Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 March 2016

Alert Number
160304-001

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

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

"Criminal-Seeking-Hacker" Requests Network Breach for Insider Trading Operation

Summary

A financially motivated cyber crime insider trading scheme targets international law firm information used to facilitate business ventures. The scheme involves a hacker compromising the law firm's computer networks and monitoring them for material, non-public information (MNPI)[1]. This information, gained prior to a public announcement, is then used by a criminal with international stock market expertise to strategically place bids and generate a monetary profit.

Threat

In a recent cyber criminal forum post, a criminal actor posted an advertisement to hire a technically proficient hacker for the purposes of gaining sustained access to the networks of multiple international law firms. The criminal provided search criteria for industry-specific information for the hackers to locate within the networks. This information when interpreted by an industry expert can contribute to an insider trading scheme.

Recommendations

Historically, industries targeted by cybercriminals have discovered that their networks were susceptible to intrusion due to lack of adherence to network security industry standards.

Measures to deter unauthorized access to a company network:

- Educate personnel on appropriate preventative and reactive actions to known criminal schemes and social engineering threats, including how employees should respond in their respective position and environment.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Disable macros. Be careful of pop-ups from attachments that require users to enable them.

[1] (U) MNPI is information not generally disseminated to the public that a reasonable investor would likely consider important in making an investment decision.

- Only download software - especially free software - from known and trusted sites
- Create a centralized Information Technology e-mail account for employees to report suspicious e-mails.
- Change network default passwords, configurations, and encryption keys. Use strong passwords.
- Recommend your company's IT professional(s) review, test, and certify the need/compatibility of a patch or update prior to installing it onto the operating system or software.
- Monitor employee logins that occur outside of normal business hours.
- Restrict access to the Internet on systems handling sensitive information.
- Install and regularly update anti-malware solutions, software, operating systems, remote management applications, and hardware.
- Do not use the same login and password for multiple platforms, servers, or networks.
- Monitor unusual traffic, especially over non-standard ports. Close unused ports.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Isolate sensitive information within the network.
- Only allow required processes to run on systems handling sensitive information.
- Implement two-factor authentication for access to sensitive systems.
- Ensure proper firewall rules are in place.
- Be aware of the corporate footprint and persona facing the Internet. Conduct searches using multiple search engines on multiple Internet domains of company names, Web addresses, key personnel, and projects to determine if there is an accidental weak point in the network security. Conduct infrastructure look-ups in the public domains to ensure additional information is not inadvertently advertised.

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: AMBER. Information contained in this product is for official use only and should not be further disseminated. Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. No portion of it should be released to the media, the general public, or over non-secure Internet servers. 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.