Hackers Use F5 BIG-IP Malware to Stealthily Steal Data

Date: 18th June 2024 | Severity: High

Summary

A group of suspected Chinese cyberespionage actors named 'Velvet Ant' are deploying custom malware on F5 BIG-IP appliances to gain a persistent connection to the internal network and steal data. Using the compromised F5 BIG-IP devices, the threat actors could stealthily steal sensitive customer and financial information from the company for three years without being detected.

Attack Vectors

- The attack observed by Sygnia started by compromising two outdated F5 BIG-IP appliances the victim organization used for firewall, WAF, load balancing, and local traffic management.
- Sygnia says they were both compromised using known remote code execution flaws to install custom malware on the networking devices.
- The attackers used this access to gain access to internal file servers where they deployed PlugX, a modular remote access Trojan (RAT), which various Chinese hackers have been using for data collection and exfiltration for over a decade now.
- Malware deployed on the F5 BIG-IP appliance includes PMCD: Connects to the C&C server hourly, executes commands received from the server via 'csh', maintaining remote control.
- MCDP: Captures network packets, executed with the 'mgmt' NIC argument, ensuring persistent network monitoring.
- SAMRID (EarthWorm): An open-source SOCKS proxy tunneler used for creating secure tunnels, previously utilized by various Chinese state-sponsored groups. ESRDE: Similar to PMCD it uses 'bash' for command execution, allowing remote command control and persistence.
- The attackers used the compromised F5 BIG-IP appliance to retain persistence on the network, allowing them to gain access to the internal network while blending attacker traffic with legitimate network traffic, making detection more difficult.

Indicator of compromise

INDICATOR TYPE	INDICATORS
FileHash	• baaa29799bdbb6c1f3fc70e25c0aee4b033fefc8 • 4a0f328e7672ee7ba83f265d48a6077a0c9068d4
IP	• 202.61.136[.]158 • 103.138.13[.]31

Recommendation

- Restrict outbound connections to minimize C&C communications.
- Implement strict controls over management ports and enhance network segmentation.
- Prioritize replacing legacy systems and tightening security controls.
- Deploy robust EDR systems with anti-tampering features and enable security measures like Windows Credential Guard.
- Enhance security for edge devices through patch management, intrusion detection, and migration to cloud-based solutions.

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-use-f5-big-ip-malware-to-stealthily-steal-data-for-years/
- https[:]//www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/#:~:text=F5%20BIG%2DIP%20%E2%80%93%20The%20Perfect,network%20traffic%20without%20arousing%20suspicion.