Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

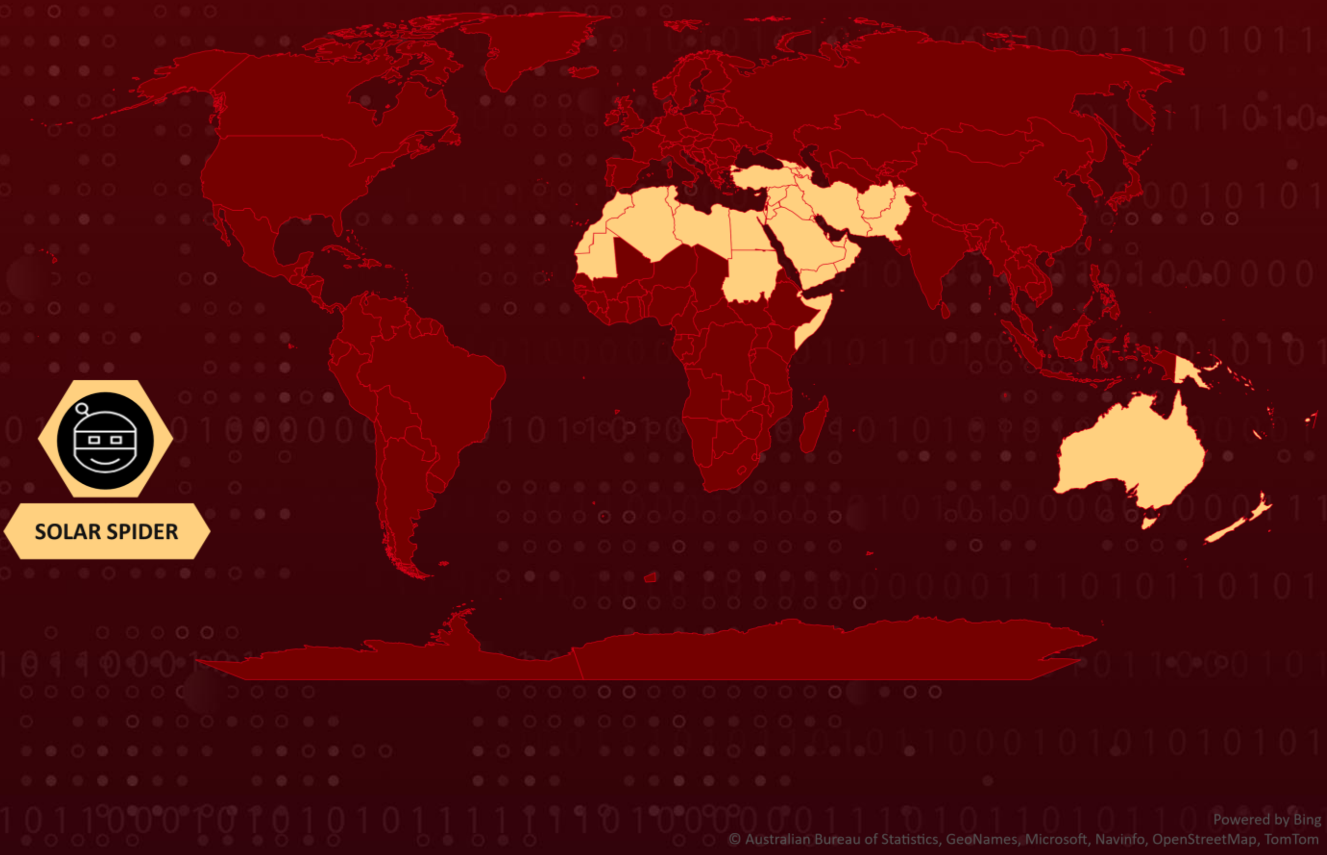
JSOutProx's Latest Incarnation Strikes Fear in Financial Circles

Date of Publication	Admiralty Code	TA Number
April 16, 2024	A1	TA2024147

Summary

Attack Commenced: February 2024
Malware: JsOutProx RAT
Threat Actor: SOLAR SPIDER
Attack Region: APAC and MENA regions
Targeted Industries: Financial Services, Banking
Attack: A cyberattack campaign, suspected to be coordinated by Solar Spider, has surfaced, employing an enhanced iteration of the advanced JavaScript remote access Trojan JSOutProx. This campaign focuses on financial institutions in the APAC and MENA regions, leveraging spear-phishing emails.

