# MoqHao Android Malware Evolves with Auto-Execution Capability

Link: https://thehackernews.com/2024/02/new-variant-of-moqhao-android-malware.html

Summary: Threat hunters have identified a new variant of Android malware called MoqHao that automatically executes on infected devices without requiring any user interaction.  
The campaign's targets include Android users located in France, Germany, India, Japan, and South Korea.  
In July 2022, Sekoia detailed a campaign that compromised at least 70,000 Android devices in France.  
What's also received a facelift is that the links shared in the SMS messages themselves are hidden using URL shorteners to increase the likelihood of the attack's success.  
MoqHao is equipped with several features that allow it to stealthily harvest sensitive information like device metadata, contacts, SMS messages, and photos, call specific numbers with silent mode, and enable/disable Wi-Fi, among others.

# Hands-on Review: Myrror Security Code-Aware and Attack-Aware SCA

Link: https://thehackernews.com/2024/02/hands-on-review-myrror-security-code.html

Summary: IntroductionThe modern software supply chain represents an ever-evolving threat landscape, with each package added to the manifest introducing new attack vectors.  
Furthermore, they do not address many supply chain attacks, such as typosquatting, malicious code injection, CI/CD attacks, etc.  
Myrror Security develops innovative solutions to these challenges by revolutionizing how organizations detect, prioritize and remediate their supply chain risks.  
This algorithm identifies which vulnerabilities are actually reachable in production, thus enabling Myrror to prioritize security issues accurately.  
ConclusionAppSec teams suffer from profound alert fatigue today, driven by an overwhelming amount of security issues and a lack of clear prioritization of what to work on first.

# New Coyote Trojan Targets 61 Brazilian Banks with Nim-Powered Attack

Link: https://thehackernews.com/2024/02/new-coyote-trojan-targets-61-brazilian.html

Summary: Sixty-one banking institutions, all of them originating from Brazil, are the target of a new banking trojan called Coyote.  
What makes Coyote a different breed from other banking trojans of its kind is the use of the open-source Squirrel framework for installing and updating Windows apps.  
Another notable departure is the shift from Delphi – which is prevalent among banking malware families targeting Latin America – to an uncommon programming language like Nim.  
The malicious dynamic-link library, named "libcef.dll," is side-loaded by means of a legitimate executable named "obs-browser-page.exe," which is also included in the Node.js project.  
It can also outright block the machine with a bogus "Working on updates..." message while executing malicious actions in the background.

# Fortinet Warns of Critical FortiOS SSL VPN Flaw Likely Under Active Exploitation

Link: https://thehackernews.com/2024/02/fortinet-warns-of-critical-fortios-ssl.html

Summary: Fortinet has disclosed a new critical security flaw in FortiOS SSL VPN that it said is likely being exploited in the wild.  
The vulnerability, CVE-2024-21762 (CVSS score: 9.6), allows for the execution of arbitrary code and commands.  
It further acknowledged that the issue is "potentially being exploited in the wild," without giving additional specifics about how it's being weaponized and by whom.  
The company, in a report published this week, divulged that N-day security vulnerabilities in its software, such as CVE-2022-42475 and CVE-2023-27997, are being exploited by multiple activity clusters to target governments, service providers, consultancies, manufacturing, and large critical infrastructure organizations.  
Previously, Chinese threat actors have been linked to the zero-day exploitation of security flaws in Fortinet appliances to deliver a wide range of implants, such as BOLDMOVE, THINCRUST, and CASTLETAP.

# Wazuh in the Cloud Era: Navigating the Challenges of Cybersecurity

Link: https://thehackernews.com/2024/02/wazuh-in-cloud-era-navigating.html

Summary: Challenges of cloud computingWhile cloud computing offers numerous benefits, such as cost savings, increased efficiency, and seamless collaboration, it also introduces unique cybersecurity challenges.  
Wazuh cloud security capabilitiesWazuh offers a range of capabilities tailored to enhance cloud security.  
Furthermore, the Wazuh Security Compliance Auditing (SCA) module empowers system administrators to validate alignment with internal policies and standards.  
As organizations embrace the benefits of cloud computing, they must also address the challenges associated with securing their cloud environments.  
Wazuh provides an effective solution for navigating the complexities of cybersecurity in the cloud era with its capabilities and flexibility.

