Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

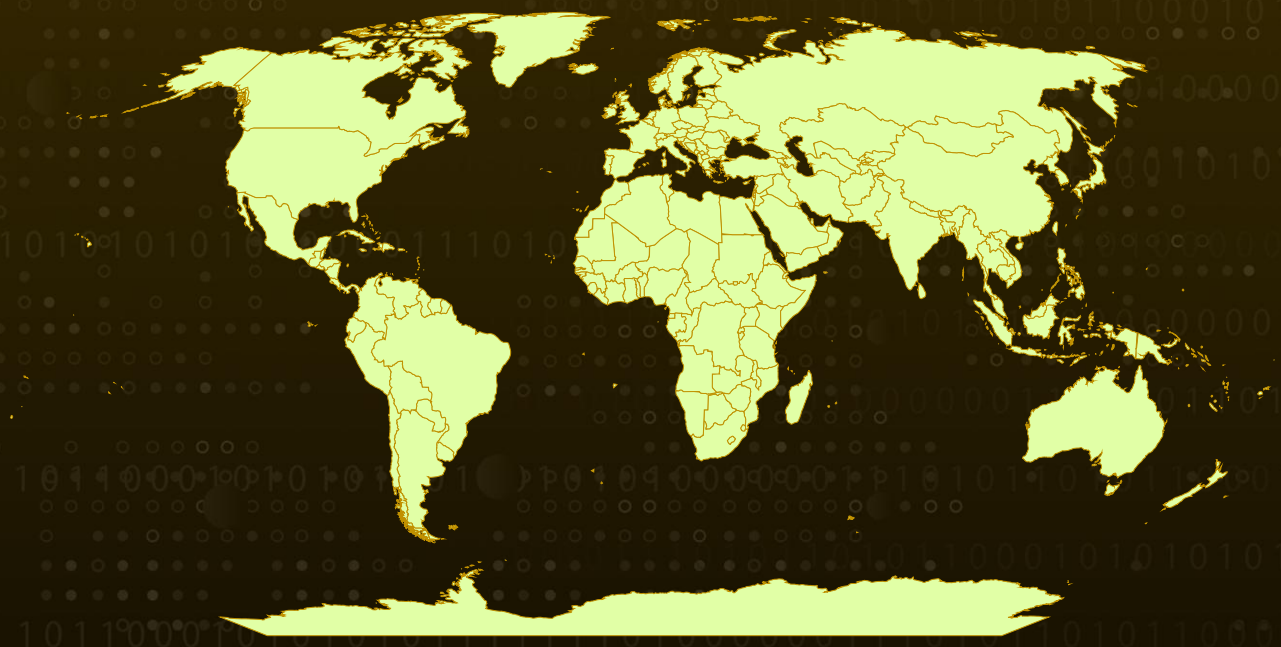
Unmasking Airstalk's Covert Supply Chain Intrusion

Date of Publication	Admiralty Code	TA Number
November 7, 2025	A1	TA2025339

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Malware: Airstalk
Affected Platform: Windows
Threat Cluster: CL-STA-1009
Attack: Airstalk is a stealthy Windows-based malware family uncovered in both PowerShell and .NET variants, designed to exploit Workspace ONE's (formerly AirWatch) API for covert command-and-control communication. Believed to be deployed by a nation-state actor in a sophisticated supply chain attack, it uses legitimate enterprise infrastructure to secretly exfiltrate sensitive browser data, screenshots, and activity logs. By hiding within trusted Mobile Device Management (MDM) systems and using a stolen digital certificate, Airstalk blurs the line between normal operations and espionage, posing a serious threat to organizations that rely on third-party vendors and BPO services for critical business functions.

Attack Regions



Attack Details

#1 Airstalk is a newly identified Windows-based malware family available in both PowerShell and .NET variants, believed to be the work of a nation-state threat actor involved in a sophisticated supply chain attack. The malware exploits the AirWatch API, now known as Workspace ONE Unified Endpoint Management (UEM), to create a covert C2 channel that blends seamlessly within legitimate network activity. Airstalk's core purpose is to exfiltrate sensitive browser data, including cookies, browsing history, bookmarks, and screenshots. It employs multi-threaded communication, incorporates versioning for development tracking, and even uses a possibly stolen digital certificate for sample signing, enhancing its credibility and stealth.

#2 The PowerShell variant of Airstalk establishes C2 communication through the AirWatch Mobile Device Management (MDM) API, using the endpoint as a dead-drop channel. Here, communication data is stored as custom attributes on compromised devices, allowing attackers to exchange information indirectly without real-time interaction. Additionally, the malware can upload files via the endpoint to support its operational requirements. Messages are exchanged in structured JSON format containing fields, ensuring that communications are well-organized and traceable within the attacker's infrastructure. This sophisticated use of legitimate enterprise APIs allows Airstalk to hide its malicious traffic in plain sight.

#3 Once the connection is established, Airstalk's PowerShell variant awaits task instructions from its operators, executing commands classified under various values. Interestingly, one of the identifiers appears deliberately omitted, likely to conceal certain functionalities or represent a reserved capability. The malware's ability to exfiltrate browser cookies through remote debugging is particularly concerning, as it allows unauthorized access to user sessions without directly stealing credentials. When integrated into a trusted MDM environment, these actions become even harder to detect, making Airstalk an especially discreet and dangerous tool.

