SIGNATURE BANK®

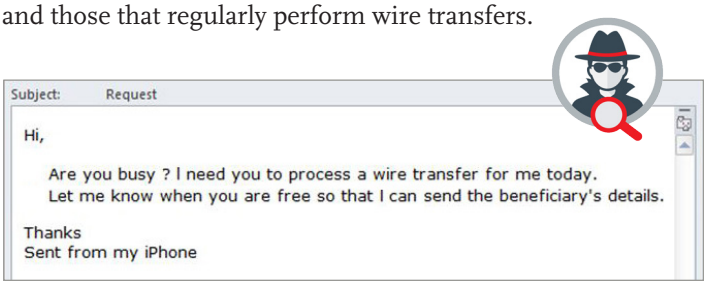
INFORMATION SECURITY NEWS BULLETIN

Winter/Spring 2018

IN THIS ISSUE:

THE MULTI-BILLION-DOLLAR SCAM OF BUSINESS E-MAIL COMPROMISE

By posing as high level executives, phishers have stolen billions of dollars from organizations large and small through Business Email Compromise (BEC) schemes. A BEC scheme typically targets companies working with foreign suppliers and those that regularly perform wire transfers.



HOW IT WORKS:

- **To avoid spam filters, the emails in BEC schemes are not mass-emailed.** Instead, they are sent to only a few employees – usually employees who regularly perform wire transfers, like financial directors or accountants.
- **BEC phishers conduct extensive research to make their emails more believable.** They will try to determine who initiates wires and who requests them. They may even find out your company's financial processes. Then, they wait for the perfect opportunity, like a change in leadership in the finance department or a CEO traveling overseas. BEC phishers typically instruct their targets to act quickly or in confidence when transferring funds. According to the FBI, phishers have stolen over 5.3 billion dollars in their scams.
- **BEC phishing emails often use spoofed email addresses, authentic signatures, and logos to look more credible.** Even if the message looks like it was sent by someone in your organization, it may not be legitimate.
- **BEC attacks often begin with a "Knock-Knock" email that engages the target in conversation.** If the target responds, the attacker continues to manipulate the target until they get them to transfer the requested funds or hand over confidential information.

According to the FBI, phishers have stolen **over 5.3 billion dollars** in their scams.

HOW TO AVOID GETTING HOOKED:

Even if you receive an email that looks legitimate, you should still use caution. Keep these three tips in mind when you receive an email requesting personal information and if anything seems suspicious, don't take the bait. It's best to be certain before initiating a wire transfer.

Even if you receive an email that looks legitimate...
Be skeptical of urgent requests that do not follow typical company procedures and policies.

Even if you receive an email that looks legitimate...
Always verify that the email is from the real sender with a quick phone call.

Even if you receive an email that looks legitimate...
Look at the domain name. Although some phishers spoof company email addresses, other phishers use domains that are slightly different. For example, if the target company's domain was www.example.com, the phishers may register "examp1e.com" or "example.co."

MELTDOWN & SPECTRE: THE NEWEST THREATS TO YOUR DATA

On January 3, 2018, **Meltdown** and **Spectre** were identified by Google as vulnerabilities that allow an attacker to exploit a feature used to optimize performance by a computer's central processing unit (CPU). **Meltdown** and **Spectre** can impact most computing systems and multiple operating systems since they reside within the design of the processor (chip) on which the software is running. If an attacker can execute malicious code that exploits one of these vulnerabilities, the attacker can then be able to read protected memory and potentially gain access to sensitive data.

Exploitation of these vulnerabilities requires an attacker to gain sufficient access to the target machine. Signature Bank already has numerous controls in place to prevent a malicious user from accessing our environment, and we maintain additional layers of control to prevent untrusted or malicious software from executing on our machines. The Bank also maintains many controls to identify any anomalies within the data environment. Finally, **Meltdown** and **Spectre** vulnerabilities are actively monitored and mitigated as vendors supply security patches following Signature Bank's vulnerability management process.

