StormBamboo uses Internet Service Providers to deploy DNS poisoning campaign

Original report published on: August 2, 2024[1]

Executive Summary

In mid-2023, Volexity discovered that the StormBamboo group, known for cyberespionage targeting Asia, successfully compromised an Internet service provider (ISP) to breach target organisations. Researchers mentioned initial access was via Domain Name System (DNS) poisoning attack at the ISP level. Automatic software updates were redirected to StormBamboo's server to deliver malware such as MGBot and MACMA. Impact includes exfiltration of victim's mail data. The ISP, upon discovering the compromise, took swift action to stop the DNS poisoning.

Background

On 1 August 2024, Volexity published about StormBamboo (alias Evasive Panda) group successfully compromising Internet Service Providers (ISP) via DNS poisoning to deploy MACMA malware on macOS or MgBot (POCOSTICK) on Windows systems. StormBamboo targets software updates via HTTP that do not validate digital signatures of installers.

Volexity investigations revealed that DNS poisoning occurred further upstream at the ISP which upon reboot, took network components offline ceasing the DNS poisoning. The attacker's method of delivering malware has evolved, abusing insecure automatic update mechanisms present in software in the victim's environment, thus requiring no user interaction. It is observed that StormBamboo targets multiple software vendors, who use insecure update workflows.

The attacker has control of the DNS response for any given DNS name and abuses this design by redirecting the HTTP request to a Command and Control (C2) server they control hosting a forged text file and a malicious installer. The installer eventually downloads either MGBot malware for Windows or MACMA for macOS.

MgBOT is a modular framework with various plugins enabling network scanning, information stealing from browser, keylogging and password dumping. MACMA is able to perform device fingerprinting, keylogging, executing commands, screen and audio capture, and uploading/downloading files.

Upon compromise of a macOS device, a customised Google Chrome extension (RELOADEXT) is installed and activated by running AppleScript command. Browser cookies and data are encoded with base64 and exfiltrated to a Google Drive using AES encryption.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Use Domain Name System Security Extensions (DNSSEC) to protect against DNS poisoning by ensuring the authenticity and integrity of DNS data.
- Enable 2 Factor Authentication (2FA) for access to DNS if possible.

- Configure your DNS server to use random source ports for outgoing DNS queries to make it difficult for attackers to predict and spoof the source port in DNS responses.
- Adjust the TTL of your DNS caching servers to help with any DNS cache poisoning issues. Lower TTLs will naturally decrease the number of DNS queries that could be led to the wrong address.
- Flush your DNS cache periodically.
- Scan for Indicators of Compromise (IOCs) on your network. Validate before adding malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR). YARA rules are available here.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise (IOCs)

IP Address	Description
103[.]96[.]130[.]107	C2 server used during the DNS poisoning
152[.]32[.]159[.]8	MACMA C2 Server
122[.]10[.]90[.]20	CATCHDNS C2
122[.]10[.]89[.]110	CATCHDNS C2
59[.]188[.]69[.]231	CATCHDNS C2

File Hash	Hash Type	Description
049e8677406de5f0061f3960f9655b5f	MD5	CATCHDNS
d14431e79dc109d7aad91a5411d406c99ffc524c	SHA1	
4f3d35f4f8b810362cbd4c59bfe5a961e559fe5713c9478294ccb3af2d306515	SHA256	
ce5fdde7db4ee41808f9c7d121311f78	MD5	CATCHDNS
bb030c405f33557bc5441165a0f8bf9a6d5a82a6	SHA1	
3f76933e053b2e8e3458f2e69d72e10b6b6a97fb8ba0f0300aa415b99c032aea	SHA256	
2a6c10a34fa1e2a38673f4ca20c303a1	MD5	CATCHDNS
038bc60a0bf004e9a7cbc3a3cf814613e61ba7cc	SHA1	
17aebd011dcd3e7c11484c2f98fa0901c2ea1325fdd6c03904d30ebfc8747a99	SHA256	
ee28b3137d65d74c0234eea35fa536af	MD5	RELOADEXT installer
66346b3d841dc56a387f48b4dfba96083c37ec2e	SHA1	
07e3b067dc5e5de377ce4a5eff3ccd4e6a2f1d7a47c23fe06b1ededa7aed1ab3	SHA256	
4958ede3b968ad464c983054479bf4d2	MD5	MACMA keylogger
68853cafd395edd08cd38ab6100c58e291a3a3d7	SHA1	
77406e090ad9214942d7ca91ddd09b0435bafe42ffa2512819a7bc6cdec112b8	SHA256	
6abf9a7926415dc00bcb482456cc9467	MD5	RELOADEXT extension
c68e86985a4cb2f69e16fb943723af63833859b3	SHA1	
7e2e1fba2fabf677d08611a59b03d646a92bb6110182b61adae207c8a88b6d13	SHA256	
25e4eef79ad4126d5dc5567949848070	MD5	MACMA sample
37ee872f05a0273446dc7e2539b9dbf9bf7d80b4	SHA1	
806eabfa6ee245eaaf817c0336e07982fffc42efb1f39a2bfb44a5db2c89b126	SHA256	
acfc69c743b733dd80c1d551ae01172b	MD5	

84875b2cf9f8c778ff1462ef478918b4ac964afe	SHA1	MACMA-GIMMICK sample
b76a9034e9abc7a62171e80f9d1f7fdf565cda286bd10fd3984eae769113c8c5	SHA256	
4c8a326899272d2fe30e818181f6f67f	MD5	DUSTPAN malware
e8e4a3fa69173a46cdb60c53877c7ad557accc51	SHA1	
b77bcfb036f5a6a3973fdd68f40c0bd0b19af1246688ca4b1f9db02f2055ef9d	SHA256	

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1659	Content Injection
Initial Access	T1195	Supply Chain Compromise
Execution	T1203	Exploitation for Client Execution
Execution	T1059	Command and Scripting Interpreter
Persistence	T1546.016	Event Triggered Execution - Installer Packages
Persistence	T1176	Browser Extensions
Defense Evasion	T1027	Obfuscated Files or Information
Credential Access	T1539	Steal Web Session Cookie
Collection	T1056.001	Input Capture: Keylogging
Command and Control	T1071	Application Layer Protocol
Exfiltration	T1567.002	Exfiltration to Cloud Storage

References

1. ^ “StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms .