July 2011

Feature Article: Real Men Don’t Do Safe Hex

Table of Contents

Real Men Don't Do Safe Hex

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Expressions based on puns about practicing Safe Hex – always use protection! – seems to have lost their popularity nowadays, even though security hygiene remains as important as sexual hygiene (though in very different contexts).

When an antivirus message pops up, do you do what it says or ignore it? Do you visit web pages flagged as dangerous by the antivirus? Do you run programs the antivirus recognizes as dangerous? These are the sort of questions ESET Ireland asked Irish computer users in their latest computer security survey carried out by Amarách research.

The results were a bit shocking, as it turns out that 34% of the surveyed computer users (n=1000) ignore the alerts their antivirus shows them. Furthermore, according to detailed demographic statistics:

- The worst (riskiest) behavior is displayed by a young male from the Dublin area (54% of age group 15-24, 35% of males and 41% in Dublin ignore warnings)

- The safest behavior is displayed by a female over 55 from Connaught or Ulster (only 23% of age group 55+, 33% of females, and 31% in the north ignore warnings)

- While 4% of the survey sample don't use **any** antivirus software at all. (8% of the young and 5% of Dubliners)

If the data collected in the survey are truly representative of the Irish population in general, they suggest that up to 1.2 million Irish computer users might be prepared to infect their computers **intentionally**. While women are proving more careful, a large percentage of young men won't be told what to do and will click on anything they please. This sort of behaviour results in thousands of lost documents, computer reinstallations, frustration and many wasted work hours. But, as David Harley observed in another article: "Surveys tell us a lot about attitudes, if they're well-designed, but they don't usually generate universally authoritative statistics in the context of populations this large."

As I commented elsewhere:

"The relation between risk factor and demographics implies that the more someone considers themselves an experienced computer user or feels 'they know what they are doing', which certainly would be the case with young urban males, the more they are willing to take the chance of getting infected, just to run that program or view that website they wanted, no matter how risky it could be. It may seem like a paradox, but less computer savvy users are treating security much more carefully. Because, unfortunately, no matter how good your antivirus program is, it serves little purpose if you ignore its warnings or reverse its security protocols."

David Harley remarked subsequently:

Years ago, when much of my job was 2nd/3rd line support, I'd regularly come across end users who wouldn't or couldn't update their antivirus. Then there were people who'd log a call for a virus-unconnected problem, but when I got there I'd routinely check their AV and find it was either disabled or even replaced with another product. And there were the real superstars who opened something apparently malicious just to see what would happen.

Urban's observations actually map to my own experience in corporate support. People who are slightly nervous about technology, follow recommended practices, and ask when they're not sure may ring the service desk more often, but their problems tend to be easier to solve. It's the self-styled guru who doesn't call for help until he's already trashed his system (or worse, someone else's) who is likeliest to have you spending your weekend rebuilding systems.

The Russia House

David Harley, ESET Senior Research Fellow

There's a lot of excellent research coming out of ESET Russia's labs these days, spearheaded by Aleksandr Matrosov and Eugene Rodionov. As readers of this newsletter, you're probably aware of the contribution they made to research into Stuxnet, though that contribution is sometimes underestimated by the media, as I discussed here very recently. Then there's their ongoing research into the TDSS malware family. The TDSS botnet, now in its 4th generation, is seriously sophisticated malware, and we recently revised their paper The Evolution of TDL: Conquering x64 to reflect the latest changes. Perhaps I can say "we" here: while it's a long time since I did much in the way of hands-on research myself, the guys in the labs in Russia and Slovakia graciously let me play Dr. Watson to their Sherlock Holmes, though in truth Watson contributed more as a chronicler than I do. Anyway, I was asked for a non-technical explanation of the significance of TDL4's shift to a peer-to-peer (P2P) model, so here it is again.

When a PC is infected by a bot, it becomes part of a network of other compromised machines which we call a botnet. So now the criminal who is managing the botnet needs to be able to issue instructions to the malware on each infected machine (zombie). And, of course, communication often needs to go the other way: depending on what the botnet is being used for, it may well have to return data to the "botmaster". A very common way of implementing two-way communication is by setting up some machines as "Command & Control" (C&C) server: this is a malicious version of the client/server model, where a single server may provide services to many client PCs. And it still works very well, but there is a drawback to this approach, as far as the criminals are concerned.

