TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

02 January 2019

PIN Number
20190102-001

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@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 criminals.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Actors Target Audio and Visual Communication Devices on Business Networks to Identify Vulnerabilities for Exploitation

Summary

The FBI identified incidents over the past few months in which cyber actors scanned for and sought to exploit audio and visual communication devices on networks to identify vulnerabilities which could later be used to gain access and unlawfully acquire information about the organization. In addition to targeting corporate information, vulnerable devices may be targeted for compromise for use in botnets or other criminal activities. The types of devices targeted include: Voice over Internet Protocol (VoIP) phones, video conferencing equipment, conference phones, VoIP routers, and cloud-based communication systems. While cyber actors have targeted VoIP and other communication devices in the past, the FBI continues to see these devices scanned by cyber actors for vulnerabilities.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

Specifically, the FBI observed cyber actors identifying and probing communication devices by issuing HTTP GET requests[a] to a business server or network to retrieve device configuration files. Information contained in configuration files often reveals IP addresses, usernames, passwords, system management URLs, and assigned phone numbers – all of which could be used by cyber actors for malicious purposes. Many of the requests are specific to particular brands of devices. Victims will often receive several GET requests in succession with the actors scanning for multiple brands of devices.

In addition, cyber actors retrieve IP addresses for further exploitation by using businesses' customer service VoIP hyperlinks, which are traditionally made available for customers to use in contacting the business. Once those hyperlinked calls are answered, the actor retrieves the IP address belonging to the phone which answered the call. Once the IP address is retrieved, an actor could send a large volume of packets to the IP address, overloading it and taking the service offline for the targeted business and its legitimate customers.

In addition to the above techniques, cyber actors target devices with brute-force attacks, attempting unauthorized access through the use of common usernames and passwords. Open source scanning tools can also be used to identify vulnerable communication devices and any associated ports.

All of the information obtained through scans and other methods are likely used for specific targeting efforts by cyber actors. This includes leveraging access to compromised audio and video devices to eavesdrop on meetings or conference calls, placing fraudulent international phone calls, leveraging the compromised device for use in botnets, and conducting man-in-the-middle attacks to redirect corporate network traffic.

Recommendations

The following recommendations may limit the success of these types of attacks:

- Conduct daily server log reviews to identify unusual activity, including GET and POST requests[b] from external IP addresses.

[a] (U) GET requests are used to request data from a resource.
[b] (U) POST requests are used to send data to create or update a resource.

- Work with the communication device/system providers to ensure servers are patched and updated regularly.
- Consider restricting access to configuration files or configuring firewalls to block traffic from unauthorized IP addresses.
- Restrict communication devices/systems to only non-sensitive business networks.
- Conduct regular penetration testing exercises on communication devices to identify and address vulnerabilities in a timely matter.
- Enable encryption on teleconference programs and applications and consider disabling auto-answer capabilities.
- Password protect configuration files, if possible.
- Regularly review and update users with access to administrative accounts.
- Segment configuration files on the network. Be sure to protect configuration and other device-related files after getting the device out of the box. Don't just plug and play.

Administrative Note

This product is marked **TLP: GREEN**. Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

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