FBI Cyber Division

Public Service Announcement

August 22, 2013

Spear-Phishing E-mail with Missing Children Theme

The FBI has become aware of a spear-phishing e-mail made to appear as if it were from the National Center for Missing and Exploited Children. The subject of the e-mail is "Search for Missing Children," and a zip file containing 3 malicious files is attached. E-mail recipients should never open attachments or click links in suspicious e-mails.

Spear-phishing attacks are often used by individuals conducting targeted, rather than opportunistic, attacks. Those responsible for the attack may be seeking precise information stored on an organization's network or systems rather than monetary gain.

Every organization is at risk of being the target of a spear-phishing attack. This type of activity can best be mitigated with increased cyber security. When weighing available options pertaining to the implementation of appropriate mitigation strategies, organizations must begin by asking themselves the following:

- If proprietary data, personally identifiable information (PII), research and development-related data, e-mail, or other critical information were stolen, what would the current and future consequences be?
- Has my organization evaluated data criticality based on risk? What must be protected in the organization?

To mitigate the threat of spear-phishing and other targeted attacks, DHS's United States Computer Emergency Readiness Team (US-CERT) recommends the following actions:

- Always treat unsolicited or unexpected e-mail containing attachments or links with caution, even (and perhaps especially) when the e-mail appears related to known events or projects.
- Monitor for and report on suspicious activity, such as spear phishing e-mails, leading up to significant events and meetings.
- Educate users about social engineering and e-mail phishing related to high-level events and meetings.
- Measure expected network activity levels so that changes in patterns can be more easily identified.

If you have received a suspicious e-mail at work, please report it to your organization in accordance with your organization's security policy. You may also report this activity to the FBI by filing a complaint at www.ic3.gov. US-CERT can be reached by telephone at 888-282-0870 or by e-mail at SOC@us-cert.gov. US-CERT's web site can be found online at www.us-cert.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.