RELATÓRIO DE MALWARES DE TODAS PÁGINAS ENCONTRADAS

Título: News Archive - June 2025

Classificações de Malware:

- exploit (Exploit)
- cve (Exploit)

Origem: pagina1.txt

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Weekly Recap: iPhone Spyware, Microsoft 0-Day, TokenBreak Hack, AI Data Leaks and More

Classificações de Malware:

- spyware (Spyware)
- cve (Exploit)
- ads (Adware)
- backdoor (Backdoor)
- rat (Backdoor)
- virus (Virus)
- infection (Virus)
- trojan (Trojan)
- dropper (Trojan)
- exploit (Exploit)
- adware (Adware)

Origem: pagina10.txt

Some of the biggest security problems start quietly. No alerts. No warnings. Just small actions that seem normal but aren't. Attackers now know how to stay hidden by blending in, and that makes it hard to tell when something's wrong.

This week's stories aren't just about what was attacked-but how easily it happened. If we're only looking for the obvious signs, what are we missing right in front of us?

Here's a look at the tactics and mistakes that show how much can go unnoticed.

Apple Zero-Click Flaw in Messages Exploited to Deliver Paragon Spyware- Apple disclosed that a security flaw in its Messages app was actively exploited in the wild to target civil society members in sophisticated cyber attacks. The vulnerability, CVE-2025-43200, was addressed by the company in February as part of iOS 18.3.1, iPadOS 18.3.1, iPadOS 17.7.5, macOS Sequoia 15.3.1, macOS Sonoma 14.7.4, macOS Ventura 13.7.4, watchOS 11.3.1, and visionOS 2.3.1. The Citizen Lab said it uncovered forensic evidence that the flaw was weaponized to target Italian journalist Ciro Pellegrino and an unnamed prominent European journalist and infect them with Paragon's Graphite mercenary spyware.

Sensitive data moves fast in the cloud. If you can't see it, you can't protect it. This guide shows how top teams use DSPM to reduce risk, improve compliance, and boost efficiency-backed by real metrics that drive measurable impact.

Attackers love software vulnerabilities - they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.

This week's list includes -CVE-2025-43200(Apple),CVE-2025-32711(Microsoft 365 Copilot),CVE-2025-33053(Microsoft Windows),CVE-2025-47110(AdobeCommerce and Magento Open Source),CVE-2025-43697, CVE-2025-43698, CVE-2025-43699, CVE-2025-43700, CVE-2025-43701(Salesforce),CVE-2025-24016(Wazuh),CVE-2025-5484, CVE-2025-5485(SinoTrack),CVE-2025-31022(PayU CommercePro plugin),CVE-2025-3835(ManageEngine Exchange Reporter Plus),CVE-2025-42989(SAP NetWeaver),CVE-2025-5353,CVE-2025-22463,CVE-2025-22455(Ivanti Workspace Control),CVE-2025-5958(Google Chrome),CVE-2025-3052(DT Research DTBios and BiosFlashShell),CVE-2025-2884(TCG TPM2.0 reference implementation),CVE-2025-26521(Apache CloudStack),CVE-2025-47950(CoreDNS),CVE-2025-4230,CVE-2025-4232(Palo Alto Networks PAN-OS),CVE-2025-4278, CVE-2025-2254, CVE-2025-5121, CVE-2025-0673(GitLab),CVE-2025-47934(OpenPGP.js),CVE-2025-49219,CVE-2025-49220(Trend Micro Apex Central),CVE-2025-49212,CVE-2025-49213,CVE-2025-49216,CVE-2025-49217(Trend Micro Endpoint Encryption PolicyServer),CVE-2025-4922(HashiCorp Nomad),CVE-2025-36631,CVE-2025-36632,CVE-2025-36633(Tenable Nessus Agent),CVE-2025-33108(IBM Backup, Recovery, and Media Services),CVE-2025-6029(KIA-branded Aftermarket Generic Smart Keyless Entry System), and apatch bypass for CVE-2024-41713(Mitel MiCollab).

Disclaimer: These newly released tools are for educational use only and haven't been fully audited. Use at your own risk-review the code, test safely, and apply proper safeguards.

4 Hidden Ways You're Tracked (and How to Fight Back) Most people know about cookies and ads, but companies now use sneaky technical tricks to track you-even if you're using a VPN, private mode, or a hardened browser. One method gaining attention islocalhost tracking: apps like Facebook and Instagram silently run a web server inside your phone. When you visit a website with a hidden code, it can ping this server to see if the app is installed-leaking your activity back to the app, without your permission.

Another trick isport probing. Some websites scan your device to check if developer tools or apps are running on certain ports (like 3000 or 9222). This reveals what software you use or whether you're running a specific company's tool-leaking clues about your job, device, or activity. Sites may even detect browser extensions this way.

On mobile, some websites silently test if apps like Twitter, PayPal, or your banking app are installed by triggeringinvisible deep links. If the app opens or responds, they learn what apps you use. That's often used for profiling or targeted phishing. Also, browser cache abuse (using things like ETags or service workers) can fingerprint your browser-even across private tabs-keeping you identifiable even when you think you're clean.

How to protect yourself:

These aren't tinfoil hat ideas-they're real-world methods used by major tech firms and trackers today. Staying private means going beyond ad blockers and learning how the web really works behind the scenes.

What goes undetected often isn't invisible-it's just misclassified, minimized, or misunderstood. Human error isn't always a technical failure. Sometimes it's a story we tell ourselves about what shouldn't happen.

Review your recent alerts. Which ones were ignored because they didn't "feel right" for the threat profile? The cost of dismissal is rising-especially when adversaries bank on it.

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: New TCESB Malware Found in Active Attacks Exploiting ESET Security Scanner

Classificações de Malware:

- cve (Exploit)
- exploit (Exploit)
- ransomware (Ransomware)

Origem: pagina11.txt

A Chinese-affiliated threat actor known for its cyber-attacks in Asia has been observed exploiting a security flaw in security software from ESET to deliver a previously undocumented malware codenamedTCESB.

"Previously unseen in ToddyCat attacks, [TCESB] is designed to stealthily execute payloads in circumvention of protection and monitoring tools installed on the device," Kasperskysaidin an analysis published this week.

ToddyCatis the name given to a threat activity cluster that has targeted several entities in Asia, with attacks dating all the way back to at least December 2020.

Last year, the Russian cybersecurity vendordetailedthe hacking group's use of various tools to maintain persistent access to compromised environments and harvest data on an "industrial scale" from organizations located in the Asia-Pacific region.

Kaspersky said its investigation into ToddyCat-related incidents in early 2024 unearthed a suspicious DLL file ("version.dll") in the temp directory on multiple devices. The 64-bit DLL, TCESB, has been found to be launched via a technique calledDLL Search Order Hijackingto seize control of the execution flow.

This, in turn, is said to have been accomplished by taking advantage of a flaw in theESET Command Line Scanner, which insecurely loads a DLL named "version.dll" by first checking for the file in the current directory and then checking for it in the system directories.

It's worth pointing out at this stage that "version.dll" is a legitimateversion-checking and file installation

libraryfrom Microsoft that resides in the "C:\Windows\system32\" or "C:\Windows\SysWOW64\" directories.

A consequence of exploiting this loophole is that attackers could execute their malicious version of "version.dll" as opposed to its legitimate counterpart. The vulnerability, tracked asCVE-2024-11859(CVSS score: 6.8), wasfixedby ESET in late January 2025 following responsible disclosure.

"The vulnerability potentially allowed an attacker with administrator privileges to load a malicious dynamic-link library and execute its code," ESETsaidin an advisory released last week. "This technique did not elevate the privileges, though - the attacker would have already needed to have administrator privileges to perform this attack."

In a statement shared with The Hacker News, the Slovak cybersecurity company said it released fixed builds of its consumer, business, and server security products for the Windows operating system to address the vulnerability.

TCESB, for its part, is a modified version of an open-source tool called EDRSandBlast that includes features to alter operating system kernel structures to disable notification routines (akacallbacks), which are designed to allow drivers to be notified of specific events, such as process creation or setting a registry key.

To pull this off, TCESB leverages another known technique referred to as bring your own vulnerable driver (BYOVD) to install a vulnerable driver, a Dell DBUtilDrv2.sys driver, in the system through the Device Manager interface. The DBUtilDrv2.sys driver is susceptible to a known privilege escalation flaw tracked asCVE-2021-36276.

This is not the first time Dell drivers have been abused for malicious purposes. In 2022, a similar privilege escalation vulnerability (CVE-2021-21551) in another Dell driver, dbutil_2_3.sys, was alsoexploitedas part of BYOVD attacks by the North Korea-linked Lazarus Group to turn off security mechanisms.

"Once the vulnerable driver is installed in the system, TCESB runs a loop in which it checks every two seconds for the presence of a payload file with a specific name in the current directory - the payload may not be present at the time of launching the tool," Kaspersky researcher Andrey Gunkin said.

While the payload artifacts themselves are unavailable, further analysis has determined that they are encrypted using AES-128 and that they are decoded and executed as soon as they appear in the specified

path.

"To detect the activity of such tools, it's recommended to monitor systems for installation events involving drivers with known vulnerabilities," Kaspersky said. "It's also worth monitoring events associated with loading Windows kernel debug symbols on devices where debugging of the operating system kernel is not expected."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Pakistan-Linked Hackers Expand Targets in India with CurlBack RAT and Spark RAT

Classificações de Malware:

- rat (Backdoor)
- trojan (Trojan)
- infection (Virus)
- backdoor (Backdoor)
- virus (Virus)
- dropper (Trojan)
- exploit (Exploit)
- cve (Exploit)

Origem: pagina12.txt

A threat actor with ties to Pakistan has been observed targeting various sectors in India with various remote access trojans like Xeno RAT, Spark RAT, and a previously undocumented malware family calledCurlBack RAT.

The activity, detected by SEQRITE in December 2024, targeted Indian entities under railway, oil and gas, and external affairs ministries, marking an expansion of the hacking crew's targeting footprint beyond government, defence, maritime sectors, and universities.

"One notable shift in recent campaigns is the transition from using HTML Application (HTA) files to adopting Microsoft Installer (MSI) packages as a primary staging mechanism," security researcher Sathwik Ram Prakkisaid.

