JULY
2022

# THREATSPLOIT ADVERSARY REPORT

*Edition 47*

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

# Introduction

" It takes twenty years to develop a reputation & a few minutes of Cyber event to trash it" Stephano Nano

Yes, indeed. It takes years & years to construct systems from start. Writing codes, testing them & finally making them live. And, in minutes, hackers destroy it. All the reputation earned falls into the drain. Clients start doubting us on our efficacy to protect their information. In order, to make you understand better, so that you are equipped to manage any circumstance. We are presenting you the latest Threatsploit report. Let me tell you, what to expect!!!

Reddit was hacked with CRPF vulnerability that compelled the viewer to watch the adult data. The whole purpose of the hack was to collect the personal data. It was patched subsequently as per the report. Pegasus, a well famous Turkish airline was hacked. At this point, airliner strikes are all too common. Spi Jet ce aircraft was the focus of attention just a month ago. Pilots' navigation charts, manuals, and charts in the EFB (Electronic Flight Bag) were stolen from Pegasus. The alleged breach included trip plans, photos, and other details. Later, they were fixed. Hackers are now targeting airlines as a new target.

Kaiser Permanente, a Washington, D.C.-based hospital, was breached, exposing patient health information. It's deja vu all over again, given that health care organisations are frequently targeted by hackers. The dark web's high price for health data is the primary factor. It's expensive, which makes it a target for hackers.

One of the most infamous scams of all time is the Coin Egg Scam. Scammers enticed victims to invest in fictitious Crypto trading through the use of a bogus domain. They then used social media to get individuals to invest more money. As dramatic as anything you'll see on the big screen, this scam has it all. The Woo commerce site was targeted by scammers who stole credit card information.

The DDO's attack on President Putin's speech was the big story. Due to a DDOS attack, he was unable to deliver his address for an hour. We're all vulnerable to hackers, even the most powerful people on Earth.

We hope you have a secure month ahead of you, and that all of your digital assets and information are protected. We've got your back when it comes to your online safety. I wish you all the best with your writing, reading, and sharing.

# Contents

# TURKISH FLIGHT OPERATOR PEGASUS AIRLINES SUFFERS DATA BREACH

Pegasus Airlines, a Turkish airline, apparently had a data breach due to an unsecured AWS cloud storage bucket.According to reports, the open bucket contained the Electronic Flight Bag (EFB) data for an unknown number of clients, making sensitive data accessible.Turkey's data protection agency has since confirmed that a leak has happened after it received a data breach notification from the company. According to Safety Detectives, which disclosed the breach, almost 23 million files were found on the bucket, totaling around 6.5 TB of data.A blog post reads: "The bucket's information was linked to an EFB software developed by PegasusEFB that pilots use for aircraft navigation, takeoff/landing, refueling, safety procedures, and various other in-flight processes."PegasusEFB's open bucket left data including flight charts, navigation materials, and crew PII accessible to anyone."The bucket also exposed the EFB software's source code, which contained plain-text passwords and secret keys that someone could use to tamper with extra-sensitive files.""This exposure could impact the safety of every Pegasus passenger and crew member around the world," according to researchers. "Affiliated airlines that are using PegasusEFB could also be affected."

Sensitive Data Exposure

23 Million files data breach

Aerospace

# KAISER PERMANENTE DATA BREACH EXPOSED HEALTHCARE RECORDS OF 70,000 PATIENTS

The healthcare and personal information of up to 70,000 Kaiser Permanente patients in Washington state may have been exposed following unauthorized access to the US healthcare giant's email system.The data breach incident, which took place in early April, potentially exposed patients' first and last name, medical record number, dates of service, and laboratory test result information of the health plan provider.According to the healthcare provider, the hack did not expose any financial sensitive information, such as Social Security and credit card details.Kaiser attempted to reassure possibly impacted members in a breach notice (PDF) released earlier this month by noting that the security event was swiftly contained. Although not specified in Kaiser's breach notice, regulators from the US Department of Health and Human Services Office for Civil Rights reports that 69,589 records were potentially exposed as a result of the email security slip-up at Kaiser's Washington unit.

In response to the incident, Kaiser said it promptly reset the employee's password for the email account where unauthorized activity was detected."The employee received additional training on safe email practices, and we are exploring other steps we can take to ensure incidents like this do not happen in the future," Kaiser Permanente concluded.

Sensitive Data Exposure

healthcare records data breach of 70,000 patients

Healthcare

# DARK WEB AWASH WITH BREACHED CREDENTIALS, STUDY FINDS

According to a recent analysis from Digital Shadows, there are an alarming 24 billion usernames and passwords available on the dark web, a rise of 65% in just two years.Even after eliminating duplicates, Digital Shadows discovered that there are 6.7 billion unique credentials-an increase of over 1.7 billion or 34% in just two years. Some combinations are offered on forums more than once. Easy-to-use tools commonly available through criminal marketplaces at minimal cost or for free make it straightforward for even unskilled script kiddies to crack weak passwords.Simply adding a ‘special character’ (such as @ # or _) to a basic 10-character password makes it far harder to crack passwords and therefore makes it much less likely that a person will fall victim to an attack, with criminals instead attacking accounts that are easier to breach.Digital Shadows reports that the sale of stolen and cracked credentials remains a mainstay of sales through cybercrime forums and marketplaces.

> "Stolen credentials are one of the most crucial access tokens for a variety of cybercriminals and state-sponsored groups’ operations," Digital Shadows told The Daily Swig. "As such, the market for them is constantly florid and threat groups scramble to put their hands on these valuable assets."

Cyber Attack

6.7 billion usernames and passwords data breach

CyberCrime

# CRYPTO SCAMMERS HAVE REPORTEDLY STOLEN ₹1000 CRORE OFF INDIAN USERS BY POSING AS FAKE EXCHANGES

Users in India continue to fall for high-profile scams despite the enormous popularity of cryptocurrencies and cryptocurrency trading in the nation.Researchers at the security company CloudSEK have discovered a brand-new scam called CoinEgg that robbed customers in the nation of up to 10 billion (1,000 crore).We uncovered a persistent harmful scheme that involved numerous payment gateway sites and Android-based applications that was used to entice people into a widespread gambling scam. The researchers claim that the threat actors produced several fictitious websites with the name "CloudEgg" in them that impersonated cryptocurrency trading platforms.The business stated that the sites are divided into seven phases and that they are "intended to mirror the dashboard and user experience of the main website."In the second stage, the attackers build a female social media profile "to approach the possible victim and form a connection" after creating the bogus domains.

The victim is persuaded to start trading and investing in cryptocurrencies using this profile.According to the company, "The profile also shares USD $100 credit, as a gift to a specific crypto exchange, which in this case is a replica of a legitimate crypto exchange." The victims are enticed to sign up for the fake exchanges using this free credit, and start trading using the same, based on instructions from the attacker. They eventually invest their own money and “seemingly” make profits, which in turn convinces them to invest even higher amounts.

## THE RUSSIAN ECONOMIC FORUM WAS TAKING PLACE IN ST. PETERSBURG WHEN ITS PROCEEDINGS WERE STALLED DUE TO A DDOS ATTACK

The 25th St. Petersburg International Economic Forum, known as the Russian equivalent of the Davos World Economic Forum, was interrupted by a Distributed Denial of Service (DDoS) attack.the incident took place.As a result, Vladimir Putin's speech at the nation's biggest forum was postponed for around 100 minutes.More than an hour after it was due to begin, Putin finally got to speak.It's also important to note that due to the recent wave of sanctions on Russia following its invasion of Ukraine, there were no Western companies or stakeholders present at the forum.However, state-owned businesses signed agreements at the forum, and many others erected floor-to-ceiling display screens.

The accreditation and admittance systems were shut down as a result of the DDoS attack, according to Dmitry Peskov, a spokesman for the Russian government, who confirmed it to Reuters.However.Peskov did not name any specific organisation or person who was behind the attack.Even during the speech of the premier, the forum had persistent slowness and poor internet access.Putin attacked Western sanctions as a "blitzkrieg" on the Russian economy throughout his speech, calling them.

