Hive Pro®

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

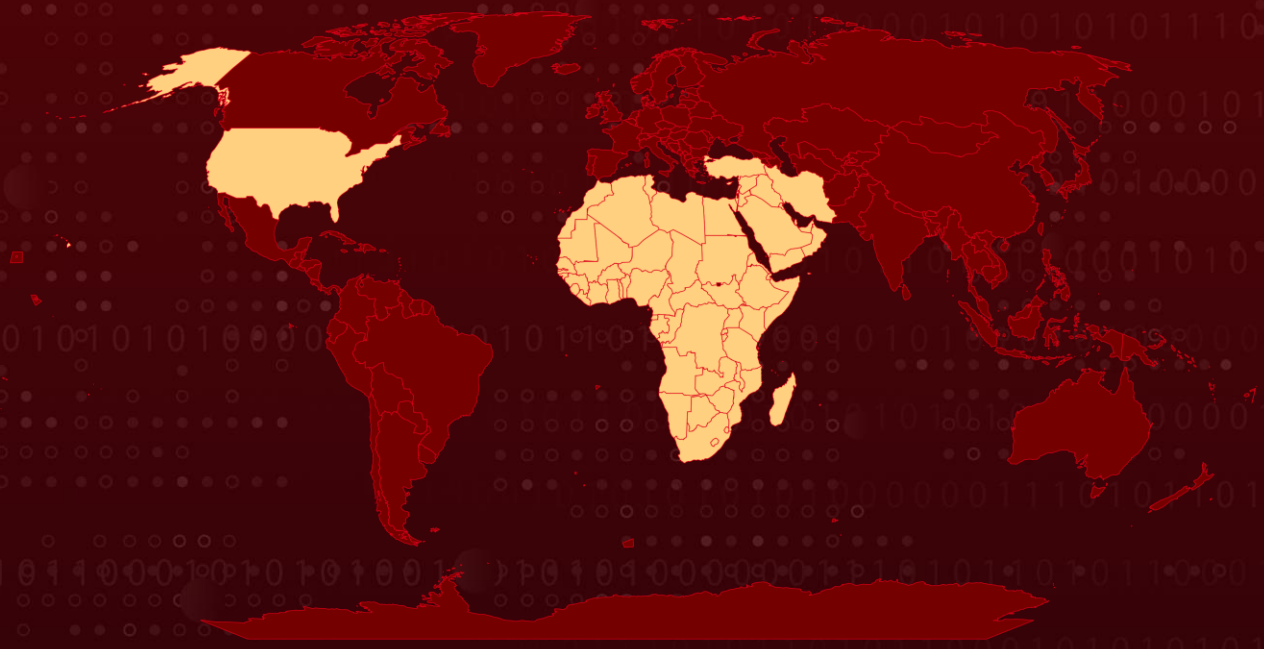
## Novel Tool Set Targeting Entities in the Middle East, Africa, and U.S.


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| December 05, 2023 | A1 | TA2023487 |

# Summary

**Attack Discovered:** December 2023
**Attack Region:** Middle East, Africa and the U.S
**Targeted Industry:** Education, Real estate, Retail, Non-profit organizations, Telecom companies, Governments
**Malware:** Agent Racoon, Ntospy
**Attack:** An undisclosed threat actor has targeted organizations in the Middle East, Africa, and the U.S., deploying a newly identified backdoor named Agent Racoon. The attacker utilizes tools like Ntospy and a customized version of Mimikatz called Mimilite to carry out malicious activities.

## Attack Regions



# Attack Details

**#1** An undisclosed threat actor has targeted organizations in the Middle East, Africa, and the U.S., deploying a recently discovered backdoor known as Agent Racoon. The attacker employs tools such as Ntospy and a customized version of Mimikatz called Mimilite to conduct various malicious activities. These activities include establishing backdoor capabilities, executing C2 operations, stealing credentials, and exfiltrating confidential information.

**#2** The threat actor strategically utilized specific tool components, deploying them across multiple organizations through temporary directories. Key tools employed include Ntospy, Mimilite, and the Agent Racoon malware, with a particular focus on nonprofit and government-related environments. Following each attack, cleanmgr.exe was employed to tidy up the compromised environment.

**#3** The threat actor employed a custom DLL module known as Ntospy to illicitly acquire user credentials during the authentication process. This malware implements Microsoft's network protocol interface. The attacker registered the Ntospy DLL module as a Network Provider, allowing them to hijack the authentication process and obtain unauthorized access to user credentials.

