America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Malicious Cyber Actor Use of Network Tunneling and Spoofing to Obfuscate Geolocation

Last Revised: October 24, 2020 **Alert Code:** AA20-198A

Give Feedback

Summary

This Activity Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) and Pre-ATT&CK frameworks. See the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v7/matrices/enterprise/> *and Pre-ATT&CK* <https://attack.mitre.org/versions/v7/techniques/pre/> *frameworks for referenced threat actor techniques.*

Attributing malicious cyber activity that uses network tunneling and spoofing techniques to a specific threat actor is difficult. Attribution requires analysis of multiple variables, including location. Because threat actors can use these techniques to obfuscate their location, it is not possible to identify the true physical location of malicious activity based solely on the geolocation of Internet Protocol (IP). This Alert discusses how threat actors use these obfuscation techniques to mislead incident responders.

Technical Details

Geolocation

The geolocation of an IP address is often obtained with publicly available information (WHOIS <https://whois.icann.org/en/about-whois> registration) or proprietary information. The level of geographic precision varies widely across sources; some provide country and locality details, while others provide neighborhood-level detail. Additionally, the accuracy of this information varies by source.

However, even if the geolocation of an IP address is accurate, the threat actor may not be physically located near it; instead, they may be hiding their true location through the use of spoofing and network tunnels.

Spoofing

A threat actor can spoof packets with an arbitrary source IP address, which in turn geolocates to a specific country (see figure 1). The actor's physical location may be elsewhere. The actor then initiates their malicious activity. Network defenders see packets originating from a source IP address that did not generate the traffic. This technique is most common with connectionless activities, such as distributed *Endpoint Denial of Service* [T1499] <https://attack.mitre.org/versions/v7/techniques/t1499/> and *Network Denial of Service* [T1498] <https://attack.mitre.org/versions/v7/techniques/t1498/>— including DNS amplification— attacks.

Figure 1: IP spoofing

Encapsulating Network Tunnels

A network tunnel encapsulates network traffic between two points (see figure 2). Often network tunnels are used for legitimate purposes, such as secure remote administration or creating virtual private networks (VPNs). However, a malicious cyber actor can use this technique to mask their true source IP address and, therefore, their physical location. The threat actor accomplishes masking by using virtual private servers (VPSs), which can be purchased through commercial providers. The threat actor will initiate a remote network tunnel from their computer to the VPS and then use the VPS to initiate malicious activity. Network defenders see the IP address, as well as geolocation information of the VPS. Attempts to identify the cyber actor's physical location by using the geolocation of the VPS will be inaccurate. Network tunneling is common with malicious *Connection Proxy* [T1090] <https://attack.mitre.org/versions/v7/techniques/t1090/> activities.

Figure 2: Network tunnel encapsulation

The ease with which IP addresses can be spoofed and the possibility that activity could be tunneled through a network to intentionally mask the true source prevents any attempt to identify the physical location of the activity based solely on the geolocation of the IP address.

Mitigations

In addition to being knowledgeable about threat actor obfuscation techniques, CISA encourages incident responders to review the following best practices to strengthen the security posture of their systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines. See Protecting Against Malicious Code.
- Ensure systems have the latest security updates. See Understanding Patches and Software Updates <https://www.us-cert.gov/ncas/tips/st04-006>.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' permissions to install and run unwanted software applications. Do not add users to the local administrators’ group unless required.
- Enforce a strong password policy. See Choosing and Protecting Passwords <https://www.us-cert.gov/ncas/tips/st04-002>.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
- Enable a personal firewall on agency workstations that is configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Give Feedback

Additional Information

Sign up to receive CISA’s alerts on security topics and threats.

Sign up for CISA’s free vulnerability scanning and testing services to help organizations secure internet-facing systems from weak configuration and known vulnerabilities. Email vulnerability_info@cisa.dhs.gov to sign up. See https://www.cisa.gov/cyber-resource-hub <https://www.cisa.gov/cyber-resource-hub> for more information about vulnerability scanning and other CISA cybersecurity assessment services.

Acknowledgements

Palo Alto Networks and IBM contributed to this Alert.

References

Cloudflare Blog: The real cause of large DDoS - IP Spoofing <https://blog.cloudflare.com/the-root-cause-of-large-ddos-ip-spoofing/>

Cisco Configuration Guide: Implementing Tunnels <https://www.cisco.com/c/en/us/td/docs/ios/12_4/interface/configuration/guide/inb_tun.html>

Revisions

July 16, 2020: Initial Version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Give Feedback