



Global threat report

September 2011

Feature Article: Backup strategy for home users



Table of Contents

Backup strategy for home users.....	3
The Art of Security.....	4
Dead Certs?	5
PDF Trojan Appears on Mac OS X.....	7
The Good News About Security and Privacy Breaches: An Opportunity to Learn	7
The Top Ten Threats.....	9
Top Ten Threats at a Glance (graph)	12
About ESET	13
Additional resources.....	13



Backup strategy for home

users

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

A shorter [version](#) of this article previously appeared in SC Magazine's Cybercrime Corner.

Years ago, when I was a security analyst/administrator at a medical research organization in the UK, one of the units (not one I was personally responsible for, fortunately) had a nasty experience with a server. All its PCs were being dutifully backed up to the server in question, but unfortunately, it hadn't occurred to anyone to back up the server. Not, at any rate, until problems hit both a PC and the server that resulted in the loss of data. Not critical data, perhaps, since the unit and the organization are still around, but significant enough to threaten managerial heads with a sudden migration from neck to guillotine basket, though to the best of my knowledge, no heads did roll in the end.

In fact, the history of security is littered with failed backup strategies. Here are a few horrible examples from [Practical UNIX and Internet Security](#), by Simson Garfinkel and Eugene Spafford.

A researcher at DEC who lost ten years worth of email because the DAT tape on which it was backed up had never been verified and failed to work because of a bad block right at the beginning.

A project group that had to retype in a system from printout because it turned out that their home-brewed backup utility only backed up the first 1024 bytes of each file.

As Garfinkel and Spafford said: "Making backups and verifying them may be the most important things that you can do to protect your data..." And losing data can be just as disastrous to a home user (especially a home business user) as it is in the enterprise. To replace stolen or mangled hardware is just a matter of spending enough money. Replacing data that is no longer accessible is another matter, and it can be the difference between survival and non-survival for a business, or even a household, financially speaking. But if hardcore IT professionals can get it wrong, what chance does the everyday home user have of ensuring that their data are safe?

We all pay lip service to the idea of backup, but until you actually lose some data that you hadn't backed up you may not really appreciate how important it is. In fact, consideration of backup strategies and mechanisms is generally a major component of generalist security courses and certifications, as it should be. Backup strategy and implementation in business is a more complex issue than you might think, and not every system administrator and/or IT manager gets it right all the time. What do you do if you're a home or small business user, with no professional system administrator to explain/set you up with RAID, hot sites, replication, and all the other esoteric paraphernalia of disaster recovery?

Unfortunately, security professionals talking to end users are apt to emphasise the need to back up without going into the practical details of how to do it. ESET's Aryeh Goretsky, however, has put together [a short paper](#) that addresses that need for the home/SOHO audience without lapsing into gratuitous marketing. He avoids overly-esoteric technical detail and uebergeek jargon, but manages to pack in enough information on a complex and difficult topic to give a home user a good grasp of what they need to know in order to take their first steps towards business continuity and disaster recovery in the home and small business.



[Options for backing up your computer](#) won't turn you into a business continuity specialist. However, if you've never been quite sure of what you need to do in case a fire, burglary, hard disk failure or other disaster threatens the electronic data that so many of us are dependent on nowadays, you'll understand the issues much better after reading it.

Table of Contents:

Both hardware and software needed to back up your computer

Hardware backup

Software backup

The value of archive programs

Syncing up

Disk imaging programs for backing up

Blended backups

Cloud-based data backup

Choosing which data to backup

How often to back up your computer

Diversify your backup methods

Where to store your backups

Replace your backups periodically

Data recovery services as a last option

A paper has been posted to ESET's ["Staying Secure Online"](#) page, which links to other material that may well be of interest to many people.

The Art of Security

Stephen Cobb, CISSP, ESET Security Evangelist

Wandering among art exhibits in a park on a sunny Saturday in September might not sound like computer security research,

but it is actually possible to learn a lot the San Diego's annual Artwalk on the Bay.

