Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

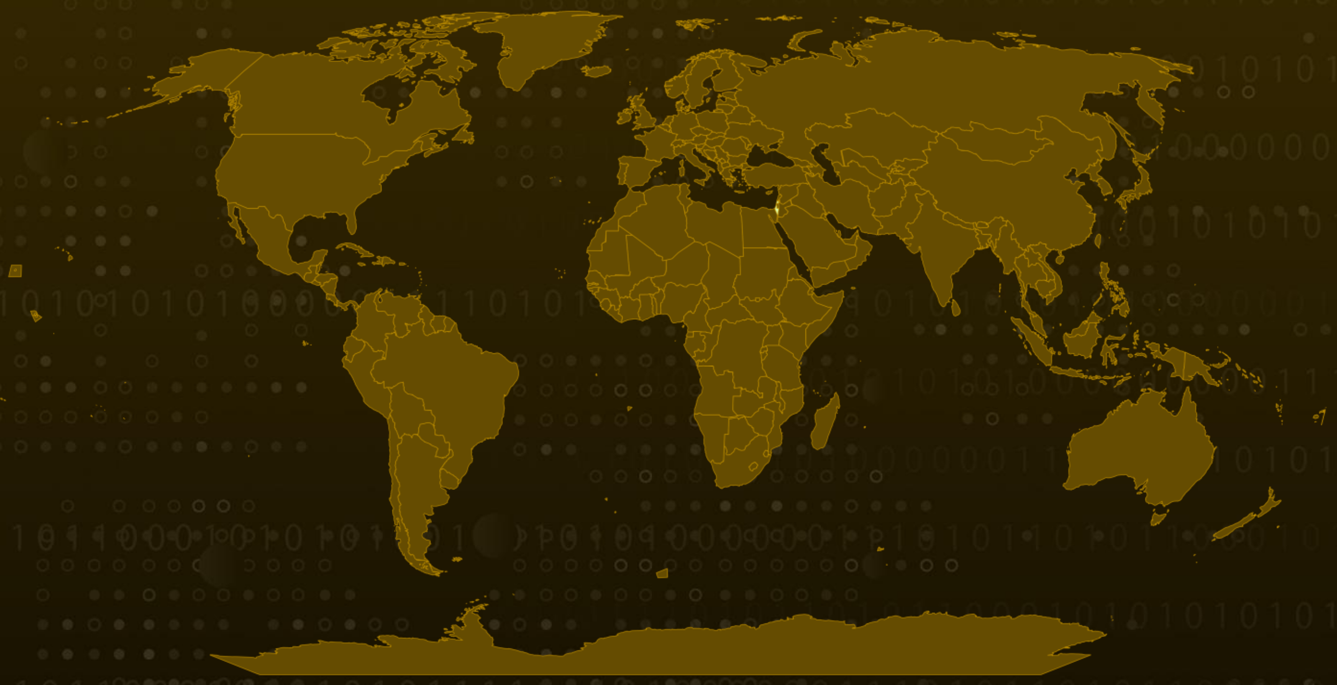
Attackers Impersonating Israeli Ministry with Blended Tools

Date of Publication	Admiralty Code	TA Number
July 7, 2024	A1	TA2024259

Summary

Attack Discovered: Late 2023
Attack Region: Israel
Affected Industry: Government
Malware: Nim Downloader, Donut, Silver
Attack: An attack campaign has been discovered targeting various Israeli entities using publicly available frameworks like Donut and Sliver. Believed to be highly targeted, the campaign leverages target-specific infrastructure and custom WordPress websites as a payload delivery mechanism. Despite its specific targeting, the campaign affects a variety of entities across unrelated verticals and relies on well-known open-source malware.

Attack Regions



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

Attack Details

#1

A sophisticated attack campaign targeting multiple Israeli entities recently emerged, utilizing accessible frameworks like Donut and Sliver. These assaults, occurring in late 2023, employed common tactics and customized WordPress sites tailored for each target. The attackers utilized well-known open-source malware tools.

#2

Initially, the attackers distributed payloads through custom-built WordPress sites using a drive-by download strategy. The vector, named 'vacation5.vhd,' was identified, though its exact origin remains unknown. It's suspected that this VHD file was distributed through a specifically crafted WordPress site using the same method. The VHD contained a link file disguised as an image icon, pointing to a hidden HTA file. Opening the link file executed the HTA file, initiating the first-stage payload 'Nim Downloader.'

#3

This malware establishes connections and initializes SSL contexts using a provided `cacert.pem` file. It accepts SSL certificates signed by various authorities and operates by storing its contents in memory and allocating executable buffers.

#4

The second-stage payload, Donut, functions as a shellcode generation framework. Donut was configured to evade security products by manipulating functions, enabling the mapping and execution of embedded payloads. Subsequently, the attackers deployed Sliver, an open-source Golang trojan, using Donut. The C2 server `www.economy-gov-il[.]com` hosted Sliver, granting the attackers full control over victims' systems to execute desired actions.

