Global threat report

September 2012

Feature Article: Irish Ransomware Is No Joke

Table of Contents

Irish Ransomware Is No Joke

David Harley, ESET Senior Research Fellow

There's nothing intrinsically funny about ransomware: ask the owner of the Australian company TDS Refrigeration, who paid $3,000 after malware encrypted essential work files. It turned out to be a total waste of cash, since the criminals in question didn't bother to provide him with a decryption key even after payment. Still, if you came across the story reported in several Irish newspapers concerning the discovery of the "first Irish language virus", you might have been mildly amused. (Of course, it doesn't seem to have been a 'real' – i.e. self-replicating – virus. Not much malware does self-replicate nowadays, and that includes most ransomware.)

In this case, however, the victim is told he has – or may have – accessed pornography, and that his machine has been locked by an Irish government agency. And the message is in Irish, though according to the computer tech/repairer from whom the story comes, it reads as if some form of automatic translation software has been used. It contains a logo incorporating the Irish flag and apparently looks convincingly official apart from the wording. But then bureaucrats are not always known for the quality of their writing.

The reports I've seen to date imply that the thing has been dubbed "as Gaeilge" or just "Gaeilge", which would be a terrible name for a malicious program, since as far as I know it simply refers to the version of the Gaelic language they use on that side of the Irish Sea. If it were to catch on, I suspect that there would be some confusion with the "Irish Virus" hoax/joke, which looks something like this:

> You have just been infected with the "IRISH VIRUS".
>
> This virus works on the honour system. Please delete all the files on your hard drive manually and forward it to everyone on your mailing list.

(Believe it or not, there are actually anti-virus company web sites that list that email as a malicious hoax and warn their readers not to spread it. I guess they have less faith in the intelligence of their customers than ESET does.)

There's also another use for the term "Irish virus" which has nothing to do with IT security but is even more disrespectful towards the Irish as a nation, so I won't mention it further.

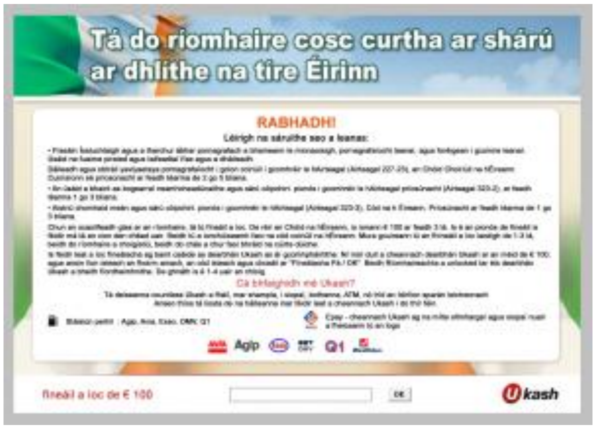
Without a sample or at least a file hash, I don't have any way of confirming that the characteristics of the malware briefly described in the Donegal story are exactly the same as the ransomware described below, but how many ransomware perpetrators are likely to be ploughing the same furrow? (Feel free to insert your own joke about the Rocks of Bawn here.)

However, a little while after this original report, I was contacted by Kafeine, who has some interesting samples of the kind of message we're talking about.

A screenshot here, though not exactly the same as the one described in the Donegal Daily and elsewhere (it has a Garda logo rather than an Irish flag, for one thing), looks similar enough to be from the same source. Come to that, I can't be sure about the content of the screenshot – Gaeilge is not one of my languages, and I don't have access to automatic translation software than can parse text from a graphic – but to my (mostly) Saxon eye, it looks as if it has similar content to screenshots on the same page in languages that I *can* read. And just to make it even easier, the scammer had a moment of inattention and re-used some text in French in the Irish scam message. Quelle dommage!

If anyone has sent in a sample of the malware reported in Donegal, from Kafeine's post it looks likely that it will turn out to be another variant of the Urausy trojan: that is, Reveton-like malware that ESET is likely to detect as 'A variant of Win32/Injector.[something]. If you Google Urausy, you may find sites that offer you a downloaded cleaner and tell you that AV is unable to detect it. Well, it's unlikely that AV detects all variants, but I'd suggest being very cautious about downloading utilities that turn up in a Google search unless you know what you're doing: it's unlikely that they're all genuine, especially if they provide misinformation about other security software.

Here's another version of the scam message, also from Kafeine, and this time it *does* come complete with Irish flag (and, to my eye, much the same social engineering).



