February 2014
Feature Article: Phishing Scam Update

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Phishing Scam Update 3

ESET Corporate News 5

The Top Ten Threats 9

Top Ten Threats at a Glance (graph) 13

About ESET 14

Additional Resources 14

Phishing Scam Update

David Harley, ESET North America
Urban Schrott, ESET Ireland

It may seem at the moment that I don’t write about anything apart from phishing scams and tech support scams. That’s not actually the case, but scammers don’t seem to take holidays, and a couple of things have come along that I couldn’t resist mentioning.
The first has the subject “RBS - Working to protect you and your card.” It appears to come from CreditCardOnlineServices(at)cards.rbs.co.uk.

RBS Credit Card Account Holder:

Your RBS Credit Card is designed to help keep you safe

Receive alerts when we spot a suspicious transaction

Sometimes we spot what looks like a fraudulent transaction on your credit card - so to make sure, we’ll call you and check. Better still, why not join our free fraud text alert service?

It’s just another way we’re working to keep your card and your money safe.

*To sign-up for this service, simply visit our **fraud text alert website**.*

Why is this interesting? Well, there are a couple of things here that indicate a scam.

- The giveaway absence of personalization – if you’re one of a financial institution’s customers, there’s no excuse for not addressing you by name and proving that they know something about you that a scammer wouldn’t.
- We’ve neutralized the link to the so-called text alert website, but it led to a site that had nothing to do with RBS or even the UK – it appeared to have a Swedish domain name – and actually contained other pages masquerading as other banks.

Apart from that – and the fact that I don’t have an RBS card! – there isn’t much here to indicate to the average user that it’s a scam. The English isn’t ‘foreign’ and does a good job of capturing the tone of a chatty advertising mailshot.

And here’s another one from ‘Lloyds’. Bizarrely, though at first sight the sender appears to be Lloyds Personal Banking, the actual mail address is toilet@ebay.com. It pays to check the mailbox address as well as the display name (Lloyds Personal Banking in this case), even though there’s no guarantee that the address used is a genuine address.

Resolving An Issue With Your Account

Dear Valued Customer

We need your help resolving an issue with your account. To give us to to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

How you can help

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions.

To help us with this and to find out what you can and can't do with your account until the issue is resolved.click on the ink *below to resolve issue*

Log in here to resolve issue.

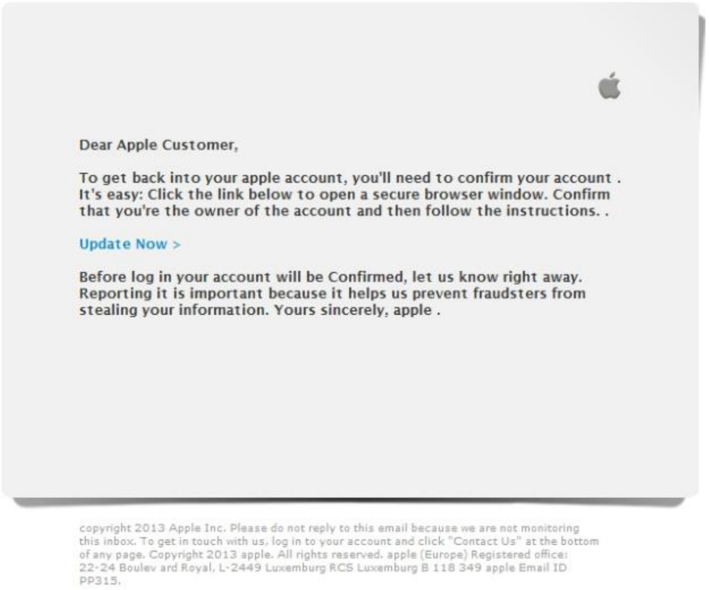
Sincerely,
Lloyds Bank

This one also lacks personalization and also links to a URL with no connection to Lloyds or the UK. The proofreader was a bit slack, too – "click on the ink below…" – and the English is a little more – well, unEnglish… Still, it's noticeable that the scammer was aiming for the same chattier, more idiomatic style, and there's some novelty to that.

