THREATSPLOIT

ADVERSARY REPORT

Edition 45

BRISK INFOSEC

CYBER TRUST & ASSURANCE

MAY - 2022

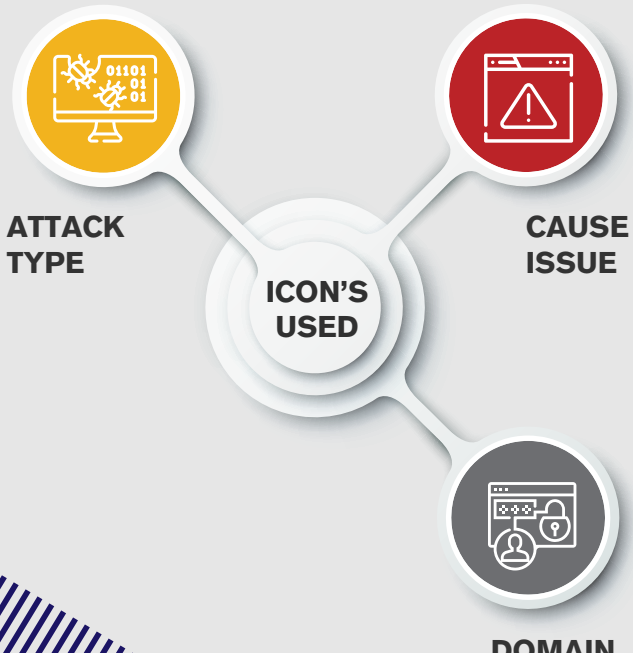
Introduction

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." – Stephane Nappo

A tarnished reputation will remain tarnished for the rest of your life. A significant portion of a company's budget goes toward the development of products and services, but protection for digital assets is sometimes overlooked. This month's Threatsploit Report is one of our favorites yet. This is to keep you safe in your own sphere of influence. Because of a cyberattack, an airline has been delayed. Is this the only vulnerability, or are there many more? Nobody really anticipates an attack on an airline. No one is safe in today's world. In Japan, the Morinaga chain sells ice cream and confections. Now, you're probably wondering how this relates to hacking. Although their stores were hacked and their data was exposed, this month's news has been dominated by these stories.

An attack on Toyota's plastics supplier, which supplies the automaker, has occurred. These days supply chain has been frequently disrupted by an attack. The supply chain has recently become a popular target for cybercriminals. This month, Japan is making headlines for a number of reasons in cybersecurity domain. Now that Pegasus is eavesdropping on Catalan politicians, he's doing havoc. Even India was rocked many months ago, as well. Ukraine's more than thirty universities have been compromised by the Monday gang. These were the standout attacks from the previous month, which drew the most attention.

To ensure that you get the most out of your stay here, we've done all in our power to help you. Distribute this issue to anybody you think would benefit from it, whether they be coworkers, friends, or business partners. We wish you a safe and pleasurable month of online exploration.



Contents

Cybercriminals Deliver IRS Tax Scams & Phishing Campaigns By Mimicking Government Vendors

On April 18, 2022, there was a notable campaign detected that utilised phishing e-mail spoofed to impersonate the Internal Revenue Service and a government vendor who provides solutions to government agencies that include emailing, and in particular one of the industry vendors who provide solutions to government agencies including e-mailing, .Cybercriminals purposely choose specific times when all of us are busy with taxes, and preparing for holidays (e.g., Easter), that's why you need to be especially careful during these times.Most major federal agencies, including the DHS, as well as state and local government WEB sites, use the IT services vendor actors impersonated.The phishing email contained an HTML attachment that resembled an electronic invoice, which the victims were instructed to pay via PayPal.

This e-mail was successfully delivered to the recipient's inbox without being flagged as spam because it contains no URLs.If the email headers are to be believed, the message was sent via several "hops" using mostly American network hosts and domains.he HTML attachment with the fake IRS invoice contains JS-based obfuscated code.After the user opens the HTML attachment, the phishing script will encourage the user to enter his credentials, this is done by leveraging an interactive form to impersonate the Office 365 authorization mechanism. Once the user enters their credentials, the phishing-kit automatically attempts to check access to the victim's e-mail account via IMAP protocol.

UK Government Staff Hit with Billions of Malicious Emails in 2021

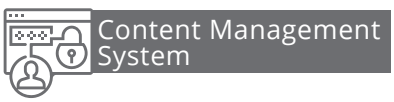
According to Comparitech, millions of malicious emails are sent to government employees in the UK each year, and they may have clicked on tens of thousands of suspicious links. More than 260 government agencies responded to a Freedom of Information (FOI) request from the tech comparison firm.An average of nearly 2.7 billion malicious emails were sent to 764,331 government employees in 2021; this works out to 2399 emails per employee.According to Comparitech, "received" meant that the emails had been identified by the organisations in question, and thus likely blocked, and not just received. On average, 0.32% of malicious emails were opened by staff in 2021, and 0.67% of these incidents resulted in employees clicking through on potentially malicious links, the report claimed."Seventy-one government departments were also happy to report that they hadn't suffered a ransomware attack in 2021 (the remainder – 187 – didn't disclose whether they had or not). Only two government organizations revealed that they had suffered a successful ransomware attack in 2021."

Android apps with 45 million installs used data harvesting SDK

More than 45 million people have downloaded apps from the Google Play Store that have collected personal information from them, according to mobile malware experts.All of this information was collected using a third-party SDK that has the ability to capture clipboard content as well as email addresses and phone numbers, as well as the MAC address and SSID of the user's router.Due to a lack of server/database security, the user's private information could be compromised.The contents of a clipboard, such as crypto wallet recovery seeds, passwords or credit card numbers, should not be stored in a third-party database because they could contain sensitive information. AppCensus, the group that first uncovered the SDK's use, says that the collected data is sent via the SDK to the domain"mobile.measurelib.com," which appears to be owned by Measurement Systems, an analytics firm based in Panama. AES encryption and base64 encoding are used to obfuscate many of the strings in the SDK's library, according to AppCensus researchers.

Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal

Access bypass and data overwrite were among the security issues which Drupal patched on Wednesday, according to the company's announcement.To begin with, a bug in the open source content management system (CMS) has been fixed that was caused by an incorrectly implemented generic API for entity revisions.For users who have access to use revisions of content in general, but not to individual node and media content, this API was not fully integrated with existing permissions, resulting in some possible access bypass." The vulnerability impacts Drupal 9.3 versions only, and solely affects sites where Drupal's revision system is in use.The vulnerability impacts Drupal 9.3 versions only, and solely affects sites where Drupal's revision system is in use.Due to this security hole, an attacker could inject disallowed values or overwrite data. The affected forms are uncommon, but Drupal notes that, in certain cases, the flaws could allow an attacker to modify critical or sensitive data.The bugs were resolved with the release of Drupal 9.3.12 and Drupal 9.2.18. Drupal 9 versions prior to 9.2.x and Drupal 8 have reached end-of-life (EOL) status and will not be updated. Drupal 7 is not impacted.



XSS vulnerability in open source tool Private Bin patched

PrivateBin, an open source secure pastebin, has had an XSS vulnerability patched.256-bit AES encryption ensures that the server has "zero knowledge of pasted data" when using PrivateBin. The vulnerability allows malicious JavaScript code to be embedded in an SVG image file, which can then be attached to pastes. A user opens a paste with a specifically crafted SVG attachment and interacts with the preview image while the instance isn't protected by an appropriate content security policy, an attacker can also execute code."Upon successful execution, it could allow access to unprotected cookies, local storage data, session storage data, etc, for other applications running on the same domain, where said cookies are present on the victim's browser. This may include authentication tokens. "Targeted phishing messages posing as messages from the Spanish government, parcel companies, and sometimes NGOs or voting technology providers were used to attempt to hack Catalan mobile phones.

" Canadian Low-Cost Airline Sunwing Suffers Flight Delays Due to Third-party Breach "

Thousands of passengers on Sunwing Airlines Inc, a Canadian low-cost carrier, are facing a fourth day of flight delays after a third-party system used by the company was hacked, according to the CEO. Because of the technical troubles that began on Sunday afternoon, people have been stranded abroad and holidays have been postponed for others, according to reports this week. Sunwing Airlines CEO Mark Williams said during an interview with CP24 that the airline's check-in and boarding system had been "breached." "Obviously, this is a terrible circumstance that we did not anticipate," Williams remarked. "We sincerely apologise for any inconvenience this has caused everyone. "The airline announced on Twitter on Tuesday that they were manually checking customers in for all flights.

How EMAIL Became the WEAKEST Link and at we can be done about it

Popular PC app 7-Zip has a major vulnerability on Windows

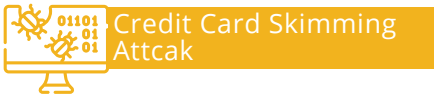
File compression and unpacking utilities like WinZip and WinRAR have been around for decades and allow you to compress and unpack files to save storage space. As a result, 7-Zip has become an essential tool for archiving files because it supports a wide range of zip formats.Now, Turkish Github user kagancapar has discovered a major flaw in the Windows version of 7-Zip.As a result of the vulnerability, someone with limited access to your computer could gain administrative privileges and run a wide range of commands and apps. The vulnerability can be exploited by dragging and dropping a 7-Zip (.7z) disguised file onto the Help > Contents area of the 7-Zip user interface. The help file included in the file archiver is used to exploit this vulnerability.Thankfully, it seems like this requires the attacker to have local access to your PC rather than enabling an attack over a network. Even so, this is a noteworthy shortcoming in a widely used PC application.The Github user offered two apparent solutions to address this vulnerability pending an app update. You can remove the 7-zip.chm file, or you can make sure that 7-Zip has only read and run permissions for all PC users by ensuring that the file is deleted.Even so, I suppose that dealing with this problem is preferable to purchasing WinRar.

Network cavity blamed for data breach at Japanese candy maker Morinaga

"Japanese confectionary manufacturer Morinaga has warned that a suspected data breach of its online store may have exposed the personal information of more than 1.6 million customers. Potentially exposed information includes the names, addresses, telephone numbers, date of birth, purchase histories, and, in fewer than 4,000 instances, email addresses of affected Morinaga Direct customers. The firm fears that attackers accessed several servers managed by the vendor after exploiting vulnerabilities in its network. After "several servers managed by the company were subjected to unauthorised access," "Morinaga says it" "cannot rule out the possibility of a leak of some personal information" of affected customers of its Morinaga Direct Store e-commerce business. Despite the company's apology to its customers, business partners, and other stakeholders, it stated that no credit card information was exposed.Morinaga shut down external access to its network after discovering the breach, before hiring external experts and setting about investigating the breach. “The initial investigation confirmed that several of the company’s servers had been subjected to unauthorized access and that access to some data had been locked,” the vendor’s official statement said, adding that one of the affected servers handled product deliveries to Morinaga Direct Store customers."

Credit card industry standard revised to repel card-skimmer attacks

In order to encourage e-commerce providers to improve their defences against JavaScript-based card-skimming attacks, the payments card industry has made significant revisions to the PCI DSS standard.PCI DSS v4.0, which sets the baseline requirements for organisations that handle payment or credit card data, has been beefed up to combat so-called Magecart-style attacks, among other improvements, in its latest revision. In order to help prevent and detect digital skimming, PCI DSS v4.0 has added two new requirements.Payment page scripts that are loaded and executed by consumers' browsers must be managed in accordance with a new e-commerce requirement. A mechanism to detect changes or indicators of malicious activity on payment pages is also a new requirement.The dynamic nature of web pages, where content is frequently updated from multiple internet locations, necessitates these requirements to mitigate the risks. “This overlapping infrastructure could include a hosting provider used by several skimming domains loading multiple, unrelated skimmers – the Inter skimmer and different versions of Grelos, for example. We even observed domains loading different skimmers from the same IP address."



Pegasus mobile spyware used zero-click exploits to snoop on Catalan politicians

"Commercial spyware called pegasus was used to hack into the phones of Catalan politicians, lawyers, and their families..

