March 2011

Feature Article: BlackHat Japanning

ESET

Table of Contents

Feature Article: BlackHat Japanning....3
Spring is Here....5
Unwanted Flattery (E-Set reset)....5
And the Firewalls Came Tumbling Down?....6
The Hole in the Wall Gang Rides Again....6
The Top Ten Threats....7
About ESET....11
Additional resources....11

Feature Article: BlackHat Japanning

David Harley, ESET Senior Research Fellow

UrbanSchrott, IT Security & Cybercrime Analyst, ESET Ireland

As Urban Schrott wrote: "…with every major natural disaster in the recent past, be it Indian ocean tsunamis, hurricane Katrina, the Haiti earthquake, the recent Christchurch earthquake, several waves of online fraud have appeared. The succession of earthquakes and tsunami that has hit Japan and affected us all in one way or another is no exception."

David Harley also blogged early on about the inevitability of criminal use of the Japanese disaster as a social engineering hook to use against the rest of us in order to make illicit profits, and shortly after put together a resource blog that gathered together a variety of sources of useful information. As that blog has been maintained purely chronologically, here is a shorter version with some resources listed by type.

Resources for reducing the risk of falling for the many fake donation scams that have been reported:

- Charity Navigator offers independent evaluation of charities.
- IRS online charities search.
- Ben Parr for Mashable: Japan Earthquake & Tsunami: 7 Simple Ways to Help
- FTC Charity Checklist.

Crisis response pages and articles:

- Google's crisis response page.
- Google's People Finder service.
- Bing's response page including several organizations offering relief initiatives.
- Stan Schroeder for Mashable: AT&T, Verizon offer free calls and texts to Japan from US
- Technet Blog: Microsoft Supports Relief Efforts in Japan
- Phil Muncaster: http://www.v3.co.uk/v3-uk/news/2033668/google-twitter-facebook-step-help-japan-earthquake-survivors
- USA.answers.gov summary: Current Situation in Japan

Warning and analysis of specific threats related in some way to the disaster:

- Kimberley of stopmalvertising.com on the early use of Black Hat Search Engine Optimization (BHSEO) to lure victims into accessing links salted with fake malware alerts. Accessing such links will result in "you have an infected PC" message attempting to persuade you to download fake AV. Fake AV is not the only malware that's being spread using Japan as a social engineering hook: similar malvertising is being used to download other undesirable content such as adware and worse.
- spamwarnings.com showing examples of spam related to this event.

- Several other sites reported videos that claim to show a whale smashing into a building and other sensational tsunami related footage. Similar sensationally-titled videos have been advertised on social media sites, especially Facebook. Following these links generally takes you to a survey scam: you are required to complete survey information before you can access the video. More often than not, there is no video, but by completing the form you have contributed to the wealth of the scammer who is carrying out some form of click fraud. You are also likely to find that your friends have received messages telling them that you like the link and inviting them to open it too. Facecrooks and other resources pointed to such eye-catching titles as "Japanese Tsunami RAW Tidal Wave Footage", "Destructive Japanese Tsunami Caught on Film", and "Giant tsunami wave eats boat as earthquake hits Japan." See: http://esetireland.wordpress.com/2011/03/15/cyberthreats-daily-as-predicted-japan-disaster-scams-in-abundance/

- The boys from Lagos have, of course, been taking full advantage of the event. As well as the usual charity donation scam emails, we've seen many reports of the classic inheritance scam, where the scammer asks you to pretend to be the next of kin to someone who has died leaving no will and no known relatives. In these cases, of course, the individual is supposed to have died as a result of the earthquake or tsunami. There are also, of course, plenty of fake appeals for various branches of the Red Cross and other relief organizations that look more like standard phishing mails than the distinctive voice of the 419 scammer.

- Hoaxes were reported as circulating via SMS (texting) in the Philippines and in Hong Kong, claiming that other parts of the world would shortly be affected by radiation from Fukishima. While the AVIEN page includes links to a number of resources that relate to the efforts being made to control the damage to the reactors, it looks unlikely from recent news that there will be a Chernobyl-sized disaster at this point. See, for instance, http://www.theregister.co.uk/2011/03/21/fukushima_after_weekend_2/.

General Advice

- Don't trust news you can't verify on generally trustworthy news sites such as the BBC, CNN and so on (but bear in mind that some fake videos claim to be provided by CNN etc.) Even better, don't click on links to sites you don't know and can't easily verify. Blackhats have a pretty shrewd idea of what keywords you'll be looking for on Google, Bing and so on, and are very practiced at getting malicious links to the top of search pages. They have also shown some ingenuity in devising attention-grabbing topics like miracle escape stories and anything to do with radiation.

- When you're told on sites like Facebook that your best friend likes a topical video with a sensational title, remember that just because you trust your friend not to intend harm, that doesn't mean you can trust him not to click on a malicious link that will disseminate through this account, contrary to his intentions.

