Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 October 2016

PIN Number
161026-001

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@ic.fbi.gov

Phone:
1-855-292-3937

Distributed Denial of Service Attack Against Domain Name Service Host Highlights Vulnerability of "Internet of Things" Devices

The exploitation of the "Internet of Things" (IOT) to conduct small-to-large scale attacks on the private industry will very likely continue due to the open availability of the malware source codes for targeting IoT devices and insufficient IoT device security.

Summary

On 21 October 2016, a domain name service (DNS) host and Internet management company for more than 80 Web sites experienced at least two waves of a distributed denial of service (DDoS) attack by botnets[a] comprised of Internet of Things[b] (IoT) devices believed to be infected with a variation of the Mirai malware. Despite certain groups claiming responsibility in open source, the FBI does not have any confirmation of a group or individuals responsible for the DDoS.

Malware Source Code Availability Enables IoT DDoS Attacks

In late September 2016 the hacker operating the Mirai botnet released its source code online - leading to the use of the malware by cyber actors to create botnets and launch independent DDoS attacks. The Mirai malware primarily targets the IoT devices such as routers, digital video records, and webcams/security cameras by exploiting their use of default usernames and passwords and coordinating them into a botnet used to conduct DDoS attacks.

[a] A botnet is a network of compromised computers controlled remotely by an attacker.
[b] The 'Internet of Things' is defined as the internetworking of physical devices, vehicles, buildings, and other items (often referred to as "smart devices"), embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

Recent reporting demonstrates that botnets comprised of IoT devices can be used to conduct unprecedented and powerful attacks that can take down Web sites. Additionally, in September 2016, two of the largest IoT DDoS attacks using the same malware disrupted the operations of a gaming server and computer security blogger Web site.

Computer security researchers over the past several months have identified dozens of new malware variants targeting Linux operating systems. The emergence of malware targeting Linux devices is likely based on the large number of mobile and IoT devices running exclusively on the Linux operating system. Most of the Linux malware variants scan the Internet for IoT devices that accept Telnet, which is used to log into a device remotely, and try to connect to vulnerable devices by using brute force attacks with common default login credentials.

Recommendations

The FBI suggests precautionary measures to mitigate a range of potential DDoS threats and IoT compromise to include, but are not limited to:

- Have a DDoS mitigation strategy ready ahead of time and keep logs of any potential attacks.
- Implement an incident response plan that includes DDoS mitigation and practice this plan before an actual incident occurs. This plan may involve external organizations such as your ISP, technology companies that offer DDoS mitigation services, and law enforcement. Ensure that your plan includes the appropriate contacts within these external organizations. Test activating your incident response team and third party contacts.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Review reliance on easily identified Internet connections for critical operations, particularly those shared with public facing Web servers.
- Ensure upstream firewalls are in place to block incoming UDP packets.
- Change default credentials on all IoT devices.
- Ensure that software or firmware updates are applied as soon as the device manufacturer releases them.

For additional information, please see the US-CERT DDos Quick Guide: https://www.us-cert.gov/security-publications/DDoS-Quick-Guide.

According to DHS Alert TA16-288A and FBI recommendation, in order to remove the Mirai malware from an infected IoT device, users and administrators should take the following actions:

Secure the Network from Threats (such as Mirai):

- **Disable Universal Plug and Play (UPnP) on your gateway router.** UPnP is a protocol to make it easy for devices inside the network to "open a port" to allow outside computers to communicate into the network. Disabling UPnP will improve the security of the network but may cause problems for some applications. It is recommended to enable UPnP only if necessary.

- **Disable remote management of the router over the Internet.** Enabling this feature often opens a remote web interface that can then be scanned and attacked. It is best to manage routers from inside the network. If it is absolutely necessary to reach the device from a remote location, consider setting up a rule in the firewall to only allow access from a specific location (IP and address).

- **Filter Ports Exploited by Mirai.** Ensure inbound ports 23 (telnet), 2323 (used for telnet on some IoT devices), and 103 (Mirai backdoor) are blocked at your Internet firewall or gateway router.

Remove Mirai from Infected Devices:

Note: It is recommended that you **disable Universal Plug and Play (UPnP) on your gateway router** (see above) before proceeding. This will help prevent reinfection of the IoT device.

1. Disconnect the IoT device from the network.

2. While disconnected from the network and Internet, perform a reboot. Because the Mirai malware exists in dynamic memory, rebooting the device clears the malware.

3. Ensure the password for accessing the device is changed from the default password to a strong password. See US-CERT Tip "Choosing and Protecting Passwords" for more information.

4. Only reconnect to the network after rebooting and changing the password. If the device reconnects before changing the password, it could be quickly reinfected with the Mirai malware.

5. Immediately upgrade the software and firmware after changing the admin password.

6. Enable automatic updates for the device. This feature will keep the device up to date with the latest software (not supported on all devices).

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as for peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

There is no additional information available on this topic at this time. For comments or questions related to the content or dissemination of this product, please contact the FBI's 24/7 Cyber Watch (CyWatch) at CyWatch@ic.fbi.gov or 855-292-3937. Press inquiries should be directed to the FBI's National Press Office at NPO@ic.fbi.gov or 202-324-3691.