Meanwhile, my colleague Urban Schrott has been writing for ESET Ireland about scams that have crossed his radar. While there's no disputing the lengths Apple goes to defend its customers from security threats, it's not possible for an operating system provider or security vendor to provide absolute protection for the user of *any* platform or security software from his own lack of caution. As Urban points out, if users are overconfident of the absolute security of their computing environment, "…that confidence can work against them when it comes to social engineering, particularly phishing, as they tend to trust "official" looking websites more [than they should] and cybercriminals know and abuse this to the maximum.

As an example, he describes how a very realistic looking phishing email is being received by Irish users, using the usual Apple visual clues and leading to a faked ITunes Connect login site at an address is that several security vendors have noted is associated with malware distribution, and which harvests users' iTunes login details. He notes that it "still lets you in if you enter any made-up nonsense though."
The prospective victim (addressed generically, of course, as 'Dear Apple Customer', is told that "in order to get back into your apple account, you'll need to confirm your account. It's easy: Click the link below to open a secure browser window. Confirm that you're the owner of the account and then follow the instructions. ."

While the mail looks fairly realistic (with an Apple logo and so on) there are one or two details that you might have spotted. The failure to capitalize Apple; a couple of proofing errors (the unfortunate space between 'account' and the following period character, two period characters separated by a space character at the end of the paragraph; and the capitalized Click after a colon, which is common US usage, but not common in the UK or Ireland.



Dear Apple Customer,

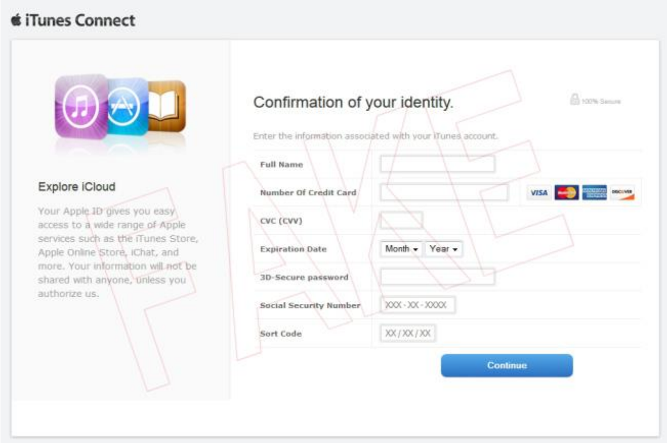
To get back into your apple account, you'll need to confirm your account . It's easy: Click the link below to open a secure browser window. Confirm that you're the owner of the account and then follow the instructions. .

Update Now >

Before log in your account will be Confirmed, let us know right away. Reporting it is important because it helps us prevent fraudsters from stealing your information. Yours sincerely, apple .

copyright 2013 Apple Inc. Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page. Copyright 2013 apple. All rights reserved. apple (Europe) Registered office: 22-24 Boulev ard Royal, L-2449 Luxemburg RCS Luxemburg B 118 349 apple Email ID PP315.

The fake iTunes Connect login is even more US-centric. Once "logged in", the page asks you to "confirm" many of your personal details, including your credit card number and security code, your password and sort code, but also your Social Security number. Are there that many Americans in Ireland, I wonder? ☺



iTunes Connect

Explore iCloud

Your Apple ID gives you easy access to a wide range of Apple services such as the iTunes Store, Apple Online Store, iChat, and more. Your information will not be shared with anyone, unless you authorize us.

Confirmation of your identity.

100% Secure

Enter the information associated with your iTunes account.

Full Name

Number Of Credit Card

CVC (CVV)

Expiration Date: Month ▾ Year ▾

3D-Secure password

Social Security Number: XXX - XX - XXXX

Sort Code: XX / XX / XX

Urban advises:

Even though Apple would ***never*** *ask their users for any of this information via email and warns exactly against such phishing on their support website, many users are still convinced by the look and feel of the site.*

If anyone has entered their login details, they handed them over to the cybercriminals and should therefore change them immediately. If they supplied them with any additional information, such as their credit card details, they should cancel their card and make all other steps to limit the potential damage of having revealed their sensitive information.

Apple's website includes some useful advice about being cautious about what information you share by email or via a link in unverified email, and Urban also cites Apple's advice on identifying email fraud.

