Edition-72

Threatsploit **Adversary** Report

August - 2024

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the August 2024 edition of the Threatsploit Adversary Report, your go-to source for the latest in cybersecurity threats and incidents. This month, we bring you detailed insights into major events that have impacted various industries, highlighting the vulnerabilities that need your attention.

A major highlight of this issue is a significant bug in CrowdStrike's software that caused widespread disruptions by triggering the infamous Windows 'Blue Screen of Death.' This incident underscores the critical importance of thorough testing and validation in software development to prevent such widespread issues.

In other news, the Indian cryptocurrency exchange WazirX suffered a $235 million hack due to a wallet exploitation, demonstrating the urgent need for stronger security measures in digital asset platforms. Hackers also exploited misconfigurations in Jenkins, allowing them to execute remote code, which emphasizes the importance of proper configuration management in development environments.

We also discuss a massive DDoS attack on OVHcloud, which experienced a record-breaking 840 million packets per second (PPS) flooding their service. This attack showcases the increasing scale and sophistication of DDoS threats faced by cloud service providers. Additionally, Evolve Bank & Trust faced a ransomware attack that resulted in a data breach affecting 7.6 million customers, highlighting the persistent danger of ransomware in the finance sector.

Our aim is to provide you with clear, actionable insights to help you stay ahead of cyber threats. This report is essential for cybersecurity professionals, business leaders, and anyone interested in the latest developments in cybersecurity.
Stay vigilant and stay secure.

Happy reading!

Best regards,

Briskinfosec Threat Intelligence Team.

Contents

CrowdStrike Bug Causes Widespread Windows 'Blue Screen of Death'

CrowdStrike, a major cybersecurity firm, caused widespread disruption when a defective software update for its Falcon Sensor product led to Windows systems crashing worldwide. This "blue screen of death" affected millions of users, disrupting businesses, airports, healthcare, and more, with estimated losses running into billions of dollars. The issue, isolated to Windows systems running CrowdStrike's software, prompted major IT outages globally. CrowdStrike quickly acknowledged and fixed the problem, but recovery for some systems could extend into the next week due to the complexity of the fix. The incident underscored vulnerabilities in centralized IT infrastructure and raised concerns about cybersecurity preparedness in global businesses.

Attack Type : Update Flaw

Cause of Issue : Coding flaw

Industry Type : Software Development Companies

$235M WazirX Hack Impacting India's Crypto Sector

On July 18, WazirX, an Indian cryptocurrency exchange, experienced a $235 million hack suspected to involve North Korean hackers, possibly from the Lazarus Group. The attack exploited vulnerabilities in WazirX's multisig wallet, allowing the attacker to alter wallet implementation and bypass transaction verifications.

The attacker moved $234.9 million in cryptocurrencies to new addresses, including Tether (USDT), Pepe (PEPE), Gala (GALA), and Shiba Inu (SHIB), swiftly converting these assets to Ethereum (ETH) to obscure their trail. The breach prompted WazirX to suspend withdrawals and launch investigations, while also reporting the incident to authorities.

The hack raises significant security concerns for India's crypto sector, amidst regulatory challenges and tax issues. WazirX has taken legal action and is collaborating with other exchanges to recover stolen funds and enhance security measures.

Attack Type : Multisig Wallet Exploit

Cause of Issue : Wallet Exploitation

Industry Type : Cryptocurrency Trading

Jenkins Script Console Exploited by Hackers for Cryptocurrency Mining

Researchers in cybersecurity have identified a significant risk associated with improperly configured Jenkins Script Console instances, potentially exploited by attackers for malicious activities such as cryptocurrency mining. Jenkins, a widely used CI/CD platform, includes a Groovy script console that, if exposed due to misconfigurations, can lead to remote code execution (RCE). This allows attackers to run arbitrary Groovy scripts, compromising Jenkins infrastructure and potentially launching cryptocurrency mining operations. To mitigate such risks, experts recommend implementing strict access controls, ensuring proper authentication mechanisms, conducting regular security audits, and preventing Jenkins servers from being accessible publicly on the internet. This issue highlights ongoing cybersecurity challenges as cryptocurrency-related thefts rise due to various hacking techniques in 2024.

Attack Type : Remote Code Execution

Cause of Issue : Misconfigured Jenkins

Industry Type : Software Development Companies

OVHcloud Targeted by Massive 840 Million PPS DDoS Attack Leveraging MikroTik Routers

In April 2024, OVHcloud thwarted a record-breaking DDoS attack, reaching 840 million packets per second (Mpps), surpassing a previous high of 809 Mpps. This attack combined a TCP ACK flood from 5,000 IPs with a DNS reflection from 15,000 servers. The majority of traffic entered the United States via four points, highlighting concentrated attack capabilities. OVHcloud noted a surge in DDoS frequency, with attacks exceeding 1 Tbps becoming common. Many attacks originate from compromised MikroTik routers, vulnerable due to outdated software, potentially forming powerful botnets capable of overwhelming defences with billions of packets per second.

Attack Type : Packet Flooding

Cause of Issue : Outdated Routers

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

Evolve Bank Cyberattack Leaks Data of 7.6 Million Customers

Evolve Bank & Trust disclosed a significant data breach affecting 7.6 million customers, including 20,000 in Maine, following a ransomware attack by the LockBit group in February 2024. The breach compromised personal data like names, Social Security numbers, bank details, and more, impacting not only customers but also partner firms like Affirm and Wise. Despite detecting the intrusion in May and refusing ransom demands, Evolve faces ongoing fallout, offering affected customers credit monitoring and identity theft protection services as mitigation measures.

Attack Type : Ransomware Attack

Cause of Issue : Ransomware Intrusion

Industry Type : Finance and Banking

Florida Health Department Faces Cyberattacks, Service Disruptions Persist as State Declines Ransom

The Florida Department of Health has been dealing with a cyberattack on its Vital Statistics System, orchestrated by the hacking group RansomHub. This attack has disrupted services, particularly in issuing death certificates, due to the system being offline. Despite laws prohibiting such payments, the state declines to pay the attackers' demanded ransom. County health departments can still issue birth certificates for babies born before June 28, 2024, but newer births require manual processing.

This incident follows a similar cyberattack on the Department of Juvenile Justice's system in March 2024, which also caused significant disruptions. Both attacks have sparked concerns about the state's cybersecurity measures and the duration it takes to recover from such incidents.

Attack Type : Ransomware Attack

Cause of Issue : Exploit Vulnerabilities

Industry Type : Healthcare Domain

Windows MSHTML Zero-Day Exploited in Malware Attacks for Over a Year

In July 2024, Microsoft addressed a critical zero-day vulnerability, CVE-2024-38112, which allowed threat actors to exploit Internet Explorer by using malicious .URL files disguised as PDFs. These files have the potential to trick users into downloading HTA files containing password-stealing malware. Despite Internet Explorer's retirement, it still poses risks due to fewer security warnings compared to modern browsers. Microsoft's fix now redirects mhtml: URIs to Microsoft Edge, mitigating the vulnerability. This issue mirrors CVE-2021-40444, highlighting ongoing security challenges with legacy technologies.

Attack Type : File download Spoofing

Cause of Issue : Exploitation of MHTML Vulnerability

Industry Type : Manufacturing and Industrial Control Systems (ICS)

Critical Zero-Click RCE Vulnerability Discovered in Microsoft Outlook

CVE-2024-38021 is a critical zero-click remote code execution vulnerability affecting Microsoft Outlook applications, now patched by Microsoft. Unlike CVE-2024-30103, which required an NTLM token, this vulnerability requires no authentication for trusted senders and one-click interaction for untrusted senders. Morphisec discovered the flaw, advised reclassifying it as "critical," reported it on April 21, 2024, confirmed it on April 26, 2024, and patched it on July 9, 2024. To mitigate risks, it is essential to update all Outlook and Office applications, disable automatic email previews, educate users, and ensure robust email security measures ,endpoint defences and ensure comprehensive coverage across the security stack with EDR and AMTD.

Attack Type : Remote Exploitation

Cause of Issue : Authentication Bypass

Industry Type : Software Development Companies

Critical Exim Mail Server Flaw Threatens Millions with Malicious Attachments

A critical vulnerability, CVE-2024-39929, in the Exim mail transfer agent has been identified, with a CVSS score of 9.1. It affects versions through 4.97.1 and allows attackers to bypass a $mime_ filename extension-blocking protection, potentially delivering executable attachments to users' inboxes. Over 1.5 million internet-accessible Exim servers are potentially vulnerable. Users should update to version 4.98 to mitigate the risk. Although there have been no reports of active exploitation, users running malicious attachments could compromise systems due to this issue.

Attack Type : Attachment Bypass

Cause of Issue : Header Misparsing

Industry Type : Software Development Companies

FishXProxy Phishing Kit Equips Cybercriminals for Effective Attacks

The FishXProxy phishing toolkit, recently reported by SlashNext Security, is an advanced phishing kit that uses Cloudflare's CDN and other sophisticated features to evade traditional security measures. It allows attackers, even those with limited technical skills, to conduct highly effective phishing campaigns. The kit's features include unique link generation, CAPTCHA integration, redirection systems, page-expiration settings, and HTML smuggling, all designed to bypass security defences and increase the success rate of attacks. Experts warn that this development will likely lead to an increase in sophisticated phishing attacks, emphasizing the need for advanced, multi-layered security solutions. Integrating human threat intelligence and training employees to recognize phishing threats is also recommended.

Attack Type : Phishing Attack

Cause of Issue : Phishing Sophistication

Industry Type : Software Development Companies

PHP Flaw Exploited for Malware Distribution and DDoS Attacks

Threat actors are exploiting a recently disclosed PHP vulnerability, CVE-2024-4577 (CVSS score: 9.8), to deploy remote access trojans, cryptocurrency miners, and DDoS botnets. The flaw, which affects PHP on Windows systems using Chinese and Japanese locales, allows remote command execution due to improper handling of Unicode to ASCII conversion. Exploit attempts were detected within a day of disclosure, targeting PHP installations with threats like Gh0st RAT, RedTail crypto-mining malware, and Muhstik DDoS botnet. Imperva has also reported ransomware attacks leveraging this vulnerability. Users are advised to update PHP to mitigate these risks. Additionally, Cloudflare's Q2 2024 report highlights a 20% year-over-year increase in DDoS attacks, with 8.5 million attacks mitigated in the first half of the year. China, Turkey, and Singapore were the most targeted countries, while Argentina was the largest source of attacks. Ukraine experienced a significant rise in HTTP DDoS attacks, with a 625% increase year-over-year.

Attack Type : Remote Command

Cause of Issue : Unicode Conversion

Industry Type : Software Development Companies

New Banking Malware Targets Southeast Asian Customers

Promon research has discovered a new malware strain, Snowblind, targeting banking customers in Southeast Asia. Snowblind uses a unique technique to disable Android banking apps' ability to detect malicious modifications, thereby avoiding detection. The malware takes advantage of accessibility services on apps, specifically designed to aid users with disabilities. Snowblind uses these services to access sensitive information, navigate devices, and bypass security measures. The malware can steal login credentials, hijack banking sessions, disable app security features, and extract sensitive information. Snowblind is effective on all modern Android devices and targets banking apps. The malware bypasses anti-tampering code in seccomp by installing its own seccomp filter and preventing excessive signals from being generated. Snowblind is more sophisticated than other techniques used to bypass anti-tampering code and has not been publicly described in use in any public tools.

Attack Type : Accessibility Exploitation

Cause of Issue : Anti-tampering Bypass

Industry Type : Finance and Banking

Cybercriminals Use Cloud Services for Malware Deployment

Malware operators are increasingly utilizing legitimate cloud services like AWS and DriveHQ for malicious activities, such as command and control operations and distributing malware like RATs and crypters. This approach ensures persistent communication and amplifies attacks by exploiting vulnerabilities in devices like routers and webservers. Fortinet's FortiGuard Labs identified new malware strains such as 'Skibidi' and botnets like Condi and Unstable that leverage cloud-based infrastructure to enhance their impact, underscoring the need for enhanced cloud security measures like patching, updates, and network segmentation to defend against these evolving threats.

