Article by Jonathan Crowe. He writes about cybersecurity from a practical point of view.

New Alert:

New Surge in Phishing Scams Nets Criminals 120,000 W-2 Forms and Counting

Scammers are posing as high-level executives to get their hands on employee W-2 forms for identity theft and tax fraud purposes.

Tax season is always a busy time for scammers seeking to gain access to sensitive information, but this year attacks are coming earlier and in greater numbers than usual. The uptick has caused the IRS to release an urgent alert warning employers to be on the lookout for what they're referring to as "one of the most dangerous email phishing scams we've seen in a long time."

Here's what to watch out for:

- These emails appear to come from a high-level executive (in many cases, it's the CEO, or, in the case of school districts, the superintendent)
- The sender email addresses are spoofed, so they look legitimate
- The requests are usually framed as "urgent" to prevent prolonged scrutiny
- **Currently, over 100 organizations have been successfully scammed, exposing more than 120,000 employees to tax fraud and identity theft.**

Key details:

- **Type of attack:** Spear-phishing / Business email compromise (BEC)
- **Attack vector:** Email
- **Damage/costs:** Over 100 organizations have already been compromised this year, exposing at least 120,000 employees to tax fraud and identify theft

On January 20, an email from Lynn Jurich, CEO of San Francisco-based solar firm Sunrun, popped up in a payroll department employee's inbox. The CEO was requesting copies of all employee W-2 forms, which were about to be sent out in preparation for tax season.

The employee responded quickly as requested, not realizing the W-2 forms — containing the addresses, social security numbers, and salary information for Sunrun's nearly 4,000 employees — were actually being delivered to a scam artist.

W-2 phishing scams are surging

Tax season is always a busy time for scammers seeking to gain access to sensitive information, but this year attacks are coming earlier and in greater numbers than usual. The uptick has caused the IRS to release an urgent alert warning employers to be on the lookout for what they're referring to as "one of the most dangerous email phishing scams we've seen in a long time."

Here's how it works:

By using email spoofing techniques, criminals are able to draft emails that look as though they are coming directly from a high-level executive at your organization. They send the message to an employee in the payroll department or HR and include a request for a list of the organization's employees along with their W-2 forms.

Their initial goal is to use the W-2 information to file fraudulent tax returns and claim refunds. But not all criminals are stopping there. Once they've found a responsive victim, a portion are also following up with additional email requesting a wire transfer be made to an account they provide.

Also referred to as business email compromise (BEC), these attacks have claimed more than 15,000 victims and cost organizations more than $1 billion over the past three years.

More than 100 organizations have already fallen victim to W-2 phishing scams in 2017

A full list of the organizations that have disclosed data breaches from these attacks publicly can be found at databreaches.net. As of March 14, the tally stands at 106, on well on pace to surpass the 175 incidents reported last year.

The attacks have already resulted in at least 120,000 employees being exposed to fraudulent tax returns and identity theft.

Criminals are targeting a wide variety of organizations

Victims range from healthcare providers to utilities companies to restaurants to even a minor league baseball team, underscoring the IRS warning that all employers should be on alert.

That said, school districts and colleges appear to be disproportionately targeted, making up nearly one third of the victim list so far.

Why victims are falling for these attacks

These unfortunately aren't your average spam emails. Attackers are going to the trouble of researching their targets to identify top executives and payroll/HR employees by name. By spoofing company email addresses they're able to make it appear like their messages are an urgent requests coming straight from the top.

Under those conditions, and with tax season being such a busy time for payroll and HR in particular, it's easy to understand how victims are being fooled.

One of this year's victims, Monarch Beverage, was successfully scammed last year, as well.