Securing Our eCity In the [May issue](#) of the Global Threat Report, it has been published an article about Securing Our eCity in which it is possible to know that it is a community initiative to raise computer security awareness, led by ESET but supported by a wide range of companies, civic groups, and law enforcement agencies. More information about SOeC can be found in <http://securingoureconomy.com/>. A short definition of SOeC is a wide security awareness and education community.

What makes this event a valuable excursion for malware research activity, is the opportunity to chat about computer security with a random sample of consumers in a relaxed setting. It has been discovered that a wide range of awareness levels when it comes to the current state of malware and other online threats. An encouraging number of people were using some form of anti-virus software. A slightly smaller number understood that such software would not protect them against revealing their private data on a bogus website to which they were led by an apparently legitimate email

At the Securing Our eCity booth people could enter a draw to win an iPad2 by writing down one thing they were doing to protect themselves online. Most people had no difficulty coming up with an answer, which was encouraging. That may be a reflection of the sentiment revealed by a recent ESET/Harris Interactive poll of more than 2,200 American adults: [91 percent feel vulnerable](#) to some type of cyber attack.

In the findings of the report—as highlighted by Dan Clark, ESET's VP of Marketing, in that Dark Reading article—it is possible to see that the drumbeat of high-profile security breaches is having an impact on consumer sentiment. More than half of those surveyed said that their faith in the ability of



companies to protect their personal data had been diminished. Another finding in the poll reflected a view that was expressed by several people were at the art event; more than 90 percent of those polled by Harris said that cybersecurity education should be part of a student's curriculum. In the meantime, major companies continue to be penetrated by attacks that rely on user ignorance and social engineering, sometimes as a vector for malware distribution, sometimes as a direct entrée into internal systems. When information system security at firms like [Mitsubishi Heavy Industries](#) and [RSA](#), or facilities like Oak Ridge National Laboratory, can be [compromised by an employee](#) making a bad decision to follow a deceptive link in a dubious email, you know the world needs a lot more security awareness and training than it is getting. That's why the latest versions of ESET's flagship products come with security training, and why ESET is supporting initiatives like Securing Our eCity. Only when security technology is backed by widespread security awareness can we hope to repel the rising tide of cyber attacks.

Dead Certs?

David Harley and Róbert Lipovský

Are we seeing the decline and fall of SSL and the Certificate Authority model?

ESET has had a few press enquiries lately about attacks on SSL/TLS/HTTPS, though really these attacks are more about trust issues with Certificate Authorities like [DigiNotar](#) and [GlobalSign](#) than about weaknesses in the underlying protocols. So Róbert Lipovský (malware researcher at ESET's mothership in Bratislava) and David Harley decided to pool their thoughts on the subject as a sort of FAQ.

1. What is an SSL attack?

The "SSL attacks" that have been mentioned recently are actually attacks on the SSL certificate scheme, against the specific certificate authority (i.e. stealing the certificate), or in the form of a man-in-the-middle (MITM) attack against the user (which is the ultimate goal). Or it could be said that they refer to all these aspects combined.

SSL is a cryptographic protocol used for secure transactions on the Internet. Very simply put, it's the underlying technology that's being used when it is possible to see https:// in the address bar (rather than http://), for example when logging in to an online banking system. (HTTP stands for Hyper Text Transfer Protocol, and HTTPS stands for HTTP Secure.) These secure sites should have a valid digital certificate (or an SSL certificate) issued by a certificate authority (CA): this certificate is intended to prove that the entity (e.g. a bank) is really who or what it says it is, not an attacker just posing as the entity.

The problems arise when an attacker is able to steal such a certificate, which gives him veneer of credibility, when executing a man-in-the-middle attack (intercepting communication between you and the bank), running a (digitally signed) phishing site, and so on.