ESET Corporate News

ESET Issues Warning About Mac Malware Disguised as Cracked Versions of Angry Birds, Pixelmator and Other Top Apps

ESET® is warning Mac® users not to download pirated software from file-sharing peer-to-peer (P2P) networks in the wake of a new malware discovery. Researchers have discovered a Bitcoin-stealing malware called OSX/CoinThief being spread via cracked apps, apps often obtained by over-riding Apple's standard security settings.

The OSX/CoinThief Trojan infects computers running Mac OS X®, stealing login credentials related to various Bitcoin exchanges and wallet sites by installing malicious browser add-ons.

ESET malware experts have discovered that CoinThief is being spread via P2P file-sharing networks, disguised as cracked versions of the following popular Mac OS X applications:

- BBEdit – an OS X text editor
- Pixelmator – a graphics editor
- Angry Birds – a game where players use a slingshot to launch birds at their targets
- Delicious Library – a media cataloguing application

"The hackers behind the CoinThief Trojan are trying to cash in on the current Bitcoin craze and fluctuating exchange rates by breaking into users' digital wallets," said security researcher Graham Cluley, who wrote about the threat on the ESET Blog. "As ESET's research team has shown, Mac users who download and install pirated software from torrent sites are not only depriving developers of their rightful income, but are also putting their computers and finances at risk."

According to detection statistics gathered by the ESET Live Grid™, the threat is mostly active amongst Mac users based in the United States. CoinThief was first spotted earlier this month by SecureMac researchers, who found it had been distributed via popular download sites, such as Download.com and MacUpdate.com, disguised as trojanized versions of Bitcoin Ticker TTM (To The Moon), BitVanity, StealthBit and Litecoin Ticker.

ESET researchers strongly recommend that all Mac users protect their computers with an up-to-date antivirus product and resist the temptation to download cracked and pirated software.

For more information on the CoinThief malware and how to clean infected devices, visit the ESET Blog.

ESET Announces the Newest Version of ESET Secure Authentication

ESET® launched the newest version of ESET Secure Authentication. The updated two-factor authentication (2FA) application continues to provide the potent combination of ultra-secure access to online applications, while introducing even greater ease of installation and support for a superior overall user experience. The added integration flexibility provided by the Software Development Kit (SDK) and API extends protection to a wider range of applications and data, making ESET Secure Authentication one of the most compelling 2FA solutions on the market.

Standard password authentication simply requires a user's password to access a given service or device. Two-factor Authentication requires two elements: a user's password and a one-time-password (OTP) which is generated on a physical device. Should the user's password be compromised, a criminal will not gain access to your network without having the complementary device.

The first version of ESET Secure Authentication was released in 2013 and proved that strong multi-factor protection is a critical component when protecting today's companies from potential damage brought on by a successful cyber attack. This simple and highly efficient application makes use of remote end-users' mobile devices to deliver a one-time password (OTP) when they connect to company networks, providing added security to the network and the device. The associated loss or theft of sensitive data, subsequent brand erosion and revenue impact can cripple a business of any size. Adding secure validation to weak and static user passwords and unsecured remote access makes businesses of all sizes dramatically less of a potential target for cyber criminals.

"We're excited to offer our next generation ESET Secure Authentication solution for companies implementing a comprehensive security strategy. Businesses of all sizes will enjoy the same easy installation, simple set-up and minimal system footprint found in all ESET products," said Andrew Lee, CEO, ESET North America. "For ESA 2.0 we have significantly improved the overall user experience and support to offer a lightweight mobile 2FA app that deploys across the most popular mobile operating systems."

With this new release, ESET provides ultra-secure access to business critical applications, such as Microsoft SharePoint Server® and Microsoft Dynamics®. Furthermore, all communication between the client-side authentication servers and the ESET Secure Authentication provisioning server is encrypted using TLS (Transport Layer Security). ESET Secure Authentication also includes PIN protection to guard against fraud in the case of loss or theft.

For more information, and full list of key features and benefits, please visit: http://www.eset.com/us/business/products/secure-authentication/

The newest version of ESET Secure Authentication is currently available, through sales, installation and support services with ESET channel partners in local markets across North America, Canada and the Caribbean. To view a live demonstration of ESET Secure Authentication during the RSA conference, please visit ESET at booth #1926.

