Global threat report

November 2012
Feature Article: Deck the Halls with Hoaxes and Holly

ESET

Table of Contents

Deck the Halls with Hoaxes and Holly

David Harley, ESET Senior Research Fellow

It's been a while since I've talked about hoaxes (here or anywhere else), but they haven't gone away, even if we don't see many of the stories about catastrophic, undetectable viruses any more. Here are three old favourites that have hit my radar recently by email or via Facebook. (Many antique hoaxes have taken on a new lease of life by migrating from email to Facebook.)

Since I haven't discussed these for a while, maybe I should explain that by hoaxes I mean false information (usually circulated by chain letter, chain email, or the social media equivalent such as re-tweets or Facebook Likes). Most of the people who forward it do so innocently, if incautiously: they don't intend to mislead. However, somewhere in the lifetime of such a hoax, someone did send out false information, often with no obvious motive except maybe to bolster their own poor self-image by making fools of other people. I don't include out-and-out scams like phishing and 419s in this category of nuisance: some people do, but I think that's just confusing.

I also use the classification semi-hoax for some chain messages: these are messages that may not be completely false, but at some point they've been represented or modified – deliberately or through misunderstanding – in such a way that the real facts are concealed or distorted.

Post Haste

I've seen this first example of a semi-hoax a couple of times this year, but it's been turning up regularly (especially at this time of year) for several years.

It claims that a warning is being circulated by or on behalf of Royal Mail (the UK's primary postal service), the Trading Standards Office, or ICSTIS (now PhonepayPlus, the body that regulates premium rate phone services in the UK. The scam is described as follows, or in similar terms:

> A card is posted through your door from a company called PDS (Parcel Delivery Service) suggesting that they were unable to deliver a parcel and that you need to contact them on 0906 6611911 (a Premium rate number).

I describe this as a semi-hoax because there is a certain amount of truth in it. There *was* a scam intended to trick people into ringing a premium rate service in Belize associated with that number. However, the number was killed off at the end of 2005 (and the company behind it was fined £10,000), and claims that just ringing the number results in your being charged £315 or even £15 are sheer embroidery. The service rate was £1.50 a minute, and 090 premium rates currently cost UK phone subscribers a maximum of £1.65 per minute (£2.55 for mobile phone calls). The hoax continues:

> If you do receive a card with these details, then please contact Royal Mail Fraud on 020 7239 6655.

Well, it's beyond unlikely that you'll receive a card with those details, but if you do receive something similar, that's not the number to ring: instead, you can ring Action Fraud at the numbers listed here. Though I'd think that you'd be more to receive a scam message by email or as an SMS text message than shoved through your letterbox.

PhonepayPlus's own statement on the hoax can be found here, and the Crime Stoppers web site lists it here. Premium rates and the number prefixes used vary from country to country, but information on UK premium numbers and the rates they attract is available here.

I've never seen this particular story outside the UK, which doesn't mean it doesn't happen: it's actually quite common for hoaxes to be 'translated' from one country to another. In the US and elsewhere, there have been many alarmist tales of cell-phone numbers that you shouldn't answer because if you do you'll be switched to a premium rate service. (Service providers generally deny that it's possible for an incoming call to be switched in this way to a chargeable, outgoing call.) This doesn't mean that there aren't current scams based on premium rate services, though.

Wangiri scam calls (wangiri is a Japanese term meaning something like "one ring and cut") work by using software to ring random numbers, especially mobile phone numbers, and dropping the call after one ring. The scammer hopes that the victim will notice the missed number and ring it back, not realizing that they'll be calling a premium-rate number. Variations on this theme include calls that play a recorded message when the call is answered. While the message may implement a range of scams, one common gambit is to offer a prize, some kind of rebate, or some other incentive, to persuade the hopeful victim to call a premium rate number. Preferably an offshore number, since the illicit profit is likely to be greater.

Our friends at ESET Latin America noted recently that malware for Android devices detected in Latin America is dominated by programs like Boxer, an SMS Trojan that covertly subscribes the victim to a premium rate SMS number.

A Load of (Red) Bull

This is an out-and-out hoax: it may have originated in some sort of misunderstanding, but if so, it has been overlaid by so many layers of misinformation and deception that it reads to a practised eye as sheer fiction.

