BRISK INFOSEC

CYBER TRUST & ASSURANCE

THREATSPLOIT

ADVERSARY REPORT

JAN-2022

EDITION 42

Introduction

Welcome to the Threatsploit Report of January 2022 covering some of the ground breaking cybersecurity events, incidents and exploits that occurred this month. This month, the cybersecurity sector witnessed a steep rise in ransomware, data breach and sovereign attacks. Besides, many other attack types have seen a spike during the first month of the year.

The primary reason is and has always been the same….

> **"Employees and stakeholders have limited or no perception of massive cyber threats or consequences. It is our job to educate them."**

Log4j and it's Vulnerabilitie are continued to be discovered across the spectrum leading to system compromise around the globe. Personal detail compromise of a huge scale was highlighted when an Attorney General flagged of a cyber-attack on small businesses. Even non-governmental organisations are facing loss of sensitive data, i.e., Red cross got hacked for high profile user database. System compromise by ransomware groups is on the rise, possibly leading to closure of businesses across the geography. An active spying attack has been uncovered on cloud services like Google Drive which will lead to data compromises for sure.

Another example of data compromise is for Wordpress users. They may have the bad news as hackers have planted backdoors in dozen WordPress plugin. Technology has been the most compromised domain followed by Service sector this month. Let us walk you through some of the important security incidents that happened this month which may affect you or your partners, colleagues, family & friends.

Contents

SSRF vulnerability in VMWare authentication software could allow access to user data

A server-side request forgery (SSRF) vulnerability in versions of VMWare authentication software could allow an attacker to obtain administrative JSON Web Tokens (JWT). The SSRF bug was found in VMware Workspace ONE Access (previously known as Identity Manager), which provides multi-factor authentication, conditional access and single sign-on to SaaS, web, and native mobile apps.This vulnerability (tracked as CVE-2021-22056), which was assigned a 'moderate' severity score of 5.5, could enable a malicious actor with network access to make HTTP requests to arbitrary origins and read the full response.JWTs are URL safe strings that are used to identify a user. They contain JSON-encoded data, making them convenient for embedding information. They are typically used as session identifiers for web applications, mobile applications, and API services. They also contain user data directly, unlike traditional session identifiers which simply point to user data on the server-side.If a user's JWTs are stolen or compromised, an attacker can potentially gain full access to the user's account.VMWare has patched both security issues in its latest version of the enterprise software."

Attack Type

Server Side Request Forgery

Cause of Issue

Server Misconfiguration

Type of Loss

System Compromise

Domain

Technology Sector

"Researchers discover Log4j-like flaw in H2 database console"

A vulnerability with the same root cause as the notorious Log4j flaw has been patched in the console of the hugely popular Java SQL database, H2 Database Engine.It is known the recent 'Log4Shell' exploits, unauthenticated attackers can achieve remote code execution (RCE) because the console accepts arbitrary Java Naming and Directory Interface (JNDI) lookup URLs.The flaw (CVE-2021-42392) "allows loading of custom classes from remote servers through JNDI", the widespread usage of JNDI suggested "there are bound to be more packages that are affected by the same root cause as Log4Shell",versions span 1.1.100 to 2.0.204 inclusive. Similar to the Log4j fix, the patch limits JNDI URLs to using the local Java protocol only, thus blocking remote LDAP/RMI queries.With almost 7,000 artifact dependencies, H2 is one of the most popular open source Maven packages.Regardless of patching "-webAllowOthers is a dangerous setting that should be avoided", warns the H2 advisory.But if the H2 console Servlet is deployed on a web server, users can add a security constraint that will allow only specific users access to the console page.

Attack Type

Zeroday Vulnerability

Cause of Issue

Lack of Patch Management

Type of Loss

Compromise Database Console

Domain

Technology Sector

New York Attorney General flags 1.1 million online accounts compromised by credential stuffing attacks

More than 1.1 million online customer accounts at 17 "well-known" businesses were compromised via credential stuffing attacks, Credential stuffing attacks use specialized software to 'stuff', at high velocity, thousands or millions of username-password combinations gleaned from data breach dumps into sign-in pages.Also called a 'password reuse' attack, the mostly automated technique is both comparatively simple and, since around two in three internet users (PDF) use the same login details across multiple online accounts, highly effective. After hijacking online accounts, attackers can then steal victims' identities and potentially bypass more stringent authentication processes implemented by banks and other custodians of high value assets. Affected organizations were then helped to determine how existing safeguards had been circumvented and given recommendations for preventing recurrences."Nearly all" of the 17 affected companies have since implemented, or devised plans to implement, additional safeguards.also urged e-commerce platforms to make purchases contingent on the re-authentication of credit card details, having encountered many instances where the absence of such a mechanism had resulted in fraudulent purchases. "Businesses have the responsibility to take appropriate action to protect their customers' online accounts and this guide lays out critical safeguards companies can use in the fight against credential stuffing."