2. What does this mean for the end user?

Well, the user should be cautious (as always) but there's no cause for panic. The implication for him is that if someone can impersonate the server with which they're communicating, in other words, something that looks like a trusted communication channel is not, in fact, trustworthy. But in order to do that, the attacker has to get inside the communication channel between the user and the server (e.g.bank). Simply put, the SSL attack enables the attacker can say "hey, I'm your bank". But he first needs to find a way to ensure that the victim will be connecting to his server instead of the real bank server.



If he can do that, then the transaction has already been compromised, with or without the SSL “vulnerability”.

3. What can the end user do to protect himself?

An end user should at least check whether that lock icon is displayed in the web browser (bearing in mind that tricks for counterfeiting that icon are almost as old as phishing). The user should ensure that his connection is https:// over port 443, not http:// over port 80. If he’s using a modern browser (and it’s not a good idea to continue using older, less well-supported and –patched browsers) he should see everything’s green in the address bar and watch out and check for extended information about the connection. And most importantly, he shouldn’t proceed with the connection (as too many users do) if something looks fishy. Obviously, the regular advice still applies – that they should use multi-layered protection, keep their anti-virus and operating system software updated and patched, and (most of all) use common sense.

4. What is a trustworthy connection?

One where:

- There is an up-to-date, fully patched browser that implements HTTPS correctly populated with trustworthy certification authorities installed and correctly configured so that it will know when certificates are revoked and CAs no longer considered trustworthy.
- The web site to which the user is connected offers a valid, up-to-date signed certificate.
- The site matches the certificate and its holder’s name.

If it is not possible to be sure that this all applies, or that the transaction is routed through a “safe” series of hops, or that the protocol itself is robust enough to withstand attacks on the encryption, it can’t be considered the connection trustworthy.

5. Is it time to ditch the CA system?

Perhaps that time is approaching. The problems aren’t so much with the technicalities of SSL, though, as with the difficulties of implementing a system that assumes trust in the provider without a realistic mechanism for determining where you can safely invest that trust. According to the Electronic Frontier Foundation, there are effectively over 650 CAs trusted by the main browsers. Looking at http://www.eff.org/files/colour_map_of_CAs.pdf it is possible to see who and where those CAs are, the question is this: how many of them are known by the user? There is no global authority that can be trusted to authenticate that mixture of state-owned, commercial and indeterminate authorities. Who, to coin a phrase, should authenticate the authenticators? Can users trust market forces, vested interests and political expediency to keep them safe where the system assumes that they will trust the provider even though there is no overarching mechanism to ensure that trust invested in CAs is justified.

6. Is there an alternative?

There is DNSSEC, though in such a case users are just investing trust in the same registrars who are (intentionally or not) providing the bad guys with malicious domains along with the legitimate domains that their victims use, and in ICANN and the same authorities that already administer Top Level Domains.

The Convergence/Moxie Marlinspike model of “trust notaries” using consensus from multiple notaries to authenticate is an



interesting idea and it will be interesting to see how much traction it gets. However, it's not a solution that spares the user the need to think for himself, and it has to compete with an entrenched commercial model.

7. Are the DigiNotar attacks really more significant than Stuxnet?

While a Stuxnet-type attack might, in principle, cause a major physical disaster (note that we're not saying that's likely, and certainly not with the Stuxnet code that we've actually seen), it does seem to have been a highly-targeted attack which has been hyped to blazes (pun not entirely unintentional).

DigiNotar is significant in itself because of the range of affected targets, but even more so as a symptom of a more generalized attack against an infrastructure we've been conditioned into regarding as secure, and clearly isn't. Will anyone who reads the news ever trust those little padlock icons again, when there are so many virtual bolt cutters around?

PDF Trojan Appears on Mac OS X

During this month a new threat targeting Mac OS X users has appeared. This Trojan aims against the Macintosh Chinese-language user community. The trojan appears to the user to be a PDF containing a Chinese language article on the long-running dispute over whether Japan or China owns the Diaoyu Islands.

At the moment that the user opens the "PDF" file, it attempts to mask the installation of a malicious payload by opening an actual PDF document that directs the user's attention to the story. As our friends at Sophos [note](#), while the user is focused on the article, the malware completes installation of a payload

designed to give the attacker remote access to the victim's computer.