A total of 65 people have been found to be under the surveillance of Israeli firm NSO Group's Pegasus or another commercial surveillance app called Candiru, thanks to Citizen Lab's collaboration with Catalan civil society groups.Victims included members of the European Parliament, regional politicians, and members of civil society organizations.

In some cases, family members were also affected.According to Citizen Lab and Amnesty International's Tech Lab, some Pegasus infections were caused by the deployment of a previously-undisclosed iOS zero-click vulnerability.There was evidence that multiple zero-click iMessage exploits were used to hack Catalan targets' iPhones with Pegasus between 2017 and 2020. Attempts to exploit the Homage (recognised to be fixed by iOS 13.2) and later Kismet iMessage zero-click exploit were made in summer 2020 against iOS 13.5.1 and iOS 13.7. “Though the exploit was never captured and documented, it was apparently fixed by changes introduced into iOS14, including the BlastDoor framework,” Mobile phones in Catalonia were targeted with phishing messages posing as messages from the Spanish government, parcel companies, and sometimes NGOs or voting technology providers. This was the method used.

Malicious SMS messages and the Candiru spyware were used to infect a large number of people. Only four people were infected with Candiru, and only one of them has been confirmed to have been infected.There were at least two victims infected by Pegasus, which was far more prevalent than Candiru.There were a total of 63 Pegasus targets.A total of 51 were successfully infected, many suffering infection multiple times. Citizen Labs' forensic work focused on iOS devices, far less preferred than their Android equivalents in Spain."

Toyota shuts down production after 'cyber-attack' on supplier

In response to a "system failure" at Kojima Industries, Toyota has suspended production at 14 plants in Japan for at least one day.A cyber-attack on Kojima Industries, which supplies Toyota with plastic parts and electronic components, has been rumoured but not confirmed.A domestic supplier (KOJIMA INDUSTRIES CORPORATION) had a system failure, so we decided to suspend 28 lines at 14 Japanese plants. The suspected cyber-attack has been described as an illustration of the growing importance of supply chain security by third-party security experts.A successful attack on the software supply chain can have a negative impact on the output of physical goods, as demonstrated by this incident,"

Vulnerability in AWS Log4Shell hot patch allowed full host takeover

Protection for containers is the goal of these patches. It was possible for malicious containers to compromise the underlying host through critical vulnerabilities in Amazon Web Services (AWS) containers that were guarded against the dangerous Log4Shell bug.Container-protection patches An Amazon Web Services (AWS) container against the Log4Shell bug had critical flaws that allowed malicious containers to gain access to the operating system of the host.Researchers at Palo Alto Networks Unit 42 discovered the vulnerability which could be exploited to take over the server or cluster running the patch service.According to their findings, the vulnerability can be exploited by every container in a cluster in order to escape and gain elevated privileges.Additionally, unprivileged processes can take advantage of the patch service to gain root-level access to the system.Java binaries are found in containers, and the hot patch uses its own server-level privileges to invoke them.As a result, the process is able to run without the usual restrictions on container processes.In order to trick the patch into invoking it with elevated privileges, a malicious container may include a java binary. This would allow it to escape the container and take control of the underlying host.The researchers posted a proof-of-concept that exploits the vulnerability to escape container limits, gain root code execution on the underlying host, and send a reverse shell to an attacker-controlled server.

Remote code execution

Host takeover

Information Technology

VMware patches critical flaws in Workspace ONE Access identity management software

Virtualization software vendor VMware has released patches addressing critical web security vulnerabilities in several of its products.The updates, released today (April 7), include patches for a remote code execution (RCE) flaw in VMware Workspace ONE Access, formerly known as Identity Manager.The vulnerability – tracked as CVE-2022-22954 and with a CVSS rating of 9.8 – arises as the result of a server-side template injection issue."A malicious actor with network access can trigger a server-side template injection that may result in remote code execution," VMware warns in a security bulletin.The flaws – tracked as CVE-2022-22957 and CVE-2022-22958 and given a severity rating of 9.1 – meant that an attacker with "administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution".