DDOS Attacks

Speach Delay

Government Sector

## ATTACKERS USE TELEGRAM BOT TO EXFILTRATE WOOCOMMERCE WEBSITES

The Telegram bot has been seen being used by a WooCommerce credit card skimmer to exfiltrate stolen information.After numerous instances of credit card theft were reported on an e-commerce website, the skimmer was discovered.Several customers initially complained to the website owner about fake card transactions occurring shortly after they made a purchase on the website.An inquiry was started just three days after the first instance of credit card theft was reported.

A lot of files were changed over the weekend, according to researchers. The first portion of the credit card skimmer was found inside the script[.]js file, where a custom file was added to the well-known Storefront WooCommerce theme and inserted at the checkout page. At the bottom of the file, a JavaScript snippet was spotted that sends a POST request whenever triggered by the Place Order button located on the checkout page of the website.

Credit Card Skimmer Attack

Credit Card Theft

MS Platform

# FALSE AIR RAID SIRENS IN ISRAEL POSSIBLY TRIGGERED BY IRANIAN CYBERATTACK

On Sunday night, air raid sirens were heard in the Israeli cities of Jerusalem and Eilat. It seems that these attacks were the result of a cyberattack, possibly by Iranian hackers. According to local media accounts, the sirens that alert the populace of rocket assaults sounded for almost an hour. The Israeli military's investigation revealed that the alarms were most likely set off by a hack that appeared to target municipal public address systems rather than the military's systems.

“It is possible that the sirens were triggered while hackers were still exploring for vulnerabilities within the municipality’s security system or that it was a false flag, being used as a distraction as another not yet published cyber attack was carried out,” Barda added.

“An example of this was the 2017 Iranian cyber attack on Saudi Arabia’s Aramco, where a breach was discovered, only to have thousands of computer systems compromised later, causing a devastating meltdown or explosion. Going after a municipality would bring a city or region to a halt, impacting supply chains, food deliveries, and more- putting a city under siege.” This incident comes roughly two years after hackers targeted several water and wastewater facilities across Israel. Those attacks were linked to Iran and experts noted at the time that the attackers appeared to have knowledge of industrial control system (ICS) hacking.

Cyber Attack

Systems Comprmise

Government Sector

In recent years, Iran’s critical infrastructure has often been targeted in cyberattacks, including airlines, nuclear facilities, railroad systems, ports, fuel services, and communication infrastructure. Some of these attacks have been blamed on Israel.

# REDDIT PATCHES CSRF VULNERABILITY THAT FORCED USERS TO VIEW NSFW CONTENT

Users were compelled to access adult content by Reddit due to a cross-site request forgery (CSRF) vulnerability.Any user who has chosen to filter adult content may instead be driven there by hostile hackers as a result of the medium severity security flaw disabling the possibility to turn on certain settings.A state-changing POST request to https://old.reddit.com/over18? lacked a sufficient modhash validator, making the sensitive action open to CSRF attacks, according to a bug report.

The option "I am over eighteen years of age and willing to access pornographic content" can be enabled or disabled in the victim account by tricking users into taking that action. The victim first creates a Reddit account, then goes to https://old.reddit.com/prefs/ to begin the reproduction process. and deselecting the checkbox indicating that the user is above 18 and wants to access adult content. The user then navigates to the "NSFW" subreddit at https://www.reddit.com/r/nsfw subreddit here>. when a window asks the user if they wish to view pornographic content.

Their settings will be adjusted and they will unknowingly be allowed to access NSFW content if they then open a specially prepared HTML file containing dangerous content. The security researcher was given a $500 bug bounty prize for reporting the problem, which was patched.

CSRF

Access to NSFW Content

Information Security

# BUSINESS EMAIL PLATFORM ZIMBRA PATCHES MEMCACHED INJECTION FLAW THAT IMPERILS USER CREDENTIALS

Security researchers have discovered a memcached injection vulnerability in Zimbra, a commercial webmail provider, which might allow attackers to obtain login credentials without user involvement.According to Synacor, the company that created Zimbra, more than 200,000 companies, 1,000 governmental and financial institutions, and other organisations utilise it as an open source substitute for email servers and collaboration tools like Microsoft Exchange.When the mail client connects to the Zimbra server, the vulnerability allows for the theft of cleartext credentials from the Zimbra instance.Attackers might inject arbitrary memcached instructions into a targeted instance and cause an overwrite of arbitrary cached entries because newline characters (rn) were not escaped in untrusted user input.

