Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

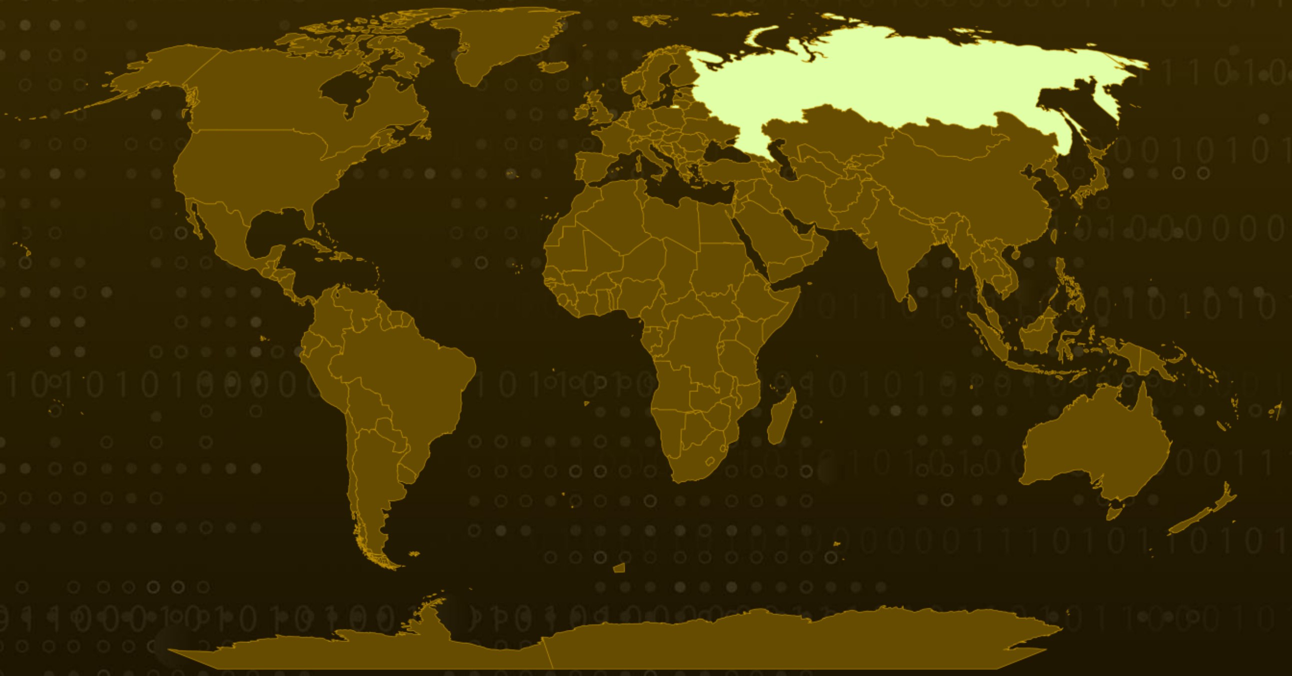
EastWind Campaign: Chinese APTs' Master Plan Against Russian Entities

Date of Publication	Admiralty Code	TA Number
August 14, 2024	A1	TA2024312

Summary

Attack Commenced: July 2024
Campaign: EastWind
Malware: GrewApacha, PlugY, CloudSorcerer
Targeted Region: Russia
Targeted Industries: Government, IT
Attack: The EastWind campaign, uncovered in late July 2024, represents a highly sophisticated cyberattack aimed at Russian government agencies and IT companies. Believed to be executed by Chinese-speaking APT groups, this operation strategically exploited legitimate platforms such as Dropbox and GitHub for command-and-control (C2) communications, enhancing its stealth and effectiveness in the cyber threat landscape.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The EastWind campaign, identified in late July 2024, represents a sophisticated and meticulously orchestrated cyber offensive targeting Russian government agencies and IT enterprises. The perpetrators, likely affiliated with Chinese-speaking APT groups, employed an array of advanced tactics to penetrate their targets, establish persistence, and potentially siphon off sensitive data with remarkable precision.

#2 The operation was initiated through a series of targeted phishing emails sent to Russian government organizations and IT firms. These emails, containing RAR archives, deployed LNK files that executed DLL sideloading techniques to surreptitiously install a backdoor via Dropbox, while simultaneously presenting a decoy document to distract the victim.

#3 Once embedded, the backdoor demonstrated the capability to execute commands, manage files, exfiltrate data, and introduce additional malicious payloads onto the compromised system. Leveraging this backdoor, the attackers deployed the GrewApacha trojan, a tool historically associated with APT31.

#4 A key element of the attack was the CloudSorcerer backdoor, which evolved after its initial discovery, demonstrating the attackers' adeptness at refining and adapting their tools in response to public exposure. Additionally, PlugY, a newly uncovered implant in this campaign, shares code similarities with DRBControl and PlugX, further tying it to APT27.

#5 The EastWind campaign highlights the increasingly sophisticated threat landscape, as APT groups exploit legitimate platforms such as GitHub, Dropbox, Quora, LiveJournal, and Yandex.Disk for command-and-control communications, complicating detection and attribution efforts. This campaign indicates the involvement of two notable Chinese-speaking APT groups, APT31 and APT27, suggesting not only a possible sharing of resources but also a potentially coordinated endeavor between these entities.

Recommendations

Enhance Email Security: To enhance email security, deploy advanced email filtering solutions that leverage machine learning and threat intelligence to effectively filter out phishing emails and malicious attachments. Additionally, conduct regular training for employees to help them recognize and understand the risks associated with opening suspicious email attachments or links.

Implement DNS Filtering and Security: Use DNS filtering solutions to block access to known malicious domains and C2 servers. Analyze DNS queries for unusual patterns or requests to unfamiliar domains that could signal an attack.

Enhance Process Monitoring: Continuously monitor for suspicious process activities, such as instances where msiexec.exe is launched for each logged-in user, which is linked to the PlugY implant. Additionally, look for the creation of named pipes with the pattern \.\PIPE\Y<number>, as these are strong indicators of PlugY implant activity.

Implement Comprehensive File Monitoring: Deploy robust file system monitoring tools to detect large DLL files (over 5 MB) located in the C:\Users\Public directory, as these can signal the presence of a backdoor distributed via email and Dropbox. Additionally, configure alerts for the detection of an unsigned file named msedgeupdate.dll, which is associated with the GrewApacha Trojan.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0007** Discovery
TA0011 Command and Control	**TA0010** Exfiltration	**T1082** System Information Discovery	**T1036** Masquerading
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1055 Process Injection	**T1574.002** DLL Side-Loading	**T1574** Hijack Execution Flow	**T1053** Scheduled Task/Job
T1071 Application Layer Protocol	**T1027** Obfuscated Files or Information	**T1083** File and Directory Discovery	**T1105** Ingress Tool Transfer
T1213 Data from Information Repositories	**T1567.002** Exfiltration to Cloud Storage	**T1567** Exfiltration Over Web Service	**T1218.007** Msiexec

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1f5c0e926e548de43e0039858de533fc, f6245f64eaad550fd292cfb1e23f0867, bed245d61b4928f6d6533900484cafc5, d0f7745c80baf342cd218cf4f592ea00, faf1f7a32e3f7b08017a9150dccf511d, 67cfecf2d777f3a3ff1a09752f06a7f5
SHA1	426bbf43f783292743c9965a7631329d77a51b61, fccdc059f92f3e08325208f91d4e6c08ae646a78, e1cf6334610e0afc01e5de689e33190d0c17ccd4, c0e4dbaffd0b81b5688ae8e58922cdaa97c8de25
SHA256	668f61df2958f30c6a0f1356463e14069b3435fb4e8417a948b6738f5f340dd9, e2f87428a855ebc0cda614c6b97e5e0d65d9ddcd3708fd869c073943ecdde1c0, 5071022aaa19d243c9d659e78ff149fe0398cf7d9319fd33f718d8e46658e41c, bd747692ab5db013cd4c4cb8ea9cafa7577c95bf41aa2629a7fea875f6dcbc41

References

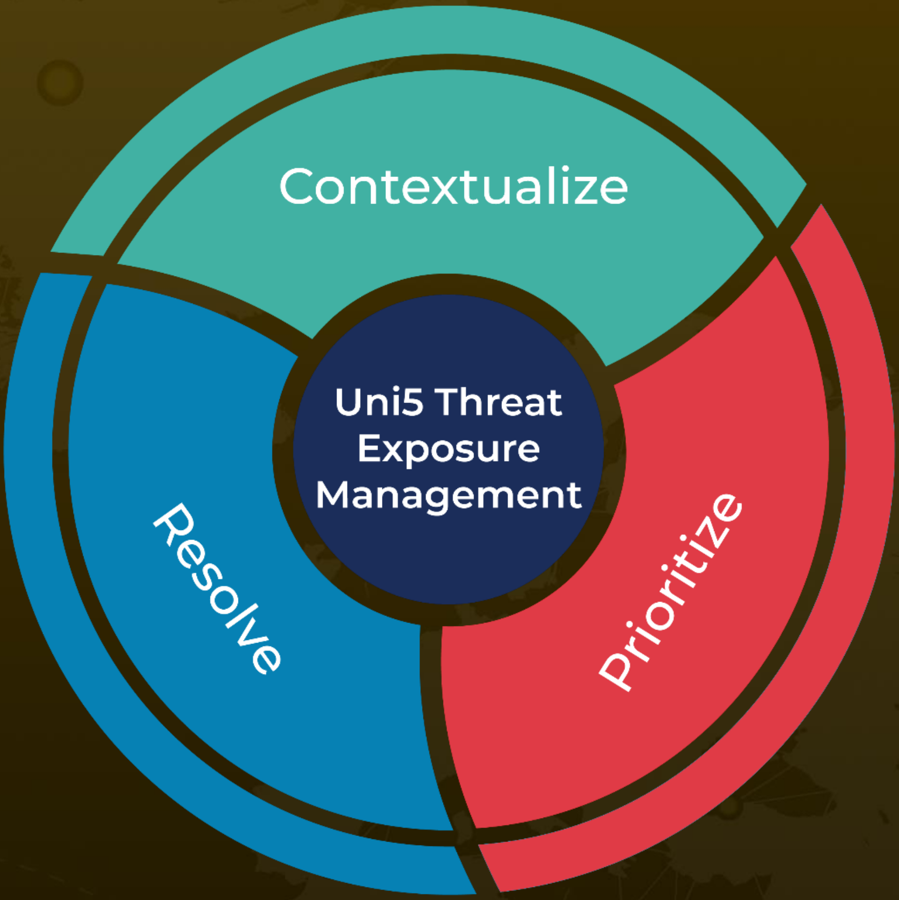
https://securelist.ru/eastwind-apt-campaign/110020/

https://hivepro.com/threat-advisory/cloudsorcerer-apt-a-stealthy-cloud-threat-targeting-russia/

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

August 14, 2024 • 6:20 AM

More at www.hivepro.com