December 2010

Year End Report 2010

Table of Contents

Feature Article I: Bflient.K

Pierre-Marc Bureau, Senior Researcher and Alexis Dorais Joncas

For three months in a row, the Bflient.k malware has been present in the Top Ten Threats list of ESET's monthly report on Global Threat Trends. This article will present two cases of Bflient.k infestation that originated from two Peerfrag botnets[1].

What is Bflient?

Bflient is a commercial kit that is sold to criminals to enable them to create and maintain botnets. Each customer receives a custom version of the kit in order to distinguish one customer from another. Once his purchase is configured and deployed, the customer can command his botnet to perform the usual tasks, such as launching a DDoS (Distributed Denial of Service attack), infect other computers, and most importantly, download and install dubious software at will.

For security researchers, it is often hard to monitor the entire lifecycle of a botnet, from its creation to its day-to-day activity and, hopefully, its takedown. There are so many botnets and so many malware families out there, it is simply impossible to track them all. But sometimes we get lucky and witness a botnet creation or a merger/acquisition. This fall, we saw two Peerfrag botnets entirely drop their 'management' software in favor of a newer model, Bflient.k. This allowed us to learn more about how botnet owners work.

Analysing Botnets

The first botnet's Peerfrag C&C server's domain resolved to a single IP located in the USA.

In the middle of November, the botmaster issued a command to the botnet instructing all the bots to download and install a software detected by ESET as Win32/Bflient.K worm. The new software immediately contacted its C&C server, which sent instructions to install a new set of malware:

- Win32/SpamTool.Tedroo.AN (massive distribution of spam).
- MSIL/Agent.M worm (malware that makes heavy use of process injection to avoid detection from anti-virus products).
- Win32/TrojanProxy.Ranky trojan (installs a proxy that may be used to hide other malicious activities).

In December, a version of IRC/SdBot with very low AV detection was also installed. This malware can be used to control a botnet, just like Bflient is.

The second botnet was managed by a Peerfrag C&C server in Luxembourg. Soon after we started monitoring this botnet, the C&C server's DNS records were updated, adding 9 IPs from three different countries: Luxembourg, Germany and the USA.

Late in November, the botmaster triggered the installation of Bflient.K. Once again, the Bflient software contacted its C&C server and was ordered to download some malware: in this case Win32/SpamTool.Tedroo.AN.

Later on, the botmaster issued commands to install more malwares. A variant of IRC/SdBot appeared soon after and a different type of spambot, detected as Win32/Injector.DPS, was installed around mid-December.

Conclusions

One of the most interesting things we saw in these examples

[1] Peerfrag is the kit used to build the infamous Mariposa botnet, which was taken down in February 2010. Later on, in July, the author of the malware was arrested. More information: http://on.msnbc.com/9ol42i

was that the botmasters totally abandoned their former botnet management software (Peerfrag) in favor of a new one, Bflient. One obvious explanation for this change is that Peerfrag is no longer being maintained, its author being in jail.

We also saw how the botmasters are using the Bflient infrastructure to install various pieces of malware to monetize their botnets, either via sending spam (Tedroo) or possibly pay-per-install (Agent.M, Injector.DPS, etc.).

Of course, the reason all these infections were possible in the first place is that no anti-virus software was running on the affected computers. Otherwise, the malware files would not have been allowed to execute.

Next month, we will see how these apparently independent botnets may actually be related. Effectively, traffic analysis revealed that some IP addresses were seen in network traffic to and from both botnet's.

Feature Article II: The Wikileaks affair and the Cyberworld

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

2010 bows out on a note of controversy and turmoil, not only in the areas of diplomatic, political, international relations and law, but also, probably for the first time in history, with the involvement (willingly or otherwise) of the whole global online community in an initiative aimed at defending the right to free information circulation through various means. Leaving aside all the aforementioned global implications to focus purely IT security issues, this is a multilayered phenomenon, where each layer could be expanded into a security analysis all on its own. For the sake of a comprehensive overview, I'll just focus on a few of its most prominent manifestations here, and on how the Wikileaks affair might prove to be a game-changer in several aspects.

