TLP: WHITE
MS-ISAC CYBER ALERT (Education Sector)

TO: All MS-ISAC Members and Intel Partners

DATE ISSUED: December 4, 2017

SUBJECT: Increase in Compromises of K-12 School Employee Direct Deposit Accounts

The MS-ISAC has seen an increase in cyber threat actors sending phishing emails to K-12 public education employees for the purposes of obtaining account login information. In these incidents, this information is then typically used to modify the employees' direct deposit account information. By changing this information, the cyber threat actors reroute the employees' paychecks to a financial account under the actors' control. No specific payroll platforms are being targeted, as reports indicate the victims have used various platforms for payroll functionality.

Historically, the MS-ISAC has seen this attack target the education sector and universities in particular. Though universities are still targeted, the MS-ISAC is currently seeing an increase in K-12 school incidents.

This type of attack utilizes the inherent risk behind the use of single sign-on (SSO) features. SSO allows for the use of a single set of credentials to gain access to connected systems, providing authentication, authorization, access control, and password synchronization across an environment. In these incidents the cyber threat actor usually sends school staff a phishing email, a PDF attachment or malicious link. The phishing email often spoofs the account of an IT administrator or senior official. Upon clicking the link or downloading the attachment, the user is prompted to enter their login credentials, which the cyber threat actor uses to log into the payroll system. The cyber threat actor then changes the direct deposit information for that employee so that the employee's paycheck is sent to a different account or pre-paid credit card. According to the FBI, in some instances the cyber threat actor is also accessing the employee's email account and creating rules that immediately forward incoming emails containing specific words to the deleted folder so the employee does not get alerted to the criminal activity.

RECOMMENDATIONS:
The MS-ISAC recommends organizations adhere to the following general best practices to limit the effect of this and similar phishing emails:

<u>Pre-Incident</u>

- Warn users to never provide credentials in response to an email from any source.
- Enable two-factor authentication. Otherwise require employees to change their direct deposit information through a non-electronic method with the human resources or finance departments.
- Consider notifying employees via an out-of-band communication channel when their financial information has been changed.
- Mark external emails with a banner denoting the email is from an external source. This will assist users in detecting spoofed emails.
- If you don't have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT

departments. When emails matching this pattern are detected, issue an immediate notification to all staff and where possible, remove the emails from the server.

- Consider blocking file attachments that are commonly associated with malware, such as .dll and .exe, and which cannot be thoroughly scanned by antivirus software, such as .zip files.
- 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.
- Routinely review logs to determine unusual access requests, based time or location analysis.
- 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, or provide personal information to any unsolicited request. Teach users to hover over a link with their mouse to verify the destination prior to clicking on the link, as well as confirm the "reply to" section of the e-mail header matches the sender's e-mail.
- 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.

Post-Incident

- While unlikely, it may be possible to recall payments to fraudulent accounts if they are discovered in less than 72 hours. To gain assistance in doing so, contact the banks involved and then contact federal law enforcement – either the local FBI or U.S. Secret Service office.
- If your organization uses single sign-on (SSO) in relation to direct deposit, you can confirm an attack by checking your logs to determine if unusual IP addresses attempted to or logged into the payroll system and if the same IP address changed the information for multiple accounts. This may aid in discovering additional victims.
- Password changes should be enforced on impacted employees.
- A breach investigation should be conducted to ensure the cyber threat actors did not access sensitive data, such as personally identifiable information (PII) or grades, or create email server rules,.

24x7 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

. . . . .