Criminal Investigation

Compromises From Business E-mails Targeting W-2s/Tax Professionals

Brian Thomas
National ID Theft Coordinator
Refund Crimes

Criminal Investigation

What is a Business Email Compromise (BEC)?

- The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

Source: FBI Public Service Announcement I-050417-PSA, May 4, 2017

Criminal Investigation

Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others

- Feb. 2, 2017
- WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry issued an urgent alert today to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits.
- In a related development, the W-2 scammers are coupling their efforts to steal employee W-2 information with an older scheme on wire transfers that is victimizing some organizations twice.
- "This is one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme," said IRS Commissioner John Koskinen.
- https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

Criminal Investigation

January 17, 2018

- The Form W-2 scam has emerged as one of the most dangerous phishing emails in the tax community. During the last two tax seasons, cybercriminals tricked payroll personnel or people with access to payroll information into disclosing sensitive information for entire workforces. The scam affected all types of employers, from small and large businesses to public schools and universities, hospitals, tribal governments and charities.
- Reports approximately 900 in 2017, compared to slightly over 100 in 2016.
- By alerting employers now, the IRS and its partners in the Security Summit effort hope to limit the success of this scam in 2018. The IRS last year also created a new process by which employers should report these scams. There are steps the IRS can take to protect employees, but only if the agency is notified immediately by employers about the theft.

Criminal Investigation

BEC Targeting Education

- Schools and Universities are targets due to the large volume of public information available.
- Targeted areas include:
  - Business Operations (Finance, Payroll & Human Resources)
  - Facilities
  - Maintenance

Criminal Investigation

- Cybercriminals are able to **identify** chief operating officers, school executives or others in position of authority (Social Engineering).
- Fraudsters mask themselves as executives or people in authoritative positions and send emails to payroll or human resources requesting copies of Forms W-2. **(Grooming)**
- Form W-2 contains the following **(Exchange of Information)**
  - Employment Identification Numbers (EIN)
  - Social Security Numbers
  - Income / Withholdings (Federal, State, Local)
  - Address
  - Retirement Plan
  - Health Benefits Plan

Criminal Investigation

W-2 Schemes

School Districts

- North Carolina released 8,000 W-2's.
- Washington released 6,000 W-2's.
- Ohio released 7,500 W-2's.

Criminal Investigation

Business E-mail Compromises

- The e-mail correspondences usually contain grammar and spelling errors.
- The data compromises usually go undetected for over 210 days.
- Information is usually sold on Dark Web to other groups.

Criminal Investigation

BEC Example #1

-----Original Message-----
From: Daisy Duck
Sent: Monday, January 03, 2018 10:01 AM
To: Goofy
Subject: Inquiry

Morning Goofy,
I'll need you to pull out 2017 W-2 of all Employees as provided by the IRS, Kindly email details attached in a PDF when you are done.

Thanks,
Daisy Duck

Sent from my iPhone

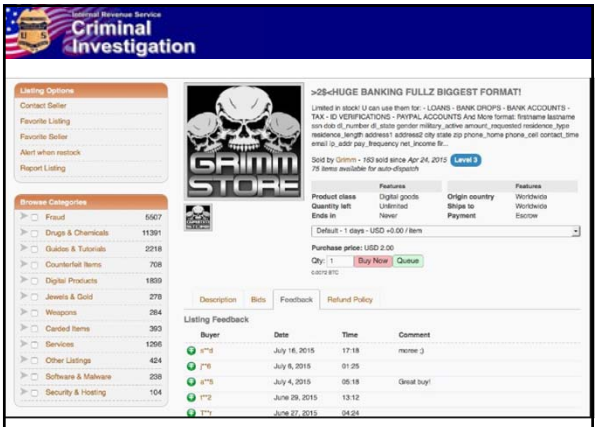
Internal Revenue Service
Criminal Investigation

What is the Dark Web?

Internal Revenue Service
Criminal Investigation

Examples of the Markets

Internal Revenue Service
Criminal Investigation



Criminal Investigation

Access to Personal Identifying Information

Criminal Investigation

Example #2

Donald, are you there?

