Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 June 2017

PIN Number
170628-001

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 in order to help cyber security professionals and system administrators to 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.

Individuals Threatening Distributed Denial of Service of Private-Sector Companies for Bitcoin

Summary

An individual or group claiming to be “Anonymous” or “Lizard Squad” sent extortion emails to private-sector companies threatening to conduct distributed denial of service (DDoS) attacks on their network unless they received an identified amount of Bitcoin. No victims to date have reported DDoS activity as a penalty for non-payment.

Threat

In April and May 2017, at least six companies received emails claiming to be from “Anonymous” and “Lizard Squad” threatening their companies with DDoS attacks within 24 hours unless the company sent an identified amount of Bitcoin to the email sender. The email stated the demanded amount of Bitcoin would increase each day the amount went unpaid. No victims to date have reported DDoS activity as a penalty for non-payment.

Reporting on schemes of this nature go back at least three years.

- In 2016, a group identifying itself as "Lizard Squad" sent extortion demands to at least twenty businesses in the United Kingdom, threatening DDoS attacks if they were not paid five Bitcoins (as of 14 June, each Bitcoin was valued at 2,698 USD). No victims reported actual DDoS activity as a penalty for non-payment.

- Between 2014 and 2015, a cyber extortion group known as "DDoS '4' Bitcoin" (DD4BC) victimized hundreds of individuals and businesses globally. DD4BC would conduct an initial, demonstrative low-level DDoS attack on the victim company, followed by an email message introducing themselves, demanding a ransom paid in Bitcoins, and threatening a higher level attack if the ransom was not paid within the stated time limit. While no significant disruption or DDoS activity was noted, it is probable companies paid the ransom to avoid the threat of DDoS activity.

Background

Lizard Squad is a hacking group known for their DDoS attacks primarily targeting gaming-related services. On 25 December 2014, Lizard Squad was responsible for taking down the Xbox Live and PlayStation networks. Lizard Squad also successfully conducted DDoS attacks on the UK's National Crime Agency's (NCA) website in 2015.

Anonymous is a hacking collective known for several significant DDoS attacks on government, religious, and corporate websites conducted for ideological reasons.

Recommendations

The FBI suggests precautionary measures to mitigate DDoS threats to include, but not limited to:

- Have a DDoS mitigation strategy ready ahead of time.

- 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 Internet Service Provider, technology companies that offer DDoS mitigation services, and law enforcement.

- Ensure 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.

- Ensure upstream firewalls are in place to block incoming User Data Protocol (UDP) packets.

- Ensure software or firmware updates are applied as soon as the device manufacturer releases them. If you have received one of these demands:

- Do not make the demand payment.

- Retain the original emails with headers.

- If applicable, maintain a timeline of the attack, recording all times and content of the attack.

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. 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: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.

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

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