Member FDIC

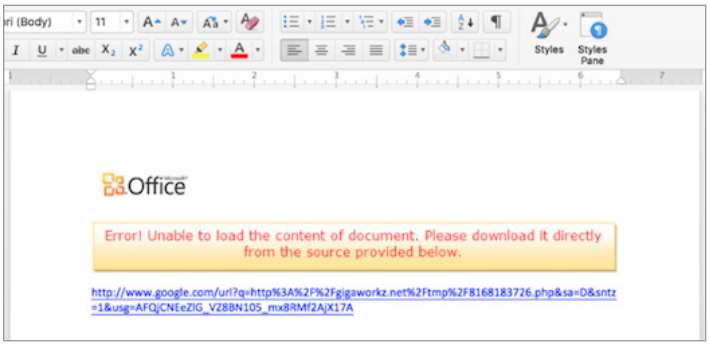
MALICIOUS LINKS IN WORD DOCUMENTS

Attackers are developing innovative techniques to deliver malware that can bypass technical controls like email filters. One recently identified threat uses clickable hyperlinks embedded in Microsoft Office files to deliver their malware.

Using social engineering techniques, such as inquiring about an order or invoice, attackers send emails that contain a Microsoft Word attachment. Unlike more commonly seen malicious Microsoft Office attachments, this attachment doesn't contain macros or exploits. Instead, it contains a malicious link that abuses a Google redirect feature to look legitimate. Clicking the link enables the malware to download and install on your computer.

These emails get past malware and anti-virus scanners because the malware isn't actually there until the target engages with the attachment by clicking the link. Once it is within the infected environment, the Ursnif malware can log keystrokes, collect system information, and can even deliver additional malware.

Below is an example of a seemingly benign Word document with a malware link:



Quick Tips

Keep these tips in mind to help you avoid spear phishing lures:

- Think twice and read emails thoroughly.
- Be on the lookout for vague content.
- Be wary of words like "Caution", "Act Now", and "Warning", which draw your attention and make you act quickly.
- Never download unsolicited attachments.
- Do not download any file attached to email or sent via hyperlink unless you know the sender and were expecting the attachment.
- Always verify that the email is from the real sender before engaging. If in doubt, call or email the sender to confirm it is legitimate.

OFFICE FILES WITH MACROS

Another technique attackers still commonly use to bypass technical controls is to send Office files that contain malicious macros. If you enable macros, the file can download malware, instantly compromising your computer and our network. Remember, never enable macros if prompted by your Office application.

CURRENT EVENTS AND NATURAL DISASTERS

To make their messages more effective, spear phishers reference current events in email narratives. Phishing emails could mention anything from a devastating tsunami to a new mobile app or viral dance video.

Spear phishers do not operate under the same moral guidelines as you do. They will use sensitive topics to elicit a response, playing on your feelings and emotions. After a natural disaster or tragic event, people typically search for more information and seek out opportunities to help. Unfortunately, spear phishers use this to their advantage.

Below are some examples of how spear phishers use current events:

- **Fraudulent Donation Websites:** Attackers exploit good Samaritans who are looking to help. After a natural disaster, heart-wrenching phishing emails and websites from fake charities requesting donations begin to appear. Be careful – phishers can also spoof or hack legitimate charities to enhance their own credibility.
- **SMS Text Scams:** Phishing isn't limited to email messages. Attackers also send text messages encouraging targets to send money to an account or click a link to make a donation.
- **News Hoaxes:** Appealing to emotions of fear and curiosity, phishers use hoaxes such as false rumors about a food recall or a disease outbreak as bait to get targets to click links or download attachments.
- **Viral Trends:** Whether it's the latest mobile app, a cat video, or a record-breaking video game, phishers often include popular trends in email messages. Recently, phishers urged Pokémon Go players to upgrade their accounts and pay a subscription fee.

Quick Tips

Keep these tips in mind to help you spot a phish:

- **Examine hyperlinks.** Hover over a link on a desktop or hold it for several seconds on a mobile device to preview the true destination of a link.
- **Keep your password private.** No reputable company will ask for a password over email.
- **Be wary of fake charity sites.** Before making a donation, make sure that the site is legitimate, and uses encryption (https).
- **Think twice.** Attackers will use emotional appeals in their emails, so stay calm and look closely at the email content before responding.