Attack Type

Credential Stuffing

Cause of Issue

Lack of Authentication

Type of Loss

Account Compromise

Domain

Technology Sector

Prosecutors file additional charges against former Uber security chief over 2016 data breach 'cover up'

Unauthorized attackers obtained access to the personal details of 57 million Uber users and the driving license information of around 600,000 drivers in October 2016.The sensitive data was downloaded from a third-party cloud provider's storage bucket and accessed by abusing credentials an Uber engineer had inadvertently posted on a code-sharing website.According to prosecutors, Sullivan made a deal with criminal hackers to keep quiet about the breach and delete the purloined data they held in exchange for a payment of $100,000 in bitcoin to individuals who refused to offer their true name.The two individuals involved were subsequently identified, arrested, charged, and convicted over attacks on LinkedIn and Uber.According to prosecutors, the non-disclosure agreements falsely stated that the hackers had neither taken nor stored Uber's data. Ube charged with three counts of wire fraud, obstruction of justice, and misprision of a felony. The wire fraud charges carry a higher maximum period of imprisonment than the other offences. So Uber – which was already under investigation in relation to an earlier 2014 breach at the time of the second, similar data leak – failed to disclose the 2016 breach to consumers or regulators from the US Federal Trade Commission until November 2017, circumstances that ultimately led to censure and a $148 million data breach settlement with the FTC.

Attack Type

Data Breach

Cause of Issue

Lack of Authentication

Type of Loss

Personal details compromise

Domain

Technology Sector

DDoS attacks increasing year on year as cybercriminals demand extortionate payouts

Distributed denial-of-service (DDoS) attacks are increasingly being accompanied by extortionate demands against their victims, according to annual survey from Cloudflare.Ransom-motivated DDoS attacks increased 29% year-on-year and 175% between Q3 2021 and Q4 2021, according to the study on cyber-attack trends.The manufacturing industry was the most attacked in Q4 of 2021 by application-layer DDoS attacks, recording an alarming seven-fold (641%) increase in the number of attacks. The business services and gaming/gambling industries were the second and third most targeted industries by application-layer DDoS attacks.A new botnet called the Meris botnet emerged in mid-2021 and became the source of multiple high-volume application-layer DDoS attacks, Cloudflare said.Application-layer DDoS attacks typically attempt to disrupt the operation of a targeted organization's web server by bombarding it with fake requests, thereby making it unable to process genuine requests efficiently or (worse yet) crash.Cloudflare recorded a persistent ransom-motivated network-based DDoS campaign against VoIP providers around the world.SYN floods and UDP (User Datagram Protocol) floods were the most frequent attack vectors, but the period also witnessed a big increase in SMTP-based network-layer DDoS attacks.

Attack Type

DDOS Attack

Cause of Issue

Lack of DDOS protection

Type of Loss

System Compromise
and reputation loss

Domain

Manufacturing Industries,
business services and gaming/gambling

Red Cross suffers cyber-attack – data of 515,000 'highly vulnerable' people exposed

The International Committee of the Red Cross (ICRC) has revealed a data breach exposing information belonging to over half a million "highly vulnerable" people.On January 19, the ICRC, the overseer of Red Cross operations, said the "sophisticated" attack was launched against an external company in Switzerland contracted by the Red Cross to store information. The Red Cross is a humanitarian outfit that works with those impacted by conflict and war internationally. In total, over 515,000 individuals are believed to have been impacted with many classed as "highly vulnerable" including those separated from their families due to conflict and disasters, others classified as missing people, and individuals being held in detention centers.

Attack Type	Cause of Issue	Type of Loss	Domain
Data Breach	Lack of Patch Management	Loss of Sensitive Data	Technology Sector

Log4J: Microsoft discovers attackers targeting undisclosed SolarWinds vulnerability

Microsoft researchers have discovered a previously undisclosed vulnerability in the SolarWinds Serv-U software while monitoring threats related to Log4J vulnerabilities.The issue, tracked as as CVE-2021-35247, and said it is an "input validation vulnerability that could allow attackers to build a query given some input and send that query over the network without sanitation."In their advisory, SolarWinds said the Serv-U web login screen to LDAP authentication was allowing characters that were not sufficiently sanitized.Microsoft urged customers to apply the security updates explained in the SolarWinds advisory and said customers can use their tools to identify and remediate devices that have the vulnerability. Microsoft Defender Antivirus and Microsoft Defender for Endpoint also detect behavior related to the activity. Netenrich's John Bambenek added that Microsoft's warning and SolarWinds' quick response time represented a positive example of how vulnerabilities need to be dealt with.

Attack Type	Cause of Issue	Type of Loss	Domain
Zero Day Attack	Lack of Patch Management	System Compromise	Technology Sector

European Commission launches new open source software bug bounty program

The European Commission (EC) has launched a bug bounty program for open source projects that underpin its public services.Bug bounty hunters will be offered up to €5,000 ($5,600) for finding security vulnerabilities in open source software used across the European Union (EU), including LibreOffice, LEOS, Mastodon, Odoo, and CryptPad.The program, led by European bug bounty platform Intigriti, will also offer a 20% bonus if a code fix for the bugs it is provided by researchers.In a statement released on January 19, the EC said it is looking for reports of security vulnerabilities such as leaks of personal data, horizontal/vertical privilege escalation, and SQL injection. The highest reward will be paid out for "exceptional vulnerabilities".This latest program comes in the wake of the EU FOSSA program, which paid out more than $220,000 in its 18 months in operation, and was heralded a "remarkable success".