Server Side Template Injection

Information Disclosure

Software Management

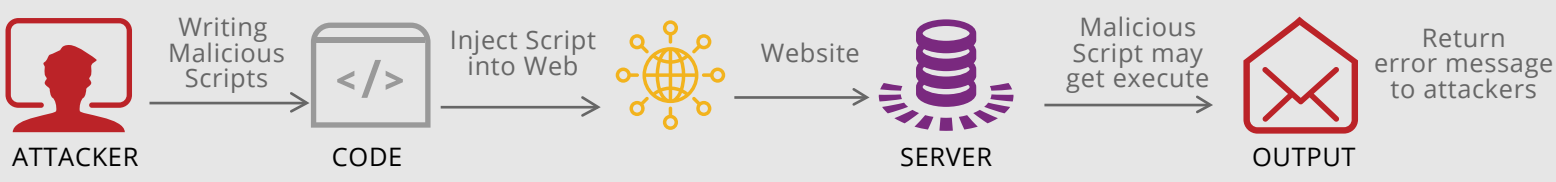
TruffleHog v3: API key leak detection tool adds support for more than 600 types

Available on GitHub, TruffleHog is an open source project tool for discovering keys leaked via JavaScript or too-permissive CORS settings in APIs.The newest version of TruffleHog has landed with support for more than 600 key types, furthering the tool's ability to hunt for credential leaks.Leaked credentials, including secret key pairs, are a serious cybersecurity issue. Keys can be abused to compromise enterprise networks, often more covertly and for longer time periods than the exploit of vulnerabilities in popular software.The system can alert developers or researchers when websites or front-end applications are accidentally leaking keys. TruffleHog can also be used to find exposed .git repository credentials.In addition, 639 key types are now supported, including AWS, Azure, Confluent, Facebook, and GitHub. "We do not know of another secrets scanning engine that supports this many key types, let alone the verification, and the fact they're all now open source,"

Cyber Attack

Credentials Leakage

Software Management



“ Java encryption implementation error made it trivial to forge credentials ”

"A catastrophic vulnerability in the implementation of certain encryption operations in Java JDK makes it easy for attackers to forge counterfeit credentials.The cryptographic weakness – which affects Java JDK versions 15 and later – was addressed by Oracle with an update released as part of its regular quarterly patch batch on Tuesday (April 19).
Both Oracle Java and OpenJDK need updating because of flaws that involve the implementation of widely-used ECDSA (Elliptic Curve Digital Signature Algorithm) signatures.The whole problem stemmed from a coding error rather than a problem with the underlying encryption technology. The flaws make it possible for an attacker to forge some types of SSL certificates and handshakes – opening the door to manipulator in the middle attacks.Signed JWTs, SAML assertions, WebAuthn authentication messages, and more can all be easily hacked because of the cryptographic blunder, security researcher Neil Madden warns.“If you are using ECDSA signatures for any of these security mechanisms, then an attacker can trivially and completely bypass them if your server is running any Java 15, 16, 17, or 18 version before the April 2022 Critical Patch Update (CPU).”

Critical infrastructure entities on red alert over ‘exceptionally rare and dangerous’ ICS malware

U.S. officials have warned that advanced persistent threat (APT) actors have developed tools capable of hijacking critical infrastructure devices.As part of a joint cybersecurity advisory (CSA) issued yesterday (April 13) by the NSA, FBI, Department of Energy, and Cybersecurity and Infrastructure Security Agency, cybercriminals can "scan for, compromise, and control affected devices once they have established initial access to the operational technology network," according to the CSA (CISA).For example, the APT actors can use the modules to conduct reconnaissance on the targeted devices, scan for them, upload malicious configuration/code to those devices, back up or restore their contents, and change their device parameters." One tool exploits a vulnerability (CVE-2020-15368) in the ASRock-signed motherboard driver, AsrDrv103.sys, to execute malicious code in the Windows kernel and provide a springboard for lateral movement and privilege escalation.

