineered to recommend people to download it. The Android version was dubbed 'Dracarys' by Meta. This malware, which was injected into illegal versions of apps such as YouTube, Signal, Telegram, Whatsapp, which have the ability to record and listen to audio, read messages, take photos, access call logs, etc. on the device, was used to steal many people's information.

The less sophisticated APT36 targeted military officials and human rights activists in Afghanistan, Pakistan, India, Saudi Arabia and the United Arab Emirates. The attackers posed as job recruiters, using both legitimate and fake companies to trap their victims, and shared malicious links to attacker-controlled sites hosting malware.

For APT36, which used the XploitSPY project on GitHub in its attacks, researchers noted that this is an attacker group that uses low-cost and readily available malicious tools in its attack campaign, rather than investing in developing its own tools.

Turkish Navy Attack MurenShark

NSFocus, a Chinese cybersecurity company, detected a cyber attack on the Turkish Navy project (MUREN) in Q2 2022. Based on the area of activity of the threat's entity and the final target they attacked (the Turkish Navy project "MUREN"), NSFOCUS Security Labs officially named it MurenShark and assigned it the identifier "APT-N-04". The monitored activities are indicated that MurenShark's main target areas cover Turkey and Northern Cyprus, targeting numerous sensitive institutions in the defense industry, universities, research institutes and the military. MurenShark particularly pays particular attention to military projects and conducts successful cyber espionage activities.

In its attack on the Turkish navy, MurenShark initially sends excel files containing malicious macros to the victim via the compromised bookstore.neu.edu.tr domain, and when the macro runs, it creates a dll file that allows the victim to download the main trojan. The deployed trojan downloads and executes shellcodes from the bookstore.neu.edu.tr domain and communicates with the CnC server.

MOST EXPLOITED SECURITY VULNERABILITIES

Spring4Shell

CVE-2022-22965

CVSS SCORE: 9.8

Spring, one of the most widely used frameworks in Java applications, basically acts as a framework that organizes the application background development process. Spring4Shell allows an attacker to remotely execute commands on the inputs it sends under certain conditions. Once threat actors are able to execute code remotely, they can install malware or use the affected server as a first foothold to escalate their authority and compromise the entire system. With more than 180,000 applications already using Spring, many systems have been affected by this vulnerability.

ICMAD RCE

CVE 2022-22536

CVSS SCORE: 10.0

CVE 2022-22536 is a vulnerability in SAP Internet Communication Manager. It was discovered on February 8 by SAP and Onapsis. The vulnerability allows an attacker to exploit the HTTPS request smuggling vulnerability where attacker-controlled data is appended to the beginning of user requests. This data can be executed by the vulnerable system with the user's identity, breaking the CIA trio of confidentiality, integrity and availability.

ProxyNotShell

CVE-2022-41040
CVE-2022-41082

CVSSV3 SCORE: 8.8
CVSSV3 SCORE: 8.8

ProxyNotShell is an SSRF vulnerability that an authenticated attacker can exploit for privilege escalation. CVE-2022-41082 is a vulnerability that allows an attacker to remotely execute code on Microsoft Exchange once it becomes accessible to the attacker. These vulnerabilities were among the notable vulnerabilities of 2022. Although the attacker must verify his or her identity before exploiting these vulnerabilities, the low level of complexity required to exploit this vulnerability and the high potential for potential damage to the confidentiality, availability, and integrity of systems turn it a vulnerability of high importance.

MOST EXPLOITED SECURITY VULNERABILITIES

F5 BIG-IP iControl REST RCE

CVE-2022-1388

CVSSV3 SCORE: 9.8

This vulnerability allows an attacker to bypass authentication by changing the HTTP request header and X-F5-Auth-Token value. It is easy to exploit and an unauthenticated actor can execute operating system commands to take malicious actions such as creating and deleting files or disabling running services. This vulnerability, which was thought to affect more than 2500 systems when it was first released, has been prevented with patch releases.

Log4Shell

CVE-2021-44228

CVSSV3 SCORE: 10.0

Log4Shell was discovered in November 2021 by Chen Zhaojun from the security team of the world-famous Alibaba company. This attack originated in Log4j, a java-based logging library. The impact of this vulnerability in Log4j, which has widespread use and the github project has been downloaded more than 400 thousand times, has affected many users. In fact, there were more than 100 attack attempts per minute against the vulnerability. Attackers using this vulnerability, which allows remote access to execute code, have mainly targeted corporate networks.