Zero Day Attack

Login credentials Takeover

Webmail Provider

# CRITICAL CITRIX ADM VULNERABILITY CREATES MEANS TO RESET ADMIN PASSWORDS

In order to prevent remote attackers from being able to reset admin passwords, Citrix has patched a significant vulnerability in its Application Delivery Management (ADM) platform. A remote, unauthenticated user ran the risk of crashing a system via a denial-of-service (DoS) exploit and subsequently resetting admin credentials on the next reboot due to the inappropriate access control vulnerability (CVE-2022-27511). The vulnerability could be exploited to force the "reset of the administrator password at the next device reboot, allowing an attacker with SSH [Secure Shell] access to connect with the default administrator credentials after the device has rebooted," according to a Citrix advisory published last week.

RCE

Reset Admin Credentials

Application Delivery
Management (ADM) Technology

The particulars of the issue turn what would normally be a system corruption problem into a much more severe vulnerability with a severity akin to that posed by an unauthenticated, remote code execution (RCE) flaw.Another, less severe vulnerability (CVE-2022-27512) creates a means to temporarily disrupt the ADM license service. An advisory from the US Cybersecurity and Infrastructure Security Agency warns that an “attacker could exploit these vulnerabilities to take control of an affected system”, emphasizing the seriousness of the potential risk.

# RESEARCHER GOES PUBLIC WITH WORDPRESS CSP BYPASS HACK

A security researcher has discovered a neat, albeit partially developed, technique to bypass CSP (Content Security Policy) controls using WordPress.The hack, discovered by security researcher Paulos Yibelo, relies on abusing same origin method execution.This technique uses JSON padding to call a function. That’s the sort of thing that might allow the compromise of a WordPress account but only with the addition of a cross-site scripting (XSS) exploit, which the researcher doesn’t have as yet.If an attacker finds an HTML injection vulnerability within the main domain (ex: website1.com – not WordPress,) using this vulnerability, they can use a WordPress endpoint to upgrade a useless HTML Injection to a full blown XSS that can be escalated to perform [remote code execution] RCE. This means having WordPress anywhere on the site defeats the purpose of having a secure CSP.

Cross Site Scripting

Account Comoromise

Content Management System

## ATTACKERS CAN USE ‘SCROLL TO TEXT FRAGMENT’ WEB BROWSER FEATURE TO STEAL DATA – RESEARCH

A security researcher has discovered that the Scroll to Text Fragment (STTF) feature, which enables users to quickly navigate to a particular text fragment on a webpage, can be leveraged to leak sensitive user data.The vulnerability, found by Maciej Piechota of SecForce, uses CSS selectors to gather data from a web page and send it to a server under the attacker's control.By using the '#:text' identifier and adding a text string to the URL of a webpage, users can access the STTF feature.The browser will immediately scroll to the string and highlight the appropriate area if it is present on the page.

STTF uses a special CSS directive to highlight the target text. Piechota found that if a page has a CSS injection vulnerability, an attacker can manipulate style specifications to cause the browser to send data to an attacker-controlled server through attributes that support the ‘url’ function.“All of attacks target and can exfiltrate data that is visible on the currently browsed website by the victim,” Piechota said.

XS Leaks

Sensitive User Data Leakage

Information Security

## RUBYGEMS TRIALS 2FA-BY-DEFAULT IN CODE REPO’S LATEST SECURITY EFFORT

RubyGems has become the latest code repository to require multi-factor authentication (MFA) for some of its largest publishers.The package manager has started alerting the maintainers of gems with more than 165 million downloads via the RubyGems command-line tool and website, recommending that they enable MFA on their accounts.While it’s currently just a recommendation, MFA will be enforced on these 100-odd accounts .

