



Global threat report


January 2012

Feature Article: Where are the 419s of Yesteryear?



Table of Contents

Where are the 419s of Yesteryear?.....	3
Do we need anti-virus, anti-malware, or anti-scam?	4
Stephen Cobb, Security Evangelist	4
Clinic for Comment Spammers.....	6
Trends for 2012	6
What is a potentially unwanted application (PUA)?	7
Facebook Events.....	8
The Top Ten Threats	9
Top Ten Threats at a Glance (graph)	12
About ESET	13
Additional resources.....	13



Where are the 419s of Yesteryear?

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

I'm not exactly fond of 419 ("Nigerian" or advance fee fraud) scammers. You know the sort of thing: African monarchs and the wives of dead dictators wanting to pay you vast sums for your help in moving their money, or messages telling you that you've won a lottery. I detest them because when they really score, they're utterly merciless when it comes to milking the "big fools" (mugu) who fall for the scams: I recently saw an interview with a very dejected victim on television who'd paid out several hundred thousand pounds in advance fees in the expectation that he'd eventually be paid several million. I don't know the details of that particular case, but victims often lose not only their money but their self-respect, not only because of their own gullibility, but sometimes because they've borrowed money from friends and relatives in order to pay the taxes, fees and bribes that are supposed to be necessary so that they can achieve their "windfall". There have even been instances where a victim has taken money from his or her employer in the expectation of being able to pay it back when the money arrives. Which, of course, it never does, and other victims have got into all kinds of trouble by actually meeting with the criminals in question.

Still, I must also admit to having got a certain amount of sour amusement from some of these guys, though I've never gone in for the kind of scammer baiting described and documented at sites like [Bait a Mugu](#) and 419eater.com. Unless you count the lady with a pronounced West African accent who rang me from Amsterdam with a curiously convoluted tale about how someone was spreading stories about my having an inappropriate relationship with her. While it was clear that she

had an unhealthy interest in my financial status, I eventually got bored and hung up before she'd got to the point and explained what exactly she wanted me to think I was paying for. As I've mentioned before in the context of PC support scams, I'm temperamentally unsuited to this kind of undercover work due to a bad case of Short Fuse Syndrome.


That said, I do get a certain perverse amusement from an ingeniously crafted example of scammer chutzpah: for example the [Nigerian Astronaut](#), the Pope's secret fund for doing good by stealth, and the ethical hitman who's decided that you don't deserve to die, so is giving you a chance to make him a counter-offer. Hey, even assassins have to eat, you know. You can learn a little more about those, and a very confused Irishwoman from Ohio who apparently got married at an age when most of us are barely old enough to start thinking about boy/girlfriends, in [an article I wrote](#) for SC Magazine last year. You may not be scam-proof once you've read it, but it's probably good for a chuckle or two.

Recently, though, a lot of scammers seem to have been losing heart and going through the motions. Maybe they're depressed at the competition from support scammers in Kolkata and New Delhi. Aryeh Goretsky recently noted what he describes as the 'lamest scam ever, from the "We're Not Even Really Trying" Department.'

Subject: FW: Your ID Has Been Awarded

Bodytext: Send Your:Names:Address:Phone Number:Country.

I've seen some pretty minimal 419s, but you'd think they'd at least mention a figure. I mean, I don't even get up in these cold mornings for less than \$200. ;-)



My wife forwarded a message to me with a certain naïve charm about it, though: apparently from the United Nations.

Dear,

You are to receive the sum of US\$750,000.00 under UN Scam victims Compensation scheme. For details, contact Mr. George Jacobs, payment officer on [email address apparently in the Ukraine]

Regards,

Mary Moore

Actually, given the 419-er predilection for names that are either gloriously over-the-top like Bayron Javier Revelo Cabrera, or clearly celebrity-influenced like Diana Spencer, I'm surprised it wasn't Mary Tyler Moore. By the way, I didn't remove my wife's name from the mail out of an exaggerated fear of exposing her personal details to the billions of readers of the ThreatSense Report: Ms Moore simply didn't bother to find a natural-looking salutation that would work for anyone, regardless of name or gender. But there's a certain irresistible classiness to the idea of offering compensation to the victim even before you scam them.

Less charmingly, it's actually not uncommon for 419s to use scam victim compensation as part of their pitch. I can't quite decide whether this is because scamming someone who's already been scammed gets them extra points in the Scammer's Hall of Shame, or whether it's because it's an enduringly successful technique to scam someone by making the mark think he's taking advantage of a random opportunity to run his own little scam.

Don't get the idea there's a Robin Hood element to this, though: 419-ers are just as happy to kid you that they're giving you the opportunity to do good works with your money. Since all they're interested in is your money, they don't care whether

you really intend to use the cash you'll never see for the relief of poverty or famine or some other natural disaster. If they think about that possibility at all...


Do we need anti-virus, anti-malware, or anti-scam?

Stephen Cobb, Security Evangelist

In this article we review several recent incidents that point to an expanding role for the category of software that has historically been referred to as anti-virus, even though a more accurate term might be anti-malware. As the bad guys continue to think up new ways to manipulate networks and network users for illegal purposes, antivirus software may need to offer even more forms of protection.

If you analyze the keywords used in Google searches related to protection against malware, the most commonly used term is still anti-virus, more often written antivirus. For many years now we have expected antivirus software to do a lot more than just prevent computer virus infections. We also expect it to protect against worms and Trojan code. The latter is not so much about spreading itself from device to device, but opening each device up to further abuse (for readers unfamiliar with the origin of the term, it comes the wooden horse which the Trojans took into the city of Troy, thinking it a gift from their enemies, the Greeks, only to find out, to their cost, that it contained Greek soldiers who opened the gates to the city, resulting in its destruction).

Some antivirus software also includes protection against spam, spyware, and potentially unwanted applications (PUAs). When included as part of a security suite, antivirus software may also be associated with end-point firewalling and content filtering. But network users are increasingly presented with threats and



distractions that don't fit neatly into any of these categories. Consider [search poisoning](#) , [survey scams](#), and phony message on social networks. We have written about these threats numerous times on the [ESET Threat Blog](#), particularly in the context of [Facebook](#). One reason for our coverage of these scams has been the apparent increase in their number and variety. Recently we got some insight into why this is, and the answer, as you might expect, is money.

Many survey scams are created to trick web surfers into clicking on a large number of links, clicks for which the scammer, or the scammer's agent or affiliate, will bill an unsuspecting advertiser. This practice is known as click-jacking and apparently there's a lot of money in click-jacking. How much? In a lawsuit filed this month in America, the Washington State Attorney General claims that a fraudulent ad network operated by Adscend Media was using this type of scam to generate "gross monthly revenues of up to \$1.2 million."

The lawsuit makes fascinating reading because it provides a detailed description of how the scam works and the labyrinth of links that lurk behind salacious messages like "OMG! See What Happens to his Ex Girlfriend" and "Cannot BELIEVE a 2 year old is doing THIS" and "My mom took my computer away when she found out I Googled this" For those who cannot resist clicking on such teasers, an endless series of web pages awaits. From bogus "Age Verification" pages to fake "Like" and "Share" links, to surveys and prize redemption contact forms, the whole charade is designed to harvest as many clicks as possible before the clicker loses interest. (You can find simple and direct links to the court documents at [SC Magazine's Cybercrime Corner](#).)

Also found in the Adscend lawsuit is an interesting statistic that sheds light on how many people fall for these messages: in February 2011, "the defendants' affiliates tricked 280,214 Facebook users into visiting their pages through solicitation".

By solicitation, the lawsuit means the publication on Facebook of alluring messages like those quoted above. How that number relates to the \$1.2 million in gross monthly revenues is not clear, but if both figures were for the same month that could indicate that an average of \$4.28 is generated per Facebook user who is led astray. In some cases the user loses nothing, the victim is the advertiser who is billed for the clicks. However, some of these scams are probably harvesting personal data for resale as well, including mobile phone numbers that can be targeted by premium rate scams.

The FBI's takedown of the DNSChanger botnet late last year in [Operation Ghost Click](#) already revealed that there is big money in bogus clicks. According to the indictments in that case, the crooks behind the botnet generated at least \$14 million worth of bogus clicks that were harvested by redirecting traffic through manipulation of DNS by Trojan code on about four million computers in 100 countries. Good antivirus software prevented such code making its way onto protected machines, but how can antivirus software stop someone clicking on a link in message from a friend on a social network that says: "Over 1 MILLION People have seen the SHOCKING revenge!?"