SideCopyis suspected to be a sub-cluster withinTransparent Tribe(aka APT36) that's active since at least 2019. It's so named formimicking the attack chainsassociated with another threat actor calledSideWinderto deliver its own payloads.

In June 2024, SEQRITEhighlightedSideCopy's use of obfuscated HTA files, leveraging a technique previously observed in SideWinder attacks. The files were also found to contain references to URLs that hosted RTF files identified as used by SideWinder.

The attacks culminated in the deployment ofAction RATandReverseRAT, two known malware families attributed to SideCopy, and several other payloads, including Cheex to steal documents and images, a USB copier to siphon data from attached drives, and a .NET-based Geta RAT that's capable of executing 30 commands sent from a remote server.

The RAT is also equipped to steal both Firefox and Chromium-based browser data of all accounts, profiles, and cookies, a feature borrowed from AsyncRAT.

"APT36 focus is majorly Linux systems whereas SideCopy targets Windows systems adding new payloads to its arsenal," SEQRITE noted at the time.

The latest findings demonstrate a continued maturation of the hacking group, coming into its own, while leveraging email-based phishing as a distribution vector for malware. These email messages contain various kinds of lure documents, ranging from holiday lists for railway staff to cybersecurity guidelines issued by a public sector undertaking called the Hindustan Petroleum Corporation Limited (HPCL).

One cluster of activity is particularly noteworthy given its ability to target both Windows and Linux systems, ultimately leading to the deployment of a cross-platform remote access trojan known asSpark RATand a new Windows-based malware codenamed CurlBack RAT that can gather system information, download files from the host, execute arbitrary commands, elevate privileges, and list user accounts.

A second cluster has been observed using the decoy files as a way to initiate a multi-step infection process

that drops a custom version ofXeno RAT, which incorporates basic string manipulation methods.

"The group has shifted from using HTA files to MSI packages as a primary staging mechanism and continues to employ advanced techniques like DLL side-loading, reflective loading, and AES decryption via PowerShell," the company said.

"Additionally, they are leveraging customized open-source tools like Xeno RAT and Spark RAT, along with deploying the newly identified CurlBack RAT. Compromised domains and fake sites are being utilized for credential phishing and payload hosting, highlighting the group's ongoing efforts to enhance persistence and evade detection."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Ripple's xrpl.js npm Package Backdoored to Steal Private Keys in Major Supply Chain Attack

Classificações de Malware:

- backdoor (Backdoor)
- cve (Exploit)
- rootkit (Rootkit)
- stealth (Rootkit)
- exploit (Exploit)

Origem: pagina13.txt

The Ripple cryptocurrency npm JavaScript library namedxrpl.jshas been compromised by unknown threat actors as part of a software supply chain attack designed to harvest and exfiltrate users' private keys.

The malicious activity has been found to affect five different versions of the package: 4.2.1, 4.2.2, 4.2.3, 4.2.4, and 2.14.2. The issue has beenaddressedin versions 4.2.5 and 2.14.3.

xrpl.js is a popular JavaScript API for interacting with theXRP Ledgerblockchain, also called the Ripple Protocol, a cryptocurrency platform launched by Ripple Labs in 2012. The package has beendownloadedover 2.9 million times to date, attracting more than 135,000 weekly downloads.

"The official XPRL (Ripple) NPM package was compromised by sophisticated attackers who put in a backdoor to steal cryptocurrency private keys and gain access to cryptocurrency wallets," Aikido Security's Charlie Eriksensaid.

The malicious code changes have been found to be introduced by a user named "mukulljangid" starting April 21, 2025, with the threat actors introducing a new function named checkValidityOfSeed that's engineered to transmit the stolen information to an external domain ("0x9c[.]xyz").

It's worth noting that "mukulljangid" likelybelongs to a Ripple employee, indicating that their npm account was hacked to pull off the supply chain attack.

The attacker is said to have tried different ways to sneak in the backdoor while trying to evade detection, as evidenced by the different versions released in a short span of time. There is no evidence that the associated GitHub repository has been backdoored.

It's not clear who is behind the attack, but it's believed that the threat actors managed to steal the developer's npm access token to tamper with the library, per Aikido.

In light of the incident, users relying on the xrpl.js library are advised to update their instances to the latest version (4.2.5 and 2.14.3) to mitigate potential threats.

"This vulnerability is in xrpl.js, a JavaScript library for interacting with the XRP Ledger," the XRP Ledger Foundationsaidin a post on X. "It does not affect the XRP Ledger codebase or GitHub repository itself. Projects using xrpl.js should upgrade to v4.2.5 immediately."

The supply chain compromise of xrpl.js has been assigned the CVE identifier CVE-2025-32965 (CVSS score: 9.3).

"Versions 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of xrpl.js were compromised and contained malicious code designed

to exfiltrate private keys,"accordingto a GitHub advisory. "If you are using one of these versions, stop immediately and rotate any private keys or secrets used with affected systems."

"Version 2.14.2 is also malicious, though it is less likely to lead to exploitation as it is not compatible with other 2.x versions. To secure funds, think carefully about whether any keys may have been compromised by this supply chain attack, and mitigate by sending funds to secure wallets, and/or rotating keys."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: SentinelOne Uncovers Chinese Espionage Campaign Targeting Its Infrastructure and Clients

Classificações de Malware:

- backdoor (Backdoor)
- ransomware (Ransomware)
- exploit (Exploit)
- cve (Exploit)

Origem: pagina14.txt

Cybersecurity company SentinelOne has revealed that a China-nexus threat cluster dubbedPurpleHazeconducted reconnaissance attempts against its infrastructure and some of its high-value customers.

"We first became aware of this threat cluster during a 2024 intrusion conducted against an organization previously providing hardware logistics services for SentinelOne employees," security researchers Tom Hegel, Aleksandar Milenkoski, and Jim Waltersaidin an analysis published Monday.

PurpleHaze is assessed to be a hacking crew with loose ties to another state-sponsored group known asAPT15, which is also tracked as Flea, Nylon Typhoon (formerly Nickel), Playful Taurus, Royal APT, and

Vixen Panda.

The adversarial collective has also been observed targeting an unnamed South Asian government-supporting entity in October 2024, employing an operational relay box (ORB) network and a Windows backdoor dubbed GoReShell.

The implant, written in the Go programming language, repurposes an open-source tool calledreverse_sshto set up reverse SSH connections to endpoints under the attacker's control.

"The use of ORB networks is a growing trend among these threat groups, since they can be rapidly expanded to create a dynamic and evolving infrastructure that makes tracking cyberespionage operations and their attribution challenging," the researchers pointed out.

Further analysis has determined that the same South Asian government entity was also targeted previously in June 2024 with ShadowPad (aka PoisonPlug), a known backdoor widely shared among China-nexus espionage groups. ShadowPad is considered to be a successor to another backdoor referred to as PlugX.

That said, with ShadowPad also being used as a conduit todeliver ransomwarein recent months, the exact motivation behind the attack remains unclear. The ShadowPad artifacts have been found to be obfuscated using a bespoke compiler calledScatterBrain.

The exact nature of the overlap between the June 2024 activity and the later PurpleHaze attacks is unknown as yet. However, it's believed that the same threat actor could be behind them.

The ScatterBrain-obfuscated ShadowPad is estimated to have been employed in intrusions targeting over 70 organizations spanning manufacturing, government, finance, telecommunications, and research sectors afterlikely exploitingan N-day vulnerability in Check Point gateway devices.

One among the victims of these attacks included the organization that was then responsible for managing hardware logistics for SentinelOne employees. However, the cybersecurity firm noted that it found no evidence of a secondary compromise.

It's not just China, for SentinelOne said it also observed attempts made byNorth Korea-aligned IT workersto secure jobs at the company, including its SentinelLabs intelligence engineering team, via approximately 360

fake personas and over 1,000 job applications.

Last but not least, ransomware operators have targeted SentinelOne and other enterprise-focused security platforms, attempting to gain access to their tools in order to evaluate the ability of their software to evade detection.

This is fuelled by an active underground economy that revolves around buying, selling, and renting access to such enterprise security offerings on messaging apps as well as forums like XSS[.]is, Exploit[.]in, and RAMP.

"Entire service offerings have emerged around this ecosystem, including 'EDR Testing-as-a-Service,' where actors can discreetly evaluate malware against various endpoint protection platforms," the researchers explained.

"While these testing services may not grant direct access to full-featured EDR consoles or agents, they do provide attackers with semi-private environments to fine-tune malicious payloads without the threat of exposure - dramatically improving the odds of success in real-world attacks."

One ransomware group that takes this threat to a whole new level is Nitrogen, which is believed to be run by a Russian national. Unlike typical approaches that involve approaching insiders or using legitimate credentials harvested from infostealer logs, Nitrogen adopts a different strategy by impersonating real companies.

This is achieved by setting up lookalike domains, spoofed email addresses, and cloned infrastructure that mimic legitimate companies, allowing the threat actor to purchase official licenses for EDR and other security products.

"This kind of social engineering is executed with precision," the researchers said. "Nitrogen typically targets small, lightly vetted resellers - keeping interactions minimal and relying on resellers' inconsistent KYC (Know Your Customer) practices to slip through the cracks."

stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Weekly Recap: iOS Zero-Days, 4Chan Breach, NTLM Exploits, WhatsApp Spyware & More

Classificações de Malware:

- spyware (Spyware)
- cve (Exploit)
- ransomware (Ransomware)
- crypto (Ransomware)
- backdoor (Backdoor)
- virus (Virus)
- infection (Virus)
- exploit (Exploit)

Origem: pagina15.txt

Can a harmless click really lead to a full-blown cyberattack?

Surprisingly, yes - and that's exactly what we saw in last week's activity. Hackers are getting better at hiding inside everyday actions: opening a file, running a project, or logging in like normal. No loud alerts. No obvious red flags. Just quiet entry through small gaps - like a misconfigured pipeline, a trusted browser feature, or reused login tokens. These aren't just tech issues - they're habits being exploited.

Let's walk through the biggest updates from the week and what they mean for your security.

Recently Patched Windows Flaw Comes Under Active Exploitation- A recently patched security flaw affectingWindows NTLM has been exploitedby malicious actors to leak NTLM hashes or user passwords and infiltrate systems since March 19, 2025. The flaw, CVE-2025-24054 (CVSS score: 6.5), is a hash disclosure spoofing bug that was fixed by Microsoft last month as part of its Patch Tuesday updates. The security flaw is assessed to be a variant of CVE-2024-43451 (CVSS score: 6.5), which was patched by Microsoft in November 2024 and has also been weaponized in the wild in attacks targeting Ukraine and Colombia by threat actors like UAC-0194 and Blind Eagle.

Companies need to rethink how they protect their private and public use of AI and how they defend against AI-powered attacks. Traditional firewalls, VPNs, and public-facing IPs expose your attack surface and are no match in the AI era. It's time for a modern approach with Zscaler Zero Trust + AI.

Attackers love software vulnerabilities-they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.

This week's list includes -CVE-2025-2492(ASUS),CVE-2025-24054(Microsoft Windows),CVE-2025-32433(Erlang/OTP),CVE-2021-20035(SonicWall Secure Mobile Access 100 Series),CVE-2025-31200, CVE-2025-31201(Apple iOS, iPadOS, macOS Sequoia, tvOS, and visionOS),CVE-2025-24859(Apache Roller),CVE-2025-1093(AIHub theme), andCVE-2025-3278(UrbanGo Membership plugin).

Stop Spam Before It Starts: Use Burner Emails the Smart Way- Most people use the same email everywhere - but when one company leaks or sells your address, your inbox starts filling with spam or phishing emails. A smarter way is to use a burner email system, where you give each company a unique email like netflix@yourdomain.com. To do this, buy a cheap domain (like myaliashub.com) and set up free forwarding with services like ImprovMX or SimpleLogin. Every email sent to any name on that domain will land in your main inbox. If one starts getting spam, just delete or block it - problem solved, no need to change your real email.

If you use Gmail, you can add +something after your name, like alex+uber@gmail.com, and Gmail will still deliver it. This helps you track who shared your email and set filters, but it's not very private since your real email is still visible. Some websites also block + emails. A better long-term option is to connect a custom domain to Gmail through Google Workspace, which gives you real aliases like shop@yourdomain.com with full control and spam filtering.

Apple users can use Hide My Email (built into iOS and macOS). It creates a random email like x2k4@privaterelay.appleid.com for each website, and forwards messages to your iCloud inbox. You can disable or delete these anytime. It's great for signups, subscriptions, or trials where you don't want to share your real email. For even more control, Apple lets you use custom domains too. These tools help you stay organized, stop spam early, and quickly trace any leaks - all without needing to change your main email ever

again.

This week made it clear: attackers aren't just hunting for big holes - they're slipping through tiny cracks we barely notice. An outdated security setting. A forgotten endpoint. A tool used slightly out of spec. And just like that, they're in. We're seeing more cases where the compromise isn't about breaking in - it's about being invited in by accident. As systems grow more connected and automated, even the smallest misstep can open a big door.

Stay sharp, stay curious - and double-check the things you think are "too minor to matter."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: U.S. Govt. Funding for MITRE's CVE Ends April 16, Cybersecurity Community on Alert

Classificações de Malware:

- cve (Exploit)
- backdoor (Backdoor)
- rat (Backdoor)
- trojan (Trojan)
- virus (Virus)
- infection (Virus)
- exploit (Exploit)

Origem: pagina16.txt

The U.S. government funding for non-profit research giant MITRE to operate and maintain its Common Vulnerabilities and Exposures (CVE) program will expire Wednesday, an unprecedented development that could shake up one of the foundational pillars of the global cybersecurity ecosystem.

The 25-year-old CVE program is a valuable tool for vulnerability management, offering a de facto standard to

identify, define, and catalog publicly disclosed security flaws using CVE IDs. The program has listed over 274,000 CVE records to date.

Yosry Barsoum, MITRE's vice president and director of the Center for Securing the Homeland (CSH), said its funding to "develop, operate, and modernize CVE and related programs, such as the Common Weakness Enumeration (CWE), will expire."

"If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure," Barsoumnotedin a letter sent to CVE Board Members.

However, Barsoum pointed out that the government continues to "make considerable efforts" to support MITRE's role in the program and that MITRE remains committed to CVE as a global resource.

The CVE program was launched in September 1999 and has been run by MITRE with sponsorship from the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA).

In response to the move, cybersecurity firm VulnCheck, which is a CVE Numbering Authority (CNA), hasannouncedthat it is proactively reserving 1,000 CVEs for 2025 to help fill the void.

"A service break would likely degrade national vulnerability databases and advisories," Jason Soroko, Senior Fellow at Sectigo, said in a statement shared with The Hacker News.

"This lapse could negatively affect tool vendors, incident response operations, and critical infrastructure broadly. MITRE emphasizes its continued commitment but warns of these potential impacts if the contracting pathway is not maintained."

Tim Peck, Senior Threat Researcher at Securonix, told The Hacker News that a lapse could have massive consequences for the cybersecurity ecosystem where CNAs and defenders may be unable to obtain or publish CVEs, causing delays in vulnerability disclosures.

"Additionally, the Common Weakness Enumeration (CWE) project is vital for software weakness classification and prioritization," Peck said. "Its halt would affect secure coding practices and risk assessments. The CVE

program is a foundational infrastructure. It's not just a nice to have 'referenceable list,' it's a primary resource for vulnerability coordination, prioritization and response efforts across the private sector, government and open source."

CISA has stepped in to extend funding to ensure the continuity of the CVE program, the agency said.

"The CVE Program is invaluable to the cyber community and a priority of CISA," it said in a statement. "Last night, CISA executed the option period on the contract to ensure there will be no lapse in critical CVE services. We appreciate our partners' and stakeholders' patience."

The development comes as a group of CVE Board members announced the launch of the CVE Foundation, a non-profit organization set up to secure the CVE program's independence.

"The formation of the CVE Foundation marks a major step toward eliminating a single point of failure in the vulnerability management ecosystem and ensuring the CVE Program remains a globally trusted, community-driven initiative," the CVE Foundationsaid.

"For the international cybersecurity community, this move represents an opportunity to establish governance that reflects the global nature of today's threat landscape."

Coinciding with the news of the potential CVE shutdown, the European Union Agency for Cybersecurity (ENISA) has also launched a European vulnerability database (EUVD), which "embraces a multi-stakeholder approach by collecting publicly available vulnerability information from multiple sources."

The Computer Incident Response Center of Luxembourg is also developing a "decentralized" system for identifying and numbering vulnerabilities called the Global CVE (GCVE) allocation system.

Título: Weekly Recap: Critical SAP Exploit, AI-Powered Phishing, Major Breaches, New CVEs & More

Classificações de Malware:

- exploit (Exploit)
- cve (Exploit)
- ransomware (Ransomware)
- lockbit (Ransomware)
- encryptor (Ransomware)
- backdoor (Backdoor)
- rootkit (Rootkit)
- stealth (Rootkit)

Origem: pagina17.txt

What happens when cybercriminals no longer need deep skills to breach your defenses? Today's attackers are armed with powerful tools that do the heavy lifting - from AI-powered phishing kits to large botnets ready to strike. And they're not just after big corporations. Anyone can be a target when fake identities, hijacked infrastructure, and insider tricks are used to slip past security unnoticed.

This week's threats are a reminder: waiting to react is no longer an option. Every delay gives attackers more ground.

Critical SAP NetWeaver Flaw Exploited as 0-Day- A critical security flaw in SAP NetWeaver (CVE-2025-31324, CVSS score: 10.0) has beenexploitedby unknown threat actors to upload JSP web shells with the goal of facilitating unauthorized file uploads and code execution. The attacks have also been observed using the Brute Ratel C4 post-exploitation framework, as well as a well-known technique called Heaven's Gate to bypass endpoint protections.

Companies need to rethink how they protect their private and public use of AI and how they defend against AI-powered attacks. Traditional firewalls, VPNs, and public-facing IPs expose your attack surface and are no match in the AI era. It's time for a modern approach with Zscaler Zero Trust + AI.

Attackers love software vulnerabilities-they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers

locked out.

This week's list includes -CVE-2024-58136, CVE-2025-32432(Craft CMS),CVE-2025-31324(SAP NetWeaver),CVE-2025-27610(Rack),CVE-2025-34028(Commvault Command Center),CVE-2025-2567(Lantronix Xport),CVE-2025-33028(WinZip),CVE-2025-21204(Microsoft Windows),CVE-2025-1021(Synology DiskStation Manager),CVE-2025-0618(FireEye EDR Agent),CVE-2025-1763(GitLab),CVE-2025-32818(SonicWall SonicOS),CVE-2025-3248(Langflow),CVE-2025-21605(Redis),CVE-2025-23249, CVE-2025-23250, and CVE-2025-23251(NVIDIA NeMo Framework),CVE-2025-22228(Spring Framework, NetApp), andCVE-2025-3935(ScreenConnect).

Don't Let Video Calls Become Backdoors- Attackers are now using fake meeting invites to trick people into giving them remote access during video calls. They set up fake interviews or business meetings, then request screen control - sometimes even changing their name to "Zoom" to make it look like a system message. If you click "Allow" without thinking, they can take over your computer, steal data, or install malware.

To stay safe, disable remote control features if you don't need them. On Zoom, turn it off in Settings under "In Meeting (Basic)." Always double-check who's asking for access, and never approve control just because it looks official. Use browser-based tools like Google Meet when possible - they're safer because they can't easily take control of your system.

For extra protection, Mac users can block Zoom (or any app) from getting special permissions like "Accessibility," which is needed for remote control. IT teams can also set this up across all company devices. And watch out for invites from odd emails or links - real companies won't use personal accounts or fake booking pages. Stay alert, and don't let a simple click turn into a big problem.

The most effective defenses often start with asking better questions. Are your systems behaving in ways you truly understand? How might attackers use your trusted tools against you?

Now is the time to explore security beyond technology - look into how your team handles trust, communication, and unusual behavior. Map out where human judgment meets automation, and where attackers might find blind spots.

Curiosity isn't just for research - it's a powerful shield when used to challenge assumptions and uncover

hidden risks.

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Ripple's xrpl.js npm Package Backdoored to Steal Private Keys in Major Supply Chain Attack

Classificações de Malware:

- backdoor (Backdoor)
- cve (Exploit)
- exploit (Exploit)

Origem: pagina18.txt

The Ripple cryptocurrency npm JavaScript library namedxrpl.jshas been compromised by unknown threat actors as part of a software supply chain attack designed to harvest and exfiltrate users' private keys.