The chain message claims the Red Bull energy drink contains a synthetic stimulant banned in some parts of the world (the version I'm looking at mentions France and Denmark) which is alleged to be associated with a range of conditions from migraine to brain tumours and cerebral haemorrhage to liver damage. Some versions of the hoax claim that Glucuronolactone was developed by the US Department of Defense to raise morale among trips in Vietnam.

In fact, Glucuronolactone is a naturally occurring component of connective tissue that metabolizes innocuously in the human body and both it and taurine (also an ingredient of Red Bull) are commonly found in food. Glucuronolactone is often found in energy drinks in relatively high concentrations, but I've been unable to find any verifiable evidence of confirmed risk. The assertion that the drink has just been banned in France and Norway are probably associated with the fact that the drink was at one time banned in France and some parts of Scandinavia due to concerns about its caffeine and/or taurine content.

There is, of course, always a possibility when a particular brand is the target of a hoax impugning its reputation that it originates with a competitor. There is, however, no evidence (as far as I know) that this is the case here.

Ironically, given that the drink is claimed to be associated with migraine, someone I know claims that Red Bull – with or without vodka – helps her recover faster from a migraine attack. I'm not aware that there's any proven medical basis for that assertion, but it's a good excuse for splicing the mainbrace, I suppose. ;-)

A Nail in your Coughing

Finally, here's a health-related semi-hoax that might actually be bad for your health, though in a context where your health is at risk anyway.

The claim is that if you have a heart attack when you're on your own and can't immediately get help, you can help yourself 'by coughing repeatedly and very vigorously.'

There is, in fact, a technique called 'cough CPR': however, it's by no means universally used and only in restricted circumstances (in emergency situations and under medical supervision): nor is the technique generally considered appropriate for most types of heart attack.

In its most usual form, (I've also seen it in the form of a Powerpoint presentation) the chain message claims authenticity from the alleged endorsement of Rochester General Hospital and Mended Hearts, a heart attack victims' support group. In fact, there seems to be no evidence that it was ever endorsed by Rochester General Hospital. And while the message reproduces text that was apparently first published in a Mended Hearts newsletter, the organization later retracted it, and has published a statement that asserts that 'Coughing Won't Fend Off a Heart Attack.'

It sounds as if using the technique inappropriately and incorrectly could be dangerous, even fatal.

Ironically, I first came upon this story when it was distributed among a group of information security professionals working for the UK's National Health Service...

Further Information and Resources

- Common Hoaxes and Chain Letters: a white paper by David Harley
- Whatever Happened to the Unlikely Lads? A Hoaxing Metamorphosis: a conference paper for Virus Bulletin 2009
- About.com Urban Legends page: http://www.urbanlegends.about.com/
- Chain letter information page (lots of links and information on pyramid-type chain letters) http://www.cs.rutgers.edu/%7Ewatrous/chain-letters.html
- Hoaxbusters.org "The Big List": http://hoaxbusters.org/
- Korova"Hoax du Jour": http://www.korova.com/virus/hoax.htm
- TruthOrFiction.com: http://www.truthorfiction.com/
- Urban legends page: http://www.snopes.com/

Safer cyber-shopping makes for happier holidays: 12 simple safety tips

The 2012 holiday shopping season is fast approaching and digital devices are sure to play a bigger role in the holiday shopping process than ever before, from pre-purchase research on the home or office computer, to in-store price checking on the smartphone. And of course, online holiday shopping is available 7×24, from before Black Friday, through Cyber Monday, all the way to end-of-year clearances and New Year Sales.

Holiday shopperAbout a year ago we blogged 10 tips for safer holiday shopping online and that blog post proved to be very popular. We are back this year with the same tips, plus two bonus tips. We hope you find them helpful.

Please feel free to share these tips with any friends and family who are planning to do their holiday shopping digitally this season. You can even go old school and hand them a printed copy of ESET's Guide to Safer Cyber-Shopping 2012 (PDF). (With thanks to Cameron Camp, Aryeh Goretsky, and David Harley who provided tips and input along the way.)

- **Tune your shopping machine:** Like the tune-up your car gets before a long drive to deliver holiday gifts to relatives, your laptop may need attention before going online for some power shopping. Give it some love, and improved protection, by updating and patching your browser, operating system, and anti-malware suite. Patching will help you avoid malware infections and scams, and keep you running smoothly throughout the season, and it's free. (You can run a free antivirus scan of your Windows PC at www.eset.com/online-scanner .)

