This advisory was prepared in collaboration with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and Internal Revenue Service Criminal Investigation (IRS-CI).

Joint Advisory Bulletin: W-2 Phishing, Tax Related Identity Theft and Business Email Compromise

12 January 2018

Increase in W-2 Phishing Campaigns

In 2017, FS-ISAC and IRS-CI continued to observe tax form related phishing campaigns, including several new variations that combine W-2 scams with business email compromise (BEC) or business email spoofing (BES) and wire transfer fraud. IRS's Online Fraud Detection & Prevention (OFDP) office—which manages phishing@irs.gov —- observed a significant increase in reports of W-2 related scams from more than 100 in 2016 to approximately 900 reports in 2017. Further, the earliest reporting date for incidents in 2017 was January 5, prior to the start of tax season while the earliest report date for 2016 was February 19. Despite the large increase, the most popular methods remain sending an email either spoofing the target organization or using a free email account and typosquatted domains to impersonate a C-level executive to an HR professional within the organization. The volume of reports jumped dramatically in February 2017, accounting for 60% of BEC/BES W-2 reports received in CY2017. Emails to phishing@irs.gov included both victims and non-victims, many of whom noted repeated contact, with multiple W-2 requests or follow-up emails. Such instances could indicate a multi-step campaign with actors following up with a fraudulent wire transfer request before, during or after the request for W-2s.

Trends

Cybercriminals use various spoofing techniques in attempts to contact an employee in the payroll or human resources departments, requesting a list of all employees and copies of their Form-W-2. Such techniques include disguising an email to make it appear as if it is from an organization executive or even compromising the email account itself gain legitimacy. This scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES). They achieve this by spoofing the "From" field and adding a "Reply-To" address or using a free email service account for the email address and spoofing the sender name. Another technique is to use a typosquatted domain.

In the latest twist, the cybercriminal follows up with an "executive" email to the payroll or comptroller and asks that a wire transfer also be made to a certain account. In one case, an administrator account was phished and the email was used to contact the company's president requesting W-2s. Although not independently tax related, the wire transfer scam is being coupled with the W-2 scam email. Some companies have lost both employees' W-2s and thousands of dollars due to wire transfers. In some cases, firms received a BEC wire transfer request simultaneously or immediately after falling victim to the BEC W-2 request.

The W-2 scam is just one of several new variations to appear in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Individual taxpayers also can be targets of phishing scams, but cybercriminals seem to have evolved their tactics to focus on mass data thefts.

Reporting

How to report a data loss related to the W-2 scam

If notified quickly after the loss, the IRS may be able to take steps that help protect your employees from tax-related identity theft. Ways to contact the IRS about a W-2 loss include:

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide your contact information listed below so that we may call you. In the subject line, type "W-2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information (PII) data.
    1. Business name
    2. Business employer identification number (EIN) associated with the data loss
    3. Contact name
    4. Contact phone number
    5. Summary of how the data loss occurred
    6. Volume of employees impacted

Note: The IRS does not ***initiate*** contact with taxpayers by email, text messages or social media channels to request personal or financial information. Any contact from the IRS will be in response to a contact initiated by you. When cybercriminals learn of a new IRS process, they often create false IRS web sites and IRS impersonation emails.

How to report data loss to state tax agencies

- Any breach of personal information could have an effect on the victim's tax accounts with the states as well as the IRS. You should email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.

How to report data loss to other law enforcement officials

- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3)
- Businesses/payroll service providers may be asked to file a report with their local law enforcement agency

What to tell your employees about a Form W-2 data loss

Cybercriminals who successfully steal Form W-2 data immediately attempt to monetize their thefts. Criminals may immediately attempt to file fraudulent tax returns claiming a refund. Alternatively, they may sell the data on the Internet's black-market sites to others who file fraudulent tax returns or use the names and social security numbers (SSNs) to create other crimes. Here is some guidance to share with your employees:

1. Review Taxpayer Guide to Identity Theft
2. Share IRS Publication 5027, Identity Theft Information for Taxpayers, with employees and direct them to the "Steps for Identity Theft Victims" which includes:
    a. Contacting one of the three credit bureaus to place a "fraud alert" on their account; they may consider placing a "credit freeze" which offers more protection.
    b. File a complaint with the Federal Trade Commission, the lead federal agency on identity theft issues.
    c. Review FTC www.identitytheft.gov information for additional steps to recover from identity theft.

1. The FTC also offers guidance to businesses on how to inform employees of the incident and additional steps businesses may take. See Data Breach Response: A Guide for Business.
2. Share IRS Publication 4524, Security Awareness for Taxpayers, with your employees

How to report receiving the W-2 phishing email

If your business received a BEC/BES W2 email, please forward the email to the IRS. The IRS needs the email header from the phishing email for its investigation, which means you must do more than just forward the email to phishing@irs.gov. Here's what to do with the W-2 email scam:

1. The email headers should be provided in plain ASCII text format. Do not print and scan.
2. Save the phishing email as an email file on your computer desktop.
3. Open your email and attach the phishing email file you previously saved,
4. Send your email containing the attached phishing email file to phishing@irs.gov. Subject line: W-2 Scam. Do not attach any sensitive data such as employee SSNs or W-2s.
5. File a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.

Recommendations and Best Practices

Customer Guidance

The key to reducing the risk from W-2 phishing scams and BEC is to understand the criminals' techniques and deploy effective mitigation processes. There are various methods to reduce the risk of falling victim to this scam and subsequently disclosing sensitive information or executing a fraudulent wire transfer. Some of these methods include:

- Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers and handle W-2 related requests or tasks;
- Use out of band authentication to verify requests for W-2 related information or wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request;
- Verify a change in payment instructions to a vendor or supplier by calling to verbally confirm the request (the phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor);
- Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions;
- Delay the transaction until additional verifications can be performed, when the staff at a victim business is contacted by the bank to verify the wire transfer; and
- Require dual-approval for any wire transfer request involving one or more of the following:
    - A dollar amount over a specific threshold;
    - Trading partners who have not been previously added to a "white list" of approved trading partners to receive wire payments;
    - New trading partners;

- New bank and/or account numbers for current trading partners; and/or
- Wire transfers to countries outside of the normal trading patterns.

ISP Guidance

To address typosquatted or malicious/compromised domains it is recommended that, if possible, affected parties contact the appropriate service providers to report the activity using the following guidelines:

- Use domain and IP WHOIS to determine the appropriate POCs
- Compromised site: report the URL to the appropriate hosting provider
- Email "dropbox" Accounts: report to email service providers for takedown
- Compromised X-Sender: report to registrar or appropriate system owner
- Typosquatted domains: report to the registrar and/or hosting provider to de-register the domain

Contact Information

- FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process and to login at fsisac.com. This reporting can be done with attribution or anonymously and will assist other members and their customers to prevent, detect and respond to similar activity. Anyone experiencing this activity is encouraged to reach out to the FS-ISAC SOC at soc@fsisac.us or call (877) 612-2622, prompt 2.
- Employers who receive or fall victim to the W-2 scam should review guidance at Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers. For general questions, visit http://www.irs.gov/identitytheft

Appendix

(IR-2016-34) https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

(IR-2017-10) https://www.irs.gov/uac/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w2-scam-targeting-payroll-human-resource-departments

(IR-2017-20) - https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others