The Microsoft subsidiary hailed the move as “the first and most critical step toward securing the supply chain”.NPM, too, has been working to enforce 2FA, initially for its top 100 Node.js package maintainers, but with a broader rollout already underway.“It can help against the simplest of attacks against developer accounts, but it’s easy enough to bypass most MFA with off-the-shelf kits like evilginx2.”“Additionally, this does nothing to protect the integrity of authorship of source code. Finally, they should be requiring phishing-resistant MFA along with source code signing that is linked to the developer identity.”

Cyber Attack

MFA

Information Security

# INTERNET SCANS FIND 1.6 MILLION SECRETS LEAKED BY WEBSITES

RubyGems has become the latest code repository to require multi-factor authentication (MFA) for some of its largest publishers.The package manager has started alerting the maintainers of gems with more than 165 million downloads via the RubyGems command-line tool and website, recommending that they enable MFA on their accounts.While it's currently just a recommendation, MFA will be enforced on these 100-odd accounts . The Microsoft subsidiary hailed the move as "the first and most critical step toward securing the supply chain".NPM, too, has been working to enforce 2FA, initially for its top 100 Node.js package maintainers, but with a broader rollout already underway."It can help against the simplest of attacks against developer accounts, but it's easy enough to bypass most MFA with off-the-shelf kits like evilginx2."

"Additionally, this does nothing to protect the integrity of authorship of source code. Finally, they should be requiring phishing-resistant MFA along with source code signing that is linked to the developer identity."

Cyber Attack

1.6 Millions Secret Information Leakage

Information Security

# CRITICAL CODE EXECUTION VULNERABILITY PATCHED IN SPLUNK ENTERPRISE

This week, Splunk disclosed the availability of out-of-band updates that fix a number of flaws in Splunk Enterprise, including a serious problem that might result in arbitrary code execution.Splunk employs Splunk Enterprise deployment servers to distribute configurations and content updates to different Enterprise instances, including forwarders, indexers, and search heads.

Splunk provides large data monitoring and search capabilities.Since Splunk Enterprise deployment servers previous to version 9.0 allowed clients to use the server to deploy forwarder bundles to other clients, the newly addressed critical-severity vulnerability, tracked as CVE-2022-32158 (CVSS score of 9.0), exists.Because of this issue, an attacker could compromise a Universal Forwarder endpoint and then abuse it to execute arbitrary code on other endpoints connected to the deployment server. Splunk has resolved the issue with the release of Enterprise deployment server version 9.0 and encourages customers to update their instances to this version or higher.

Zero-Day Attack

Arbitrary Code Execution

Splunk Cloud Platform

# PACMAN ATTACK TARGETS APPLE M1 CHIP EMBEDDED CPUS

A new hardware attack targeting Pointer Authentication in Apple M1 chip-based CPUs with speculative execution was developed by researchers.Attackers can use this to execute arbitrary code on Mac systems.The security feature known as Pointer Authentication Code adds a cryptographic signature to operating system pointers (PAC).This enables the OS to recognise and prevent unforeseen changes that can cause data leaks. This new type of attack, which was discovered by researchers at MIT's CSAIL, enables someone with nefarious motives to physically access Macs with M1 CPUs and access the underlying filesystem.Attackers initially discover a memory fault impacting software on the targeted Mac that would be stopped by PAC then, after getting past PAC safeguards, escalate into a more significant security hole. Apple has claimed that the issue does not pose an immediate risk to users and is insufficient to bypass device protection. Further, experts stated that the attack doesn't come with real-world impact yet and that it was validated by a student and one of the four researchers behind PACMAN.

Pacman Attack

Arbitrary Code Execution on Mac Systems

Apple Technologies

# GITLAB ISSUES SECURITY PATCH FOR CRITICAL ACCOUNT TAKEOVER VULNERABILITY

GitLab has taken action to fix a serious security hole in its software that, if abused, could lead to account takeover.The problem was identified internally by the business and is tracked as CVE-2022-1680. It has a CVSS severity score of 9.9.All GitLab Enterprise Edition (EE) versions beginning with 11.10 and ending with 14.9.5, 14.10 and ending with 14.10.4, and 15.0 and ending with 15.0.1 are affected by the security bug. When group SAML SSO is configured, the SCIM feature (available only on Premium+ subscriptions) may allow any owner of a Premium group to invite arbitrary users through their username and email, then change those users' email addresses via SCIM to an attacker controlled email address and thus — in the absence of 2FA — take over those accounts,Also resolved by GitLab in versions 15.0.1, 14.10.4, and 14.9.5 are seven other security vulnerabilities, two of which are rated high, four are rated medium, and one is rated low in severity.Users running an affected installation of the aforementioned bugs are recommended to upgrade to the latest version as soon as possible.

