Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

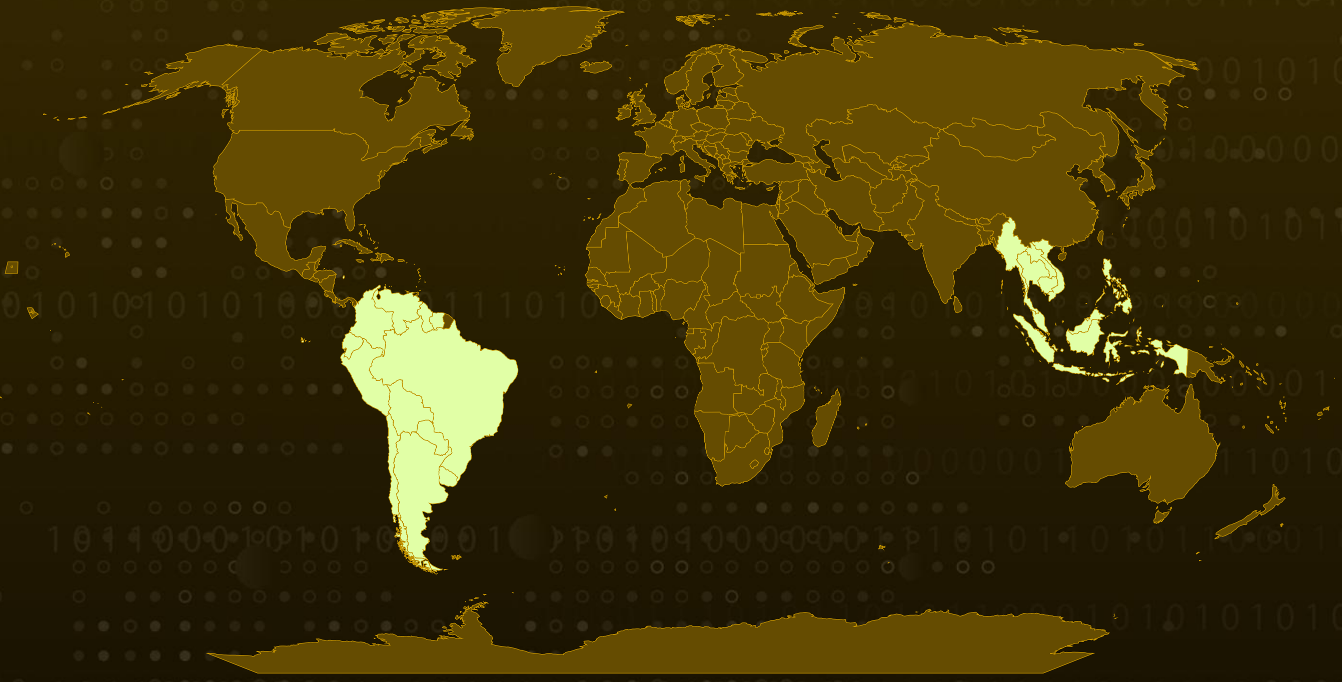
REF7707 Cyberespionage Campaign Exploiting Legitimate Cloud Services

Date of Publication	Admiralty Code	TA Number
February 14, 2025	A1	TA2025042

Summary

First Seen: November 2024
Targeted Region: South America and Southeast Asia
Malware: PATHLOADER, FINALDRAFT, GUILOADER
Campaign: REF7707
Targeted Industry: Government, Telecommunications, Education
Affected Platform: Windows and Linux
Attack: A sophisticated cyberespionage operation codenamed REF7707 has been discovered targeting government institutions, with confirmed activity against a South American foreign ministry. The campaign employs multiple advanced malware families and demonstrates significant technical capabilities, though certain operational security oversights have provided researchers with valuable intelligence about their methods.

Attack Regions



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

Attack Details

#1

A newly identified cyberespionage campaign, REF7707, has been targeting government entities, particularly a foreign ministry in South America. This operation employs sophisticated malware families, including FINALDRAFT, GUIDLOADER, and PATHLOADER, to establish persistence and execute malicious payloads. Despite the attackers' technical expertise, certain operational security flaws have exposed elements of their infrastructure, allowing researchers to gain valuable insights into their methods.

