

Stonefly APT's Advanced Extortion Campaign: A Persistent Threat to U.S. Critical Infrastructure

Campaign Analysis:

- **Threat Actor:** Andariel (APT45, DarkSeoul, Onyx Sleet, Silent Chollima, Stonefly/Clasiopa)
 - **The adversary tries to** extort organizations **by** targeting critical data **using** data exfiltration techniques (T1567.002).
 - **The modus operandi is** financial extortion **through** targeted attacks on critical infrastructure using customized backdoor malware.
 - **The entry point of the attack is** reconnaissance and spear-phishing **through** the use of malicious attachments and exploiting known vulnerabilities (Cyber Kill Chain).
 - **The attack sophistication is** high **due to** the customized nature of malware, long-term persistence, and targeted approach, combined with multiple stages of data exfiltration and encryption.
 - **The attack vector is** MITRE ATT&CK IDs **T1486 (Data Encrypted for Impact), T1005 (Data from Local System), T1059 (Command and Scripting Interpreter)** for encrypting sensitive files to cause disruption, collecting information from compromised systems, and executing scripts or shell commands to maintain control and exploit systems.
 - **The recommended defence-in-depth is** enforcing network segmentation, regularly updating software patches, employing robust intrusion detection systems (IDS) for abnormal outbound traffic, and implementing email filtering with anti-phishing mechanisms.
 - **Start investigating by** monitoring network activity for known C2 infrastructure associated with Stonefly APT and analyzing endpoint activity for signs of lateral movement or anomalous system behaviour.
-

Malware Infection Killchain Flow:

1. **Delivery:** Phishing email with a malicious document attachment (.docx or .pdf) containing macros.
 2. **Execution:** When opened, the macro executes a malicious script that downloads the malware payload.
 3. **Persistence:** The malware establishes persistence by modifying registry keys or adding scheduled tasks.
 4. **Privilege Escalation:** The malware exploits system vulnerabilities to gain elevated privileges.
 5. **Lateral Movement:** The malware moves through the network using stolen credentials or brute-forcing other machines.
 6. **Command and Control (C2):** The malware establishes encrypted communication with C2 servers to receive further instructions.
 7. **Exfiltration:** Sensitive data is exfiltrated over HTTPS to attacker-controlled servers.
 8. **Impact:** Data encryption occurs (T1486), followed by an extortion demand from the attackers.
-

High-Level Malware Process Flow:

- Phishing Email → Malicious Attachment → User Interaction → Macro Execution → Malware Download → PowerShell Command Execution → Persistence via Registry Modification → C2 Communication → Data Exfiltration (T1005) and Encryption (T1486).
-

Indicators of Compromise (IOCs):

- f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5 - Backdoor.Preft
- a65cefb3c2ccdb50704b1af1008a1f8c7266aa85bd24aaf21f6eb1ddd5b79c81 - Backdoor.Preft
- 12bf9fe2a68acb56eb01ca97388a1269b391f07831fd37a1371852ed5df44444 - Backdoor.Preft
- f0bc0f94ac743185e6d0c865a9e162f4ce2f306df13b2ea80df984160eb3363c - Backdoor.Preft
- 243ad5458706e5c836f8eb88a9f67e136f1fa76ed44868217dc995a8c7d07bf7 - Backdoor.Preft
- 96118268f9ab475860c3ae3edf00d9ee944d6440fd60a1673f770d150bfb16d3 - Backdoor.Preft
- 2b254ae6690c9e37fa7d249e8578ee27393e47db1913816b4982867584be713a - Backdoor.Preft
- 28149b1e55551948a629dcd2dacad32f6a197ed9324dc08b27ff00fa0bf0d909 - Chisel
- 485465f38582377f9496a6c77262670a313d8c6e01fd29a5dbd919b9a40e68d5 - Keylogger
- d867aaa627389c377a29f01493e9dff517f30db8441bf2ccc8f80c48eaa0bf91 - Keylogger
- d71f478b1d5b8e489f5daafda99ad203de356095278c216a421694517826b79a - Keylogger
- a7711b8314b256d279e104ea3809f0668d3615fba584ca887d9c495795d0a98e - Malicious file
- 42d52a78058954fcb85f538c86253214bacf475b4abecf3b426dad9d5b6543d6 - Malicious file
- 5633691b680b46b8bd791a656b0bb9fe94e6354f389ab7bc6b96d007c9d41ffa - Malicious file
- ee7926b30c734b49f373b88b3f0d73a761b832585ac235eda68cf9435c931269 - Malicious file
- 4ef8f3be7615392e4fe5751c9647ede1c6be2d2723af9b0fab69b6e58543e6ca - Megatools
- 37b1c57120760acefb6ad9a99eb1a7dfa49d4ee6c4e6afcc09b385c24c5f0639 - Mimikatz
- 511a75b2daca294db39d0e82e7af6161e67aab557b6b86bfea39ccbd2d7b40ae - Nukebot
- 94eef46095c231b1ee33cd63e063d8a2fc663e44832e45a294cf8d8cf9df31f8 - Nukebot
- 7bec0b28eb52f7a2e218367c0fef91e83c9df8f0463d55f3a064a2d6ca77c8d0 - Plink
- 3f880395c9d5820c4018daecf56711ce4ee719736590792f652ea29cbcbdb8f3 - Plink
- ee017325a743516155210f367272ac736bbfc8284b9613180744f26dda6502b0 - Plink
- 89aa7b67e9476d0f91df71a2b92ebe21f63f218afb6446296403f34f91831d15 - PuTTY
- cdd079bcb01e0f1229194f1f0ff9b6261e24ee16f8f75ec83763a33561c2071a - Sliver
- 6de5219d913ed93389ae8e9e295695da1adc889c0352a9069f9921a0a2cb5ec6 - Sliver
- 58d267dd80298c6d582ea7e45cf85a6e665d172d4122cc029cbcd427a33c2472 - Sliver
- e5d56cb7085ed8caf6c8269f4110265f9fb9cc7d8a91c498f3e2818fc978eee2 - Sliver
- 216.120.201[.]112:443 - Command-and-control server
- 51.81.168[.]157:443 - Command-and-control server
- 217.195.153[.]209 - IP address used by Plink
- 172.96.137[.]224 - IP address used by Plink
- 144.208.127[.]115 - IP address used by Plink