Pagina 9 - 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)

If this had been a security drill, someone would've said it went too far. But it wasn't a drillit was real. Th
e access? Everything looked normal. The tools? Easy to find. The detection? Came too late.This is how attacks
happen nowquiet, convincing, and fast. Defenders aren't just chasing hackers anymorethey're struggling to trus
t 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 matteredand why they're worth your attention.APT41
Exploits Google Calendar for Command-and-Control The Chinese state-sponsored threat actor known as APT41 deplo
yed a malware called TOUGHPROGRESS that uses Google Calendar for command-and-control (C2). Google said it obse
rved 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 Cale
ndar, and extract the commands specified in them for subsequent execution. The results of the execution are wr
itten back to another Calendar event from where they can be accessed by the attackers. The campaign targeted m
ultiple other government entities, although the company did not name the organizations that were singled out.W
ith 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, drastical
ly 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. B
elow are this week's critical vulnerabilities you need to know about. Take a look, update your software prompt
ly, 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-2025-2
7462, CVE-2025-27463, CVE-2025-27464(Citrix XenServer VM Tools for
Windows),CVE-2025-4793(PHPGurukul Online Co
urse 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),CV
E-2025-1907(Instantel Micromate),CVE-2025-26383(Johnson Controls iSTAR Configuration Utility),CVE-2018-1285(Ro
ckwell Automation FactoryTalk Historian ThingWorx),CVE-2025-26147(Denodo Scheduler),CVE-2025-24916, and CVE-20
25-24917(Tenable Network Monitor).Use AI Models to Challenge Your Security Assumptions AI tools like OpenAI's
o3 aren't just for writing codethey can now help spot serious bugs, including vulnerabilities that even expert
s may miss. In one real case, o3 helped uncover a hidden flaw in Linux's kernel code by analyzing how differen
t threads could access the same object at the wrong timesomething that's easy to overlook.How to apply this: W
hen 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 assumptionsabout timing, logic,
or structurethat attackers won't. AI doesn't assume. It explores every path, including the unlikely ones wher
e real threats hide.Use AI to think differently, and you may catch weak spots before

someone else does.The too
ls 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 qu
estion assumptions, update plans, and strengthen the weak spots that don't always show up on dashboards. Good
security isn't just about staying aheadit's about staying sharp.Discover real-time defense tactics to detect a
nd block deepfakes, fake domains, and multi-channel scams before they cause damage.We'll unpack how leading te
ams 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.

Link: https://thehackernews.com/2025/02/gitvenom-malware-steals-456k-in-bitcoin.html