The first consideration, the original sin you might say, is of course data protection itself. More specifically, the question of how potentially compromising data was being gathered, how it was transported and how it was stored. And where in all these processes people with various levels of clearance were able to get their hands on it and misuse it. Various IT security analysts have been pointing out for years now, how insider data abuse is far the most common source of data leakage. According to a 2009 Ponemon study, 59% of corporate workers surveyed stated they would leave with sensitive corporate data upon layoff or departure; 79% of these respondents admitted that their company did not permit them to leave with company data and 68% were planning to use such information as email lists, customer contact lists and employee records that they stole from their employer.

Even though these data have been available for nearly two years, there seems to have been no significant global trend towards major policy changes regarding in-house data protection, nor has there been a reported widespread increase of the use of specialised protection hardware and software. So since nowadays most data, including data formally classified as sensitive, are no longer collected as neatly organised papers in filing cabinets, but digitally, and are therefore very easy to copy and distribute for anyone who can gain access to them, it was inevitable that a major incident would take place sooner or later. And while such incidents in the corporate environment can usually be accommodated within the bounds of economic sustainability, in this case, since the breaches concern classified government documents, mainly related to US international involvement in sensitive areas, the damage done has greatly affected already brittle international relations.

Now to the next part of the story, the after-effects. The first and most immediate development was a series of futile attempts to shut the stable door, firstly through shutting down Wikileaks servers, then by the exertion of coordinated corporate pressure from some of the major online players to disable funding and hamper further distribution of the compromised data. The varied national legislations regarding webhosting made it impossible to block the distribution of data globally, while the funding issue and the involvement of (presumably) independent companies such as PayPal and Amazon sparked an unprecedented backlash from netizens worldwide which resulted in yet another previously unheard of situation. I am talking, of course, about the much publicised Operation Payback, a concerted global hacking offensive, which was in December directed against the supposed offenders against the freedom of information.

This quick and well organised response surprised many, even if the "relative ease" and success of the attacks chosen didn't. Jan-Keno Janssen, Jürgen Kuri, Jürgen Schmidt wrote about it in a thoughtful article for Heise (The H), while ESET's Jeff Debrosse wrote in more detail about the DDoS (Distributed Denial of Service) attacks in his article "Web Weaponization and WikiLeaks", where yet another twist is disclosed: cybercriminals were quick to attach their own interests to all the buzz created around the topic, spreading infected links supposedly leading to more info or resources, and SEO-ing (using Search Engine Optimization techniques) around the Wikileaks buzzwords.

Opinion has been divided on the concept of "ethical hacking", especially in the context of the viability and morality of using measures that may cause inconvenience (and worse) to users of targeted services who may or may not be sympathetic to the Wikileaks stance. Consider, for example, this post which describes an attack on Spamhaus launched on the assumption that the blacklisting of the wikileaks.info site was a further example of harassment of Wikileaks. Spamhaus, however, claims that wikileaks.info is a malicious site intended to take advantage of all the fuss to pursue its own unethical purposes. While we can't say authoritatively who is "in the right" in this particular case, it seems all too likely that criminals will continue to use this controversy to their own advantage We can only hope that the defenders of information's right to "want to be free" do not see the efforts of malware distributors, bot-herders and phishers as "free speech."

A different approach, aimed at a greater dissemination of controversial data rather than disrupting anyone else's work, is now also in effect through the means of Operation Leakspin, but that's already going beyond the field of IT security. Overall it's still not sure whether the whole evolution of the Wikileaks affair is best described as a domino effect or a butterfly effect, or the combination of both, given all the repercussions and sub-plots developing all over the web. However, we are very likely to see change in some of the established protocols regarding data handling and distribution as a direct or indirect result of this incident, or perhaps even the introduction of new ones.

Back to the future?

Daniel Delbert McCracken: "Don't make predictions about computing that can be checked in your lifetime."[2]

Most anti-malware researchers do not consider crystal ball gazing to be within their comfort zone. No-one wants to responsible for self-fulfilling prophecies, giving ideas to the bad guys, or being jeered at a year from now for getting some things wrong. On the other hand, some people do find it useful to hear what people who are considered expert in their field consider likely to be coming down the turnpike. So we asked

[2] David Harley, Robert Slade & Urs Gattiker, "Viruses Revealed", page 552. McGraw-Hill, 2007.

some of our researchers across the globe to read the tea-leaves in an attempt at divination of what the next twelve months hold in terms of upcoming threat trends. It turned out that quite a few of them don't actually drink tea, and most of those who do make use of teabags. However, when we pointed out to them that they could also use coffee grounds or wine sediment[3], we got a much more enthusiastic response, for some reason.

ESET Latin America's research team has put together a paper in Spanish on anticipated trends in 2011, and a translation will be available shortly on the white papers page. However, here is a brief summary of their predictions:

While botnets are far from new, they will continue to grow in significance during 2011: Shadowserver data suggests continuing growth in botnet volumes, while ThreatSense.Net data suggests comparable growth in bot malware volumes, which all indicates that zombie PCs will constitute a higher proportion of all infected systems. It is also expected that following the prominence in 2010 of botnets controlled through Twitter, botherders will experiment with other Command and Control channels. The good news is that recent successes in taking down botnets are expected to continue and perhaps even increase. The Cyber Threat Analysis Center (CTAC) team also agreed that botnets will continue to be a major problem, but hoped that more people will realize that smaller low-profile botnets pose at least as big a threat as the big name botnets monitored so closely by security researchers that they may be abandoned by their creators.

Following the Koobface lookalike Boonana, which has the potential to infect on several operating systems, it's probable that there will be more malware that uses environments like Java to work on multiple platforms: for example, botnets that include zombies running on both Windows and non-Windows operating systems.

BHSEO or BlackHat SEO (Search Engine Optimization), sometimes referred to as index poisoning or index hijacking[4], is by no means new: however the use of social media allows blackhats considerable scope for optimization of this technique for driving user traffic towards malicious sites in real time searching, as was discussed at some length at the 2010 Virus Bulletin conference.

The paper "Trends 2011: Dynamic Malware and the Botnet" will also discuss a number of other trends that are expected to continue in the next year: software vulnerabilities (think Win32/Stuxnet), social engineering, privacy issues in social media, and region-specific malware.

The CTAC team based in San Diego agreed that social media would be a focus for social engineering attacks such as those already commonly experienced by users of Facebook and Google, and believe tthat it's likely that there will be an increasing volume of attacks on other social networking sites such as LinkedIn, Orkut and Twitter, and other search engines such as Bing and Yahoo, especially if the market leaders take extraordinary measures that increase the cost of social engineering attacks on Facebook and Google.

Facebook presents a particular danger: it may continue to try to cure the symptom rather than the disease by presenting the social media privacy invasive issue as something that is what their customers actually want, so that it's the responsibility of their customers to ensure that their data are not shared in ways they wouldn't agree to if they were specifically asked. Some sites (Bebo for example) have actually moved away from the "deny nothing" end of the spectrum towards "deny some

[3] http://en.wikipedia.org/wiki/Tasseography

[4] "A Tangled Web", by Igor Muttik, in "AVIEN Malware Defense Guide" (ed. Harley), Chapter 3. Syngress, 2007.

things" even though sharing as much as possible of their customers' data is fundamental to their business model. Facebook remains equivocal:

The question is, do most of the people who blithely embrace the concept of "information wants to be free" in the social media context do so because they're not equipped to appreciate the security implications of that world view? Automated social networking site scraping tools, as well as leakage of data, will reduce the cost of creating spear phishing attacks, leading to more high-profile attacks. Incautious use of social media and inappropriate or naïve acceptance of publicly available data for authentication[5] can only increase the risks.

