Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 28-JUN-2024, 04:30 IST

Title	**Rust-Based P2PInfect Botnet Evolves with Miner and Ransomware Payloads**
Summary	• The peer-to-peer malware botnet known as P2PInfect has been found targeting misconfigured Redis servers with ransomware and cryptocurrency miners. • With its latest updates to the crypto miner, ransomware payload, and rootkit elements, it demonstrates the malware author's continued efforts into profiting off their illicit access and spreading the network further, as it continues to worm across the internet. • It typically spreads by targeting Redis servers and its replication feature to transform the victim systems into a follower node of the attacker-controlled server, subsequently allowing it to issue arbitrary commands to them. • Besides taking steps to prevent other attackers from targeting the same server, P2PInfect is known to change the passwords of other users, restart the SSH service with root permissions, and even perform privilege escalation.
Severity	Medium
Attack Vectors	• As the name suggests, it is a peer-to-peer botnet, where every infected machine acts as a node in the network and maintains a connection to several other nodes. • Besides taking steps to prevent other attackers from targeting the same server, P2PInfect is known to change the passwords of other users, restart the SSH service with root permissions, and even perform privilege escalation. • This results in the botnet forming a huge mesh network, which the malware author makes use of to push out updated binaries across the network, via a gossip mechanism. The author simply needs to notify one peer, and it will inform all its peers and so on until the new binary is fully propagated across the network. • Among the new behavioral changes to P2PInfect include the use of the malware to drop miner and ransomware payloads, the latter of which is designed to encrypt files matching certain file extensions and deliver a ransom note urging the victims to pay 1 XMR (~$165). • It's suspected that P2PInfect is advertised as a botnet-for-hire service, acting as a conduit to deploy other attackers' payloads in exchange for payment. • The choice of a ransomware payload for malware primarily targeting a server that stores ephemeral in memory data is an odd one, and P2Pinfect will likely see far more profit from their miner than their ransomware due to the limited amount of low-value files it can access due to its permission level.
Indicator of Compromise	INDICATOR TYPE: IP — INDICATORS: 129[.]144[.]180[.]26:60107; 88[.]198[.]117[.]174:19999; 159[.]69[.]83[.]232:19999; 195[.]201[.]97[.]156:19999 INDICATOR TYPE: File Hash — INDICATORS: 4f949750575d7970c20e009da115171d28f1c96b8b6a6e2623580fa8be1753d9; 2c8a37285804151fb727ee0ddc63e4aec54d9460b8b23505557467284f953e4b; 8a29238ef597df9c34411e3524109546894b3cca67c2690f63c4fb53a433f4e3; 9b74bfec39e2fcd8dd6dda6c02e1f1f8e64c10da2e06b6e09ccbe6234a828acb
Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Ensure all software, including Redis, is up to date. P2PInfect exploits vulnerabilities in outdated versions. • Restrict external access to Redis servers. Only allow necessary IPs. • Implement strong authentication mechanisms. • Never trust or open links and attachments received from unknown sources/senders. • Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. **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.**

References	• https://thehackernews.com/2024/06/rust-based-p2pinfect-botnet-evolves.html • https://www.cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer