Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

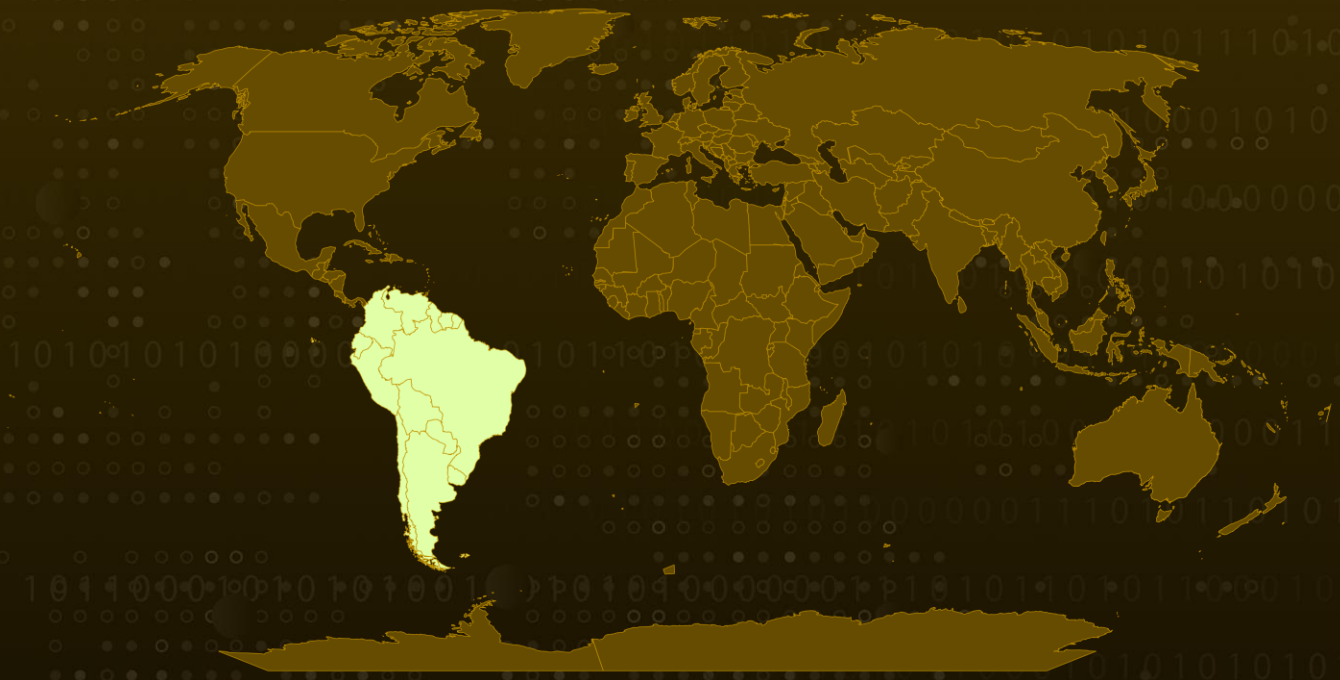
BITSLOTH Backdoor Leverages BITS for C2

Date of Publication	Admiralty Code	TA Number
August 5, 2024	A1	TA2024295

Summary

First Seen: June 2024
Malware: BITSLOTH Backdoor
Affected OS: Windows
Targeted Region: South America
Targeted Industry: Government
Attack: BITSLOTH is a newly discovered, highly advanced Windows backdoor malware. Leveraging the Background Intelligent Transfer Service (BITS) for its command-and-control (C2) mechanism, BITSLOTH highlights the technical prowess of its likely Chinese developers. First identified in June 2024, this malware has been linked to a significant cyber attack on the Foreign Ministry of a South American government.

Attack Regions



Attack Details

#1 The recently identified malware strain, BITSLOTH, is an undocumented Windows backdoor that leverages a built-in feature called Background Intelligent Transfer Service (BITS) as its command-and-control (C2) mechanism. BITSLOTH includes logging functions and strings, suggesting that its creators are native Chinese speakers.

#2 BITSLOTH offers a broad range of capabilities, such as discovery, enumeration, and command-line execution, indicating its purpose is to collect data from targeted victims. Discovered in June 2024, BITSLOTH was connected to a cyber attack on an undisclosed Foreign Ministry of a South American government.

#3 This activity cluster is tracked under the codename REF8747. Following initial access, the attacker moved laterally within the network, deploying BITSLOTH as a DLL in the ProgramData directory before executing the FL Studio music-making program.

#4 BITSLOTH can run and execute commands, upload and download files, perform enumeration and discovery, and harvest sensitive data through keylogging and screen capturing.

#5 Furthermore, BITSLOTH can configure its communication mode to either HTTP or HTTPS, remove or reconfigure persistence, terminate arbitrary processes, log users off, restart or shut down the system, and even update or delete itself from the host. A defining feature of this malware is its use of BITS for C2 communications.

