December 2011

Year End Report 2011

Table of Contents

2011: A dangerous year online

***Urban Schrott**, IT Security & Cybercrime Analyst, ESET Ireland*

ESET Ireland's research in 2011 showed that 1 in 4 Irish computer users has had his or her computer crashed or otherwise damaged by viruses or malware. We found that 1 in 5 users had experienced a malware infection or data theft while 14 percent said they were hacked or had their social media accounts hijacked. Nearly ten percent of the survey population had been cheated, had their credit cards or private information abused, or found their system was used to transmit spam. We think these numbers reflect the following trends that we observed in 2011, both in Ireland and around the world.

Online incentives

In 2011 we saw further expansion of social media, with more and more businesses using social networks as a platform for communication with customers and a means of building their brand. Online shopping and financial transactions also increased sharply in spite of a sluggish global economy. The latest statistics show that the amount of money spent for Christmas shopping online rising around 14% over last year and almost 39% over 2008. All this has made it more worthwhile than ever for cybercriminals to invest time and resources in trying to divert some of the money that is spent or transferred online into their own pockets.

Faking it

While advanced technologies are constantly being developed to combat malware, cybercriminals are busier than ever finding ways to circumvent security software by aiming directly for the computer users themselves. The human factor has always been the weakest link in cyber-security and making people's curiosity work against them has always been a tactic favored by scammers. In 2011 we saw social media users targeted by this form of "social engineering" in a big way.

Fake links to stories or videos hit social networks such as Facebook or Twitter throughout the year. These links purported to offer "shocking news" or "rare video" about a widely publicized topic but in reality lead to malicious sites, often infecting users with malware, or to survey scams that automatically spammed their online friends with more fake links. Some of the more notable topics abused in this fashion in 2011 were the Japan earthquake, the Royal wedding, the killing of Bin Laden, the Oslo massacre and the deaths of Amy Winehouse and Steve Jobs. Due to people's inquisitive nature, many kept clicking and compounding the problem, indicating that the numerous warnings about this behavior have not yet sunk in.

Search engine poisoning

A widespread variation of the "hot news" scam came in the form of search engine poisoning. Because people tend to search online for hot topics (or news of hot celebrities), cybercriminals try to poison web search results by creating web pages that refer to current hot topics. Through fraudulent abuse of legitimate search engine optimization (SEO) techniques that are widely used in online marketing, the bad guys trick search engines into featuring their pages prominently in search results. The effect of this "black hat SEO" can be that people clicking on apparently legitimate search results are taken to malicious websites where their computer gets infected with malware, diverted to online pharmacy or pornography sites, or subjected to a variety of scams that try to part the user from their money or their personal data.

Botnets

In 2011, a lot more computer users learned that, once their computer became infected with malware, it could become a "zombie" machine. These machines are routinely orchestrated into large networks called botnets, thousands upon thousands of infected computers remotely controlled to do the bidding of their controller or "botmaster". These botnets are used, without permission or knowledge of the owners the computers that make up the network, to send out spam, attack websites, and distribute malware or illegal content (such as pirated software or child pornography). While several large botnet organizations have been successfully defeated this year, the scope of them surprised some researchers and, as is the case with icebergs, the fear is that a lot more danger remains hidden, including smaller botnets that are intended to be less conspicuous but still profitable and capable of taking down websites. For example, qqq.

Support scams

As computer users learn more about avoiding malware infections and get smarter about spending money on dodgy websites, cybercriminals have a backup plan to scam users: call them on the phone. These "cold call" support scams go like this: "Hello, we're calling you from We-Fix-Computers-Company and we will remotely rid your computer of any viruses and other trouble for a modest fee of several hundred euros."

