A PROFILE OF IRS SCAMMERS

Behind Tax Fraud

Loucif Kharouni
Forward-Looking Threat Research Team

CONTENTS

INTRODUCTION

Reports say tax fraud victims have lost more than US$15 million to cybercriminals since 2013. [1] The most recent victims were tricked into paying thousands of dollars each after receiving phone calls supposedly from Internal Revenue Service (IRS) agents. Call recipients were threatened to pay up or get sued.

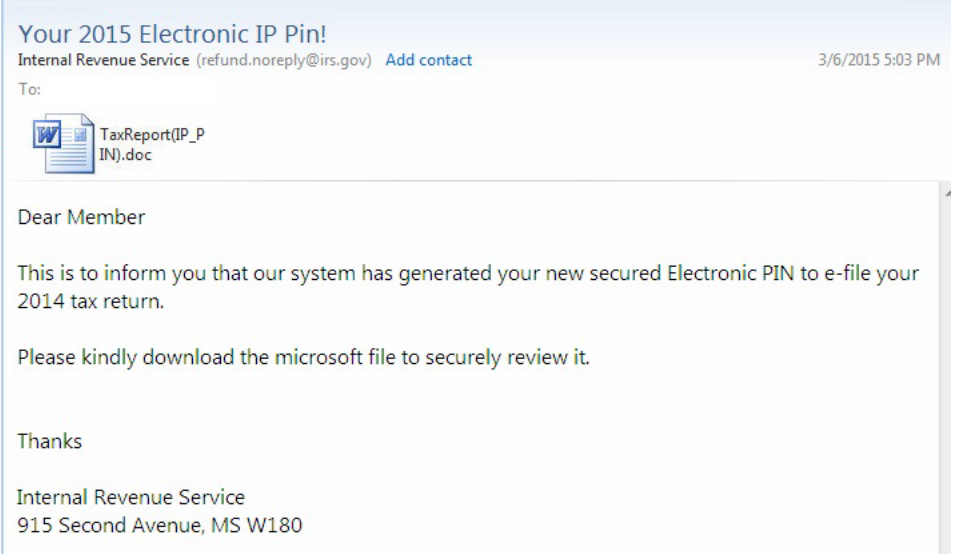
As early as February of this year, the IRS paid US$5.8 billion for fraudulent refunds and no one, not even the agency, may ever know how much it has paid over the years to fraudsters. [2] The Treasury Inspector General for Tax Administration even issued a warning to taxpayers to be on “high alert” for phone scams. [3]

Over the years, the attackers’ means may have evolved but their goal remains the same—to trick victims into giving out personal information or money. [4–6] Scammers often used malware—Trojan spyware, banking Trojans, or remote access tools (RATs)—to gain access to potential victims’ computers or bank accounts. The IRS has not been remiss in warning taxpayers about scams. It has, in fact, been coming up with the “Dirty Dozen” list of tax fraud scams since 2004 to help taxpayers stay safe from fraudsters. [7]

This research paper explains how IRS tax scams work, takes an in-depth look at noteworthy scam components, profiles some possible scammers based on open source intelligence (OSINT), and provides guidance on how taxpayers can avoid becoming fraud victims.

HOW IRS TAX SCAMS WORK

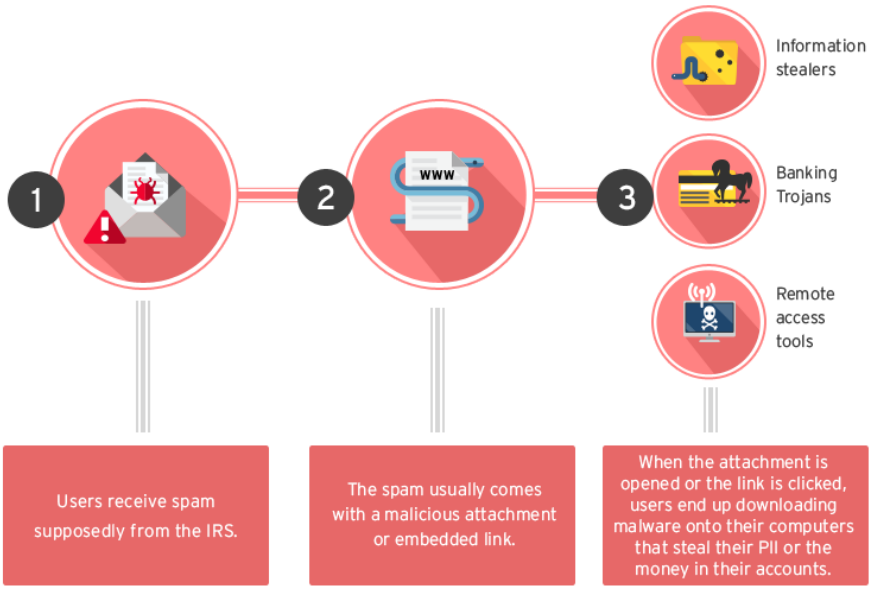
IRS tax scams normally begin with cybercriminals sending spam to as many potential victims as possible shortly before or after tax-filing season. The emails spread malware either by asking readers to open a malicious attachment or click a link that leads to the download of a malicious file. The malware, normally a Trojan spyware, banking Trojan, or RAT, allows the cybercriminals to steal victims' personally identifiable information (PII) or gain access to their financial accounts.



IRS tax scam spam sample

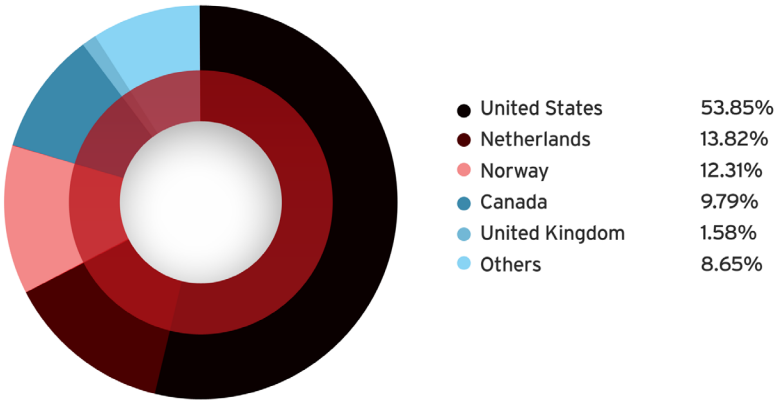
The IRS has identified 12 tax scam types: [8]

- Phone scams (IR-2015-5) [9]
- Phishing (IR-2015-6) [10]
- Identity theft (IR-2015-7) [11]
- Return preparer fraud (IR-2015-8) [12]
- Offshore tax avoidance (IR-2015-09) [13]
- Inflated refund claims (IR-2015-12) [14]
- Fake charities (IR-2015-16) [15]
- Hiding income with fake documents (IR-2015-18) [16]
- Abusive tax shelters (IR-2015-19) [17]
- Falsifying income to claim credits (IR-2015-20) [18]
- Excessive claims for fuel tax credits (IR-2015-21) [19]
- Frivolous tax arguments (IR-2015-23) [20]



How IRS tax scams work

Based on Trend Micro Smart Protection Network™ data from 1 January to 22 March 2015, a little more than half of the total number of possible IRS tax scam victims were, as expected, from the United States.