Attack Type : Cloud-based Command and Control (C2)

Cause of Issue : Vulnerability Exploitation

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

New OpenSSH Flaw Revealed : Risk of Remote Code Execution

A new vulnerability in the OpenSSH secure networking suite, CVE-2024-6409, can trigger remote code execution (RCE) in versions 8.7p1 and 8.8p1 shipped with Red Hat Enterprise Linux 9. The vulnerability is distinct from CVE-2024-6387 and relates to code execution in the privsep child process due to a race condition in signal handling. Security researcher Alexander Peslyak discovered the bug during a review of CVE-2024-6387. The signal handler race condition vulnerability is the same as CVE-2024-6387, where if a client does not authenticate within LoginGraceTime seconds, the OpenSSH daemon process' SIGALRM handler is called asynchronously, triggering various functions that are not async-signal-safe. An active exploit for CVE-2024-6387 has been detected in the wild, targeting servers primarily located in China.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Signal Handling

Industry Type : Software Development Companies

GitHub Token Breach Risks Security of Python's Core Repositories

Cybersecurity researchers discovered an accidentally leaked GitHub token in a public Docker container, potentially allowing elevated access to the GitHub repositories of the Python language, Python Package Index (PyPI), and the Python Software Foundation (PSF). A compiled Python file contained the token, which PyPI Admin Ee Durbin quickly revoked after responsible disclosure on June 28, 2024. There is no evidence that the token was exploited. The incident highlights the risk of a supply chain attack. Simultaneously, Checkmarx detected malicious PyPI packages that leak sensitive data to a Telegram bot associated with cybercriminals in Iraq.

Attack Type : Code Injection

Cause of Issue : Token Exposure

Industry Type : Software Development Companies

Advance Auto Parts Breach Exposes Data of 2.3 Million People

Advance Auto Parts is notifying over 2.3 million current and former employees, as well as job applicants, of a data breach involving personal information stolen from its Snowflake cloud environment. Beginning in April 2024 and confirmed on June 19, 2024, the breach exposed sensitive data, including names, Social Security numbers, and driver's licenses. The company is offering affected individuals 12 months of free identity theft protection and credit monitoring. While the stolen data is less extensive than initially claimed by the attackers, customers may receive future notifications if their information is also exposed.

Attack Type : Data Theft

Cause of Issue : Stolen Credentials

Industry Type : Manufacturing and Industrial Control Systems (ICS)

Sibanye-Stillwater Hit by Cyber Attack on Worldwide IT Systems

Sibanye-Stillwater, a multinational mining and metals processing company listed on the JSE, was hit by a global cyber-attack that affected its IT systems. The company quickly implemented containment measures to isolate affected systems and protect data, though the investigation is still ongoing. Despite the attack, global operations have faced limited disruption so far. The incident underscores a broader trend of increasing cybercrime in South Africa, where recent statistics reveal a surge in data breaches. Over the course of a decade, the Department of Public Works and Infrastructure reported R300 million in losses due to cybercrime, and the number of reported breaches has more than tripled from the previous year. Other notable victims of cyber-attacks include TransUnion, Dis-Chem, and Experian.

Attack Type : Network Breach

Cause of Issue : Cyber Attack

Industry Type : Software Development Companies

Chinese Hackers Target Cisco Switches Zero-Day to Deploy Malware

A China-based cyber espionage group called Velvet Ant is exploiting a zero-day vulnerability (CVE-2024-20399) in Cisco NX-OS software, used in various Cisco switches, to deliver custom malware. This command injection flaw allows attackers with administrator access to execute arbitrary commands on affected devices without logging the activities, enabling stealthy operations. The vulnerability impacts multiple Nexus switch models and requires administrator credentials for exploitation. Cisco became aware of the issue in April 2024, while Sygnia detected active exploitation during a broader investigation. Additionally, threat actors are exploiting a critical vulnerability (CVE-2024-0769) in D-Link DIR-859 routers to extract sensitive user account information, with no patch available due to the product's end-of-life status.