Security veteran Graham Cluley joins ESET's WeLiveSecurity.com

ESET announces that independent security veteran Graham Cluley is joining ESET's WeLiveSecurity.com editorial team to write articles on the latest security news and research, providing opinion and advice to readers of WeLiveSecurity. ESET is also broadening its global reach by offering Spanish speakers a native version of WeLiveSecurity from ESET Latin American lab at www.welivesecurity.com/la-es.

ESET's WeLiveSecurity has enjoyed a 60% increase in traffic since April of last year. Over 450 articles were published on the site in 2013, attracting over a million page views. Backed by ESET's network of security expertise, WeLiveSecurity.com publishes security news daily, as well as how-tos, papers, videos and podcasts. The site's content attracts audiences from the "security curious" to the "security savvy," providing tips on topics such as how to remove adware from your computer and publishing deep-dive research on the latest threats.

"WeLiveSecurity continues to deliver industry-leading security news and research for our growing community of readers," said Andrew Lee, CEO, ESET North America. "In 2014, we are expanding our voice by adding veteran IT security professional Graham Cluley to our team as well as offering our Spanish-speaking community access to this world-class security news resource with the launch of WeLiveSecurity En Espanol."

Graham Cluley is one of the security world's most well-known voices, making regular appearances in the media sharing his opinions on the latest security threats. He has worked in the computer security industry since the early 1990s, having been employed by a number of companies including Dr. Solomon's, McAfee and, most recently, Sophos, where he acted as Senior Technology Consultant and Naked Security's main writer, before becoming an independent consultant last year.

"Antivirus software and security updates go a long way to protect millions of computers around the world from infection and hacker attacks," said Cluley. "But the other half of the equation is to ensure that users are properly educated about the latest threats, with timely common-sense advice. WeLiveSecurity has an experienced team of experts sharing information with readers on a daily basis, and I'm tickled pink to add my voice to theirs."

After months of development and testing, the Latin American Spanish-language version of ESET's www.welivesecurity.com/la-es has now gone live. Over the last 10 years, the security company has built a strong brand in Spain and Latin America. The latest research* shows that one out of every two people in these regions recognize the ESET brand.

With an established foothold in the region, ESET wants to show its commitment to these regions by offering security best practices, easy access to the in-depth research, as well as the latest security news and advice.

"I've looked after ESET's Latin American market for almost a decade, and I am so proud of what we have achieved so far," said Ignacio Sbampato, Chief Sales and Marketing Officer at ESET. "Not only have we built a strong local presence across the region, ESET has never wavered from delivering award-winning products, service and support. This launch of www.welivesecurity.com/la-es is further evidence of our commitment to our Spanish-speaking community by providing free computer news, opinion and education."

New ESET Multi-Device Security Packs Offer Comprehensive Protection with Easy Setup

ESET announced the availability of ESET® Multi-Device Security Pack. The bundled offerings include multiple ESET products to provide comprehensive proactive protection across multiple devices and operating systems.

"ESET recognizes that the IT needs of individuals are not the same, and with that in mind set out to create a flexible, all-in-one security offering that could protect multiple operating systems across their mix of desktop and mobile devices," said Andrew Lee, CEO, ESET North America. "As a result, ESET Multi-Device Security Pack offers comprehensive protection with an easy set up at an affordable cost."

ESET Multi-Device Security Packs provide protection and flexibility, especially for families or single users having more than one device they need to cover with an AV solution. With one license, customers can activate any ESET consumer product, desktop or mobile, depending on their needs. Current ESET customers are eligible to upgrade to the ESET Multi-Device Security Packs from any product and complete protection for their entire home or small office, whether it includes PCs, Macs or Android devices.

For more information on the new Multi-Device Security Packs, please visit: www.eset.com/us/home/products/multi-device-security/

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 2.9%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address, and it tries to download several files from the address. The files are then executed and the HTTP protocol is used. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

2. LNK/Agent.AK

Previous Ranking: 5
Percentage Detected: 1.86%

LNK/Agent.AK is a link that concatenates commands to run the real or legitimate application/folder and, additionaly runs the threat in the background. It could become the new version of the autorun.inf threat. This vulnerability was known as Stuxnet was discovered, as it was one of four that threat vulnerabilities executed.