#2

The attackers leverage credentialed access to move laterally within compromised networks, primarily using Windows Remote Management (WinrsHost.exe). Their malware deployment strategy includes renaming Microsoft debugging tools and using weaponized INI files to execute shellcode. Additionally, they rely on widely used cloud services, such as Microsoft Graph API, for command-and-control (C2) communications. This approach allows them to blend malicious traffic with legitimate network activity, making detection more difficult.

#3

REF7707's infrastructure reveals the use of domains that mimic legitimate services, such as support.vmphere[.]com and digert.ictnsc[.]com. Some of these domains show links to Southeast Asia, suggesting that the campaign may have a broader geographic scope. The adversaries' use of cloud-based C2 infrastructure further complicates attribution and detection, as they exploit the trusted nature of these services to evade security measures.

#4

Further examination of the malware shows that the attackers employ various persistence mechanisms, including scheduled tasks and startup scripts, ensuring long-term access to compromised systems. The use of certutil.exe for downloading payloads highlights their ability to abuse built-in system utilities to avoid triggering traditional security alerts. These tactics demonstrate a well-planned and evolving cyberespionage effort aimed at maintaining access and exfiltrating sensitive information.

#5

While the REF7707 campaign showcases advanced techniques, its operational inconsistencies provide opportunities for detection and disruption. By analyzing its attack patterns, infrastructure, and malware behavior, security researchers continue to track and understand its evolving tactics. This campaign underscores the growing trend of state-sponsored cyberespionage efforts that exploit trusted services and legitimate tools to achieve their objectives.

Recommendations

Enhance Endpoint Security and Monitoring: Organizations should deploy advanced endpoint detection and response (EDR) solutions to monitor for suspicious processes, such as the abuse of Microsoft debugging tools and the execution of unauthorized scripts. Regularly auditing scheduled tasks and startup scripts can help identify persistence mechanisms used by attackers.

Strengthen Access Controls and Authentication: Since the attackers leverage credentialed access for lateral movement, implementing multi-factor authentication (MFA) and strict access controls can reduce the risk of unauthorized access. Organizations should also conduct frequent password audits and enforce strong password policies to prevent credential-based attacks.

Improve Network Visibility and Anomaly Detection: Security teams should closely monitor network traffic for unusual connections to cloud services, especially those using the Microsoft Graph API. Implementing network segmentation can also limit the spread of intrusions, reducing the attacker's ability to move laterally within an organization.

Harden System Configurations and Patch Management: Regularly updating software and operating systems can help protect against known vulnerabilities. Disabling unnecessary tools like certutil.exe and restricting PowerShell execution can prevent attackers from abusing built-in system utilities.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0043 Reconnaissance	TA0006 Credential Access

T1566 Phishing	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1059 Command and Scripting Interpreter
T1041 Exfiltration Over C2 Channel	T1543 Create or Modify System Process	T1027 Obfuscated Files or Information	T1021.006 Windows Remote Management
T1021 Remote Services	T1059.001 PowerShell	T1053.005 Scheduled Task	T1053 Scheduled Task/Job
T1567 Exfiltration Over Web Service	T1530 Data from Cloud Storage		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	39e85de1b1121dc38a33eca97c41dbd9210124162c6d669d28480c833e059530, 83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c, f45661ea4959a944ca2917454d1314546cc0c88537479e00550eef05bed5b1b9, 9a11d6fcf76583f7f70ff55297fb550fed774b61f35ee2edd95cf6f959853bcf, 41a3a518cc8abad677bb2723e05e2f052509a6f33ea75f32bd6603c96b721081, d9fc1cab72d857b1e4852d414862ed8eab1d42960c1fd643985d352c148a6461, f29779049f1fc2d45e43d866a845c45dc9aed6c2d9bbf99a8b1bdacfac2d52f2, 17b2c6723c11348ab438891bc52d0b29f38fc435c6ba091d4464f9f2a1b926e0, 20508edac0ca872b7977d1d2b04425aaa999ecf0b8d362c0400abb58bd686f92, 33f3a8ef2c5fbd45030385b634e40eaa264acbaeb7be851cbf04b62bbe575e75, 41141e3bdde2a7aebf329ec546745149144eff584b7fe878da7a2ad8391017b9, 49e383ab6d092ba40e12a255e37ba7997f26239f82bebcd28efaa428254d30e1,