SQL injection protections in ImpressCMS could be bypassed to achieve RCE

Vulnerabilities in ImpressCMS could allow an unauthenticated attacker to bypass the software's SQL injection protections to achieve remote code execution (RCE),The vulnerabilities, an SQL injection flaw (CVE-2021-26599) and an access control bug, have now been patched in the latest version of the popular open source content management system (CMS).However, the same technique could be used modified to bypass other well-known security tools – ultimately meaning that features designed to protect against SQL injection exploits can be abused and turned against the host application."To successfully exploit this vulnerability you have to deal with Protector, which is a sort of built-in Web Application Firewall (WAF) in ImpressCMS, and this is where the idea to use this 'new' SQL Injection technique came in.There are some limitations, namely that ImpressCMS must be installed with the PDO database driver, which allows for stacked queries, but "in general, there are only two requirements for this SQL Injection technique to work – the application should be vulnerable to SQL injection, of course, [and] the application should support execution of multiple (stacked) SQL queries".


SQL Injection


Remote Code Execution


Content Management System

Ukraine invasion : WordPress-hosted university websites hacked in 'targeted attacks'

According to report atleast 30 Ukrainian university websites have been hacked in a targeted attack allegedly launched in support of Russia's invasion of the European country.."Massive attack" on Ukrainian educational institutions by threat actors known as the "Monday Group" has been witnessed by Wordfence researchers, who say the group has publicly supported Russia's recent actions.Since Russian troops invaded Ukraine on February 24, a group known as 'the Mx0nday' has targeted WordPress-hosted sites more than 100,000 times.

Maunder added : "An attacker was making a concerted effort to attack universities in Ukraine, and they started immediately after the Russian invasion started."An investigation into the attacks has identified four IP addresses behind the campaign, which are routed through a VPN service based in Sweden.The hacking group also appears to have links to Brazil, where Wordfence has claimed it is based.

However, the individuals behind the incident have not yet been publicly identified.


Cyber Attack


Wordpress-hosted sites


Government Sector

African banking sector targeted by malware-based phishing campaign

"Using phishing emails and HTML smuggling techniques, a cybercrime campaign aims to infect the African banking sector.Hackers posing as potential employers have tricked West African victims into downloading malicious files. It is possible to open HTML files that prompt users to download an ISO file that contains a malicious Visual Basic script. Attackers can sneak malicious files past email gateway security using a technique known as HTML smuggling. According to HP Wolf Security researchers who have been tracking the campaign, an employee of an unnamed West African bank received an email pretending to be from a recruiter at another African bank, with information about job opportunities.Attackers were utilising GuLoader, which is executed via PowerShell by code stored in the Registry and is otherwise only run in memory, according to HP Wolf Security researchers.Malware can only be found in the memory and registry of a computer, making it difficult to detect a chain of infection.Phishing emails, for example, aren't necessarily sophisticated, but the researcher noted that ""such attacks still lead to infections.""As a result of its difficulty in detection, the HTML smuggling technique stands out as a particularly dangerous one. "

Apple paid out $36,000 bug bounty for HTTP request smuggling flaws on core web apps – research

Following the discovery of three critical HTTP request smuggling vulnerabilities in three of Apple's primary web applications, one security researcher claims to have earned $36,000 in bug bounties.It is claimed that a security researcher made $36,000 in bug bounties after discovering critical HTTP request smuggling flaws in three of Apple's core web services.He said that they used the same technique to achieve queue poisoning on the domains, opening the door to data leakage and account takeover with no user interaction required.

The bug hunter is a 20-year-old hacker who goes by the online moniker "Stealthy."According to reports, the bugs were found on servers used by businesses, schools, and other non-profit organisations to claim and manage business listings on Apple's Maps app, including business.apple.com, school.apple.com, and mapsconnect.apple.com./static/docs is the smuggled path, according to the researcher, because of a redirect using the Host header value.As a result, "I could redirect live users to my server to ensure that request smuggling affects production users."

Trezor cryptocurrency wallets targeted with phishing attacks following Mailchimp compromise

"A phishing scam using Mailchimp email distribution services has been targeted at cryptocurrency hardware wallet owners.The Mailchimp email distribution service is being used to spread a crypto wallet phishing scam to its users. Mailchimp-powered newsletters sent by Trezor are being used to send out fake data breach notifications to their customers, the company announced on social media.Trezor says the phishing attacks, which are also aimed at other cryptocurrency firms, are the work of a " "insider," " according to the company. MailChimp has confirmed that their service has been hacked by an insider who is targeting crypto companies," " the tweet continues.The phishing domain has been taken offline.To find out how many email addresses have been compromised, we're conducting an investigation."