Number of victims who accessed IRS tax scam-related links from 1 January to 22 March 2015

TECHNICAL ANALYSIS: NOTEWORTHY IRS TAX SCAM COMPONENTS

The Awdaw2214a Mutex

Samples of about the same size and used similar file names were compiled and tested via Trend Micro™ Deep Discovery sandboxing technology. [21] Analysis of the sandbox reports and manual double-checking revealed similarities among the files. They not only shared a domain name, some samples also shared a mutex name—*awdaw2214a.*

A mutex is an object that allows multiple program threads to share the same resource such as file access though not simultaneously. [22] When a program is started, a mutex is created with a unique name. After this stage, any thread that needs the resource must lock the mutex from other threads while it uses the resource. The mutex is set to unlock when the data is no longer needed or the routine is finished. As such, the use of the same mutex by different programs can mean a single creator or owner.

The *awdaw2214a* mutex was used by malware associated with at least five toolkits or Trojan builders—HawkEye Keylogger, Limitless Keylogger,

DarkComet, Pony Loader, and ZeuS. [23–26] Some of the samples analyzed differed a little, as they were used as droppers of hacking tools.

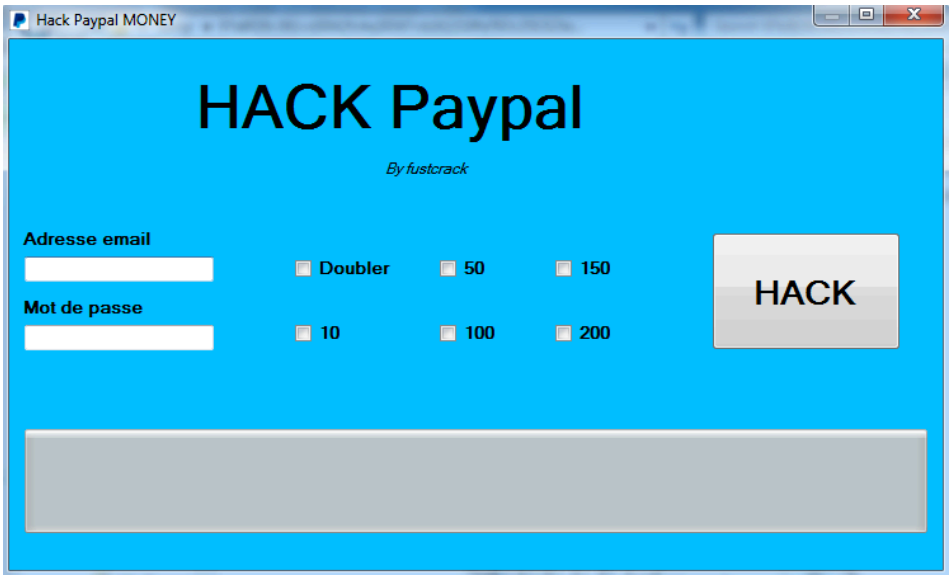
HKTL_VBINDER, which used the *awdaw2214a* mutex, was analyzed. This had varying arrival methods and payloads. [27]

FIRST VARIANT

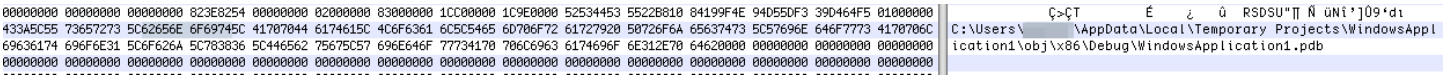
The first variant (SHA-1: *f9611b43cc53fac250c841f0258d98bc8212c1ed)* drops two malicious files—*HACK PAYPAL.EXE* and *TESTV2.EXE*—when executed.

HACK PAYPAL.EXE

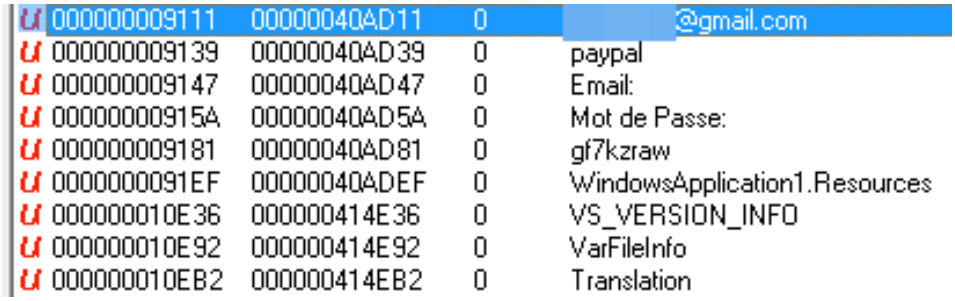
HACK PAYPAL.EXE is a hacking tool that cybercriminals use to increase the balances of chosen PayPal accounts. A closer look at the program's code brought to light a French-sounding name, which could very well belong to the code's creator or owner.



HACK Paypal's graphical user interface (GUI)



Code string that shows a French-sounding name, possibly its creator's



A Gmail™ address, probably the code's creator's, was also shown; parts of the code were also written in French

TESTV2.EXE

TESTV2.EXE creates malicious mutexes and processes that are injected into *taskmgr.exe.* It has the capability to evade detection, maintain persistence by creating a registry key, hook a Windows® function to install a keylogger, and open communication port 1607. It is interesting to note that DarkComet malware, by default, communicate via port 1607 with the command-and-control (C&C) server, *benben74.no-ip.org.*

Process, service, or memory object change	
Characteristic	**Details**
Creates mutex	Mutex: awdaw2214a
Creates mutex	Mutex: DC_MUTEX-X7MWQ70
Creates process	Process ID: 572 Image Path: %TEMP%\HACK PAYPAL.EXE
Creates process	Process ID: 552 Image Path: %TEMP%\TESTV2.EXE

Mutexes and processes that TESTV2.EXE *creates*

Injects memory with dropped files	Injecting Process ID: 552 Target Process ID: 2076 Target Image Path: %windir%\SysWOW64\taskmgr.exe File: MZP
Injects memory with dropped files	Injecting Process ID: 552 Target Process ID: 1340 Target Image Path: %windir%\SysWOW64\taskmgr.exe File: MZP
Injects memory with dropped files	Injecting Process ID: 552 Target Process ID: 2340 Target Image Path: %windir%\SysWOW64\taskmgr.exe File: MZP

Malicious processes that are injected into taskmgr.exe

Rootkit, cloaking	
Characteristic	**Details**
Attempts to hide file	%APPDATA%\Microsoft\Windows\Cookies\BxU\TESTV2.exe
Attempts to hide file	%TEMP%\TESTV2.EXE

Processes that the malicious file adds to evade detection

Autostart or other system reconfiguration	
Characteristic	**Details**
Adds autorun in registry	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\sidebar Value: %APPDATA%\Microsoft\Windows\Cookies\Sample.lnk Type: REG_SZ

Autorun key that the malicious file adds to the registry to maintain persistence

Hijack, redirection, or data theft	
Characteristic	**Details**
Installs keylogger	Hooked File: %windir%\SysWOW64\taskmgr.exe Hook Type: WH_KEYBOARD_LL

Windows function to install the keylogger

SECOND VARIANT

The second variant (SHA-1: *5af2279b5107ec97e77dca9a7271e8a64446d3c3)* also opens communication port 1607 with the help of the same type of mutexes as those tied to *TESTV2.EXE*—one of the first variant's payloads.