Attack Type : Command Injection

Cause of Issue : Insufficient Validation

Industry Type : Digital Communication and Technology

mSpy Data Breach Exposes Millions of Spyware Users

In May 2024, a data breach at mSpy, a phone surveillance app company, exposed millions of customer support tickets containing personal information, emails, and documents. The data, which dates back to 2014, was stolen from mSpy's Zendesk-powered customer support system. The Ukrainian company Brainstack operates mSpy, which frequently monitors individuals without consent. The leaked information includes requests from various individuals, including U.S. military personnel, government officials, and law enforcement. Despite the breach, mSpy has not publicly acknowledged it. The incident highlights the security risks associated with spyware operations.

Attack Type : Unauthorized Access

Cause of Issue : Data Breach

Industry Type : Software Development Companies

Poco RAT Infiltrates Mining Industry

Access trojan (RAT) called Poco RAT, targeting the mining and manufacturing sector in Latin America. The malware uses the popular POCO C++ libraries as an evasion tactic, spreading in an email campaign that initially targeted an unnamed LATAM company in the mining sector. Since then, Poco RAT has targeted manufacturing, hospitality, and utility organizations. The campaign follows a consistent pattern, with emails using finance themes and malicious Google Drive and HTML files. The malware uses legitimate file hosting services like Google Drive to bypass secure email gateways (SEGs), a tactic used by various actors and advanced persistent threat (APT) groups. Most messages hide the Poco RAT payload either via a direct link to a 7zip archive hosted on Google Drive, while about 40% used a malicious HTML file with an embedded link that then downloads a 7zip archive hosted on Google's service. Poco RAT also uses its reliance on the cross-platform, open-source POCO C++ libraries, making it less likely to be detected than if the malware were to use its own custom code or a less widely used library.

Attack Type : Phishing Campaign

Cause of Issue : Email Phishing

Industry Type : Finance and Banking

60 Malicious Packages Found in NuGet Supply Chain Breach

The NuGet package manager has published a new wave of malicious packages, introducing a new level of stealth to evade detection. The packages, spanning 290 versions, demonstrate a refined approach from the previous set, which used NuGet's MSBuild integrations. The attackers used Intermediary Language (IL) Weaving, a.NET programming technique, to insert simple, obfuscated downloaders into legitimate PE binary files. The goal of the counterfeit packages is to deliver an off-the-shelf remote access trojan called SeroXen RAT. All identified packages have been taken down. The latest collection of packages uses IL weaving to inject malicious functionality into a Portable Executable (PE).NET binary associated with a legitimate NuGet package. This latest campaign highlights new ways in which malicious actors are scheming to fool developers and security teams into downloading and using malicious or tampered with packages from popular open source package managers like NuGet.

Attack Type : Supply Chain

Cause of Issue : Malicious Packages

Industry Type : Software Development Companies

Australian Arrested for Fake Wi-Fi Scam on Flights

An Australian man has been charged for setting up fake Wi-Fi access points on domestic flights and in airports across Perth, Melbourne, and Adelaide. Using an "evil twin" Wi-Fi attack, he impersonated legitimate networks to capture personal data from unsuspecting users who connected to his phony networks. Victims were prompted to enter their credentials on a captive portal, potentially exposing their email, social media, and financial information. The suspect faces multiple charges related to electronic communication impairment and data theft, with a maximum penalty of 23 years in prison if convicted. Users are advised to avoid entering personal details on public Wi-Fi and to use a reputable VPN for secure internet browsing.

Attack Type : Evil twin WiFi

Cause of Issue : Fake WiFi

Industry Type : Airlines

DarkGate Malware Targets Samba File Shares in Brief Attack

Cybersecurity researchers have discovered a short-lived DarkGate malware campaign that used Samba file shares to initiate infections. The campaign targeted North America, Europe, and parts of Asia. The malware, which first emerged in 2018, has evolved into a malware-as-a-service (MaaS) offering with capabilities to remotely control compromised hosts, execute code, mine cryptocurrency, launch reverse shells, and drop additional payloads. The campaign began with Microsoft Excel files that prompted targets to click on an embedded Open button, which then ran VBS code on a Samba file share. The malware works by scanning for anti-malware programs and checking CPU information to hinder analysis. The disclosure comes as Proofpoint revealed that a spam distributor used DarkGate in a global campaign to infiltrate over 1,000 organizations and sell access to other attackers for follow-on exploitation.