If we're able to trace and close down some or all of the C&C servers which are supplying information to the infected "zombie" PCs and telling them what to do, then we cut the head off the dragon: the zombies that rely on a server for their instructions are no longer able to carry out the wishes of the botmaster. (Or dragonmaster, if you prefer…)

Using the Kademilia P2P protocol, TDSS-infected machines are both client and server. All botnets use a perverted form of distributed processing, but this approach makes good use of distributed data, too. The information is shared between all the machines in the network. A compromised PC can get the information it needs from its neighbours, and it knows where they are because it keeps a sort of virtual phonebook hidden on the hard disk, only contacting the C&C server when the number of neighbouring nodes drops below ten (like a householder who realizes that his neighbours are all moving away and he needs to order a new telephone directory).

This doesn't make TDL4 invulnerable, by any means, but it does mean that it's harder to disable large swatches of the botnet at a stroke.

Unfortunately, the idea subsequently spread that the switch to P2P does make the botnet indestructible. Randy Abrams remarked:

"Calling the botnet indestructible is tantamount to calling the Internet unsustainable … I suspect that, in time, we'll discover the 'T' in TDL stands for 'Titanic,' and a currently unseen iceberg will sink it."

I agree that there's no such thing as an indestructible botnet, though this one may not be as susceptible to immediate takedown as Rustock, for example. However, TDSS has introduced new twists on old ideas like P2P networks and hiding malware – just as previous malware has used sectors marked as bad, slack space, or streams, TDL uses a hidden file system.

It's also very adaptive, and its use of Pay Per Install (PPI) business model rather like that used for distribution of browser toolbars via affiliates like DogmaMillions and GangstaBucks, as described in our article at, has been very effective - and so has ruthlessly eliminating some of the competition. But there is no indestructible malware.

More recently a cybercrime group called "Ready to Ride" has attracted their attention, by distributing malware of the Win32/Cycbot family. This group started in the fall last year, judging from the domain name registration date – readytoride.su was registered on 8th September 2010. Its primary activities were substitution (index hijacking) of search engine results (Google, Bing, Yahoo), and clickjacking. Although the "Ready to Ride" group originated in Russia it distributes Win32/Cycbot outside the borders of the Russian Federation. Going by the prices per installation (see figure 1) the primary target of the group is the US.

Win32/Cycbot is also distributed using a PPI (Pay Per Install) scheme, but doesn't currently use a P2P botnet model. To download the malicious executable each partner uses the URL it has paid for and after activation submits its current status to the C&C (Command and Control) server from which it gets its instructions. The C&C URLs are hardcoded into the Win32/Cycbot executable and are updated when a new version of Win32/Cycbot is downloaded. By means of injecting java script, diverting web searches, and modifying HTML code Cycbot is able to pass itself off as a user surfing web pages, so as to counteract systems intended to block clickjacking. It is able to modify the settings of the most popular browsers (Internet Explorer, Opera, Firefox). Win32/Cycbot is a multithreaded application and just a single instance of the bot can handle dozens of tasks, clicking advertisements or poisoning web searches.

Their latest discoveries relate to Win32/Hodprot, a malware family previously referred to in a presentation "Cybercrime in Russia: Trends and issues" delivered at CARO2011 by Robert Lipovsky, Aleksandr Matrosov and also Dmitry Volkov of Group-IB. (An excellent presentation, by the way: one of the best of the workshop, in my unbiased opinion…)

In each case of bank fraud connected with Win32/Hodprot, a great deal of money was stolen. On average each fraudulent operation pulls in several hundred thousand USD.

More interestingly, the Win32/Hodprot botnet is connected to other botnets working in the field of bank fraud in Russia. In particular, it is Win32/Hodprot that was used to download Win32.Sheldor, Win32/RDPdoor and Win32/Platcyber onto the victims' machines. The period of time when Win32/Sheldor and Win32/RDPdoor appear to have been most active matches that of Win32/Hodprot.