Attack Type	Cause of Issue	Type of Loss	Domain
NA	NA	NA	Technology Sector

Open debug mode in Cisco mobile networking software created critical security hole

Cisco has patched a pair of vulnerabilities in its telco-focused Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS software, including a critical flaw that presented a remote code execution risk.RCM is a management technology that handles the failover between different virtualized systems involved in provisioning, billing, and other telecom services.Multiple systems are run in parallel in order to offer reliability to mobile network systems. The CVE-2022-20649 vulnerability stems from a failure to disable the debug mode that's there to help out during the product development process."This vulnerability exists because the debug mode is incorrectly enabled for specific services," Cisco explains. "An attacker could exploit this vulnerability by connecting to the device and navigating to the service with debug mode enabled.The vulnerability only lends itself to exploitation by an authenticated attacker and would require reconnaissance and maximum severity flaw earns a CVSS rating of 9.0.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Patch Management

Type of Loss

System Compromise

Domain

Technology Sector

Ransomware groups increasingly using data leak threats to pile pressure on victims

Data on 2,371 companies were released on ransomware data leak sites over the second half of 2020 and first half of 2021 (a 935% increase).More recently, ransomware peddlers have threatened to leak sensitive information if ransom demands are not met – a so-called 'double extortion' threat that relies on data leak sites. onti became the most aggressive ransomware strain, which accounted for public information about 361 victims being available through data leak sites. Companies whose data was posted on data leak domains by ransomware operators in 2021 were based in the US (968 companies), Canada (110), and France (103), while most organizations affected belonged to the manufacturing (9.6%), real estate (9.5%), and transportation industries (8.2%).Victims can still find their data on data leak sites even if the ransom is paid, according to Group-IB, which estimates that a little less than a third of ransomware demands result in payments. "The popularity of initial access brokers (IABs) has risen as the barrier to entry for cybercriminals has lowered. Using IABs allows ransomware operators and other cybercriminals to expedite their time on task."By using IABs, cybercriminals can complete the reconnaissance and weaponization stages of the cyber kill chain at a far faster rate, allowing them to gain access to targeted networks for subsequent exploitation quickly,".As partnerships between ransomware operators and IABs under the RaaS model have grown from strength to strength other long-running scams such as carding (the trade in stolen credit and debit cards) have gone into something of a decline. The carding market dropped by 26%, from $1.9 billion to $1.4 billion when compared to the previous period. "The decrease can be explained by the lower number of dumps (data stored on the magnetic stripe on bank cards) offered for sale: the number of offers shrank by 17%, from 70 million records to 58 million, due to the infamous card shop Joker's Stash shutting down.," according to Group-IB. The average price for text data climbed from $12.78 to $15.20, according to the threat intel firm.

Attack Type

Ransomeware Attack

Cause of Issue

Lack of Malware Protection tools

Type of Loss

System Compromise

Domain

Technology Sector

Sixth member of notorious SIM-swapping cybercrime gang sentenced

The final member of an international hacking group known as 'The Community' has been sentenced for his role in a multimillion-dollar SIM-swapping campaign.Garrett Endicott, 22, of Warrensburg, Missouri, has become the sixth member of the crime syndicate to have been jailed for the campaign, which saw millions of dollars' worth of cryptocurrency stolen from victims. SIM hijacking was accomplished by a member of The Community contacting a mobile phone provider's customer service – posing as the victim – and requesting that the victim's phone number be swapped to a SIM card (and thus a mobile device) controlled by The Community."Once the perpetrators had control of a victim's phone number, that number was leveraged as a gateway to gain control of online accounts such as a victim's email, cloud storage, and high-value cryptocurrency accounts.They could then reset passwords on online accounts and/or request two-factor authentication (2FA) codes that allowed them to bypass securiy measures."Individual victims lost cryptocurrency valued, at the time of theft, ranging from under $2,000 to over $5 million."

Attack Type

SIM Hijacking

Cause of Issue

Lack of Patch Management

Type of Loss

Control on Cryptocurrency Accounts

Domain

Technology Sector

SSRF vulnerability patched in Jamf Pro mobile security platform

A vulnerability in Jamf Pro, a popular mobile device management (MDM) platform for Apple devices, allowed attackers to stage server-side request forgery (SSRF) attacks on the application's servers, security researchers at Assetnote have found.The Assetnote researchers came across an on-premise installation of Jamf Pro while examining the attack surface of a client. Since Jamf Pro is usually exposed to the internet, the researchers became interested in potential vulnerabilities it could have.They initially looked for pre-authentication vulnerabilities that would be accessible to attackers who did not have valid credentials in the system. Having found none, they sought post-authentication bugs, and during their probe, they found an HTTP sink function that made requests to external resources. This became their window to SSRF attacks."From my experience, in most enterprise applications, there is a need to make HTTP requests to external sources. This pattern is worth reviewing because it can often lead to SSRF," "Given that it is possible to perform brute-force attacks against users of Jamf Pro, I see the impact to be of high nature," he said. "An attacker can attempt to brute-force valid credentials to the Jamf Pro instance and then leverage this bug to access the internal network"Since this bug is post-authentication, I see it being used in an exploitation chain once access to Jamf is achieved."Jamf also has a cloud-hosted version, in which the SSRF could have a critical impact. Jamf employed a web application firewall (WAF) rule to block exploitation of the bug on cloud instances until a patch was later applied.

