Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

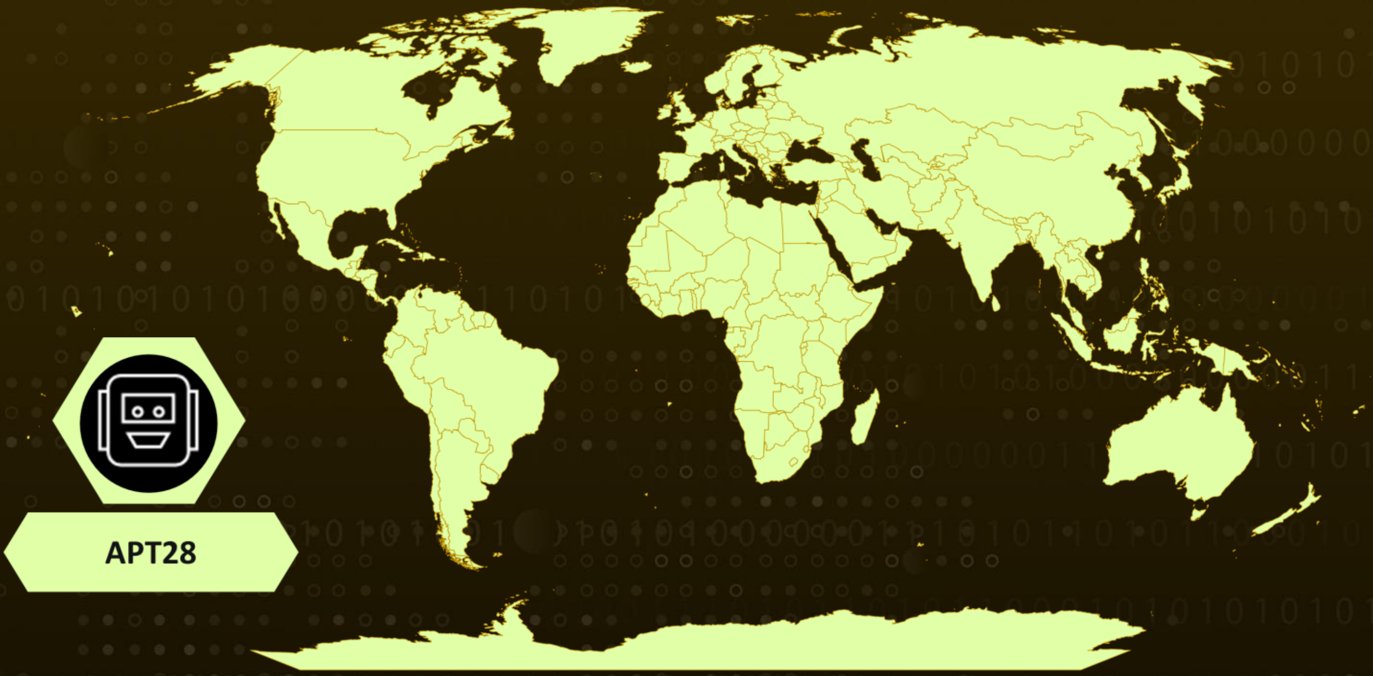
Car Sale Scam: APT28 Delivers Malware Instead of the Vehicle

Date of Publication	Admiralty Code	TA Number
August 5, 2024	A1	TA2024294

Summary

Attack Discovered: March 2024
Attack Region: Worldwide
Targeted Industry: Diplomats
Affected Platform: Windows
Threat Actor: APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)
Malware: HeadLace
Attack: The Russian threat actor APT28, also known as, Fancy Bear, has been identified in a campaign targeting diplomats using fake car sale advertisements to distribute the HeadLace backdoor malware. This campaign leverages legitimate services like Webhook.site to host malicious URLs, complicating detection and mitigation efforts.

Attack Regions



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

Attack Details

#1 The Russian-linked threat actor APT28, also known as Fancy Bear, has been linked to a new campaign employing a car-for-sale phishing lure to deliver a modular Windows backdoor called HeadLace. This campaign, likely targeting diplomats, began as early as March 2024.

#2 The URL that initiated the infection chain was hosted by Webhook.site, a legitimate service often used for development projects. Webhook.site allows users to create randomized URLs for custom automation, which APT28 abused to create a malicious HTML page. The HTML code attempts to automate an attack by first checking if the visiting computer is Windows-based. If so, it redirects to a decoy image hosted by ImgBB, ensuring that further actions are only executed for Windows visitors.

#3 The HTML page then creates a ZIP archive from Base64 text, offers it for download, and attempts to open it using the JavaScript 'click()' function. The ZIP archive 'IMG-387470302099.zip' contains three files: 1. WindowsCodecs.dll – A DLL component of the HeadLace backdoor, 2. IMG-387470302099.jpg.exe - A legitimate 'calc.exe', disguised with a double file extension which is employed to sideload the DLL file, and 3. zqtxmo.bat- The final payload, executed by a function within the dll file, completing the malware's infection chain.

#4 Finally, the batch file executes a Base64-encoded command to retrieve a file from another Webhook.site URL. The file is initially saved as IMG387470302099.jpg in the user's Downloads directory. It is then moved to the %programdata% directory, renamed to .cmd, and executed as IMG387470302099.cmd. To remove any visible signs of malicious activity, the batch file deletes itself after execution.

#5 The use of a legitimate executable to sideload the DLL and the modular nature of HeadLace highlight the sophisticated methods employed by the attackers to maintain stealth and evade detection. This approach demonstrates APT28's continued use of creative phishing lures and legitimate services to enhance the effectiveness of their campaigns and complicate detection and mitigation efforts.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0010 Exfiltration	TA0011 Command and Control	T1592 Gather Victim Host Information	T1566 Phishing
T1189 Drive-by Compromise	T1132 Data Encoding	T1132.001 Standard Encoding	T1059 Command and Scripting Interpreter
T1036 Masquerading	T1036.007 Double File Extension	T1070 Indicator Removal	T1070.004 File Deletion
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	cda936ecae566ab871e5c0303d8ff98796b1e3661885afd9d4690fc1e945640e, 7c85ff89b535a39d47756dfce4597c239ee16df88badefe8f76051b836a7cbfb, dad1a8869c950c2d1d322c8aed3757d3988ef4f06ba230b329c8d510d8d9a027, c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b, 6b96b991e33240e5c2091d092079a440fa1bef9b5aecbf3039bf7c47223bdf96, a06d74322a8761ec8e6f28d134f2a89c7ba611d920d080a3ccbfac7c3b61e2e7
URLs	hxxps[:]//webhook[.]site/66d5b9f9-a5eb-48e6-9476-9b6142b0c3ae, hxxps[:]//webhook[.]site/d290377c-82b5-4765-acb8-454edf6425dd, hxxps[:]//i.ibb[.]co/vVSCr2Z/car-for-sale.jpg

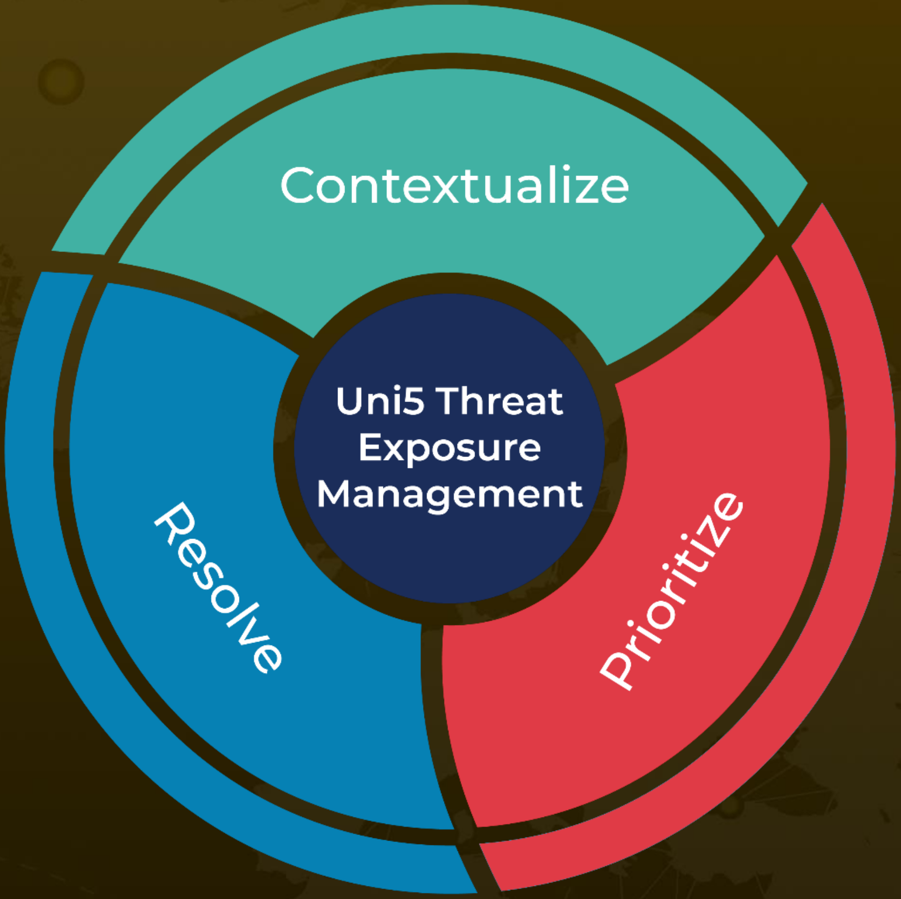
References

https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

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 5, 2024 • 7:00 AM

More at www.hivepro.com