Taking into account its implementation details Win32/Hodprot is a very complex threat, designed to deeply penetrate into an infected system and stay hidden for a long time. The main modules of the malware are stored in the system registry

(HKLM\SOFTWARE\Settings) rather than being stored as files in the file system. This makes forensics much more difficult: it is very difficult to find the malicious payload as there is no corresponding file in the file system, and the payload relies on an intricate customized encryption algorithm. Win32/Hodprot uses advanced techniques to infect the system and stay hidden which distinguish it from other malware: the Russian lab will be releasing a detailed analysis of the threat shortly.

1 in 20 mobile devices infected next year?

The mobile devices of late have more compute power than the full desktop PC of yesterday year, and they fit it your pocket, great news for folks "on the go." And since you're so multi-tasked anyway, why not load it up with things to make your life easier; after all, it's really a phone with a few embellishments, right? During the app install (while you wait for the trolley) it asks inane questions about permissions, but you plow right through and get on the trolley, can't miss the trolley, right?

Problem is, many folks "on the go" carry more and more personal information on these handy devices, and eventually they have your whole life on them. I've turned around and driven miles back home to get my Android if I've forgotten it, we're glued to them. Turns out prying eyes have also figured this out, so now you can be robbed while in traffic, using nothing more than a malicious app. You download an app, use it a few times and forget it, or move on to the next one. But in the background, it's potentially harvesting the rich personal information you have typed, touched and tapped in, building a profile and sending it down the line to the highest bidder, all without you knowing.

A recent report from Trusteer points this out. According to their estimate, 1 in 20 mobile devices of various families will be infected with financial malware in the next 12 months, not too shabby for nasty hackers, very bad for the rest of us. According to Trusteer CEO Mickey Boodaei, "Fraudsters have all the tools they need to effectively turn mobile malware into the biggest customer security problem we've ever seen. They are lacking just one thing – customer adoption." But don't worry, customers are snapping up the latest fangled mobile devices in droves, and moving their lives slowly (or sometimes quickly) to center around the technology.

As they become more prevalent and we become more integrated with them, we will transact more and more with vendors using our mobile devices. This is where the environment gets "target rich." Mr. Boodaei continues along this vein, "The number of users who bank online from their mobile devices is still relatively low. Additionally, transactions are not yet enabled for mobile devices on many banks' websites. Since online fraud is mostly a big numbers game, attacking mobile bankers is not yet an effective fraud operation. But expect a change. In a year from now this is all going to look completely different as more users start banking from their mobile phone and fraudsters release their heavy guns."

So how do you protect yourself and your financial information in the wake of this disconcerting trend? 2 simple steps will help you get headed in a good direction. These are targeted for people (like me) with short attention spans, you can do much more, but here are some quick ones that won't cramp your style too much:

1) Take 2 minutes (more if you have it) instead of 1 minute to look around a bit at what other users have to say about an app before you install it. Is the company reputable? Have users had issues?

2) Be careful about allowing escalated privileges to the app when it prompts you instead of just clicking along until it installs. If it's a simple app, it really shouldn't be asking to probe the deep recesses of your device, or you should know why.

Also, various vendors are releasing anti-malware products for mobile devices, expect to see more hitting the market down the road. While there is no "magic bullet" for security, mobile or otherwise, an extra minute or 2 of research and a healthy dose of curiosity if something "just doesn't seem right" will go along ways toward protecting your online life you've grown so fond of.

Stop spam/botnets? Follow the money

It's no secret that spam/botnets are big business. There are a multitude of variations on a familiar theme, but after they trick unwitting users, what happens to the money? University of California wondered the same thing. In their recent report, "Click Trajectories: End-to-End Analysis of the Spam Value Chain" they analyze where the money goes, with a goal of stopping it at some major pinch point.