In 2011 we heard a lot of variations on this theme, with some scammers being more credible and persistent than others. The result? A surprisingly large number of trusting people allowed scam artists access to their computer under these false pretenses. What the scammers then do with that "authorized" access is pretty much whatever they feel like doing, from stealing as much personal information as they can find on the computer's hard drive, to installing a back door for future illicit access, all from the safety of a remote connection. Then the trusting consumer hands over their credit card details to pay the "fee" for this support/abuse.

What to do?

The first step towards being safe from any of these threats is knowing about the dangers. Do not count on software alone to protect you, but stay informed of the threats and scams out there in order to be better able to avoid them. ESET Ireland keeps computer users informed through Facebook and our own blog. You will also find valuable news and information on the ESET Threat Blog.

But most of all, as we keep repeating: Think before you click.

2011: Not all bad news on the cyber-front

***Stephen Cobb**, Security Evangelist ESET, North America*

There's no doubt that 2011 was a year of threat proliferation in cyberspace. Old threats were revived and new attack vectors opened up. For example, sales of smartphones and tablets soared, all of them potential attack platforms, and we saw social engineering on the rise in social media and targeted email attacks like spear-phishing. Meanwhile, mean-spirited, human-on-human social engineering flared up in cold-call support scams. Malware continued to evolve throughout the year, as we documented on the ESET Threat Blog and in conference papers and published articles. ESET's Virus Lab continues to collect well over 100,000 unique malware samples per day.

So you might be tempted to conclude that 2011 was a bad year for those concerned about protecting data and information systems. Yet there were some hopeful signs throughout the year, steps taken to take down the bad guys, and strong signals to the good guys to do better. One of the most notable areas of success was the international assault on botnets, some operators of which are now in custody. There were also arrests in a variety of cybercrime cases, from the Florida man who was hacking celebrity email accounts, to phone hackers working for the News of the World in the UK, and a Seattle gang that combined old-fashioned breaking-and-entering with war-driving and network hacking to steal everything from computers to paychecks.

Botnet operators are especially loathed, by companies and consumers alike, not just because of the crimes they enable—everything from spam to fraud, financial theft, DDoS and data ransoming—but also because of the huge waste of resources that botnets represent. The time and energy consumed by efforts to fend off botnet-enabled activities, like the massive server resources required to cope with spam, are a drain on the global economy.

In the first quarter of 2011 we saw the Rustock botnet fall in the face of combined efforts from Microsoft, the U.S. Marshals Service, the Dutch High Tech Crime Unit, and China's National Computer Network Emergency Response Technical Team (CNCERT). One of the key steps in that takedown occurred in the first month of the year; that's when Microsoft filed a temporary restraining order against "John Does controlling a computer botnet thereby injuring Microsoft and its customers." The significance of this order was the platform it created for a sudden and coordinated seizure of the botnet's command and control servers before the bot herders had a chance to react and move them elsewhere.

At one point in its five year existence existence Rustock was pumping out nearly half of the world's spam. Based on McAfee's helpful 2009 carbon footprint analysis, that spam was wasting electricity at the rate of 15 billion kilowatt-hours per year, enough to power over a million homes in the United States. You could say that taking down Rustock reduced greenhouse gas emissions by the same amount as taking 1.5 million passenger cars of the road.

In September, Microsoft announced it had taken down another botnet, known as Kelihos (Waledac 2.0). In an operation code-named Operation b79, Microsoft used legal and technical measures similar to those employed in its previous botnet takedowns, including an ex parte temporary restraining order—enabling the seizure of assets such as domain names without first notifying the other party—and claims of trademark infringement under the 1946 Lanham Act (an anti-spam strategy advocated by the author over ten years ago).

The FBI also engaged in some spectacular takedowns in 2011. In April they hit the botnet based on the Coreflood Trojan which had infected millions of PCs with a keylogger that sent banking credentials and other sensitive information to the botnet's command-and-control servers. The FBI seized the servers and replaced them with new ones that could distribute instructions to disable the Trojan on user machines, thereby opening a new front in the war on malware: legally sanctioned removal of malware by a third party. In November the U.S. Department of Justice took down "DNS Changer," arguably the biggest botnet dismantled so far (said to be more than twice the size of Rustock).