"Propagated" by an external actor, who had conducted a successful social engineering attack on Mailchimp employees, resulting in the compromise of employee credentials.This was a targeted attack on users in the cryptocurrency and finance industries, and all of them have been notified."" "We also conducted a robust investigation and engaged outside forensic counsel to understand what happened and the impact."Based on our investigation, we found that 319 Mailchimp accounts were viewed and audience data was exported from 102 of those accounts."Our findings show that this was a targeted incident focused on users in industries related to cryptocurrency and finance, all of whom have been notified."

T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code

"The LAPSUS$ mercenary gang was able to gain access to T-networks Mobile's in March, the telecom company confirmed on Friday.Within hours of the seven LAPSUS$ members being arrested in March, investigative journalist Brian Krebs published internal conversations belonging to the group's core members that revealed multiple intrusions by LAPSUS$.

"The bad actor" used stolen credentials to access internal systems, according to a T-Mobile statement,""several weeks ago.""Systems accessed by the intruder contained no sensitive information, and we have no evidence that the intruder accessed anything of value,"" the company said in a statement.The initial access credentials for the VPN were reportedly obtained from illegal websites like Russian Market in order to gain control of T-Mobile employee accounts, which would allow the threat actor to carry out SIM swapping attacks at their discretion.

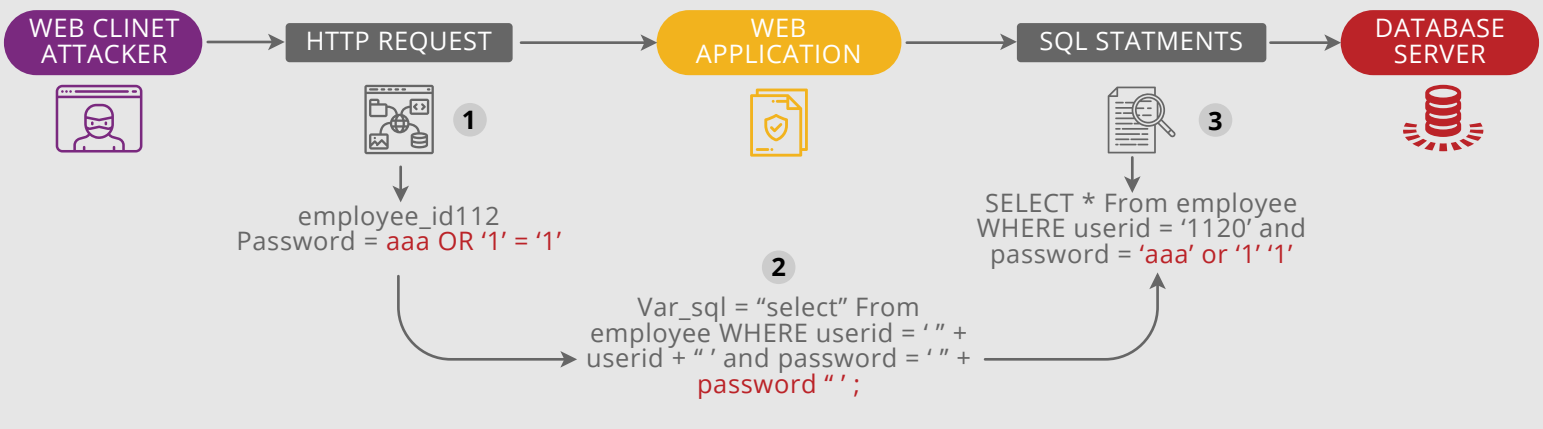
Additionally, the chats reveal that LAPSUS$ hacked T-Slack Mobile's and Bitbucket accounts, downloading more than 30,000 source code repositories while in control of an internal customer account management tool called Atlas. LAPSUS$ has gained notoriety for its breaches of Impresa, NVIDIA, Samsung, Vodafone, Ubisoft, Microsoft, Okta, and Globant in a short period of time since its appearance on the threat landscape.Two of the seven teenagers, a 16-year-old and a 17-year-old, were charged earlier this month by the City of London Police for their alleged ties to the LAPSUS$ data extortion gang. "