The malicious activity has been found to affect five different versions of the package: 4.2.1, 4.2.2, 4.2.3, 4.2.4, and 2.14.2. The issue has beenaddressedin versions 4.2.5 and 2.14.3.

xrpl.js is a popular JavaScript API for interacting with theXRP Ledgerblockchain, also called the Ripple Protocol, a cryptocurrency platform launched by Ripple Labs in 2012. The package has beendownloadedover 2.9 million times to date, attracting more than 135,000 weekly downloads.

"The official XPRL (Ripple) NPM package was compromised by sophisticated attackers who put in a backdoor to steal cryptocurrency private keys and gain access to cryptocurrency wallets," Aikido Security's Charlie Eriksensaid.

The malicious code changes have been found to be introduced by a user named "mukulljangid" starting April 21, 2025, with the threat actors introducing a new function named checkValidityOfSeed that's engineered to

transmit the stolen information to an external domain ("0x9c[.]xyz").

It's worth noting that "mukulljangid" likelybelongs to a Ripple employee, indicating that their npm account was hacked to pull off the supply chain attack.

The attacker is said to have tried different ways to sneak in the backdoor while trying to evade detection, as evidenced by the different versions released in a short span of time. There is no evidence that the associated GitHub repository has been backdoored.

It's not clear who is behind the attack, but it's believed that the threat actors managed to steal the developer's npm access token to tamper with the library, per Aikido.

In light of the incident, users relying on the xrpl.js library are advised to update their instances to the latest version (4.2.5 and 2.14.3) to mitigate potential threats.

"This vulnerability is in xrpl.js, a JavaScript library for interacting with the XRP Ledger," the XRP Ledger Foundationsaidin a post on X. "It does not affect the XRP Ledger codebase or GitHub repository itself. Projects using xrpl.js should upgrade to v4.2.5 immediately."

The supply chain compromise of xrpl.js has been assigned the CVE identifier CVE-2025-32965 (CVSS score: 9.3).

"Versions 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of xrpl.js were compromised and contained malicious code designed to exfiltrate private keys,"accordingto a GitHub advisory. "If you are using one of these versions, stop immediately and rotate any private keys or secrets used with affected systems."

"Version 2.14.2 is also malicious, though it is less likely to lead to exploitation as it is not compatible with other 2.x versions. To secure funds, think carefully about whether any keys may have been compromised by this supply chain attack, and mitigate by sending funds to secure wallets, and/or rotating keys."

stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: SentinelOne Uncovers Chinese Espionage Campaign Targeting Its Infrastructure and Clients

Classificações de Malware:

- backdoor (Backdoor)
- ransomware (Ransomware)
- exploit (Exploit)

Origem: pagina19.txt

Cybersecurity company SentinelOne has revealed that a China-nexus threat cluster dubbedPurpleHazeconducted reconnaissance attempts against its infrastructure and some of its high-value customers.

"We first became aware of this threat cluster during a 2024 intrusion conducted against an organization previously providing hardware logistics services for SentinelOne employees," security researchers Tom Hegel, Aleksandar Milenkoski, and Jim Waltersaidin an analysis published Monday.

PurpleHaze is assessed to be a hacking crew with loose ties to another state-sponsored group known asAPT15, which is also tracked as Flea, Nylon Typhoon (formerly Nickel), Playful Taurus, Royal APT, and Vixen Panda.

The adversarial collective has also been observed targeting an unnamed South Asian government-supporting entity in October 2024, employing an operational relay box (ORB) network and a Windows backdoor dubbed GoReShell.

The implant, written in the Go programming language, repurposes an open-source tool calledreverse_sshto set up reverse SSH connections to endpoints under the attacker's control.

"The use of ORB networks is a growing trend among these threat groups, since they can be rapidly expanded to create a dynamic and evolving infrastructure that makes tracking cyberespionage operations and their attribution challenging," the researchers pointed out.

Further analysis has determined that the same South Asian government entity was also targeted previously in June 2024 with ShadowPad (aka PoisonPlug), a known backdoor widely shared among China-nexus espionage groups. ShadowPad is considered to be a successor to another backdoor referred to as PlugX.

That said, with ShadowPad also being used as a conduit todeliver ransomwarein recent months, the exact motivation behind the attack remains unclear. The ShadowPad artifacts have been found to be obfuscated using a bespoke compiler calledScatterBrain.

The exact nature of the overlap between the June 2024 activity and the later PurpleHaze attacks is unknown as yet. However, it's believed that the same threat actor could be behind them.

The ScatterBrain-obfuscated ShadowPad is estimated to have been employed in intrusions targeting over 70 organizations spanning manufacturing, government, finance, telecommunications, and research sectors afterlikely exploitingan N-day vulnerability in Check Point gateway devices.

One among the victims of these attacks included the organization that was then responsible for managing hardware logistics for SentinelOne employees. However, the cybersecurity firm noted that it found no evidence of a secondary compromise.

It's not just China, for SentinelOne said it also observed attempts made byNorth Korea-aligned IT workersto secure jobs at the company, including its SentinelLabs intelligence engineering team, via approximately 360 fake personas and over 1,000 job applications.

Last but not least, ransomware operators have targeted SentinelOne and other enterprise-focused security platforms, attempting to gain access to their tools in order to evaluate the ability of their software to evade detection.

This is fuelled by an active underground economy that revolves around buying, selling, and renting access to such enterprise security offerings on messaging apps as well as forums like XSS[.]is, Exploit[.]in, and RAMP.

"Entire service offerings have emerged around this ecosystem, including 'EDR Testing-as-a-Service,' where actors can discreetly evaluate malware against various endpoint protection platforms," the researchers explained.

"While these testing services may not grant direct access to full-featured EDR consoles or agents, they do provide attackers with semi-private environments to fine-tune malicious payloads without the threat of exposure - dramatically improving the odds of success in real-world attacks."

One ransomware group that takes this threat to a whole new level is Nitrogen, which is believed to be run by a Russian national. Unlike typical approaches that involve approaching insiders or using legitimate credentials harvested from infostealer logs, Nitrogen adopts a different strategy by impersonating real companies.

This is achieved by setting up lookalike domains, spoofed email addresses, and cloned infrastructure that mimic legitimate companies, allowing the threat actor to purchase official licenses for EDR and other security products.

"This kind of social engineering is executed with precision," the researchers said. "Nitrogen typically targets small, lightly vetted resellers - keeping interactions minimal and relying on resellers' inconsistent KYC (Know Your Customer) practices to slip through the cracks."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Google Chrome Zero-Day CVE-2025-2783 Exploited by TaxOff to Deploy Trinper Backdoor

Classificações de Malware:

- cve (Exploit)
- backdoor (Backdoor)
- exploit (Exploit)
- rootkit (Rootkit)

- trojan (Trojan)
- dropper (Trojan)
- rat (Backdoor)
- virus (Virus)

Origem: pagina2.txt

A now-patched security flaw in Google Chrome was exploited as a zero-day by a threat actor known as TaxOff to deploy a backdoor codenamedTrinper.

The attack, observed in mid-March 2025 by Positive Technologies, involved the use of a sandbox escape vulnerability tracked as CVE-2025-2783 (CVSS score: 8.3).

Googleaddressedthe flaw later that month after Kaspersky reported in-the-wild exploitation in a campaign dubbed Operation ForumTroll targeting various Russian organizations.

"The initial attack vector was a phishing email containing a malicious link," security researchers Stanislav Pyzhov and Vladislav Luninsaid. "When the victim clicked the link, it triggered a one-click exploit (CVE-2025-2783), leading to the installation of the Trinper backdoor employed by TaxOff."

The phishing email is said to have been disguised as an invitation to the Primakov Readings forum - the same lure detailed by Kaspersky - urging users to click on a link that led to a fake website hosting the exploit.

TaxOff is the name assigned to ahacking groupthat was first documented by the Russian cybersecurity company in late November 2024 as targeting domestic government agencies using legal and finance-related phishing emails to deliver Trinper.

Written in C++, the backdoor makes use of multithreading to capture victim host information, record keystrokes, gather files matching specific extensions (.doc, .xls, .ppt, .rtf, and .pdf), and establish a connection with a remote server to receive commands and exfiltrate the results of the execution.

The instructions sent from the command-and-control (C2) server extend the implant's functionality, allowing it to read/write files, run commands using cmd.exe, launch a reverse shell, change directory, and shutdown itself.

"Multithreading provides a high degree of parallelism to hide the backdoor while retaining the ability to collect

and exfiltrate data, install additional modules, and maintain communications with C2," Lunin noted at the time.

Positive Technologies said its investigation into the mid-March 2025 intrusion led to the discovery of another attack dating back to October 2024 that also commenced with a phishing email, which purported to be an invitation to an international conference called "Security of the Union State in the modern world."

That email contained a link, which downloaded a ZIP archive file containing a Windows shortcut that, in turn, launched a PowerShell command to ultimately serve a decoy document while also dropping a loader responsible for launching the Trinper backdoor by means of the open-sourceDonutloader. A variation of the attack has been found to swap out the Donut loader in favor of Cobalt Strike.

This attack chain, per the company, shares several tactical similarities with that of another hacking group tracked asTeam46, raising the possibility that the two threat activity clusters are one and the same.

Interestingly, another set of phishing emails sent by the Team46 attackers a month before claimed to be from Moscow-based telecom operator Rostelecom, alerting recipients of supposed maintenance outages last year.

These emails included a ZIP archive, which embedded a shortcut that launched a PowerShell command to deploy a loader that had been previously used to deliver another backdoor in an attack targeting an unnamed Russian company in the rail freight industry.

The March 2024 intrusion,detailedby Doctor Web, is notable for the fact that one of the payloads weaponized a DLL hijacking vulnerability in Yandex Browser for Windows (CVE-2024-6473, CVSS score: 8.4) as a zero-day to download and execute unspecified malware. It wasresolvedin version 24.7.1.380 released in September 2024.

"This group leverages zero-day exploits, which enables it to penetrate secure infrastructures more effectively," the researchers said. "The group also creates and uses sophisticated malware, implying that it has a long-term strategy and intends to maintain persistence on the compromised systems for an extended period."

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Weekly Recap: iOS Zero-Days, 4Chan Breach, NTLM Exploits, WhatsApp Spyware & More

Classificações de Malware:

- spyware (Spyware)
- cve (Exploit)
- exploit (Exploit)

Origem: pagina20.txt

Can a harmless click really lead to a full-blown cyberattack?

Surprisingly, yes - and that's exactly what we saw in last week's activity. Hackers are getting better at hiding inside everyday actions: opening a file, running a project, or logging in like normal. No loud alerts. No obvious red flags. Just quiet entry through small gaps - like a misconfigured pipeline, a trusted browser feature, or reused login tokens. These aren't just tech issues - they're habits being exploited.

Let's walk through the biggest updates from the week and what they mean for your security.

Recently Patched Windows Flaw Comes Under Active Exploitation- A recently patched security flaw affectingWindows NTLM has been exploitedby malicious actors to leak NTLM hashes or user passwords and infiltrate systems since March 19, 2025. The flaw, CVE-2025-24054 (CVSS score: 6.5), is a hash disclosure spoofing bug that was fixed by Microsoft last month as part of its Patch Tuesday updates. The security flaw is assessed to be a variant of CVE-2024-43451 (CVSS score: 6.5), which was patched by Microsoft in November 2024 and has also been weaponized in the wild in attacks targeting Ukraine and Colombia by threat actors like UAC-0194 and Blind Eagle.

Companies need to rethink how they protect their private and public use of AI and how they defend against AI-powered attacks. Traditional firewalls, VPNs, and public-facing IPs expose your attack surface and are no match in the AI era. It's time for a modern approach with Zscaler Zero Trust + AI.

Attackers love software vulnerabilities-they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.

This week's list includes -CVE-2025-2492(ASUS),CVE-2025-24054(Microsoft Windows),CVE-2025-32433(Erlang/OTP),CVE-2021-20035(SonicWall Secure Mobile Access 100 Series),CVE-2025-31200, CVE-2025-31201(Apple iOS, iPadOS, macOS Sequoia, tvOS, and visionOS),CVE-2025-24859(Apache Roller),CVE-2025-1093(AIHub theme), andCVE-2025-3278(UrbanGo Membership plugin).

Stop Spam Before It Starts: Use Burner Emails the Smart Way- Most people use the same email everywhere - but when one company leaks or sells your address, your inbox starts filling with spam or phishing emails. A smarter way is to use a burner email system, where you give each company a unique email like netflix@yourdomain.com. To do this, buy a cheap domain (like myaliashub.com) and set up free forwarding with services like ImprovMX or SimpleLogin. Every email sent to any name on that domain will land in your main inbox. If one starts getting spam, just delete or block it - problem solved, no need to change your real email.

If you use Gmail, you can add +something after your name, like alex+uber@gmail.com, and Gmail will still deliver it. This helps you track who shared your email and set filters, but it's not very private since your real email is still visible. Some websites also block + emails. A better long-term option is to connect a custom domain to Gmail through Google Workspace, which gives you real aliases like shop@yourdomain.com with full control and spam filtering.

Apple users can use Hide My Email (built into iOS and macOS). It creates a random email like x2k4@privaterelay.appleid.com for each website, and forwards messages to your iCloud inbox. You can disable or delete these anytime. It's great for signups, subscriptions, or trials where you don't want to share your real email. For even more control, Apple lets you use custom domains too. These tools help you stay organized, stop spam early, and quickly trace any leaks - all without needing to change your main email ever again.

This week made it clear: attackers aren't just hunting for big holes - they're slipping through tiny cracks we barely notice. An outdated security setting. A forgotten endpoint. A tool used slightly out of spec. And just like

that, they're in. We're seeing more cases where the compromise isn't about breaking in - it's about being invited in by accident. As systems grow more connected and automated, even the smallest misstep can open a big door.

Stay sharp, stay curious - and double-check the things you think are "too minor to matter."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Weekly Recap: Windows 0-Day, VPN Exploits, Weaponized AI, Hijacked Antivirus and More

Classificações de Malware:

- ransomware (Ransomware)
- cve (Exploit)
- exploit (Exploit)
- trojan (Trojan)
- builder (Backdoor)
- stealth (Rootkit)
- backdoor (Backdoor)
- rootkit (Rootkit)

Origem: pagina21.txt

Attackers aren't waiting for patches anymore - they are breaking in before defenses are ready. Trusted security tools are being hijacked to deliver malware. Even after a breach is detected and patched, some attackers stay hidden.

This week's events show a hard truth: it's not enough to react after an attack. You have to assume that any system you trust today could fail tomorrow. In a world where AI tools can be used against you and ransomware hits faster than ever, real protection means planning for things to go wrong - and still staying in

control.

Check out this week's update to find important threat news, helpful webinars, useful tools, and tips you can start using right away.

Windows 0-Day Exploited for Ransomware Attacks- A security affecting the Windows Common Log File System (CLFS) wasexploitedas a zero-day in ransomware attacks aimed at a small number of targets, Microsoft revealed. The flaw, CVE-2025-29824, is a privilege escalation vulnerability that could allow an attacker to obtain SYSTEM privileges. An exploit for the vulnerability has been found to be delivered via a trojan called PipeMagic, with the unknown threat actors, tracked by Microsoft as Storm-2460, conducting credential harvesting and dropping a ransomware payload as part of post-compromise exploitation activities. The exact nature of the payload is unclear, however, the ransom note dropped after encryption included a TOR domain tied to the RansomEXX ransomware family. CVE-2025-29824 wasaddressedby Microsoft as part of its Patch Tuesday update for April 2025.

In cloud-native environments, the security of your code repositories and development pipelines is critical. Do you know the most pressing risks facing your organization today? By analyzing hundreds of thousands of repositories, the Wiz Threat Research team uncovered key vulnerabilities and attacker strategies in the new2025 State of Code Security Report.

Key stats include:

Download the report to explore all the findings in detail and learn actionable strategies to protect your organization.

Attackers love software vulnerabilities-they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.

This week's list includes -CVE-2025-3102(OttoKit plugin),CVE-2025-23359(NVIDIA Container Toolkit),CVE-2025-30406(Gladinet CentreStack),CVE-2025-29824(Windows Common Log File System),CVE-2024-48887(Fortinet FortiSwitch),CVE-2024-53150, CVE-2024-53197(Google Android),CVE-2025-2945(pgAdmin),CVE-2025-2244(Bitdefender

GravityZone),CVE-2025-31334(WinRAR),CVE-2025-30401(WhatsApp for Windows),CVE-2025-23120(Rockwell Automation Industrial Data Center),CVE-2025-25211,CVE-2025-26689(Inaba Denki Sangyo CHOCO TEI WATCHER),CVE-2024-4872,CVE-2024-3980(Hitachi Energy MicroSCADA Pro/X SYS600),CVE-2025-2636(InstaWP Connect - 1-click WP Staging & Migration plugin),CVE-2025-3439(Everest Forms - Contact Form, Quiz, Survey, Newsletter & Payment Form Builder for WordPress plugin), andCVE-2025-31565(WPSmartContracts plugin).

1Learn to Detect and Block Hidden AI Tools in Your SaaS Stack- AI tools are quietly connecting to your SaaS apps - often without Security's knowledge. Sensitive data is at risk. Manual tracking won't keep up.

In this session, learn:

Join Dvir Sasson from Reco to get ahead ofhidden AI threats.

2Learn How to Secure Every Step of Your Identity Lifecycle- Identity is your new attack surface. AI-powered impersonation and deepfakes are breaking traditional defenses. Learn how to secure the full identity lifecycle - from enrollment to daily access to recovery - with phishing-resistant MFA, device trust, and Deepfake Defense.

Join Beyond Identity and Nametag tostop account takeoversbefore they start.

Monitoring for Unauthorized Account Activations- Attackers are using a clever trick to stay hidden inside networks: reactivating the built-in Windows Guest account. Normally, this account is disabled and ignored by system admins. But when attackers enable it and set a new password, it blends in as part of the system - making it easy for them to quietly log in, escalate privileges, and even access devices remotely through RDP. Since the Guest account looks normal at first glance, many security teams miss it during reviews.

To catch this tactic early, monitor your security logs closely. Set alerts for Event ID 4722 - this signals when any disabled account is reactivated, including Guest. Also track the use of native Windows tools like net.exe, wmic, and PowerShell for any commands that modify accounts. Pay special attention to any Guest account being added to privileged groups like Administrators or Remote Desktop Users. Cross-check with your endpoint protection or EDR tools to spot changes outside normal maintenance windows.

If you find an active Guest account, assume it's part of a larger breach. Check for signs of hidden accounts, unauthorized remote access tools, and changes to RDP settings. Regular threat hunting - even just checking that all default accounts are truly disabled - can break an attacker's persistence before they move deeper into your environment.

Every breach, every evasion technique, and every new tool attackers use is also a learning opportunity. If you're in cybersecurity today, your advantage isn't just your tech stack - it's how quickly you adapt.

Take one tactic you saw in this week's update - privilege escalation, AI misuse, stealth persistence - and use it as a reason to strengthen a weak spot you've been putting off. Defense is a race, but improvement is a choice.

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: Iran Slows Internet to Prevent Cyber Attacks Amid Escalating Regional Conflict

Classificações de Malware:

- crypto (Ransomware)
- ransomware (Ransomware)
- exploit (Exploit)
- cve (Exploit)
- trojan (Trojan)
- dropper (Trojan)
- backdoor (Backdoor)
- rootkit (Rootkit)
- rat (Backdoor)
- virus (Virus)

Origem: pagina3.txt

Iran has throttled internet access in the country in a purported attempt to hamper Israel's ability to conduct covert cyber operations, days after the latter launched an unprecedented attack on the country, escalating geopolitical tensions in the region.

Fatemeh Mohajerani, the spokesperson of the Iranian Government, and the Iranian Cyber Police, FATA,saidtheinternet slowdownwasdesignedto maintain internet stability and that the move is "temporary, targeted, and controlled, to ward off cyber attacks." Datasharedby NetBlocks shows a "significant reduction in internet traffic" around 5:30 p.m. local time.

The development comes amid deepening conflict, with Israel and Iran trading missile attacks since Friday. These attacks have spilled over into cyberspace, as security experts warned of retaliatory cyber operations by Iranian state actors and hacktivist groups.

The digital warfare unfolding behind the scenes goes two ways. Earlier this week, a pro-Israeli group known asPredatory Sparrowclaimed responsibility for a cyber attack on Iran's Bank Sepah,crippling accessto its website and ATMs.

"'Bank Sepah' was an institution thatcircumvented international sanctionsand used the people of Iran's money to finance the regime's terrorist proxies, its ballistic missile program, and its military nuclear program," the groupsaidin a public statement posted on X.

Predatory Sparrow also said it sabotaged the bank's infrastructure with help from "brave Iranians," adding "this is what happens to institutions dedicated to maintaining the dictator's terrorist fantasies." Israel has a storied history ofsophisticatedcyber operations, most notably theStuxnetattack targeting Iran's nuclear program.

Tel Aviv-based cybersecurity firm Radwaresaidit has observed heightened activity from threat actors affiliated with Iran across public and private Telegram channels.

Some of the groups, including Mysterious Team Bangladesh and Arabian Ghost, have warned neighboring countries Jordan and Saudi Arabia against supporting Israel and claimed to have shut down Israeli radio stations.

Furthermore, the Iranian government has urged citizens to delete WhatsApp, one of the country's most

popular messaging platforms, stating without giving any evidence that the Meta-owned app has been weaponized by Israel to spy on its users.

WhatsApp has denied the allegations. In astatementto the Associated Press, the company said it does not track users nor does it provide "bulk information to any government."

The cyber conflict also follows an announcement from the U.S. Department of State that they were seeking information on Iranian hackers who they accused of targeting critical infrastructure in the U.S., Israel, and other countries using theIOCONTROL(aka OrpaCrab) malware to breach Industrial Control Systems (ICS).

"Cyber Av3ngers, which is associated with the online persona Mr. Soul, has launched a series of malicious cyber activities against U.S. critical infrastructure on behalf of Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC)," the department's Rewards for Justice (RFJ) programsaid.

"Cyber Av3ngers actors have utilized malware known as IOCONTROL to target ICS/SCADA devices used by critical infrastructure sectors in the United States and worldwide."

On June 18, Predatory Sparrowsaidit was behind a cyber attack on Iranian cryptocurrency exchange Nobitex. The hacktivist collective also said they would publish the platform's source code and data from its internal network within 24 hours.

"The Nobitex exchange is at the heart of the regime's efforts to finance terror around the world," the group said. "This exchange is the regime's most popular tool for circumventing international sanctions."

In a security alert, Nobitexsaidit suspended all access after it detected "signs of unauthorized access to a portion of our reporting infrastructure and hot wallet." It further reassured users that all of their assets are secure and that it would compensate for all damages.

According to blockchain investigator ZachXBT, around $81.7 million worth of digital assets werestolenfrom the exchange across Tron, EVM and BTC chains. "The attacker used the vanity address TKFuckiRGCTerroristsNoBiTEXy2r7mNX," ZachXBTsaidin a post on Telegram.

Blockchain analysis firm Elliptic said the hackers "burned" the stolen funds by sending them to inaccessible wallets, effectively pulling the assets out of circulation. It also noted that it identified the use of Nobitex by

sanctioned operatives from the Iranian Islamic Revolutionary Guard Corps (IRGC).

"The hack also does not appear to be financially motivated," Ellipticsaid. "The vanity addresses used by the hackers are generated through 'brute-force' methods - involving the creation of large numbers of cryptographic key pairs until one contains the desired text."

"But creating vanity addresses with text strings as long as those used in this hack is computationally infeasible. This means that Predatory Sparrow would not have the private keys for the crypto addresses they sent the Nobitex funds to, and have effectively burned the funds in order to send Nobitex a political message."

On June 19, 2024, the pro-Israel grouppreleasedwhat it said was Nobitex's "full source code," after it's said to have stolen over $90 million in digital currency from the crypto exchange. Nobitex, in a series of posts on X, said the total value of stolen assets is estimated to be around $100 million.

"The stolen assets were transferred to a wallet with a non-standard address composed of arbitrary characters - an approach that deviates significantly from conventional crypto exchange hacks," the companysaid, noting that the "situation is now under control."

"These wallets were used to burn and destroy user assets. It is clear that the intention behind this attack was to harm the peace of mind and assets of our fellow citizens under false pretenses."

Nobitex has sincesaidthe "scope and impact of the attack are more complex than initially estimated," and pointed out that the current internet disruptions in the country and its limited on-site access due to the conflict have impacted its response efforts.

Título: Iranian APT35 Hackers Targeting Israeli Tech Experts with AI-Powered Phishing Attacks

Classificações de Malware:

- keylogger (Spyware)
- spyware (Spyware)
- ransomware (Ransomware)
- crypto (Ransomware)
- trojan (Trojan)
- trojanized (Trojan)
- virus (Virus)
- infected (Virus)
- infection (Virus)
- exploit (Exploit)
- cve (Exploit)
- dropper (Trojan)
- backdoor (Backdoor)

Origem: pagina4.txt

An Iranian state-sponsored hacking group associated with the Islamic Revolutionary Guard Corps (IRGC) has been linked to a spear-phishing campaign targeting journalists, high-profile cyber security experts, and computer science professors in Israel.

"In some of those campaigns, Israeli technology and cyber security professionals were approached by attackers who posed as fictitious assistants to technology executives or researchers through emails and WhatsApp messages," Check Pointsaidin a report published Wednesday. "The threat actors directed victims who engaged with them to fake Gmail login pages or Google Meet invitations."

The cybersecurity company attributed the activity to a threat cluster it tracks asEducated Manticore, which overlaps with APT35 (and its sub-clusterAPT42), CALANQUE, Charming Kitten, CharmingCypress, Cobalt Illusion, ITG18, Magic Hound, Mint Sandstorm (formerly Phosphorus), Newscaster, TA453, and Yellow Garuda.

The advanced persistent threat (APT) group has alonghistoryoforchestrating social engineering attacksusing elaborate lures, approaching targets on various platforms like Facebook and LinkedIn using fictitious

personas to trick victims into deploying malware on their systems.

Check Point said it observed a new wave of attacks starting mid-June 2025 following theoutbreak of the Iran-Israel warthat targeted Israeli individuals using fake meeting decoys, either via emails or WhatsApp messages tailored to the targets. It's believed that the messages are crafted using artificial intelligence (AI) tools due to the structured layout and the absence of any grammatical errors.

One of the WhatsApp messages flagged by the company took advantage of the current geopolitical tensions between the two countries to coax the victim into joining a meeting, claiming they needed their immediate assistance on an AI-based threat detection system to counter a surge in cyber attacks targeting Israel since June 12.

The initial messages, like those observed in previous Charming Kitten campaigns, are devoid of any malicious artifacts and are primarily designed to gain the trust of their targets. Once the threat actors build rapport over the course of the conversation, the attack moves to the next phase by sharing links that direct the victims to fake landing pages capable of harvesting their Google account credentials.

"Before sending the phishing link, threat actors ask the victim for their email address," Check Point said. "This address is then pre-filled on the credential phishing page to increase credibility and mimic the appearance of a legitimate Google authentication flow."

"The custom phishing kit [...] closely imitates familiar login pages, like those from Google, using modern web technologies such as React-based Single Page Applications (SPA) and dynamic page routing. It also uses real-time WebSocket connections to send stolen data, and the design allows it to hide its code from additional scrutiny."

The fake page is part of a custom phishing kit that can not only capture their credentials, but also two-factor authentication (2FA) codes, effectively facilitating 2FA relay attacks. The kit also incorporates a passive keylogger to record all keystrokes entered by the victim and exfiltrate them in the event the user abandons the process midway.

Some of the social engineering efforts have also involved the use of Google Sites domains to host bogus Google Meet pages with an image that mimics the legitimate meeting page. Clicking anywhere on the image directs the victim to phishing pages that trigger the authentication process.

"Educated Manticore continues to pose a persistent and high-impact threat, particularly to individuals in Israel during the escalation phase of the Iran-Israel conflict," Check Point said.

"The group continues to operate steadily, characterized by aggressive spear-phishing, rapid setup of domains, subdomains, and infrastructure, and fast-paced takedowns when identified. This agility allows them to remain effective under heightened scrutiny."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: New Chrome Zero-Day Actively Exploited; Google Issues Emergency Out-of-Band Patch

Classificações de Malware:

- exploit (Exploit)
- cve (Exploit)
- virus (Virus)
- infected (Virus)
- trojan (Trojan)
- adware (Adware)
- ads (Adware)
- backdoor (Backdoor)
- rat (Backdoor)
- ransomware (Ransomware)
- crypto (Ransomware)
- trojanized (Trojan)
- infection (Virus)

Origem: pagina5.txt

Google on Monday released out-of-band fixes to address three security issues in its Chrome browser, including one that it said has come under active exploitation in the wild.

The high-severity flaw is being tracked asCVE-2025-5419(CVSS score: 8.8), and has been flagged as an out-of-bounds read and write vulnerability in the V8 JavaScript and WebAssembly engine.

"Out-of-bounds read and write in V8 in Google Chrome prior to 137.0.7151.68 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page," reads thedescriptionof the bug on the NIST's National Vulnerability Database (NVD).

Google credited Clement Lecigne and Benot Sevens of Google Threat Analysis Group (TAG) with discovering and reporting the flaw on May 27, 2025. It also noted that the issue was addressed the next day by pushing out a configuration change to the Stable version of the browser across all platforms.

As is customary, the advisory is light on details regarding the nature of the attacks leveraging the vulnerability or the identity of the threat actors perpetrating them. This is done so to ensure that a majority of users are updated with a fix and to prevent other bad actors from joining the exploitation bandwagon.

"Google is aware that an exploit for CVE-2025-5419 exists in the wild," the tech giantacknowledged.

CVE-2025-5419 is the second actively exploited zero-day to be patched by Google this year afterCVE-2025-2783(CVSS score: 8.3), which was identified by Kaspersky as being weaponized in attacks targeting organizations in Russia.

