Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Paper Werewolf: A Cyberespionage Group Turning to Destruction

Date of Publication

January 3, 2024

Admiralty code

A1

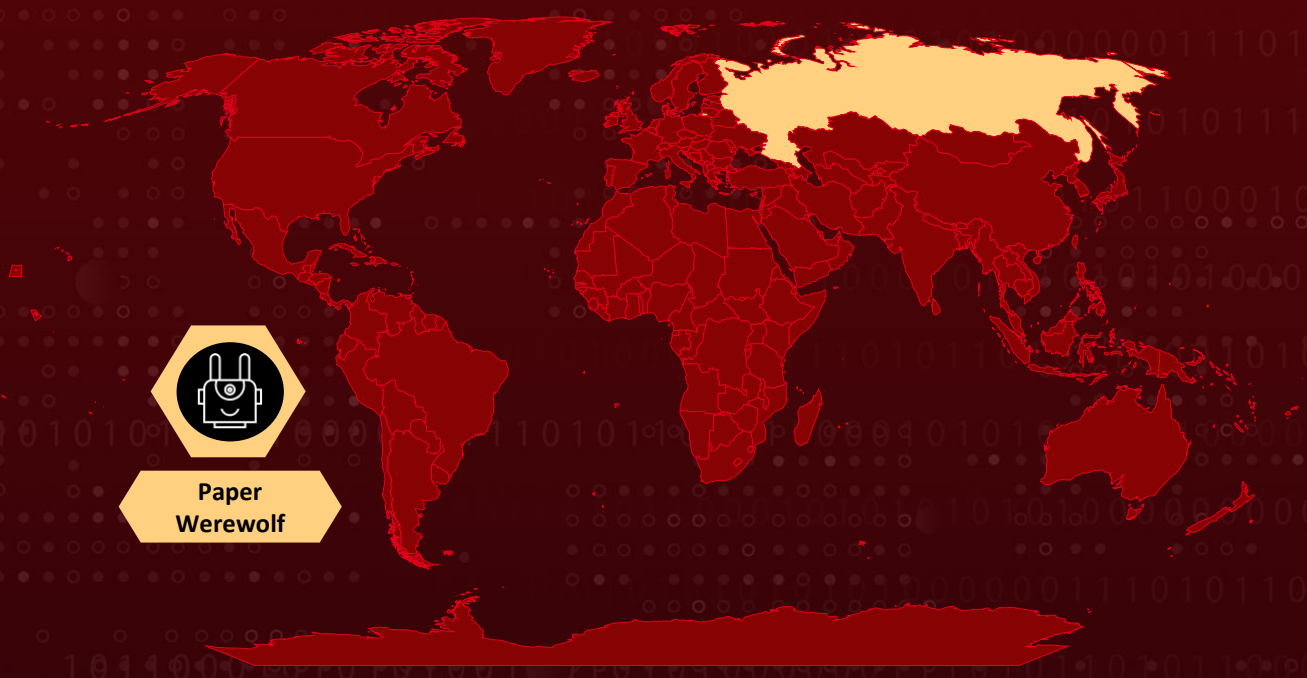
TA Number

TA2025003

Summary

First Seen: 2022
Malware: PowerRAT, PowerTaskel and QwakMyAgent
Threat Actor: Paper Werewolf (aka GOFFEE)
Targeted Country: Russia
Affected Platforms: Windows
Targeted Industries: Government, Energy, Financial, and Media

Actor Map



Actor Details

#1

The Paper Werewolf cyberespionage group, also known as GOFFEE, has intensified its operations since 2022, targeting sectors such as government, energy, finance, and media, primarily within Russia. Their campaigns typically begin with phishing emails that contain Microsoft Word attachments embedded with malicious macros. These emails are often crafted to appear as though they originate from reputable organizations, including large institutions, regulators, and law enforcement agencies, to deceive recipients into enabling the malicious content.

#2

Once the victim enables macros, the embedded document decrypts its content, deploying a PowerShell-based reverse shell known as PowerRAT. This tool facilitates remote control over the compromised system and employs various techniques to evade detection, such as hiding malicious files using environment variables and encrypting payloads. The attackers also utilize the Gophish open-source framework to organize their phishing campaigns, further enhancing their deceptive tactics.

#3

In addition to PowerRAT, Paper Werewolf has developed custom implants and adapted open-source tools to strengthen their post-exploitation capabilities. They have created agents like PowerTaskel and QwakMyAgent, which are integrated into the Mythic post-exploitation framework, complicating detection efforts. Furthermore, they employ a malicious IIS module named Owowa to extract credentials from Outlook Web Access (OWA) sessions, storing the intercepted data temporarily in RAM to avoid leaving traces on the disk.

#4

Notably, Paper Werewolf has expanded its activities beyond espionage to include destructive operations. In certain instances, after achieving their primary espionage objectives, they have executed commands to delete critical registry keys, force system restarts, and change account passwords, thereby disrupting the normal operations of the compromised infrastructure. These actions suggest a willingness to cause operational damage, possibly out of spite or to hinder incident response efforts.

#5

To maintain persistence and establish redundant access channels within compromised networks, the group utilizes tools like Chisel and PsExec. Chisel is employed to create secure tunnels for data exfiltration and command execution, while PsExec facilitates the execution of processes on remote systems. These tools enable the attackers to sustain their presence within the network, even if some access points are discovered and remediated. Paper Werewolf represents a growing cyberthreat that combines espionage with destructive actions, posing significant challenges to cybersecurity defenses.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Paper Werewolf (aka GOFFEE)	- **MOTIVE** Espionage and Destruction	Russia	Government, Energy, Financial, and Media

Recommendations

Strengthen Email Security: Given that phishing is a primary attack vector, organizations should implement advanced email filtering systems that can detect suspicious attachments and links. It's crucial to educate employees on the dangers of phishing emails, especially those that urge them to enable macros or download files from untrusted sources.

Implement Multi-Factor Authentication (MFA): MFA can significantly reduce the risk of unauthorized access, even if attackers manage to steal credentials. Enforcing MFA on all critical systems, including email accounts, VPNs, and administrative access points, adds an extra layer of protection.

Regularly Update and Patch Systems: Paper Werewolf's use of exploits and custom malware highlights the importance of keeping software and systems up to date. Regular patching cycles, especially for vulnerabilities in widely used software like Microsoft Office, can prevent attackers from exploiting known weaknesses. Automated patch management solutions should be considered to ensure timely updates.

Network Segmentation and Access Control: Proper network segmentation limits the damage that can be done if an attacker gains access to one part of the system. By segmenting critical infrastructure from less sensitive data, organizations can better contain breaches and make lateral movement more difficult for attackers. Tightening access control policies can also limit the attacker's ability to move across the network.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact	TA0011 Command and Control
TA0003 Persistence	TA0006 Credential Access	T1008 Fallback Channels	T1105 Ingress Tool Transfer
T1583 Acquire Infrastructure	T1583.001 Domains	T1583.003 Virtual Private Server	T1587 Develop Capabilities
T1587.001 Malware	T1588 Obtain Capabilities	T1588.002 Tool	T1608 Stage Capabilities
T1608.001 Upload Malware	T1566 Phishing	T1059.001 PowerShell	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1204 User Execution	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1505 Server Software Component	T1204.002 Malicious File	T1505.004 IIS Components	T1140 Deobfuscate/Decode Files or Information
T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1027.007 Dynamic API Resolution	T1027 Obfuscated Files or Information
T1027.009 Embedded Payloads	T1027.011 Fileless Storage	T1027.013 Encrypted/Encoded File	T1056.003 Web Portal Capture
T1056 Input Capture	T1082 System Information Discovery	T1033 System Owner/User Discovery	T1570 Lateral Tool Transfer
T1529 System Shutdown/Reboot	T1071 Application Layer Protocol	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1485 Data Destruction	T1071.001 Web Protocols		

Indicator of Compromise (IOCs)

TYPE	VALUE
SAH256	fa8853aaa156485855b77a16a2f613d9f58d82ef63505be8b19563827089bf52, 13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b, 8ba4cd7ea29f990cb86291003f82239bfafe28910d080b5b7d3db78e83c1b6f3, 37b3fa8a3a05e4aedb25eb38d9e4524722f28c21fac9f788f87113c5b9184ef5, 804cd68f40d0bb93b6676447af719388e95cafd5a2b017a0386eb7de590ebf17
IPv4	94[.]103[.]85[.]47, 185[.]244[.]182[.]87, 5[.]252[.]176[.]55, 85[.]198[.]110[.]216
Domains	disk-yanbex[.]ru, lobbyluxuries[.]com

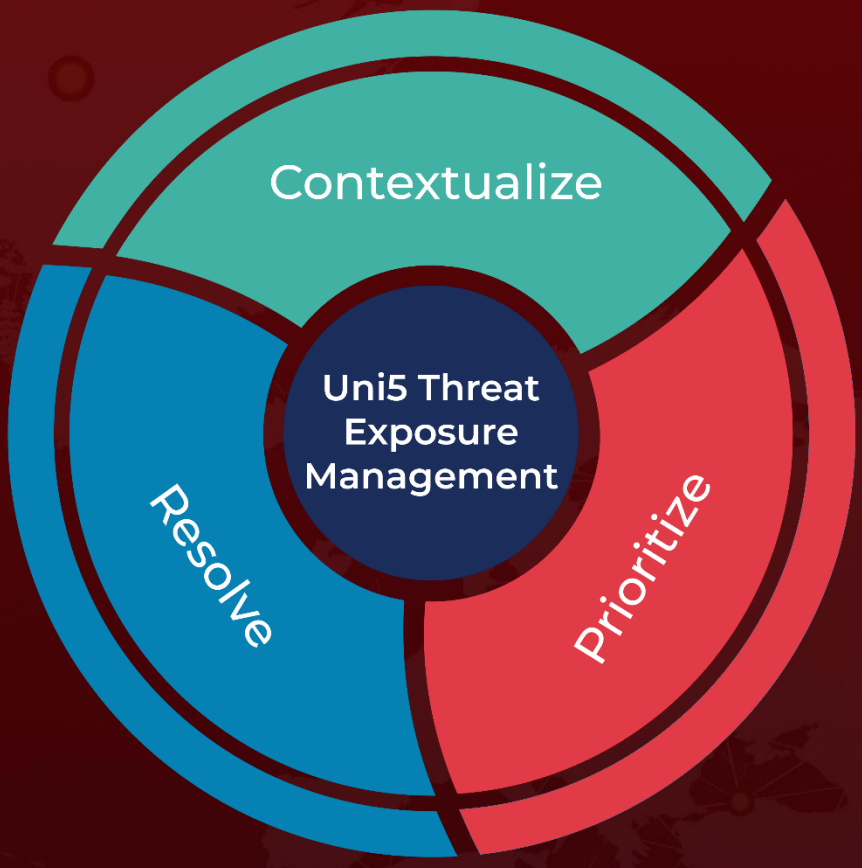
References

https://bi.zone/eng/expertise/blog/paper-werewolf-sovmeshchaet-kibershpionazh-s-destruktivnymi-deystviyami/

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

January 3, 2025 • 5:30 AM

More at www.hivepro.com