Besides taking down botnets, the FBI was busy making cases against the bad guys and making life harder for cybercriminals on the run. Two big cases came to light in December alone. On December 15 in Las Vegas, 16 people were charged with bogus

Internet sales of merchandise like automobiles, travel trailers and watercraft. A week later, 14 Romanian citizens were charged with conspiracy, fraud and identity theft offenses stemming from their alleged participation in an extensive "phishing" scheme; three of the charged defendants have been extradited from Romania to the United States.

Of course, reducing cyber-threats is not just about locking up the bad guys. Legitimate companies that earn returns for their investors by operating in cyberspace need to play their part in helping cyber-citizens protect their personal data, even as we spend more time online and use an ever-expanding range of digital communication channels. According to Nielsen, Google and Facebook were the most visited sites of 2011. Some 153.4 million people visited Google sites each month, on average, while Facebook traffic averaged 137.6 million (based on web traffic from home and work computers from January through October 2011 and does not include mobile visits).

Besides being 2011's two most visited websites, Facebook and Google this year became two of the largest companies operating under an FTC consent decree due to complaints about privacy practices. Consumers concerned about privacy and security should see this is a good thing, considering what has happened to Microsoft over the last 9 years. Prior to the 2002 FTC action, Microsoft had a fairly dismal information security track record. Since then the company has transformed itself into a leading force in several key areas of cyber-security, botnet takedowns being just one of them. What Google and Facebook have in common with Microsoft is a business model that relies on the continued growth of, and trust in, networked technology. In other words, they have every incentive to work hard to reduce cyber-threats. Here's hoping we get more good news to report in 2012.

2011 in Review, a Wordsmith's Diary

*The year as a series of malware-related posts on the ESET Threat Blog, aggregated by **David Harley**, ESET Senior Research Fellow.*

January

Blog posts in January 2011 continued themes already familiar from 2010: Stuxnet and comment spam. Comment spam is with us always, of course, and from time to time over the year I've shared some of the more amusing examples in the blog (I particularly like Agony Column for Comment Spammers and Responsible Disclosure and Fish Pedicure).

Stuxnet seemed at one point to be almost as constant a feature of our blogging lives. Well, mine, anyway. In fact, such was the deluge of Stuxnet-related information (not to mention the misinformation) that for a while I was maintaining a series of resource blogs with pointers to some of the better commentary, even after the ESET research team had moved on to other malware. January saw publication of the last update of our Stuxnet Under the Microscope report (or War and Peace, as it's known in some quarters on account of its extreme length). Of course, the fuss hasn't died away yet: even as I write this in December I've had to turn down requests to write chapters or articles on Stuxnet, and I would venture to predict that we will go on hearing more interesting theories like the one that links Stuxnet, Duqu and Conficker. (What next? Brain and Elk Cloner?)

Cold-call scamming of the Windows support call kind raised its ugly head again, and continued to be a threat to innocent PC users throughout the year. And while Win32/Sheldor hasn't received much individual attention over the year, its name has

cropped up again and again in presentations by our Russian research team and their associates Group-IB, most recently in connection with the currently hot topic of Win32/Carberp. Meanwhile, Sebastian Bortnik shared some very interesting information on phishing. And Facebook changed its privacy settings yet again.

February

Aryeh Goretsky posted about Microsoft's inadvertent inclusion of a Trojan in the Microsoft Catalogue, and Randy explained how it might have happened (but not when he was working there!). Randy also explained how to update Facebook privacy and security settings, and I commented on a 419 spreading through Facebook. We both met a lot of people at RSA (and in my case at the first AMTSO meeting of the year). There was a spate of free iPad scams on Facebook. Library users in Manchester, England, risked getting more than the latest Maeve Binchy novel when public access machines were found to be booby-trapped with keyloggers, and charity scammers took advantage of the recent earthquakes in New Zealand to line their own pockets.

