Mphasis
The Next Applied

Bondnet Threat Actor Still Active, Using Bots as C2 Servers

Date: 17th June 2024 | Severity: High

Summary

(ASEC) has published a report detailing a significant shift in the tactics employed by the Bondnet threat actor. Traditionally associated with cryptocurrency mining operations, Bondnet has been observed leveraging compromised machines with high computational capabilities as clandestine command and control (C2) servers.

Threat actors abuse high-performance bots to carry out large-scale automated attacks efficiently.

These bots can work quickly, flood systems, steal information, and conduct and orchestrate sophisticated cyber operations largely autonomously.

Attack Vectors

- ASEC's analysis reveals that Bondnet modifies an open-source proxy program, FRP, to establish reverse Remote Desktop Protocol (RDP) connections on these compromised systems. This process is facilitated through the use of proxy servers and Cloudflare tunneling, ultimately linking the targeted machine to Bondnet's C2 domain.
- While ASEC was unable to fully observe the conversion process due to environmental constraints on the affected system, the available evidence strongly suggests a deliberate attempt to establish a botnet C2 infrastructure. This conclusion is supported by the execution of Cloudflare tunneling and HTTP File Server (HFS) programs on the compromised machine, the distinctive user interface (UI) similarities between the HFS program and the Bondnet C2, and the observation of new and restored malicious files on the C2 following an initial failed attempt.
- ASEC's findings also indicate that Bondnet is specifically targeting systems with specific language settings (Russian, Korean, English, or Japanese) and substantial computational resources, likely prioritizing those that can best serve as robust C2 servers.
- This revelation underscores the evolving nature of cyber threats and the continued importance of robust cybersecurity measures. Bondnet's adaptation of its tactics highlights the need for organizations and individuals to remain vigilant and proactive in protecting their systems and data from increasingly sophisticated attacks.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• D6B2FEEA1F03314B21B7BB1EF2294B72(smss.exe) • 2513EB59C3DB32A2D5EFBEDE6136A75D(mf) • E919EDC79708666CD3822F469F1C3714(hotfixl exe) • 432BF16E0663A07E4BD4C4EAD68D8D3D(main.exe) • 9B7BE5271731CFFC51EBDF9E419FA7C3(dss.exe) • 7F31636F9B74AB93A268F5A473066053(BulletsPassView64.exe) • D28F0CFAE377553FCB85918C29F4889B(VNCPassView.exe) • 6121393A37C3178E7C82D1906EA16FD4(PstPassword.exe) • 0753CAB27F143E009012053208B7F63E(netpass64.exe) • 782DD6152AB52361EBA2BAFD67771FA0(mailpv.exe) • 8CAFDBB0A919A1DE8E0E9E38F8AA19BD (PCHunter32.exe • 057D5C5E6B3F3D366E72195B0954283B(check.exe) • 35EE8D4E45716871CB31A80555C3D33E(UpSql.exe) • 1F7DF25F6090F182534DDEF93F27073D(svchost.exe) • DC8A0D509E84B92FBF7E794FBBE6625B(svchost.com) • 76B916F3EEB80D44915D8C01200D0A94(RouterPassView.exe) • 44BD492DFB54107EBFE063FCBFBDDFF5(rdpv.exe) • E0DB0BF8929CCAAF6C085431BE676C45(mass.dll) • DF218168BF83D26386DFD4ECE7AEF2D0(mspass.exe) • 35861F4EA9A8ECB6C357BDB91B7DF804(pspv.exe)
URL	• 223.223.188[.]19 • 185.141.26[.]116/stats.php • 185.141.26[.]116/hotfixl.ico • 185.141.26[.]116/winupdate.css • 84.46.22[.]158:7000 • 46.59.214[.]14:7000 • 46.59.210[.]69:7000 • 47.99.155[.]111 • d.mymst[.]top

Recommendation

- This revelation underscores the evolving nature of cyber threats and the continued importance of robust cybersecurity measures. Bondnet's adaptation of its tactics highlights the need for organizations and individuals to remain vigilant and initiative-taking in protecting their systems and data from increasingly sophisticated attacks.
- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Submit the File Hash to the Antivirus team to update their database with the file hashes. Monitor network traffic and run antivirus scans to identify if any infection remains.

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://securityonline.info/bondnet-threat-actor-still-active-using-bots-as-c2-servers/
- https://cybersecuritynews.com/bondnet-high-performance-bots-c2-server/