FlyingYeti Exploits WinRAR Vulnerability to Deliver COOKBOX Malware

Date: 31st May 2024 | Severity: High

Summary

- COOKBOX is a PowerShell script designed to load and execute PowerShell commands on an infected device. It serves as a foothold for threat actors, allowing them to maintain persistence and control over the compromised system.
- TheFlyingYeti campaign capitalized on anxiety over the potential loss of access to housing and utilities by enticing targets to open malicious files via debt-themed lures.
- Cloudforce One has taken measures to prevent FlyingYeti from launching their phishing campaign – a campaign involving the use of Cloudflare Workers and GitHub, as well as exploitation of the WinRAR vulnerability CVE-2023-38831.

Attack Vectors

- Each Infected device receives a unique identifier computed using cryptographic transformations (SHA256/ MD5 hash functions) based on a combination of the computer name and disk serial number.
- The threat actor as primarily focused on targeting Ukrainian military entities, adding it utilizes dynamic DNS (DDNS) for their infrastructure and leverages cloud-based platforms for staging malicious content and for command-and-control (C2) purposes.
- The email messages have been observed employing debt restructuring and payment-related lures to entice recipients into clicking on a now-removed GitHub page (komunalka.github[.]io) that impersonates the Kyiv Komunalka website and instructs them to download a Microsoft Word file (“Рахунок.docx”).
- But in reality, clicking on the download button in the page results in the retrieval of a RAR archive file (“Заборгованість по ЖКП.rar”), but only after evaluating the HTTP request to a Cloudflare Worker. The RAR file, once launched, weaponizes CVE-2023-38831 to execute the COOKBOX malware.
- “The malware is designed to persist on a host, serving as a foothold in the infected device. Once installed, this variant of COOKBOX will make requests to the DDNS domain postdock[.]serveftp[.]com for C2, awaiting PowerShell cmdlets that the malware will subsequently run,” Cloudflare said.
- The development comes as CERT-UA warned of a spike in phishing attacks from a financially motivated group known as UAC-0006 that are engineered to drop the SmokeLoader malware, which is then used to deploy additional malware such as TALESHOT.”The most prevalent malware families used in these spear-phishing campaigns were Agent Tesla, Remcos, SmokeLoader, Snake Keylogger, and GuLoader.”

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• postdock[.]serveftp[.]com
URL	• hxxp[:]//canarytokens[.]com/stuff/tags/ni1cknk2yq3xfcw2al3efs37m/payments.js • hxxps[:]//worker-polished-union-f396[.]vqu89698[.]workers[.]dev • hxxps[:]//pixeldrain[.]com/api/file/ZAJxwFFX?download= • hxxp[:]//canarytokens[.]com/stuff/terms/images/k22r2dnjrvjsme8680ojf5ccs/index.html

Recommendation

- Deploy Cloud Email Security to ensure that email services are protected against phishing, BEC and other threats.
- Leverage browser isolation to separate messaging applications like LinkedIn, email, and Signal from your main network.
- Scan, monitor and/or enforce controls on specific or sensitive data moving through your network environment with data loss prevention policies.
- Ensure your systems have the latest WinRAR and Microsoft security updates installed.
- Consider preventing WinRAR files from entering your environment, both at your Cloud Email Security solution and your Internet Traffic Gateway.
- Run an Endpoint Detection and Response (EDR) tool such as CrowdStrike or Microsoft Defender for Endpoint to get visibility into binary execution on hosts.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//thehackernews.com/2024/05/flyingyeti-exploits-winrar.html
- https[:]//blog.cloudflare.com/disrupting-flyingyeti-campaign-targeting-ukraine/