If companies like Facebook are prepared to commit to accommodating "comfort levels" of privacy while sharing data where appropriate, social networking will have taken an enormous step forward. In the meantime, though, Facebook's half a billion customers are beset by hoaxes, scams, malware, fake survey-related fraud, and links to malicious sites/SEO/fake security apps: deny-nothing default profiles and advice to "be careful out there" don't offer sufficient security and privacy. That kind of advice has been a feature of security recommendations forever since the Bronze age, but phrases like "don't click on anything suspicious" are less helpful than pointers to what "suspicious" actually means...

The CTAC team confirmed that social engineering would continue to be one of the biggest problems, and not only in the context of malware. Most malware will continue to infect through the usual channels (email, malicious URLs, forums, newsgroups) by tricking the victim into clicking on something ugly. However, it's to be expected that unpleasant surprises like the .LNK vulnerability will also turn up from time to time, possibly long after the bad guys discover them. Further SCADA data-stealing attacks are likely, but probably using spear-phishing and social engineering malware as well as or instead of 0-days, and Trojans rather than self-replicating malware like Win32/Stuxnet. However, Stuxnet's main purpose seems to have been sabotage: while suggestions that the Stuxnet code could easily be adapted to attack all sorts of unrelated installation are largely hype, it's to be expected that the use of malware for purposes of sabotage will remain the subject of speculation and active investigation.

There will be an uptick in automated packet capture and manipulation tools. Firesheep is probably the precursor to many more hijacking tools, and certainly lowers the bar on ID theft. We envisage all sorts of misuse (think teenagers and celebrities getting into each others' accounts). Of course, the hijacking of accounts for purposes of specific fraud (such as Londoning) is already far too common.

Malvertizing campaigns are likely to grow in size and scale, with more effort made to create credible "fake" companies which issue the malvertisements. More targeted attacks of this type are likely, as ability to deploy advertisements to specific niches improves, such as housewives with family incomes over $200K, or male gamers between 18 and 34 years old with incomes above $70K and so forth. One possible group for targeting for many kinds of attack includes baby boomers and the newly-retired, as they may have larger amounts of savings but in some cases may be less aware of social engineering threats and countermeasures.

As utility functions get increasingly computerized, malware will get blamed—incorrectly—for causing or contributing to problems with the services provided by devices. Telephone scams using unsolicited calls from call centres of the type that ESET has been tracking for some time will move away from relying on fear of malware as a "hook" for the installation and

[5] http://blog.eset.com/2009/12/14/your-data-and-your-credit-card and http://www.eset.com/resources/white-papers/EsetWP-SocialSecurityNumbers20090810.pdf

misuse of security software, and instead offer more general support packages, though the misleading use of tools like Event Viewer to flag "problems" will continue to scare victims into buying a service.

On the non-PC side, there will be continued research into infecting cable and ADSL modems and residential gateway routers, with some small-but-notably successful attacks on devices shipping with very old operating systems containing unpatched vulnerabilities. There may be some investigation into targeted attacks on users of MFD devices (hybrid printers, copiers, scanners) Ransomware attacks have been increasing recently: an approach we may see more of is the creation of malware that looks for hard and solid disk state drives incorporating inactive full-disk encryption hardware, and activate them in order to sell the passphrase key for ransom.

Security vendors in the anti-malware space will become increasingly reliant on cloud-based telemetry for reputational analysis and scheduling of malware processing by reverse engineers. At the CARO workshop in Helsinki in May 2010, the number of unique malicious "known" samples was accepted generally as being well over 40 million. We would anticipate that the count will significantly exceed 50 million in the course of 2011. In fact, that figure is certainly pretty conservative: however, gaining an accurate count is something of a challenge, due to such factors as differences in the way that companies count and the time it takes to check for duplicates. However, the virus lab is planning some relevant analysis that we may be able to reference in a future article.