Account Takeover Vulnerability

Account Takeover

Github Repository

# HACKERS EXPLOIT RECENTLY PATCHED CONFLUENCE BUG FOR CRYPTOMINING

The recently discovered remote code execution vulnerability in Atlassian Confluence servers has been used by a cryptomining hacking organisation to install miners on exposed servers.

The manufacturer provided a fix on June 3, 2022, but the vulnerability—tracked as CVE-2022-26134—was found as an actively exploited zero-day around the end of May.

In the days that followed, other proof of concept (PoC) attacks were made available, allowing a larger group of hostile actors a simple way to use the issue for their purposes.One of the threat actors who took advantage of this offering is a cryptomining group called the “8220 gang,” who, according to Check Point, perform mass net scans to find vulnerable Windows and Linux endpoints to plant miners.

Miners are special-purpose programs that use the host’s available computational resources to mine cryptocurrencies like Monero for the threat actor.The direct consequence of this activity is reduced server performance, increased hardware wear, increased running costs, and even business disruption.Additionally, by having access to the system, these actors can upgrade their attack anytime and drop more potent payloads.

Zero Day Vulnerability

Servers Exposed

Cryptomining Industry

# US SUBSIDIARY OF AUTOMOTIVE HOSE MAKER NICHIRIN HIT BY RANSOMWARE

The Japanese business Nichirin, which manufactures hoses for the automotive industry, recently experienced ransomware attack on one of its US subsidiaries. Investigations are being conducted to determine the entire effects of the incident, including any potential data breaches. The incident made the corporation switch to manual procedures and shut down part of its production control systems. Nichirin manufactures hoses for cars, motorbikes, as well as household goods. The business operates globally, including facilities in North America, Europe, and other parts of Asia, including China.Nichirin issued a warning to clients about phoney emails purporting to be from the business on its website. “If you reply to these emails,there are risks of fraud,virus infection,or leakage and misuse of your personal information,” reads the alert from Nichirin. “Please do not reply to any unknown email,access the URL listed,open any attachments,etc., and delete the email immediately.”

Ransomeware Attack | Email IDs Compromised | Automobile Sector

# HACKERS EXPLOIT MITEL VOIP ZERO-DAY IN LIKELY RANSOMWARE ATTACK

A Mitel VoIP equipment was used as an entry point in a suspected ransomware intrusion attempt against an undisclosed target in order to obtain remote code execution and acquire initial access to the setting.The information was discovered by cybersecurity company CrowdStrike, which also discovered a previously unknown exploit and a few anti-forensic measures used by the actor on the device to hide their tracks. The attack originated from a Linux-based Mitel VoIP device that was located on the network perimeter.The aforementioned zero-day attack is identified as CVE-2022-29499 and was patched by Mitel in April 2022 via a remediation script that it distributed to clients.

According to the CVSS vulnerability ranking methodology, it receives a severity rating of 9.8 out of 10, making it a major flaw. The exploit entailed two HTTP GET requests — which are used to retrieve a specific resource from a server — to trigger remote code execution by fetching rogue commands from the attacker-controlled infrastructure.In the incident investigated by CrowdStrike, the attacker is said to have used the exploit to create a reverse shell, utilizing it to launch a web shell ("pdf_import.php") on the VoIP appliance and download the open source Chisel proxy tool.etwork.

The binary was then executed, but only after renaming it to "memdump" in an attempt to fly under the radar and use the utility as a "reverse proxy to allow the threat actor to pivot further into the environment via the VOIP device." But subsequent detection of the activity halted their progress and prevented them from moving laterally across the network.

