Many thanks to Fred Gutierrez and Geri Revay for their contributions to this blog.

FortiGuard Labs Research

Affected Platforms: Windows Impacted Users: Windows users Impact: Compromised machines are under the control of the threat actor. Stolen personally identifiable information (PII), credential theft, monetary loss, etc. Severity Level: Medium

Malicious email and phishing scams are usually topical and follow a pattern of current events. They are usually crafted around calendar and/or trending issues as attackers realize that victims are interested in all things relevant to the moment. Threat actors are aware that not all recipients will bite, but some will, hence the origination of the term "phishing."

Threat actors often put in the least amount of work possible for a maximum return, sending out phishing emails to thousands of targets. Even if less than one percent of victims respond, the return on investment is still significant due to the gain of personally identifiable information (PII) and/or establishing a foothold within an organization using stolen credentials, malware, or other means.

This blog highlights some examples we've encountered that may help users better spot suspicious emails. Recent examples observed by FortiGuard Labs include emails related to tax season and the Ukrainian conflict, which reflect the timeliness of current and newsworthy events at the time of writing.

Tax Season Scams

Tax season comes around annually, like other seasonal events or holidays. Targeting calendar-based events enables threat actors to prepare ahead of time and have a new selection of targets on rotation.

The following set of examples highlights two IRS/tax-themed scams. The first is a malicious email pretending to originate from the U.S. Internal Revenue Service (IRS) containing a maliciously crafted Microsoft Excel file to deliver malware (Emotet). The second is a phishing scam that asks a recipient to send personally identifiable information (PII) via written correspondence to a phone number.

IRS-themed email delivering Emotet

This attack starts with an IRS impersonation email that contains a ZIP attachment called "W-9 form.zip". The email is sent to the target, and a password is provided within the body of the email for convenient extraction. The zipped attachment contains a file, "W-9 form.XLM." The XLM extension is simply an Excel file that contains Excel 4.0 macros:

Figure 1. Fake IRS email with malicious attachment

For those not familiar with Form W-9 (Request for Taxpayer Identification Number and Certification), it is used by U.S. individuals to provide a correct taxpayer identification number (TIN) to payers (or brokers) who are required to file information returns with the IRS. Red flags that this is a phishing scam include the non-capitalization of "assistant" and the incorrect usage of "Treasure" instead of "Treasury" in the signature body. It should also be noted that the IRS does not communicate with U.S. taxpayers via email and instead uses the traditional postal service for all communications.

Analysis

Upon observation, and in a similar fashion to our recent Emotet blog, the XLM file asks the user to enable macros upon opening the file.

The XLM file contains the following obfuscated Excel 4.0 macro:

Figure 2. Screenshot of Excel 4.0 macro

The document contains five hidden sheets: "Vfrbuk1", "Sheet", "Lefasbor1", "EFALGV", "Je1" and "Je2". Sheet EFALGV contains the main code, which uses the other sheets to compile commands. It does this without user interaction, performing its behind-the-scenes magic to download a copy of Emotet from multiple remote locations:

Figure 3. Hidden Sheets

Another variation observed was sent to a State Attorney General's office in the United States. The "From" address is clearly seen in the email. It was sent from an automotive tire shop located in Japan, which is most likely compromised and serves as an open mail relay:

Figure 4. Variation of the same scam

Microsoft takes action

Microsoft announced in January 2022 that Excel 4.0 macros are disabled by default starting in Excel (Build 16.0.14427.10000). The move came as no surprise because the feature is continuously abused by threat actors. Other welcome news from Microsoft is the restricted usage of macros in Access, Excel, PowerPoint, Visio, and Word by default starting in April 2022 via the disablement of VBA macros (also abused by Emotet). Based on the examples shown above, we can see this did not deter the attacker one bit from abusing Excel 4.0 macros.

Also, administrators are able to control the usage of Excel 4.0 macros via group policy settings, as well as cloud and ADMX policies. This feature was introduced in July 2021. For more details, please visit Microsoft's tech community page - "Restrict usage of Excel 4.0 (XLM) macros with new macro settings control".

It's important to note that these potential victims were not targeted. Emotet utilizes what is colloquially known in the industry as a "spray and pray" tactic to spread via malicious email campaigns. Emotet is known to have delivered other malware variants in the past, with the most disruptive being ransomware. Some ransomware as a service (RaaS) groups have specific policies to not deploy ransomware to government sectors, defense industry, and other critical infrastructures (hospitals, etc.). However, actual attacks are often carried out by RaaS affiliates who may or may not abide by the policy set by RaaS groups.

Request to fill and send a W-8 form via a fax number

A different scam recently observed is an email with the subject line of: "NEW YEAR-NON-RESIDENT ALIEN TAX EXEMPTION UPDATE." This example contains an attachment, titled "W8-ENFORM.PDF." While not malicious, this PDF file is essentially a photocopy of the IRS W-8 form. It is simply the W8 form from the IRS with an appended number added by the bad actors at the end of the document.

