Mphasis
The Next Applied

FIN7 Hackers Using Signed Malware and Fake Google Ads to Evade Defenses

Date: 11th May 2024 | Severity: High

Summary

The financially motivated threat actor known as FIN7 has been observed leveraging malicious Google ads spoofing legitimate brands as a means to deliver MSIX installers that culminate in the deployment of NetSupport RAT.

“The threat actors used malicious websites to impersonate well-known brands, including AnyDesk, WinSCP, BlackRock, Asana, Concur, The Wall Street Journal, Workable, and Google Meet,” cybersecurity firm eSentire said in a report published earlier this week.

Attack Vectors

Over the years, the threat actor has refined its tactics and malware arsenal, adopting various custom malware families such as BIRDWATCH, Carbanak, DICELOADER (aka Lizar and Tirion), POWERPLANT, POWERTRASH, and TERMITE, among others.

FIN7 malware is commonly deployed through spear-phishing campaigns as an entry to the target network or host, although in recent months the group has utilized malvertising techniques to initiate the attack chains.

In December 2023, Microsoft said it observed the attackers relying on Google ads to lure users into downloading malicious MSIX application packages, which ultimately led to the execution of POWERTRASH, a PowerShell-based in-memory dropper that’s used to load NetSupport RAT and Gracewire.

Sangria Tempest [...] is a financially motivated cybercriminal group currently focusing on conducting intrusions that often lead to data theft, followed by targeted extortion or ransomware deployment such as Clop ransomware,” the tech giant noted at the time.

In the attacks observed by eSentire in April 2024, users who visit the bogus sites via Google ads are displayed a pop-up message urging them to download a phony browser extension, which is an MSIX file containing a PowerShell script that, in turn, gathers system information and contacts a remote server to fetch another encoded PowerShell script.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• findoutcredit[.]com • againcome[.]com • modestoobgyn[.]com • myshortbio[.]com • estetictrance[.]com • internethabit[.]com • bestsecure2020[.]com • chyprediction[.]com • domenuscdm[.]com • spontaneousance[.]com • fashionableeder[.]com • incongruousance[.]com • electroncador[.]com • astara20[.]com • coincidencious[.]com
File Hashes	• 0c6b41d25214f04abf9770a7bdfcee5d • 21f153810b82852074f0f0f19c0b3208 • 02699f95f8568f52a00c6d0551be2de5 • 0291df4f7303775225c4044c8f054360 • 0fde02d159c4cd5bf721410ea9e72ee2 • 2cbb015d4c579e464d157faa16994f86 • 3803c82c1b2e28e3e6cca3ca73e6cce7 • 5a6bbcc1e44d3a612222df5238f5e7a8 • 833ae560a2347d5daf05d1f670a40c54 • b637d33dbb951e7ad7fa198cbc9f78bc • bce9b919fa97e2429d14f255acfb18b4 • d1d8902b499b5938404f8cece2918d3d • edb1f62230123abf88231fc1a7190b60 • d405909fd2fd021372444b7b36a3b806 • 122cb55f1352b9a1aeafc83a85bfb165 • 936b142d1045802c810e86553b332d2d • 23e1725769e99341bc9af48a0df64151 • 4d56a1ca28d9427c440ec41b4969caa2 • 50260f97ac2365cf0071e7c798b9edda • 6fba605c2a02fc62e6ff1fb8e932a935 • 49ac220edf6d48680f763465c4c2771e • 52f5fcaf4260cb70e8d8c6076dcd0157 • 78c828b515e676cc0d021e229318aeb6 • 70bf088f2815a61ad2b1cc9d6e119a7f • 4961aec62fac8beeafffa5bfc841fab8 • ab29b9e225a05bd17e919e1d0587289e • 1c3b19163a3b15b39ae00bbe131b499a • 230a681ebbcdba7ae2175f159394d044 • bf41fc54f96d0106d34f1c48827006e4 • c4da0137cbb99626fd44da707ae1bca8 • 28e9581ab34297b6e5f817f93281ffac • 38786bc9de1f447d0187607eaae63f11 • 6fba605c2a02fc62e6ff1fb8e932a935

Recommendation

- Vigilance when interacting with pop-ups and downloads, even from seemingly reputable sources.
- Regular updates to antivirus and anti-malware solutions to detect and prevent the execution of malicious scripts.
- Educating employees about the dangers of sponsored ads and the importance of verifying software through official channels.
- Deploy Endpoint Detection and Response (EDR) solutions across all devices.
- Implement Phishing and Security Awareness Training (PSAT) program.
- Control MSIX execution via AppLocker policies.
- Report incidents of certificate misuse by threat actors.

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://cloud.google.com/blog/topics/threat-intelligence/evolution-of-fin7
- https://thehackernews.com/2024/05/fin7-hacker-group-leverages-malicious.html
- https://cybersecuritynews.com/fin7-hackers-sponsored-google-ads-msix-payloads/