Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

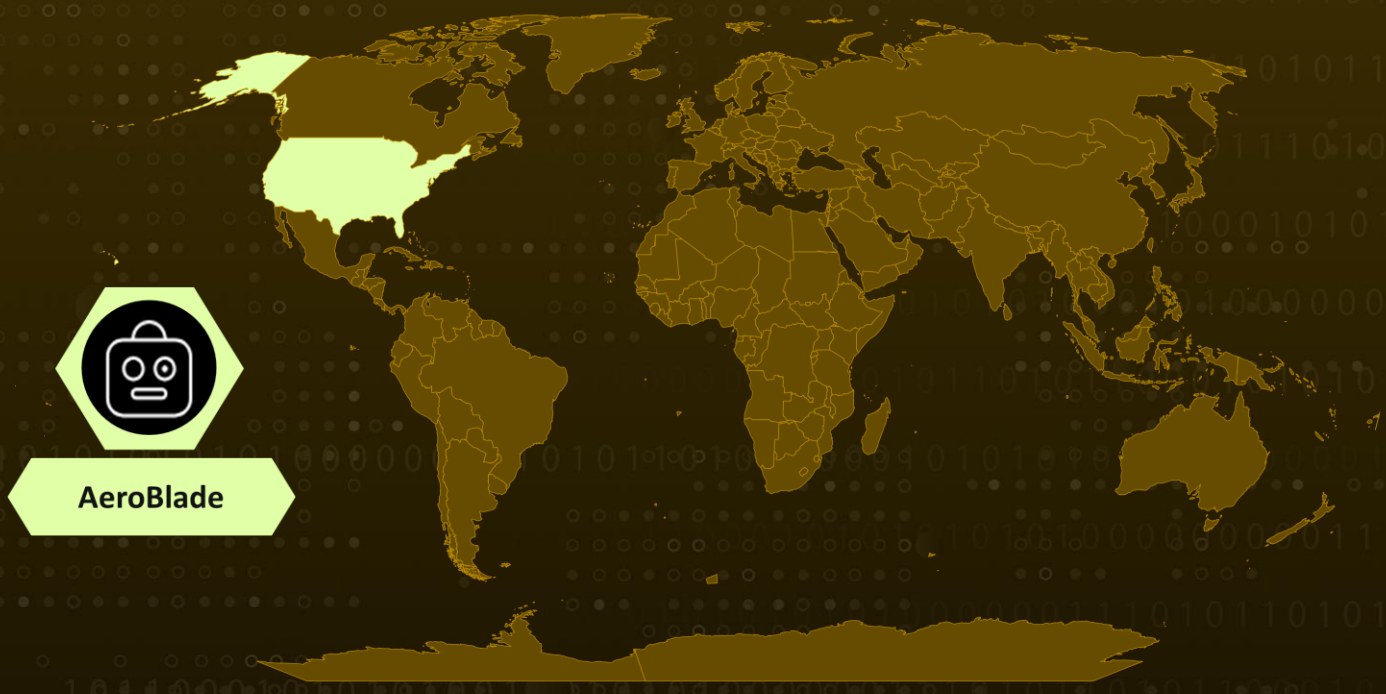
AeroBlade Swoops Down on U.S. Aerospace Giants

Date of Publication	Admiralty Code	TA Number
December 5, 2023	A1	TA2023488

Summary

Attack Began: September 2022
Actor Name: AeroBlade
Target Region: United States
Target Sectors: Aerospace

Actor Map



Actor Details

#1 A US-based aerospace corporation fell victim to an extensive, year-long commercial cyberespionage campaign orchestrated by the entity identified as AeroBlade. The onset of this sophisticated attack, in September 2022, involved spear-phishing as the primary delivery mechanism.

#2 A weaponized document, discreetly embedded within an email attachment, carried a remote template injection technique and malicious VBA macro code, paving the way for subsequent stages leading to the final payload execution. The culmination of this attack chain saw the activation of a dynamic-link library (DLL) acting as a reverse shell.

#3 This DLL established a connection with a pre-programmed command-and-control (C2) server, facilitating the transmission of critical system information to the perpetrators. The scope of information gathering extended to a comprehensive enumeration of directories on the compromised host, suggesting a reconnaissance effort aimed at identifying valuable data and assisting AeroBlade in formulating strategic next steps.

#4 The DLL employed robust obfuscation techniques, incorporating measures to prevent disassembly. The executable featured control flow obfuscation and the deliberate execution of dead code instructions. This strategic approach does not impact the malware but introduces an additional layer of complexity to the analysis.

#5 Dead code, in this context, denotes a section in the program's source code that executes without yielding any meaningful result in subsequent computations. AeroBlade's likely objective was to enhance visibility into the internal resources of its target, evaluating its vulnerability to a potential future ransom demand.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
AeroBlade	Unknown **MOTIVE** Information theft and espionage	United States	Aerospace

Recommendations

Implement Email Security Measures: Deploy advanced email filtering systems to detect and block malicious attachments and links. Utilize email authentication mechanisms to prevent the infiltration of forged emails.

Network Security: Enhance network security measures, including firewalls and intrusion detection/prevention systems, to detect and block unauthorized access attempts. Monitor network traffic for anomalous patterns and behaviors indicative of APT activities.

Enable Audit Logging: Activate audit logging for DLL loading events on Windows endpoints. This allows for the collection of detailed information about DLL loads, helping security teams identify anomalous behavior.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1001** Data Obfuscation
T1016 System Network Configuration Discovery	**T1027** Obfuscated Files or Information	**T1598.002** Spearphishing Attachment	**T1029** Scheduled Transfer
T1033 System Owner/User Discovery	**T1041** Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1059.003** Windows Command Shell
T1059.005 Visual Basic	**T1071.001** Web Protocols	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1105 Ingress Tool Transfer	**T1106** Native API	**T1137.001** Office Template Macros	**T1140** Deobfuscate/Decode Files or Information
T1203 Exploitation for Client Execution	**T1204.002** Malicious File	**T1221** Template Injection	**T1559.002** Dynamic Data Exchange

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	16bd34c3f00288e46d8e3fdb67916aa7c68d8a0622f2c76c57112dae36c76875, 6d515dafef42a5648754de3c0fa6adfcb8b57af1c1d69e629b0d840dab7f91ec, abc348d3cc40521afc165aa6dc2d66fd9e654d91e3d66461724ac9490030697f
MD5	885b04081bd89f5e23cbc59723052601, 62d3ff36ec8a721488e512e1c94b2744, a04d2c0aa0a798047161118b5d5816aa

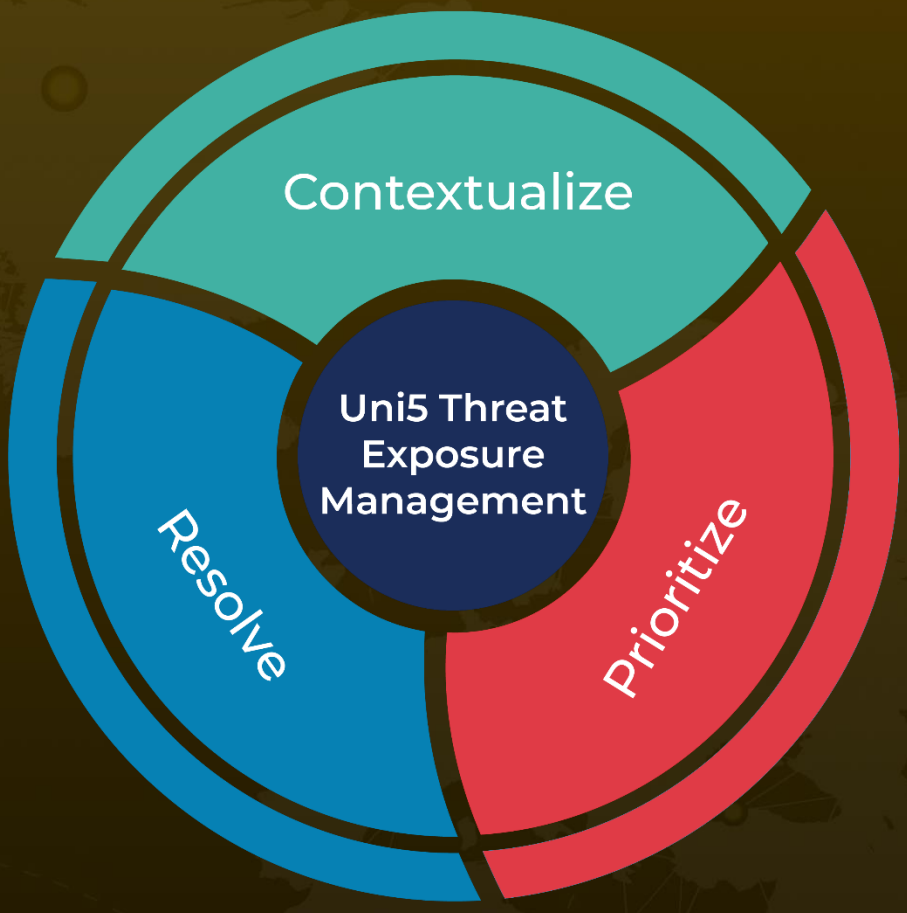
References

https://blogs.blackberry.com/en/2023/11/aeroblade-on-the-hunt-targeting-us-aerospace-industry

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 5, 2023 . 6:00 AM

More at www.hivepro.com