Attack Type

Server Side Request Forgery

Cause of Issue

Lack of Secure Data Validation

Type of Loss

Data Compromise

Domain

Technology Sector

Drive-by RCE in Windows 10 'can be executed with a single click'

A drive-by remote code execution (RCE) vulnerability in Windows 10 that can be triggered simply by clicking a malicious URL could allow attackers full access to a victim's files and data.The security flaw, an argument injection in the Windows 10/11 default handler for ms-officecmd: URIs, is present in Windows 10 via Internet Explorer 11/Edge Legacy browsers and Microsoft Teams.Windows internally uses ms-officecmd: URIs to start various Microsoft programs.The attack starts with a victim either visiting a malicious website in IE11/Edge Legacy or clicking a malicious link in another browser or desktop application"The link is then forwarded to LocalBridge.exe, which in turn runs various Office executables with a segment of the link as argument."We found that it's possible to inject additional arguments, which allowed us to achieve code execution by triggering the launch of Microsoft Teams with an additional --gpu-launcher argument that is then interpreted by Electron.The exploit works in several steps. The malicious HTML file contains an invisible iframe, placed on top of a button in the page to carry out a clickjacking attack.The iframe's source is set to the discovery page of the debugging portal for the headless browser. When the user clicks on it, the iframe invisibly navigates to the Chrome DevTools portal and passes on the WebSocket token in the URL. Next, a second iframe is created in the exploit page, which uses a cross-site scripting (XSS) vector in the Chrome DevTools portal to set the href value of the page's parent frame and the clickjacking frame to the same origin. This setting allows the page to circumvent cross-origin security policies."Exploitation through other browsers requires the victim to accept an inconspicuous confirmation dialog.Alternatively, a malicious URI could also be delivered via a desktop application performing unsafe URL handling. However, a precondition for this particular exploit is to have Microsoft Teams installed but not running.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Patch Management

Type of Loss

System Compromise

Domain

Technology Sector

Severe Chrome bug allowed RCE on devices running remote headless interface

A fixed bug in Chrome allowed attackers to read and write local files and install malicious scripts on devices running the browser's headless interface, researchers at Contrast Security have discovered.he headless browser can be controlled programmatically and debug According to a discussion thread on the Chromium bug portal, an attacker can exploit the bug if a machine is running headless Chrome in debugging mode.Debugging mode enables the DevTools protocol, which allows developers to remotely connect to a running instant of Chrome and perform tasks such as inspecting, profiling, and instrumenting. Since 2017, Chrome has included a headless mode that allows developers to run an instance of the browser without launching the user interface.The WebSocket token is then passed to the exploit page, which uses it to connect to Chrome's remote debugging protocol. From there, the exploit page can read local files and write arbitrary files to the target device.In the POC video, the attacker stores a malicious Launch Agent file in the target device. Launch Agent is a script that runs automatically when the user logs into the operating system.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Patch Management