Attack Type : Malware Campaign

Cause of Issue : Exploited Samba

Industry Type : Software Development Companies

AT&T Reports Data Breach Impacting Almost All Wireless Customers

AT&T has confirmed that threat actors have unlawfully accessed data belonging to nearly all of its wireless customers and customers of mobile virtual network operators (MVNOs) using AT&T's wireless network. Snowflake, a third-party cloud platform, confirmed the connection between the breach and the hack that affected other customers like Ticketmaster, Santander, Neiman Marcus, and LendingTree. The company has activated its response efforts and is working with law enforcement to arrest those involved. The malicious cyber campaign targeting Snowflake has landed as many as 165 customers in the crosshairs, with Google-owned Mandiant attributing the activity to a financially motivated threat actor dubbed UNC5537. The criminals have demanded payments of between $300,000 and $5 million in return for the stolen data. AT&T has reportedly paid the threat actors behind the breach $370,000 in cryptocurrency to delete what's believed to be the "only copy" of the data and provide a video demonstrating proof of deletion. The U.S. Federal Communications Commission (FCC) has an ongoing investigation into the AT&T breach and is coordinating with its law enforcement partners.

Attack Type : Data Breach

Cause of Issue : Cloud Exploitation

Industry Type : Businesses Sector

APT40 Hackers Exploit SOHO Routers for Attacks

A joint advisory from international cybersecurity agencies and law enforcement warns of the tactics used by the Chinese state-sponsored APT 40 hacking group, which has been active since at least 2011. Instead of human interaction, APT40 exploits vulnerabilities in public-facing infrastructure and edge networking devices, such as phishing emails and social engineering. The group is known to rapidly exploit new vulnerabilities as they are publicly disclosed, with flaws in Log4J, Atlassian Confluence, and Microsoft Exchange as examples. After breaching a server or networking device, the Chinese hackers deploy web shells for persistence using Secure Socket Funnelling and then use valid credentials captured via Kerberoasting along with RDP for lateral movement through a network. They commonly breach end of life small-office/home-office (SOHO) routers using N-day vulnerabilities and hijack them to act as operational infrastructure. Other Chinese APT groups also use operational relay box (ORBs) networks, which are made up of hijacked EoL routers and IoT devices. The advisory contains two case studies from 2022, highlighting APT40's tactics and procedures.

Attack Type : Cyberespionage

Cause of Issue : Router Hijacking

Industry Type : Telecommunications

SocGholish Malware Hijacks BOINC Projects for Stealthy Cyber Attacks?

The SocGholish (Fake Updates) malware is delivering AsyncRAT, a remote access trojan, and BOINC, a legitimate open-source computing platform. The malware disguises BOINC as "Security-HealthService.exe" or "trustedinstaller.exe" to avoid detection and connects to actor-controlled domains to collect data and potentially deploy further attacks. BOINC's use for malicious purposes is being investigated. The attack sequence often starts with a fake browser update prompt on compromised websites, leading to the installation of malware. Recently, malware authors have used compiled V8 JavaScript to evade detection.

Attack Type : Downloader Trojan

Cause of Issue : Malicious Exploitation

Industry Type : Software Development Companies

Twilio Breach Exposes 33 Million Authy Numbers Due to Unsecured API

A data breach by the ShinyHunters Group exposed 33 million Authy phone numbers, along with additional data. Twilio has confirmed the breach and updated its Android and iOS apps in response. The breach, revealed in late June, was publicized when ShinyHunters dumped the data on BreachForums. Authy, a popular two-factor authentication app, may face a surge in phishing attacks as a result. Hackers are likely to craft convincing phishing messages to exploit this data. Jason Kent highlights the need for proper authentication and authorization on API endpoints. The breach occurred because ShinyHunters tested a large list of phone numbers against an unauthenticated Authy API endpoint. This method of attack potentially pairs the stolen numbers with information from other breaches. Users should be vigilant for phishing attempts and review their security practices.