Attack Regions


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

Attack Details

#1 A cyberattack campaign, apparently orchestrated by Solar Spider, has emerged, wielding an updated version of the complex JavaScript remote access Trojan known as JSOutProx. This campaign is currently targeting financial institutions across the Asia-Pacific (APAC) and the Middle East and North Africa (MENA) regions. JSOutProx, initially detected in 2019, was originally associated with SOLAR SPIDER's phishing activities.

#2 The attack method typically involves spear-phishing emails containing malicious JavaScript attachments disguised as harmless PDFs or hidden within ZIP archives containing rogue HTA files. These payloads deploy heavily obscured implants.

#3 JSOutProx, a sophisticated offensive framework, combines JavaScript and .NET technologies. It leverages .NET deserialization features to interact with a core JavaScript module operating on the victim's system. Recent attacks have been observed using fake SWIFT or MoneyGram payment notifications to entice recipients into executing the malicious code.

#4 Upon execution, the malware enables the deployment of various plugins, facilitating further malicious activities against the target. The latest version of JSOutProx demonstrates remarkable flexibility and organization from a developmental perspective, allowing attackers to customize its functionalities to fit the victim's environment.

#5 Following a successful compromise by Solar Spider, sensitive information such as primary account numbers and user credentials is harvested, leading to a barrage of nefarious activities against the compromised entity. Artifacts associated with these attacks have been detected on GitHub and GitLab repositories. After delivery, the malicious actor promptly removes the repository, replacing it with a new one, highlighting the relentless and sophisticated nature of these malicious operations.

Recommendations

Enhance Email Security Measures: It's crucial to bolster email security protocols. Implementing advanced email filtering and scanning technologies can help detect and block suspicious emails containing malware payloads.

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Heighten Employee Awareness: Educate employees on cybersecurity best practices, emphasizing the importance of vigilance against phishing attempts. Encourage reporting of any suspicious emails or activities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0011** Command and Control	**TA0010** Exfiltration
T1036 Masquerading	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript
T1204 User Execution	**T1047** Windows Management Instrumentation	**T1543** Create or Modify System Process	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1212** Exploitation for Credential Access	**T1056** Input Capture	**T1082** System Information Discovery
T1567 Exfiltration Over Web Service	**T1657** Financial Theft	**T1566** Phishing	**T1567.001** Exfiltration to Code Repository

Indicators of Compromise (IOCs)

TYPE	VALUE
C2	eopgupgdpopopfuupi.ddns[.]net, hudukpgdgfytpddswq.ddns[.]net, hudukpgdgfytpddswq.ddns[.]net:8843/, kiftpuseridsfryiri.ddns[.]net, kiftpuseridsfryiri.ddns[.]net:8907/, mdytreudsgurifedei.ddns[.]net, mdytreudsgurifedei.ddns[.]net, mdytreudsgurifedei.ddns[.]net:9708/, suedxcapuertggando.ddns[.]net:8843/, ykderpgdgopopfuvgt.ddns[.]net, ykderpgdgopopfuvgt.ddns[.]net:7891/
IPv4	103[.]212[.]81[.]155, 103[.]212[.]81[.]157, 185[.]244[.]30[.]218, 185[.]244[.]30[.]218, 79[.]134[.]225[.]17, 79[.]134[.]225[.]17, 79[.]134[.]225[.]17
MD5	118b6673bd06c8eb082296a7b35f8fa5, 1bd7ce64f1a7cf7dc94b912ceb9533d0, 3a2104953478d1e60927aa6def17e8e7, 3d46a462f262818cada6899634354138, 66514548cdffab50d1ea75772a08df3d, 6764dbc4df70e559b2a59e913d940d4b, 72461c94bd27e5b001265bbccc931534, 81b9e7deb17e3371d417ad94776b2a26, 89a088cd92b7ed59fd3bcc7786075130, 9c9df8fbcef8acd1a5265be5fd8fdce9, bea8cf1f983120b68204f2fa9448526e, d22f76e60a786f0c92fa20af1a1619b2, efad51e48d585b639d974fcf39f7ee07, f1858438a353d38e3e19109bf0a5e1be
Filename	MoneyGram_AML_Compliance_review.pdf.js, MoneyGram_AML_Compliance_review.pdf.zip, MoneyGram_Global_Compliance_pdf.js, MoneyGram_Global_Compliance_pdf.zip, Swift_Copy_jpg.js / TRXN-00000087312_pdf.js, Swift_Copy_jpg.zip, Transaction_details_jpg.js, Transaction_details_jpg.zip,

