FakeBat Malware

Date: 10th May 2024 | Severity: High

Summary

FakeBat (also known as EugenLoader) is a malicious software loader and dropper that has emerged as a significant player in the world of cyber threats.

FakeBat utilizes multiple delivery tactics, with malvertising being the primary strategy. This involves exploiting online advertising platforms, including Google Ads, to spread the malware. What makes FakeBat unique is that the threat actor uses MSIX installers packaged with heavily obfuscated PowerShell code.

In a recently observed campaign, users were lured with a Trello MSIX software installer containing an obfuscated PowerShell script. This script communicates with a command-and-control (C2) server to retrieve subsequent stage payloads. These payloads typically consist of SectopRAT or ArechClient2, which are injected into the MSBuild process using the IDAT loader technique.

Attack Vectors

- FakeBat is distributed through malicious advertisements and websites impersonatingpopular software, such as WinRAR. The malware utilizes signed MSIX installation packagesto appear legitimate which aids in deceiving victims to execute the malware.
- FakeBat loader being distributed through compromised websites. These websites contain injected malicious JavaScript that triggers fake browser update notifications, misleading users into believing they need to install legitimate browser updates.
- Distribution methods-Malicious ads, fake websites, infected email attachments, socialengineering, software 'cracks'.
- FakeBat uses a complex infection chain, with multiple redirect stages, and relies on PowerShell scripts to carry out a range of malicious tasks. These scripts can download and execute additional payloads, ensure persistence, and avoid detection by tweaking systemsecurity settings.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• f7fbf33708b385d27469d925ca1b6c93b2c2ef680bc4096657a1f9a30e4b5d18 • 40c9b735d720eeb83c85aae8afe0cc136dd4a4ce770022a221f85164a5ff14e5 • 0d906e43ddf453fd55c56ccd6132363ef4d66e809d5d8a38edea7622482c1a7a • 15ce7b4e6decad4b78fe6727d97692a8f5fd13d808da18cb9d4ce51801498ad8 • 07b0c5e7d77629d050d256fa270d21a152b6ef8409f08ecc47899253aff78029 • 70c8ba4cb07d29019a35a248b5647a14 • 04d77db9b7c18444b3bd50ee1b99c11c • 569d206636b75c33240ba4c1739c04d6 • 9bf32f3037b62a387aca6038cf95ca03 • 12647292d6c0f73a655a1a84ddbed9a2244c35cf • 4a57cbce13def4a4d9f7bccc49a8af52 • 3c24d4cda44e9f3156d62986a4998bdf • 06165e8da7bf1b22962c8272f19d707f • c03be50c6fbfd3aec108a7bcd7aaea82 • 3f8f35d694ee1b4fd0038e39e1e4271f • 5102b64a838bd84f4273bce2a0bda67df77fdb1a33a2b939988ccb51f2246e07 • 909db8913f0ebd6e9359bd2ec3697df6f7d71f28 • 11fdea09f5223df7814e84b5980e72419c447bdf • d6a6b73c273c508417898c02a142c496158ad2d0432495bff3a4f94f574d5bc4 • b2e8277064af7791a3a73479ff2f2c45be3591c96567addb9421faed3dc7e2be • 80f4405270b8fd7f557c6831dd2785b55fdee43d48d967401a8b972e147be948 • cefc3d2ef6a2e6032c84fde546bc2d99
URL	http[:]//doggygangers.com/YfMv2QsjpCQl845BWSYNfNOQitweyze_Z6lIlrRr43MRjX_HrM/stats/get_stats.php http[:]//doggygangers.com/YfMv2QsjpCQl845BWSYNfNOQitweyze_Z6lIlrRr43MRjX_HrM/land/universal_land/ http[:]//bezynet.com/OBS-Studio-30.0.2-Full-Installer-x64.msix http[:]//church-notes.com/Onenote_setup.msix http[:]//bezynet.com/Bandicam_7.21_win64.msix http[:]//doggygangers.com/YfMv2QsjpCQl845BWSYNfNOQitweyze_Z6lIlrRr43MRjX_HrM/downloadsdownloadfile/dwnl_standart.php http[:]//church-notes.com/Epic-Games_Setup.msix http[:]//church-notes.com/Braavos-Wallet.msix https[:]//sivaspastane.com/Notion-x86.msix http[:]//bitbucket.org/ganhack123/load/downloads/ZipCosdaz.exe.gpg http[:]//avr-energie.com/Trello-Full-Installer-x64.msix http[:]//bitbucket.org/ganhack123/load/downloads/ZipCosdaz1.exe.gpg http[:]//winrar.software/index-install.html http[:]//avr-energie.com/Notion%20Setup%203.2.1.msix
Domain	• breavas[.]app • ads-pill[.]xyz • ads-pill[.]top • ads-tooth[.]top • church-notes[.]com • blcnder[.]org • ads-eagle[.]top • ads-strong[.]online • shatterbreathepsw[.]shop • ads-analyze[.]site • ads-analyze[.]xyz • ads-moon[.]top • ads-strong[.]xyz • ads-change[.]site • ads-change[.]online

INDICATOR TYPE	INDICATORS
IP Address	• 45.11.182[.]97 • 91.242.217[.]28 • 91.241.93[.]98 • 79.132.128[.]109 • 91.241.93[.]111 • 62.204.41[.]98 • 79.132.128[.]108

Recommendation

- Refrain from clicking on unsolicited or suspicious links, especially in emails or onunfamiliar websites. The same applies to opening attachments in suspicious emails
- Be cautious of downloading files or software from unverified sources, and always ensureyou are using official websites or trusted app stores..
- Do not trust ads (e.g., pop-ups or banners) on dubious sites.
- Regularly update your operating system and software to patch known vulnerabilities, as cybercriminals often exploit these weaknesses
- Utilize reputable antivirus and anti-malware software to provide an additional layer ofprotection.

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

Reference Links

- https://www.threatdown.com/blog/fakebat-delivered-via-several-active-malvertising-campaigns/
- https://www.esentire.com/blog/recent-fakebat-activity-observed-in-december-2022.