There will be ongoing debate over anti-malware testing: while it's increasingly accepted that dynamic testing is potentially a better representation of the current threat landscape as it affects AV users in real life, the jury is still out on the best ways in which to implement it effectively and accurately. Testers and researchers within AMTSO will continue to play a prominent part in attempting to establish appropriate guidance, but some controversy is inevitable in such a difficult technical area.

There will be more security issues (vulnerabilities and malware) using stolen or fake certificates. (cf. Stuxnet, Zeus, Adobe 0-day, faked SSL cert MITM attacks). Mobile devices will be targeted increasingly: brands that are protected by sound application whitelisting will be much less vulnerable to malware attack, but it's to be expected that fraudulent social engineering attacks will continue.

Contributors to this article include Sebastian Bortnik on behalf of ESET Latin America, Aryeh Goretsky, David Harley, Randy Abrams, and Paul Laudanski.

What happened in 2010?

This is a summary of the most important events in malware during 2010. Considering the most important incidents related to malicious code during the year, and other several events, they could be considered under two major categories (targeted attacks and botnets) plus some other stuff. Below are detailed the most important aspects of each of the attacks that were highlighted during the year.

Targeted attacks

There were two major events related to targeted attacks in 2010: one right at the beginning of the year, and the other one just a few months ago.

First, just a few days after the New Year, it became known that an attack which became known as Aurora Operation had been launched against large technology companies. It was an attack intended to steal intellectual property information from big companies, including Google, who published details of the attack (it was assumed at the time that its primary purpose was

to steal the Gmail accounts of human rights activist in China). The attack consisted of sending malicious e-mails, targeting people in high positions within the companies concerned. During the infection process, the attack attempted to exploit a 0-day vulnerability in Internet Explorer, using Drive-by-Download techniques. Despite being a targeted attack, within a few days it was known that many more companies had been hit, making this incident the most notorious mass attack from the year. According to ESET researchers, they detected more than 650 versions of the exploit code in January, all of them detected by ESET NOD32 as Trojan.JS/Exploit.CVE-2010-0249. There were also identified more than 220 distribution points of the threat, mostly located in Asia (all clues suggest that the attack was of Chinese origin).

Secondly, there was Stuxnet, considered the malware of the year, which consisted of targeted malicious code: not in terms of the organizations that it was sent to, but rather in terms of the technologies that it attacks. That's because the worm was designed to damage only SCADA systems, especially two products developed by Siemens. The malicious code used several 0-day vulnerabilities to spread worldwide through systems, but particularity affected thousands of Windows systems. These only served as a channel for the worm to spread by, but the core malicious routines were designed to damage only industrial systems, used for various critical systems and automatic control of industrial processes, apparently in order to control specialist applications in nuclear power plants. Detected as Win32/Stuxnet.A, it infected 45.000 industrial control systems throughout the world. In its first weeks of life, ESET researchers found that 52.2% of infections of the threat had been detected in Iran, inspiring speculation about whether Iran was the primary target. Over subsequent weeks, the rates were reduced to more normal values throughout the world. Stuxnet occupied the attention of the information security community because of the ways in which it infected, as without doubt it was developed by a highly skilled group of people, with an unusually comprehensive knowledge of SCADA systems, which inspired multifarious opinions about the possible origins of the threat.

For more information read the white paper "Stuxnet under the microscope"

Botnet

Secondly, incidents have been observed over past months that prove the botnet's growth as a threat. Threats like Zeus, the administration panel for botnets used around the world, have made several appearances throughout the year. These are especially associated with the theft of banking credentials, one of its most significant functionalities. That was the case of Koobface, another bot that remained active throughout the year, with several campaigns spread in April (false videos and codecs campaign), May (similar campaign on Flash videos) and August (fake security camera videos). Finally, in October there appeared a new Trojan variant affecting Linux and Mac OS, called Boonana.