VMware vCenter Server RCE

CVE-2021-21972

CVSSV3 SCORE: 9.8

VMware has confirmed a high criticality (CVSS score of 9.8) remote code execution vulnerability in a vCenter plug-in for VMware vSphere Client (HTML5). With the vulnerability confirmed with CVE-2021-21972 code, attackers can have unlimited privileges on target systems by escalating authorisation with code activities over 443 network connections.

As the vSphere structure includes the ESXi hypervisor layer and vCenter management software installed in infrastructures, threat actors can carry out activities by accessing the entire target infrastructure.

MOST EXPLOITED SECURITY VULNERABILITIES

PetitPotam

CVE-2022-26925

CVSSV3 SCORE: 5.9

With this vulnerability, a threat actor can gain control of a domain controller by forcing authentication to a controlled NTML relay server. Subsequently, the threat actor can act as a client by intercepting the traffic flow. In fact, this vulnerability (AD CS) exists on Windows servers hosting directory certificate services that are not configured with protection against NTLM relay attacks.

The vulnerability can be remediated by applying the published security patch "KB5005413", which requires services that allow NTLM authentication to use extended protection for authentication.

Zoho ManageEngine RCE

CVE-2021-40539

CVSSV3 SCORE: 9.8

Zoho ManageEngine ADSelfService Plus, up to and including version 6113, was found to be vulnerable to a REST API authentication bypass and subsequent remote code execution. The bug, patched in September 2021, allows attackers to use specially-crafted Rest API URLs to bypass authentication due to an error in normalizing the URL before attempting validation.Having bypassed the authentication filter, attackers are able to exploit endpoints and perform attacks such as arbitrary command execution.

ProxyLogon

CVE-2021-26855

CVSSV3 SCORE: 9.8

ProxyLogon vulnerability was published by the DEVCORE team in August 2021. It is a vulnerability that directly affects Microsoft Exchange 2013, 2016 and 2019. This vulnerability allows an attacker to bypass authentication and thus impersonate an administrator. It remains one of the most exploitable vulnerabilities in 2022 due to the lack of updates to the internal infrastructure. The vulnerability has been added to various automated toolkits and has been used by various threat actors to deploy malicious code when the vulnerability is present. This flaw can be easily exploited on port 433 without user interaction, opening the door for lateral movement, persistent access, and remote manipulation.

MOST EXPLOITED SECURITY VULNERABILITIES

Microsoft Exhange Server RCE

CVE-2020-0688

CVSSV3 SCORE: 8.8

It is a remote code execution vulnerability detected in Microsoft Exchange Server, which first appeared in 2020, announced with the code CVE-2020-0688. The vulnerability occurs due to the unique key not being generated correctly during the initial setup. Using a known authentication key, it allows an authenticated user with a mailbox to pass arbitrary objects to be deserialized by the web application running with SYSTEM privileges. The CISA investigation found that Chinese actors used this RCE vulnerability to collect e-mails. In further investigations, it was also found that Russian threat actors used similar activities for similar purposes.

PCS Directory Traversal

CVE-2019-11510

CVSSV3 SCORE: 10.0

It is a vulnerability identified in Pulse Secure VPN devices, identified with vulnerability code CVE-2019-11510. With this vulnerability, attackers can gain unauthorised access to target networks. Attackers can read any file on the target system without the need for authentication through specially crafted URIs. Another determination made by CISA on the subject is that especially CVE-2019-11510 vulnerability is used by some threat actors for exploitation purposes on the US government and some commercial organisations.

Zimbra RCE

CVE-2022-27925
CVE-2022-41352

CVSSV3 SCORE: 7.2
CVSSV3 SCORE: 9.8

This vulnerability was found in the archive unpacking utility named cpio, which is used by the Significant vulnerabilities identified for the Zimbra Collaboration Suite platform. In the vulnerability published with the CVE-2022-41352 code, attackers could use the discovered RCE vulnerability to allow arbitrary shell access on the target server. An unpacking application called "cpio", which was used as an assistant by the content filter, could create a .tar archive containing malicious shell access. In this way, when the Amavis content filter is running, it can easily enable shell access on the target server by unpacking the malicious archive file to one of the directories in public use by calling the cpio application. The vulnerability published with the CVE-2022-27925 code allowed malicious RCE activity. The vulnerabilities have been patched in Zimbra versions 8.8.15P31 and 9.0.0P24.