- If you click on a site and start getting messages that your system is infected, or you have some system problem not related to the type of site you're accessing, be suspicious. (If an online virus scanner like ESET's – that you fully intended to visit – tells you that you have an infection, that's one thing. If a news site or YouTube tells you the same thing, why would you assume that it's true?)

- Don't send money or credit card details to anyone without checking very carefully that it's a trustworthy charitable or disaster relief organization. Anyone can claim to be the Red Cross. Rather than assume that japanese_disaster_relief_scam.com is a genuine appeal, check out a resource like Charity Navigator to verify known, experienced and most of all verified relief organizations.

Here are one or two general resources offering more advice:

- Robert Slade at Securiteam with an older post on training for disaster.
- Guy Bruneau at Internet Storm Center.
- An old but much-to-the-point article on disaster scams from PC World.
- US-CERT includes links to documents such as Recognizing Fake Antivirus.
- Mark Rockwell's article for Government Security News at includes some good advice from the FBI and the National Center for Disaster Fraud

Spring is Here…

Which means it's nearly time for the annual InfoSecurity Europe expo, to be held at Earls Court, London, 19-21 April? As ever, there will be an education programme with a packed program of presentations and workshops. ESET's Senior Research Fellow David Harley will be talking in the Business Strategy Theatre about "Infrastructure Attacks – The Next Generation" on the 19th April at 12:00. His presentation will look at the real lessons that SCADA utilities and the wider business community can learn from the Stuxnet and what came after.

David will be pretty active in May, too, representing ESET and the AMTSO Board of Directors at the next Anti-Malware Testing Standards Organization workshop in Prague (contiguous to the CARO workshop at the same venue). The AMTSO workshop is going to be particularly interesting, since there are several significant changes in process, including a cheap subscription model and the availability of a web forum. Immediately after he'll be at EICAR and presenting a paper on "Security Software and Rogue Economics", asking why people find it so hard to distinguish between rogue and legitimate security software: is it partly the security industry's fault? And since we're on the subject of rogue antivirus...

Unwanted Flattery (E-Set reset)

Back in October 2010, ESET researcher Tasneem Patanwala blogged about a rogue AV product calling itself Smart Security, clearly in imitation of one of ESET's flagship products. In March, Randy Knobloch passed some information to us about an even more blatant ESET impersonation: the malware in question calls itself E-Set Antivirus 2011. Apart from the curious variation on our brand name, there is of course no product of that name in our range. The site that pushes the malware will tell you that you have active malware or a keylogger, or that you have unlicensed software on your system, or that some random IP address is attacking your system. Oddly enough, Neil Rubenking, security commentator, product reviewer and member of the AMTSO Advisory Board, commented subsequently that the same malware was being dropped by one of the sites flagged by Phishtank.

Here's Tasneem's blog about the older malware, and ESET has published more information, There's also Cristian Borghello's paper for ESET on "Free but Fake: Rogue Anti-malware".

And the Firewalls Came Tumbling Down?

Mark James of ESET UK and ESET North America's David Harley were invited to comment for an article Tom Brewster wrote for IT Pro on "Five IT Sectors Staring Into The Abyss", specifically on "the death of the firewall". David told us later:

The firewall was never the 100% solution it was seen as being in the early 90s. Although, you could say much the same of antivirus. What has definitely happened over the years is that firewall functionality has widened far beyond basic packet filtering, and incorporated into a wide variety of contexts. So you'll probably see less of the basic desktop firewalls (which tend to be either limited in functionality or too complicated for the everyday user to use), and perhaps even of industrial strength devices around the gateway and DMZ, but the functionality will continue to be a layer of functionality within other systems with a more generalized intrusion prevention role.

Whether it's in the enterprise or in the home, on the desktop, at the perimeter, or somewhere back in the cloud, protection is (or should be) much more about multilayering than it is about single defensive layers. It would be a bold ISP who would say "we're not going to do firewalling anymore..."

The Hole in the Wall Gang Rides Again

Randy Abrams, ESET North America's Director of Technical Education, pointed out an interesting twist on ATM (Automated Teller Machine) fraud reported in San Francisco. We usually think of ATM fraud in terms of skimming – in this context usually an electronic reader device attached to the card slot of a "hole in the wall" cash machine, sometimes in conjunction with a pinhole camera used to capture the victims PIN (Personal Identification Number), or even simple shoulder-surfing.(http://chainmailcheck.wordpress.com/2011/03/10/atm-attacks-glued-to-the-screen/).