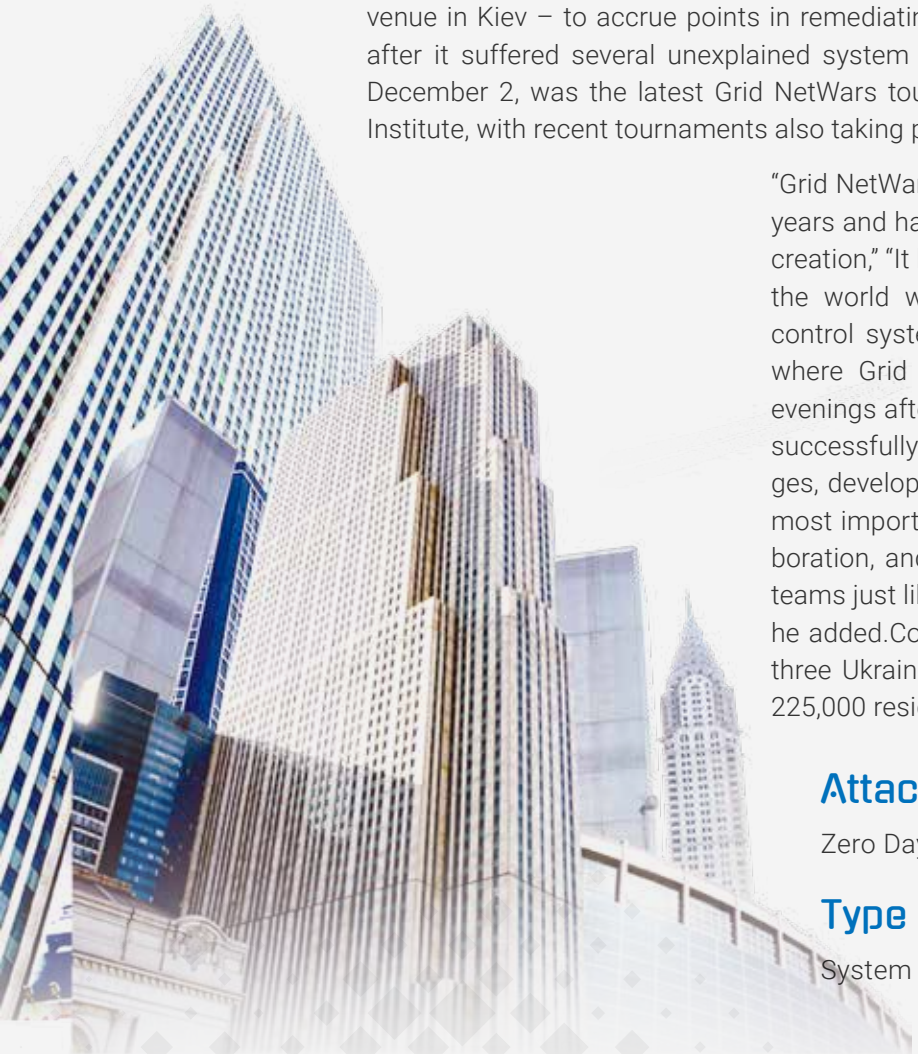
Type of Loss

System Compromise

Domain

Technology Sector

Ukraine hosts large-scale simulation of cyber-attack against energy grid



Cybersecurity professionals from across Ukraine have tackled a large-scale cyber-attack simulation with echoes of the hugely damaging real-world assault against the country's power grid in 2015.Comprising 250 participants, 49 teams competed – either virtually or in-person at a venue in Kiev – to accrue points in remediating an attack against a fictional energy provider after it suffered several unexplained system failures.The competition, which took place on December 2, was the latest Grid NetWars tournament from US infosec training body SANS Institute, with recent tournaments also taking place in Singapore, India, Japan, and Australia.

"Grid NetWars is a product that has existed for a number of years and has been used in country-level exercises since its creation," "It has also been leveraged by practitioners around the world who attend critical infrastructure or industrial control system-specific events like the SANS ICS Summit where Grid NetWars competitions are conducted in the evenings after courses."The latest, Ukraine-based event had successfully enabled "participants to face real world challenges, develop skillsets, gain exposure to technical tools, and most importantly 'practice the way they play' through collaboration, and provided the opportunity to work together in teams just like they would in a real world incident response", he added.Conway helped to investigate the 2015 attack on three Ukrainian power distribution centers that left around 225,000 residents without power for up to six hours.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Patch Management

Type of Loss

System Compromise

Domain

Service Industry

Chain of vulnerabilities led to RCE on Cisco Prime servers

A series of vulnerabilities in the web interface of Cisco Prime opened servers to remote code execution (RCE) attacks, Cisco Prime is a network management service that provides tools for provisioning, monitoring, optimizing, and troubleshooting wired and wireless devices.-The main culprit in the Cisco Prime vulnerability is a cross-site scripting (XSS) vector that is exploited through SNMP, the protocol used to discover devices in a network.Finstad had already found similar vulnerabilities in at least two other web-based network management tools, which led him and Donkers to wonder if other networking tools had similar vulnerabilities.Cisco Prime sends SNMP requests to gather information about devices present in the network. Among the information network devices provide is the address for an image file.The researchers placed a Linux-based device on the network and in its SNMP configuration file, they set the address of the image to a JavaScript snippet that loaded a malicious script hosted on a server they controlled.When the server's admin navigated to Prime's device discovery page, the malicious script was loaded and run in the browser, resulting in an XSS attack.

The first vulnerability was an unprotected session ID cookie stored in LocalStorage, which enabled them to hijack the active administrator session.Using the stolen administrator token, they next tried to submit commands to Prime's management interface. Like most web applications, Prime's management interface prevents such commands through anti-CSRF (cross-site request forgery) tokens. But by probing Prime's development tools, Finstad and Donkers were able to discover a function that generated the tokens, making it possible to bypass the CSRF protections.With the improved access, the researchers were able to create an additional administrator account for themselves, giving them persistence in the server. They were also able to clean their tracks by purging the logs and removing the device that gave them the initial foothold into the server."This gave control over every switch in the network. VLAN boundaries could be easy to traverse, change routing on devices, change network addresses and other network admin capabilities.