Process, service, or memory object change	
Characteristic	**Details**
Creates mutex	Mutex: awdaw2214a
Creates mutex	Mutex: Global\{0062c16a-656c-48da-91f0-6c860ecdc5e4}
Creates mutex	Mutex: Global\.net clr networking
Creates mutex	Mutex: DC_MUTEX-UQY5TRL

Mutexes that the second variant creates

This HKTL_VBINDER variant drops files, one of which is a hacking tool called "HACK Facebook," which was created by the same person behind HACK Paypal—fustcrack. Cybercriminals can use HACK Facebook to obtain chosen accounts' passwords.

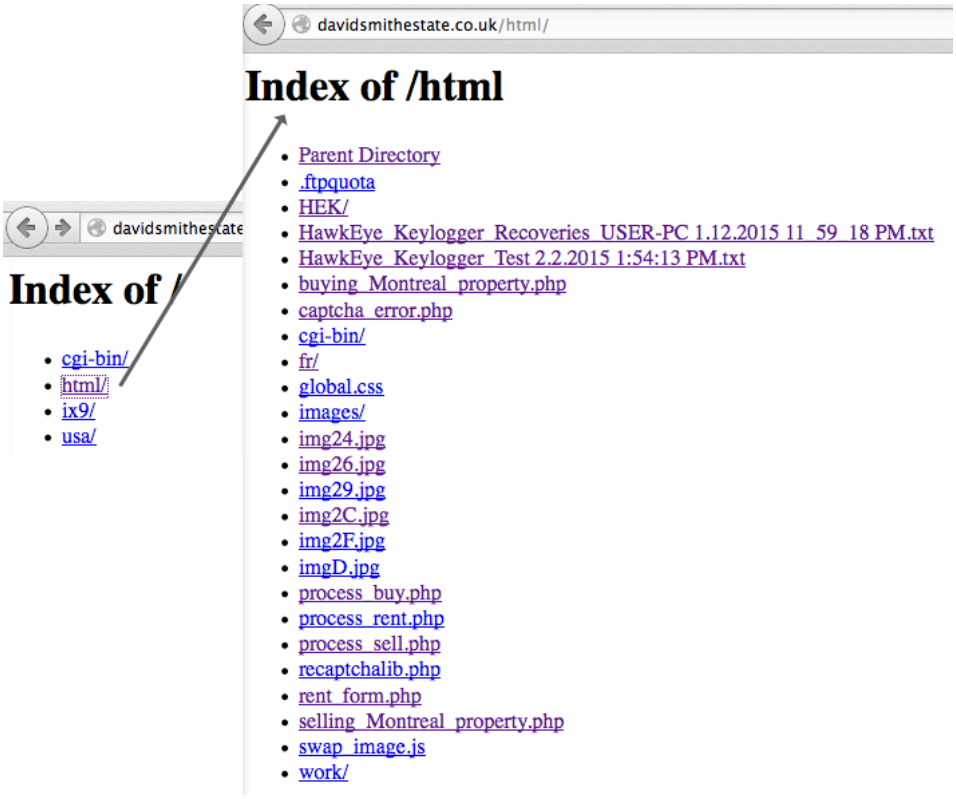
HACK Facebook's GUI

Macro-Based Malware: Tax(IP.PIN).doc

Macro-based malware are also commonly used to spread tax-filing season mayhem. Commonly embedded in malicious files attached to spam, these malware drop others to phish data from infected systems.

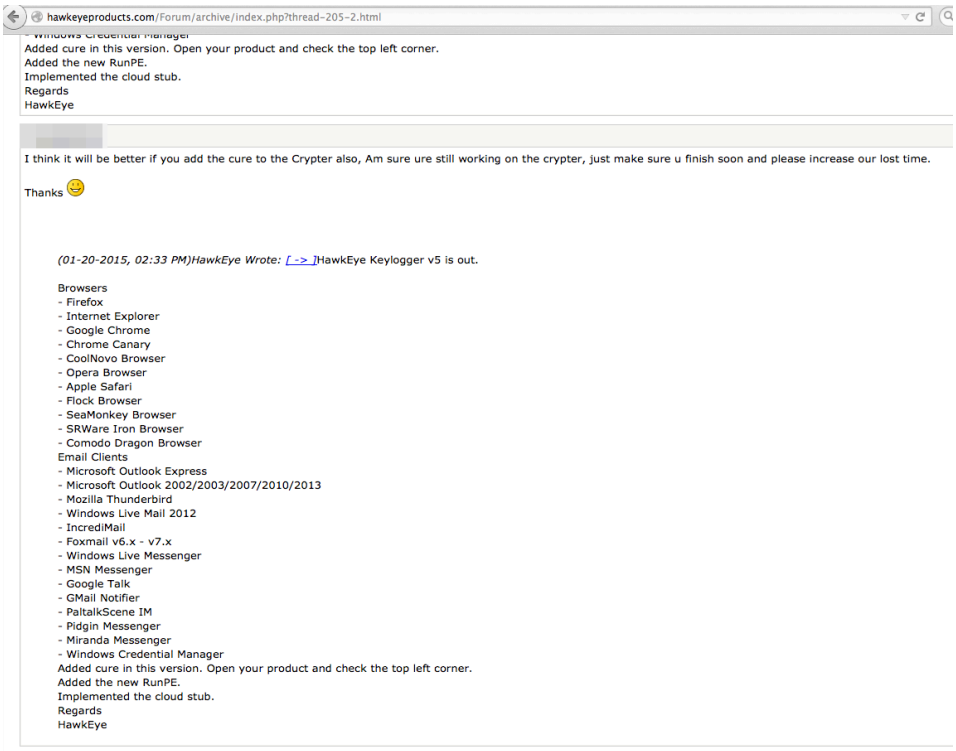
We took a look at one particular IRS spam named *"Tax(IP.PIN).doc* (SHA-1: *e53030c8a6364df879f32ee5e459b1b0ed0a50a7; 667a68dc226eafe2464b1ecd9826b409674223ff),"* detected by Trend Micro as W2KM_DLOAD.A and W2KM_MUPDATER.B, respectively. [28] These macro-based malware drop *google.exe* (SHA-1: *1d075575dd2c3999fe7c34850c81dc5848a05495; 3b750393f3420e6bf06a842a5bf82398de823153),* which Trend Micro detects as BKDR_FYNLOS.WIO and TSPY_MSILOG.B, respectively. [29]

Google.exe is actually a HawkEye Keylogger variant that communicates with the C&C server, *davidsmithestate.co.uk.* It was hosted by hostinger, which also hosts another malicious server, *dunlam007.ru.* Upon closer inspection, *davidsmithestate.co.uk* had open folders, which we were able to examine before they were cleaned up.



Open folders found on the davidsmithestate.co.uk *server*

Log file snippet from the davidsmithestate.co.uk *server*



hawkeyeproducts.com/Forum/archive/index.php?thread-205-2.html

Added cure in this version. Open your product and check the top left corner.
Added the new RunPE.
Implemented the cloud stub.
Regards
HawkEye

I think it will be better if you add the cure to the Crypter also, Am sure ure still working on the crypter, just make sure u finish soon and please increase our lost time.

