Mphasis
The Next Applied

New WARMCOOKIE Windows Backdoor Pushed via Fake Job Offers

Date: 12th June 2024 | Severity: High

Summary

- Elastic Security Labs observed a wave of email campaigns in late April targeting environments by deploying a new backdoor we're calling WARMCOOKIE based on data sent through the HTTP cookie parameter. During initial triage, our team identified code overlap with a previously publicly reported sample by eSentire. The unnamed sample (resident2.exe) discussed in the post appears to be an older or deviated version of WARMCOOKIE. While some features are similar, such as the implementation of string obfuscation, WARMCOOKIE contains differing functionality. Our team is seeing this threat distributed daily with the use of recruiting and job themes targeting individuals.
- WARMCOOKIE appears to be an initial backdoor tool used to scout out victim networks and deploy additional payloads. Each sample is compiled with a hard-coded C2 IP address and RC4 key.

Attack Vectors

- The phishing campaign utilizes fake job and recruitment offers sent via emails with attention-grabbing subjects. They target individuals with touches of personalization, using their names and those of their current employers.
- To add legitimacy, those fake pages prompt the victim to solve a CAPTCHA before they download a heavily obfuscated JavaScriptfile named similar to 'Update_23_04_2024_5689382'.
- "When executed, the JS script executes a PowerShell script that uses the Background Intelligent Transfer Service (BITS) to download the Warmcookie DLL file from a specified URL and execute it via rundll32.exe.
- The Warmcookie payload is copied to C:\ProgramData\RtlUpd\RtlUpd.dll, and upon first execution, it creates a scheduled task named 'RtlUpd' that runs every 10 minutes.
- In the final setup phase, Warmcookie establishes communication with its command and control (C2) server and begins fingerprinting the victim's machine.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• omeindia[.]com • assets.work-for[.]top
File Hash	• ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13
IP address	• 45[.]9[.]74[.]135 • 80[.]66[.]88[.]146 • 185[.]49[.]69[.]41

Recommendation

- Confirm that all devices are protected with Endpoint Detection and Response (EDR) solutions.
- Using Phishing and Security Awareness Training (PSAT), educate your employees regarding the risk of commodity stealers and drive-by downloads.
- Ensure standard procedures are in place for employees to submit potentially malicious content for review.
- Use Windows Attack Surface Reduction rules to block JavaScript and VBScript from launching downloaded content.

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://www.bleepingcomputer.com/news/security/new-warmcookie-windows-backdoor-pushed-via-fake-job-offers/
- https://www.elastic.co/security-labs/dipping-into-danger