Users are recommended to upgrade to Chrome version 137.0.7151.68/.69 for Windows and macOS, and version 137.0.7151.68 for Linux to safeguard against potential threats. Users of Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi are also advised to apply the fixes as and when they become available.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: New Malware Campaign Uses Cloudflare Tunnels to Deliver RATs via Phishing Chains

Classificações de Malware:

- trojan (Trojan)
- rat (Backdoor)
- stealth (Rootkit)
- virus (Virus)
- infected (Virus)
- backdoor (Backdoor)
- ransomware (Ransomware)
- infection (Virus)
- adware (Adware)
- ads (Adware)

Origem: pagina6.txt

A new campaign is making use of Cloudflare Tunnel subdomains to host malicious payloads and deliver them via malicious attachments embedded in phishing emails.

The ongoing campaign has been codenamedSERPENTINE#CLOUDby Securonix.

It leverages "the Cloudflare Tunnel infrastructure and Python-based loaders to deliver memory-injected payloads through a chain of shortcut files and obfuscated scripts," security researcher Tim Pecksaidin a report shared with The Hacker News.

The attack starts with sending payment- or invoice-themed phishing emails bearing a link to a zipped document that contains a Windows shortcut (LNK) file. These shortcuts are disguised as documents to trick victims into opening them, effectively activating the infection sequence.

The elaborate multi-step process culminates in the execution of a Python-based shellcode loader that executes payloads packed with the open-source Donut loader entirely in memory.

Securonix said the campaign has targeted the United States, United Kingdom, Germany, and other regions

across Europe and Asia. The identity of the threat actor(s) behind the campaign is presently unknown, although the cybersecurity company pointed out their English fluency.

Thethreat activity clusteris also notable for its shifting initial access methods, pivoting from internet shortcut (URL) files to using LNK shortcut files masquerading as PDF documents. These payloads are then used to retrieve additional stages over WebDAV via the Cloudflare Tunnel subdomains.

It's worth mentioning here that avariation of this campaignwas previously documented by eSentire and Proofpoint last year, with the attacks paving the way for AsyncRAT, GuLoader, PureLogs Stealer, Remcos RAT, Venom RAT, and XWorm.

"While the infrastructure and delivery mechanics are very similar, there is definitely evidence to suggest that the SERPENTINE#CLOUD campaign could be a continuation of a prior campaign, though with notable differences," Peck told the Hacker News.

"The differences in payload complexity and targeting suggest they may be unrelated or represent distinct threat actors converging on a popular tactic that simply works."

Some of these differences include the use of extensive code obfuscation, additional stages to help it slide under the radar, and the deployment of Python shellcode loaders to deliver the main payloads, as opposed to directly serving commodity malware.

"Given the similarities, it's possible that the same threat actors behind it have retooled and modernized their attack chain, or it's possible that this could be an entirely different threat actor who is capitalizing on known attack chains that prove effective," Peck added.

The abuse of TryCloudflare offers manifold advantages. For starters, malicious actors have long made it harder to detect by using legitimate cloud service providers as a front for their operations, including payload delivery and command-and-control (C2) communication.

By using a reputable subdomain ("*.trycloudflare[.]com") for nefarious ends, it makes it exceedingly tough for defenders to distinguish between harmful and benign activities, thereby allowing it to evade URL or domain-based blocking mechanisms.

Furthermore, it obviates the need to register domains or rent VPS servers, as well as allows the attackers to host malicious content on a local machine and expose them to the public internet with a temporary "*.trycloudflare[.]com" subdomain.

The initial infection occurs when the LNK files are launched, causing it to download a next-stage payload, a Windows Script File (WSF), from a remote WebDAV share hosted on a Cloudflare Tunnel subdomain. The WSF file is subsequently executed using cscript.exe in a manner without arousing the victim's suspicion.

"This WSF file functions as a lightweight VBScript-based loader, designed to execute an external batch file from a second Cloudflare domain," Peck said. "The 'kiki.bat' file serves as the main payload delivery script next in the series of stagers. Overall, it's designed for stealth and persistence."

The primary responsibility of the batch script is to display a decoy PDF document, check for antivirus software, and download and execute Python payloads, which are then used to run Donut-packed payloads like AsyncRAT or Revenge RAT in memory.

Securonix said there is a possibility that the script may have been vibe-coded using a large language model owing to the presence of well-defined comments in the source code.

"The SERPENTINE#CLOUD campaign is a complex and layered infection chain that blends a bit of social engineering, living-off-the-land techniques, and evasive in-memory code execution," the company concluded. "The abuse of Cloudflare Tunnel infrastructure further complicates network visibility by giving the actor a disposable and encrypted transport layer for staging malicious files without maintaining traditional infrastructure."

The disclosure comes as Acronis identified an active malware campaign dubbedShadow Vectortargeting users in Colombia using booby-trapped scalable vector graphics (SVG) files as the malware delivery vector in phishing emails that impersonate court notifications.

"Attackers distributed spear-phishing emails impersonating trusted institutions in Colombia, delivering SVG decoys with embedded links to JS / VBS stagers hosted on public platforms, or password-protected ZIP files containing the payloads directly," Acronis researchers Santiago Pontiroli, Jozsef Gegeny, and Ilia Dafchevsaid.

The attacks led to the deployment of remote access trojans likeAsyncRATandRemcos RAT, with recent campaigns also utilizing a .NET loader associated withKatz Stealer. These attack chains involve hiding the payloads within Base64-encoded text of image files hosted on the Internet Archive.

A noteworthy aspect of the campaign is the use ofSVG smugglingtechniques to deliver malicious ZIP archives using SVG files. These payloads are hosted on file-sharing services such as Bitbucket, Dropbox, Discord, and YDRAY. The download archives contain both legitimate executables and malicious DLLs, the latter of which are sideloaded to ultimately serve the trojans.

"A natural evolution from its earlier SVG smuggling techniques, this threat actor has adopted a modular, memory-resident loader that can execute payloads dynamically and entirely in memory, leaving minimal traces behind," the researchers said.

"The presence of Portuguese-language strings and method parameters within the loader mirrors TTPs commonly observed in Brazilian banking malware, suggesting potential code reuse, shared development resources or even cross-regional actor collaboration."

The findings also coincide with a rise in social engineering attacks that employ theClickFixtactic to deploy stealers and remote access trojans like Lumma Stealer and SectopRAT under the guise of fixing an issue or completing a CAPTCHA verification.

According to statistics shared by ReliaQuest, drive-by compromises accounted for 23% of all phishing-based tactics observed between March and May 2025. "Techniques like ClickFix were central to drive-by downloads," the cybersecurity companysaid.

ClickFix is effective primarily because it deceives targets into carrying out seemingly harmless, everyday actions that are unlikely to raise any red flags, because they're so used to seeing CAPTCHA screening pages and other notifications. What makes it compelling is that it gets users to do the main work of infecting their own machines instead of having to resort to more sophisticated methods like exploiting software flaws.

"External remote resources dropped from third to fourth place as attackers increasingly exploit user mistakes rather than technical vulnerabilities," ReliaQuest said. "This shift is likely driven by the simplicity, success rate, and universal applicability of social engineering campaigns like ClickFix."

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.

Título: New Supply Chain Malware Operation Hits npm and PyPI Ecosystems, Targeting Millions Globally

Classificações de Malware:

- trojan (Trojan)
- trojanized (Trojan)
- infection (Virus)
- backdoor (Backdoor)
- rat (Backdoor)
- rootkit (Rootkit)
- stealth (Rootkit)
- ransomware (Ransomware)
- exploit (Exploit)
- virus (Virus)
- adware (Adware)
- ads (Adware)

Origem: pagina7.txt

Cybersecurity researchers haveflaggeda supply chain attack targeting over a dozen packages associated with GlueStack to deliver malware.

The malware, introduced via a change to "lib/commonjs/index.js," allows an attacker to run shell commands, take screenshots, and upload files to infected machines, Aikido Security told The Hacker News, stating these packages collectively account for nearly 1 million weekly downloads.

The unauthorized access could then be used to perform various follow-on actions like mining cryptocurrency, stealing sensitive information, and even shutting down services. Aikido said the first package compromise

was detected on June 6, 2025, at 9:33 p.m. GMT.

The list of the impacted packages and the affected versions is below -

Furthermore, the malicious code injected into the packages issimilarto the remote access trojan that was delivered following the compromise of another npm package "rand-user-agent" last month, indicating that the same threat actors could be behind the activity.

The trojan is an updated version that supports two new commands to harvest system information ("ss_info") and the public IP address of the host ("ss_ip").

The project maintainers have sincerevoked the access tokenand marked the impacted versions as deprecated. Users who may have downloaded the malicious versions are recommended to roll back to a safe version to mitigate any potential threats.

"The potential impact is massive in scale, and the malware's persistence mechanism is particularly concerning - attackers maintain access to infected machines even after maintainers update the packages," the company said in a statement.

However, in an incident report published on June 9, 2025, the project maintainers acknowledged that a public access token associated with one of their contributors was compromised, thereby allowing threat actors to publish tampered versions of react-native-aria packages along with a @gluestack-ui/utils package to npm.

"The compromised package was published by a compromised account of an authorized maintainer," Suraj Ahmed Choudhurysaid. "React Native ARIA is a frontend-only library. It does not execute any code in CLI or scripts post-install, meaning the likelihood of the malicious code executing on user systems is extremely low to none. Based on our current understanding and usage patterns, no system-level compromises are expected."

The maintainers also said they have also revoked GitHub repository access for all non-essential contributors, and enabled two-factor authentication (2FA) for publishing and GitHub access.

The development comes as Socket discovered two rogue npm packages - express-api-sync and system-health-sync-api - that masquerade as legitimate utilities but implant wipers that can delete entire

application directories.

Published by the account "botsailer" (email: anupm019@gmail[.]com), the packages were downloaded 112 and 861 times, respectively, before being taken down.

The first of the two packages, express-api-sync, claims to be an Express API to sync data between two databases. However, once installed and added by an unsuspecting developer to their application, it triggers the execution of malicious code upon receiving an HTTP request with a hard-coded key "DEFAULT_123."

Upon receipt of the key, it executes the Unix command "rm -rf *" to recursively delete all files from the current directory and below, including source code, configuration files, assets, and local databases.

The other package is a lot more sophisticated, acting both as an information stealer and a wiper, while also modifying its deletion commands based on whether the operating system is Windows ("rd /s /q .") or Linux ("rm -rf *").

"Where express-api-sync is a blunt instrument, system-health-sync-api is a Swiss Army knife of destruction with built-in intelligence gathering," security researcher Kush Pandyasaid.