**#4** Mimilite is a tailored variant of Mimikatz employed by threat actors for the purpose of collecting credentials and sensitive information. It necessitates a password and employs a stream cipher for payload decryption. Verification of successful decryption is conducted through a comparison of the MD5 hash. Upon successful execution, the tool extracts credentials, storing them in the file masquerading as a legitimate Microsoft update file.

**#5** The Agent Racoon malware, developed in the.NET framework, provides backdoor functionalities, including command execution, file uploading, and downloading. It employs DNS for establishing a concealed communication channel with the C2 server. The threat actor camouflages the binary as Google Update and MS OneDrive Updater binaries, making subtle adjustments to evade detection.

**#6** The targets of these attacks cut across diverse sectors. While the responsible threat actor remains unidentified, the nature of the targets, coupled with the sophisticated detection and defense evasion techniques employed, suggests a potential alignment with nation-state activities.

# Recommendations

**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.

**Network Segmentation:** Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of malware and prevent it from accessing critical systems and sensitive data.

**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 the systems.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence |
| **TA0004** Privilege Escalation | **TA0005** Defense Evasion | **TA0006** Credential Access | **TA0007** Discovery |
| **TA0008** Lateral Movement | **TA0009** Collection | **TA0010** Exfiltration | **TA0011** Command and Control |
| **T1003** OS Credential Dumping | **T1018** Remote System Discovery | **T1021** Remote Services | **T1021.006** Windows Remote Management |
| **T1027** Obfuscated Files or Information | **T1027.009** Embedded Payloads | **T1030** Data Transfer Size Limits | **T1036** Masquerading |
| **T1036.005** Match Legitimate Name or Location | **T1036.008** Masquerade File Type | **T1041** Exfiltration Over C2 Channel | **T1046** Network Service Discovery |

| | | | |
|---|---|---|---|
| T1047 Windows Management Instrumentation | T1053 Scheduled Task/Job | T1053.005 Scheduled Task | T1059 Command and Scripting Interpreter |
| T1059.001 PowerShell | T1059.003 Windows Command Shell | T1070 Indicator Removal | T1070.004 File Deletion |
| T1070.006 Timestomp | T1071 Application Layer Protocol | T1071.004 DNS | T1074 Data Staged |
| T1078 Valid Accounts | T1078.002 Domain Accounts | T1087 Account Discovery | T1087.002 Domain Account |
| T1112 Modify Registry | T1114 Email Collection | T1132 Data Encoding | T1132.001 Standard Encoding |
| T1136 Create Account | T1136.002 Domain Account | T1140 Deobfuscate/Decode Files or Information | T1505 Server Software Component |
| T1505.003 Web Shell | T1556 Modify Authentication Process | T1556.008 Network Provider DLL | T1560 Archive Collected Data |
| T1560.001 Archive via Utility | T1564 Hide Artifacts | T1564.002 Hidden Users | T1570 Lateral Tool Transfer |
| T1573 Encrypted Channel | T1573.001 Symmetric Cryptography | T1583 Acquire Infrastructure | T1583.001 Domains |
| T1583.002 DNS Server | T1587 Develop Capabilities | T1587.001 Malware | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | b855dfde7f778f99a3724802715a0baa |
| Registry key path | HKLM\SYSTEM\CurrentControlSet\Services\credman |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 2632bcd0715a7223bda1779e107087964037039e1576d2175acaf61d3759360f, ae989e25a50a6faa3c5c487083cdb250dde5f0ecc0c57b554ab77761bdaed996, e30f8596f1beda8254cbe1ac7a75839f5fe6c332f45ebabff88aadbce3938a19, 1a4301019bdf42e7b2df801e04066a738d184deb22afcad9542127b0a31d5cfa, e7682a61b6c5b0487593f880a09d6123f18f8c6da9c13ed43b43866960b7aa8e, 58e87c0d9c9b190d1e6e44eae64e9a66de93d8de6cbd005e2562798462d05b45, 7eb901a6dbf41bcb2e0cdcbb67c53ab722604d6c985317cb2b479f4c4de7cf90, f45ea12579f636026d29009190221864f432dbc3e26e73d8f3ab7835fa595b86, bcd2bdea2bfecd09e258b8777e3825c4a1d98af220e7b045ee7b6c30bf19d6df, 4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, e0748ce315037253f278f7f8f2820c7dd8827a93b6d22d37dafc287c934083c4, baed169ce874f6fe721e0d32128484b3048e9bf58b2c75db88d1a8b7d6bb938d, 3a2d0e5e4bfd6db9c45f094a638d1f1b9d07110b9f6eb8874b75d968401ad69c, 4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, 354048e6006ec9625e3e5e3056790afe018e70da916c2c1a9cb4499f83888a47, dee7321085737da53646b1f2d58838ece97c81e3f2319a29f7629d62395dbfd1, 086a6618705223a88734484657l7e288cf7cc6a3af4d9bf18ddd44df6f400488 |
| Domain | geostatcdn[.]com, telemetry.geostatcdn[.]com, fdsb.telemetry.geostatcdn[.]com, dlbh.telemetry.geostatcdn[.]com, lc3w.telemetry.geostatcdn[.]com, hfhs.telemetry.geostatcdn[.]com, geoinfocdn[.]com, telemetry.geoinfocdn[.]com, g1sw.telemetry.geoinfocdn[.]com |

| TYPE | VALUE |
| --- | --- |
| File path | C:\Windows\Temp\install.bat,<br>c:/programdata/microsoft/~ntuserdata.msu,<br>c:/programdata/packag~1/windows 6.1-kb4537803.msu,<br>c:/programdata/package cache/windows10.0-kb5009543-x64.msu,<br>c:/programdata/package cache/windows10.0-kb5000736-x64.msu,<br>c:\windows\system32\ntoskrnl.dll,<br>C:\Windows\Temp\ntos.dll,<br>C:\Windows\Temp\ntoskrnl.dll,<br>C:\temp\update.exe,<br>c:/windows/temp/onedriveupdater.exe,<br>c:/windows/system32/msmdlb.exe,<br>c:/windows/temp/onedriveupdater.exe,<br>c:/program files (x86)/google/update/googleupdate.exe,<br>c:\windows\temp\mslb.ps1,<br>c:\windows\temp\set_time.bat,<br>c:\windows\temp\pscan.ps1,<br>c:\windows\temp\crs.ps1,<br>c:\windows\temp\usr.ps1,<br>c:\windows\temp\pb.ps1,<br>c:\windows\temp\ebat.bat,<br>c:\windows\temp\pb1.ps1,<br>c:\windows\temp\raren.exe |

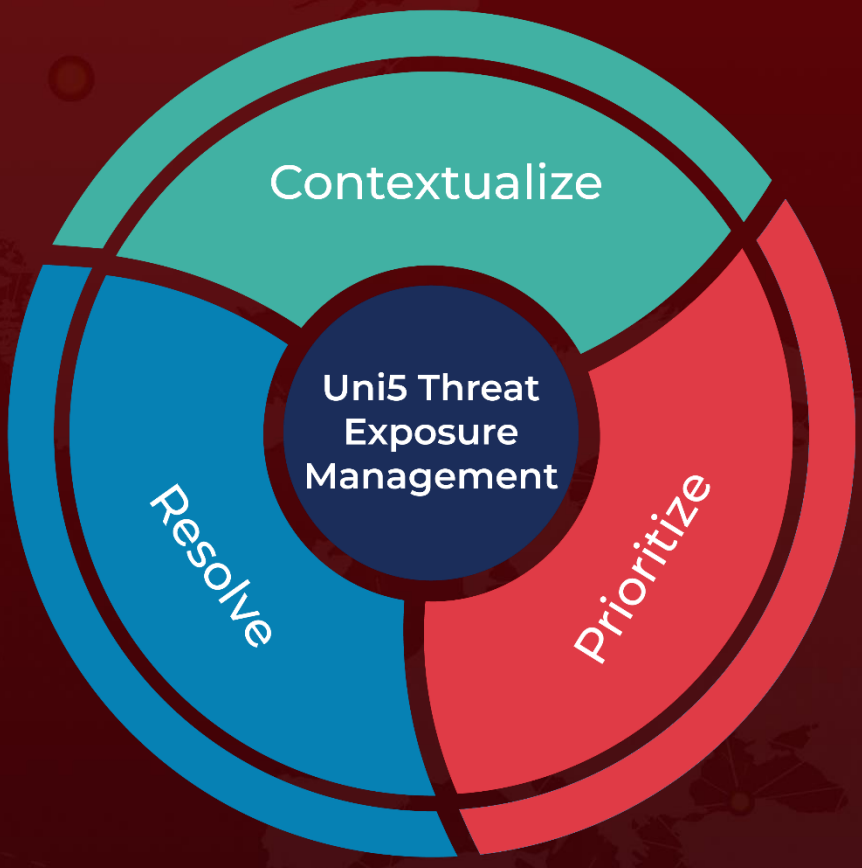
# References

https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/

# 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

**December 05, 2023 . 4:30 AM**



More at www.hivepro.com