Ransomeware Attack Remote Code Execution Information Technology

## INSIGHT : RUSSIA IS ‘FAILING’ IN ITS MISSION TO DESTABILIZE UKRAINE’S NETWORKS AFTER A SERIES OF THWARTED CYBER-ATTACKS

As Ukraine continues to successfully prevent cyberattacks from its oppressor, Russia is failing in its aim to undermine the nation's cyber resiliency.The conclusion from WithSecure's Sphere conference this week was that Putin's government is "mostly failing," according to chief research officer Mikko Hyppönen.Mikko provided insight into the war between the two nations, which has been going on for more than three months, during the event, which was held in Helsinki, Finland. Russia has launched a number of cyberattacks against Ukraine's essential services and internet infrastructure since even before its invasion of the country started on February 24, 2022, in an effort to destabilise Ukraine.Reports of cyber activity between the two states have dwindled somewhat in recent months, Hyppönen told attendees, but not due to a lack of such attacks. Hyppönen argues that the decline in media coverage is actually a result of Ukraine's effectiveness in preventing Russian cyberattacks.He argues that unsuccessful attacks don't frequently make the headlines.

Cyber Attack Data Breach Government Sector

## CRITICAL FLAW FOUND INSIDE THE UNISOC SMARTPHONE CHIP

The smartphone chip made by UNISOC, which powers cellular connectivity in 11% of the world's smartphones, has what Check Point Research is describing as a major security risk.

According to the corporation, the flaw was discovered in the UNISOC modem firmware rather than the Android OS.A Shanghai-based semiconductor business called UNISOC, formerly known as Spreadtrum Communications, creates chipsets for mobile devices and smart TVs.If the vulnerability is not fixed, an attacker might use it to remotely block communications and disable modem services. The flaw affects 4G and 5G UNISOC chipsets, and Google will be publishing the patch in the upcoming Android Security Bulletin, CPR said. The company disclosed its findings to UNISOC, which it said gave the vulnerability a score of 9.4 out of 10. UNISOC has since patched the CVE-2022-20210 vulnerability.

Zero Day Vulnerability

4G and 5G UNISCO Chipsets affected

Semiconductor Industry

## BROWSER-IN-THE BROWSER SEXTORTION SCAM MAKES VICTIMS PAY BY IMITATING INDIAN GOV

Phishing has been a prominent cyber threat for decades, stealing the spotlight as the most prevalent attack vector for years, but the latest breed of attacks is more sophisticated and complicated to protect against than ever before. Attackers are always looking for new techniques to bypass security measures and remain undetected by victims. In the past year, Browser-in-the Browser (BITB) attacks have emerged as a very effective technique for evading detection and convincing users to hand over credentials.Underlining this trend, the Zscaler ThreatLabz team recently observed a new Browser-in-the Browser (BITB) attack impersonating an Indian government website to deliver a sextortion demand with the threat of releasing sensitive information about victims if they refuse to pay. This layered phishing attack appears to be the first of its kind, delivering a pop-up window that states a victim’s browser is blocked due to repeated visits of pornographic websites prohibited by the Government of India. Attackers then prompt the victim with an extortion demand requiring them to enter a credit card and pay a fine to avoid being arrested by the police.The homepage of this scam depicts a notice from the Indian government that due to repeatedly visiting pornographic sites user's browser is blocked and asks users to pay a fine by entering their card details. The mechanism by which the scam link is delivered to the victims is still unknown, but our research indicates that this may be linked to a landing page pop-up with a common alert that the user is about to leave the current page without saving the changes.

Browser-in-the Browser Attack

Login Credentials Takeover

Government Sector

# CORPORATE OFFICES

Briskinfosec
No:21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034.
+91 86086 34123 | 044 4352 4537

**INDIA**

3839 McKinney Ave,
Ste 155 - 4920,
Dalls TX 75204.
+1 (214) 571 - 6261

**USA**

Imperial House 2A,
Heigham Road, Eastham,
London E6 2JG.
+44 (745) 388 4040

**UK**

Urbansoft, Manama Center, Entrance One,
Building No.58, No.316, Government Road,
Manama Area, Kingdom of Bahrain.
+973 777 87226

**BAHRAIN**