Thanks

(01-20-2015, 02:33 PM)HawkEye Wrote: [->]HawkEye Keylogger v5 is out.

Browsers
- Firefox
- Internet Explorer
- Google Chrome
- Chrome Canary
- CoolNovo Browser
- Opera Browser
- Apple Safari
- Flock Browser
- SeaMonkey Browser
- SRWare Iron Browser
- Comodo Dragon Browser

Email Clients
- Microsoft Outlook Express
- Microsoft Outlook 2002/2003/2007/2010/2013
- Mozilla Thunderbird
- Windows Live Mail 2012
- IncrediMail
- Foxmail v6.x - v7.x
- Windows Live Messenger
- MSN Messenger
- Google Talk
- GMail Notifier
- PaltalkScene IM
- Pidgin Messenger
- Miranda Messenger
- Windows Credential Manager

Added cure in this version. Open your product and check the top left corner.
Added the new RunPE.
Implemented the cloud stub.
Regards
HawkEye

Old forum post tying the username for davidsmithestate.co.uk *to the HawkEye Keylogger*

The following table shows *davidsmithestate.co.uk's* contents before and after cleanup.

Before Cleanup	After Cleanup
HawkEye keyloggers	PayPal phishing page
HawkEye logs that contained PII stolen from U.S. and U.K. victims	
PayPal phishing pages	
Ice9 malware	
Pony Loader malware	

Before Cleanup	After Cleanup
Malicious documents: • *2014TaxReturn(IPPin).doc* (SHA-1: *c3a4f194ebd90e1de96a79824fb433c39de6425c* or W2KM_DLOADR.CP) • *sample.doc* (SHA-1: *e7d924e1dd6a0407636430f026bad24f473d9ed6* or TROJ_MUPDATER.A) • *CA2014(TaxElectronicPin).doc* (SHA-1: *75215151f8265582f4235230aa37181a20ff903d* or W2KM_DLOADR.CP) • *HMRC(TaxReport).doc* (SHA-1: *39e35b0c0d41875f28e1313240f6534f5bf1bffa* or W2KM_DLOADER.DT) • *PayPalTransaction_Dispute.doc* (SHA-1: *870c6153637b713d8bdce94611bf7da4ed218dfb* or W2KM_DLOADR.CP) • *Tax(IP.PIN).doc* (SHA-1: *667a68dc226eafe2464b1ecd9826b409674223ff* or W2KM_MUPDATER.B; *e53030c8a6364df879f32ee5e459b1b0ed0a50a7* or W2KM_DLOAD.A; *e7d924e1dd6a0407636430f026bad24f473d9ed6* or TROJ_MUPDATER.A) • *TaxReport(IP_PIN).doc* (SHA-1: *eab345a3897f4c11ebaee2b260ca1e3f95257433* or TROJ_MUPDATER.A)	

Pony Loader and Ice9 Malware

Traces of Pony Loader and Ice9 malware, both affiliated with well-known banking Trojan family, ZeuS, were also found on 27 February 2015 in at least two new domains related to IRS tax scams—*davidestlincon.com* and *dunlamisdavid.com.*

POSSIBLE IRS TAX SCAMMERS

Extensive OSINT research was conducted to gather more information on the *awdaw2214a* mutex. Findings revealed more hashes and sandbox reports on samples with the said mutex (see *Appendix).* A closer look at three of the hashes found allowed us to identify three possible IRS tax scammers—two individuals and a group.

The individuals or groups identified in this section have some apparent connection with IRS tax scams. Trend Micro would, however, like to point out that they may or may not be involved with cybercrime. We simply intend to lay out verified facts that link them to the campaigns' infrastructure and malware. Several other reasons such as having their email accounts stolen and used to register C&C servers, deliberate impersonation, and the like could also account for their links to the campaigns.

AyoolaD

One of the domains related to the *awdaw2214a* mutex was *ayool2day.biz.*

Domain Name:	AYOOL2DAY.BIZ
Domain ID:	D56051873-BIZ
Sponsoring Registrar:	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Sponsoring Registrar IANA ID:	303
Registrar URL (registration services):	www.publicdomainregistry.com
Domain Status:	clientTransferProhibited
Registrant ID:	DI_29415003
Registrant Name:	[redacted]
Registrant Organization:	N/A
Registrant Address1:	[redacted]
Registrant City:	wildwood
Registrant State/Province:	New Jersey
Registrant Postal Code:	08260
Registrant Country:	United States
Registrant Country Code:	US
Registrant Phone Number:	+1.[redacted]
Registrant Email:	[redacted]@outlook.com

WHOis data for ayool2day.biz

We found a username in the log file obtained from *davidsmithestate.co.uk,* an awdaw2214a mutex C&C server. OSINT research was done on the Microsoft™ Outlook® email address used to register *ayool2day.biz.* We used the same username as search term and found several possibly related accounts on Facebook, Twitter, Skype™, and OkCupid.

According to the profiles found, AyoolaD was born in 1984 and now resides in Puchong Batu Dua Belas, Kuala Lumpur, Malaysia. He has traveled to Nigeria as well as the United States, particularly Fort Worth, Texas City, and Framingham. He also apparently had email accounts on Gmail, Mail.com, Hotmail, Inbox.com, Outlook, and Yahoo!®.

Further investigation on AyoolaD suggests that he may have recruited people from the United States to work as mules for IRS tax scams. These recruits appear to have opened bank accounts and applied for credit cards using different identities to participate in IRS tax scams seemingly associated with AyoolaD. Evidence of his use of TurboTax® to regularly file taxes on other people's behalf was seen with the aid of associates who resided in the United States. AyoolaD also knew people who resided in Malaysia.

MahmoudD

We took a look at another malicious file (SHA-1: *3bf8b1e76d5397a3c77d7c0ef99ac6acaf14c13b),* detected by Trend Micro as TROJ_ZBOT.YKW. This file usually came in the guise of a .PDF file named *"report.pdf.exe,"* which accessed the following:

- *ma2dayzs.com/Panel/gate.php*
- *ma2dayzs.com/Panel/shit.exe*

An OSINT investigation of the domain, *ma2dayzs.com,* revealed that it was registered with a law office email address.

A search for *ma2dayz* turned up several results, including Facebook, YouTube™, Instagram, and Gmail accounts that had ties to a "MahmoudD." MahmoudD is of Egyptian descent but resides, according to his profiles at least, in São Paulo, Brazil. *Ma2dayz* was also registered in hacking forums such as *hackcommunity.com, crackingforum.com,* and *cardersforum.se.*

```
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin City: CASPER
Admin State/Province: WY
Admin Postal Code: 82601
Admin Country: US
Admin Phone: +1.
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:                    lawoffice.com
```

WHOis data for ma2dayzs.com

Interestingly, AyoolaD had ties to MahmoudD on Facebook. MahmoudD could be providing compromised sites to AyoolaD. How MahmoudD obtained access to these, however, was unclear.

