Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

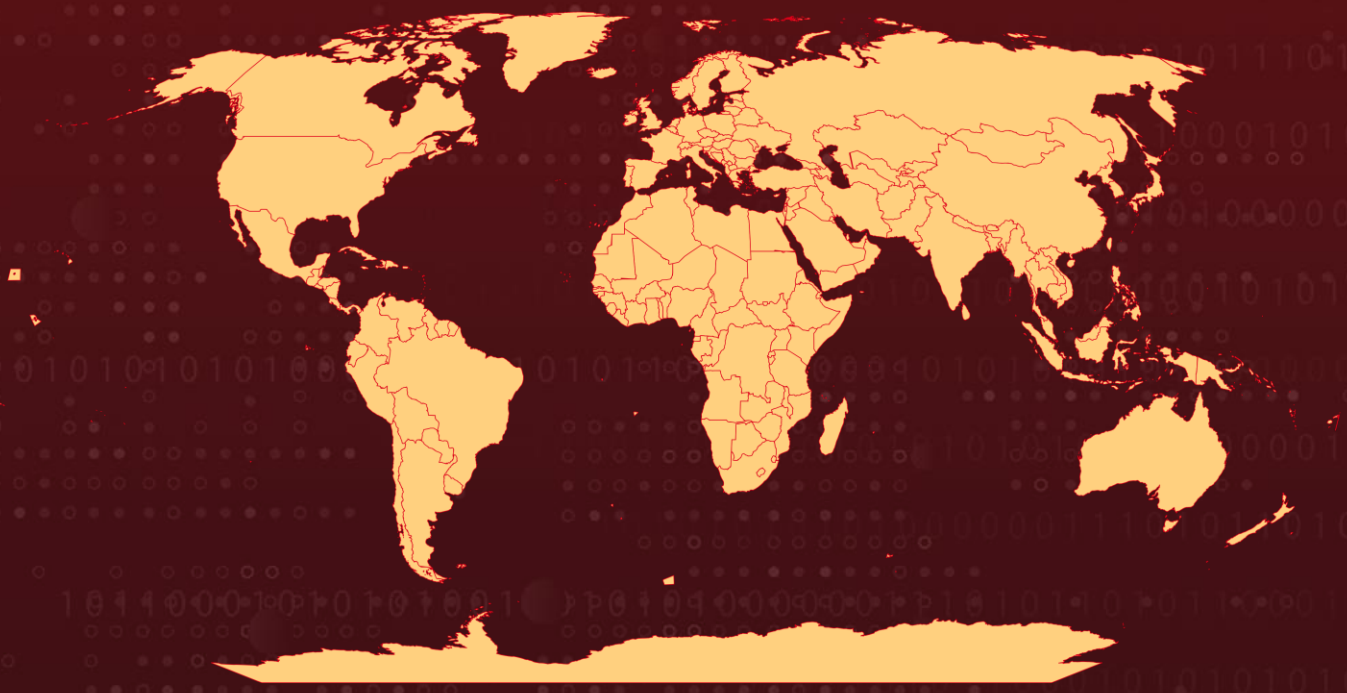
WARMCOOKIE Backdoor: Rising via Recruitment-Themed Phishing

Date of Publication	Admiralty Code	TA Number
June 12, 2024	A1	TA2024226

Summary

Attack Discovered: Late April 2024
Attack Region: Worldwide
Malware: WARMCOOKIE
Campaign: REF6127
Attack: A newly discovered Windows malware called ‘WARMCOOKIE' is being spread via phishing campaigns that disguise themselves as job offers. WARMCOOKIE functions as an initial backdoor tool, used to explore victim networks and deploy further malicious payloads. Each instance is compiled with a hard-coded C2 IP address and an RC4 key. It is also utilized to fingerprint machines, capture screenshots of victim machines, and deploy additional payloads.

Attack Regions



Attack Details

#1 In late April 2024, a concerning wave of email campaigns emerged, introducing a new backdoor known as WARMCOOKIE. This backdoor operates uniquely, leveraging data passed through the HTTP cookie parameter. Its primary function is to conduct initial reconnaissance within victim networks and pave the way for further malicious activities. Each instance of WARMCOOKIE comes equipped with predefined command and control (C2) settings, including a fixed IP address and RC4 encryption key.

#2 The email campaign, codenamed REF6127, has employed personalized phishing tactics. In this scheme, attackers entice recipients with appealing job opportunities. Clicking on the links, provided in the emails, redirects users to seemingly authentic job description pages. After successfully completing a CAPTCHA challenge, users unwittingly download an obfuscated JavaScript file. This file subsequently triggers PowerShell to load WARMCOOKIE. The script ingeniously leverages the Background Intelligent Transfer Service (BITS) to retrieve and install the WARMCOOKIE DLL.

#3 The threat actors are actively creating new landing pages, primarily hosted on IP address 45.9.74[.]135. These pages specifically target recruitment firms, utilizing industry-specific keywords to maximize effectiveness. The adversaries continuously pivot between domains to evade detection and preserve their infrastructure's integrity.

#4 WARMCOOKIE itself is a sophisticated Windows DLL, utilized in a two-stage process by threat actors. The malware employs advanced encryption techniques to safeguard its strings and dynamically loads APIs to evade static analysis. Additionally, it incorporates anti-debugging measures and gathers system identifiers before initiating any outbound network communication.

#5 With its rapid proliferation, WARMCOOKIE now poses a significant global threat, facilitating unauthorized access to target environments and enabling the dissemination of various malware strains. Vigilance and robust cybersecurity measures are paramount to mitigate its impact effectively.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Proactive PowerShell Security Measures: Configure PowerShell execution policies to limit script execution solely to those that are signed or originate from trusted locations. Additionally, enhance security by creating a firewall rule to block outbound traffic for PowerShell and using Endpoint Application Control to whitelist approved applications and scripts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1204 User Execution	T1204.001 Malicious Link	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1059.003 Windows Command Shell	T1082 System Information Discovery	T1053 Scheduled Task/Job	T1113 Screen Capture

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13
Domain	omeindia[.]com, assets.work-for[.]top
IPv4	45[.]9[.]74[.]135, 80[.]66[.]88[.]146, 185[.]49[.]69[.]41

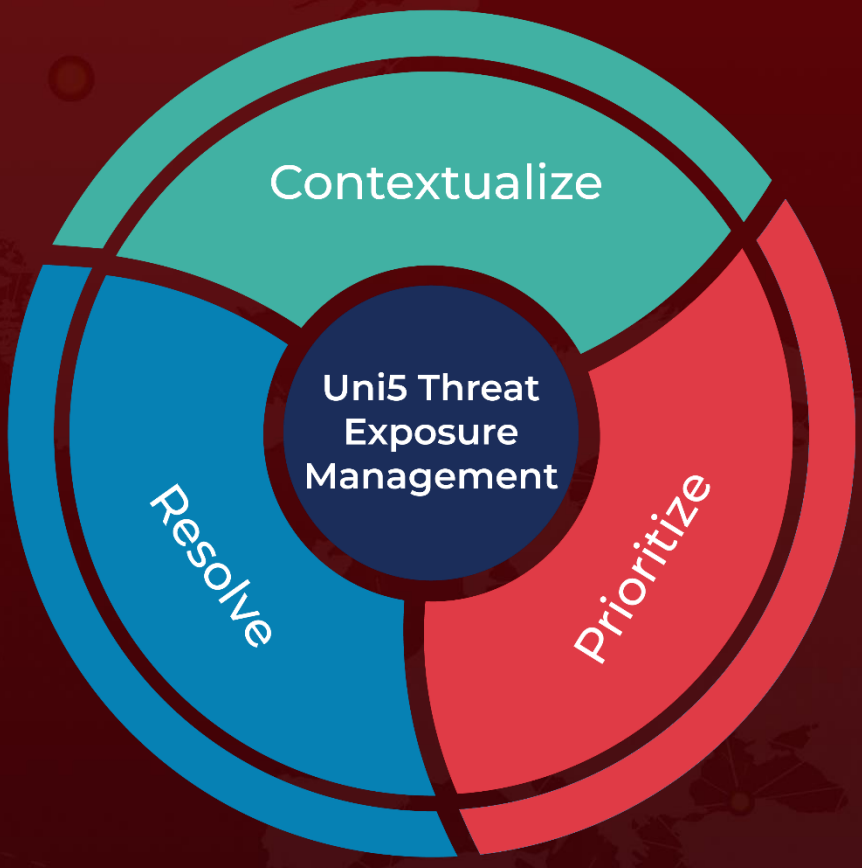
References

https://www.elastic.co/security-labs/dipping-into-danger#ref6127-campaign-overview

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 12, 2024 • 6:50 AM

More at www.hivepro.com