

THREATS TO WATCH OUT FOR DURING THE TAX SEASON

Cybercriminals often capitalize on the tax season to launch a plethora of attacks and that is not surprising. The most common tax-related threats are phishing attacks that leave users at risk of information or, worse, identity and financial theft apart from system infections.

While tax-related scams are no longer new, they remain prevalent, targeting home and enterprise users alike. Most of these scams start from spam supposedly from the Internal Revenue Service (IRS). These email messages threatened users with bogus warnings of underreporting their incomes, tricked them into thinking they were getting tax refunds, or asked them to provide additional information due to supposed process changes, all to get them to give out their personal credentials.

Tax-related scams often use the following tactics to prey on users:

- Threatening them with bogus warnings of underreporting their incomes
- Tricking them into thinking they were getting tax refunds
- Asking them to provide additional information due to supposed process changes

The Tax Season Translates to Profit

The fact that taxes are usually filed online in most countries allows cybercriminals to instigate malicious tax-related scams. They use proven social engineering techniques to lure unwitting users into their specially crafted traps.

Scary Tax-Related Warnings

- In September 2009, U.S. taxpayers with foreign bank and other financial accounts were targeted by scammers in line with the tax-filing extension issued by the IRS. A spammed message that bore the subject "Notice of Underreported Income" led recipients to malicious sites where TSPY_ZBOT.BZJ, TSPY_ZBOT.BZT, TSPY_ZBOT.BZS, and TSPY_ZBOT.COB were hosted.

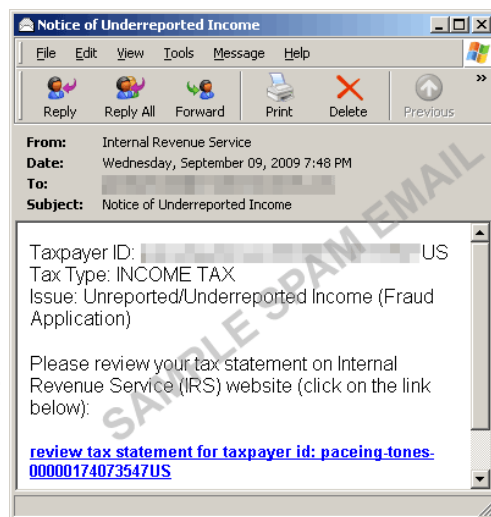


Figure 1. Sample IRS spam using scare tactics

Promises of Tax Refunds

- Last month, TrendLabsSM engineers received spam samples with a **.ZIP file attachment** that supposedly contained a document that users needed to download and print in order to get refunds. In reality, however, the document was a malware detected as **TSPY_ZBOT.SMHA**. Like other ZBOT variants, it also steals banking-related and other financial information from infected systems.
- In 2008, phishers led unwitting users to a fake IRS site by tricking them into thinking they would receive tax refunds. They were asked to **choose the name of the bank** to which their money should be deposited. This then brought them to a fake login page of their chosen bank. Of course, instead of receiving supposed refunds, they instead ended up losing their login credentials to phishers.
- Earlier that same year, spammed messages informing users that they would **receive tax refunds worth US\$93.60** were found. In return, they were asked to fill in a tax refund request form by clicking a link to a phishing site where they were asked to enter their social security and ATM personal identification numbers (PINs).