This type of PDF exploit is common on Windows where it is often seen as .pdf.exe double-extension files. However, this type of attack is new to the Mac platform and reminds Mac users that they should be aware that files appearing to be PDFs may not be what they seem.

Best practices to reduce the risk of infection are to:

1. Never open file attachments in email that you did not expect to receive without first confirming the file was actually sent to you by the mailer
2. When downloading files online, don't trust sites that are not reputable outlets for content.
3. Run antivirus/Internet security software on all your devices

[ESET Cybersecurity for Mac](#) detects these threats as OSX/Revir.A Trojan and OSX/Imuler.A Trojan. More information about this attack can be found in

<http://blog.eset.com/2011/09/23/pdf-trojan-appears-on-mac-os-x>

The Good News About Security and Privacy Breaches: An Opportunity to Learn

During the last week of september there was a report of a "health data breach" at Indiana University School of Medicine, hot on the heels of the "medical privacy breach" the week before at Stanford Hospital in Palo Alto, California. In the



Stanford breach, a commercial website was found to contain data relating to 20,000 emergency room patients including "names, diagnosis codes, account numbers, admission and discharge dates, and billing charges for patients seen at Stanford Hospital's emergency room during a six-month period in 2009." ([New York Times](#))

The Indiana breach involved an unencrypted laptop from the department of surgery at the Indiana University School of Medicine. This laptop was "apparently" stolen from a physician's car in August according to the report in [Health Data Management](#). The laptop contained health information related to more than 3,000 people, including name, age, gender, and diagnosis. In addition, for some 178 patients, the records included Social Security numbers.

While both incidents are regrettable and should never have happened, they are quite different in several respects. For a start, the Stanford data was published online, and stayed online, for nearly a year. That is serious exposure. Even though criminal intent does not appear to be a factor in the data showing up online, there is no way to predict the intent of people who may have seen and/or downloaded the data while it was exposed. The Indiana data has not, as far as we know, been published, and it is quite possible that access to the data was not the motive for the theft.

The one "good" thing that both incidents have in common is the potential to educate individuals and organizations about information security and data privacy. The Stanford case, as detailed by Kevin Sack in the excellent New York Times coverage cited earlier, highlights the importance of outside contractor security and speaks to a well-established cybersecurity best practice: Any organization that uses outside contractors needs to make sure that those contractors adhere to the same standards of information security as the

organization itself.

Stanford Hospital transferred patient data to a billing contractor that apparently failed to afford the data adequate protection because it showed up online in a spreadsheet used by a homework assistance website called Student of Fortune (as sample data in an example of how to produce bar graphs). This breach is bad news for the contractor, but also for Stanford Hospital, even though the hospital spokesperson is quoted in the New York Times as saying: "there is no employee from Stanford Hospital who has done anything impermissible."

If the hospital does not routinely follow best practices and obtain written assurances from its contractors that they have specific and well-documented policies and procedures in place to prevent exposure of personally identifiable information. The hospital would also need to show that it has been diligent in verifying those assurances and auditing those policies and procedures.

Regarding to the Indiana incident, the lessons are perhaps more straightforward. Reports of the incident state that the laptop was password-protected, but a system access password alone does not prevent a person from getting to data on the hard drive. Although the HIPAA Security Rule does not require patient data on a hard drive to be encrypted there are compelling reasons to use encryption, not least of which is avoiding the embarrassing and costly exposure of patient data.

Furthermore, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which introduced mandatory notification of patients in the event that their records are exposed by a security breach, specifically exempts encrypted health data from these notification requirements. In other words, encrypted health information is not considered, under HIPAA, to be at risk if it falls into the wrong hands. (If you



handle medical data, the American Medical Association has a very useful [document on encryption here](#).)