March

Facebook privacy remained a contentious issue. (Ho-hum.) Steve Gold quoted me as saying Android malware was terrifying, which seemed a bit overblown at the time even to me, but the spirits must have been whispering in my ear: almost immediately about 50 malicious applications had to be pulled from the Android Market (no wonder some people think anti-malware experts write the malware ourselves).

We discovered an interesting case of TDL4 being used to install other malware (courtesy of Aleksandr Matrosov and Pierre-Marc Bureau). Scammers started iPeddling "free" iPad 2s. There was some belated fuss about how easily SSNs are cracked in the post titled Social Security Numbers: deja vu all over again. There was a flurry of ATM attacks, skimming and the like. We reported on various ugly manifestations that arose in the wake of the Japanese earthquake/tsunami: Black Hat SEO, spam, scams, hoaxes, and even Microsoft got into the act by promising to contribute funds if people would promote Bing on Twitter. (In the end they backed off, but did contribute a sizeable sum). The BBC reported that the News of the World had hired a hacker to steal emails (that story is still evolving, with numerous arrests occurring as the year wore on). Facebook was slammed for using its customers' names and faces in "sponsored stories" (another story that is still running).

April

Alexandr Matrosov, Eugene Rodionov and myself put together a series of articles on the TDSS botnet for the Infosec Institute. RSA told us they'd been victims of an APT attack but were pretty sparse on detail: however, it became clear that this was probably a phased attack on a number of companies. Internet connections to Georgia and Armenia were cut by a 75-year-old woman stealing cable. 2011's quota of data breaches took off in a big way: Epsilon, the State of Texas, Sony, et al.

May

Paul Laudanski blogged comprehensively on Facebook privacy, such as it is. Your humble scribe combined AMTSO and CARO workshops in Prague with a presentation at the EICAR conference in Austria. It's a tough job, but someone has to do it. Osama Bin Laden was killed and a million scammers used the occasion to catch the interest of potential victims. The Electronic Frontier Foundation noted some interesting updates concerning the FBI's monitoring of the PCs of suspected criminals, foreshadowing the later fuss about the German

government's Bundestrojaner. Ulm University reported that 99.7% of Android users are open to compromise. Paul Laudanski also blogged (a little more briefly) on password practice, a blog that seems to have attracted enormous attention over the year. The end of the world didn't happen.

June

Aryeh Goretsky's long-awaited paper on backing up data was published. Paul Laudanski wrote about LinkedIn privacy and Randy Abrams wrote about the disconnect between perception, behaviour and safety among social media users. Cameron Camp wrote about everything in sight, everyone got uptight about Anonymous and LulzSec, and the International Monetary Fund came under threat. The TDSS network tried out a peer-to-peer topography as an alternative to a more traditional C&C model.

July

There was a great deal of continuing fuss about the evolution of TDSS into an "indestructible" botnet. (No, Virginia, that isn't quite what peer-to-peer means!) ESET invited you to Tell ESET about Facebook malware. (You still can, by emailing askeset@eset.com: we're always interested in new spam, scams and badware.) Randy Abrams talked about Google+ in several blogs, and Cameron Camp got a head start on the prognostication game that preoccupies so many people at the *end* of the year by asking "1 in 20 mobile devices infected next year?" Aleksandr and Eugene dug up some interesting data about Win32/Cycbot and the Ready to Ride group, and built on their work with Group-IB on Hodprot.

Google got very heavy on G+ users they suspected of concealing their identity behind a pseudonym, at least one of whom turned out to be genuinely famous. Or infamous, if you're unlucky enough to have heard William Shatner's early foray into pop music, the very essence of a criminal record. Indian support scammers developed an interesting new technique, trying to convince you they could "see" your "infected" computer by identifying its CLSID. Android malware became increasingly in-yer-face, Stuxnet speculation continued to flourish, and Robert Lipovsky uncovered a personal message to the ESET lab from the packer writer for a Zbot variant.