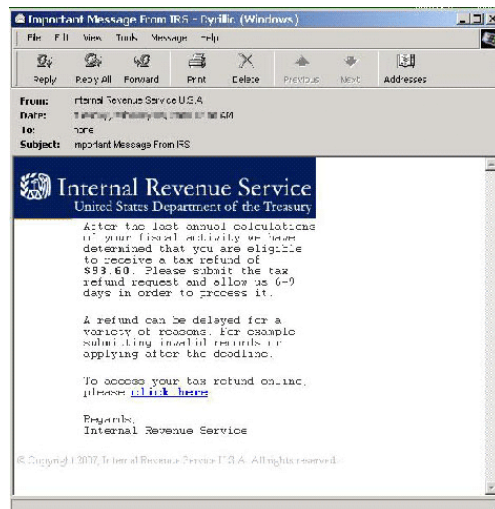


Figure 2. Sample IRS spam that promises a US\$93.60 refund

Fake Tax Forms

- Earlier last year, cybercriminals also urged users to download and fill in a **fake IRS W-2 form** due to supposed important changes. The .RTF file, however, was actually an .EXE file detected as **BKDR_POISON.BQA**. A component of the **DarkMoon Remote Administration Tool (RAT)**, it allows a remote user to execute commands on an infected system, hence compromising its security.
- Noncitizen residents of the United States were also targeted with a **bogus W-8BEN form** in 2009. They were asked to fill in and return the form to which additional requirements like bank account numbers have been added via email.

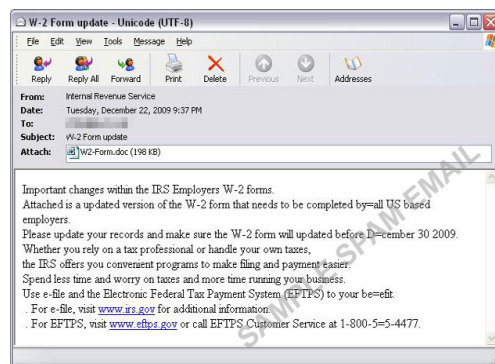


Figure 3. Sample IRS spam with W-2 form attachment

Apart from the usual IRS-related tax scams, we have also seen spammed messages that offered to help users **save money on tax preparations** and that scared CEOs with **fake subpoenas** or **tax petitions** in relation to supposedly making insufficient payments, which led to the download of malware like **TROJ_AGENT.AMAL**.

It is also worth noting that one of cybercriminals' favorite targets last month is the Electronic Federal Tax Payment System (EFTPS), as **9.5 million U.S. taxpayers use it** at present. It has also been responsible for over 1 billion electronic tax payments, allowing it to post revenue amounting to almost US\$22.8 trillion since it began operating in 1996.

The Cybercrime Driving Force

Financial gain is the primary motive behind tax-related attacks. Cybercriminals steal user information like banking credentials, user names, passwords, and social security numbers and sell these underground. They also use these for other malicious activities.

