October 2014
Feature Article: Irish Tax Refund Phishing Scam

ENJOY SAFER TECHNOLOGY™

Table of Contents

Irish Tax Refund Phishing Scam

David Harley, ESET Senior Research Fellow
Urban Schrott, ESET Ireland

Where there's a tax return deadline, there's a scam, often a tax refund phish. ESET Ireland's Urban Schrott has seen and reported many such in recent years, and this one is worth a closer look, being notably elaborate and sophisticated. David Harley adds a few further thoughts.

ESET Ireland has seen a steady increase of Revenue-related phishing scams in Irish mailboxes over time. This cleverly constructed example appears to come from an email address *refund@revenue.ie*, which appears legitimate but is faked and lures potential victims with the following text:

> *Dear Applicant,*
>
> *After the last annual calculations of your fiscal activity we have determined that you are eligible to receive tax refund.*
> *To access your tax refund, please download and fill the Tax Refund Form attached to this email – open it in a browser (recommended mozilla firefox or google chrome)*
>
> *Please submit the tax refund request and allow us 2-5 days in order to process it.*
> *A refund can be delayed for a variety of reasons. As example, for submitting invalid records or applying over the deadline.*
>
> *IMPORTANT:*
> *If you find this email in Bulk, Spam or Junk please move it to your inbox as not to jeopardize the future our communication with you. It is essential to receive all emails from us to be in touch.*
>
> *Sincerely*
> *Anthony Poole.*
> *Irish Revenue Credit Office*
> *TAX REFUND ID: IE461708-REVENUE*
>
>

There are some interesting features here:

- While the English isn't perfect here, sounding slightly foreign and ungrammatical, it's certainly better than many scam mails. Bad English is usually a red flag but 'slightly off' English is harder to spot.
- Recommending that the reader use Firefox or Chrome has no real utility and certainly doesn't add any security in this instance, but may help to trick those who believe that Internet Explorer is less secure. (A claim often made, but harder to demonstrate when comparing like to like.)
- There is the usual request to allow processing time. This is perfectly normal, of course, in financial transactions, but in this case it works to the advantage of the scammer, since it gives him plenty of time to plunder the victim's account.

- We often point out that the absence of any personalization is a huge red flag. In this case, the scammer has taken that into account by including a 'TAX REFUND ID'. However, there is no real personalization here: it's just an arbitrary number which is probably the same for every recipient of the message, and doesn't prove that the sender has any real knowledge of the recipient. Clearly, he has no such knowledge, since it's addressed to 'Dear Applicant.'

Below that it offers a form to be filled with ALL personal and banking details saying *"Please enter your Personal Information and a valid Credit / Debit Card where you want the refund to be made."*

And just what is that information?

- Email Address
- First Name and Surname
- Date of Birth
- Address
- Account Number
- Sort Code
- Credit Card Type [VISA is default]
- Credit Card Number
- Expiry Date
- CVV/CSC
- 3D Secure Password
- Password Question [default: What is your mother's maiden name?]
- Password Answer

Whoa! If phishers use checklists, there can't be many boxes left unchecked on that one.

Needless to say, things will happen to victim's accounts if they do this, but "receiving a refund" will NOT be one of those things.

Irish Revenue warns of these scams on their website: *"If you receive an email purporting to be from Revenue and you suspect it to be fraudulent or a scam please forward it to webmaster@revenue.ie. Alternatively, you can contact your tax district to check the status of any refund that may be due."* They also point out that ***"Revenue will never send emails which require customers to send personal information via email or pop-up windows."*** This is an important point, and shows that at least some organizations take some notice of the advice the security industry never tires of giving.

- Email (and other messaging services) can be spoofed and/or hijacked. Don't assume a message is genuine just because it seems to come from someone or an organization that you know.

- If asked to open an attachment or a link embedded in a message, don't unless you're able to verify independently that the message (and link) are genuine.

- If there is no genuine personalization (a clear and verifiable indication that the sender and the recipient have a genuine business relationship using information that could not be simply guessed from knowledge of the recipient's email address), assume that it's a scam.

- In this case, it's manifestly improbable that the Revenue office would make a tax refund at all via the lucky recipient's credit card. Unless, equally improbably, the taxpayer was in the habit of paying his income tax by credit card. (For most of us, that would require a heck of a credit limit!)

- In this case, if the victim was to fill in that form, the scammer would already have more than enough information to pay the 'refund' direct to his bank account, if it was a genuine offer. As it is, the sheer volume of information required is in itself a good indicator of malice aforethought. Filling in that amount of data offers the scanner not only sensitive financial data but enough information for some heavy ID theft.

ESET Corporate News

ESET Launches Its Flagship Products: ESET NOD32 Antivirus 8 and ESET Smart Security 8

ESET announced the latest versions of its flagship security software products: ESET NOD32® Antivirus 8 and ESET Smart Security® 8. The latest line-up includes Botnet Protection and Enhanced Exploit Blocker that protects against exploits and offer anti-phishing and social media scanning capabilities. *"These new features provide users of ESET NOD32® Antivirus 8 and ESET Smart Security® 8 enhanced level of security, whether they are checking email, surfing the web or checking their bank balance online," said Ignacio Sbampato, Chief Sales and Marketing Officer at ESET. "Combined with our award-winning anti-malware protection, we are confident these added features will bring tremendous value to our customers."*

Deloitte Technology Fast 50: ESET Ranks Among Fastest Growing Big Tech Companies in Central Europe for More than a Decade

ESET has ranked among the fastest growing large tech companies in the region for 12th time in 2014, finds Deloitte in its annual Technology Fast 50 CE report. With a 274% growth over the past five years, ESET has been listed among the elite "Big 5" group which recognizes those companies which consistently achieve fast growth rates, but are too big to compete for the top spots in the main ranking.