MOST EXPLOITED SECURITY VULNERABILITIES

FortiGate SSLVPN Path Traversal

CVE-2018-13379

CVSSV3 SCORE: 9.8

A path traversal vulnerability has been detected on FortiProxy SSL VPN web portal, identified as CVE-2018-13379. This vulnerability allows FortiProxy system files to be downloaded without the need for authentication. The attacker can access the relevant files through specially created HTTTP resource requests. This vulnerability has been exploited for a long time. It has been used to operate major threats such as data theft, ransomware positioning. SentinelLabs has determined that the Iranian threat actor TunnelVision has made good use of the CVE-2018-13379 vulnerability, along with other vulnerabilities mentioned above, such as Log4Shell and ProxyShell, to target organisations.

Google Chrome Heap Corruption

CVE-2022-0609

CVSSV3 SCORE: 8.8

This vulnerability, which affects all Chrome users regardless of operating system, is a remote code execution vulnerability that was discovered as a result of an attack campaign by North Korean government-sponsored attack groups that exposed users to fake job opportunity emails from major companies such as Google, Oracle and Disney. This exploits Zero-Day UAF (use-after-free). According to MITRE, once memory is released, this exploit can cause a program to use unexpected values, corrupt valid data, crash, or execute code. This vulnerability has been fixed in subsequent updates of Google Chrome.

Follina

CVE-2022-30190

CVSSV3 SCORE: 7.8

Follina is a zero-day vulnerability in Microsoft Support Diagnostic Tool, Microsoft's troubleshooting tool, and Microsoft Office, which is used daily on many computers. It is a high-severity vulnerability that hackers can exploit for remote code execution (RCE) attacks.

Hackers can use malicious Word documents to exploit the Follin vulnerability. The executable MSDT in this document is executed using the Microsoft URL handler, and this executable can execute PowerShell commands, allowing attackers to access the target system and execute code.

MOST EXPLOITED SECURITY VULNERABILITIES

Atlassian Confluence RCE

CVE-2022-26134

CVSSV3 SCORE: 9.8

This vulnerability, also known as "OGNL Injection", discovered in Atlassian Confluence Collaboration Platform, allows an attacker to execute any code on the system. This can lead to various attack scenarios such as code injection, complete domain takeover, data theft, the use of remote access trojans (RATs) or ransomware.

FortiOS / FortiProxy / FortiSwitchManager Authentication bypass

CVE-2022-40684

CVSSV3 SCORE: 9.8

Vulnerability CVE-2022-40684 allows threat actors to bypass authorization in FortiOS, FortiProxy and FortiSwitchManager and perform unauthorized customized HTTP/HTTPS requests to the management interface. More than 150,000 devices were affected by this vulnerability.

ProxyShell

CVE-2021-31207
CVE-2021-34473
CVE-2021-34523

CVSSV3 SCORE: 7.2
CVSSV3 SCORE: 9.8
CVSSV3 SCORE: 9.8

In August 2021, it was discovered that a security vulnerability called ProxyShell allows RCE activity on Microsoft Exchange mail servers. Through this vulnerability, the attacker can perform authorisation escalation and create a basis for persistence activities on the targeted system. By executing malicious Powershell commands, full control of Microsoft Exchange servers can be taken. This vulnerability could be exploited at all points in Microsoft Internet Information Services (IIS) running on port 443, where users can access the mail service from mobile devices and web browsers.

The identified vulnerability on above that allow the following unauthorized operations respectively:

- Provides a mechanism for pre-authentication remote code execution, enabling malicious actors to remotely execute code on an affected system.
- Enables malicious actors to execute arbitrary code post-authentication on Microsoft Exchange servers due to a flaw in the PowerShell service not properly validating access tokens.
- Enables post-authentication malicious actors to execute arbitrary code in the context of the system and write arbitrary files.

MOST EXPLOITED SECURITY VULNERABILITIES

Zyxel Firewall Command Injection

CVE-2022-30525

CVSSV3 SCORE: 9.8

This vulnerability, found and reported by Rapid7, affects Zyxel firewalls that support ZTP. This vulnerability allows an unauthenticated and remote attacker to execute arbitrary code as a nobody user on the affected device. Given the severity of the security issue and the damage it could cause, NSA Cybersecurity Director Rob Joyce encouraged users on Twitter to update their vulnerable Zyxel software.

Zerologon

CVE-2022-1388

CVSSV3 SCORE: 10.0

A vulnerability has been released that severely affects Windows Server and Active Directory components. This vulnerability allows threat actors to illegally gain access to systems via RDP service or malwares, and allows the use of many attack techniques using escalation and lateral movement techniques. The vulnerability is due to a flaw in the cryptographic authentication scheme used by MS-NRPC to update passwords and provide access.

