Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

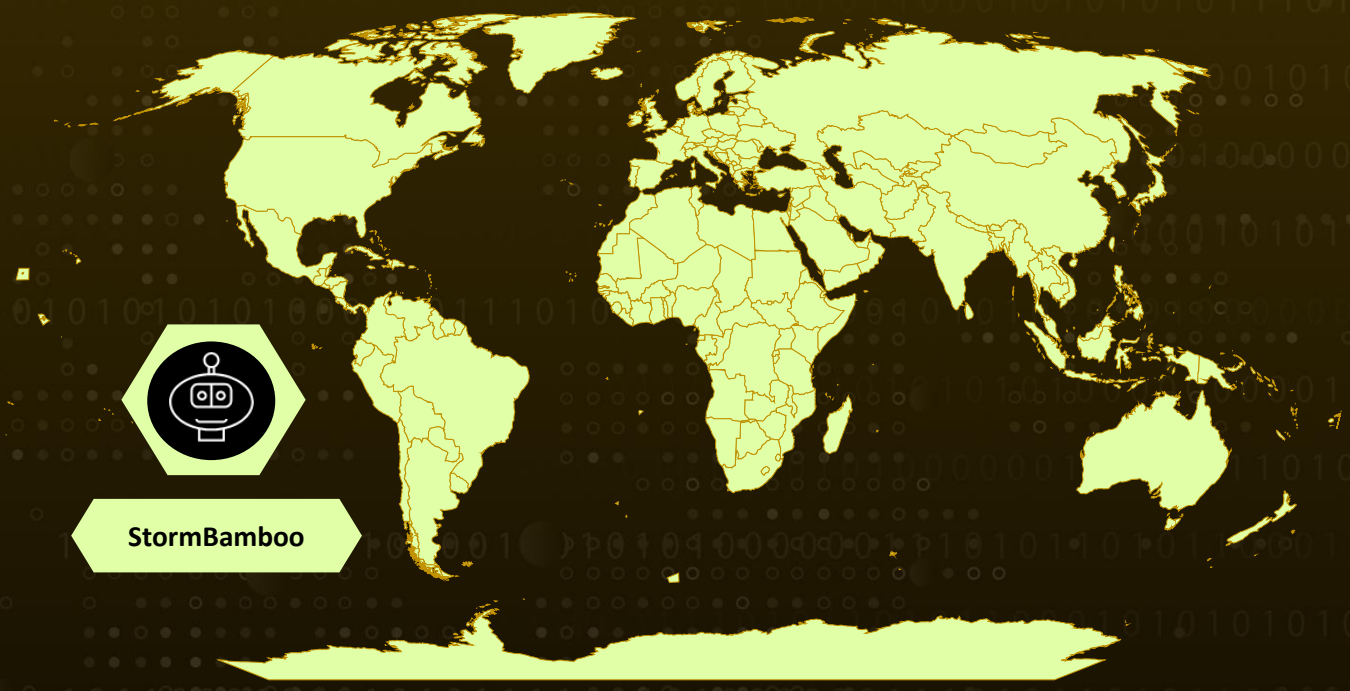
StormBamboo Abuses ISP to Push Malware via Software Updates

Date of Publication	Admiralty Code	TA Number
August 7, 2024	A1	TA2024301

Summary

Attack Began: 2023
Targeted Countries: Worldwide
Malware: MACMA and POCOSTICK (aka MGBot)
Affected Platform: Windows and macOS
Threat Actor: StormBamboo (aka Evasive Panda, StormCloud)
Attack: The StormBamboo group executed a sophisticated attack by compromising an ISP and using DNS poisoning to redirect software updates to malicious servers, installing MACMA and POCOSTICK malware on macOS and Windows systems. This malware facilitated data exfiltration and installed a stealthy browser extension for persistent access. The attack exploited insecure update mechanisms, highlighting the need for robust integrity checks and enhanced DNS security.

Attack Regions



Attack Details

#1 The StormBamboo group executed a sophisticated cyberattack by compromising an internet service provider (ISP) to exploit insecure software update mechanisms. The attackers employed DNS poisoning to manipulate DNS responses, redirecting legitimate software update requests to malicious servers. This led to the download and installation of malware on both macOS and Windows systems, specifically MACMA and POCOSTICK.

#2 The malware facilitated follow-on activities, including data exfiltration and the installation of a malicious browser extension designed to maintain persistent access and steal data. This extension operated stealthily, complicating detection and enabling prolonged exploitation of the infected systems.

#3 The attackers use a similar workflow to a previous incident attributed to DriftingBamboo, a possibly related threat actor. In a previous incident, DriftingBamboo used DNS poisoning to modify content of pages users browsed; however, in this case, the attackers abuse insecure automatic update mechanisms.