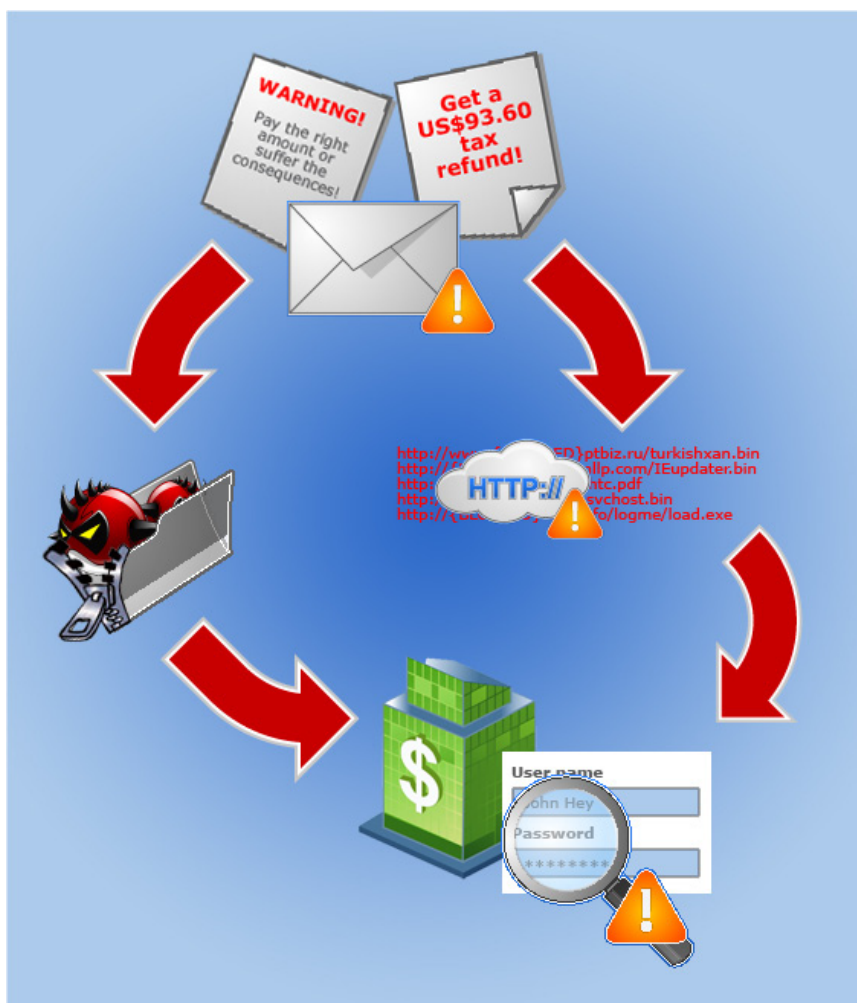


Figure 4. Typical tax-related threat diagram

Spammed messages that bear links to malware download sites are also staple tools in stealing user information. Aided by ZBOT and now SpyEye variants, which are known for targeting and even **bringing companies to the brink of bankruptcy**, cybercriminals are able to reap millions in profit from taxpayers.

In some instances, cybercriminals specifically **prey on Fortune 500 companies** and other well-known organizations, as senior threat researcher Paul Ferguson believes that apart from committing financial fraud, they also wish to infiltrate these companies for more nefarious reasons.

Awareness Is Still Key

Knowing the latest security news goes a long way. Lack of awareness of scams leads to the success of tax-related attacks. Because taxes involve huge sums of money, it is only natural for cybercriminals to come up with all kinds of scams to trick users into parting with their cash. The IRS, as one of the most commonly used institutions for instigating such attacks, has therefore made it a mission to constantly inform users of cybercriminals' malicious schemes through its site.



We at Trend Micro also consistently warn users about these threats because we believe that social engineering will **continue to play a crucial role** in propagating malware and in instigating cybercrime. In fact, cybercriminals will continue to spam users with warnings, enticing promises of refunds, and in relation to taxes to infect their systems and to profit.

Users should always be wary of tax-related scams. They should be careful of downloading files attached to or clicking links embedded in email messages claiming to come from the IRS come tax season. They should keep in mind that institutions like the IRS will never send official correspondence via email. They should also only obtain tax forms from their countries' respective tax authorities. Finally, they should always be wary of unbelievable offers like help in computing their taxes. If an offer is too good to be true, it most likely is.

We also highly recommend that users install an **effective security software** that can prevent spam from even reaching their inboxes, can block access to malicious sites, and can detect and prevent the download and execution of malicious files.

References:

- Bernadette Irinco. (September 16, 2009). *TrendLabs Malware Blog*. "Social Engineering Watch: Another IRS Scam." <http://blog.trendmicro.com/social-engineering-watch-another-irs-scam/> (Retrieved March 2011).
- Elizabeth Bookman. (December 9, 2010). *TrendLabs Malware Blog*. "Trend Micro 2011 Threat Predictions." <http://blog.trendmicro.com/trend-micro-2011-threat-predictions/> (Retrieved March 2011).