Attack Type

Cross Site Scripting

Cause of Issue

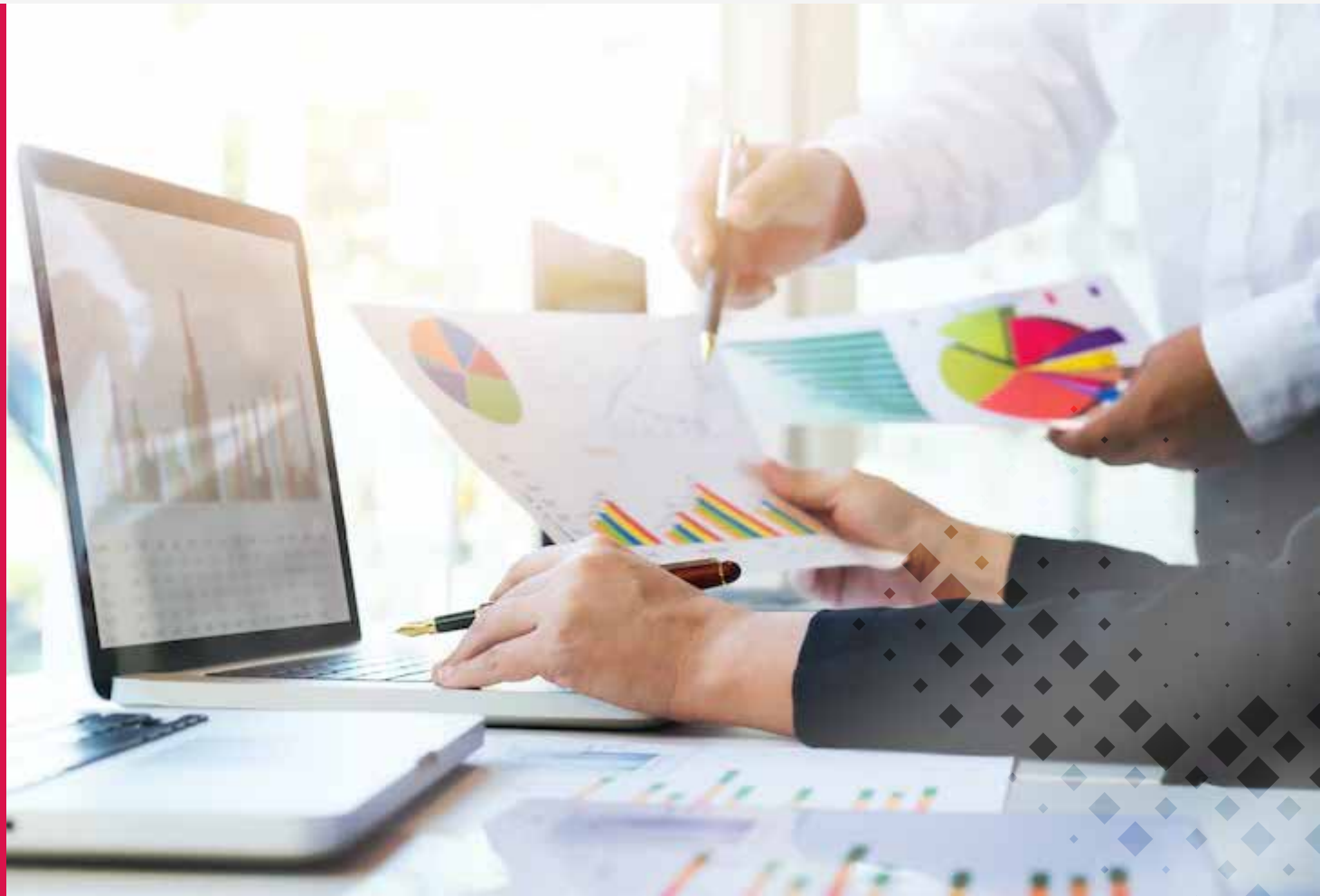
Lack of Secure Data Validation

Type of Loss

Client Data Loss

Domain

Technology



VMware Horizon under attack as China-based ransomware group targets Log4j vulnerability

A China-based ransomware operator has for the past week been actively exploiting the Log4j vulnerability in VMware Horizon, the desktop and app virtualization platform, Microsoft has warned."Based on our analysis, the attackers are using command and control (CnC) servers that spoof legitimate domains," Microsoft has previously documented ransomware attacks on Minecraft servers via Log4Shell and access brokers compromising networks before selling access to ransomware-as-a-service affiliates."We have observed many existing attackers adding exploits of these vulnerabilities in their existing malware kits and tactics, from coin miners to hands-on-keyboard attacks," said Microsoft. "Organizations may not realize their environments may already be compromised.Microsoft recommends that customers review devices where vulnerable installations are discovered, and "assume broad availability of exploit code and scanning capabilities to be a real and present danger to their environments."Due to the many software and services that are impacted and given the pace of updates, this is expected to have a long tail for remediation, requiring ongoing, sustainable vigilance."

Attack Type

Ransomeware Attack

Cause of Issue

Lack of Malware Protection tools

Type of Loss

Loss of Sensitive Data

Domain

Technology Sector

F5 fixes high-risk NGINX Controller vulnerability in January patch rollout

Networking and application delivery technology vendor F5 has fixed a pair of high impact, web security-related vulnerabilities.First up for triage was a code injection risk involving F5's NGINX Controller API Management technology, which allows DevOps teams to "define, publish, secure, monitor, and analyze APIs".F5 explains: "An authenticated attacker with access to the 'user' or 'admin' role can use undisclosed API endpoints on NGINX Controller API Management to inject JavaScript code that is executed on managed NGINX data plane instances."The vulnerability – tracked as CVE-2022-23008 – earns a CVSS score of 8.7, marking it out as the highest severity flaw in F5's latest patch batch.

DOM-based cross-site scripting (XSS) vulnerability involving F5's BIG-IP load balancer. The CVE-2022-23013 vulnerability in BIG-IP configuration utility could allow an attacker to execute JavaScript in the context of the current logged-in user.The flaw earns a CVSS score of 7.5, marking it out as another high severity threat. The issue was also discovered internally by engineers from F5.F5's latest quarterly patch batch addresses a total of 15 'high' severity vulnerabilities, nine 'medium' risk flaws, and one 'low' severity bug. Many of the flaws involve memory handling or system crashing (denial of service) risks.A full breakdown on the content of the patches, released last Wednesday (January 19), together with suggested remediation advice, can be found in F5's related security advisory.