The answer is education. If antivirus software can educate the user about best practices for safe computing, then the user will resist the urge to click on links that, given just a moment's reflection, are a waste of time, or worse. ESET has taken steps in that direction and in the future we may see more antivirus offerings that incorporate user education. The reality is that computer users have come to expect antivirus to mean protection against a wide range of computer and network abuse, and scams like click-jacking are very hard to defeat with technology alone. But education has the ability to reduce more than the probability that users will fall for scams. Education can also reduce security exposure across a range of risks, from poor password selection to phishing attacks.

Clinic for Comment Spammers

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

ESET's former Agony-Aunt-in-Residence, Letitia Teaspoon, recently moved to [Small Blue-Green World](#) in a similar capacity, giving spammers the encouragement they deserve. However, she left one last batch of good advice on her desk in San Diego to pass on as her swansong.

Dear Robin, thank you for your kind comments to one of Mr Harley's posts about Win32/Carberp, whatever that is. We also appreciate detailed information, so I'm emboldened to ask whether the Mini-Palms in your email address are PDAs or very small [Arecaceae](#). I ask because when I tried to grow Palm Pilots in my orchard in Coronado, I was unable to persuade them to flower at all. Do you think that iPhones and Blackberries would produce better fruit?

Dear Nail Fungus Product, thank you for your interesting reflections on the persistence of life and lifestyle. It's reassuring to know that my nail fungus will, in some form, survive even the supernova that is expected to engulf the solar system in 5 billion years or so.

Dear Colton, yes I'm afraid that you do have the wrong area. We have no opinions concerning an organization advertizing an IT Sales job, and will not be approving a comment listing its contact details.

Dear Zachary, thank you for your interesting list of pharmaceuticals. If you think we're going to approve it, maybe you should spend less time sampling them yourself.

Dear Louisa, yes we do have methods for protecting against

hackers. Comment moderation is just one of them.

Dear Facebook Friends, I'm so pleased that you consider yourself lucky to have discovered our web site unintentionally. I'm afraid I have no idea why this twist of fate didn't happen in advance. However, I...


Thank you, Letitia. I'm afraid I'm going to cut you short there, as I don't think the joke you're working round to is quite seemly for a lady of your age and gentility.

Trends for 2012

Our Latin American Research Team brought us the report "**Trends for 2012: Malware Goes Mobile**", that highlights that during 2011, the existence of threats for mobile was accelerated due to the growth of Smartphones on the market and marks Android based threats as the main trend for 2012. According to the report, there are more than 5 billion mobile devices on the world, of which 500 million are from Latin American countries. This adds to the information published by Gartner, claiming that Android was the leader in mobile platforms (with around 400 million mobile devices on the market).

Some interesting tips to notice:

- Out of 41 malicious codes that were analyzed, only 5 appeared in 2010.
- Most threats were downloaded from non-official repositories (7 out of 10)
- 15 out of 41 were identified as SMS Trojans
- 60% of the analyzed malicious codes botnet



characteristics and functionality.

There is another hint that **malicious codes for mobile devices will be the main trend for this year**. One example of the relevance of this type of malware is DroidDream, since there were more than 250.000 downloads of this threat from the Android Market, being regarded as the first malicious code for mobile devices with such massive impact.

In addition to this, ESET Latinoamérica's report claims that nowadays malicious software developers have found in Android the same exploitability that Windows XP has offered for years: not only because of the characteristics inherent to the platform, but also because most users have unsafe habits.

For more information you can read the complete report [here](#).

What is a potentially unwanted application (PUA)?


Our Distinguished Researcher, **Aryeh Goretsky** has updated his white paper [Problematic, Unloved and Argumentative: What is a potentially unwanted application \(PUA\)?](#), including information about how legitimate software can become classified as a PUA due to its misuse, a discussion of a type of downloader called a *software wrapper* and updated screen shots.