#5

The attackers combined publicly available tools with custom-built components and dedicated infrastructure. These tactics illustrate how cyber adversaries can execute complex operations using readily accessible tools, underscoring the challenges faced by cybersecurity experts in effectively tracing and mitigating such threats.

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

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
TA0011 Command and Control	**T1566** Phishing	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter
T1059.005 Visual Basic	**T1105** Ingress Tool Transfer	**T1036** Masquerading	**T1204** User Execution
T1204.002 Malicious File	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1608** Stage Capabilities
T1608.004 Drive-by Target	**T1071** Application Layer Protocol	**T1573** Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a8948dd8e4e4961da537b40bf7e313f0358510f93e25dea1a2fafd522bfd0e84, 6fb531839410b65be4f4833d73f02429b4dba8ed56fa236cce76750b9a1be23b, d891f4339354d3f4c4b834e781fa4eaca2b59c6a8ee9340cc489ab0023e034c8, d7a66f8529f1c32342c4ed06c4a4750a93bd44161f578e5b94d6d30f7cc41581, c21ad804c22a67ddb62adf5f6153a99268f0b26e359b842ebeabcada824c277f, 2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223df090bb26b3cd7
URLs	hxxps://auth.economy-gov-il[.]com/SUPPOSED_GRASSHOPPER[.]bin?token=ghhdjsdgsd, hxxps://portal.operative-sintecmedia[.]com/SAD_ATTENUATION[.]bin, hxxps://portal.operative-sintecmedia[.]com/report[.]vhd, hxxps://employees.carlsberg[.]site/voucher[.]vhd
Hostname	auth.economy-gov-il[.]com, www.economy-gov-il[.]com, login.operative-sintecmedia[.]com, portal.operative-sintecmedia[.]com, login.carlsberg[.]site, employees.carlsberg[.]site, portal.carlsberg[.]site, carls.employers-view[.]com, login.microsofonlline[.]com

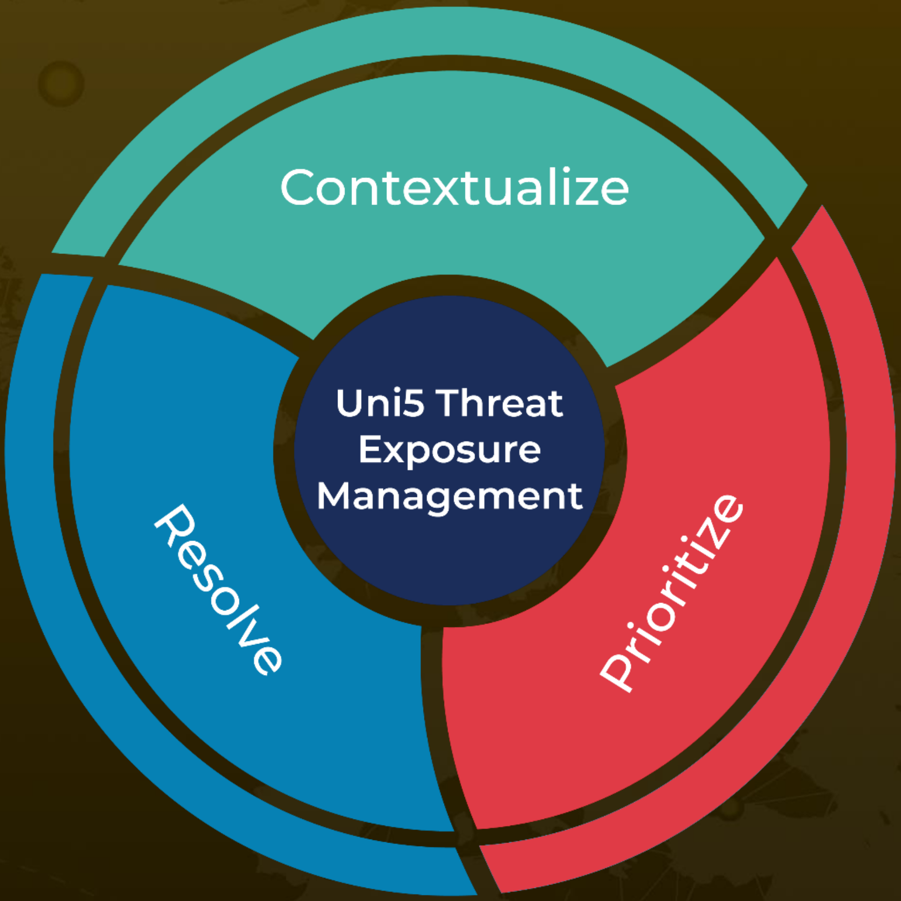
References

https://harfanglab.io/en/insidethelab/supposed-grasshopper-operators-impersonate-israeli-gov-private-companies-deploy-open-source-malware/

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

July 5, 2024 • 7:00 AM

More at www.hivepro.com