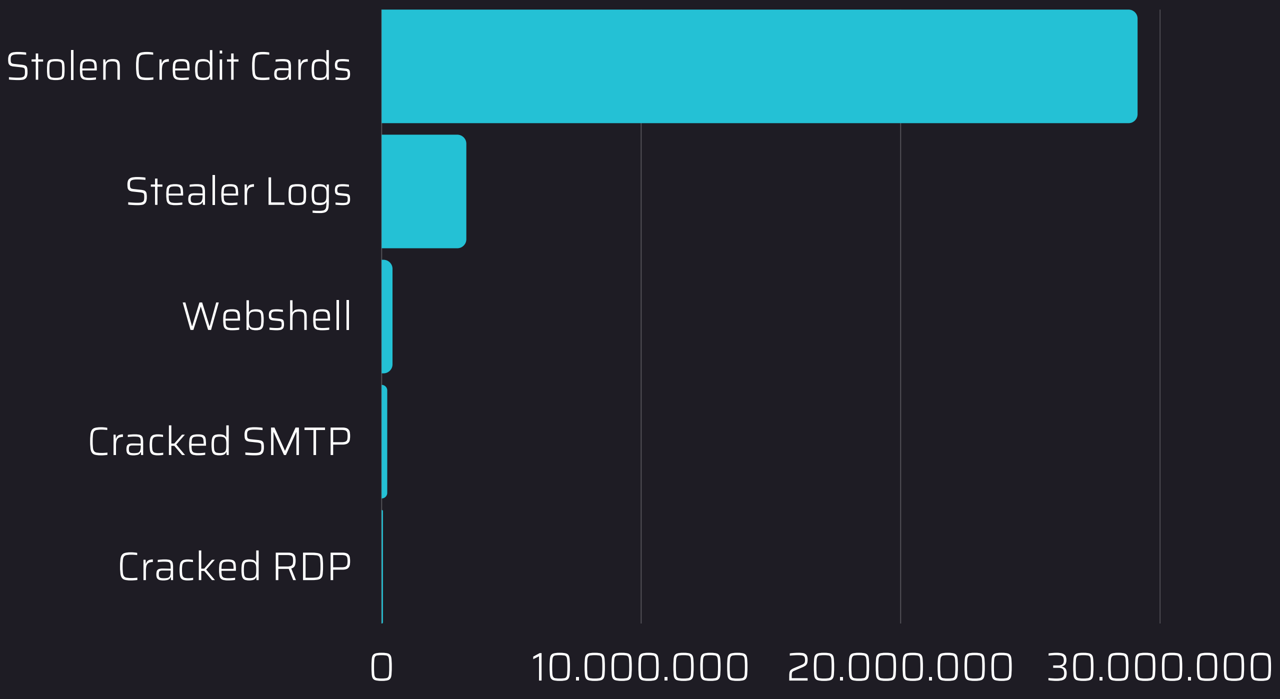
BLACK MARKET STATISTICS

Logs, which can contain important account information such as mail and VPN access, are used by threat actors for the "Initial Access" stage to infiltrate company systems.

In 2022, the following data was obtained by conducting detailed analysis of compromised accounts, credit cards, remote desktop connections, email accounts and unauthorized access websites offered for sale by hackers to generate revenue through popular and exclusive digital Black Market platforms.

30.000.000 Elements Offered for Sale

By Types of Products Sold in Black Markets



According to data publicly shared by the Tor Browser, nearly 2.5 million daily active users use the Tor Browser to access the Dark Web. We are sharing with you the 2022 statistics for the Dark Web, whose market network is growing and developing day by day.

Dark Web Revenues Drop by Half

The closure of Hydra Market which had been active since 2015 and was one of the dark web markets with the highest number of users, in April 2022, caused the total revenue from the dark web to halve. So that, while the total dark web revenue was 3.1 billion dollars in 2021, this number dropped to 1.5 billion dollars in 2022.

The Rise of Phishing Attacks

The human factor always remains a threat to security. Malicious actors who exploit this threat with social engineering methods target users and companies with various phishing attacks.

If there is no security weakness in the external attack surfaces of organizations, especially APT groups launch a well-designed Phishing campaign for the "Initial Access" phase in their targets.

