THE DIR CYBERSECURITY INSIGHT

JANUARY FY2018 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

'Tis the [*tax*] season to be leery!

As the new year begins, citizens nationwide will be eagerly awaiting their tax forms to arrive, as the commencement of the tax season is upon us. This is an especially profitable time for cyber-criminals. Phone scams, email phishing, wire fraud, and evil twins are just a few of the tricks some of us may see while we prepare to file. However, with a little knowledge and proper vigilance, we may be able to avoid the pitfalls and file our returns with confidence.

Phone scams, or "robo-calls," are an impersonation tactic used by cyber-criminals to present potential targets with a situation of severe importance. They use automated callback requests to inform taxpayers that they must call back, immediately, to settle a matter with their "tax bill." These callbacks also make note that it is the last attempt to contact the taxpayer, before legal actions follow. This creates a sense of urgency for the intended target to resolve the matter quickly. When the target does call back, they are often solicited for payment information and verification of W-2 and other tax information over the phone. However, there are several telltale signs that you are a victim of a robo-call scam. The IRS will **never**:

- Call to demand payment over the phone, nor will they call about owed taxes without first informing the taxpayer, through mail, that they have a bill.
- Threaten to have local authorities brought to a taxpayer's home to immediately arrest them for non-payment.
- Demand payment for taxes without giving the taxpayer the opportunity to appeal the amount owed.
- Require that a specific payment method be used to settle a tax bill, such as iTunes or other gift cards, wire transfers, or prepaid debt cards.
- Ask for debit or credit card information over the phone.

If any of these situations happen to you, the IRS suggests that you:

- Hang up immediately.
- Contact TIGTA (U.S. Treasury Inspector General for Tax Administration) to report the call.
- Report the call to the FTC (Federal Trade Commission)
- Call the IRS directly @ 800-829-1040, if you think you owe any taxes.

CONTENTS

Monthly Article

'Tis the [tax] season to be leery!.....**P.1-3**

Updates

Events.....**P.1-2**

Meltdown & Spectre: Adding froth to an existing wave of exploits.....**P.3**

Time to prepare for interns!.....**P.4**

EVENTS

- **1/23/2018 – Meltdown/Spectre Issue Discussion with Intel Webinar @ 1:00PM CST**
- 1/25/2018 – Dark Reading Webinar. Becoming a Threat Hunter in Your Enterprise @ 12:00PM CST. Register here.
- **1/25/2018 – Save the Date! MS-ISAC Hot Topics Webinar Initiatives @ 1:00PM CST**
- 2/1/2018 – GDPR – What You Don't Know Can Hurt You @ 11:00PM CST. Register here.
- 2/6/2018 – Security Intelligence Webinar. Fraud Protection: The Rise in Phishing Attacks and How to Mitigate Your Risk @ 11:00AM CST. Register here.
- **2/8/2018 – DIR Monthly Security Meeting @ 9:00 AM CST**
- 2/12/2018 – Security Intelligence Webinar. Threat Hunting on the Front Line @ 11:00AM CST. Register here.

EVENTS cont.

- 2/15/2018 – Infosecurity Magazine. Beyond the Hype of Meltdown & Spectre: How to Patch, Fix or Replace Flaws & Bugs @ 10:00AM CST. Register here.
- 2/15/2018 – Dark Reading Crash Course. The Real Risks of Mobile Technology In the Enterprise @ 12:PM CST. Register here.
- 2/22/2018 – Dark Reading Crash Course. Insider Threats and Data Leaks: What You Don't Know CAN Hurt You @ 12:00PM CST. Register here.

Email phishing, or the W-2 phishing attack, is another tool in a cyber-criminal's arsenal during tax season. It gets its name from phishers strategically targeting (or *spear phishing*) employees in corporate HR and Payroll departments with urgent emails, seemingly from supervisors or executives, requesting employee names and W-2 forms. Once a W-2 phishing attack is successful, fraudulent tax return filings are sure to follow. Here are some suggestions on how to defend against a W-2 phishing attack.

- Be suspicious of any email from unknown parties and never click on any links provided.
- Train employees on how to spot phishing email red flags such as unknown senders, odd or misspelled titles, poor grammar, and abnormal, out-of-the-ordinary, requests.
- Employees should communicate quickly with the proper staff about a potential W-2 scam – usually your organization's IT department.
- Notify the authorities if you feel like you may be the target of a phishing scam. Again, the TIGTA, FTC, and even the FBI's Internet Crime Complaint Center (IC3).

Wire transfer is the newest twist to follow the W-2 phishing scam, mentioned above. Not only do phishers target corporate HR and Payroll employees, they now follow up their W-2 email requests with instructions to send a wire transfer to a specific account. Though the wire transfer scam is not tax-related, its implementation with the W-2 phishing scam has been successful in causing the loss of millions of corporate dollars, annually. To combat this scamming method, follow the safety recommendations mentioned in the W-2 email phishing section of this article.

Another scam mentioned is the use of an **evil twin**. As we prepare to file our returns in the coming months, most of us will rely on the internet (and our cloud-based, tax preparation software) to get it done. And with the prominence of Wi-Fi as a transfer medium, one problem we face is the susceptibility of an evil twin attack. Evil twins are just access points that have been purposely setup by hackers to mimic legitimate access points in an attempt to fool users into connecting to it, where the hacker can then view and capture user network traffic. This scam is a little harder to detect, so vigilance is key. Here are some helpful tips:

- **Avoid using auto-connect in unfamiliar surroundings.** Most places (like hotels, institutes, etc.) will have both the SSID name and a temporary password to provide you, should you need to use Wi-Fi.
- **If you're device is constantly dropping then re-adding your connection, be suspicious.** It could be interference or your proximity to the access point. However, if you're close enough to the AC and you're still having issues maintaining a connection, it's cause for concern.
- **Be cautious of free rides.** There are plenty of free Wi-Fi hotspots these days. However, if you're using a known, paid hotspot that doesn't prompt you for login creds, it's best to stay away.
- **Look for certificate warnings.** Web servers use secured certificates to establish SSL transmissions for sensitive data. If you visit a known SSL site (like your bank's webpage) and the URL is not resolving to HTTPS or you get a certificate warning, don't proceed.
- **Out-of-Service VPNs.** If you absolutely need to transmit/view sensitive data, then use a VPN. They're a great way to defeat man-in-the-middle attacks for which evil twins are notorious. If a public Wi-Fi doesn't permit your VPN software to establish a secured connection because it's out-of-service, then that could signify an evil twin in use. Don't take a chance by surpassing the use of a VPN connection for convenience' sake.

Finally, don't let yourself become a victim this tax season. KrebsOnSecurity suggest the following steps to lessen your chances of becoming a victim of tax fraud:

- **File before the fraudsters do it for you**. Filing early is a good deterrent. Why would a scammer waste their time and effort trying to convince the IRS they're someone else, when there are so many potential targets who have yet to file their return?

- **Get on a schedule to request a free copy of your credit report**. It's usually a good habit to request your credit report every three to four months. Look it over, carefully, and dispute any discrepancies or suspicious activities. Credit monitoring services are good for this type of prevention.
- **File form 14039 and request an IP PIN from the government**. This is a great option for those who feel that they are a victim of identity fraud.
- **Consider placing a "security freeze" on one's credit files with the major credit bureaus**. This may not help to keep scammers from filing a fraudulent tax return, but it does keep them from obtaining your IP PIN.
- **Monitor, then freeze**. Take advantage of any free credit monitoring service(s) available to you, and then freeze your credit file with the three (or four) major credit bureaus.

OCISO Updates

Meltdown & Spectre: Adding froth to an existing wave of exploits

Hardware based exploits are not a new phenomenon. The vulnerabilities exploited by Meltdown and Spectre were first warned about in a 1995 analysis, "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems" (Sibert, Porras, and Lindell). Unfortunately, these vulnerabilities take advantage of some of the basic architecture of modern CPUs, and show no sign of slowing down. Replacing your hardware will not mitigate all the threats, and is not always feasible (there is no hardware replacement that alleviates Spectre). Intel's Active Management Technology was found to have a flaw a week after Meltdown and Spectre were confirmed that would let a user bypass locks.

In the past few years, exploits have been found on variety of hardware platforms, including multiple attacks on Intel's Management Engine, a subsystem build into most Intel CPUs to aid system administrators. In February of 2017, AMD CPUs were found to be vulnerable to side-channel attacks on MMU operations. 2015's Rowhammer attack could remotely overload the capacitors in modern DRAM, resulting in the ability to read memory outside of the program's sandbox.

Then there is the Internet of Things (IoT). Attacks on IoT devices, which rely heavily on embedded software, are also persistent, and some are essentially unfixable. End users do not routinely think to patch their smart devices, instead opting to let whatever automatic patching that was built into their device handle it. Some smart devices do not even automatic patching. Osram smart bulbs were found to have vulnerabilities in 2016, not all of which will ever be patched. How many end users think to check if their smart light bulbs offer patches? IoT devices that are past their end of support will also stay online until the IoT device breaks and the owner replaces it with a new model, which can be years, if not decades later. An LED has a life expectancy of up to 50,000 hours. If used 10 hours a day, that smart bulb will stay online for 13.7 years.

Nobody heeded the 1995 warning about cash registers. In 2015, multi-billion dollar corporations missed the warnings on their compromised cash registers. As commercially available products continue to evolve in scope and integration with public and private systems, how many more will neglect to check their light bulbs? This is a huge concern for the state as technology integrates even more into our daily lives and the everyday objects we take for granted.

As with any information security threat, we do our best to make sure the systems are secure and threats mitigated. But as the old English proverb goes, "Where there's a will, there's a way." These hardware based attacks show that even when we think we know which direction new attacks may arrive from, there is always another way. Information security specialists and executives would be wise to prepare for the day a malicious actor finds their way into a system, and have incident response plans prepared.

Time to prepare for interns!

It may not seem like it with the cold weather outside, but spring is just around the corner! That means college students looking for summer internships are not far behind. This is an excellent opportunity to polish your job posting criteria and work with your human resources divisions to snag an aspiring technologist for the summer.

Working with interns is a great learning opportunity, not only for the students, but for those taking on the interns. It allows us to show interns the inner workings of information security at the state, while the interns bring in new and unique perspectives that we may have overlooked during our busy days. Interns are also more likely to apply for and accept offers of employment from employers they have worked with. A 2015 survey by the Nation Association of Colleges and Employers found that up to 90% of interns accepted a job offer from an employer they have previously interned for. Interns will also relay their experiences to their peers, potentially expanding your candidate pools. Information Security is a field where there are more opportunities than employees looking for work; offing an internship may be the crucial difference in attracting qualified candidates.

Some tips if you are planning on bringing in some interns this summer:

- Prepare an orientation. The new workplace will be confusing and may even be a little overwhelming for someone with very little work experience.
- Have work planned that they can learn from. Don't expect them to just sit with your existing staff and learn via osmosis, give them something to do! This is a great learning opportunity for them, help them take advantage of it.
- Talk to them. If they seem disengaged or overwhelmed, a simple chat with them can usually resolve whatever underlying issue exists. Feedback is also important to keep your interns engaged and developing.