August

ESET Canada's Sébastien Duquette did some well-received blogging about Win32/PSW.OnlineGames.OUM, a very prevalent gaming password stealer. Hodprot graduated to a white paper all of its own. Dmitry Alperovitch's Shady Rat report generated a surprising amount of controversy, considering that it was just one example of a long-known cyberissue, i.e. targeted malware pursuing a political agenda. (I think I just coined another buzzword.) Robert Lipovsky told us about a surprisingly conversational Trojan downloader. Cameron wrote about Android malware and concerns about mobile Facebook, and the UK government fretted about the use of social media and mobile devices to foster anarchy in the UK. I got very philosophical about IP theft, for someone whose books have been massively pirated, and had a very public discussion with Aryeh about his newly published paper on PUAs, PUPs, the universe and everything. Pierre-Marc alerted us to links between Kelihos, Storm/Nuwar, Waledac and mule-recruitment spam. Aryeh reflected on 1000 days of Conficker. Hasta La Vista, Bootkit: Exploiting the VBR discussed interesting developments in x64 malware (well, it interested us). And another paper by Aryeh discussed good backup practice for consumers/home users.

September

As usual, the month of September marks the start of a very busy conference season. The anniversary of 9/11 was, once again, shamelessly used by spammers and scammers as a hook to hang Bad Things on. There were further claims that antivirus is dead. (Yet here we still are.) The Induc virus, which in 2009 was an interesting oddity with shades of a 1980s Proof of Concept paper, returned in an altogether less cuddly guise.

Certificate Authorities started to look like a decidedly flaky concept, and Robert and I joined forces to consider the implications of some of the failures. I dished the dirt on certs and SSL got another workout. Stephen Cobb introduced himself with an article about an online rental scam he came across while looking for an apartment to rent near ESET's North America headquarters in San Diego.

The UK's National Health Service continued to hemorrhage data on USB devices and I considered going back to offer my services for at least 30 nanoseconds. The state of Massachusetts meanwhile released information on about 2.1 million users' lost data, including 14 years worth of data relating to 800,000 people from one hospital alone. Dan Clark wrote about a couple of minor Mac threats while Qbot played with certificates and Stephen joined the dots on Digital Certificate Security. Cameron and I mulled over various aspects of the endlessly fascinating Facebook phenomenon.

October

Barcelona was invaded by the antivirus industry for the Virus Bulletin conference, where it was hard to avoid tripping over ESET presentations. Stephen noted another healthcare data leakage disaster and Cameron observed that US government security breaches have risen 650% in five years. Meanwhile Andrew Lee (like so many of us) mourned the passing of Steve Jobs.

A little more encouragingly, Operation Swiper busted a $13 million dollar ID theft ring. One person demonstrated dramatically how much data Facebook may hold on individual users, and the Chaos Computer Club drew our attention once more to the issue of "government Trojans" (expect to hear more about those in 2012…) Andrew Lee, ESET CEO and de facto obituary correspondent, noted the passing of Dennis Ritchie, to whom all of us who've ever programmed in C owe a debt (though I was always more of a Pascal man myself). Then Symantec detected Facebook as a malicious site, and not all of us were convinced that it should be considered a false positive, so Cameron's notes on making your FB account more secure were well-timed. My Russian colleagues shared some more information on the ongoing evolution of TDL4. Stephen and I blogged on search poisoning generated around the death of Gaddafi, while Robert and Pierre-Marc wrote about OSX/Tsunami. We shared some Duqu analysis and I was reminded of the venerable Craig Shergold hoax by a Facebook sharing sympathy hoax.