SIM Swapping Attack | Security Breach | Telecom Company

Hive hackers are exploiting Microsoft Exchange Servers in ransomware spree

Attackers from the Hive group are using ransomware to infect Microsoft Exchange servers.Cyber criminals can use the Hive ransomware strain in attacks using the Ransomware-as-a-Service (RaaS) model.The criminals behind the ransomware use a leak site with a.onion address to publish the identities of those who have fallen victim to their attacks.Double-extortion is also used by malware operators, who steal sensitive corporate data from a victim organisation before encrypting the disc.They will put their name everywhere, and they'll also put a timer on it, if a victim refuses to pay for a decryption key.Increased pressure means more extortion opportunities for the assailants. In new research published on April 19 by the Varonis Forensics Team, a recent ransomware incident has allowed the company to examine the group's tactics and procedures in depth.An unnamed customer's networks were infiltrated, and the attack was complete in 72 hours. Once exploited, a webshell backdoor is executed to maintain persistence and grant the attack group a path into the server to deploy Powershell code with SYSTEM-level privileges. Hive launches a Cobalt Strike beacon in the next step and creates a new administrator user account. Mimikatz comes into play, and the domain Administrator NTLM hash is stolen. The Go-based Hive ransomware payload, buried in a file called "windows.exe," will encrypt files, delete shadow copies, disable security solutions, and clear Windows event logs. The malware will also try to disable the Windows Security Accounts Manager (SAM) to stop alerts from being sent to SIEM.

Hive Ransomeware Attack | Microsoft Exchange Servers Compromised | Microsoft Company



Access control vulnerability in Easy! Appointments platform exposed sensitive personal data

A security researcher has discovered a flaw in the open source scheduling platform Easy!Appointments that allowed unauthenticated attackers to gain access to personal information (PII).Only three parameters were passed: startDate, endDate, and csrfToken, and when Carlucci tried to remove all cookies from his request, he received a 403 error.In order to access the unprotected API and download data about scheduled appointments, malicious hackers need only visit the public bookings form to obtain a CSRF token.Carlucci explained that there are a variety of attack options.This includes the user's phone number, physical address, and city — all juicy information that can be used for identity theft and 'password recovery attacks' on other websites, according to the attacker.In addition, the attacker is privy to personal information like the identity of the person the user is meeting and the reason for their visit.“

Last but not least, the HTTP response included the ‘reference’ (hash) of the booking, which can be used by the attacker to cancel the booking on behalf of the user (on a different endpoint : index.php/appointments/index/{hash}). An attacker can automate this to loop through bookings and wipe out the whole booking database.”Easy!Appointments, which is also available as a WordPress plugin, has been downloaded more than 100,000 times. The appointment management system is based on CodeIgniter, which Carlucci says is riskier than alternative PHP frameworks such as Laravel because developers have to code their own authentication and other basic features.

Sensitive Data Exposure

Data Exposure

Information Technology

MALWARE IS **EVERYWHERE**

HERE IS THE SCOPE OF THE THREAT AND WAYS TO PROTECT YOURSELF

ON THE RISE UP
40.9% IN 2011
403 MILLION VS 2010
286 MILLION

ATTACK FLOW

Common Paths for a Phishing Email Attack

Malicious Email Arrives

Email is Blocked by Spam Filter

User Opens Malicious Email

User Clicks on Embedded Link

User Downloads Attachements

User Replies to the Message

Webpage Opens

Malware Infection

User Sends Sensitive Info

Page Requests User Credentials (Phishing)

Webpage Forces Malware Onto the User's System (Driven- by Download)

Malware Infection

User Sends Sensitive Info

CRISIS AVERTED

Corporate Offices

INDIA

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

UK

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

USA

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

BAHRAIN

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

contact@briskinfose.com | www.briskinfosec.com