"Send me the list of W-2 copy of employees wage and tax statement for 2017, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap. Thanks, Mickey (CEO)."

Criminal Investigation

Email Header pertaining to BEC

Delivered-To: D.Duck@MMschools.org
Received: by 10.103.135.11 with SMTP id j11csp735677vsd;
Fri, 24 Feb 2017 09:09:29 -0800 (PST)
X-Received: by 10.28.6.210 with SMTP id 201mr3679203wmg.85.1487956169066;
Fri, 24 Feb 2017 09:09:29 -0800 (PST)
Return-Path: <ceo@ceooffices.info>
Received: from mout.perfora.net (mout.perfora.net. [74.208.4.196])
by mx.google.com with ESMTPS id g3si11034851wrb.153.2017.02.24.09.09.27
for <D.Duck@MMschools.org>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Fri, 24 Feb 2017 09:09:29 -0800 (PST)
Received-SPF: neutral (google.com: 74.208.4.196 is neither permitted nor denied by best guess record for domain of ceo@ceooffices.info) client-ip=74.208.4.196;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 74.208.4.196 is neither permitted nor denied by best guess record for domain of ceo@ceooffices.info) smtp.mailfrom=ceo@ceooffices.info
Received: from oxusgaltgw05.schlund.de ([10.72.72.51]) by mrelay.perfora.net
(mreueus002 [74.208.5.2]) with ESMTPSA (Nemesis) id 0LwHJA-1cGPbU0uju-0184J6
for <D.Duck@MMschools.org>; Fri, 24 Feb 2017 18:09:26 +0100
Date: Fri, 24 Feb 2017 12:09:25 -0500 (EST)
From: Mickey Mouse <ceo@ceooffices.info>
Reply-To: Mickey Mouse <ceo@ceooffices.info>

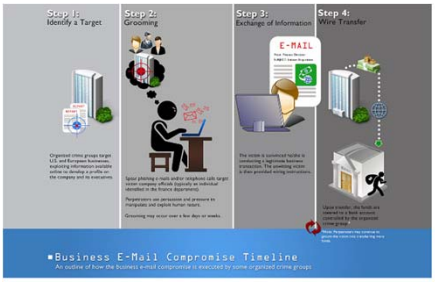
Internal Revenue Service
Criminal Investigation

New Twist to W-2 Scam: Companies Also Being Asked to Wire Money

- 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. Although not tax related, the wire transfer scam is being coupled with the W-2 scam email, and some companies have lost both employees' W-2s and thousands of dollars due to wire transfers.
- The IRS, states and tax industry urge all employers to share information with their payroll, finance and human resources employees about this W-2 and wire transfer scam. Employers should consider creating an internal policy, if one is lacking, on the distribution of employee W-2 information and conducting wire transfers

https://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

Internal Revenue Service
Criminal Investigation



Internal Revenue Service
Criminal Investigation

BEC Schemes

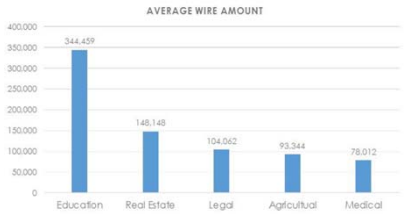
- Financial Payments (Wire Transfers)

➢ A Texas-based university was the victim of a vendor impersonation scheme, where the attacker sent an e-mail providing phony payment instructions. It was later determined that bank wires of $531,667 and $8 million were fraudulent

➢ Two California-based universities suffered BEC attacks, each involving single disbursements of $4.1 million involving fraudulent vendor requests.

Criminal Investigation

Average per Transaction



Criminal Investigation

BEC Trends

- Between June 2015 and December 2016, there was a 2,370% increase in identified exposed losses.
- In 18 months:

Total U.S. victims:	3,044
Total U.S. exposed dollar loss:	$346,160,957

- **TRENDS:** W-2/PII Data Theft
  This scenario of BEC/EAC was identified in 2016 in which a human resource department or counterpart was targeted with a spoofed e-mail seemingly on behalf of a business executive requesting all employee PII or W-2 forms for tax or audit purposes.