Red flags within the body of the email are the improper usage of grammar, typos, and punctuation:

Figure 5. W-8 themed tax scam

This scam uses social engineering verbiage to target nonresident aliens of the United States based on "official" records discovery. However, in a weird miscue, the email contains a contradictory statement:

"if you are a USA citizen and resident, this W8BEN-FORM is not meant for you…"

The email continues with instructions to reply back and to state on the attached form that the recipient is, indeed, a U.S. citizen/resident. After this step is completed, the bad actor provides a different form to complete.

Figure 6. W-8 Form

Figure 7. W8 Form with added phone number to document

Once this form is filled out, all PII included on this form appears to be sent to an 806 phone number, which is the area code for the state of Texas. As of the time of writing this number has an active fax service, which most likely is internet-based and can receive the content and distribute as an attachment to the malicious actor anywhere in the world. It is possible, if there are a lot of respondents, they could be using OCR (Optical Image Recognition) image technology to store victim data in a database for later use.

It is important to again note that the IRS does not handle any official correspondence via email. Official W-9 forms are available on the IRS Web page. Official W8 forms can be found here.

Refugee war scams

Spam commonly uses techniques such as current events (sports, tax season), using money as an incentive to click, playing on our natural greed (tax refunds, free money) and use the threat of running out of time to get us to take immediate action.

In the example below, all three techniques are employed, albeit in a more unusual way — with an impassioned plea give money to others with the subject line "URGENT RESPONSE REQUIRED! (UKRAINE)."

While the email does not contain a malicious attachment or link, the scammer is asking for a response. This is likely to contain a follow up message for further information. Perhaps the threat actor may engage in dialog with the victim and will ask the victim to send payment via wire transfer, third-party payment processors (such as Venmo, Zelle, etc.), or via cryptocurrency. The email address of the sender uses a gmail.com email address to likely evade spam filters.

Figure 8. Email Screenshot

Bitcoin Variation

The screenshot below highlights a brazenly opportunistic scam with the subject line "URGENT DONATION RESPONSE FOR WAR REFUGEE CAMP IN UKRAINE." It purports to originate from a trusted organization, The United Nations. Red flags are the forged email address of the UN High Commissioner "info@seca[.]cam" in the "From" line, as well as some grammatical and punctuation errors. Another red flag is that the seca[.]cam domain was only registered a few weeks ago, on February 23, 2022.

Figure 9. Refugee scam soliciting for Bitcoin

Checking the Bitcoin wallet address, we can see that this is an active wallet that had its first transaction on September 29th, 2021. Since the first discovery of the campaign on the 7th of March, several transactions have been made to this wallet. Its current value at time of writing is $46.82 USD, with total transactions valued at $712.79 USD. Assuming that this wallet was used for malicious purposes, it appears that various campaigns have netted the threat actor a modest profit. However, it can also be safely surmised that this might not be the scammers only wallet. As with the IRS, it is also important to mention is that the U.N. will never send unsolicited emails for donations. For further details, please reference the U.N. Fraud Alert page.

Figure 10. Bitcoin wallet details

Conclusion

Emotet and the War in Ukraine

With the current tragic situation in Ukraine unfolding, internal chatter within ransomware groups have surfaced. Some ransomware groups side with Russia and other groups side with the West. A well-known RaaS group (which used Emotet)——that we will not publicize for obvious reasons——has made a very strong statement that any attacks directed towards Russia will be met with a retaliatory act towards the West.

As the situation is fluid, and with potentially compromised government sectors likely being infected or targeted with ransomware at this very moment either for monetary or political reasons, this threat is not out of the question. The point is that important sectors such as government agencies are no longer exempt from attacks, especially from Emotet threat actors, regardless of bias or opinion.

Phishing scams aren't going anywhere. They are a part of the threat landscape and will likely always be a component of an attackers' arsenal. This is because the return on investment for an attacker is very high. A crafted email containing specific language designed to trick users into opening an attachment, following a link, responding with confidential or sensitive information, etc. will always work on a percentage of targets. This is because of the one major weakness security software cannot address: the human element.

Training programs constantly remind and teach users how to spot malicious email/phishing/spearphishing scams for a good reason. Out of thousands of recipients, it only takes a few to respond to make it all worthwhile to an attacker. And when the right person falls prey it can unleash a trove of information to the attacker that can be exploited for various purposes. Although such scams are well known and publicized, they are still pervasive for one simple fact——they work and will continue to work for the foreseeable future.