At the end of the year, Zeus regained prominence as the author announced the end of the development (and possible merger with SpyEye) and a few weeks later, various operations ended in the arrest of criminals using Zeus throughout the world: eight people were caught in both the U.S. and Moldova.

Earlier this year we saw the takedown of two major bot networks , Mariposa and Waledac. (ESET researchers have been collaborating in the provision of information relating to this botnet through the year.) In the second half of the year in the Netherlands we saw the dismantling of Bredolab, another major network that had been active for two years, infecting more than 30 million systems. However, there is some evidence of renewed activity, new variants of the Trojan having been

identified. Finally, although it could not be completely dismantled, some of the command and control centers of Koobface were compromised, which allowed researchers to ascertain important detail about their operation and success.

Finally, also in the botnet arena, there were new experiments involving the creation of smartphone zombies, setting up a network of more than eight thousand victims: however, this was only used for research purposes. New technologies to manage botnets througt Twitter were also highlighted. Throughout the year, ESET Laboratory detected two threats using these technologies, sending commands and instructions to zombies via tweets.

Other threats

To complete this summary of 2010's biggest threats, it is important to mention the continued activity of Conficker, still infecting organizations throughout the world. The worm that emerged in 2008 is still in operation and spreading with remarkably high infection rates, considering that it spreads through vulnerabilities that have already long been patched.

Also, there have also been several cases of threats to various non-Windows platforms such as Mac OS, which has suffered some incidents, especially Trojan incidents. Malware has also been propagated against Linux. In one such case a Trojan was hosted on an official repository of free software for over six months. New variants of malware for mobile devices were also identified, notably the first variants for some operating systems. For example, Android saw its first SMS Trojan: in this case the infected device sent text messages to premium numbers, resulting in economic loss to the victim.

Conclusion

In terms of malware it was a busy year, with threats in various platforms, a growing incidence of botnets, the emergence of innovative new malicious code, as well as the continuance of some threats that have been for years in the wild.

This last attribute (the combination of old threats with other, more recent threats) has made 2010 a year of dramatic growth for malware.

The Top Ten Threats of 2010

1. Win32/Conficker

Percentage Detected: 8.45%

The Win32/Conficker threat is a network worm originally propagated by exploiting a 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 Autorun nonetheless: 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.

2. INF/Autorun

Percentage Detected: 6.76%

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.

3. Win32/PSW.OnLineGames

Percentage Detected: 3.59%

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

4. Win32/Agent

Percentage Detected: 2.25%

ESET NOD32 describes this detection of malicious code as generic, as it applies to members of a broad malware family capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which refer to this file or similar ones created randomly in other operating system folders, which enables the process to run at every system startup.

This label covers such a range of threats, using a wide range of infection vectors that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product ☺), good patching practice, disable Autorun, and think before you click.

5. Win32/Sality

Percentage Detected: 1.69%

Sality is a polymorphic file infector. When run, it starts a service and manipulates registry keys to hamper security activities in the system and to ensure the start of malicious process at 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

6. INF/Conficker

Percentage Detected: 1.57%

INF/Conficker is related to the INF/Autorun detection: the detection label is applied to a version of the file autorun.inf used to spread later variants of the Conficker worm.

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun above.

7. Win32/Tifaut.C

Percentage Detected: 1.04%

The Tifaut malware is based on the Autoit scripting language. This malware spreads between computers by copying itself to removable storage devices and by creating an Autorun.inf file to start automatically.
The autorun.inf file is generated with junk comments to make it harder to identify by security solutions. This malware was created to steal information from infected computers.

See INF/Autorun above for discussion of the implications of software that spreads using Autorun.inf as a vector.

