Mphasis
The Next Applied

Chinese Actor ‘SecShow’ Performs Wide-Reaching DNS Probing – Active IOCs

Date: 14th June 2024 | Severity: High

Summary

Cybersecurity researchers have shed more light on a Chinese actor codenamed SecShow that has been observed conducting Domain Name System (DNS) on a global scale since at least June 2023. according to Infoblox security researchers Dr. Renée Burton and Dave Mitchell, operates from the China Education and Research Network (CERNET), a project funded by the Chinese government.

Attack Vectors

- DNS servers that are capable of accepting and resolving domain names recursively for any party on the internet, making them ripe for exploitation by bad actors to initiate distributed denial-of-service (DDoS) attacks such as a DNS amplification attack.
- CERNET nameservers to identify open DNS resolvers and calculate DNS responses. This entails sending a DNS query from an as-yet-undetermined origin to an open resolver, causing the SecShow-controlled nameserver to return a random IP address.
- Cortex Xpanse treats the domain name in the DNS query as a URL and attempts to retrieve content from the random IP address for that domain name,” the researchers explained. “Firewalls, including Palo Alto and Check Point, as well as other security devices, perform URL filtering when they receive the request from Cortex Xpanse.
- SecShow is the second China-linked threat actor after Muddling Meerkat to perform large-scale DNS probing activities on the internet.”Muddling Meerkat queries are designed to mix into global DNS traffic and [have] remained unnoticed for over four years, while Secshow queries are transparent encodings of IP addresses and measurement information.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• Attacker[.]fit • nameserver[.]fit • victim[.]fit • prey[.]fit • secdns[.]site • ns1.c.secshow[.]net • ns1.l-test.secdns[.]site • savme[.]xyz • ns2.c.secshow[.]net • 1-103-170-192-121-103-170-192-9.f.secshow[.]online • 0-53aa2a46-202401201-ans-dnssec.l-test.secdns[.]site • 6a134b4f-1.c.secshow[.]net • ns2.l-test.secdns[.]site • secshow[.]net • secshow[.]online
IP	• 202[.]112[.]47[.]45

Recommendation

- Block all threat indicators at your respective controls.Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Ensure all operating systems and software are up to date with the latest security patches.Employ reliable antivirus and antimalware software to detect and block known threats.
- Regularly update these tools to maintain the latest threat intelligence. Implement IDPS to detect and prevent unusual network activity, system behavior, or similar threats.
- Enable two-factor authentication (2FA) on your accounts adds an extra layer of security and can help prevent unauthorized access even if your login credentials have been stolen.
- Regularly backing up your important data can help ensure that you don't lose any critical information in the event of a malware infection or other data loss event.
- Be wary of emails, attachments, and links from unknown sources. Also, avoid downloading software from untrusted sources or clicking on suspicious ads or pop-ups.

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.rewterz.com/threat-advisory/chinese-actor-secshow-performs-wide-reaching-dns-probing-active-iocs
- https[:]//thehackernews.com/2024/06/chinese-actor-secshow-conducts-massive.html