Things to Consider:

1. Think twice when enabling macros (they are disabled by default for good reason) especially in tax form XLM files.
2. The IRS will never send correspondence via email (including attachments) without first obtaining your consent. IGNORE all unsolicited emails purporting to be from the IRS as they are not real.
3. The IRS has a dedicated webpage to report scams along with an FAQ page - Report Phishing | Internal Revenue Service (irs.gov) (Note: Scams mentioned in this blog have been sent to the IRS before publication)
4. The UN will also never send unsolicited emails for donations. According to the UN website, "The United Nations strongly recommends that the recipients of solicitations, such as those described above exercise extreme caution in respect of such solicitations" Please see the U.N Fraud Alert page for further details. IGNORE all unsolicited emails purporting to be from the UN as they are not real. (Note: Scams mentioned in this blog have been sent to the UN before publication)
5. Unsolicited emails asking for donations of any kind via email (especially via cryptocurrency) is a red flag regardless of cause.
6. Responding to any email (even if it doesn't contain a link or malicious attachment) from an untrusted sender will validate your email address to threat actors, either adding you to spam lists or subjecting to future attacks and scams.

Remember:

Threat actors are playing the numbers game. If they spam out 1,000 emails at a very minimal cost, and 10 people bite giving them valuable data, then the effort spent was well worth the return on investment.

Fortinet Coverage

Fortinet customers are protected from this campaign by FortiGuard Web Filtering, AntiVirus, FortiMail, FortiClient, FortiEDR, and CDR (content disarm and reconstruction) services, as follows:

The malicious macro inside the Excel sample (Emotet) can be disarmed by the FortiGuard CDR (content disarm and reconstruction) service.

FortiEDR detects both the Excel file and Emotet-related files as malicious based on behavior.

All relevant URIs to campaigns mentioned in the blog are blocked by the FortiGuard Web Filtering service.

The malicious Excel sample and associated downloaded files are detected as:

“XML/Dloader.802!tr, “W32/Emotet.C!tr", “W32/Emotet.CV!tr”, and “W32/Emotet.1150!tr” are blocked by the FortiGuard AntiVirus service.

The IRS phishing email targeting nonresident aliens is detected as:

IRS PDF/Fraud.10F1!phish

Ukraine Related Scams

URGENT RESPONSE REQUIRED! (UKRAINE) campaign

ecres231[.]servconfig[.]com

Is classified as a spam server and is blocked by our Web Filtering client.

URGENT DONATION RESPONSE FOR WAR REFUGEE CAMP IN UKRAINE campaign

seca[.]cam

is classified as a spam sender and is blocked by the Web Filtering client.

Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

In addition to these protections, we suggest that organizations also have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats that is designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

Indicators of Compromise

URLs (Emotet)

hxxp://piajimenez.com/Fox-C/dS4nv3spYd0DZsnwLqov/ hxxps://getlivetext.com/Pectinacea/AL5FVpjleCW/ hxxp://inopra.com/wp-includes/3zGnQGNCvIKuvrO7T/ hxxp://biomedicalpharmaegypt.com/sapbush/BKEaVq1zoyJssmUoe/ hxxp://janshabd.com/Zgye2/ hxxps://justforanime.com/stratose/PonwPXCl/

Sample SHA-256 involved in the attack: (Emotet)

e5a1123894f01197d793d1fe6fa0ecc2bf6167a26ec56bab8c9db70a775ec6bc 6fa0c6858688e1c0cbc9072c9d371f2183e0bf0c30a1187453cbbe080e0167ca
06ac89a138858ed0f5eb5a30a43941b67697f8a3b47106170d879f3d51bc0e8d
9f2686b83570b7940c577013d522b96ba19e148dac33b6983267470be6a6064b
4c0ae17817c218c4b7973670f0458978efac4e6a67d1ec3abfb11ab587560d49

0758b3cde229886a039202120cda4485426c56eed3596be75fbce0d38986bf03 9a40dfc271fa3adf20e76cb6f7a27036c77adbe9882a8ef73bc977a0ea9c36ff

feec12c64c8bf47ae20dc197ac1c5f0c087c89e9a72a054ba82a20bf6266b447 50351e6d541f57fccb0261514acb43cb905e4f6dde7e8716ce1b82df7d3c4867

91795e5b49eabd94c9d8b70067f68f45f9bf56e36ec9d3529576e13569074113

8ac29489154a4c39e74070063ce71bfada00cd9883466c1e28cd1e66cab1b56c

7d4897d33893f0835a982424af2f3eb77463dad1ef96fcb4021eaf15fd28c9e9 64d3d585c41577b0cfa2f9c63035a95ac785f9b5aeefeaba2490110c84aa7d00

809c990279928640c23ecc27d134f73967c7ec7269e90bb8d916f9e35b69654f

7536ed21e14ee026424d9c07edbcecb59706129d31f6be4e8788edd904df6a20

8f05a6ee54b89de50e84fcd9db9191f3dd80c701a436ab4c81a1309b2d649368

3a1f0cfbea0de5acca77595a6a5384c31859c255defa12449861e6755b41aa20

6516d944f93186e7d422e7b93a476d4b04db0ed279ba93c4854d42387347d012

9ca7f4e809a8d381fa0bc8e02627d597add2de4c5d57632cae422c59a1e971e2

Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.