Hopefully, both hospitals are wiser now, and other hospitals have learned from these incidents. If you don't exercise due care with medical data shared with contractors or encrypt such data when it is stored on laptops, then the consequences can be damaging, to patients and to hospitals, and to society in general. After all, security failures like these undermine the potential of information systems to deliver benefits such as reduced healthcare costs and increased productivity.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.49%

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: 3.65%

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&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.msp>. 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/Dorkbot

Previous Ranking: 4
Percentage Detected: 3.23%

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.

4. Win32/Sality

Previous Ranking: 5
Percentage Detected: 2.29%

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

5. HTML/Iframe.B

Previous Ranking: 3
Percentage Detected: 1.97%

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.

6. Win32/Autoit

Previous Ranking: 7
Percentage Detected: 1.65%

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.

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.

7. HTML/ScrInject.B

Previous Ranking: 6
Percentage Detected: 1.56%

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

8. Win32/Ramnit

Previous Ranking: 10
Percentage Detected: 1.09%

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 remotely 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.

9. Win32/PSW.OnLineGames

Previous Ranking: 8
Percentage Detected: 1.09%

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](http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf)

10. JS/TrojanDownloader.Iframe.NKE

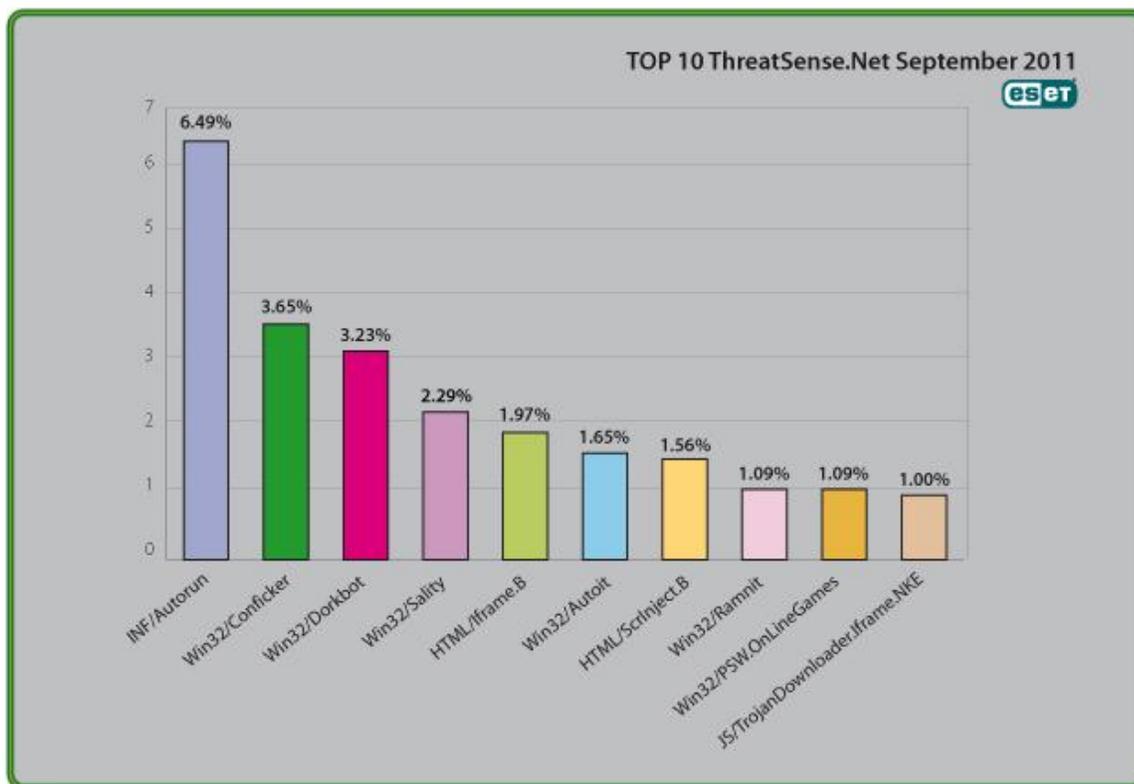
Previous Ranking: 9
Percentage Detected: 1.00%

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.

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 6.49% 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](#)