"These companies are still growing at a rapid pace for their size," says Deloitte about its "Big Five" list. Among the criteria for being listed in the prestigious ranking, the company must have revenues more than 25 million and be in business for a minimum of five years. ESET has easily met these criteria for many years.

ESET to host AVAR 2014 in Sydney, Australia

ESET is the official organizer of the 17th Association of Anti-Virus Asia Researchers International Conference (AVAR) 2014, the largest Asia Pacific conference on anti-malware, to be held in Sydney, Australia from 12 to 14 November 2014.

AVAR2014 is a great opportunity for anyone interested in safe computing and Internet security. Experts on IT security from around the world will present their findings on the hottest topics in the anti-malware industry. The line-up of experts and exceptional speakers opens with Graham Cluley, a well-regarded security thought leader and ESET WeLiveSecurity.com blogger, who will present his keynote 'What 20 years working in the Anti-Virus industry taught me'. ESET invites all IT security experts to meet at the most awaited IT security gathering of the year and the biggest anti-malware conference in the Asia-Pacific region.

The Top Ten Threats

1. HTML/Refresh

Previous Ranking: 1
Percentage Detected: 3.66%

HTML/Refresh is a Trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 2.24%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address from which it tries to download several files. The files are then executed and HTTP protocol is used for comunication with the C&C to receive new commands. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. JS/Kryptik.I

Previous Ranking: 3
Percentage Detected: 2.17%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

4. Win32/RiskWare.NetFilter

Previous Ranking: 5
Percentage Detected: 1.49%

Win32/RiskWare.NetFilter is an application that includes malicious code designed to force infected computers to allow an attacker to remotely connect to the infected system and control it, in order to steal sensitive information or install other malware.

5. Win32/Adware.MultiPlug

Previous Ranking: 4
Percentage Detected: 1.47%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it's present into the users system might cause applications to displays advertising popup windows during internet browsing.

6. HTML/ScrInject

Previous Ranking: n/a
Percentage Detected: 1.45%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

7. LNK/Agent.AK

Previous Ranking: 6
Percentage Detected: 1.40%

LNK/Agent.AK is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat. This vulnerability became known at the time of discovery of Stuxnet, as it was one of four vulnerabilities that were executed by Stuxnet variants.

8. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.34%

Sality is a polymorphic file infector. When executed it starts a service and created/deleted registry keys related to security applications activite in the system and to ensure that the malicious process restarts at each reboot of operating system.
It modifies EXE and SCR files and disables services and processes implemented by and associated with security solutions.
More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. HTML/Iframe

Previous Ranking: 8
Percentage Detected: 1.24%

Type of infiltration: Virus

HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

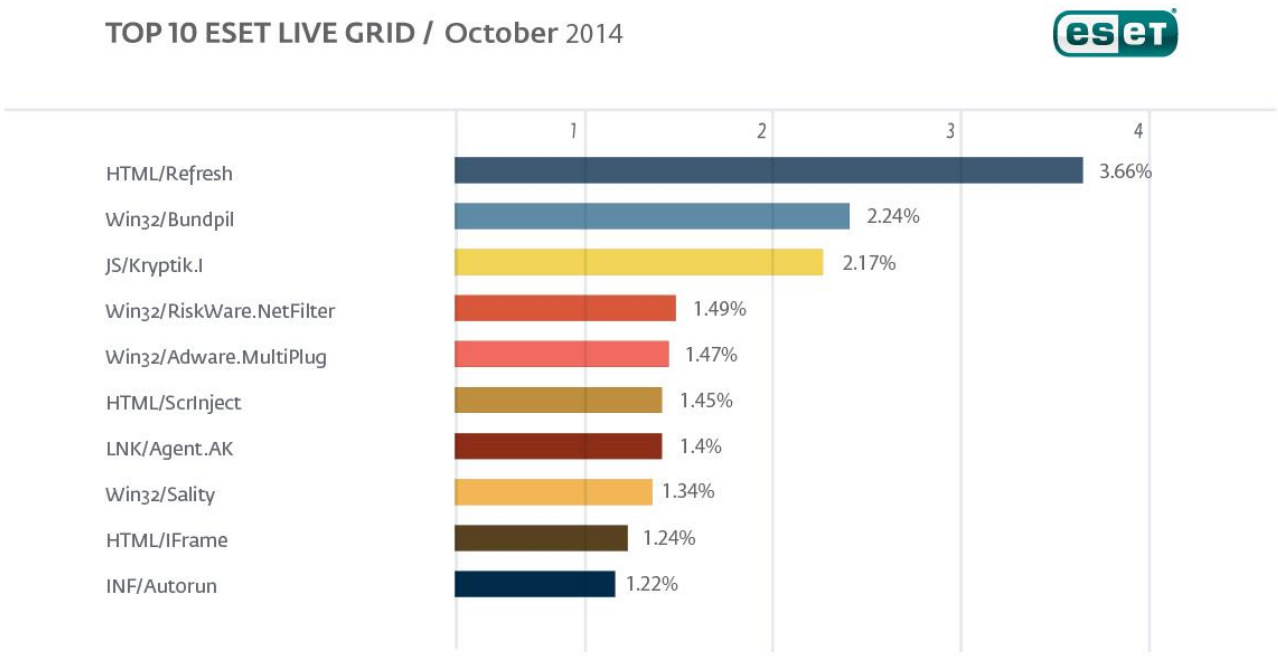
10. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.22%

INF/Autorun is a generic detection of versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to autorun a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in an attempt to hide the file from Windows Explorer.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 3.66% of the total, was scored by the HTML/Refresh class of treat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- We Live Security
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation