Mphasis
The Next Applied

US Govt Sanctions Cybercrime Gang behind Massive 911 S5 Botnet

Date: 29th May 2024 | Severity: High

Summary

The U.S. Treasury Department has sanctioned a cybercrime network comprising three Chinese nationals and three Thailand-based companies linked to a massive botnet controlling a residential proxy service known as "911 S5."

Attack Vectors

- The 911 S5 botnet was a malicious service that compromised victim computers and allowed cybercriminals to proxy their internet connections through these compromised computers," said the Office of Foreign Assets Control (OFAC) on Tuesday.
- Once a cybercriminal had disguised their digital tracks through the 911 S5 botnet, their cybercrimes appeared to trace back to the victim's computer instead of their own."
- OFAC added that the residential proxy botnet compromised approximately 19 million IP addresses. These infected devices allowed cybercriminals to submit tens of thousands of fraudulent applications for programs related to the Coronavirus Aid, Relief, and Economic Security Act, resulting in billions of dollars in losses.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• vpn[.]maskvpn[.]org • net[.]dewvpn[.]com
File Hash	• a220528f31dceddc955b791b13ac4989 • 12059484a8951a8356c60c46f659a35e • f9634d85ca0138cfddfe6e58fa1c6160 • c6b1934d3e588271f27a38bfeed42abb • 8e8b072c93246808a7f24554ca593c59 • 5feb35a7186a5be50b7aa158866b8aa3

Recommendation

- Network Monitoring and Traffic Analysis: Implement robust network monitoring solutions to detect and analyze suspicious traffic patterns associated with the 911 S5 botnet.
- Endpoint Security: Deploy endpoint security solutions with advanced threat detection capabilities to identify and mitigate malware infections associated with the 911 S5 botnet.
- Patch Management: Ensure all software and systems are regularly patched and updated.
- User Education and Awareness: Educate employees and users about the risks associated with phishing emails, social engineering attacks.
- Blocking Known Command and Control (C2) Servers: Utilize threat intelligence feeds and security information and event management (SIEM) systems to identify and block known C2 servers associated with the 911 S5 botnet.
- Incident Response Planning: Develop and regularly update an incident response plan that outlines procedures for responding to security incidents related to the 911 S5 botnet.

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/us-govt-sanctions-cybercrime-gang-behind-massive-911-s5-botnet-linked-to-illegitimate-residential-proxy-service/
- https://gric.recherche.usherbrooke.ca/rpaas/