Attack on Remarkable Rise: Cryptojacking

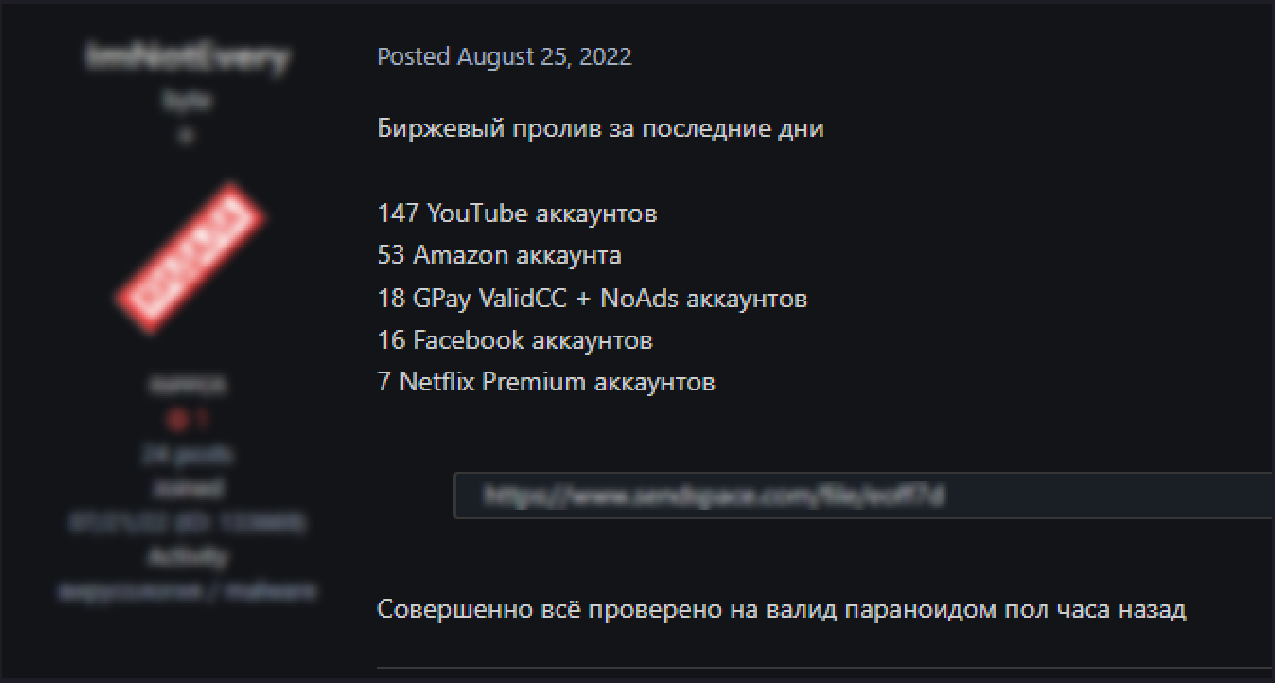
The use of cryptojacking, a type of attack that silently exploits victims' devices for cryptocurrency mining, increased by 230% in 2022. Ethiopia ranks first on the list of countries exposed to these attacks. AAs a result of the nature of its silent operation, this malware can work on its target victim's system for months without making itself known.

Drugs and Weapons At The Top of The List Again

According to the United Nations Office on Drugs and Crime(UNODC), weapons and drugs are the most commonly listed products on dark markets. It is thought that the rise of alternative social media, radical rhetoric and terrorist propaganda have contributed to these markets.

MALWARE VICTIMS' ACCOUNTS SCRAPED AND SOLD/SHARED

Threat actors scrape browser password logs obtained from computers infected with malware such as Stealer/RAT/Botnet and extract accounts, especially from platforms such as Spotify, Netflix, Disney, HBO, which operate on a subscription system, and offer them for sale or share them for free. In 2022, Netflix was the platform where the most user account information was leaked and shared/sold on the Dark Web.



[redacted]