Attack Type

Code Injection,
Cross Site Scripting

Cause of Issue

Lack of Patch Management

Type of Loss

System Compromise

Domain

Service Industry

High-Severity Rust Programming Bug Could Lead to File, Directory Deletion

The maintainers of the Rust programming language have released a security update for a high-severity vulnerability that could be abused by a malicious party to purge files and directories from a vulnerable system in an unauthorized manner."An attacker could use this security issue to trick a privileged program into deleting files and directories the attacker couldn't otherwise access or delete," the Rust Security Response working group (WG) said in an advisory. ust 1.0.0 through Rust 1.58.0 is affected by this vulnerability. The flaw, which is tracked as CVE-2022-21658 (CVSS score: 7.3), has been credited to security researcher Hans Kratz, with the team pushing out a fix in Rust version 1.58.1 shipped last week.Specifically, the issue stems from an improperly implemented check to prevent recursive deletion of symbolic links (aka symlinks) in a standard library function named "std::fs::remove_dir_all." This results in a race condition, which, in turn, could be reliably exploited by an adversary by abusing their access to a privileged program to delete sensitive directories.the standard library first checked whether the thing it was about to delete was a symlink, and otherwise it would proceed to recursively delete the directory,". "This exposed a race condition: an attacker could create a directory and replace it with a symlink between the check and the actual deletion."Rust, while not a widely-used programming language, has witnessed a surge in adoption in recent years for its memory-related safety guarantees.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Secure Data Validation

Type of Loss

Loss of server side data

Domain

Technology Sector

Molerats Hackers Hiding New Espionage Attacks Behind Public Cloud Infrastructure

An active espionage campaign has been attributed to the threat actor known as Molerats that abuses legitimate cloud services like Google Drive and Dropbox to host malware payloads and for command-and-control and the exfiltration of data from targets across the Middle East.1, according to cloud-based information security company Zscaler, continuing previous efforts by the hacking group to conduct reconnaissance on the target hosts and plunder sensitive information.

Molerats, also tracked as TA402, Gaza Hackers Team, and Extreme Jackal, is an advanced persistent threat (APT) group that's largely focused on entities operating in the Middle East. Attack activity associated with the actor has leveraged geopolitical and military themes to entice users to open Microsoft Office attachments and click on malicious links.The implant, which uses specific command codes to commandeer the compromised machine, supports capabilities to take snapshots, list and upload files in relevant directories, and run arbitrary commands. Investigating the attack infrastructure, the researchers said they found at least five Dropbox accounts used for this purpose.

Attack Type

Zero Day Attack

Cause of Issue

Lack of Patch Management

Type of Loss

Data Compromise

Domain

Technology Sector

Hackers Planted Secret Backdoor in Dozens of WordPress Plugins and Themes

In yet another instance of software supply chain attack, dozens of WordPress themes and plugins hosted on a developer's website were backdoored with malicious code in the first half of September 2021 with the goal of infecting further sites.The backdoor gave the attackers full administrative control over websites that used 40 themes and 53 plugins belonging to AccessPress Themes, a Nepal-based company that boasts of no fewer than 360,000 active website installations."The infected extensions contained a dropper for a web shell that gives the attackers full access to the infected sites," security researchers from JetPack, a WordPress plugin suite developer, said in a report published this week. "The same extensions were fine if downloaded or installed directly from the WordPress[.]org directory."The vulnerability has been assigned the identifier CVE-2021-24867. Website security platform Sucuri, in a separate analysis, said some of the infected websites found utilizing this backdoor had spam payloads dating back almost three years, implying that the actors behind the operation were selling access to the sites to operators of other spam campaigns.Site owners who have installed the plugins directly from AccessPress Themes' website are advised to upgrade immediately to a safe version, or replace it with the latest version from WordPress[.]org. Site owners who have installed the plugins directly from AccessPress Themes' website are advised to upgrade immediately to a safe version, or replace it with the latest version from WordPress[.]org. "This flaw made it possible for an unauthenticated attacker to inject malicious JavaScript that would execute whenever a site administrator accessed the template editor," . "This vulnerability would also allow them to modify the email template to contain arbitrary data that could be used to perform a phishing attack against anyone who received emails from the compromised site."

Attack Type	Cause of Issue	Type of Loss	Domain
Malware Attack	Lack of Malware Protection tools	Data Compromise	Technology Sector

Critical Bugs in Control Web Panel Expose Linux Servers to RCE Attacks

Researchers have disclosed details of two critical security vulnerabilities in Control Web Panel that could be abused as part of an exploit chain to achieve pre-authenticated remote code execution on affected servers.Tracked as CVE-2021-45467, the issue concerns a case of a file inclusion vulnerability, which occurs when a web application is tricked into exposing or running arbitrary files on the web server.Specifically, the issue arises when two of the unauthenticated PHP pages used in the application — "/user/login.php" and "/user/index.php" — fail to adequately validate a path to a script file, according to Octagon Networks' Paulos Yibelo, who discovered and reported the flaws.This means that in order to exploit the vulnerability, all an attacker has to do is to alter the include statement, which is used to include the content of one PHP file into another PHP file, to inject malicious code from a remote resource and achieve code execution.Interestingly, while the application had protections in place to flag efforts to switch to a parent directory (denoted by "..") as a "hacking attempt" it did nothing to prevent the PHP interpreter from accepting a specially crafted string such as ".$00." and effectively achieving a full bypass.