3. Win32/Sality

Previous Ranking: 2
Percentage Detected: 1.67%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

4. INF/Autorun

Previous Ranking: 4
Percentage Detected: 1.57%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

5. Win32/Qhost

Previous Ranking: 9
Percentage Detected: 1.55%

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

6. HTML/ScrInject

Previous Ranking: 3
Percentage Detected: 1.54%

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

7. Win32/Ramnit

Previous Ranking: 6
Percentage Detected: 1.27%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

8. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.26%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This treat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145.

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders.

9. Win32/Dorkbot

Previous Ranking: 10
Percentage Detected: 1.1%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX. The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

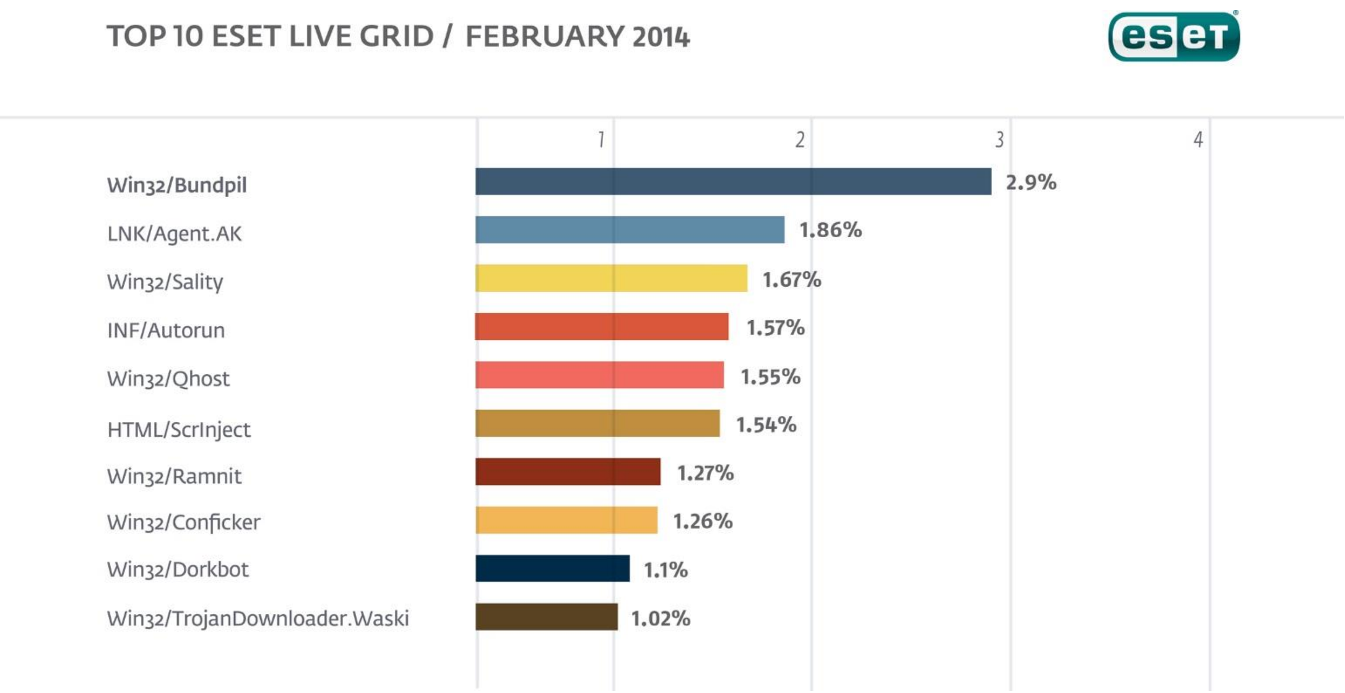
10. Win32/TrojanDownloader.Waski

Previous Ranking: n/a
Percentage Detected: 1.02%

Win32/TrojanDownloader.Waski is a trojan which tries to download other malware from the Internet. It contains a list of two URLs and tries to download a file from the addresses. The HTTP protocol is used. The file is stored in the location %temp%\miy.exe, and is then executed.

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 almost 2.9% of the total, was scored by the Win32/Bundpil 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
- WeLiveSecurity
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation

ENJOY SAFER TECHNOLOGY™