- **Stick with familiar faces:** Buy from websites that have established a reputation for doing what they say, providing accurate descriptions of merchandise, and delivering it in good shape and on time. When you're getting down to the wire with shipping deadlines, the last thing you need is friends and relatives getting the wrong gifts, which could be worse than no gifts at all.

- **Be wary of AMAZING deals:** If a deal looks too good to be true, it probably is, particularly if it's an amazing offer on one of the hottest products of the season. Such deals can be very tempting, but it really is safer to avoid following links that offer goods, services, or gift cards at impossibly cheap prices, they are just too risky. Not all discount vendors are scammers, but ask yourself if the promised savings are worth the gamble (or Google the offer and/or vendor to see what others are saying).

- **Insist on secure transactions**: When you are in the ordering process on a website check to make sure it is using SSL, the standard in secure transactions that shows up in several ways. You should be able to see https in front of the web address instead of http. There may also be a lock or key symbol in the browser window as well. Using SSL encrypts the exchange of information, such as your credit card, so eavesdroppers cannot read it. When in doubt, a quick search in Google for the word "scam" or "fraud" along with the site name should tell you if that site has a history of problems.

- **Think before you act:** Watch out for URGENT deals that arrive in unsolicited email or purport to be from friends on social networking sites. Exercise extra caution if the message uses broken English (or whatever your native language might be) or if it doesn't seem quite right for some reason (like an unexpected email from a delivery service with an attachment). If you think the deal is real, open a browser and type the name of the website directly into the address bar. This will keep you from getting swept away by scam links to fake websites built by cyber crooks that harvest your information and spirit it off to the underworld (there is a thriving black market in stolen identity data which crooks purchase to commit credit card fraught, tax fraud, and other crimes).

- **Don't shop at a leaky hotspot:** If you need to do any shopping over Wi-Fi, at home or at a hotspot, make sure it is secure (look for the lock symbol in the Wi-Fi connection dialog). The last thing you want is someone snatching your personal and financial details out of thin air as you transmit them from your laptop (or smartphone or tablet). When using Wi-Fi outside your home consider using a VPN or virtual private network such as PrivateTunnel or Private WiFi (bear in mind that there are bandwidth limits on most free VPNs so you may need to pay for heavy use).

- **Use credit instead of debit:** If you get scammed and try to get your money back you may have better luck with credit card transactions versus debit cards. While some vendors, whether at the mall or online, prefer debit cards because the transaction is cheaper for them, avoid this when holiday shopping. Credit cards can put an extra layer of protection in between you and the bad guys.

- **Question detailed info requests**: Some malware is able to add questions to forms you use online, so if a shopping website is asking for Too Much Information relative to your purchase, like wanting your Social Security Number to complete a simple order for flowers, abandon the transaction and run an anti-malware scan right away.

- **Don't expect money for answering questions:** There are many legitimate website satisfaction surveys, but when a window pops up promising you cash or gift cards just for answering a simple survey like "Do you use the Internet?" close it and move on. And do NOT enter your cell phone number to claim the $1,000 gift card that a website is promising you, unless you are prepared to pay for premium services you never ordered.

- **Stay awake after the holidays:** When New Year lull sets in, there's a tendency to avoid looking at the credit card statements arriving by mail (or email). Maybe you're hoping you didn't spend as much as you THINK you may have. But if you got scammed, that statement may be the first sign, so at least skim the statement to see if there are any transactions you don't recognize. For example, if you have never been to Russia and don't know anyone who lives on the outskirts of Moscow, it's a safe bet that any wire transfers to the region are fraudulent, and the sooner you act, the more likely you are to recover your money.

- **Lock up your devices:** Password protect your laptop, tablet, and smartphone so that, if lost or stolen, your data will be harder for strangers to access. Each of these devices should have a settings menu from which the security options should be readily accessible. Choose a password or code that is easy for you to remember but hard for other people to guess. Set the timing so that the device locks after a short period of inactivity. You are now better protected against multiple scary holiday scenarios, such as leaving your device in a taxi or on the plane, someone stealing your device, or a friend "borrowing" your device and then using it inappropriately.

