Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 June 2015

PIN Number
150626-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CYWATCH**.

E-mail:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

Bitcoin Extortion Campaigns Expanding Distributed Denial of Service Attacks to a Wider Array of Business Sectors

General Observations

Recent FBI investigations and open source reporting reveal that extortion campaigns conducted via e-mails threatening Distributed Denial of Service (DDoS) attacks continue to expand targets from unregulated activities, such as illegal gaming activity, to now include legitimate business operations. The increase in scope has resulted in additional attacks with Bitcoin ransom amounts trending upwards as well.

First identified approximately one year ago, Bitcoin extortion campaigns originally focused on targets unlikely to contact law enforcement for assistance. In early April 2015, the extortion campaigns began regularly contacting legitimate businesses operating in the private sector.

In a typical scenario, a short-term DDoS attack is conducted on a victim's web site lasting for approximately one hour. The DDoS is followed by an e-mail containing an extortion demand for payment via Bitcoin. If the victim has not paid the demanded payment, there is usually a second, more powerful DDoS attack within 24 hours, which lasts for an additional hour. This is followed by a second e-mail warning and extortion demand with an increased price. In most cases, victim companies have successfully mitigated the attack using third party DDoS mitigating services rather than paying the ransom.

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

TLP: GREEN

Technical Details

- The first DDoS attack is usually delivered prior to the sending of a ransom demand at 20-40 Gigabytes per second (Gbps) with a duration of approximately one hour.
- After the initial DDoS attack, an extortion e-mail is sent to the victim introducing the attacker, highlighting the initial demonstrative DDoS attack, and demanding payment in Bitcoin (ranging from 20-40) to ensure no further DDoS attacks are conducted against the business. If payment does not occur within 24 hours, a second demonstrative DDoS is generally conducted at a higher rate (40-50 Gbps) for an additional hour followed by an additional extortion e-mail.
- The types of DDoS attacks primarily consist of Simple Service Discovery Protocol (SSDP) and Network Time Protocol (NTP) reflection/amplification attacks with the occasional SYN-flood and, most recently, Wordpress XML-RPC reflection/amplification attacks.

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.

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 with 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, contact CyWatch.