According to this paper "a potentially unwanted application (PUA) is a type of computer program **and** a set of associated behaviors. While a PUA may **not** perform the same type of malicious activities typically associated with computer viruses and worms, it may instead install additional unwanted software, change the behavior of the digital device, or perform

activities not approved or expected by the user."

Some examples of real PUA behavior are:

- **Programs that install toolbars in the web browser.** Such add-ons are not necessarily malicious, but if they install without clearly informing the user of their presence, don't offer the opportunity to opt out of installing, provide no means to effect a clean uninstall or fail to provide assistance with uninstalling; then they join the category of potentially unwanted applications.
- Programs that contain an **adware component but do not clearly indicate the presence of such a component** or provide a method or instructions for removing the adware after the parent application has been uninstalled.
- **Software of dubious quality and reputation**, including programs that make outlandish, unverifiable and unsupportable claims about their efficacy and/or generate deceptive false-positive alarm reports of threats that do not exist in order to mislead people into purchasing something they do not really want or need.
- **Programs sold through spam and/or sold through rogue affiliate marketing networks** that pay a commission based on software installations (the "pay-per-install" business model).
- **Programs that make changes to web browser settings** such as the default home page or search engine selection in an unannounced or otherwise



deceptive fashion.

- **Programs compressed** with packers or protectors that are widely used (or abused) by **malicious software**.
- **Legitimate programs that are misused** by malware to perform malicious activities.

Another category is the **potentially unsafe applications** which are close to potentially unwanted applications. This category includes the following:

- **Software cracking tools and license key generators.**
- **Hacking tools.**
- **Product key finders.**
- **Remote control programs:** A company's IT department might use this type of program to access a computer in a server room or repair a computer at a remote location, but they might not want their other employees to run such programs, which are, for instance, commonly used by fake support service centers.
- **Software that displays advertising.**

To learn more about PUAs, visit [Aryeh Goretsky's white paper](#).

Facebook Events

It's been a busy month in terms of security in Facebook and many events were reported in ESET's blog:

Stephen Cobb described how Facebook implemented a new feature (a.k.a. "timeline") that replaces the traditional profile page, and caused some confusion among Facebook users and of course, some scams surfaced taking advantage of this confusion. As of January 3rd there were **16 Timeline-related scam pages** which had collectively gained **more than 71,000 likes** and also were among the top search results when searching Facebook for "timeline". According to Stephen, these changes may cause the appearance of many many Facebook bogus pages offering the removal of the timeline feature. You can see an example in Stephen Cobb's post "[Facebook's timeline to fraud-a-geddon?](#)".

David Harley wrote a post entitled "Facebook, your birthday #1, and survey scams" explaining a new scam on Facebook. This particularly scam tells what was the song number one in the charts the day you were born, providing in some cases, a link to a video. For more information on this scam you can visit [David Harley's post](#)

Cameron Camp explained in his article "Welcome to Facebook f-commerce platform - and Own/Want features" how there's a possibility of adding "own" and "want" buttons on Facebook platform to indicate possession and desire. These features may be handy for advertisers to market their products but nevertheless, this can incur in certain risks. Since criminals can search through profile to know if a user has a particular product, it's a fair bet that if they break in to a house, there's a good chance of finding what they are looking for. This, combined with some users' tendencies to report where they are from mobile devices, can alert criminals when the user is away from home, and a rough time frame for how much time they have for their deeds before the user may return. For more



information visit [Cameron Camp's post](#).

David Harley mentioned some new facts relating to Win32/Carberp trojan activity in his post "Facebook Fakebook: New Trends in Carberp Activity". The scheme used here for financial fraud is simple: if the victim attempts to log in to Facebook, instead of accessing the log in page, he sees instead a fake Facebook page which displays the message "Your Facebook account is temporary locked!". After this, e-Cash is demanded to continue. For more detailed information about this threat, you can visit [David Harley's post](#).

The Top Ten Threats

1. HTML/ScrInject.B

Previous Ranking: 1
Percentage Detected: 4.98%

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

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 4.41%

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://blog.eset.com/?p=94> ; <http://blog.eset.com/?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.

3. HTML/Iframe.B


Previous Ranking: 3
Percentage Detected: 2.74%

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.

4. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 2.01%

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 subsystem 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&lang=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://blog.eset.com/?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.

5. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 1.31%

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.