Source: FBI Public Service Announcement I-050417-PSA, May 4, 2017

Criminal Investigation

I've Suffered a Data Loss of W-2 Information. Now What?

- Don't Panic
- Act Immediately
  - "Delays in Reporting Favor the ID Thief"
  - "24 Hour Rule"

21

Criminal Investigation

Actions When Compromised

Payroll Related Compromises

- Organizations who actually lost W-2 information via a scam email should e-mail IRS via dataloss@irs.gov and follow instructions.
- Organizations who did not actually lose W-2 information via a scam email should e-mail IRS via phishing@irs.gov and follow instructions.
- Lost Payroll data can impact State Agencies as well. Victims should email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report States Tax Agencies.
- Follow State Reporting Requirements (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)
- Organizations that receive the scam or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.
- Contact Local Police or Other Law Enforcement
- Report Compromise to Federal Trade Commission https://www.identitytheft.gov/

Criminal Investigation

How Can I Help Protect My Company?

- **Do not use the "Reply" option** to respond to any business e-mails asking for PII
- Educate your employees
- Be careful what you post to social media and company websites
- Be suspicious of requests for secrecy or pressure to take action quickly
- Carefully scrutinize all e-mail requests for PII or financial transactions

Criminal Investigation

Victim Experience

- Electronic Return Rejected (Paper Return)
- Verification Letters (5071C, 4883C, and others)
- https://www.irs.gov/individuals/irs-notice-or-letter-for-individual-filers
  - Response to Filed Return
  - Did not File (Paper Return)
- Transcripts
- Receipt of US Treasury Refund Check
- Receipt of Reloadable Prepaid Card
- Receipt of Refund Transfer Company Check

Criminal Investigation

Form 14039 IRS Affidavit

– When in Doubt File (Possibly Changing)
  • Phone reps can't see screening processes
– Always attach to top of Paper Return when required to file via paper.
– Mail paper return to normal address used to file paper returns via IRS
  • https://www.irs.gov/uac/where-to-file-paper-tax-returns-with-or-without-a-payment

Criminal Investigation

Resources

- IRS Security Summit
  https://www.irs.gov/uac/security-summit
- IRS.gov Identity Theft Resources
  https://www.irs.gov/individuals/identity-protection

Criminal Investigation

TAXES + SECURITY "TOGETHER"

- The "Taxes. Security. Together" awareness campaign is an effort to better inform taxpayers, tax preparers and businesses, about the need to protect personal, tax and financial data online and at home.

Criminal Investigation

"Taxes-Security-Together"
https://www.irs.gov/individuals/taxes-security-together

- **Help for Taxpayers**
  - Common sense suggestions can make a big difference. See IRS Security Awareness Tax Tips for a recap of IRS tips to help secure your data.
  - **Also see Publication 4524, Security Awareness for Taxpayers**
- **How Tax Preparers Can Help**
  - Tax preparers are critical and valued partners in the tax administration process, and they have an important role to play in helping prevent identity theft.
  - Tax preparers should review their own security features. We've updated Publication 4557, Safeguarding Taxpayer Data, to help provide an easy check list for you to review and update your security plan.
  - Tax preparers can share Publication 4524 with clients to help raise awareness about important security steps.
- **How Businesses Can Help**
  - Businesses and other organizations also can help combat identity theft by helping educate their employees, clients and customers. Businesses can share Publication 4524 or create their own messages.
- **Other Victim Information** https://www.irs.gov/pub/irs-pdf/p4535.pdf

Criminal Investigation

Atlanta Field Office - ID Theft Coordinator
Georgia & Alabama
(**Local Contact**)

Special Agent Gary Traina (251) 341-5980 (Primary)

Special Agent Mathew Temples (205) 802-4652 (Alternate)

Headquarters – Refund Crimes (National ID Theft Coordinator)

Special Agent Brian Thomas

(267) 941-6373 - Brian.Thomas@ci.irs.gov

Criminal Investigation

Questions?