Hackers hijack antivirus updates to drop GuptiMiner malware

Date: 24th April 2024 | Severity: High

Summary

GuptiMiner as “a highly sophisticated threat” that can perform DNS requests to the attacker’s DNS servers, extract payloads from images, sign its payloads, and perform DLL sideloading. GuptiMiner leverages a man-in-the-middle attack to exploit vulnerabilities in the update process of the eScan antivirus, a product of an Indian cybersecurity firm. By hijacking this process, the attackers have been able to distribute their malware to unsuspecting users stealthily.

Attack Vectors

- The GuptiMiner campaign is not limited to a single type of malware but includes a variety of tools designed to breach large corporate networks.
- Two distinct backdoors have been identified, each with the capability to provide attackers with remote access to infected systems.
- Additionally, the campaign’s final payload involves deploying XMRig, a well-known cryptocurrency mining software, which harnesses the processing power of infected machines to mine Monero (XMR).

Since 2018, GuptiMiner has undergone significant evolution, with its developers continuously enhancing its capabilities. The malware exhibits a complex infection chain and employs advanced techniques such as:

- DNS requests to attacker-controlled servers
- Sideload malicious payloads
- Extracting executable code from seemingly benign images
- Utilizing a custom trusted root anchor certification authority to sign payloads.

Indicator of compromise

INDICATOR TYPE	INDICATORS
IOCs	• c3122448ae3b21ac2431d8fd523451ff25de7f6e399ff013d6fa6953a7998fa3 • 7a1554fe1c504786402d97edecc10c3aa12bd6b7b7b101cfc7a009ae88dd99c6 • 3515113E7127DC41FB34C447F35C143F1B33FD70913034742E44EE7A9DC5CC4C • e0dd8af1b70f47374b0714e3b368e20dbcfa45c6fe8f4a2e72314f4cd3ef16ee • de48abe380bd84b5dc940743ad6727d0372f602a8871a4a0ae2a53b15e1b1739 • 8e96d15864ec0cc6d3976d87e9e76e6eeccc23c551b22dcfacb60232773ec049 • FF884D4C01FCCF08A916F1E7168080A2D740A62A774F18E64F377D23923B0297 • 294B73D38B89CE66CFDEFA04B1678EDF1B74A9B7F50343D9036A5D549ADE509A • 6305d66aac77098107e3aa6d85af1c2e3fc2bb1f639e4a9da619c8409104c414 • 357009a70daacfc3379560286a134b89e1874ab930d84edb2d3ba418f7ad6a0b • 364984e8d62eb42fd880755a296bd4a93cc071b9705c1f1b43e4c19dd84adc65 • 4dfd082eee771b7801b2ddcea9680457f76d4888c64bb0b45d4ea616f0a47f21 • 487624b44b43dacb45fd93d03e25c9f6d919eaa6f01e365bb71897a385919ddd • 1c31d06cbdf961867ec788288b74bee0db7f07a75ae06d45d30355c0bc7b09fe
Domains	• _spf.microsoft[.]com • acmeautoleasing[.]net • b.guterman[.]net • breedbackfp[.]com • crl.microsoft[.]com • crl.peepzo[.]com • crl.sneakerhost[.]com • desmoinesreg[.]com • dl.sneakerhost[.]com • edgesync[.]net • espcomp[.]net • ext.microsoft[.]com • ext.peepzo[.]com • ext. • icamper[.]net • m.airequipment[.]net • m.cbacontrols[.]com • m.m.insomniaccinema[.]com

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

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.bleepingcomputer.com/news/security/hackers-hijack-antivirus-updates-to-drop-guptiminer-malware/
- https://decoded.avast.io/janrubin/guptiminer-hijacking-antivirus-updates-for-distributing-backdoors-and-casual-mining/