#4 The attack exploited the lack of integrity checks in the software update process, demonstrating a significant vulnerability in the way automatic updates are managed. The attackers' ability to manipulate DNS responses highlighted the need for improved DNS security and secure update mechanisms.

Recommendations

Use Secure Update Mechanisms: Ensure all software updates are delivered over HTTPS to prevent man-in-the-middle attacks. Verify the integrity and authenticity of updates using cryptographic signatures.

Regular Security Audits: Conduct regular security assessments of your infrastructure, focusing on DNS security and software update mechanisms to identify and address vulnerabilities.

Implement DNS Security Measures: Utilize DNS Security Extensions (DNSSEC) to protect against DNS poisoning by ensuring the authenticity and integrity of DNS data.

ISP-Level Protections: ISPs should deploy advanced threat detection systems and DNS filtering to identify and mitigate malicious activities targeting their networks.

Strengthen Network Security: Implement network segmentation to limit the spread of malware within the organization. Use firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to detect and block malicious traffic. Monitor network traffic for unusual activities and connections to known malicious domains.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0009 Collection	TA0006 Credential Access
TA0011 Command and Control	TA0005 Defense Evasion	TA0003 Persistence	TA0010 Exfiltration
TA0042 Resource Development	T1566 Phishing	T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information
T1071.004 DNS	T1557 Adversary-in-the-Middle	T1071 Application Layer Protocol	T1588.004 Digital Certificates
T1588 Obtain Capabilities	T1584.001 Domains	T1584 Compromise Infrastructure	T1059.007 JavaScript
T1176 Browser Extensions	T1059.002 AppleScript	T1185 Browser Session Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	6abf9a7926415dc00bcb482456cc9467, ee28b3137d65d74c0234eea35fa536af
IPv4	103[.]96[.]130[.]107, 122[.]10[.]90[.]20

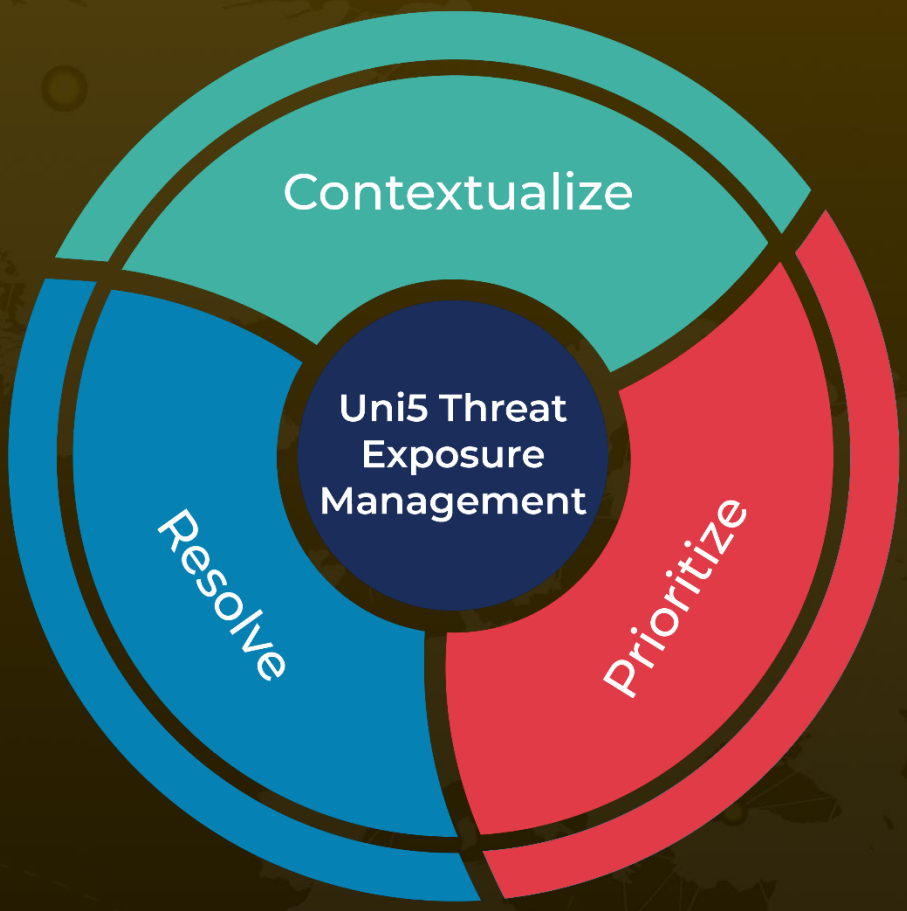
References

https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

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 7, 2024 • 6:00 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com