# Warning: New Ivanti Auth Bypass Flaw Affects Connect Secure and ZTA Gateways

Link: https://thehackernews.com/2024/02/warning-new-ivanti-auth-bypass-flaw.html

Summary: Ivanti has alerted customers of yet another high-severity security flaw in its Connect Secure, Policy Secure, and ZTA gateway devices that could allow attackers to bypass authentication.  
The issue, tracked as CVE-2024-22024, is rated 8.3 out of 10 on the CVSS scoring system.  
"An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication," the company said in an advisory.  
CVE-2024-22024 affects the following versions of the products -Ivanti Connect Secure (versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, and 22.5R1.1)Ivanti Policy Secure (version 22.5R1.1)ZTA (version 22.6R1.3)Patches for the bug are available in Connect Secure versions 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3, and 22.6R2.2; Policy Secure versions 9.1R17.3, 9.1R18.4, and 22.5R1.2; and ZTA versions 22.5R1.6, 22.6R1.5, and 22.6R1.7.  
"XXE is an introduction to a variety of impacts: DOS, Local File Read, and SSRF," it said.

# Hands-On Review: SASE-based XDR from Cato Networks

Link: https://thehackernews.com/2024/02/hands-on-review-sase-based-xdr-from.html

Summary: Announced in January, Cato XDR is, as Cato Networks puts it, the first "SASE-based" XDR product.  
It's important to understand that Cato XDR is not sold as a standalone product, but as part of the larger Cato SASE Cloud.  
So, to fully appreciate Cato XDR, one should be familiar with the rest of the Cato platform to best appreciate the simplicity and – what Cato calls "elegance" – of the platform.  
To explore Cato XDR capabilities, visit Cato XDR.  
Putting Cato XDR to the TestClicking on the Stories Dashboard of Cato XDR gives us an overall view of the stories in the enterprise (see below).

# Stealthy Zardoor Backdoor Targets Saudi Islamic Charity Organization

Link: https://thehackernews.com/2024/02/stealthy-zardoor-backdoor-targets-saudi.html

Summary: An unnamed Islamic non-profit organization in Saudi Arabia has been targeted as part of a stealthy cyber espionage campaign designed to drop a previously undocumented backdoor called Zardoor.  
The intrusion targeting the Islamic charitable organization involved the periodic exfiltration of data roughly twice a month.  
While the former is the core backdoor element that facilitates C2 communications, the latter ensures that "zar32.dll" has been deployed with administrator privileges.  
The origins of the threat actor behind the campaign are unclear, and it does not share any tactical overlaps with a known, publicly reported threat actor at this time.  
That said, it's assessed to be the work of an "advanced threat actor."

# Chinese Hackers Operate Undetected in U.S. Critical Infrastructure for Half a Decade

Link: https://thehackernews.com/2024/02/chinese-hackers-operate-undetected-in.html

Summary: The U.S. government on Wednesday said the Chinese state-sponsored hacking group known as Volt Typhoon had been embedded into some critical infrastructure networks in the country for at least five years.  
Targets of the threat actor include communications, energy, transportation, and water and wastewater systems sectors in the U.S. and Guam.  
"The group also relies on valid accounts and leverages strong operational security, which combined, allows for long-term undiscovered persistence."  
Further, Volt Typhoon's operational security is enhanced by targeted log deletion to conceal their actions within the compromised environment."  
The Toronto-based digital watchdog, which dubbed the influence operation PAPERWALL, said it shares similarities with HaiEnergy, albeit with different operators and unique TTPs.

# Unified Identity – look for the meaning behind the hype!

Link: https://thehackernews.com/2024/02/unified-identity-look-for-meaning.html

Summary: not every "unified" "identity" "security" "platform" is made equal.  
For this hospital, unified identity means strong access management for customers and frontline workers, strong joiner-leaver-mover handling, AD hardening and enterprise-grade reporting.  
The key driver for unified identity is this extreme fragmentation: a large organization has on average 45 different security tools.  
And a unified identity solution removes the complexity of the multi-vendor approach, eliminating at least one factor.  
Unified identity sounds wonderful but betting the house on a single vendor is a high ask.