Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

22 March 2017

PIN Number
170322-001

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

Cyber Criminals Targeting FTP Servers to Compromise Protected Health Information

Summary

The FBI is aware of criminal actors who are actively targeting File Transfer Protocol (FTP)[a] servers operating in "anonymous" mode and associated with medical and dental facilities to access protected health information (PHI) and personally identifiable information (PII) in order to intimidate, harass, and blackmail business owners.

Threat

Research conducted by the University of Michigan in 2015 titled, "FTP: The Forgotten Cloud," indicated over 1 million FTP servers were configured to allow anonymous access, potentially exposing sensitive data stored on the servers. The anonymous extension of FTP allows a user to authenticate to the FTP server with a common username such as "anonymous" or "ftp" without submitting a password or by submitting a generic password or e-mail address.

While computer security researchers are actively seeking FTP servers in anonymous mode to conduct legitimate research, other individuals are making connections to these servers to compromise PHI and PII for the purposes of intimidating, harassing, and blackmailing business owners. Cyber criminals could also use an FTP server in anonymous mode and configured to allow "write" access to store malicious tools or launch targeted cyber attacks. In general, any misconfigured or unsecured server operating on a business network on which sensitive data is stored or processed exposes the business to data theft and compromise by cyber criminals who can use the data for criminal

[a] (U) FTP is a protocol widely used to transfer data between network hosts.

purposes such as blackmail, identity theft, or financial fraud.

Recommendations

The FBI recommends medical and dental healthcare entities request their respective IT services personnel to check networks for FTP servers running in anonymous mode. If businesses have a legitimate use for operating a FTP server in anonymous mode, administrators should ensure sensitive PHI or PII is not stored on the server.

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@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. Victims of cyber crime are encouraged to file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov.

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 CyWatch.

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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu