Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

3 August 2017

PIN Number

170803-001

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

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order 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: WHITE**: The information in this product is useful for the awareness of all participating organizations within their sector or community.

Internet-Connected Printer Vulnerabilities Exploited by Criminal Actors

Summary

Over the past year, criminal actors exploited Internet-connected printers to manipulate print jobs and distribute violent threats or hate speech to US victims nationwide, according to multiple reports received by the FBI. The FBI received reports from US businesses in every sector concerning this threat, including law enforcement and academia. The reporting reflected that criminal actors often appeared to target unsecured, Internet-connected printers with open ports, making the victims targets of opportunity.

Threat

In late May 2017, more than 130 businesses, universities, and law enforcement agencies nationwide received fake bomb threats from an individual threat actor by facsimile, or as a forced print job on misconfigured Internet-connected printers. In all instances, the actor did not appear to target a specific printer model. The actor exploited Internet-connected printers that allowed external connections over port 9100 and did not require authentication. In one instance, the actor sent a bomb threat to a networked printer by compromising a vulnerable server running an outdated version of a PHP-based web application used to control security cameras. Following the intrusion, the actor wiped all logs associated with the incident.

According to FBI and open source reporting, in February 2017 a hacker using the alias Stackoverflowin compromised over 160,000 printers with open connections to the Internet by scanning for printers open on ports 515, 631, and 9100. Stackoverflowin sent print jobs to the affected printers and claimed the devices were part of a "flaming botnet." Stackoverflowin claimed the goal of the attack was to demonstrate vulnerabilities exist in Internet-connected printers and were subject to exploitation.

Also in February 2017, computer security researchers from University Alliance Ruhr identified and published flaws in 20 printer models based on common printing languages (Postscript and PJL), which would allow malicious actors to steal information, manipulate print jobs, shut down devices, or cause physical damage to the printer.

Between March 2016 and August 2016, an identified hacker compromised unsecured network printers at universities nationwide to print anti-Semitic flyers.

The FBI judges it is highly likely criminal actors will exploit Internet-connected device vulnerabilities and use them as pivot points for network intrusions. Vulnerable printers and other Internet-connected devices can easily be identified through open source scanning tools and search engines, such as Shodan.

Recommendations

The FBI has identified the following recommendations to prevent these types of cyber attacks:

- Ensure ports 515, 631, and 9100 are not publicly accessible over the Internet. If keeping these ports open is necessary, consider whitelisting specific IP addresses or subnets to ensure only legitimate traffic can connect to the printer.

- Consider the use of alternative ports for Internet-connected printers and other devices.

- Ensure all Internet-connected printers and devices on the network have strong usernames and passwords. Default usernames and passwords should be changed.

- Conduct daily reviews of printer logins to identify and flag unauthorized IP addresses.

- Configure firewalls to block traffic from unauthorized IP addresses to printers and other network devices.

- Restrict Internet-connected printer and device connectivity to non-sensitive business networks.

The FBI encourages recipients of this notification 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@ic.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@ic.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