ISA Hackers

The third sample we analyzed (SHA-1: *9cc1dff14d9b964f8d2abe713b10792df764f437),* which arrived as *IRS Payment Slip.scr,* is detected by Trend Micro as TSPY_ZBOT.NCA. [30] This Trojan spyware accessed the site, *idontknows.biz/user/adm/gate.php,* which was registered using a Yahoo! email address.

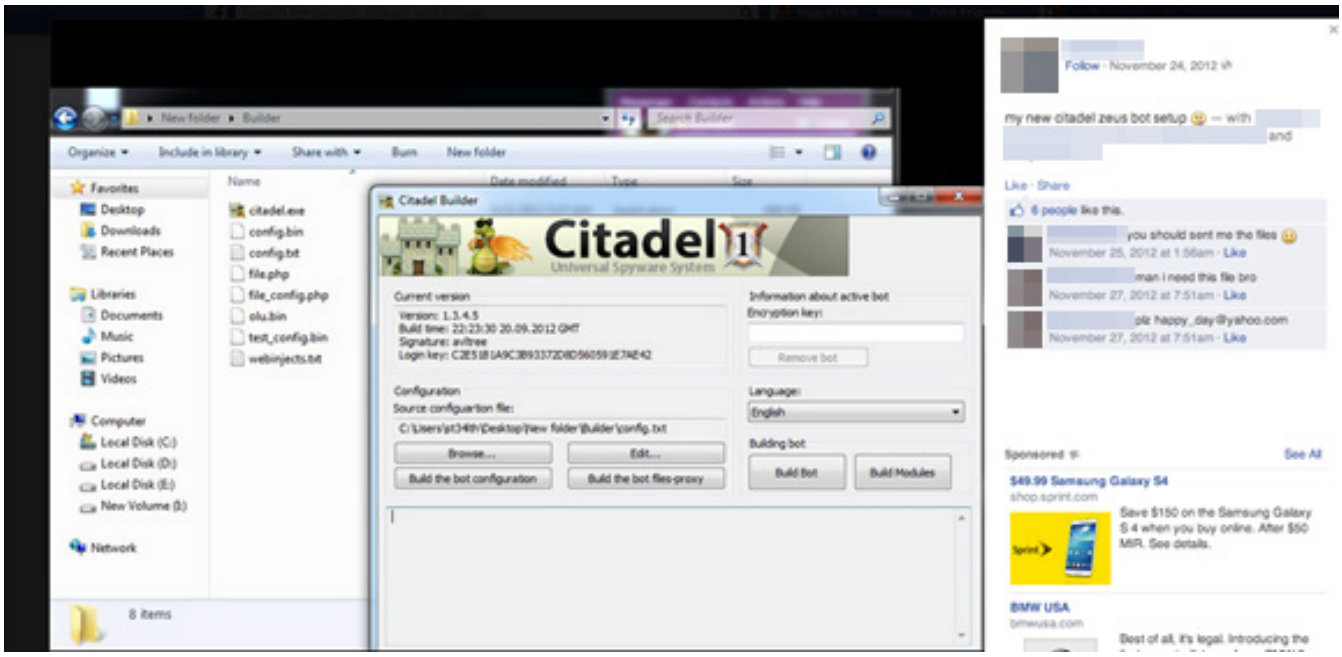
```
Domain Name:                          IDONTKNOWS.BIZ
Domain ID:                            D54306030-BIZ
Sponsoring Registrar:                 PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Sponsoring Registrar IANA ID:         303
Registrar URL (registration services): www.publicdomainregistry.com
Domain Status:                        clientDeleteProhibited
Domain Status:                        clientHold
Domain Status:                        clientTransferProhibited
Domain Status:                        clientUpdateProhibited
Registrant ID:                        DI_27510983
Registrant Name:
Registrant Organization:
Registrant Address1:
Registrant Address2:                  omalur
Registrant City:                      salem
Registrant State/Province:            Tamil Nadu
Registrant Postal Code:               60000028
Registrant Country:                   India
Registrant Country Code:              IN
Registrant Phone Number:              +91.
Registrant Email:                     @yahoo.com
```

WHOis data for idontknows.biz

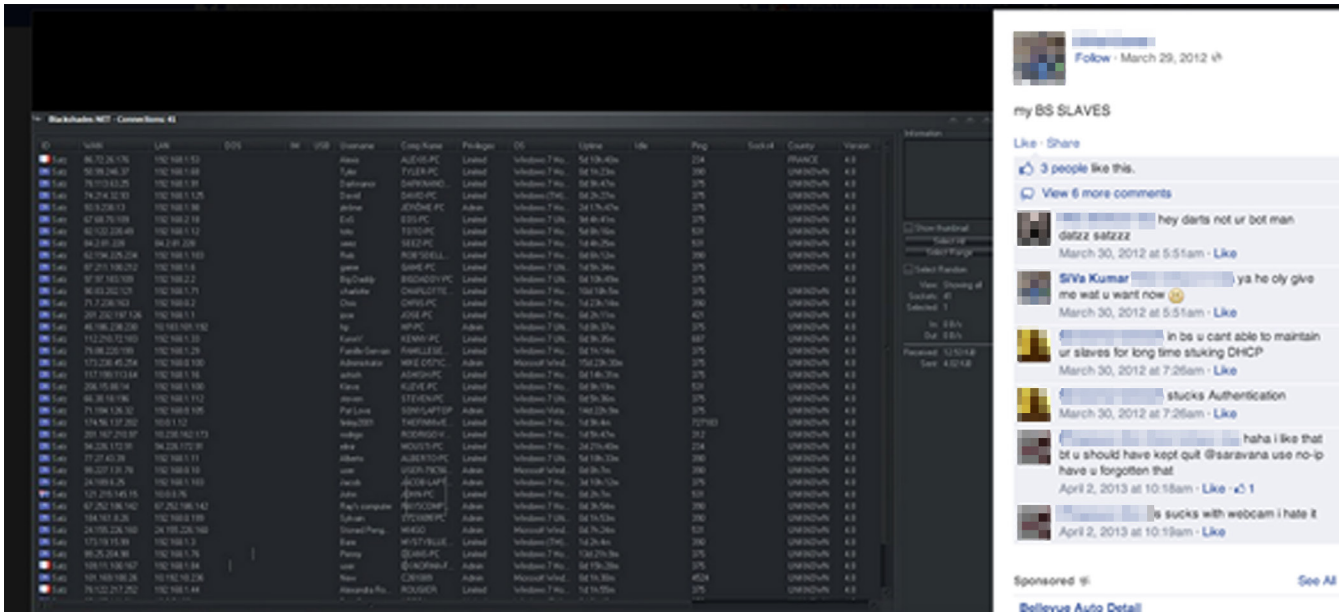
An OSINT investigation on the owner of the Yahoo! email address led to a Gmail address. Interestingly, the Yahoo! account owner also used the same handle on ISA Hackers, a hacking group with its own forum site. The forum site's owner is based in India and uses the Gmail address related to *idontlnows.biz.*

A look at several other malicious domains revealed ties between the two bad actors with regard to malware campaigns. One particular domain, *svkmrhosting.biz,* a known ZeuS C&C server, was registered using the forum owner's Gmail address, according to its Start of Authority (SOA) record. [31] A WHOis lookup of the same domain, meanwhile, revealed the Yahoo! address as the registrant's.