November

Robert told us about a rather interesting PHP Autorun worm from the Czech republic. Peter Stancík (a colleague in Slovakia) and I got into a lengthy discussion about sites like pwnedlist.com that offer a way to check on whether your credentials have found their way into one of the account-name/password pair databases dumped onto the Internet by various bad actors for anyone to access, and I summarized that debate into a lengthy blog post. There were so many Facebook issues I can't be bothered to list them all separately, but Facebook Likes and cold-call scams combines two of my "favourite" bêtes noires. In Facebook Facing FTC Mandated

Privacy Changes, Stephen looked at what may be make-or-break issues for Facebook and its treatment of privacy, and I wrote about a Facebook video scam, which caught a great deal of attention, looking at a classic scam. Stephen even produced a short video to further explain the threat.

Andrew's open letter to Congress on the ill-considered SOPA/PIPA legislation proposals also garnered much attention. Aryeh picked up the theme of Facebook problems with a couple of posts considering a spate of reports concerning some very disturbing material that found its way onto Facebook's pages. Stephen prepared us for Cyber Monday with a collection of ten tips for safer online shopping, and the first of a new spate of blogs on Carberp and banking Trojans hit your screens, while Facebook proved once again to be the natural home of old virus hoaxes.

December

CarrierIQ proved to be a continuing theme through December, as the story evolved from accusations of rootkit installation to concerns about which devices and carriers were involved, to the involvement of the FBI. Carberp continued to attract attention and got its own white paper. In fact, Russia in general attracted much attention, with the political DDoS-ing flagged by Sébastien associated with the Win32/Flooder.Ramagedos botnet. ESET researchers kicked off the series of predictive material that the media traditionally demand at the end of the year, and our paper on "the top ten things you can do to protect yourself online" was updated. Cameron wrote several posts about the importance of protecting customer credit card data, then we read the news on Christmas Day that Anonymous had charged charitable donations to customer credit cards found unencrypted on the servers of a company called Stratfor.

Some published papers and articles

Conference Papers

Same Botnet, Same Guys, New Code

By Pierre-Marc Bureau

A paper describing the functionality and P2P protocol of Win32/Kelihos, its evolution and its points of similarity to Win32/Nuwar (Storm) and Win32/Waledac.

First published in Virus Bulletin 2011 Conference Proceedings*

Fake But Free and Worth Every Cent

By Robert Lipovsky, Daniel Novomesky, Juraj Malcho

Two years on from "Is there a lawyer in the lab", greyware and Possibly Unwanted Applications offer serious challenges for security vendors.

First published in Virus Bulletin 2011 Conference Proceedings*

Daze of Whine and Neuroses

By David Harley and Larry Bridwell

The Anti-Malware Testing Standards Organization (AMTSO) has shaken up the AV testing world and attracted much controversy. But has it outlived its usefulness? And what is the future of detection testing?

First published in Virus Bulletin 2011 Conference Proceedings*

Security Software & Rogue Economics: New Technology or New Marketing?

By David Harley

Presented at the 2011 EICAR conference in May 2011, this paper contrasts existing malicious and legitimate technology and marketing, considering ways in which integration of security packages might mitigate the current wave of fake applications and services.

Articles

Socialisation, social engineering, and securing the enterprise

By David Harley, November 2011

An article for (SC)2's Security Zone column in Computer Weekly, on how businesses should empower all IT users to play an active part in protecting corporate data.

Hearing a PIN drop

By David Harley, September 2011

An article for Virus Bulletin offering preliminary results from research into selection strategies for numeric passcodes such as ATM and smartphone PINs.

Originally published in Virus Bulletin, September 2011.*

Security Zone: Antivirus testing standards at a crossroads

By David Harley, May 2011

An article for Computer Weekly (May 2011) that suggests that the latest paper approved and released by AMTSO may be its most important document in years.

TDSS part 1: The x64 Dollar Question

By Aleksandr Matrosov, Eugene Rodionov & David Harley, April 2011

Considers and contrasts the distribution and installation of the TDL3 and TDL4 bootkits.

TDSS part 2: Ifs and Bots

By Aleksandr Matrosov, Eugene Rodionov & David Harley, April 2011

Looks in more depth at the internals of the TDSS malware.

TDSS part 3: Bootkit on the other foot

By Aleksandr Matrosov, Eugene Rodionov & David Harley, April 2011

The last part of the series describes the TDSS loading process.

Perfect Ten: Truth and Prognostication

By David Harley, January 2011

David Harley meditates on security soothsaying and takes a peek into his own crystal ball.

Rooting about in TDSS

By Aleksandr Matrosov & Eugene Rodionov

This article for Virus Bulletin describes a utility for dumping the TDSS rootkit's file system. Made available January 2011, but originally published in Virus Bulletin, October 2010.*

ESET researchers also contributed too many articles to list to SC Magazine's Cybercrime Corner, and to blogs such as (ISC)2, Securiteam, AVIEN, Infosecurity Magazine, AMTSO, Security Week, and many others.

White Papers

Ten Ways to Dodge CyberBullets: Reloaded

By David Harley, December 2011

An updated version of the paper "Ten Ways to Dodge CyberBullets", addressing the question "what are the top 10 things that people can do to protect themselves against malicious activity?"

Problematic, Unloved and Argumentative: What is a potentially unwanted application (PUA)?

By Aryeh Goretsky, November 2011

This paper was started as the result of a rather innocuous request: A co-worker asked for an explanation of what the class of software ESET calls potentially unwanted applications (PUAs).

Win32/Carberp: When You're in a Black Hole, Stop Digging

By Aleksandr Matrosov, Eugene Rodionov, Dmitry Volkov and David Harley, December 2011

This paper consolidates information published by ESET and Group-IB researchers on Russian malware that attacks Russian RBS (Remote Banking Systems) transactions: now updated to version 1.1 to include additional material.

Options for backing up your computer

By Aryeh Goretsky, August 2011

If you know you need to back up your data but you're not sure how to do it, here's a practical guide on how to get started.

Hodprot: Hot to Bot

By Eugene Rodionov, Aleksandr Matrosov, and Dmitry Volkov, August 2011

A comprehensive analysis of Win32/Hodprot, one of the families of malware most used in banking fraud in Russia and its neighbours.

Problematic, Unloved and Argumentative

By Aryeh Goretsky, July 2011

What is a potentially unwanted application (PUA)? This paper gives some examples of "potentially unwanted" and "potentially unsafe" applications, explaining how they differ from out-and-out malware.

The Evolution of TDL: Conquering x64 (revision 1.1)

By Eugene Rodionov and Aleksandr Matrosov, June 2011

A comprehensive analysis of the TDSS/Olmarik/Alureon family, which has learned some radical new tricks. Updated to include information on a new plugin making radical changes to Olmarik's botnet.

Hanging on the Telephone

By David Harley, Urban Schrott and Jan Zeleznak, February 2011

As if fake anti-virus products weren't bad enough, nowadays we have unsolicited phone-calls from fake AV helpdesks. ESET researchers tell you more about support scams.

Stuxnet Under the Microscope

By Alexandr Matrosov, Eugene Rodionov, David Harley and Juraj Malcho, January 2011

Version 1.31 of a comprehensive analysis of the Stuxnet phenomenon, updated to add pointers to additional resources. This is probably the last update of the document, but further relevant resources will be added to a list here.