- **Backup your data:** If you have to face a worst-case scenario this holiday season, like a laptop going missing or a smartphone being stolen, the situation will be a lot less upsetting if you have your device backed up, that is, copies of your files safely stored somewhere else. Your smartphone is probably backed up to your computer already–now is the time to check–and your computer can be backed up to an external hard drive, or online backup such as BackBlaze, but preferably both.

Follow these tips and you should sleep a little better during the holiday shopping season. Remember, as in life, there are online deals that can seem too good to be true, and probably more of them during the holiday shopping season. A cautious and skeptical approach may sound boring, but it can pay off. After all, if you feel you don't have enough time to get your shopping done, you certainly don't have time to deal with fraudulent charges, flaky deals, or stolen data.

Windows 8: there's more to security than the Operating System

David Harley, ESET Senior Research Fellow

There are things almost as certain as death and taxes: crime is one of them. And there are certain events that always seem to trigger certain kinds of cybercrime. One is disaster, natural or man-made. So my colleague Urban Schrott has called attention to the likelihood of scams piggybacking the serious impact of 'Superstorm' Sandy on the East Coast of the US, and the FTC has some good advice on spotting charity scams. And this type of scam has been addressed in the Threatblog quite a lot before, so I won't go belabour the point about Sandy-related 419s, phishing attacks, Blackhat SEO, and even out-and-out hoaxes with no apparent cash motive. This graphic, featured in Urban's blog, is actually a doctored still from the disaster movie The Day After Tomorrow, and the Huffington Post noted last week that the number of sites registered with names potentially associated with the hurricane had already reached 1,100.

Then there's the release of new technology. We tend to expect to see all significant new technology become the subject of social engineering attacks, though personally I would not be at all disappointed if that failed to happen for once. But I'm not holding my breath. We've already seen scams specific to the new iPad mini (but 'free iPad' scams via Facebook apps, email, SMS and so on, are a persistent feature of the threatscape, not surprisingly given the popularity of tablets in general and that particular product specifically). Then there's Windows 8. While I agree with Aryeh that there are lots of good things in the latest version of Windows, security-wise – I have to, as he's far more knowledgeable on Windows internals than I am! – the fact is that there is much more to being safe online than the operating system, though having a well-secured and maintained OS is no bad thing.

Secure as Windows 8 seems to be – though it's clear that the search for ways in which to compromise it has been underway since long before its public release, and there are already reports of exploits – it has already been used extensively for social engineering attacks of various kinds. Trend Micro has sounded the alarm on fake anti-virus passing itself off as a Win8-specific security program, and both Trend and Sophos have flagged email messages offering a 'free upgrade' to Windows 8.

However, the link in one such email takes you to a form that looks a lot like this. I got this screen capture yesterday, several days after the articles by our friends at Sophos and Trend Micro so it would seem the phishing scam, unlike the storm, has not yet passed. If you complete the form, your information is redirected to an unknown address. And you may notice that the form doesn't mention Windows 8: it's so generic that it could be used for almost any scam, with a little bit of careful social engineering in the initial phishing message. (The phish message flagged by Trend and Sophos is actually pretty unconvincing.)

But here's a slightly different angle of attack. Vicki, who quite often comments on our blogs, told me today that "…a friend of mine recently received a call from a female who sounded foreign … who claimed Microsoft was having them call everyone about a nasty virus all people with Windows 7 were experiencing…"

As it happens, I've heard about (and received) calls rather like that before. We've already mentioned here that support scammers from India used a spike in detections of Quervar/Dorifel in the Netherlands to offer 'help' to people in that region with disinfection, and I've received calls here in the UK from scammers who claimed that they could help me with a virus that was epidemic in this region, though they were unable to tell me which virus.

Can we expect scam calls like the one Vicki's friend received, offering help with a Windows 8 virus or perhaps with other Windows 8 problems? I don't know, but it's certainly far from impossible. As more people get to hear about the older forms of the scam, the scammers are likely to seek new variations, and it's a short step from 7 to 8…

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 4.61%

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, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. HTML/ScrInject.B

Previous Ranking: 4
Percentage Detected: 4.24%

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

3. Win32/Conficker

Previous Ranking: 3
Percentage Detected: 3.40%

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 threat 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. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

4. HTML/Iframe.B

Previous Ranking: 2
Percentage Detected: 2.08%

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

5. Win32/Qhost

Previous Ranking: 7
Percentage Detected: 1.87%

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. Win32/Sirefef

Previous Ranking: 5
Percentage Detected: 1.62%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

7. Win32/Dorkbot

Previous Ranking: 6
Percentage Detected: 1.51%

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.

8. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 8
Percentage Detected: 1.34%

It 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.

9. JS/Exploit.Pdfka

Previous Ranking: 16
Percentage Detected: 1.32%

JS/Exploit.Pdfka.PWN is a detection for specially crafted PDF files, which exploit the CVE-2009-0927 vulnerability. It is written in JavaScript. By exploiting this vulnerability, an attacker may be able to execute remote arbitrary code on a vulnerable system.

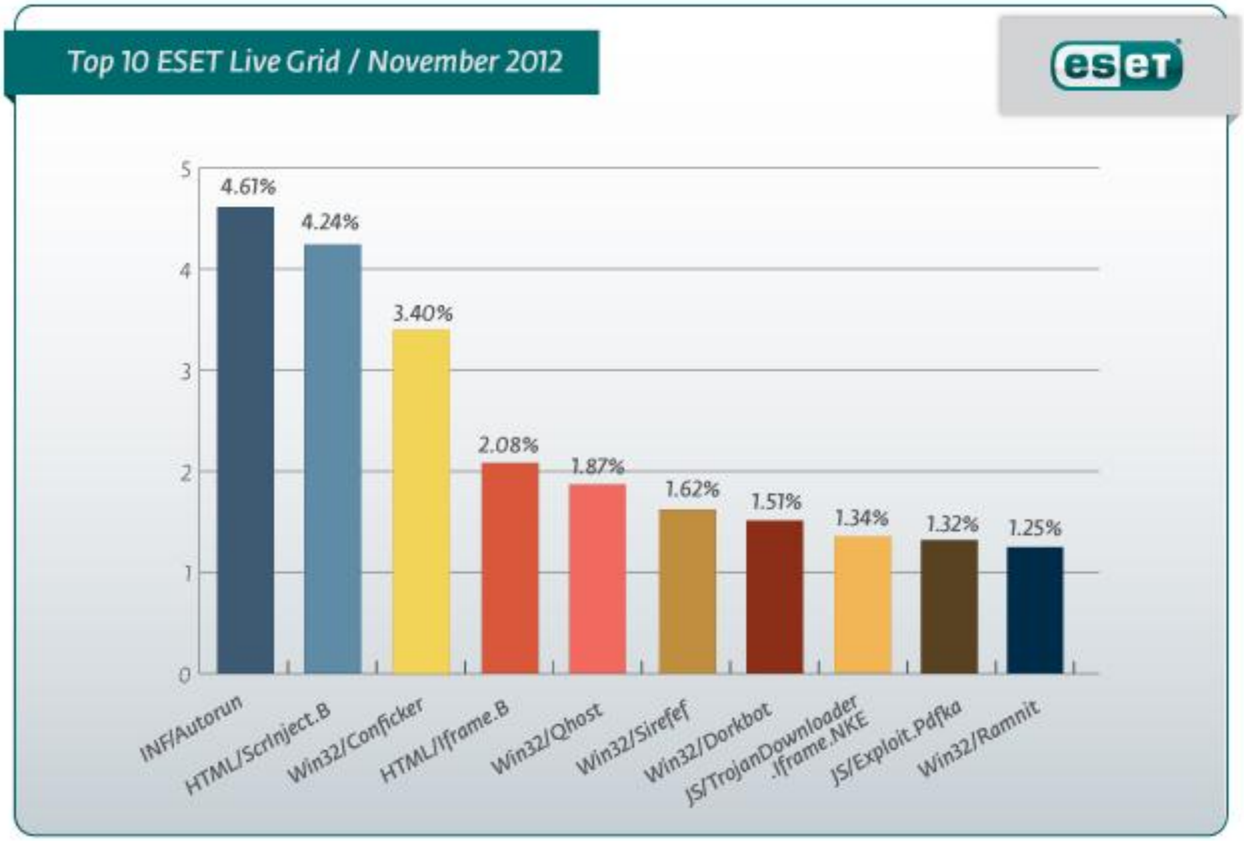
10. Win32/Ramnit

Previous Ranking: 10
Percentage Detected: 1.25%

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

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 4.61% of the total, was scored by the INF/Autorun class of threat.



About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

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
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation