MS-ISAC

MS-ISAC Security Primer

Spear Phishing

March 2017, SP2017-0413

Cyber threat actors utilize phishing emails to compromise systems, networks, and/or gather information using social engineering techniques. A phishing email is designed to prompt a response from the recipient, such as clicking on a link or opening an attachment. Through the response, the recipient may download malware or be redirected to a website prompting them to provide sensitive information, such as login credentials, that will be sent to the cyber threat actors. Spear phishing involves a cyber threat actor sending targeted emails to a small group of users.

TECHNICAL RECOMMENDATIONS:

- Implement filters at the email gateway to filter out emails with known phishing indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Consider blocking file attachments that are commonly associated with malware, such as .dll and .exe, and that cannot be thoroughly scanned by antivirus software, such as .zip files.
- Implement Domain-based Message Authentication, Reporting, & Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures. Learn more at http://dmarc.globalcyberalliance.org.
- Adhere to the principal of least privilege. If a user has no need for administrative access on a machine to carry out their daily activities; they should not have an administrative account. This can minimize the damage caused by malicious activity carried out under the user's credentials.
- Apply appropriate patches and updates provided by Microsoft, Oracle, Adobe, and other third party application providers to vulnerable systems immediately after appropriate testing. Malware frequently exploits vulnerabilities for which a software patch was released.
- Use antivirus programs with automatic updates of signatures and software.
- Provide social engineering and phishing training to employees. Urge them to not open suspicious emails, click links contained in such emails, post sensitive information online, and never provide usernames, passwords, and/or personal information to any unsolicited request.
- Create a policy for reporting phishing emails to the Information Technology (IT) department.

Other types of phishing include:

- Smishing ("SMS phishing") involves a user opening a malicious SMS, or text, message on a mobile device.
- Vishing involves a cyber threat actor attempting to gather information over Voice over IP (VoIP) phones.
- Whaling is a spear phishing attempt directed towards a senior executive or other high profile target.

USER RECOMMENDATIONS:

- Do not open suspicious emails or attachments, as they may contain malware. Only open expected attachments from trusted senders.
- The easiest way to check a link is by hovering over it with your mouse. This action allows the true destination of the link to appear in the bottom left corner of your browser window or next to your mouse pointer in Microsoft Outlook.
- Never reveal personal or financial information in response to an email. Legitimate organizations will never ask for this information in an unsolicited email.
- If the message appears to be a phishing or spam email, do not respond. Report it to the IT department immediately and await further instruction.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.