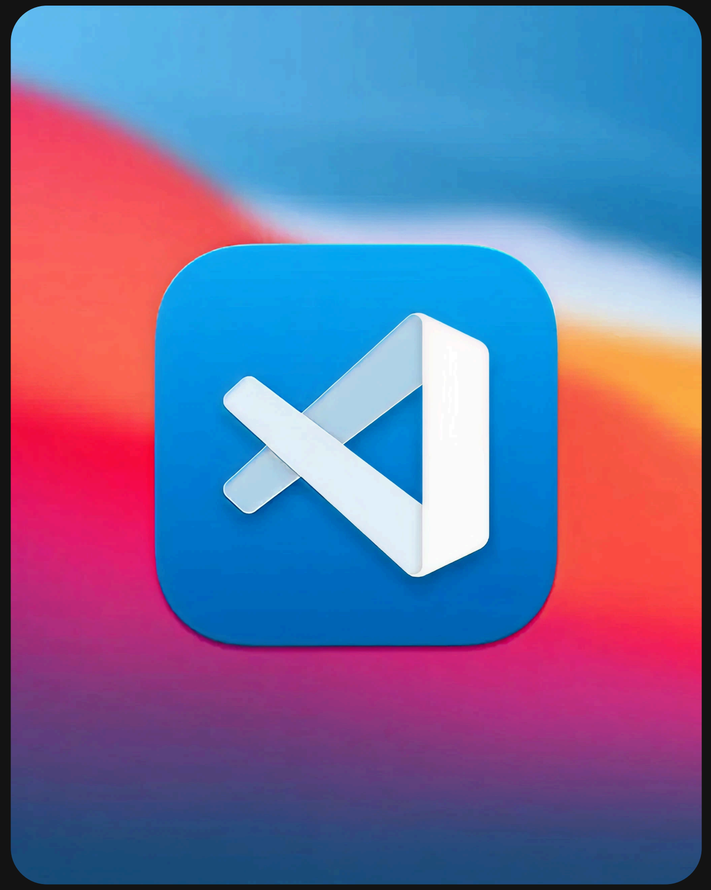
External Cyber News Journal

VOL. 7

birbank

Attackers Abuse Velociraptor Forensic Tool to Deploy Visual Studio Code for C2 Tunneling



Cybersecurity experts have raised the alarm about a new wave of attacks where hackers are misusing legitimate tools for malicious purposes. In a recent incident, threat actors exploited the Velociraptor forensic tool: a malicious MSI file was downloaded via Windows' msiexec from Cloudflare, Velociraptor was installed, and later Visual Studio Code was fetched and run using a PowerShell command.

According to Sophos, this method could be the first step in a ransomware attack. Organizations are urged to deploy Endpoint Detection and Response (EDR) solutions and keep a close eye on unexpected software activity.

Meanwhile, attacks using Microsoft Teams are on the rise. Hackers impersonate IT support staff to convince users to install remote administration tools, then execute malicious PowerShell scripts. Their objectives include stealing credentials, maintaining persistent access, and running code remotely.

In a separate campaign, attackers tricked users into visiting a fake Microsoft 365 login page by exploiting office[.]com links and the Active Directory Federation Services (ADFS) system. This approach makes phishing attempts more convincing and harder to spot.

Overall, the misuse of legitimate software is becoming more common, moving beyond classic phishing and paving the way for increasingly sophisticated cyberattacks.

Recommendations:

Avoid installing programs from untrusted sources. Never download software or files from unfamiliar links. Especially avoid additional plugins, scripts, or suspicious files, as they can be dangerous. If you are unsure, only use official sources.

Be cautious if a PowerShell window opens. If you do not use PowerShell in your daily work and suddenly see such a window on your computer, this is not normal. Sometimes this can be an early sign of a ransomware attack.

Phishing emails remain a major threat to both organizations and customers. Always verify the sender's identity, avoid clicking unknown links, and never share sensitive information by email. For organizations, regular staff training and strong email security tools are key defenses.

https://thehackernews.com/2025/08/attackers-abuse-velociraptor-forensic.html

Hundreds of Salesforce Customers Hit by Widespread Data Theft Campaign

Hackers stole data from hundreds of Salesforce customer instances in a widespread campaign earlier this month, Google Threat Intelligence Group (GTIG) warns.

The attacks did not exploit a vulnerability within the core Salesforce platform, but relied on compromised OAuth tokens for Salesloft Drift, a third-party AI chat bot.

The campaign, GTIG says, was carried out by a threat actor tracked as UNC6395 between August 8 and August 18, 2025.

“The actor systematically exported large volumes of data from numerous corporate Salesforce instances. GTIG assesses the primary intent of the threat actor is to harvest credentials,” Google’s threat intelligence unit says.

UNC6395 was seen searching the stolen information for secrets and sensitive information, including AWS access keys, passwords, and Snowflake-related access tokens.

“The threat actor used a python tool to automate the data theft process for each organization that was targeted,” GTIG principal threat analyst Austin Larsen told SecurityWeek.