Attack Type	Cause of Issue	Type of Loss	Domain
Zero Day Attack	Lack of Patch Management	System Compromise	Technology Sector

Google Details Two Zero-Day Bugs Reported in Zoom Clients and MMR Servers

An exploration of zero-click attack surface for the popular video conferencing solution Zoom has yielded two previously undisclosed security vulnerabilities that could have been exploited to crash the service, execute malicious code, and even leak arbitrary areas of its memory.Natalie Silvanovich of Google Project Zero, who discovered and reported the two flaws last year, said the issues impacted both Zoom clients and Multimedia Router (MMR) servers, which transmit audio and video content between clients in on-premise deployments.The goal of a zero-click attack is to stealthily gain control over the victim's device without requiring any kind of interaction from the user, such as clicking on a link. The two flaws identified by Project Zero are as follows

CVE-2021-34423 (CVSS score: 9.8) – A buffer overflow vulnerability that can be leveraged to crash the service or application, or execute arbitrary code.

CVE-2021-34424 (CVSS score: 7.5) – A process memory exposure flaw that could be used to potentially gain insight into arbitrary areas of the product's memory.

By analyzing the RTP (Real-time Transport Protocol) traffic used to deliver audio and video over IP networks, Silvanovich found that it's possible to manipulate the contents of a buffer that supports reading different data types by sending a malformed chat message, causing the client and the MMR server to crash.

Attack Type

Zero Day Attack, Buffer Overflow Vulnerability

Cause of Issue

Lack of Patch Management

Type of Loss

System Compromise

Domain

Technology Sector

New BHUNT Password Stealer Malware Targeting Cryptocurrency Wallets

A new evasive crypto wallet stealer named BHUNT has been spotted in the wild with the goal of financial gain, adding to a list of digital currency stealing malware such as CryptBot, Redline Stealer, and WeSteal."BHUNT is a modular stealer written in .NET, capable of exfiltrating wallet (Exodus, Electrum, Atomic, Jaxx, Ethereum, Bitcoin, Litecoin wallets) contents, passwords stored in the browser, and passphrases captured from the clipboard," Bitdefender researchers said in a technical report on Wednesday.The campaign, distributed globally across Australia, Egypt, Germany, India, Indonesia, Japan, Malaysia, Norway, Singapore, South Africa, Spain, and the U.S., is suspected to be delivered to compromised systems via cracked software installers. The modus operandi of using cracks as an infection source for initial access mirrors similar cybercrime campaigns that have leveraged tools such as KMSPico as a conduit for deploying malware. "Most infected users also had some form of crack for Windows (KMS) on their systems," .NET malware that incorporates different modules to facilitate its malicious activities, the results of which are exfiltrated to a remote server — blackjack – steal wallet file contents,chaos-crew – download additional payloads etc. The information theft could also have a privacy impact in that the passwords and account tokens stolen from the browser cache could be abused to commit fraud and to gain other financial benefits."The most effective way to defend against this threat is to avoid installing software from untrusted sources and to keep security solutions up to date," the researchers concluded.

Attack Type

Malware Attack

Cause of Issue

Lack of Malware Protection tools

Type of Loss

Data Compromise

Domain

Finance Sector

FIN8 Hackers Spotted Using New 'White Rabbit' Ransomware in Recent Attacks

The financially motivated FIN8 actor, in all likelihood, has resurfaced with a never-before-seen ransomware strain called "White Rabbit" that was recently deployed against a local bank in the U.S."One of the most notable aspects of White Rabbit's attack is how its payload binary requires a specific command-line password to decrypt its internal configuration and proceed with its ransomware routine," the researchers noted. "This method of hiding malicious activity is a trick that the ransomware family Egregor uses to hide malware techniques from analysis."White Rabbit adheres to the double extortion scheme and is believed to have been delivered via Cobalt Strike, a post-exploitation framework that's put to use by threat actors to reconnoiter, infiltrate, and drop malicious payloads into the affected system.Double extortion, also known as pay-now-or-get-breached, refers to an increasingly popular ransomware strategy in which valuable data from the targets is exfiltrated prior to launching the encryption routine, followed by pressurizing the victims into paying up to prevent the stolen information from being published online.Indeed, the ransom note displayed after the completion of the encryption process warns the victim that their data will be published or sold once the four-day deadline to meet their demands elapses. "Given that FIN8 is known mostly for its infiltration and reconnaissance tools, the connection could be an indication of how the group is expanding its arsenal to include ransomware," Trend Micro said. "So far, White Rabbit's targets have been few, which could mean that they are still testing the waters or warming up for a large-scale attack."

Attack Type

White Rabbits Attack, Ransomeware

Cause of Issue

Lack of Malware Protection tools

Type of Loss

Data Compromise

Domain

Finance Sector

Conclusion

According to an article, online threats has risen by as much as six times their usual levels recently as the Covid 19 pandemic provided greater scope for cyber attacks. All the attacks mentioned above - their types, the financial and reputation impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like a drop in an ocean. There are more unreported than that meets the eye. Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being 'lack of awareness. Well, as the saying goes,

"Prevention is better than Cure" - be it COVID-19 or Cyber threats.

Briskinfosec is ready to help you in your journey to protect your information infrastructure and assets. We assure you that we will help you to keep your data safe and also give you clear information on your company's current status and what are the steps needed to be taken to stay away from any kind of cyber attack.

Corporate Offices

INDIA

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

USA

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

UK

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

BAHRAIN

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