8. HTML/ScrInject.B

Percentage Detected: 0.92%

This is a generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

Malicious scripts and malicious iframes are a major cause of infection, and it's a good idea to disable scripting by default where possible, not only in browsers but in PDF readers. NoScript is a useful open source extension for Firefox that allows selective disabling/enabling of Javascript and other potential attack vectors.

9. Win32/Spy.Ursnif.A

Percentage Detected: 0.78%

This label describes a spyware application that steals information from an infected PC and sends it to a remote location, creating a hidden user account in order to allow communication over Remote Desktop connections. More information about this malware is available at http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm?lng=en

10. Win32/Qhost

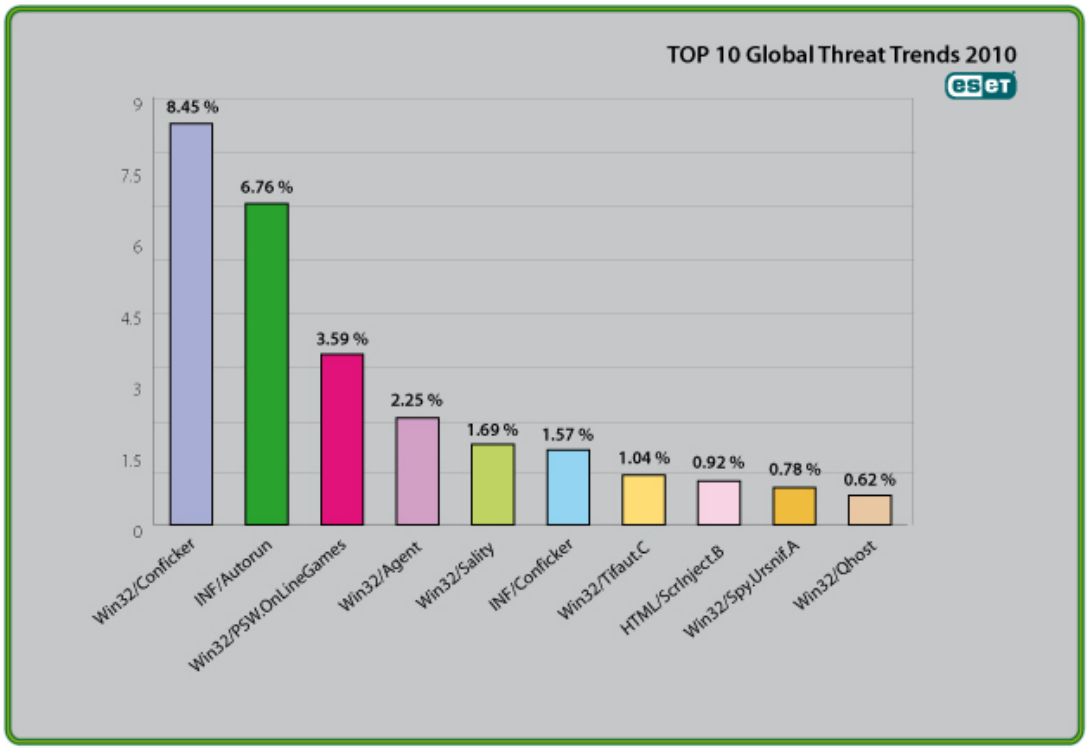
Percentage Detected: 0.62%

This threat copies itself to the %system32% folder of Windows before starting. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker. This group of trojans modifies the host's file in order to redirect traffic for specific domains.

This is an example of a Trojan that modifies the DNS settings on an infected machine in order to change the way that domain names are mapped to IP addresses. This is often done so that the compromised machine can't connect to a security vendor's site to download updates, or to redirect attempts to connect to one legitimate site so that a malicious site is accessed instead. Qhost usually does this in order to execute a Man in the Middle (MITM) banking attack. It doesn't pay to make too many assumptions about where you are on the Internet.

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 the past year, with almost 8.45% of the total, was scored by the Win32/Conficker 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