MS-ISAC™

MS-ISAC Security Primer

The Risk of Online Shopping During the Holiday Season

November 2017, SP2017-1750

TLP: WHITE State, local, tribal and territorial (SLTT) government employees who choose to shop online while on SLTT government organizational systems expose those systems to malware infections and account compromises and themselves to phishing attempts. Although there is a year-round risk of exposure to malware and other attacks, the risk during the holiday season is heightened because of the increase in online shopping and associated emails. The National Retail Federation's yearly "Cyber Monday Expectations Survey" estimated that 122 million Americans would shop online in 2016 and every year this figure is expected to rise. The individuals surveyed also supplied that they would shop during business hours. This augments the likelihood that SLTT government systems will be infected. According to Nippon Telegraph and Telephone (NTT) Group's 2016 Global Threat Intelligence Report, retailers experience the most cyber-attacks of any industry sector. It is likely that holiday shoppers will encounter websites intentionally or unintentionally concealing malicious code.

- Employees can introduce malware to networks by opening malware laden emails and attachments or clicking on links to infected websites. Malware may also come through malvertising (malicious advertising), which is the use of online, malicious advertisements to spread malware.
- During the online shopping season, employees are more likely to open emails, create new accounts, and potentially share their work email addresses or reuse passwords. This can result in employees opening and acting on emails they do not realize are malicious. In addition, using their official email addresses for online orders discloses where the employees work and may expose their passwords through password reuse.

TLP: WHITE **RECOMMENDATIONS:**

- Harness your employees increased interest on online shopping by refreshing their knowledge of social engineering tactics. Be sure to stress that employees should never register for online accounts utilizing work emails or re-use passwords used for work accounts.
- Keep all operating systems, applications, antivirus, and essential software up-to-date.
- Ensure that organizational firewall, proxy server, and browser configurations prevent access to risky websites or those known to be malicious. Web browser configurations should alert users when accessing websites using http instead of https.
- Implement the email authentication protocol, Domain-based Message Authentication, Reporting & Conformance (DMARC) which builds upon the sender policy framework (SPF), as advised in DHS BOD 18-01 available at https://cyber.dhs.gov.
- If permissible, within the confines of organizational Internet use policies, consider providing employees with guest wireless access and allowing employees to bring their own devices to work in order to reduce the likelihood SLTT government systems are accidentally infected.
- Ensure that systems are hardened with industry-accepted guidelines, such as those provided by the CIS SecureSuite. Review and consider implementation of the 20 CIS Controls, where appropriate, as a means of bolstering your organization's security posture.
- Consider developing a cybersecurity awareness training program and supplement it with the MS-ISAC's newsletters and webinars to promote online safety practices; available at https://learn.cisecurity.org/ms-isac-subscription.

TLP: WHITE 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.