Tá do ríomhaire cosc curtha ar shárú ar dhlíthe na tíre Éirinn

RABHADH!

Léirigh na sáruithe seo a leanas:

[illegible]

Cá bhfaighidh mé Ukash?

[illegible]

fíneáil a íoc de € 100

OK

If you'd like to get some information on this particular branch of the graphic design cottage industry, complete with a nice range of other designs in a range of languages (including English), you might want to check out Kafeine's post here (and Malekal's – in French – on Ransomware « Trojan.Casier » Panel).

There's also an example of a particularly fine miscommunication between designer and scammer: a design in Iranian targeting Irish speakers. Now there's an Irish joke worth a shot or two of *uisce beatha*. Unless they know something about the ethnic makeup of the Irish population that I don't. Meanwhile, I look forward to the first design in Welsh. Iechyd da!

I'll finish this article with a rough guide to what this type of ransomware looks like, at least in the format highlighted by Kafeine.

- It looks pretty official, though to a native speaker of the language concerned it may be obvious that it's been translated automatically.

- It may suggest that you've broken laws within the targeted jurisdiction: these laws are claimed to pertain to copyright infringement, pornography (including paedophiliac and bestiality content), and letting your computer broadcast malware – thus putting you in breach of a law requiring you to protect your PC properly. While there may be such laws – certainly as regards pornography and copyright – in the region in which you live, the details of the local penal code and penalties that might be incurred are not related to real legislation. They're merely intended to frighten.

- In order to avoid greater punishment, you're required to pay a fine of 100 dollars/Euros/Swiss Francs etc. within 72 hours – this is a common scam technique, designed to panic you into action without giving you time to think.

- You are required to pay using Ukash, Moneypak, or paysafecard: it's really not very credible that a police or judicial agency would require you to use one of these prepay cash transfer methods, which are all too easy to misuse for criminal purposes (as you'll be aware if you've read some of the blogs from my colleagues in Russia).

The message tells you that your system will be unlocked in 48 hours. It won't be, of course. I'd suggest that if you are caught by something like this, your first move should probably be to contact your AV vendor helpdesk.

In the meantime you might also derive some amusement from a story Urban Schrott (of ESET Ireland) and I joined forces on a while ago, regarding a lottery scam, also in the Irish language. Not that 419 (Advance Fee Fraud) scams are funny in principle – some people lose a great deal of money to the scammers – but there's something irresistibly dumb about this story: Irish 419-er seeks Spanish Lady.

Defeating anti-forensics in contemporary complex threats

Eugene Rodionov ESET

Aleksandr Matrosov ESET

Forensic analysis plays a crucial role in cybercrime group investigation, as it allows investigators to obtain such information as bot configuration data, C&C URLs, payload, stolen data and so on. Some of the modern malware falling into the class of complex threats employs various tricks to resist forensics and conceal its presence on the infected system. This paper will present technical and in-depth analysis of the most widely used anti-forensic technique, the implementation of hidden encrypted storage, as used by complex threats currently in the wild:

- Win64/Olmarik (TDL4)
- Win64/Olmasco (MaxSS)
- Win64/Rovnix/Carberp
- Win64/Sirefef (ZeroAccess)
- Win32/Hodprot

These complex threats use hidden encrypted storage areas to conceal their data and avoid relying on the file system maintained by the operating system. In the presentation the authors will focus on the details of hidden storage implementation as well as the ways in which it is maintained within the system by various kinds of malware. The analysis begins with the initialization procedure and the mechanisms behind it. It is shown which system mechanisms are used to store and retrieve data from the hidden container and the degree to which the malware depends on them. Close attention is paid to the self-defence mechanisms employed by the malware in order to conceal the content kept in its hidden storage areas and protect those contents against modification by the system or by security software. Also a detailed description of the hidden file system is presented for each threat considered, as well as a comparison of its features to the other threats analysed here.

To conclude, an approach is presented on the retrieval of data from hidden storage. We will discuss the steps that should be taken to defeat self-defence mechanisms, locate hidden storage on the hard drive and read plain data.

BYOD:(B)rought (Y)our (O)wn (D)estruction?

Righard Zwienenberg ESET

Nowadays all employees bring their own Internet-aware devices to work. Employers and institutions such as schools think they can save a lot of money by having their employees or students use their own kit. But is that true, or are they over-influenced by financial considerations?