The Yahoo! address's owner also did work related to Citadel and Blackshades. [32–33] He is based in Chennai, India, and claims to work for HTC.



Yahoo! email address owner's last Citadel setup



Yahoo email address owner's Blackshades connection

The forum owner, according to his Facebook profile, is from Chennai, India, as well.

HOW TO AVOID BECOMING AN IRS TAX SCAM VICTIM

Note that the IRS will never do any of the following:

- Initiate contact by email to request personal or financial information
- Call to demand immediate payment nor call about taxes owed without first having mailed you a bill
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount you owe
- Require you to use a specific payment method for your taxes such as a prepaid debit card
- Ask for credit or debit card numbers over the phone
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying

Unsolicited emails claiming to be from the IRS or an IRS-related component such as the Electronic Federal Tax Payment System (EFTPS) should be reported to the IRS via *phishing@irs.gov.* [34] The usual tips to avoid becoming a phishing victim also apply:

- Refrain from clicking links embedded in or downloading attachments to unsolicited emails.
- It pays to know how social engineering works by staying abreast of the latest security threats. [35]
- Use the latest security technologies.

CONCLUSION

A crackdown on all IRS tax scammers may be next to impossible but every step toward that direction counts. The IRS has been constantly exerting effort to warn taxpayers about all kinds of fraud. [36] Unfortunately, tax scams work because a lot of users constantly fall for the ruse. The truth is—fighting cybercrime is everyone's responsibility. Authorities that are usually spoofed to scare users into doing something they would not otherwise do should continuously issue warnings. Security vendors should constantly update their products to protect against the latest threats. And users should follow best practices to avoid becoming victims.

Awareness is the first step to avoid becoming an IRS tax scam victim. Every taxpayer needs to know how the IRS works so they will not be tricked even by the most elaborate and very convincing scams. A little technical help from products and services that prevent spam and phishing emails from even reaching inboxes should also help. These technologies can also block access to malicious sites even if links that lead to them are clicked. They also prevent the download and installation of malicious programs or components on computers, thus thwarting threats even before they can wreak havoc. [37]

APPENDIX

DOMAINS THAT AYOOLAD APPARENTLY REGISTERED

- *124.248.205.92*
- *212.7.208.77*
- *82.145.41.7*
- *ayool.no-ip.org*
- *ayool1.no-ip.org*
- *ayool2day.biz*
- *ayool3.no-ip.org*
- *baleareson.net*
- *bamisoro.no-ip.biz*
- *benben74.no-ip.org*
- *business11.no-ip.org*
- *chuks052.no-ip.org*
- *clak64.no-ip.org*
- *d19.no-ip.biz*
- *davidsmithestate.co.uk*
- *davolointernational.comoj.com*
- *dmosole.zapto.org*
- *dunlam007.ru*
- *dunlamisdavid.com*
- *dvd.selfip.net*
- *fjkabelo.no-ip.biz*
- *ftp.2013update.net*
- *ftp.mozero1.yzi.me*
- *hessu.zapto.org*
- *hessubs.zapto.org*
- *koby1.no-ip.org*
- *koby2.no-ip.biz*
- *leeyou.no-ip.org*
- *logicrat.no-ip.org*
- *magicconnect.no-ip.biz*
- *mail.kngkong.com*
- *mcsoft.noip.me*
- *misakikoikoi.no-ip.biz*
- *oathsworn.org*
- *oboyouk.comoj.com*
- *ohis052.no-ip.biz*
- *r0c.ddns.net*
- *rainbowie.no-ip.biz*
- *rapadar333.zap.org*
- *serveurben44.no-ip.org*
- *sgpon.webege.com*
- *tazbot.mooo.com*
- *tazbox.zapto.org*
- *tripplem78.no-ip.biz*
- *uzzikie.netdns.net*

IRS TAX SCAM MALWARE

SHA-1	File Name	Trend Micro Detection Name
609b0d5a5552a9b7a1cc566fea6600cd223a9f16		TROJ_SCAR
44389df2d6dcc01ae68506ae9481282427c318fe		SPYW_LIMITLESS
12deef8d9cb51f7c33870a72a227ee6bebc99b71		BKDR_ANDROM.OM
1bd6bf50eb014e39d743eff7041caf85597b3b0d		BKDR_FYNLOSKI.CF
cb05b325601beb70cf67b76ef82cd6ba124db032		BKDR_BOTINTIN.C
65942b6c23a2850e7a77d1be1e4411c31ac92fc5		TROJ_SCAR
2eeabfc5902e2548f89ffb706c90e385f2e9a72a		TROJ_SCAR
b34430c3ced52950875214844f7ffe557319ef46		TSPY_FAREIT.AQO
ee926fc88e9e506c80ffd411202a4bd692ed40bd	*2013_Early_Tax_Return_Report.pdf.exe*	TSPY_FAREIT.AQL
154324f1d446d8a8bb9a8362876eae6760d0f28c		TROJ_APATE.DAM
19174eef360cd5c7b14a0641ab85597195fd6eb3		ADW_IdleKMS
1f7660384eceea5919fd0c6790a561db650d0f84		TSPY_FAREIT.CAB
6160c03743ea3dff4cfd98cc9d390fd30747e070	*Your_2013_TaxReturnReport.pdf.exe*	TROJ_KRYPTIK.YUY
b3b2d7c824d220b2b2f326612a97486faee053e1		SPYW_LIMITLESS
31cb7393be49539e9f6a419049decf544c47ff6b	*Your_2013_TaxReturnReport.exe*	TROJ_KRYPTIK.YUU
fc6f3eff01e12cc991edd68c334aa13fd56c17dd	*Early2013TaxReturnReport.exe*	TSPY_FAREIT.ARD
908a11bf72f40ff5facc4d989e73945df82ffa0c		TROJ_UPATRE.AQ
bf1d1662d9fa1160603c7fbffe158d80ffa201d0		TROJ_DROPPR.XF
972485a192cec6bc6a22cf22b7a227239799d314	*2013TaxReturnReport.exe*	TROJ_UPATRE.YYKF
b51fe1dd35047387a9ae86ec5a9ddbb0b5f6f112		BKDR_NETWIREDRC.B