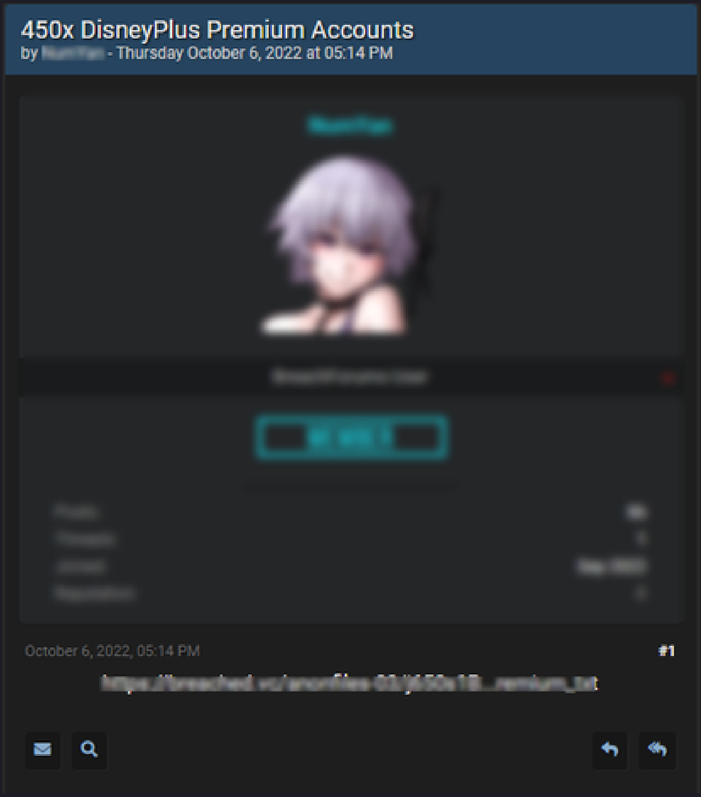
Posted August 25, 2022

Биржевый пролив за последние дни

147 YouTube аккаунтов
53 Amazon аккаунта
18 GPay ValidCC + NoAds аккаунтов
16 Facebook аккаунтов
7 Netflix Premium аккаунтов

[redacted]

Совершенно всё проверено на валид параноидом пол часа назад

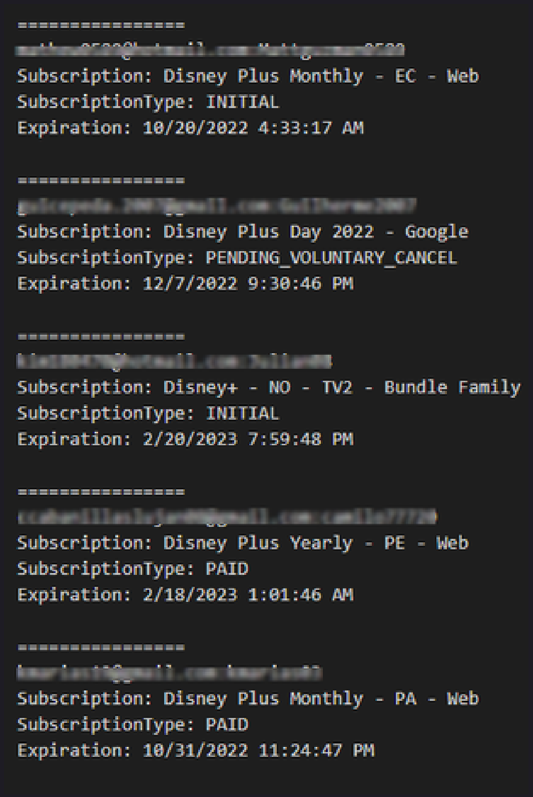


450x DisneyPlus Premium Accounts
by [redacted] - Thursday October 6, 2022 at 05:14 PM

[redacted]

October 6, 2022, 05:14 PM #1

[redacted]



```
================
[redacted]
Subscription: Disney Plus Monthly - EC - Web
SubscriptionType: INITIAL
Expiration: 10/20/2022 4:33:17 AM

================
[redacted]
Subscription: Disney Plus Day 2022 - Google
SubscriptionType: PENDING_VOLUNTARY_CANCEL
Expiration: 12/7/2022 9:30:46 PM

================
[redacted]
Subscription: Disney+ - NO - TV2 - Bundle Family
SubscriptionType: INITIAL
Expiration: 2/20/2023 7:59:48 PM

================
[redacted]
Subscription: Disney Plus Yearly - PE - Web
SubscriptionType: PAID
Expiration: 2/18/2023 1:01:46 AM

================
[redacted]
Subscription: Disney Plus Monthly - PA - Web
SubscriptionType: PAID
Expiration: 10/31/2022 11:24:47 PM
```

GLOBAL CYBER RISKS FROM NATION-STATE CYBER ATTACKS

As of early 2022, physical conflicts between countries and groups, which have increased to a degree that will shape the world agenda, also have an impact on the cyber world. Especially the field conflicts, which have also emerged in the Ukraine-Russia conflict, have also found their counterparts on cyber surfaces.

In addition to being used as a distraction during active warfare, it is not even inevitable that this fire will spread within the allies/alliances of the conflicting states. Slowing down the Ukrainian war and spreading it over time should be expected to have different reflections on the cyber level in the future, especially for Europe and the US. Threats of sanctions at the economic level should also be considered in terms of financial losses for the parties. Presently, this can be most easily achieved through targeted cyber attacks.

From a technical perspective, it is predicted that there will be a significant increase especially in 0-Day and malware. For example, wild activities such as service interruptions and espionage activities that the Blackenergy APT group has been experienced in the past in the energy sector are among the high expectations of security strategists in the coming period.

It is a well-known fact that 0-day stockpiles are increasing exponentially in order to be activated by major states in the event of future crises. In particular, similar threats against public organizations and ISPs could directly impact national economic activity. Effective implementation of Zero-Trust concepts will play a role in reducing security risks in this area. With the right IT staff employment, security tightening measures in organizations will have a high positive impact on their security posture.

"AVALANCHE" OF RANSOMWARE ATTACKS

Ransomware attacks, which have become the nightmare of IT Operations over time, are expected to increase their effectiveness in 2023 and beyond. IT operations will need to spend extra effort to increase their cyber resilience for ransomware attacks that they may face in a linear proportion.

As a new perspective, ransomware groups have also started to change the way they receive payments. Instead of relying on blockchain infrastructure, they are expected to focus on receiving payments through VISA, PayPal and other services. An important factor in their change in orientation is the difficulty in crypto conversions of those who are willing to pay the ransom.

In the meantime, with the temporary arrangements being made at the state level will be able to intervene in crypto transfers when deemed necessary. It is expected that large crypto transfers, which have become a major disadvantage for large cybercrime organizations operating as Ransomware-as-a-Service, will gradually become out of favor. It is predicted that institutions and organizations in Europe, which leads the way in terms of regulations, will be particularly affected by ransomware attacks in 2023.

INCREASING CYBER THREATS IN THE MOBILE WORLD

When we look at the cyber threats faced in the mobile world, it was determined that there was a 22% increase compared to the previous year with reference to Verizon MSI 2022 statistics. As the reason for this increase, it is stated that the new developments are around 80% effective. The MFA (Multi Factor Authentication) structure, which has become an important barrier in attacks on mobile applications, will continue to cause high security problems by obtaining and overcoming SMS-based OTP (One Time Passwords) obtained by attacks.

The increase in attacks predicted for 2023 will lead to a reduction in security risk by tightening controls instead of moving away from the MFA structure. Device-dependent and time-dependent MFA methods can be preferred. Mobile attacks, which are expected to accelerate, will continue to take place in our lives in the coming period.

HACKTIVISM AND DEEPFAKES FRAUDS

Keeping pace with the development of technology, cybercriminals & criminals are nowadays giving more importance to their development than ever before. Especially artificial intelligence applications & deepfake technology, which have been revolutionized in this field, have caused them to rub their hands for use in human and application manipulations.

In 2023, the increase will continue in the same way, with the prediction that politics, business and the art world will be affected first and foremost. Technical measures should be tightened without the need for preemptive feelings of forgeries to be made as audio, image/video and e-mail on virtual business models.

In the adventures that usually start with phishing content, attackers shuttle between industries and target organizations that verify their business processes through the virtual environment. In the recent past, there are known examples of millions of dollars of damage caused by this type of attacks.

CYBER THREATS FROM 5G DEPLOYMENT EXPANSIONS

With the introduction of 5G technology in recent years, cybercriminals are eager to travel on this roller coaster as bandwidth speeds multiplication. Vulnerabilities in deployments for hardware (especially routers) used in integrations for 5G access on mobile and PC devices create a useful attack surface.

It is predicted for 2023 that IoT elements used to support production in various industries will be remotely accessed and deployed over 5G, providing the basis for new leaks. The semiconductor component crisis affecting the IT supply chain will also be an obstacle to infrastructure reinforcement and renewal, creating the basis for 5G infrastructure-targeted attacks.

CHAIN REACTION: SUPPLY CHAIN ATTACKS

Supply chain refers to the ecosystem of people, organizations and distributors involved in the process. Supply chain attacks rank high among the primary threats due to their potential to cause significant impact.

Looking at the lifecycle of a supply chain attack, it can be seen that the attack (usually) includes two APT attacks. The first attack targets one or more suppliers (after the infiltration is successful), while the second attack takes place, targeting customers. This type of cyber-attack is more difficult to detect as customers already trust suppliers.