TYPE	VALUE
Filename	Transaction_Ref_01302024_jpg.js, Transaction_Ref_01302024_jpg.zip, Transaction_Ref_jpg.js, Transaction_Ref_jpg.zip, Transactions_Copy_65880983136606696162127010122,65890982136606696162127010102.js, Transactions_Copy_65880983136606696162127010122_65890982136606696162127010102.zip

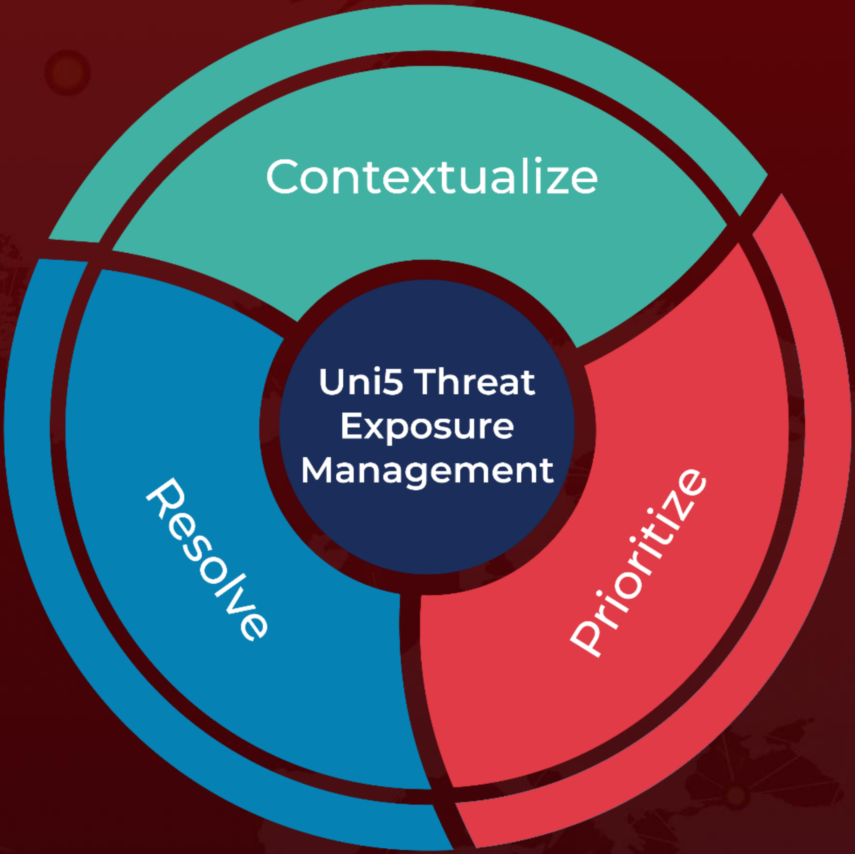
References

https://www.resecurity.com/blog/article/the-new-version-of-jsoutprox-is-attacking-financial-institutions-in-apac-and-mena-via-gitlab-abuse

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

April 16, 2024 • 6:00 AM

More at www.hivepro.com