SHA-1	File Name	Trend Micro Detection Name
82295a6edca2009886f12d126f159a7dfdccc436		SPYW_LIMITLESS
bc60772665a0268b5472992d28f05dc01c03ce15		SPYW_LIMITLESS
ca7bcd7839610f6b0eb82797c5622a1ae57f92d1		TROJ_INJECT.DLB
2174cc9c14a21708359f2f14a7d73d08a2b1c3fe		SPYW_LIMITLESS
a1ab29491e9ea126e7d94a48569be3cc4a3a42d5	*Your_2013_TaxReturnReport.exe*	TROJ_KRYPTIK.YUU
6a6dd2939f395555c8eef0a7004ef07e63c91ebf		TROJ_MSIL.BBK
cd75834c76e553c1bd5b79f17f6e15eb588682eb		SPYW_KEYLOG
598abe576bfe1becbf3d991b9ac0cd1e4acde592		TSPY_INFOSTIL.BE
38aee74c66313165188891f6921324bda81024114		SPYW_LIMITLESS
bdf561f8fc52fa26afb9741a6f3124bb62d8a93e		SPYW_LIMITLESS
3ea1c53c91a9f85971a408679fce862d65f3cd36		SPYW_LIMITLESS
c4bfd7579a37c92899fa612e0dba3e89ff258656		SPYW_LIMITLESS
cdd73e1274be39cc00902b0cf2772904078548f3		SPYW_LIMITLESS
e2f8874b8e2989efa037fa7e8268e27a8d0479c6		SPYW_LIMITLESS
18bd850f24092a47150228e5673dbb1c471b72f6	*Image_001_040214.exe*	TROJ_UPATRE.YYKF
ee4a66fdaca21c468b66cd61a3eb25ef3db4f61f		TROJ_MSIL.BFS
3bf8b1e76d5397a3c77d7c0ef99ac6acaf14c13b		TSPY_ZBOT.YKW
61d09580e3bece91fffec0cc80f7727999bec241		BKDR_DARKKOME.DR
49abe98235421771f8c486e5e0d14cde0607fa6c		TROJ_APATE.A
8ac215a349b2c8c2fa0424daff2a729d00131e4e		TSPY_SPYBOT.CMS
5c4d47a18c18da60e2ee0e45e541dce54fce190f		WORM_GAMARUE.JT

SHA-1	File Name	Trend Micro Detection Name
fb0f011771874fa246aa7e5072436467b2018f96		TROJ_AINSLOT.CC
ef1753acb3ffb6089126d84fb5a6311cd3565bf0		TROJ_INJECT.IRS
022d3b48f9b9288df2eb5a46b171d276852b6881		SPYW_LIMITLESS
8bb377f1c27fe790cc5f9bac3c0b75689e178f37		BKDR_ANDROM.FAV
9ff0f93aa9f51d3ecaf21be507da900b73e8f0f2		BKDR_ANDROM.PB
181ddf0091bbb7c59cfa01fba694c55e600ae950		TROJ_NOTOOLS
c0428f3d4e6a66362f252352ec61d8b2751e3677	*2013StateTaxRefund.exe*	TROJ_KAZY.AU
08e61abcd2c351e22ebc3536cf7d2a15ac8cbf06		TROJ_INJECT.FAP
387bfeb2372f9bd69860d9176e919803d12a6734		TROJ_DLOADR.CAB
fb57991dd4300848e0e53d389c3eef0b5332f8ce		TROJ_SCAR
ed2a3d6e7d437fcca00666c2fdd74bb44a67a052		BKDR_FYNLOSKI.CA
f3b3da6f11b7779b896579c39761757e65f91b5a		TROJ_MSIL.INJ
77e3bcef2ebf77b6b6fb00235f707b6e9236bb86		SPYW_LIMITLESS
c8ed319d45ea0bd5b67be3c49af3f674da06e22e		SPYW_LIMITLESS
cb77e715a55ce55f4633b30d2a5a89bbd00e77c6		TROJ_INJECT.YFK
b43ad394d8fca98077bfc33c96dd8a526e145793	*i_Early2013TaxReturnReport.exe*	TSPY_FAREIT.ASF
8f2ebf0422d34a7e0bc1480bc0efea859f2f56e8		SPYW_LIMITLESS
045d94462a505b8b7250c9836620d1373af6798f		SPYW_LIMITLESS
cfea6c4f6f44ca9c79a3d613edef820dcd4d5876		TROJ_DROPPE.WR
06d01b8299c3a11403ba32228b19cff4d1438509		SPYW_LIMITLESS
fc9441983b0c119bbc3f2fc221af15da5a621c57		BKDR_FYNLOSKI.CA

SHA-1	File Name	Trend Micro Detection Name
9f7d6d8a2a7c36e953369703421c3f6274144619		TROJ_SCAR
15b4a4c05bd3847ececb1fbdecb5c2cbb89309ea	*2013StateTaxReturn.exe*	TROJ_INJECTO.BSV
cb5a4923317bc840be1c7a7a1527aa80f9241991		TROJ_SCAR
724ed96e7eb10b1be9ad817f2e42a4a9f31d81d1		SPYW_LIMITLESS
060a3b4fd165f87e7fc650c806c9dec17469ed45		TROJ_SCAR
9cc1dff14d9b964f8d2abe713b10792df764f437		TSPY_ZBOT.NCA
2164cd3db503d2d0bd3a4bdfacffa13fb0ceb540		SPYW_LIMITLESS
0d96bf07de613c46920d99282408421024472d11		TSPY_FAREIT.CDO
1d075575dd2c3999fe7c34850c81dc5848a05495		TSPY_MSILOG.B
a4c95a755685c6802ae41a7b8272c87a8d399af9		TROJ_NONCORE.B
5af2279b5107ec97e77dca9a7271e8a64446d3c3		HKTL_VBINDER
e7d924e1dd6a0407636430f026bad24f473d9ed6		TROJ_MUPDATER.A
39e35b0c0d41875f28e1313240f6534f5bf1bffa		W2KM_DLOADER.DT
3b750393f3420e6bf06a842a5bf82398de823153		TSPY_MSILOG.B
c3a4f194ebd90e1de96a79824fb433c39de6425c		W2KM_DLOADR.CP
02ba7427340ed41c1f6c4fa1cfec23ae610672a0		W2KM_MUPDATER.B
eab345a3897f4c11ebaee2b260ca1e3f95257433		TROJ_MUPDATER.A
75215151f8265582f4235230aa37181a20ff903d		W2KM_DLOADR.CP
8fc7dafe6f09d0343bad260cb4892e8b9381e2fd		W2KM_DLOAD.A
d02d8de75930154642725b8f6de5b86526078960		BKDR_FYNLOS.WIO
870c6153637b713d8bdce94611bf7da4ed218dfb		W2KM_DLOADR.CP

SHA-1	File Name	Trend Micro Detection Name
5de76f097d9ca06fe1498f888ce67bf29ac5d651		BKDR_FYNLOS.WIO
667a68dc226eafe2464b1ecd9826b409674223ff		W2KM_MUPDATER.B
f9611b43cc53fac250c841f0258d98bc8212c1ed		HKTL_VBINDER
e53030c8a6364df879f32ee5e459b1b0ed0a50a7		W2KM_DLOAD.A

REFERENCES

[1] Sara Ganim and David Fitzpatrick. (14 March 2015). *CNN.* "IRS Scam Costing Victims $15 Million." Last accessed on 24 March 2015, http://edition.cnn.com/2015/03/13/us/irs-scam.

[2] Robert W. Wood. (19 February 2015). *Forbes.* "IRS Paid $5.8 Billion in Fraudulent Refunds, Identity Theft Efforts Need Work." Last accessed on 24 March 2015, http://www.forbes.com/sites/robertwood/2015/02/19/irs-paid-5-8-billion-in-fraudulent-refunds-identity-theft-efforts-need-work/.

[3] Treasury Inspector General for Tax Administration. (21 January 2015). *Press Release.* "J. Russell George Urges Taxpayers to Be on 'High Alert' to Phone Fraud Scam: TIGTA Reminds Taxpayers to Beware of Calls from IRS Impersonators This Filing Season." Last accessed on 24 March 2015, http://www.treasury.gov/tigta/press/press_tigta-2015-01_home.htm.

[4] Ryan Certeza. (22 April 2014). *TrendLabs Security Intelligence Blog.* "The Timely Tale of Tax-Related Threat Troubles." Last accessed on 24 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-timely-tale-of-tax-related-threat-troubles/.

[5] Gelo Abendan. (4 April 2013). *TrendLabs Security Intelligence Blog.* "Cybercriminals Threaten Tax Day Once Again." Last accessed on 24 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-threaten-tax-day-once-again/.

[6] Neil Pondo. (21 January 2012). *TrendLabs Security Intelligence Blog.* "Tax Season Opens, Tax Spam Follows." Last accessed on 24 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/tax-season-opens-tax-spam-follows/.

[7] IRS. (1 March 2004). *IRS.* "IRS Updates the 'Dirty Dozen' for 2004: Agency Warns of New Scams." Last accessed on 24 March 2015, http://www.irs.gov/uac/IRS-Updates-the-%E2%80%98Dirty-Dozen%E2%80%99-for-2004:-Agency-Warns-of-New-Scams.

[8] IRS. (9 February 2015). *IRS.* "IRS Completes the 'Dirty Dozen' Tax Scams for 2015." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/IRS-Completes-the-Dirty-Dozen-Tax-Scams-for-2015.

[9] IRS. (22 January 2015). *IRS.* "Phone Scams Continue to Be Serious Threat, Remain on IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Phone-Scams-Continue-to-be-Serious-Threat-and-Remain-on-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[10] IRS. (23 January 2015). *IRS.* "Phishing Remains on the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Phishing-Remains-on-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[11] IRS. (26 January 2015). *IRS.* "Identity Theft a Major Concern on the IRS Annual 'Dirty Dozen' List of Tax Scams to Avoid." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Identity-Theft-a-Major-Concern-on-the-IRS-Annual-Dirty-Dozen-List-of-Tax-Scams-to-Avoid.

[12] IRS. (27 January 2015). *IRS.* "Return Preparer Fraud Hits IRS Annual 'Dirty Dozen' List of Tax Scams to Avoid During the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Return-Preparer-Fraud-Hits-IRS-Annual-Dirty-Dozen-List-of-Tax-Scams-to-Avoid-During-the-2015-Filing-Season.

[13] IRS. (28 January 2015). *IRS.* "Hiding Money or Income Offshore Among the 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Hiding-Money-or-Income-Offshore-Among-the-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[14] IRS. (29 January 2015). *IRS.* "Inflated Refund Claims Remain on the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Inflated-Refund-Claims-Remain-on-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[15] IRS. (30 January 2015). *IRS.* "Fake Charities Among the IRS 'Dirty Dozen' List of Tax Scams for 2015." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Fake-Charities-Among-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-2015.

[16] IRS. (2 February 2015). *IRS.* "Filing Fake Documents to Hide Income Is Again on the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Filing-Fake-Documents-to-Hide-Income-Is-Again-on-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[17] IRS. (3 February 2015). *IRS.* "Abusive Tax Shelters Again on the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Abusive-Tax-Shelters-Again-on-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[18] IRS. (4 February 2015). *IRS.* "Falsifying Income to Claim Tax Credits Hits the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Falsifying-Income-to-Claim-Tax-Credits-Hits-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[19] IRS. (5 February 2015). *IRS.* "Excessive Claims for Fuel Tax Credits Make the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Excessive-Claims-for-Fuel-Tax-Credits-Make-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[20] IRS. (6 February 2015). *IRS.* "Frivolous Tax Arguments Completes the IRS 'Dirty Dozen' List of Tax Scams for the 2015 Filing Season." Last accessed on 23 March 2015, http://www.irs.gov/uac/Newsroom/Frivolous-Tax-Arguments-Completes-the-IRS-Dirty-Dozen-List-of-Tax-Scams-for-the-2015-Filing-Season.

[21] Trend Micro Incorporated. (2015). *Trend Micro.* "Deep Discovery: Advanced Network Security." Last accessed on 20 March 2015, http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/#email-protection.

[22] QuinStreet Inc. (2015). *Webopedia.* "Mutex." Last accessed on 20 March 2015, http://www.webopedia.com/TERM/M/mutex.html.

[23] Ryan Flores. (11 November 2014). *TrendLabs Security Intelligence Blog.* "Predator Pain and Limitless: Behind the Fraud." Last accessed on 20 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/.

[24] Nart Villeneuve. (20 April 2012). *TrendLabs Security Intelligence Blog.* "Fake Skype Encryption Software Cloaks DarkComet Trojan." Last accessed on 20 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/fake-skype-encryption-software-cloaks-darkcomet-trojan/.

[25] Eduard Kovacs. (27 June 2014). *SecurityWeek.* "Pony Loader 2.0 Malware Source Code for Sale." Last accessed on 20 March 2015, http://www.securityweek.com/pony-loader-20-malware-source-code-sale.

[26] Lord Alfred Remorin. (2 June 2014). *TrendLabs Security Intelligence Blog.* "GameOver: ZeuS with P2P Functionality Disrupted." Last accessed on 20 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/gameover-zeus-with-p2p-functionality-disrupted/.

[27] Trend Micro Incorporated. (2015). *Threat Encyclopedia.* "HKTL_VBINDER." Last accessed on 25 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/HKTL_VBINDER.

[28] Trend Micro Incorporated. (2015). *Threat Encyclopedia.* "W2KM_DLOAD.A." Last accessed on 24 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/W2KM_DLOAD.A.

[29] Trend Micro Incorporated. (2015). *Threat Encyclopedia.* "TSPY_ZBOT.NCA." Last accessed on 23 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TSPY_ZBOT.NCA.

[30] Aetrion LLC. (2015). *dnsimple.* "What Is an SOA Record?" Last accessed on 23 March 2015, https://support.dnsimple.com/articles/soa-record/.

[31] Trend Micro Incorporated. (September 2, 2013). *TrendLabs Security Intelligence Blog.* "Citadel Makes a Comeback, Targets Japan Users." Last accessed on 23 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/citadel-makes-a-comeback-targets-japan-users/.

[32] Rhena Inocencio. (26 May 2014). *TrendLabs Security Intelligence Blog.* "The Blackshades RAT—Entry-Level Cybercrime." Last accessed on 23 March 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-blackshades-rat-entry-level-cybercrime/.

[33] IRS. (2015). *IRS.* "Tax Scams/Consumer Alerts." Last accessed on 23 March 2015, http://www.irs.gov/uac/Tax-Scams-Consumer-Alerts.

[34] Trend Micro Incorporated. (3 February 2015). *Trend Micro Security News.* "The Most Popular Social Engineering Lures Used in 2014." Last accessed on 23 March 2015, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-most-popular-social-engineering-lures-used-in-2014.

[35] IRS. (2015). *IRS.* "IRS Wants You to Know About Schemes, Scams, and Cons." Last accessed on 24 March 2015, http://www.irs.gov/uac/IRS-Wants-You-to-Know-About-Schemes,-Scams-and-Cons:.

[36] Trend Micro Incorporated. (2015). *Trend Micro*. “Smart Protection Network—Data Mining Framework.” Last accessed on 24 March 2015, http://cloudsecurity.trendmicro.com/us/technology-innovation/our-technology/smart-protection-network/#fighting-cyber-crime.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569.8900