The FROZEN#SHADOW campaign

Date: 26th April 2024 | Severity: High

Summary

The FROZEN#SHADOW campaign was first reported by cybersecurity researchers in April 2024. The campaign targets entitiaes in Asia, Europe, and the Americas.

Attack Vectors

- The FROZEN#SHADOW operators gain initial system access using phishing email messages embedded with malicious links. The links lead to the retrieval of an obfuscated JavaScript file from a remote URL. The script executes a command through Windows Management Instrumentation (WMI) to map the victim's network drive, and then remotely installs an MSI package from the mapped network drive using msiexec.exe (the MSI file closely resembles the BazarBackdoor malware). Once the file is executed, a payload of the SSLoad malware is downloaded and executed through the Rundll32.exe process. To evade detection, the malware file is digitally signed with a fake certificate of the Malwarebytes Anti-Exploit software.
- SSLoad connects to a command and control (C2) server, and then starts exfiltrating system and user data for both the local host and domain over HTTPS. In addition, the malware executes various commands to prepare the victim's environment for the deployment of next-stage payloads, including Cobalt Strike and remote monitoring and management (RMM) software, such as ScreenConnect. Using these tools, the threat actors move laterally to other systems within the domain while harvesting credentials and other critical system details. Eventually, the attackers completely take over the victim's Windows domain by creating their own domain admin account.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 17ddc339b14845bc9d67c5c3cd9a0e617387cc0569131ff3641035d82043effa • 9629e313a6299e600ff2c6086a24e3ad6ff6ba59 • fc21a125287c3539e11408587bcaa6f3b54784d9d458facbc54994f05d7ef1b0 • ba3fa920708db856737a66f70e2c7e86bba73c73836f7f30c2ce42cd70d0c5bd • 24cb279eebcd49e1327905ab2bd19b9b2e09efa3e0a5e1875f3989c398a5da81 • c189e585a4aea11380082f7c25aef6b8

	• 7f97adff1d298ccf1f3c7991fcb01008dda22722ebbc11af48fcbf2adb58afb4 • 52cae521d7a808c8206f4b5afd6b037bc573b50e • 791c28d4201e8b9ea5162fbee3908feb34793b1c51f5aaedc43916e86068248d • 805b59e48af90504024f70124d850870a69b822b8e34d1ee551353c42a338bf7 • 3d84e7bdd40cd41df467830563d0f62779469a1b • 2118c5b95d5d57492b2e8b8c0403e23b21acc4ff50282f8b6007ba89adfaa992 • 3584ca9c1e7e0a38e47f59bb16c21203a60833d0f826294d535a98e7ca76d9c1 • 09e7f7428e6ecc68ef036c0751f53985882f6760cf3892f1d26af44f3b9730de • 7dff08656413a737483ecee2a50e412338ebfee3d36a1a5c04e74b25949b2306 • 9856b816a9d14d3b7db32f30b07624e4bcda7f1e265a7bb7a3e3476bfd54a759 • 4d81be09c23e02fab7364e508c21c111 • 29a0f183b8352154315af0568ce3806a • ae610eb8f8622653b9be9692a7d2a680b0c2154022704ca58af0eaeed0066d03 • 7206eafc475f246e7c9c258afdaaa64b5193c1c7427d927be417e53dec890078 • a557f891f4d50e458d745c7eaf7d0be3eceea36f0398097e977cd3f6ec463875 • 18d60c9c807da021bc2c31e3ba7ec2737865a8c96060134caa3cf033e43e26fe • 96212917b7b0dc881332db7ece0bacfe21d9ac713af1abe078f6d3e74baacd01 • 0737fa0b403fab17331c9835497a4f3b2955543e2fac85009dcc66df41a015f8 • 780b970dad15835d138546be9b615fc1b4124c1060a8efd91b9c52f9c3160d5b • 232f8f8dc9e5b9723c43c78cb942cc810ef56e305e4bd650110a484334f568a8 • b28a478eb5b99efcdc7caf428bffb89a • d4674ab328c69dc0fb721d7d4520574f • 6d7a94b7551f15732e193a07357375b98b463f0dce6b1fed871a42fcbdde9f48 • d174e68fe3458262e53dee5036eeb15e • 7dbebb7c76511fc063b5ace0a9359b655f66a55a494200b8fd11905c78b5fb90 • d394c7b8fe15753bfbff79fb4f648f6f8bae70f9 • f5bf914415faf7587958bbdc3312536fd9abea647f1541d44d2e757f0e683650 • f8fc9b40b946b742d6044f291914439727e1a7f53ea87562446f682b26cce65a • 68e1caf530366b1890993185157c01161b3d625063d75a41c88d2d1bb8edfe02 • e259102dc1ddd3d465c8b911313910c983586197 • ec183d55d6c11480bc167da468a526fa • caf8295570e8a8244c7099a8eabfd1bd55ea50f026b4461e9f0f5425d54703e8 • 4f52b4a2a781f366ed534d8c4b2fafef48a7848c4c20b4229b98747ca8ab06d3 • 63283e012f067a3ffb27ed4fe6803f740c80f6f65213fe5507f0cd1ee0019b96 • 2b026343214c3d2c10fdfa9b04b7694e57ee8d3605fbf9a2e127fe6fa9a58309 • e8e76b851fc78d87fe58ad7d29bc6356a8965236d1b96c5f572334dd695d5de9 • 828ef3e4ca064891836913015c48ac9807ecd43b32f6e7e4bff
Domain	• sokingscrosshotel[.]com • titnovacrion[.]top • winarkamaps[.]com • skinnyjeanso[.]com • globalsolutionunlimitedltd[.]com • krd6[.]com • maramaravilha[.]com • stratimasesstr[.]com • bjsdg0[.]pintaexoticfashion[.]co.in • wireoneinternet[.]info • danteshpk[.]com • kasnackamarch[.]info • simplyfitphilly[.]com
IP	• 45.95.11[.]134 • 85.239.54[.]190 • 23.95.209[.]148 • 23.159.160[.]88

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the IPs to Network team to block in the firewall.
- Block the Domain in the Proxy.
- Make regular backups of important and critical files.
- Avoid downloading files or attachments from external sources, especially if the source was unsolicited. Common file types include zip, rar, iso, and pdf. Zip files were used during this campaign.
- Monitor common malware staging directories, especially script-related activity in world- writable directories. In the case of this campaign the threat actors staged in subdirectories in C:\ProgramData as well as the user's %APPDATA%
- Through various phases of the FROZEN#SHADOW campaign, the threat actors leveraged encrypted channels over port 443 to evade detection. Because of this, we strongly recommend deploying robust endpoint logging capabilities. This includes leveraging additional process-level logging such as Sysmon and PowerShell logging for additional log detection coverage.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.securonix.com/blog/securonix-threat-research-security-advisory-frozenshadow- attack-campaign/
- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/662a2dba9edcffc72a633f0f