Recommendations

Enhance Network Monitoring: Use network monitoring tools to track unusual activity, especially communication channels utilizing BITS or similar services. Implement network segmentation to limit lateral movement of potential threats.

Integrate Sysmon logs with SIEM Solutions: Integrate Sysmon logs with Security Information and Event Management (SIEM) solutions for centralized analysis and alerting. This helps in correlating Sysmon events with other security data for comprehensive threat detection.

Use File Integrity Monitoring (FIM): Implement file integrity monitoring to detect unauthorized changes to critical system files and directories. Monitor the ProgramData directory for the creation of unexpected DLL files. Define, reassess, and update baseline profiles for critical files and directories to understand normal behavior. Periodically reflect changes in your environment, such as software updates or system modifications.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1197 BITS Jobs	**T1082** System Information Discovery	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading
T1113 Screen Capture	**T1056** Input Capture	**T1056.001** Keylogging	**T1090** Proxy
T1543 Create or Modify System Process	**T1562** Impair Defenses	**T1070** Indicator Removal	**T1573** Encrypted Channel
T1070.004 File Deletion	**T1529** System Shutdown/Reboot	**T1036** Masquerading	**T1071** Application Layer Protocol
T1059 Command and Scripting Interpreter			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	216[.]238[.]121[.]132, 45[.]116[.]13[.]178, 15[.]235[.]132[.]67
SHA256	4a4356faad620bf12ff53bcfac62e12eb67783bd22e66bf00a19a4c404bf45df, dfb76bcf5a3e29225559ebbdae8bdd24f69262492eca2f99f7a9525628006d88, 4fb6dd11e723209d12b2d503a9fcf94d8fed6084aceca390ac0b7e7da1874f50, 0944b17a4330e1c97600f62717d6bae7e4a4260604043f2390a14c8d76ef1507, 0f9c0d9b77678d7360e492e00a7fa00af9b78331dc926b0747b07299b4e64afd
File Name	s.dll, 125.exe, setup_wm.exe, 1242.exe, flengine.dll
URL	hxxp[:]//updater[.]microsoft[.]com/index[.]aspx

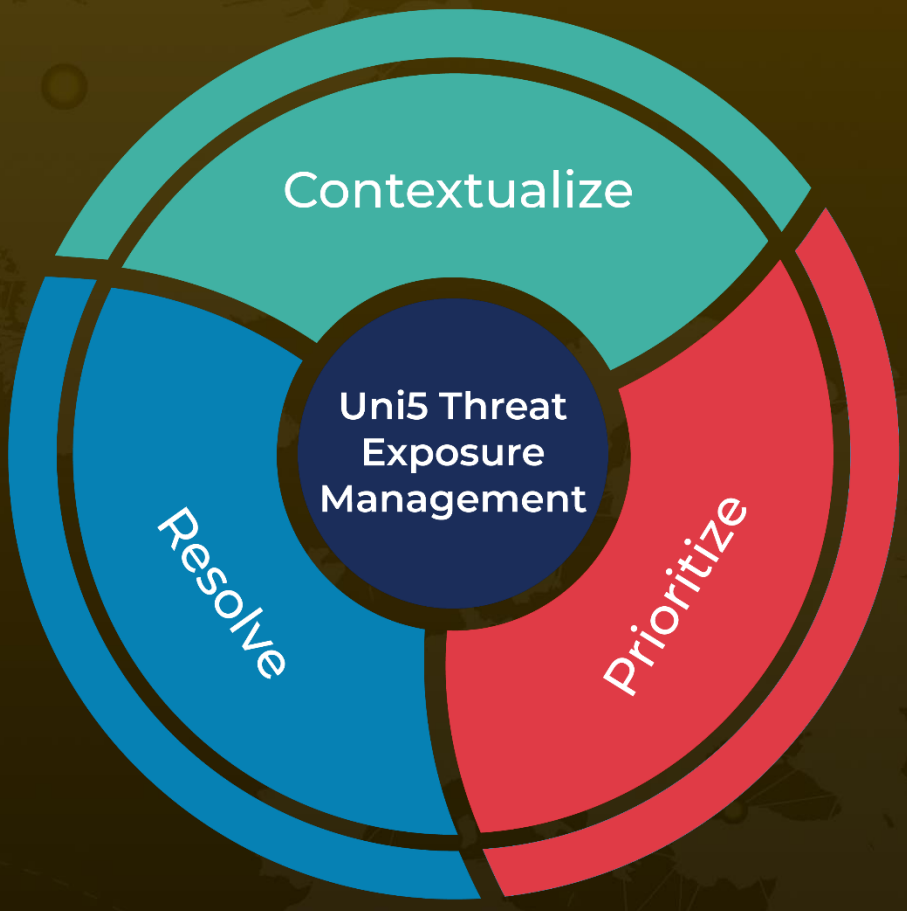
References

https://www.elastic.co/security-labs/bits-and-bytes-analyzing-bitsloth

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 • 9:00 PM

More at www.hivepro.com