A notable aspect of the npm package is that it uses email as a covert communication channel, connecting to the attacker-controlled mailbox via hard-coded SMTP credentials. The password is obfuscated using Base64-encoding, whereas the username points to an email address with a domain that's associated with a real estate agency based in India ("auth@corehomes[.]in").

"Every significant event triggers an email to anupm019@gmail[.]com," Socket said. "The email includes the full backend URL, potentially exposing internal infrastructure details, development environments, or staging servers that shouldn't be publicly known."

The use of SMTP for data exfiltration is sneaky as most firewalls do not block outbound email traffic, and allows malicious traffic to blend in with legitimate application emails.

Furthermore, the package resisters endpoints at "/_/system/health" and "/_/sys/maintenance" to unleash the platform-specific destruction commands, with the latter acting as a fallback mechanism in case the main backdoor is detected and blocked.

"Attackers first verify the backdoor via GET /_/system/health which returns the server's hostname and status," Pandya explained. "They can test with dry-run mode if configured, then execute destruction using POST /_/system/health or the backup POST /_/sys/maintenance endpoint with the key "HelloWorld."

The discovery of the two new npm packages shows that threat actors are beginning to branch out beyond using bogus libraries for information and cryptocurrency theft to focus on system sabotage -- something of an unusual development as they offer no financial benefits.

It also comes as the software supply chain security firm discovered a new Python-based credential harvester imad213 on the Python Package Index (PyPI) repository that claims to be an Instagram growth tool. According to statistics published on pepy.tech, the package has been downloaded 3,242 times.

"The malware uses Base64-encoding to hide its true nature and implements a remote kill switch through a Netlify-hosted control file," Pandyasaid. "When executed, it prompts users for Instagram credentials, and broadcasts them to ten different third-party bot services while pretending to boost follower counts."

The Python library has been uploaded by a user namedim_ad__213(aka IMAD-213), who joined the registry on March 21, 2025, and has uploaded three other packages that can harvest Facebook, Gmail, Twitter, and VK credentials (taya, a-b27) or leverage Apache Bench to target streaming platforms and APIs with distributed denial-of-service (DDoS) attacks (poppo213).

The list of packages, which are still available for download from PyPI, is below -

In a GitHub README.md document published by IMAD-213 about two days before "imad213" was uploaded to PyPI, the threat actorclaimsthat the library is mainly for "educational and research purposes" and notes that they are not responsible for any misuse.

The GitHub description also includes a "deceptive safety tip," urging users to utilize a fake or temporary Instagram account to avoid running into any issues with their main account.

"This creates false security, users think they're being cautious while still handing over valid credentials to the attacker," Pandya said.

Once launched, the malware connects to an external server and reads a text file ("pass.txt") and proceeds further with the execution only if the file content matches the string "imad213." The kill switch can serve multiple purposes, allowing the threat actor to determine who gets access to run the library or turn off every downloaded copy by simply changing the context of the control file.

In the next step, the library prompts the user to enter their Instagram credentials, which are then saved locally in a file named "credentials.txt" and broadcast to ten different dubious bot service websites, some of which link to a network of Turkish Instagram growth tools likely operated by the same entity. The domains were registered in June 2021.

"The emergence of this credential harvester reveals concerning trends in social media-targeted malware," Socket said. "With ten different bot services receiving credentials, we're seeing the early stages of credential laundering - where stolen logins are distributed across multiple services to obscure their origin."

Título: SonicWall NetExtender Trojan and ConnectWise Exploits Used in Remote Access Attacks

Classificações de Malware:

- cve (Exploit)
- trojan (Trojan)
- trojanized (Trojan)
- virus (Virus)
- infection (Virus)
- exploit (Exploit)
- backdoor (Backdoor)

Origem: pagina8.txt

Unknown threat actors have been distributing a trojanized version of SonicWall's SSL VPN NetExtender application to steal credentials from unsuspecting users who may have installed it.

"NetExtender enables remote users to securely connect and run applications on the company network," SonicWall researcher Sravan Ganacharisaid. "Users can upload and download files, access network drives, and use other resources as if they were on the local network."

The malicious payload delivered via the rogue VPN software has been codenamedSilentRouteby Microsoft, which detected the campaign along with the network security company.

SonicWall said the malware-laced NetExtender impersonates the latest version of the software (10.3.2.27) and has been found to be distributed via a fake website that has since been taken down. The installer is digitally signed by CITYLIGHT MEDIA PRIVATE LIMITED."

This suggests that the campaign is targeting users searching for NetExtender on search engines like Google or Bing, and tricking them into installing it through spoofed sites propagated via known techniques like spear-phishing, search engine optimization (SEO) poisoning, malvertising, or social media posts.

Two different components of the installer have been modified to facilitate the exfiltration of the configuration information to a remote server under the attacker's control.

These include "NeService.exe" and "NetExtender.exe," which have been altered to bypass the validation of digital certificates various NetExtender components and continue execution regardless of the validation results and exfiltrate the information to 132.196.198[.]163 over port 8080.

"The threat actor added code in the installed binaries of the fake NetExtender so that information related to VPN configuration is stolen and sent to a remote server," Ganachari said.

"Once the VPN configuration details are entered and the "Connect" button is clicked, the malicious code performs its own validation before sending the data to the remote server. Stolen configuration information includes the username, password, domain, and more."

The development comes as G DATA detailed a threat activity cluster dubbed EvilConwi that involves bad actors abusing ConnectWise to embed malicious code using a technique calledauthenticodestuffing without

invalidating the digital signature.

The German cybersecurity companysaidit has observed a spike in attacks using this technique since March 2025. The infection chains primarily leverage phishing emails as an initial access vector or through bogus sites advertised as artificial intelligence (AI) tools on Facebook.

These email messages contain a OneDrive link that redirects recipients to a Canva page with a "View PDF" button, which results in the surreptitious download and execution of a ConnectWise installer.

The attacks work by implanting malicious configurations in unauthenticated attributes within the Authenticode signature to serve a fake Windows update screen and prevent users from shutting down their systems, as well as including information about the external URL to which the remote connection should be established for persistent access.

What makes EvilConwi notable is that it offers malicious actors a cover for nefarious operations by conducting them using a trusted, legitimate, and maybe elevated system or software process, thereby allowing them to fly under the radar. ConnectWise has since revoked the certificate used to sign these binaries.

"By modifying these settings, threat actors create their own remote access malware that pretends to be a different software like an AI-to-image converter by Google Chrome," security researcher Karsten Hahn said. "They commonly add fake Windows update images and messages too, so that the user does not turn off the system while threat actors remotely connect to them."

Título: Weekly Recap: APT Intrusions, AI Malware, Zero-Click Exploits, Browser Hijacks and

More

Classificações de Malware:

- spyware (Spyware)
- cve (Exploit)
- ads (Adware)
- exploit (Exploit)
- ransomware (Ransomware)

Origem: pagina9.txt

If this had been a security drill, someone would've said it went too far. But it wasn't a drill-it was real. The access? Everything looked normal. The tools? Easy to find. The detection? Came too late.

This is how attacks happen now-quiet, convincing, and fast. Defenders aren't just chasing hackers anymore-they're struggling to trust what their systems are telling them.

The problem isn't too few alerts. It's too many, with no clear meaning. One thing is clear: if your defense still waits for obvious signs, you're not protecting anything. You're just watching it happen.

This recap highlights the moments that mattered-and why they're worth your attention.

APT41 Exploits Google Calendar for Command-and-Control- The Chinese state-sponsored threat actor known as APT41 deployed a malware called TOUGHPROGRESS that uses Google Calendar for command-and-control (C2). Google said it observed the spear-phishing attacks in October 2024 and that the malware was hosted on an unspecified compromised government website. TOUGHPROGRESS is designed to read and write events with an attacker-controlled Google Calendar, and extract the commands specified in them for subsequent execution. The results of the execution are written back to another Calendar event from where they can be accessed by the attackers. The campaign targeted multiple other government entities, although the company did not name the organizations that were singled out.

With a Zero Trust Everywhere security approach, organizations free themselves from firewalls and other network-centric appliances. They unify security and policy across all users, all locations, and all devices, drastically reducing cost and complexity.

Attackers love software vulnerabilities - they're easy doors into your systems. Every week brings fresh flaws,

and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.

This week's list includes -CVE-2025-3935(ConnectWise ScreenConnect),CVE-2025-47577(TI WooCommerce Wishlist plugin),CVE-2025-2760,CVE-2025-2761(GIMP),CVE-2025-0072(Arm Mali GPU),CVE-2025-27462, CVE-2025-27463, CVE-2025-27464(Citrix XenServer VM Tools for Windows),CVE-2025-4793(PHPGurukul Online Course Registration),CVE-2025-47933(Argo CD),CVE-2025-46701(Apache Tomcat CGI servlet),CVE-2025-48057(Icinga 2),CVE-2025-48827,CVE-2025-48828(vBulletin),CVE-2025-41438, CVE-2025-46352(Consilium Safety CS5000 Fire Panel),CVE-2025-1907(Instantel Micromate),CVE-2025-26383(Johnson Controls iSTAR Configuration Utility),CVE-2018-1285(Rockwell Automation FactoryTalk Historian ThingWorx),CVE-2025-26147(Denodo Scheduler),CVE-2025-24916, and CVE-2025-24917(Tenable Network Monitor).

Use AI Models to Challenge Your Security Assumptions AI tools like OpenAI's o3 aren't just for writing code-they can now help spot serious bugs, including vulnerabilities that even experts may miss. In one real case, o3 helped uncover a hidden flaw in Linux's kernel code by analyzing how different threads could access the same object at the wrong time-something that's easy to overlook.

How to apply this: When reviewing code or systems, try giving an AI model a specific function, some background about how it's used, and ask it questions like:

Why it works: Even experienced security teams make assumptions-about timing, logic, or structure-that attackers won't. AI doesn't assume. It explores every path, including the unlikely ones where real threats hide.

Use AI to think differently, and you may catch weak spots before someone else does.

The tools may keep changing, but the core challenge remains: knowing what to act on, and when. As new threats emerge and familiar ones resurface in unexpected ways, clarity becomes your sharpest defense.

Use these insights to question assumptions, update plans, and strengthen the weak spots that don't always show up on dashboards. Good security isn't just about staying ahead-it's about staying sharp.

Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.

We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025.

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders - all for free.