The Top Ten Threats of 2011

1. INF/Autorun

Percentage Detected: 5.84%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course,

malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://blog.eset.com/?p=94 ; http://blog.eset.com/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. Win32/Conficker

Percentage Detected: 3.69%

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://blog.eset.com/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. Win32/Sality

Percentage Detected: 1.88%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.
It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:
http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

4. Win32/PSW.OnLineGames

Percentage Detected: 1.85%

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

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

5. HTML/Iframe.B

Percentage Detected: 1.23%

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. HTML/ScrInject.B

Percentage Detected: 1.22%

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

7. Win32/Autoit

Percentage Detected: 1.17%

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

8. Win32/Bflient

Percentage Detected: 0.92%

Win32/Bflient is a worm that spreads via removable media and contains a backdoor. It can be controlled remotely and ensures it is started each time infected media is inserted into the computer.

9. Win32/Tifaut

Percentage Detected: 0.77%

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.

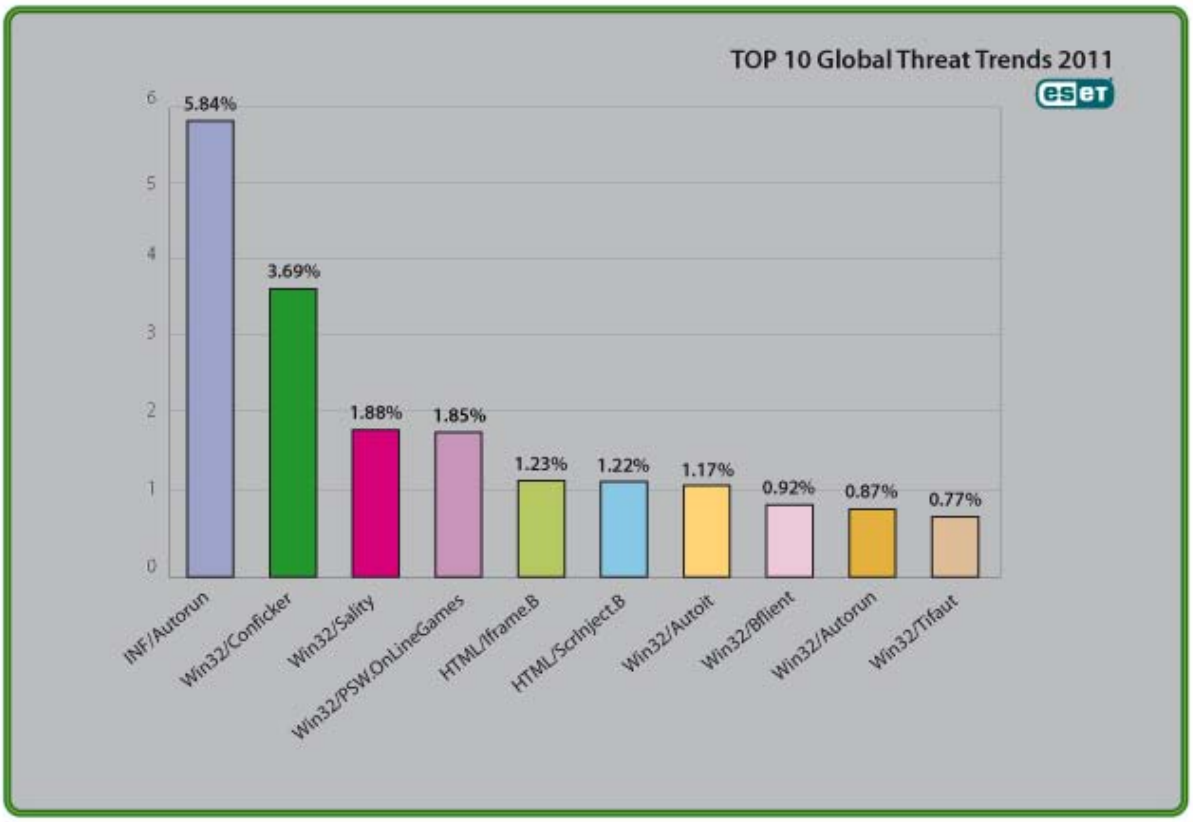
10. Win32/Spy.Ursnif.A

Percentage Detected: 0.74%

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

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 5.84% 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