According to CBS, however, criminals in San Francisco were using a novel, lo-tech approach, using superglue to disable the Clear, Enter and Cancel keys on cash machines outside banks and similar institutions. When the victim, having already entered his PIN, notices that the keys aren't working, he naturally goes into the bank to ask for help (understandably wanting at least to get his card back). While he's inside, the crook takes advantage of his absence to withdraw some of his cash using the touch screen. Of course, not all ATMs have touch screens, so the attack won't work everywhere. Still, it makes sense for anyone finding himself unable to use some of the keys on an ATM to try the touch screen approach rather than going straight into the bank. It might also, as Randy has suggested, be worth checking that keys work even before entering your PIN, though that probably won't be possible on all ATMs either.

Coincidentally, security commentator Brian Krebs has also posted recently on more conventional skimming attacks in Green Skimmers Skimming Green. However, as David Harley commented, the chip and pin approach that is discussed in the comment thread, although pretty successful in Europe and elsewhere in reducing the impact of several kinds of credit card fraud, is nevertheless not a complete answer, nor completely impregnable.

More info at:

http://blog.eset.com/2010/02/18/pin-money

http://chainmailcheck.wordpress.com/2011/03/10/atm-attacks-glued-to-the-screen/

http://www.eset.com/threat-center/blog/2010/02/12/has-chip-pin-had-its-chips

And that "Hole in the Wall Gang" reference? That refers to the Hole-in-the-Wall Pass in Wyoming, out of which a number of outlaw gangs operated, and which provided shelter for such noted black hats (in a more traditional sense) as Butch Cassidy and the Sundance Kid.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 5.79%

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

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

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

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

2. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 4.29%

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.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 2.23%

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/Sality

Previous Ranking: 4
Percentage Detected: 1.86%

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

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

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

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.46%

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.

6. Win32/Bflient

Previous Ranking: 10
Percentage Detected: 1.05%

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.

7. Win32/Autorun

Previous Ranking: 23
Percentage Detected: 1.02%

Threats identified with the label 'AutoRun' are known to use the Autorun.INF file. This file is used to automatically start programs upon insertion of a removable drive in a computer. The file itself doesn´t represent a threat, but combined with a binary file it turns into a deploying feature.

8. Win32/Tifaut.C

Previous Ranking: 6
Percentage Detected: 0.94%

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.

9. Win32/Autoit

Previous Ranking: 32
Percentage Detected: 0.83%

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.

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry.

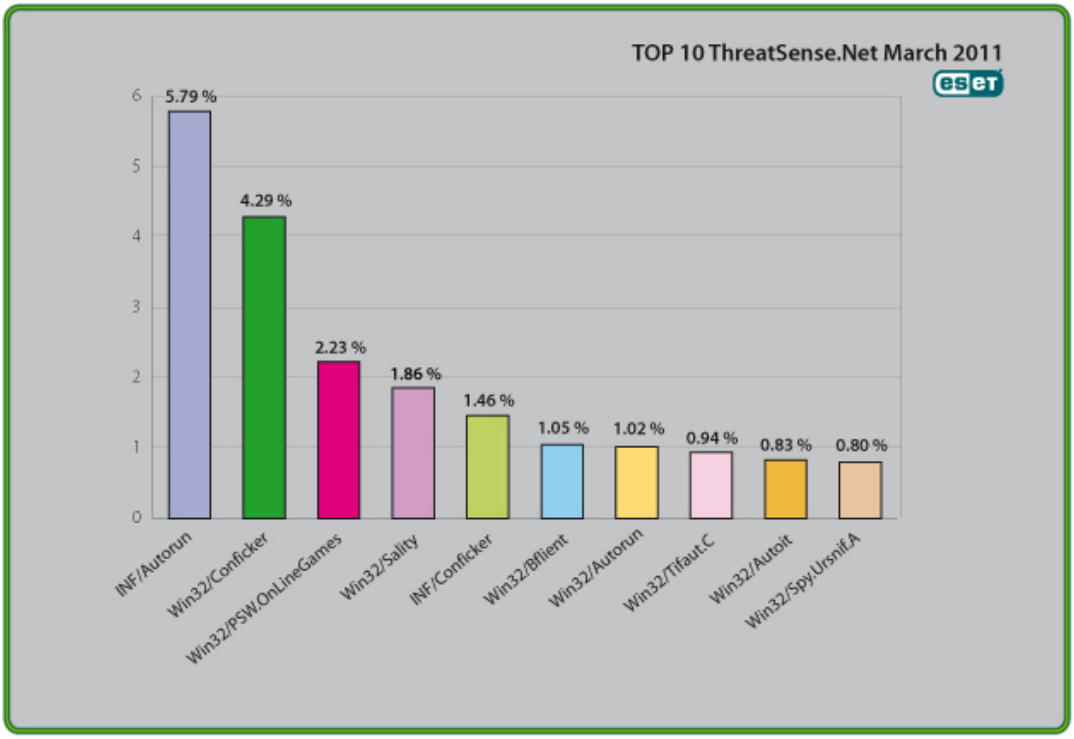
10. Win32/Spy.Ursnif.A

Previous Ranking: 8
Percentage Detected: 0.80%

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 5.79% 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