American Technology Services

Security Advisory

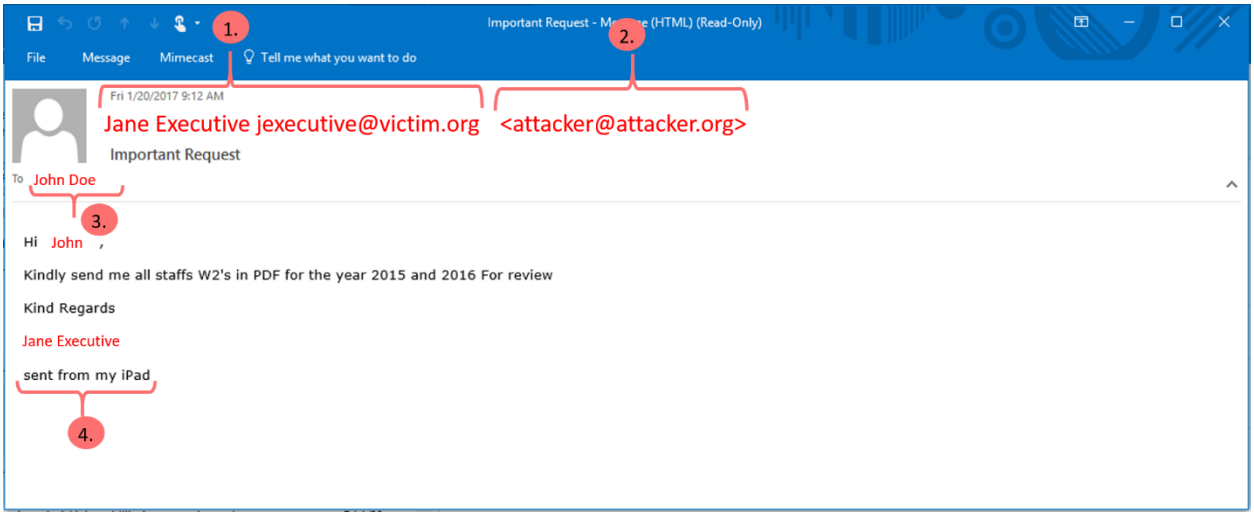
Tax Season Phishing Scheme Targeting Payroll and Human Resources Professionals

Summary

Criminals are targeting payroll and HR professionals in the United States with phishing emails to gain access to employee tax records. Frequently, these targeted emails impersonate an executive within an organization. They may urgently request PDF copies of employee W-2 forms, or other financial records. If given access to this information, criminals will attempt to steal refund checks, or engage in identity theft.

Technical Details

These phishing campaigns are targeted specifically to payroll and HR staff within an organization. The attackers use public information pulled from websites and social networks to understand the roles and relationships between staff within a targeted organization. With this information, an attacker can plausibly impersonate a victim. An example email can be seen below. The red text has been changed to be used as an example.



1) The name and email of an executive was pulled from a publicly accessible source (corporate website, LinkedIn, etc.) to seem legitimate.
2) The reply address, if not internal to your organization, appears in angle brackets. *This is the first hint that this email is not a legitimate request.*
3) The email address of a specific employee is pulled from a publicly accessible source, as above. The attacker either knows this person works in HR/payroll or is sending the email at random in hopes that users will not report the email if it is not relevant to the user.

4) The ‘sent from my iPad’ signature is a clever way to mask the fact that the attacker does not know what the company’s email footer looks like. *This is another red flag.*

When possible, attackers will impersonate (spoof) the email address of the impersonated user in the SMTP “from” field, while setting the “reply-to” field as the attacker email.

```
From: jexecutive@victim.org
To: jdoe@victim.org
Subject: Important Request
Reply-To: attacker@attacker.org
```

With this technique, the email appears to come from a legitimate email address within the organization. However, when the targeted user hits “reply” on their email client, the email is addressed to the attacker email address.

If a victim organization has controls in place to prevent email spoofing, the attacker may simply append the impersonated user’s email address in the “name” portion of the “From:” field to make the email more plausible, as seen in the screenshot above.

```
From: "Jane Executive jexecutive@victim.org" attacker@attacker.org
To: John Doe <jdoe@victim.org>
Subject: Important Request
```

Attackers may also use other techniques for impersonation. If a user feels that a communication is suspicious, they should be cautious.

Guidance

It is important that payroll and HR professionals are aware of this attack and spear phishing attacks in general. Organizations should have clear policies in place that precludes sensitive, private information being sent through email. If a user has misgivings about a particular email, they should reach out to the sender in person, or through a separate channel, like telephone.

In the event that an attacker successfully gains access to private information, management should be notified immediately. Management should assess the situation and proceed with steps to protect any victims. This may involve notifying the IRS and enrolling victims in identity theft protection.

If you suspect that an email is malicious, please forward the email to security@networkats.com so that we may investigate further.

Additional Resources

IRS Alerts Payroll and HR Professionals - https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

IRS Suspicious Emails and Identity Theft - https://www.irs.gov/uac/suspicious-e-mails-and-identity-theft