Mphasis SOC – Information Security News
Date & Time Issued: 26-JUN-2024, 21:00 IST

Title	**P2PInfect botnet targets REdis servers with new ransomware module**
Summary	• P2PInfect, originally a dormant peer-to-peer malware botnet with unclear motives, has finally come alive to deploy a ransomware module and a cryptominer in attacks on Redis servers. • According to Cado Security, which has been tracking P2PInfect for some time now, there is evidence the malware operates as a "botnet for hire," although conflicting information prevents the researchers from drawing safe conclusions at this time. • Cado Security's subsequent examination of the malware revealed that it leveraged a Redis replication feature to spread. • Despite that elevated activity, P2PInfect did not perform any malicious actions on compromised systems, so its operational goals remained blurry.
Severity	Medium
Attack Vectors	• The ransomware targets files with specific extensions related to databases (SQL, SQLITE3, DB), documents (DOC, XLS), and media files (MP3, WAV, MKV) and appends the 'encrypted' extension to the resulting files. • The ransomware iterates through all directories, encrypting files and storing a database of encrypted files in a temporary file with the 'lockedfiles' extension. • The damage from the ransomware module is contained by its privilege level, which is limited to that of the compromised Redis user and the files accessible to them. Also, because Redis is often deployed in memory, not much beyond configuration files are eligible for encryption. • The XMR (Monero) miner seen dormant in previous iterations has now been activated, dropped to a temporary directory, and launched five minutes after the primary payload has started. • The pre-configured wallet and mining pool in the examined samples has so far made 71 XMR, which is about $10,000, but Cado says there's a good chance the operators use additional wallet addresses. • A peculiar characteristic of the new P2PInfect is that the miner is configured to use all the available processing power, often hampering the operation of the ransomware module. • Of note is also a new user-mode rootkit that enables P2PInfect bots to hide their malicious processes and files from security tools, hijacking multiple processes to achieve this concealment.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• 88601359222a47671ea6f010a670a35347214d8592bceaf9d2e8d1b303fe26d7 • b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c • 68eaccf15a96fdc9a4961daffec5e42878b5924c3c72d6e7d7a9b143ba2bbfa9 • 89be7d1d2526c22f127c9351c0b9eafccd811e617939e029b757db66dadc8f93
	IP	• 35.183.81[.]182 • 66.154.127[.]38 • 66.154.127[.]39 • 8.218.44[.]75 • 97.107.96[.]14

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • 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://live.paloaltonetworks[.]com/t5/community-blogs/p2pinfect-the-rusty-peer-to-peer-self-replicating-worm/ba-p/550505 • https://www.bleepingcomputer.com/news/security/p2pinfect-botnet-targets-redis-servers-with-new-ransomware-module/