Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

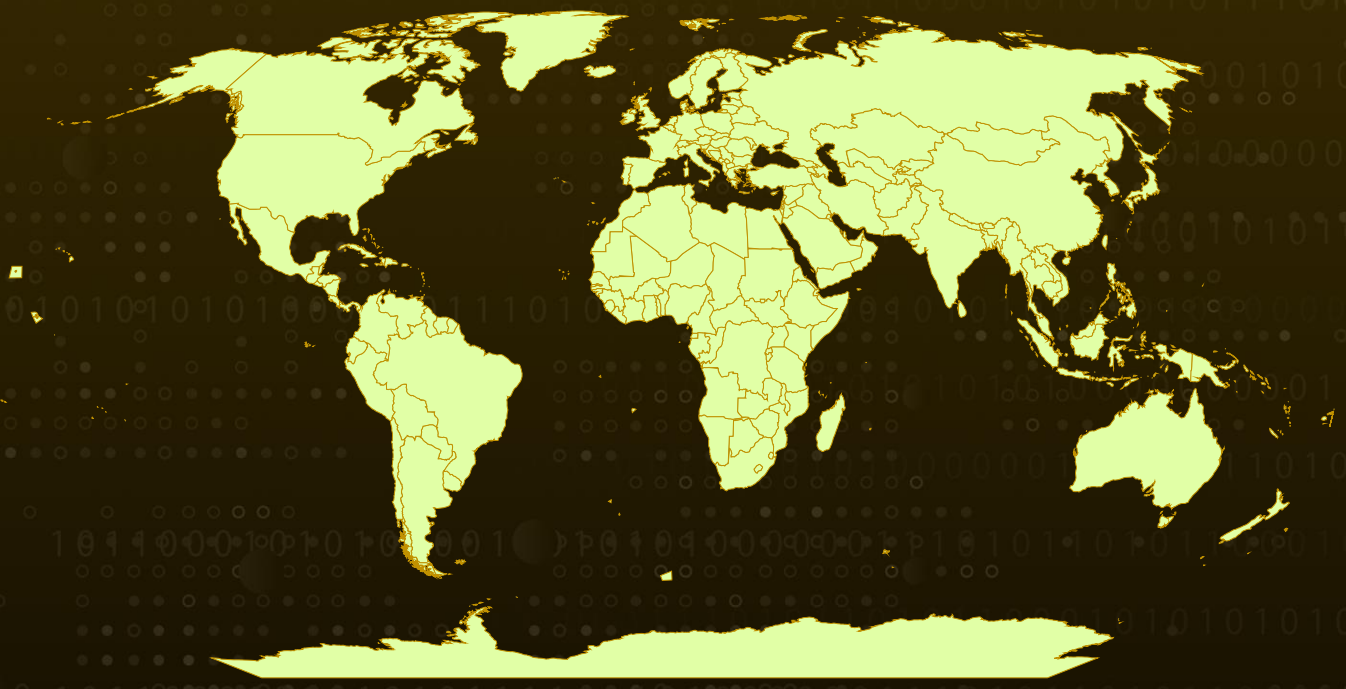
Unmasking OtterCookie Malware in the Contagious Interview Campaign

Date of Publication	Admiralty Code	TA Number
December 27, 2024	A1	TA2024474

Summary

First Seen: September 2024
Targeted Countries: Worldwide
Malware: OtterCookie
Threat Actor: North Korean Threat Actors
Targeted Industries: Finance and Cryptocurrency
Attack: A new malware named OtterCookie used in the Contagious Interview attack campaign, which is linked to North Korea. OtterCookie primarily targets financial gains and employs sophisticated techniques like downloading JavaScript code remotely and executing commands via Socket.IO. It can steal sensitive information, including cryptocurrency wallet keys, and clipboard data. Observations suggest it has evolved since September 2024, adding features for remote command execution and data theft, posing a significant threat to financial security.

Attack Regions



Attack Details

#1 A new malware called OtterCookie, which is used in the Contagious Interview attack campaign. This malware has been linked to North Korean cybercriminal groups and primarily focuses on financial theft, particularly targeting cryptocurrency assets.

#2 OtterCookie employs advanced techniques to compromise victims, including remotely downloading and executing JavaScript code, enabling attackers to dynamically control and expand its functionalities. It represents a significant threat due to its adaptability and focus on stealing sensitive financial data.

#3 One of OtterCookie's key features is its use of Socket.IO, a WebSocket-based communication protocol, to establish persistent connections with its command-and-control (C2) servers. This allows it to receive commands in real time, making it highly responsive and capable of performing dynamic actions.

#4 It can harvest information such as clipboard data, cookies, and cryptocurrency wallet keys, posing a severe risk to individual and organizational security. These features make the malware particularly dangerous for businesses handling financial transactions and sensitive data.

#5 The malware has undergone rapid development since its initial detection in September 2024, with new capabilities being added over time. Its evolving nature suggests that the attackers are actively refining their methods to bypass traditional security defenses. For example, OtterCookie now supports remote command execution, enabling attackers to install additional malicious code or exfiltrate data as needed. This adaptability highlights the need for organizations to stay updated with their cybersecurity measures.

#6 Given its sophisticated architecture and evolving threat profile, OtterCookie demonstrates the increasing sophistication of financially motivated cyberattacks.