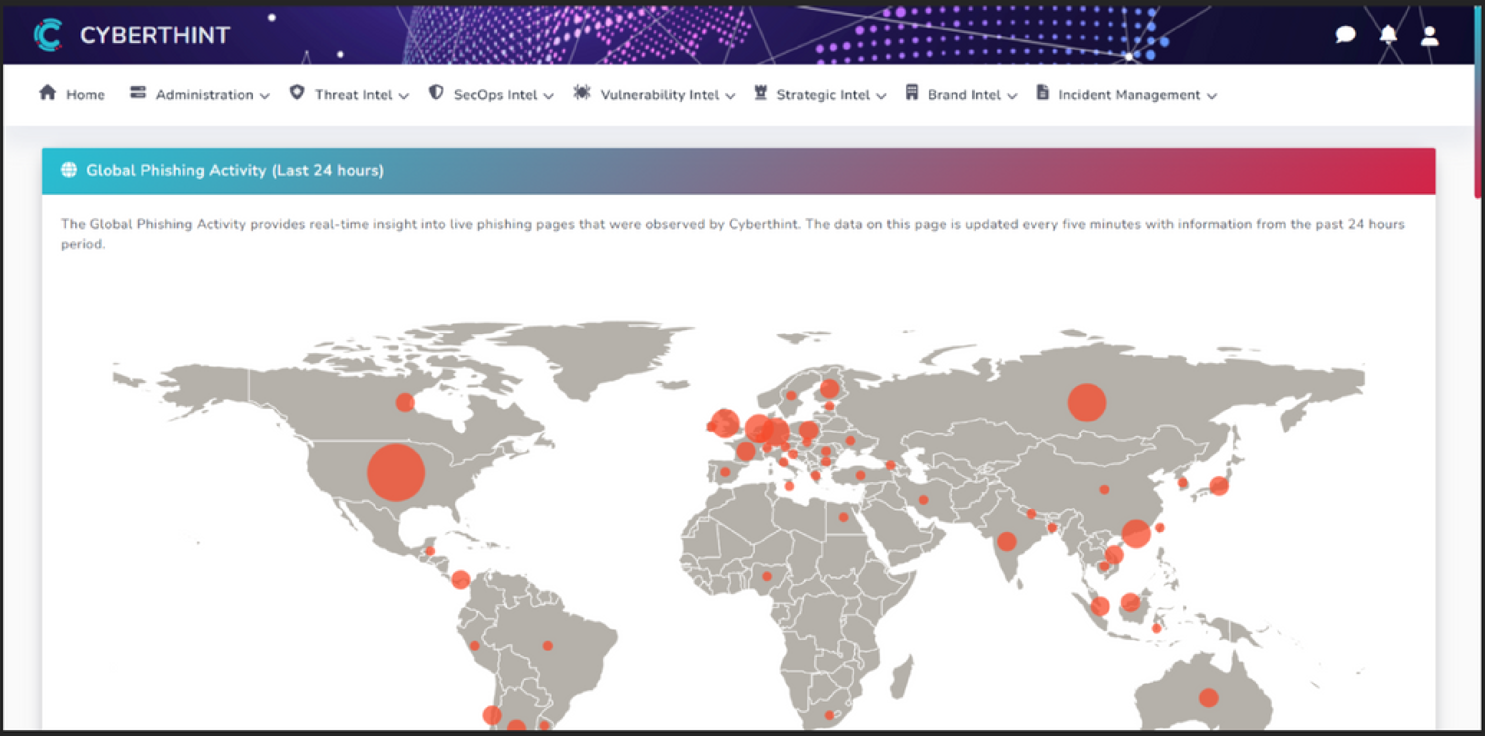
Supply chain attacks have long been a concern for cybersecurity experts, as the chain reaction triggered by an attack on a single supplier can compromise an entire network of providers.

The SolarWinds and Kaseya attacks are examples of the most memorable supply chain attacks.

The Cost of Cybercrime to the World

Cybercrime is estimated to cost companies $10.5 trillion in 2025, up from $3 trillion in 2015.

Cybersecurity Ventures reports that cybercrime represents the largest economic asset transfer in history, with an annual growth rate of 15 percent. This is evidenced by the increasing impact of incidents such as system downtime, monetary loss and reputational damage. Supply chain attacks are expected to increase over last year, which calls for urgent action by lawmakers and the cybersecurity community to take more stringent protective measures.



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.

cyberthint

Request a demo

Questions? Contact us.

Our cyber threat intelligence and security analyst team is ready to help you.

www.cyberthint.io

info@cyberthint.io

@cyberthint

t.me/cyberthint