14 Apr 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics DC3 Cyber Crime Center

Articles

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

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 called CurlBack 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. SideCopy is suspected to be a sub-cluster within Transparent Tribe (aka APT36) that's active since at least 2019. It's so named for mimicking the attack chains associated with another threat actor called SideWinder to deliver its own payloads.

https://thehackernews.com/2025/04/pakistan-linked-hackers-expand-targets.html

SpyNote, BadBazaar, MOONSHINE Malware Target Android and iOS Users via Fake Apps

Cybersecurity researchers have found that threat actors are setting up deceptive websites hosted on newly registered domains to deliver a known Android malware called SpyNote. These bogus websites masquerade as Google Play Store install pages for apps like the Chrome web browser, indicating an attempt to deceive unsuspecting users into installing the malware instead. "The threat actor utilized a mix of English and Chinese-language delivery sites and included Chinese-language comments within the delivery site code and the malware itself," the DomainTools Investigations (DTI) team said in a report shared with The Hacker News. SpyNote (aka SpyMax) is a remote access trojan long known for its ability to harvest sensitive data from compromised Android devices by abusing accessibility services.

https://thehackernews.com/2025/04/spynote-badbazaar-moonshine-malware.html

Slow Pisces Targets Developers with Coding Challenges and Introduces New Customized Python Malware

Slow Pisces (aka Jade Sleet, TraderTraitor, PUKCHONG) is a North Korean state-sponsored threat group primarily focused on generating revenue for the DPRK regime, typically by targeting large organizations in the cryptocurrency sector. This article analyzes their campaign that we believe is connected to recent cryptocurrency heists. In this campaign, Slow Pisces engaged with cryptocurrency developers on LinkedIn, posing as potential employers and sending malware disguised as coding challenges. These challenges require developers to run a compromised project, infecting their systems using malware we have named RN Loader and RN Stealer.

https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/

Paper Werewolf Deploys PowerModul Implant in Targeted Cyberattacks on Russian Sectors

The threat actor known as Paper Werewolf has been observed exclusively targeting Russian entities with a new implant called PowerModul. The activity, which took place between July and December 2024, singled out organizations in the mass media, telecommunications, construction, government entities, and energy sectors, Kaspersky said in a new report published Thursday. Paper Werewolf, also known as GOFFEE, is assessed to

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

2

have conducted at least seven campaigns since 2022, according to BI.ZONE, with the attacks mainly aimed at government, energy, financial, media, and other organizations.

https://thehackernews.com/2025/04/paper-werewolf-deploys-powermodul.html

PlayPraetor Reloaded: CTM360 Uncovers a Play Masquerading Party

CTM360 has now identified a much larger extent of the ongoing Play Praetor campaign. What started with 6000+ URLs of a very specific banking attack has now grown to 16,000+ with multiple variants. This research is ongoing, and much more is expected to be discovered in the coming days. As before, all the newly discovered play impersonations are mimicking legitimate app listings, deceiving users into installing malicious Android applications or exposing sensitive personal information. While these incidents initially appeared to be isolated, further investigation has revealed a globally coordinated campaign that poses a significant threat to the integrity of the Play Store ecosystem.

https://thehackernews.com/2025/04/playpraetor-reloaded-ctm360-uncovers.html

Phishing Campaigns Use Real-Time Checks to Validate Victim Emails Before Credential Theft

Cybersecurity researchers are calling attention to a new type of credential phishing scheme that ensures that the stolen information is associated with valid online accounts. The technique has been codenamed precision-validating phishing by Cofense, which it said employs real-time email validation so that only a select set of high-value targets are served the fake login screens. "This tactic not only gives the threat actors a higher success rate on obtaining usable credentials as they only engage with a specific pre-harvested list of valid email accounts," the company said.

https://thehackernews.com/2025/04/phishing-campaigns-use-real-time-checks.html

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

3