6. Win32/Autoit

Previous Ranking: 6
Percentage Detected: 1.08%

Win32/Autoit is a worm that spreads via removable media, and some of its 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.

7. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 8
Percentage Detected: 0.96%

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.

8. Win32/Sality

Previous Ranking: 7
Percentage Detected: 0.92%

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

9. JS/Iframe.AS

Previous Ranking: 12

Percentage Detected: 0.70%

JS/Iframe.AS 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.

10. Win32/Spy.Ursnif

Previous Ranking: 10

Percentage Detected: 0.70%

This is a spyware application that steals information from an infected computer and sends it to a remote location, creating a hidden user account, in order to allow communication over Remote Desktop connections.

What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with esoteric Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created.

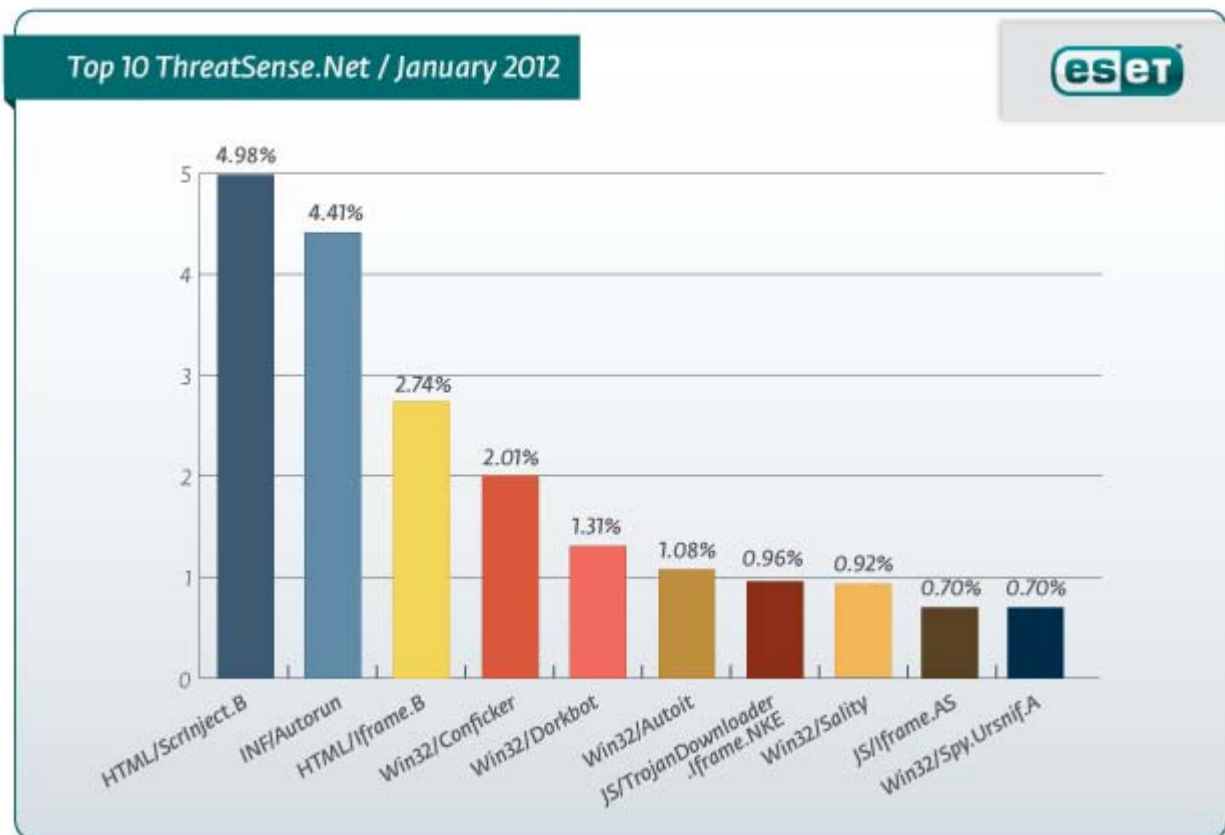
In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in

patching, and in avoiding unexpected file downloads/transfers and attachments.

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 4.98% of the total, was scored by the HTML/Scrinject.B 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](#)