TYPE	VALUE
SHA256	5e3dbfd543909ff09e343339e4e64f78c874641b4fe9d68367c4d1024fe79249, 7cd14d3e564a68434e3b705db41bddeb51dbb7d5425fd901c5ec904dbb7b6af0, 842d6ddb7b26fdb1656235293ebf77c683608f8f312ed917074b30fbd5e8b43d, f90420847e1f2378ac8c52463038724533a9183f02ce9ad025a6a10fd4327f12
Domains	poster[.]checkponit[.]com, support[.]fortineat[.]com, update[.]hobiter[.]com, support[.]vmphere[.]com, cloud[.]autodiscovar[.]com, digert[.]ictnsc[.]com, d-links[.]net, vm-clouds[.]net
IPv4	47[.]83[.]8[.]198, 8[.]218[.]153[.]45, 45[.]91[.]133[.]254, 8[.]213[.]217[.]182, 47[.]239[.]0[.]216

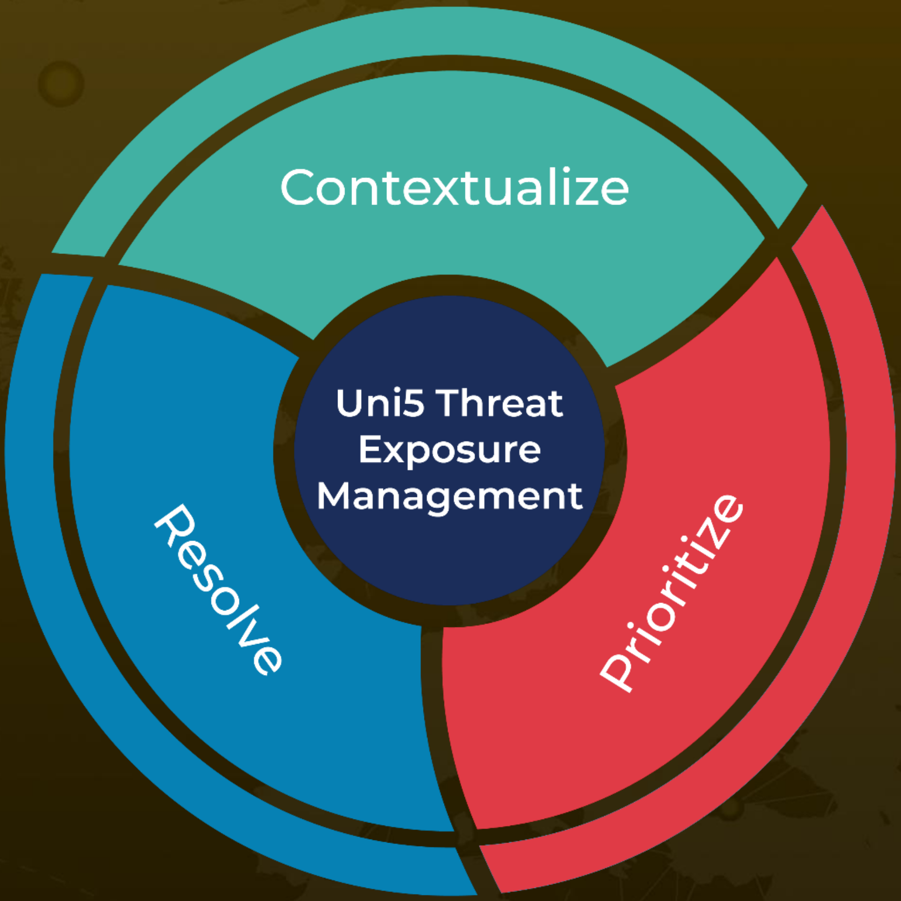
References

https://www.elastic.co/security-labs/fragile-web-ref7707

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

February 14, 2025 • 08:00 AM

More at www.hivepro.com