It seems the lowest hanging fruit is the few number of venues where operators can "cash out" after a spree of cyber-nastiness. The study found only a handful of banks are typically used by the whole sector. They found, in fact, that 95% of the operations use just 3 banking institutions. This is a much smaller link to disrupt than anywhere else in the chain; stop these, and the whole rest of the chain becomes precarious. Stopping botnets and other cyber-nonsense is an ongoing "Whack-a-mole" exercise, where as soon as one problem gets solved, another 10 pop up, but solve the money flow issue at the bank and they die of attrition, or so the theory goes.

They argue there are 3 distinct stages in the money flow chain:

1) Advertising

2) Click support

3) Realization.

The advertising phase has received the most study due to the more numeric customer facing incidents it creates; flooding e-mail inboxes and the like. But it's only one link in the chain. Increasingly, botnet operators rent out their botnet to the highest bidder, so they're really only a provider for the larger operation.

Additionally, while many other aspects of the operation are fluid, it is more difficult and time consuming for the spam operator to change banking institutions, since "the replacement cost for new banks is high, both in setup fees and more importantly in time and overhead. Acquiring a legitimate merchant account directly with a bank requires coordination with the bank, with the card association, with a payment processor and typically involves a great deal of due diligence and delay (several days or weeks)."

Banks who don't ask many questions of online transactions seem to be highly concentration in very specific regions. The bulk is located in only four: St. Kitts, Azerbaijan, Latvia and Russia. Though there are others elsewhere, these process the bulk of the transactions studied. Seemingly, if these were targeted successfully, much of the spam ecosystem would be forced to regroup into other regions, which would take time and effort, causing profits to dip in the interim, having an effect

on the profitability of the botnet operators.

While it seems like an obvious step, cracking down on financial institutions in far flung regions may not be the simplest endeavor. Still, it's an interesting potential choke point, and one that could be an effective tool in the battle, if executed successfully.

Latin America chosen for Trojan bankers attack and Hotmail accounts

During the last month we have seen many campaigns using public figures such as presidents or famous artist in order to propagate these threats through Latin America. Some of the countries selected for this purpose were Colombia, Guatemala, Brasil and Venezuela.

This month Colombia has been chosen as a target for Anonymous. This gang hacked into Juan Manuel Santos´s Facebook account and posted a Youtube video against the celebration of Colombian´s independence on july 20th. Also ex-president Álvaro Uribe´s Twitter account was compromised posting the same link to the video.

The Colombian actual president and the ex-president Uribe recognized what happened, and both of them complained about the actions performed by the hacktivist group.

One of the most important attacks were performed in Brazil, where two malware campaigns, created by the same group of ciber criminals stole more than 8000 Hotmail accounts trough a phishing attack aiming to Brazilian Banks. These stolen accounts were use to propagate this threat over the region, having success and more than 27000 visits to the fake websites in less than 5 days.

Actually this is one of many campaigns performed by the same group of criminals using Social Engineering, which activities are being followed since February. In every campaign they use the same methodology; fake emails are being sent through a hacked email account.

The malware industry development in Latin America has grown over the years and has begun to emerge attacks targeting users of many banking institutions in the region.Brazil is not only the leader in Latin America it is also one of the world´s leaders in phishing Trojan development.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.51%

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. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 3.88%

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.

3. Win32/Sality

Previous Ranking: 3
Percentage Detected: 2.03%

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. Win32/PSW.OnLineGames

Previous Ranking: 4
Percentage Detected: 1.67%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf

5. HTML/Iframe.B.Gen

Previous Ranking: 6
Percentage Detected: 1.67%

Type of infiltration: Virus

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

6. HTML/ScrInject.B

Previous Ranking: 9
Percentage Detected: 1.56%

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

7. Win32/Dorkbot

Previous Ranking: 11
Percentage Detected: 1.47%

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. Win32/Autoit

Previous Ranking: 5
Percentage Detected: 1.27%

Win32/Autoit is a worm that spreads via removable media, and some of it variants spread also thru MSN. It may arrive on a system as a downloaded file from a malicious Web site. It may also be dropped by another malware. After infecting a system, it searches for all the executable files and replace them with a copy of itself. It copies to local disks and network resources. Once executed it downloads additional threats or variants of itself.
In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry.

9. HTML/StartPage.NAE

Previous Ranking: 8
Percentage Detected: 1.08%

HTML/StartPage.NAE is a trojan which tries to promote certain web sites by modifying the window's registry. The program code of the malware is usually embedded in HTML pages. The aim of this malware is to change the website that is first opened when running Microsoft Internet Explorer (only affected browser). This way it promotes a specific website, and the owner of it profits of the increasing amount of visitors. This specific variant of HTML/StartPage redirects the affected users to the following website: hxxp://duzceligenclik.com

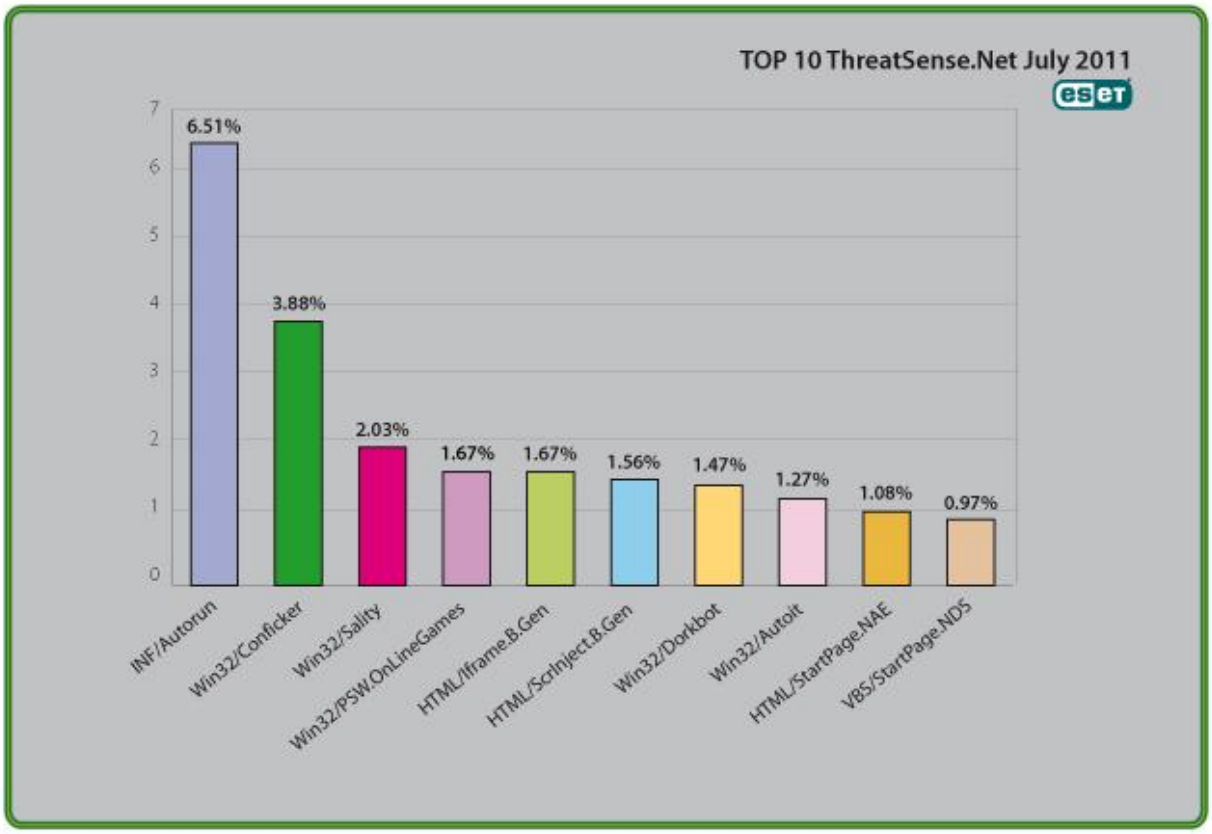
10. VBS/StartPage.NDS

Previous Ranking: 48
Percentage Detected: 0.97%

It is a trojan that changes the home page of certain web browsers.

Top Ten Threats at a Glance (graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 6.51% 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