Recommendations

Enhance Endpoint Protection: Deploy advanced endpoint detection and response (EDR) solutions to identify and block suspicious activities. Utilize behavior-based detection mechanisms to recognize anomalies related to malware execution, such as unauthorized script downloads or command-and-control (C2) communications. Ensure that antivirus and anti-malware tools are updated regularly to detect the latest threats.

Implement Network Monitoring and Filtering: Monitor network traffic for unusual patterns, including unauthorized WebSocket connections and data exfiltration attempts. Configure firewalls to block malicious IP addresses and domains associated with OtterCookie's C2 infrastructure. Employ DNS filtering to prevent access to known malicious sites and utilize intrusion detection systems (IDS) for early alerts.

Update and Patch Systems Regularly: Keep operating systems, browsers, and software updated with the latest security patches. Vulnerabilities in outdated software are often exploited by malware to gain access, so automated patch management tools can ensure systems remain secure against evolving threats.

Strengthen Email and Web Security: As phishing emails and malicious websites are common infection vectors, deploy email security gateways to filter out phishing attempts. Enable web filtering to block malicious URLs and enforce safe browsing practices. Train employees to recognize phishing attempts and avoid clicking suspicious links or downloading unverified attachments.

Implement Multi-Factor Authentication (MFA): Enable MFA across all critical systems and user accounts to add an additional layer of security. Even if credentials are compromised, MFA can prevent unauthorized access, reducing the risk of data breaches and malware deployment.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0003 Persistence	TA0009 Collection	TA0011 Command and Control
TA0008 Lateral Movement	TA0040 Impact	T1041 Exfiltration Over C2 Channel	T1027 Obfuscated Files or Information
T1059.007 JavaScript	T1059 Command and Scripting Interpreter	T1082 System Information Discovery	T1496 Resource Hijacking
T1115 Clipboard Data	T1021 Remote Services	T1204 User Execution	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fcef13ad2106, 7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e, 4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79, 32257fb11cc33e794fdfd0f952158a84b4475d46f531d4bee06746d15caf8236
Domains	zkservice[.]cloud, w3capi[.]marketing, payloadrpc[.]com
IPv4	45[.]159[.]248[.]55

References

https://jp.security.ntt/tech_blog/contagious-interview-ottercookie

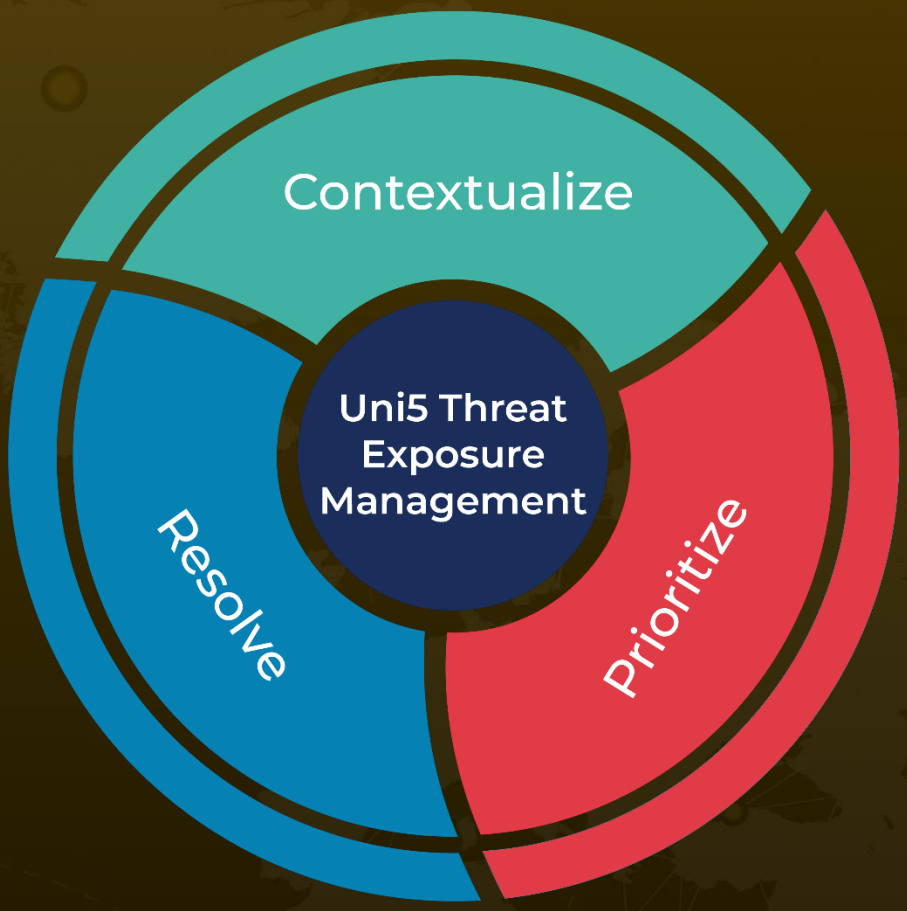
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

https://hivepro.com/threat-advisory/north-korean-hackers-go-after-remote-job-openings/

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

December 27, 2024 • 5:30 AM

More at www.hivepro.com