- Internal Revenue Service. (December 14, 2010). *IRS.gov*. "EFTPS: A Secure Way to Pay All Your Federal Taxes." <http://www.irs.gov/efile/article/0,,id=98005,00.html> (Retrieved March 2011).
- Jake Soriano. (February 6, 2008). *TrendLabs Malware Blog*. "IRS Used by Spammers Again." <http://blog.trendmicro.com/irs-used-by-spammers-again/> (Retrieved March 2011).
- Jovi Umawing. (May 23, 2008). *TrendLabs Malware Blog*. "Then Subpoenas, Now Tax Petitions." <http://blog.trendmicro.com/then-subpoenas-now-tax-petitions/> (Retrieved March 2011).
- Macky Cruz. (April 17, 2008). *TrendLabs Malware Blog*. "Bogus Subpoena Serves Up Trojans." <http://blog.trendmicro.com/bogus-subpoena-serves-up-trojans/> (Retrieved March 2011).
- Maria Alarcon. (April 22, 2009). *TrendLabs Malware Blog*. "Fake Form W-8BEN Used in IRS Tax Scams." <http://blog.trendmicro.com/fake-form-w-8ben-used-in-irs-tax-scams/> (Retrieved March 2011).
- Mary Ermitaño. (January 11, 2010). *TrendLabs Malware Blog*. "Bogus IRS W-2 Form Leads to Malware." <http://blog.trendmicro.com/bogus-irs-w-2-form-leads-to-malware/> (Retrieved March 2011).
- Mary Ermitaño. (April 7, 2009). *TrendLabs Malware Blog*. "Tax Season Is Phishing Season." <http://blog.trendmicro.com/tax-season-is-phishing-season/> (Retrieved March 2011).
- Paul Ferguson. (April 8, 2008). *TrendLabs Malware Blog*. "More IRS Malware: As the U.S. Tax Deadline Looms, Cybercriminals Ramp Up." <http://blog.trendmicro.com/more-irs-malware-as-us-tax-deadline-looms-cyber-criminals-ramp-up/> (Retrieved March 2011).
- Ryan Certeza. (March 2011). *Threat Encyclopedia*. "Social Engineering Facilitates Tax Season Malware Attacks." <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Social+Engineering+Facilitates+Tax+Season+Malware+Attacks> (Retrieved March 2011).
- Threat Research Team. (March 2010). *TrendWatch*. "ZueS: A Persistent Criminal Enterprise." <http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf> (Retrieved March 2011).
- Trend Micro Incorporated. (February 18, 2011). *Threat Encyclopedia*. "TSPY_ZBOT.SMHA." http://about-threats.trendmicro.com/malware.aspx?language=us&name=TSPY_ZBOT.SMHA (Retrieved March 2011).
- Trend Micro Incorporated. (January 6, 2010). *Threat Encyclopedia*. "BKDR_POISON.BQA." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=BKDR_POISON.BQA (Retrieved March 2011).

- Trend Micro Incorporated. (November 6, 2009). *Threat Encyclopedia*. "TSPY_ZBOT.BZJ." http://about-threats.trendmicro.com/ArchiveGrayware.aspx?language=us&name=TSPY_ZBOT.BZJ (Retrieved March 2011).
- Trend Micro Incorporated. (September 15, 2009). *Threat Encyclopedia*. "TSPY_ZBOT.BZT." http://about-threats.trendmicro.com/ArchiveGrayware.aspx?language=us&name=TSPY_ZBOT.BZT (Retrieved March 2011).
- Trend Micro Incorporated. (September 14, 2009). *Threat Encyclopedia*. "TSPY_ZBOT.BZS." http://about-threats.trendmicro.com/ArchiveGrayware.aspx?language=us&name=TSPY_ZBOT.BZS (Retrieved March 2011).
- Trend Micro Incorporated. (May 7, 2009). *Threat Encyclopedia*. "TSPY_ZBOT.COB." http://about-threats.trendmicro.com/ArchiveGrayware.aspx?language=us&name=TSPY_ZBOT.COB (Retrieved March 2011).
- Verna Sagum. (August 1, 2008). *TrendLabs Malware Blog*. "Phishers Hit Multiple Banks with One Stone." <http://blog.trendmicro.com/phishers-hit-multiple-banks-with-one-stone/> (Retrieved March 2011).
- Trend Micro Incorporated. (April 15, 2008). *Threat Encyclopedia*. "TROJ_AGENT.AMAL." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_AGENT.AMAL (Retrieved March 2011).