TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC Partners

DATE: April 6, 2017

SUBJECT: MS-ISAC CYBER ALERT – Increased Levels of Data Breaches Driven by W-2 Phishing Scam

The Multi-State Information Sharing and Analysis Center (MS-ISAC) observed a higher than anticipated number of reported data breaches in the first quarter of 2017, due in large part to a substantial increase in the number of successful W-2 phishing scams. The W-2 phishing scam is a variant of the Business Email Compromise (BEC) scam, in which malicious actors impersonate (spoof) or compromise the accounts of authorized officials to send finance or human resources staff emails requesting employee W-2 information. The scam is successful when the finance or human resources staff send W-2 information to the malicious actor, resulting in a data breach, with the information used for identity theft and/or file fraudulent tax returns.

Due to the substantial increase in W-2 phishing scams, the number of reported data breaches in the first quarter of 2017 already exceeds 80% of the total number of data breaches reported in 2016. Based on the 2016 pattern, the MS-ISAC expects that this scam will decrease in frequency but continue to occasionally target state, local, tribal, and territorial (SLTT) governments after April 2017.

- In 2016, the MS-ISAC identified 68 data breaches, 7 of which were related to the W-2 phishing scam.
- In the first quarter of 2017, the MS-ISAC has already identified 55 data breaches, 37 of which were related to the W-2 phishing scam. Of note, K-12 schools accounted for 54% of reported phishing-related data breaches in 2017 to date.

The MS-ISAC has identified several other variants of BEC scams targeting SLTT governments, including the variant where the impersonated or compromised senior executive account requests that a wire transfer be issued. These variants do not result in data breaches, but are worth noting as any training or awareness activities should include the wire transfer variant.

Key indicators of BEC scams include short poorly written messages purportedly from smartphones, spoofed email addresses, requests made when the executive is out of the office, and unusual requests.

If you experience similar targeting, please do not hesitate to reach out to the MS-ISAC for assistance on this matter. We perform a variety of free incident response services including log analysis, malware analysis, computer forensics, and can assist with the development of a mitigation and recovery strategy. Requests for these services can be obtained by calling 1-866-787-4722, replying to this email, or sending an email to SOC@msisac.org.

The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

RECOMMENDATIONS:
We recommend the following actions be taken:

1. Craft a policy for identifying and reporting BEC and similar phishing email scams. Make sure to include the following:
    a. When receiving unusual financial or sensitive data requests, users should **verify the identity** and authority of the email sender via standard (non-email) channels.
    b. Users should **hover to discover**, to ensure that the email is going to the correct person. The true recipient of an email can often be verified by hovering the mouse over the address in the email header.
    c. Users should reply through a new email, and not by hitting the “reply” button, which helps to prevent successful spoofing attacks.
    d. Users should **report** suspicious emails to security staff. Tax-related suspicious emails should be reported to the IRS. Other BEC related emails can be reported to the Internet Crime Complaint Center (IC3). The MS-ISAC also appreciates receiving notifications of all BEC scam attempts.
2. **Train staff** in the finance, human resources, and other potentially targeted departments to follow the policy so that they will recognize W-2 and wire transfer phishing emails.
3. **Implement filters** at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall. For example, Domain-based Message Authentication, Reporting & Conformance (DMARC) is a filter that allows organizations to better protect themselves against fraudulent emails.
4. **Monitor email addresses** to flag similar-looking company email domains and known phishing attempt indicators. Where possible, add a banner or warning line to emails from external domains.
5. **Reach out and warn** other departments, agencies, and especially K-12 schools, of the BEC scam.

REFERENCES:

https://www.ic3.gov/media/2016/160614.aspx
https://dmarc.org/

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/