Attack Type : API Enumeration

Cause of Issue : Unauthenticated API Endpoint

Industry Type : Manufacturing and Industrial Control Systems (ICS)

Compromised jQuery Packages Identified on npm, GitHub, and jsDelivr

Threat actors have been discovered spreading trojanized jQuery versions on npm, GitHub, and jsDelivr in a complex supply chain attack. The attack, which affected 68 packages, involved hiding malware in the rarely used 'end' function of jQuery. This malware exfiltrates website form data to a remote URL. The malicious files were manually assembled and published over a month, with some hosted-on GitHub and accessed via jsDelivr to appear more legitimate. In a related incident, malicious packages on PyPI were found to download additional payloads based on CPU architecture.

Attack Type : Supply chain Attack

Cause of Issue : Trojanized Packages

Industry Type : Software Development Companies

New Ransomware Targets Veeam Backup Flaw

EstateRansomware, a ransomware operation targeting Veeam Backup & Replication software, exploits a patched security flaw. The attack was discovered by Singapore-based Group-IB in April 2024, and the modus operandi involved exploiting CVE-2023-27532. The attacker accessed the target environment via a Fortinet FortiGate firewall SSL VPN appliance using a dormant account. They then established RDP connections from the firewall to the failover server and deployed a persistent backdoor named "svchost.exe" to evade detection. The backdoor connected to a command-and-control (C2) server over HTTP and executed arbitrary commands issued by the attacker. The attacker aimed to enable xp_cmdshell on the backup server and create a rogue user account named "VeeamBkp." The attack culminated in the deployment of the ransomware, but not before taking steps to impair defences and moving laterally from the AD server to all other servers and workstations using compromised domain accounts. This e-crime group prioritizes establishing initial access using security flaws in public-facing applications, phishing attachments, or breaching valid accounts.

Attack Type : Ransomware Attack

Cause of Issue : Exploited Vulnerability

Industry Type : Software Development Companies

Pro-Palestinian Hacker Group Launches Six-Day DDoS Assault on UAE Bank

A financial institution in the United Arab Emirates faced a record-setting DDoS attack by the pro-Palestinian hacktivist group BlackMeta, also known as DarkMeta. The attack, which lasted six days, averaged 4.5 million requests per second and targeted the institution 70% of the time. BlackMeta, affiliated with Anonymous Sudan, utilized the InfraShutdown service, providing DDoS attacks at a cost of $500 to $625 per week. The group, motivated by pro-Palestinian ideology and an anti-Western stance, has targeted various critical infrastructures. Traditional defences, such as rate-limiting and firewalls, proved ineffective against the attack's sophisticated Layer 7 techniques.

Attack Type : Application-layer DDoS

Cause of Issue : Prolonged DDoS

Industry Type : Finance and Banking

Top 5 Cybersecurity Games 2.0

1. NITE Team 4 : Military Hacking Division

A sophisticated hacking simulation game that combines tactical operations with hacking missions. Players join a cyber defense team and tackle various cyber threats and operations.

https://store.steampowered.com/app/544390/NITE_Team_4__Military_Hacking_Division/

2. Cyber Ops

A tactical stealth game where players take on the role of a cyber warfare operator. The game involves hacking into enemy networks, securing critical data, and coordinating with field agents.

https://store.steampowered.com/app/863460/Cyber_Ops/

3. Hacknet Labyrinths

An expansion to the popular "Hacknet" game, adding new hacking challenges, tools, and a deeper storyline. Players dive into more complex systems and uncover hidden secrets.

https://store.steampowered.com/app/521840/Hacknet__Labyrinths/

4. Exapunks

A puzzle game where players hack various systems to achieve objectives. The game features a unique, retro-style programming environment where players write code to complete missions.

https://store.steampowered.com/app/716490/EXAPUNKS/

5. Midnight Protocol

A tactical narrative-driven hacking RPG where players hack into servers and complete missions using a text-based interface. The game focuses on strategic planning and decision-making.

https://store.steampowered.com/app/1162700/Midnight_Protocol/

Briskinfosec Technology and Consulting Pvt ltd,

No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

Office : +91 44 4352 4537 | Mobile : +91 86086 34123
contact@briskinfosec.com | www.briskinfosec.com