Salesloft, which shared indicators of compromise (IOCs) to help customers identify potential compromises, has pointed out that only organizations integrating Drift with Salesforce have been affected by the incident.

Recommendations:

Change the password of your Salesforce account immediately.

Update the access keys for AWS and other cloud services.

Enable Multi-Factor Authentication (MFA): Google Authenticator, Microsoft Authenticator.

https://www.securityweek.com/hundreds-of-salesforce-customers-hit-by-widespread-data-theft-campaign/

The First AI-Powered Ransomware Discovered

Cybersecurity company ESET has disclosed that it discovered an artificial intelligence (AI)-powered ransomware variant codenamed PromptLock.

Currently, the program is only in the testing phase, but like traditional ransomware, it has the ability to encrypt files and steal data.

The malicious program, named PromptLock, is written in GoLang and operates using OpenAI's open-source AI model.

The program generates small commands based on specific instructions and uses them to scan files, collect information, and perform encryption.

PromptLock can run on both Windows and Linux systems and uses the SPECK 128-bit algorithm to encrypt files.

ESET stated:
"The program can steal, encrypt, or even destroy user data. However, the data destruction feature is not yet fully functional."

Experts note that such AI-powered malware could make future attacks more sophisticated and harder to detect. This also demonstrates how artificial intelligence is reshaping cybersecurity capabilities for both defense and offense.

Recommendations:

Regularly update the computers and mobile devices you use.

Ensure that antivirus protection is active on your device. Windows users can rely on Windows Defender, while Mac users are advised to use Malwarebytes.

Download software only from official websites, and avoid clicking on advertisement links such as "free antivirus."

https://thehackernews.com/2025/08/someone-created-first-ai-powered.html

WhatsApp Desktop Users At Risk of Code Execution Attacks with Python on Windows PCs

WhatsApp Desktop users who have Python installed on their Windows PCs are at risk of arbitrary code execution due to a flaw in how the application handles Python archive files.

A malicious .pyz file crafted by attackers can be executed with a single click, granting them full control over the victim's system. Currently, Meta has not classified this behavior as a security vulnerability, leaving millions of users at potential risk.

Attack Process:
The attacker creates a Malicious.pyz file and sends it to the victim via WhatsApp Desktop.
WhatsApp Desktop previews the file and allows it to be opened without displaying any warning.
Upon execution, Windows launches Python to run the archive, executing the embedded malicious code.

This sequence bypasses standard user protections because WhatsApp Desktop does not properly validate or sandbox .pyz files, unlike with media and document formats.

Meta's Response:

A similar vulnerability was discovered earlier this year in Telegram Desktop, where .pyz files were automatically executed, leading to remote code execution. Telegram addressed the issue by enforcing stricter file-type validation and adding warning prompts. Meta, however, maintains that WhatsApp Desktop only handles "safe" desktop file types and does not treat Python archives as executable content.

As a result, no measures are currently in place to block .pyz file previews or to require explicit user confirmation before execution.

Recommendations:

Be cautious with unknown .pyz files. Never open .pyz files received via WhatsApp. Delete suspicious files without opening them and do not forward them to others.

Exercise caution on Windows devices with Python installed. Since .pyz files may run automatically if Python is present, open files only from trusted and verified sources.

https://cybersecuritynews.com/whatsapp-desktop-users-at-risk/

Ransomware Group Exploits Hybrid Cloud Gaps, Gains Full Azure Control in Enterprise Attacks

The financially motivated threat actor tracked as Storm-0501 has shifted focus on targeting cloud environments for data theft and extortion, Microsoft warns. The group has been active since 2021 and is known for attacks associated with ransomware families such as Sabbath, BlackCat, Hive, and LockBit.

In the latest attack, the threat actors took over multiple Active Directory domains, obtained global administrator privileges in Entra ID, and leveraged the lack of multi-factor authentication (MFA) to add a new MFA method under their control. As a result, they gained full access to the Azure portal and deployed backdoors to take over all subscriptions. The attackers then discovered critical data repositories, stole Azure Storage account keys, and exfiltrated data using the AzCopy CLI. Following the data theft, files were massively deleted and encrypted. After exfiltrating the data, the group contacted victims via Microsoft Teams to demand ransom.

“Storm-0501 has continued to demonstrate proficiency in moving between on-premises and cloud environments, exemplifying how threat actors adapt as hybrid cloud adoption grows. They hunt for unmanaged devices and security gaps in hybrid cloud environments to evade detection and escalate cloud privileges and, in some cases, traverse tenants in multi-tenant setups to achieve their goals,” the company notes.

Recommendations:

Secure your cloud accounts. Enable Multi-Factor Authentication (MFA) on Azure and other cloud services.

Back up your data carefully. Do not store critical photos, videos, and documents in a single location. For example, keep your photos both on Google Drive and on a USB flash drive.

https://www.securityweek.com/ransomware-group-exploits-hybrid-cloud-gaps-gains-full-azure-control-in-enterprise-attacks/

birbank

Should you have any suggestions or feedback, please contact **cyberjournal@kapitalbank.az**