Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 July 2020

PIN Number

20200721-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Cyber Actors Exploiting Built-In Network Protocols to Carry Out Larger, More Destructive Distributed Denial of Service Attacks

Summary

Cyber actors have exploited built-in network protocols, designed to reduce computational overhead of day-to-day system and operational functions, to conduct larger and more destructive distributed denial of service (DDoS) amplification attacks against US networks. A DDoS amplification attack occurs when an attacker sends a small number of requests to a server and the server responds with more numerous responses to the victim. Typically, the attacker spoofs the source Internet Protocol (IP) address to appear as if they are the victim, resulting in traffic that overwhelms victim resources. Cyber actors likely will increasingly abuse built-in network protocols. Such abuse likely will enable DDoS amplification attacks to be carried out with limited resources and result in significant disruptions and impact on the targets.

Threat Overview

As early as December 2018, cyber actors began exploiting built-in network protocols[a] to carry out destructive DDoS attacks against US networks. As recently as February 2020, cybersecurity researchers identified new built-in network protocol vulnerabilities that have not yet been exploited, but increase the attack surface. This is based on open-source evidence of host-based, mobile, and Internet of Things (IoT) device protocol exploitation, resulting in amplification attacks in networked environments.

- In February 2020, UK security researchers identified a vulnerability in the built-in network discovery protocols of Jenkins servers—free, open source, automation servers used to support the software development process that cyber actors could exploit to conduct DDoS amplification attacks — according to open source reporting. Researchers estimated cyber actors could use vulnerable Jenkins servers to amplify DDoS attack traffic 100 times against the online infrastructure of targeted victims across sectors.

- In October 2019, cyber actors exploited the Apple Remote Management Service (ARMS), a part of the Apple Remote Desktop (ARD) feature, to conduct DDoS amplification attacks, according to open source reporting. With ARD enabled, the ARMS service started listening on port 3283 for incoming commands to remote Apple devices, which attackers used to launch DDoS amplification attacks with a 35.5:1 amplification factor. ARD is used primarily to manage large fleets of Apple Macs by universities and enterprises.

- In May and August 2019, cyber actors exploited the Web Services Dynamic Discovery (WS-DD) protocol to launch more than 130 DDoS attacks, with some reaching sizes of more than 350 Gigabits per second (Gbps), in two separate waves of attack, according to open source reporting. Later the same year, several security researchers reported an increase in cyber actors' use of non-standard protocols and misconfigured IoT devices to amplify DDoS attacks, according to separate open source reporting. IoT devices are attractive targets because they use the WS-DD protocol to automatically detect new

[a] For the purposes of this Private Industry Notification, "built-in network protocols" refers to built-in network management protocols, network device discovery protocols, and web transfer protocols, each of which was designed to reduce computational overhead of day-to-day system and operational activities on end-user machines.

Internet-connected devices nearby. In addition, WS-DD operates using UDP, which allows actors to spoof a victim's IP address and results in the victim's being flooded with data from nearby IoT devices. As of August 2019, there were 630,000 Internet-accessible IoT devices with the WS-DD protocol enabled.

- In December 2018, cyber actors started abusing the multicast and command transmission features of the Constrained Application Protocol (CoAP) to conduct DDoS reflection and amplification attacks, resulting in an amplification factor of 34, according to open source reporting. As of January 2019, the vast majority of Internet-accessible CoAP devices were located in China and used mobile peer-to-peer networks.

Threat Outlook

Cyber actors increasingly are likely to abuse built-in network protocols for DDoS attacks against US networks. While a defense-in-depth strategy calls for the disabling of built-in features, such as ARMS, WS-DD, and CoAP, the loss of functionality to business productivity and connectivity may make implementing these strategies challenging. Moreover, device manufacturers are unlikely to disable such features by default because it would interfere with the user experience.

Cyber actors' abuse of built-in network protocols may enable DDoS amplification attacks to be carried out with limited resources and result in significant disruptions and impact on the targets. In the near term, cyber actors likely will exploit the growing number of devices with built-in network protocols enabled by default to create large-scale botnets capable of facilitating devastating DDoS attacks.

Identification

- Unusually slow network performance (opening files or accessing websites).
- Inability to access websites or other web-based resources.

Recommended Mitigations

- Enroll in a Denial of Service mitigation service that detects abnormal traffic flows and redirects traffic away from your network.

- Create a partnership with your local internet service provider (ISP) prior to an event and work with your ISP to control network traffic attacking your network during an event. The ISP may retain forensic data necessary for law enforcement investigations.
- Change the default username and passwords for all network devices, especially IoT devices. If the device's default username or password cannot be changed, ensure the device(s) providing Internet access to that device has a strong password and a second layer of security, such as multi-factor authentication or end-to-end encryption.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.
- Ensure all network devices are up to data and security patches are incorporated when available.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey