# North Korean Hackers Deploy BeaverTail Malware via 11 Malicious npm Packages

North Korean threat actors are spreading their tentacles on the npm ecosystem by publishing more malicious packages. The packages deliver the BeaverTail malware, as well as a new remote access trojan (RAT) loader. The disclosure comes nearly a month after a set of six packages were discovered distributing the JavaScript stealer. The end goal of the campaign is to infiltrate developer systems under the guise of a job interview process, steal sensitive data, siphon financial assets, and maintain long-term access to compromised systems. South Korean cybersecurity company AhnLab detailed a recruitment-themed phishing campaign that delivers BeaverTail. The program is then used to deploy a previously undocumented Windows backdoor codenamed Tropidoor. Artifacts analyzed by the firm show that BeaverT tail is being used to target developers in South Korea. The email message claimed to be from a company called AutoSquare, and contained a link to a project hosted on Bitbucket, urging the recipient to clone the project locally to review their understanding of the program.

# Malicious Python Packages on PyPI Downloaded 39,000+ Times, Steal Sensitive Data

Two packages masquerade as fixes for recent issues detected in a legitimate Python module called bitcoinlib. Third package, disgrasya, contained a fully automated carding script targeting WooCommerce stores. The authors of the counterfeit libraries are said to have joined a GitHub issue discussion and unsuccessfully attempted to trick unsuspecting users into downloading the purported fix and running the library. "The malicious payload was introduced in version 7.36.9, and all subsequent versions carried the same embedded attack logic," the Socket Research Team said. "Disgrasya" is a powerful carding utility disguised as a harmless library. It can be used to test stolen credit cards against real checkout systems without triggering fraud detection. It was created by embedding this logic inside a Python package published on PyPI and downloaded over 34,000 times. It could be easily used in larger automation frameworks, making disgrasya a powerfulCarding Utility disguised by a harmlessLibrary. The tool was created to test a legitimate shopper's journey through an online store.

# Critical Ivanti Flaw Actively Exploited to Deploy TRAILBLAZE and BRUSHFIRE Malware

Ivanti has disclosed details of a now-patched critical security vulnerability impacting its Connect Secure. The vulnerability, tracked as CVE-2025-22457, concerns a case of a stack-based buffer overflow. The flaw impacts the following products and versions - Ivanti Connect Secure (versions 22.7R2.5 and prior) and Pulse Connect Secure, versions 9.1R18.9 and prior. There is no evidence that Policy Secure or ZTA gateways have come under in-the-wild abuse. UNC5221 has been assessed to share overlaps with threat groups such as APT27, Silk Typhoon, and UTA0178. Microsoft theorized that the threat actor likely analyzed the February patch released by Ivanti and figured out a way to exploit prior versions. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-22457 to its Known Exploited Vulnerabilities (KEV) catalog, requiring federal agencies to apply the fixes by April 11, 2025.

# OPSEC Failure Exposes Coquettte's Malware Campaigns on Bulletproof Hosting Servers

A novice cybercrime actor has been observed leveraging the services of a Russian bulletproof hosting (BPH) provider. The findings come from DomainTools, which detected the activity after it discovered a phony website named cybersecureprotect[.]com hosted on Proton66. The threat intelligence firm said it identified an operational security (OPSEC) failure in the domain that left its malicious infrastructure exposed, thereby revealing the malicious payloads staged on the server. Coquettte is believed to be loosely tied to a broader hacking group that goes by the name Horrid.

# CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware

Three cyber attacks recorded against state administration bodies and critical infrastructure facilities in Ukraine. Campaign involved the use of compromised email accounts to send phishing messages. Follows discovery of a phishing campaign that has focused on defense and aerospace entities with links to the ongoing conflict in Ukraine to harvest webmail credentials via fake login pages. Comes as Kaspersky warned that the threat actor known as Head Mare has targeted several Russian entities with a malware known as PhantomPyramid that's capable of processing instructions issued by the operator over a command-and-control server. The activity makes use of social engineering ploys, disguising malware-laced PDFs as research invitations and government communiqués to entice unsuspecting users into triggering the attack chain. The threat entity delivers a malicious RAR file which contains a .NET malware dropper, which further drops a Golang-based shellcode loader along with the legitimate OneDrive application and a decoy-based PDF with a final Cobalt Strike payload. have started around December 2024, security researcher Subhajeet Singha said.

# Critical Flaw in Apache Parquet Allows Remote Attackers to Execute Arbitrary Code

A maximum severity security vulnerability has been disclosed in Apache Parquet's Java Library. If successfully exploited, the flaw could allow a remote attacker to execute arbitrary code on susceptible instances. The vulnerability in question is tracked as CVE-2025-30065 and carries a CVSS score of 10.0. There is no evidence that the flaw has been exploited in the wild, but vulnerabilities in Apache projects have become a lightning rod for threat actors looking to opportunistically breach systems and deploy malware. Last month a critical security flaw in Apache Tomcat came under active exploitation within 30 hours of public disclosure.

# Microsoft Warns of Tax-Themed Email Attacks Using PDFs and QR Codes to Deliver Malware

Microsoft warns of several tax-related phishing campaigns. The campaigns use redirection methods like URL shorteners and QR codes. They are delivered via a phishing-as-a-service (PhaaS) platform codenamed RaccoonO365. Also delivered are remote access trojans (RATs) like Remcos RAT, as well as other malware and post-exploitation frameworks such as Latrodectus, AHKBot, Gu loader, and BruteRatel C4. Microsoft warns of another Storm-0249 campaign that redirected users to fake websites advertising Windows 11 Pro. The disclosure also follows a surge in campaigns that use QR codes in phishing documents to disguise malicious URLs. These findings also come in the wake of several phishing and social engineering campaigns that have been flagged in recent weeks. To mitigate the risks posed by these attacks, it's essential that organizations adopt phishing-resistant authentication methods for users, use browsers that can block malicious websites, and enable network protection.