Even executives at KnowBe4, a company that provides anti-phishing training and software, were almost fooled last year when they received this email, purportedly from CEO Stu Sjouwerman:

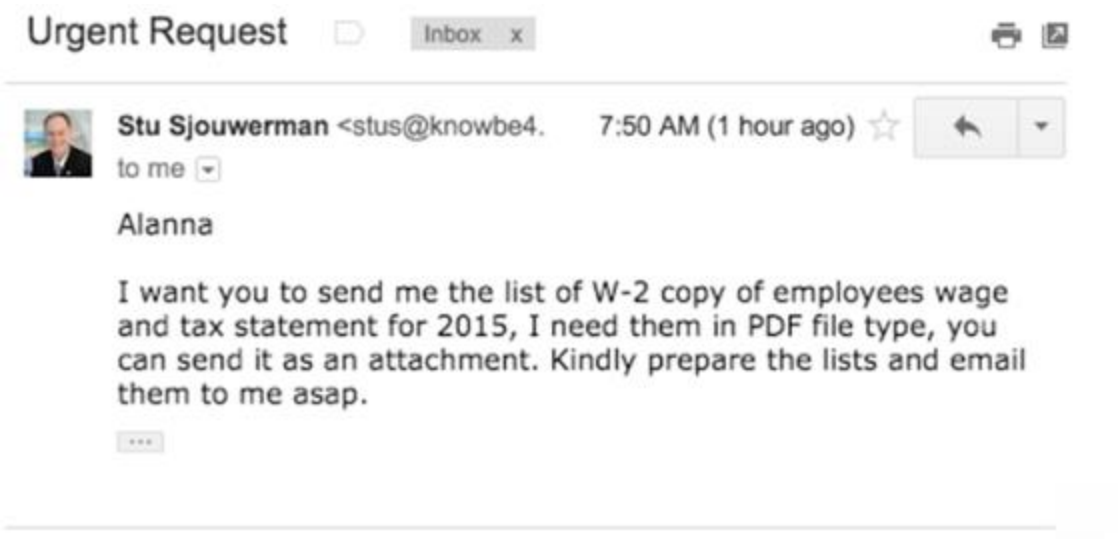

Image source: KrebsonSecurity

Luckily, the recipient had just completed the company's awareness training and decided to confirm the request with Sjouwerman in person.

How to protect your organization from these attacks

Step 1: Make employees aware

Share alerts like this one with all relevant employees, specifically those in payroll or HR departments. Let them know this is an active threat and show them an example email like the one above so they can see just how realistic they are and know what to look for.

Step 2: Implement a policy of confirming sensitive requests

Ideally, you can have systems in place to avoid sending sensitive information like W-2 forms over email altogether. At the very least, though, any request for sensitive information should be confirmed outside of email. You have to assume the executive's account may be compromised, so follow up should happen either over the phone, via Slack or another messaging platform, or face-to-face.

Step 3: Make it more difficult for scammers to guess your company's email structure

Criminals love finding legitimate business email addresses they can use to make these attacks more realistic. Find out how many of your company's email addresses are exposed on the Internet along with where they can be found with KnowBe4's free email exposure tool.

Step 4: Be prepared for attacks that also drop malware

Criminals targeting larger organizations are also taking advantage of this time of year to infect victims with malware.

Researchers recently uncovered a spear-phishing operation targeting employees responsible for submitting financial information to the U.S. Securities and Exchange Commission (SEC).

As with the W-2 scams, attackers spoof email addresses to make it look like their messages are coming from an official domain. But instead of asking for sensitive information, the emails include an updated Form 10-K, an actual form required by the SEC.

Image source: FireEye

When victims download and open the document, however, they are infected with a fileless PowerShell script backdoor.

Because the attack is using a script instead of a file on disk, traditional file-scanning antivirus software won't detect it. By utilizing runtime malware defense, however, Barkly can see when malicious scripts are running and block these attacks before any damage is done.

Have you received a phishing scam email?

The IRS recommends you forward it to phishing@irs.gov and place “W2 Scam” in the subject line. Organizations that receive the scams or fall victim to them are also instructed to file a complaint with the Internet Crime Complaint Center (IC3,) operated by the FBI.

Employees whose W-2 forms have been stolen should review the recommended actions by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft.

Bottom line: Phishing attacks continue to cost companies millions in stolen data, damage, and downtime. To make matters worse, they're also becoming increasingly sophisticated.

Training users to be more aware of the threat that phishing poses, and helping them recognize the tell-tale signs of phishing emails is crucial. As is making sure you have the right security in place to protect your organization if and when a user does get fooled.