#4 Further analysis uncovered a more advanced .NET variant of Airstalk, showing clear evolution from the PowerShell version. This iteration expands its reach by targeting not only Google Chrome but also Microsoft Edge and Island Browser. The .NET version introduces enhanced obfuscation, new communication mechanisms, and multiple dedicated execution threads that handle C2 management, debug log exfiltration, and regular beaconing every ten minutes. It also incorporates version tracking; samples have been identified with versions 13 and 14 and use legitimate-looking code signing to disguise themselves as a benign legacy application.

#5 With moderate confidence, this activity attributes Airstalk's deployment to a suspected nation-state threat actor, designated as cluster CL-STA-1009, likely involved in a targeted supply chain intrusion. Such attacks often focus on critical vendors and Business Process Outsourcing (BPO) firms that handle sensitive operational data for multiple organizations. By compromising a single BPO, adversaries can gain simultaneous access to numerous downstream clients making these entities highly valuable targets.

Recommendations

- **Review and Monitor MDM Activity Closely:** Regularly audit Mobile Device Management (MDM) and Workspace ONE configurations. Look for unusual API calls, especially those writing or modifying device attributes, to detect hidden communication channels like those used by Airstalk.
- **Validate Certificates and Signing Sources:** Ensure that all software and executables are signed with legitimate and active certificates. Flag any binaries signed with expired or revoked certificates, as Airstalk abused a stolen certificate to appear trustworthy.
- **Watch for Abnormal Browser Data Access:** Implement browser isolation or endpoint protection solutions that monitor unauthorized attempts to access or extract browser cookies, history, or bookmarks. These data points are Airstalk's key targets for session hijacking.
- **Strengthen Endpoint Visibility and Logging:** Enable detailed logging for PowerShell and .NET executions. Correlate event logs with network data to uncover unusual process behaviors or scripts interacting with enterprise APIs.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1102 Web Service	T1071 Application Layer Protocol	T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers	T1113 Screen Capture	T1059 Command and Scripting Interpreter	T1059.001 PowerShell

T1083 File and Directory Discovery	**T1217** Browser Information Discovery	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task
T1218 System Binary Proxy Execution	**T1195** Supply Chain Compromise	**T1567** Exfiltration Over Web Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0c444624af1c9cce6532a6f88786840ebce6ed3df9ed570ac75e07e30b0c0bde, 1f8f494cc75344841e77d843ef53f8c5f1beaa2f464bcbe6f0aacf2a0757c8b5, dfdc27d81a6a21384d6dba7dcdc4c7f9348cf1bdc6df7521b886108b71b41533, b6d37334034cd699a53df3e0bcac5bbdf32d52b4fa4944e44488bd2024ad719b, 4e4cbaed015dfbda3c368ca4442cd77a0a2d5e65999cd6886798495f2c29fcd5, 3a48ea6857f1b6ae28bd1f4a07990a080d854269b1c1563c9b2e330686eb23b5

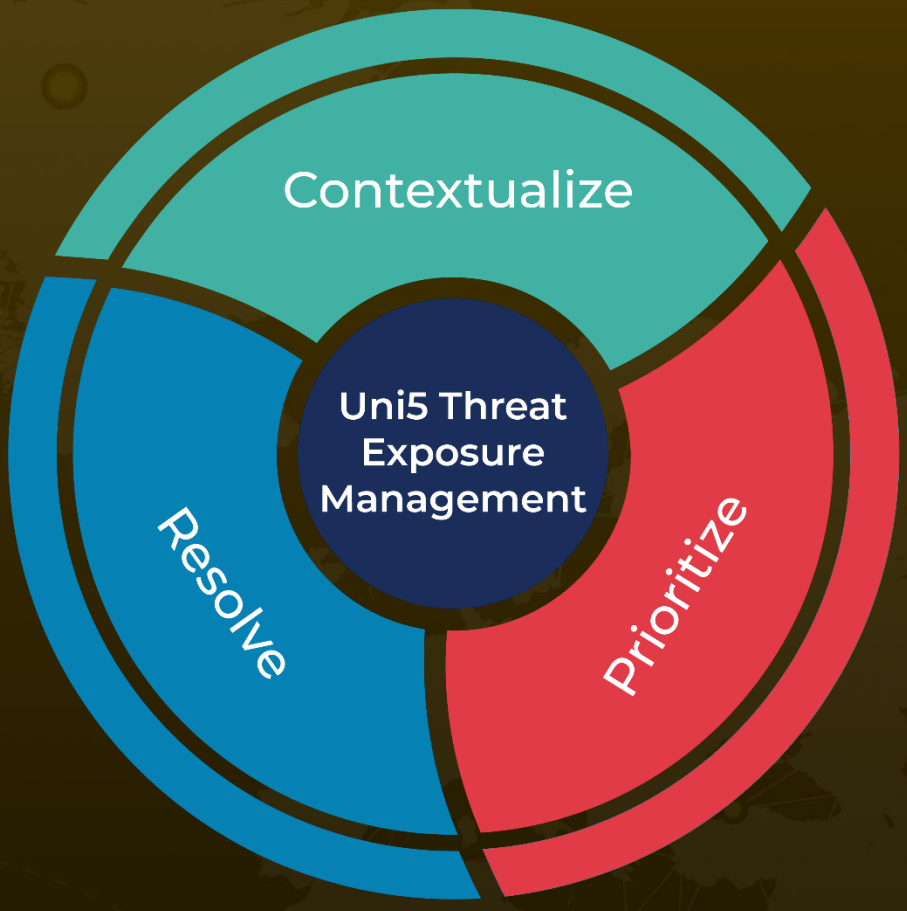
References

https://unit42.paloaltonetworks.com/new-windows-based-malware-family-airstalk/

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

November 7, 2025 • 7:00 AM

More at www.hivepro.com