There are many pros and cons with the BYOD trend. The sheer range of different devices that might need to be supported can cause problems, not all of them obvious. This paper will list the pros and cons, including those for Internet-aware devices that people do not think of as dangerous or even potentially dangerous.

These devices are often 'powered' by applications downloaded from some kind of App-Store/Market. The applications there should be safe, but are they? What kind of risks do they pose for personal or corporate data? Furthermore, the paper will describe different vectors of attack towards corporate networks and the risk of intractable data leakage problems: for example, encryption of company data on portable devices is by no means common practice. Finally, we offer advice on how to handle BYOD policies in your own environment and if it is really worth it. Maybe 'Windows To Go' - a feature of Windows 8 that boots a PC from a Live USB stick which contains Win8, applications plus Group Policies applied by the admin - is a suitable base model for converting BYOD into a Managed By IT Device.

Remember: BYOD isn't coming, it is here already and it is (B)ig, (Y)et (O)utside (D)efence perimeters!

Dorkbot: hunting zombies in Latin America

Pablo Ramos ESET

Win32/Dorkbot appeared at the beginning of 2011, and in just a couple of months the volume of Dorkbot detections increased until it became the malware with the most impact in Latin America over the whole year. This threat uses removable media and social networks as its means of spreading and achieved the highest position in threat ranking statistics in only three months. Ngrbot (as its author prefers to call it, or Win32/Dorkbot as the AV industry prefers) stands out as the favourite crime pack for Latin America's cybercriminals and it is widely disseminated through a wide variety of media and vectors.

Lots of small botnets have been detected and are being used for information theft such as personal data and home banking credentials from compromised computers. Spreading through .LNK files via removable media, customized messages through social networks like Facebook, and using local news or compromised web pages, systems are being converted into bots controlled through the IRC protocol.

In this paper the main capabilities and features of Win32/Dorkbot are introduced, and we show its evolution into different versions, starting with AUTORUN spreading, and moving on to the use of LNK files and information-stealing techniques. Win32/Dorkbot.B is the most widely spread variant of this worm, its constructor having been leaked and made available on the web. We tracked down one of the active botnets in the region and reviewed the main activities performed by the cybercriminals.

The investigation came up with thousands of bot computers reporting to the bot master, who used several servers and vulnerable web pages for the implementation of phishing attacks and propagation of threats.

Social media messages have been used to spread copies of this malware through Facebook and Windows Live Messenger. Some of the topics used for spreading included presidents, celebrities and accidents all over the continent and the rest of the world. Also, email accounts are being stolen/hijacked by this malware.

We also comment on why and in what ways Win32/Dorkbot's activity in Latin America differs from the rest of the world, including trends that involve Internet usage, social media and user education. These combinations are a direct cause of the massive infection rates detected in the region. The main features, including botnet control, bot commands and protocols are described in this paper.

Malware and Mrs Malaprop: what do consumers really know about AV? (sponsor presentation)

Stephen Cobb ESET

Friends and family do it, even industry experts sometimes do it: they make inaccurate statements about malware. Some of these malapropisms and misstatements are a slip of the tongue; others reflect more worrying misconceptions about what malicious code is, what it can do, and how it spreads. This presentation reveals the results of a vendor-neutral survey of computer-using consumers who were asked a series of questions about malware in order to better understand what people actually grasp about the malware threat.

We reason that solving a problem requires an understanding of the problem. Anti-virus researchers have worked wisely and diligently over the decades to understand the inner workings of each new wave of malicious code that has infected the world's computing devices, thereby creating numerous problems - no small number of which are ongoing. The outer manifestation of those infections has also been studied in an effort to understand the part of the problem that can be summed up in the question: Why are computers still getting infected? This presentation does not propose to answer that question, but it will attempt to shed fresh light on some variables that play, one might argue, a significant role in understanding the problem:

- What do consumers know about malware?

- Where are they getting their knowledge?

- To what extent do they understand concepts such as risky behaviour?

- Do they change their behaviour after discovering an infection?

LAST-MINUTE PAPER: Gataka: a banking trojan ready to take off?

Jean-Ian Boutin ESET

Seldom do we see a new banking trojan with the size and complexity of Win32/SpyEye appearing. This happened last year with the discovery of Win32/Gataka: a banking trojan that is able to inject content in HTML pages and which exhibits a modular architecture that is easily extensible with plug-ins. Once installed on a computer, Win32/Gataka can be used by botnet operators to steal personal information. As of now, it has been used to steal banking credentials in various countries including Germany, the Netherlands and Australia.

This presentation documents the discovery of this banking trojan along with its internal design and its similarities with another well-known banking trojan: Win32/SpyEye. Among other things, both share the same webinject configuration file syntax. This is a good example of malware writer specialization: webinject files targeting specific institutions are interoperable between different malware platforms. We will also discuss advanced webinject configuration files and how scripts contained in these files can be used to automatically steal personal information and/or attempt fraudulent bank transfers. Finally, we will go over some of the campaigns we have tracked in the past year and show how this new strain of malware is targeting national institutions and how it is evading different two-factor authentication processes.

LAST-MINUTE PAPER: ACAD/Medre: industrial espionage in Latin America?

Robert Lipovsky ESET

Sebastian Bortnik ESET

The malware news today full of new, targeted, high-tech, military grade malicious code such as Stuxnet, Duqu and Flamer, all of which have grabbed headlines. A few months ago, researchers at ESET Security Research Lab noticed a significant spike in the detection rates of a piece of malware occurring in a specific Latin American country. It is quite uncommon to find this kind of propagation pattern, since most of the time the detection rates have similarities across many countries. In addition, it was a very peculiar detection: ACAD/Medre, a signature created for a piece of malware related to the popular design software AutoCAD.

Based on this information, we have analysed the sample and identified an industrial espionage attack developed for stealing designs, maps and blueprints; and which apparently spreads to steal information from Peruvian institutions and companies.

The worm, written in AutoLISP and Visual Basic Scripting language, employs functionality that leads to every AutoCAD file that is opened on an infected machine landing in the attackers' mailbox (in different Chinese email accounts). Furthermore, the fact that it has spread almost exclusively in Latin America makes this targeted attack the first advanced targeted threat of this magnitude reported in the region.

The investigation of the attacks revealed that more than 10,000 AutoCAD drawings were leaked over the period of the last two years.

This paper presents the results of our research and documents the case study from the beginning to the end: its discovery, why it was noticed, how it was analysed, the key features of the code and the overall design of the attack.

My PC has 32,539 errors: how telephone support scams really work

David Harley ESET
Martijn Grooten Virus Bulletin
Steven Burn Malwarebytes
Craig Johnston Independent researcher

Fake security products, pushed by variations on Black Hat SEO and social media spam, constitute a highly adaptive, longstanding and well-documented area of cybercriminal activity. By comparison, lo-tech Windows support scams receive far less attention from the security industry, probably because they're seen as primarily social engineering not really susceptible to a technical 'anti-scammer' solution. Yet, they've been a consistent source of fraudulent income for some time, and have quietly increased in sophistication.

In this paper, we consider:

- The evolution of the FUD and Blunder approach to cold-calling support scams, from 'Microsoft told us you have a virus' to more technically sophisticated hooks such as deliberate misinterpretation of output from system utilities such as Event Viewer and Assoc.
- The developing PR-oriented infrastructure behind the phone calls: the deceptive company websites, the flaky Facebook pages, the scraped informational content and fake testimonials.
- Meetings with remarkable scammers: scammer and scam-victim demographics, and scammer techniques, tools and psychology, as gleaned from conversational exchanges and a step-through remote cleaning and optimization session.
- The points of contact between the support scam industry, other telephone scams, and mainstream malware and security fakery.
- A peek into the crystal ball: where the scammers might go next, some legal implications, and some thoughts on making their lives more difficult.

Cyberwar: reality, or a weapon of mass distraction?

Andrew Lee ESET

Over the last few years, in its insatiable thirst for the new, the security industry has increasingly co-opted military terminology for its marketing, and in return obliging government and military offices (particularly, but not exclusively in the western world) have predicted dire and terrifying scenarios. Couching the threats in the terms of modern warfare, spiced with the magic of 'Cyber', security wonks insist we exist in a new world of CyberWar, CyberTerrorism, CyberAttacks and CyberEspionage where devastation and carnage to our most sacred institutions lurk only a mouse-click away.

Following these now well worn mantras, nation states are gearing up their budgets and their personnel to track, mitigate, offensively counter and defeat these 'new' threats. But where is the evidence? Do we really exist in this strange new world, where we must add to the usual loosely amalgamated mix of malware authors, criminals, hactivists, jihobbyists and straight up vandals the spectre of sinister hacker cells deployed by nation states? Or, are these ideas simply a case of paranoia fuelled by undirected angst about real-world, boots-on-the-ground warfare and the endless 'wars' on drugs and terror? Is security dialogue being hijacked by hype and political expediency? Perhaps the constant exposure to the fantasy and science fiction novels so beloved of the uber-geek has fed into the security industry's hero complex wherein we become the fantastical knights in shining armour (or long leather coat, depending on your milieu), deploying our Low Orbit Ion Cannons against the evil (but faceless) phantoms of the global military industrial complex.

This presentation will take a no-holds-barred, highly opinionated and doubtlessly controversial look at the modern malware industrial complex to examine these important questions.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 4.87%

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: 2
Percentage Detected: 4.45%

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

3. HTML/Iframe.B

Previous Ranking: 5

Percentage Detected: 3.62%

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: 3
Percentage Detected: 2.98%

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.

5. Win32/Sirefef

Previous Ranking: 4
Percentage Detected: 2.13%

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

6. JS/Iframe

Previous Ranking: 6
Percentage Detected: 1.67%

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.

7. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.49%

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/Qhost

Previous Ranking: 8
Percentage Detected: 1.42%

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.

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 9
Percentage Detected: 1.40%

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.

10. Win32/Sality

Previous Ranking: 10
Percentage Detected: 1.29%

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.

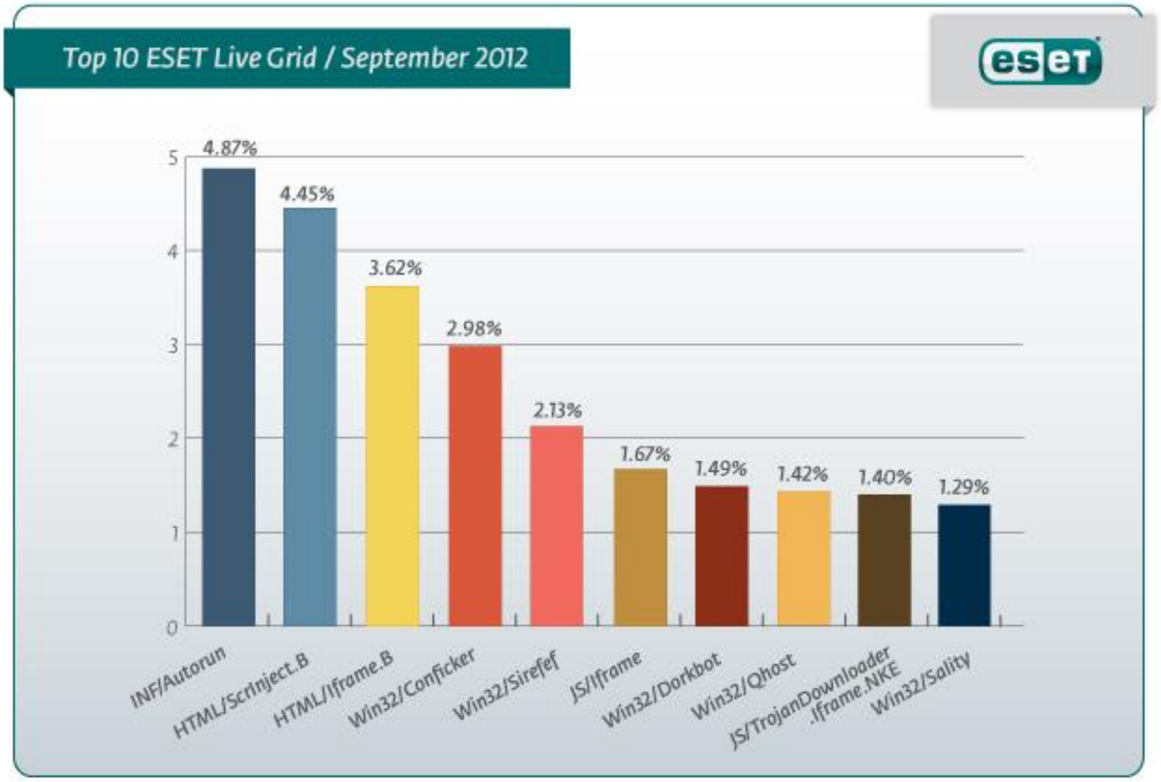
It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

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 4.87% 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