April 2011

Feature Article: 419s Still a la Mode

Table of Contents

Feature Article: 419s Still a la Mode

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

After being around for years (hundreds of years, if you trace it back through the ancient Spanish Prisoner scam), and with relatively few different twists to the main plot, I'd imagine by now that pretty much everyone would recognize 419 scams and stay well away from the "reply" button. But while reports on the actual damage done by these are, as much as everything else in dealing with cybercrime, estimations and guesswork, the persistence with which these emails keep coming, suggests someone must still be finding them a worthwhile effort.

Just recently a very stereotypical 419 was put together, using the Libyan crisis as bait and "government funds" as hook. Yep, every time a dictator is deposed or dies, someone seizes the opportunity to offer his fortune.

Lottery scams also continue to thrive, apparently. It seems unlikely that many people fall for anything as minimal as the one flagged by David Harley, telling us how the splendidly named Bayron Javier Revelo Cabrera informed him that he'd won £750,000 in the Mega BO Promotion. The body of the message follows:

Name:.....

Address:.....

Ocupation.....

Country:.....

That, we're sure, reassures potential victims that they're getting professional yet personal service. Well, maybe not. Well, to give the scammers some "credit", they do attempt a twist on the old routine now and then, which seems to be working extraordinarily well in India. .

Likewise a Japanese tsunami survivors scam has been reported along the same traditional lines. Using current events and hot topics to catch attention is common and sensible enough from the scammers viewpoint, but does anyone still fall for the old chat-up lines? Apparently they do. Some sources claim someone falls for a 419 scam every 44 seconds. An Ars technica report for 2009 claims $9.3 billion were lost to such scams that year.

Why are people still falling for this? Is the saying that "if someone is daft enough to fall for a 419, they deserve it" true? Or should there be a more concerted approach to educating people about scams? After all, to the average user "viruses", "hackers", "spam", "scams" now all fall under some undefined category between "I don't really care", "It can't happen to me" and "I don't understand what all this is".

Companies like Microsoft, Yahoo, Western Union and Coca Cola are already part of a Coalition that aims to combat advance fee frauds through education, and post clear warnings and suggestions regarding the problem. And that, in combination with the efforts of the various national crimefighters, the whole security industry and other agencies, should be affecting some sort of mitigation. But it seems the impact of all this remediation is still pretty low-key, compared to the huge estimated total damages of this sort of crime.

Perhaps it would help if some of the countries most associated with this kind of scam would take it more seriously at a governmental and legal level. Nigeria is so inextricably

associated with advance fee fraud and other scams such as "Londoning" that Advance Fee Frauds are often referred to as Nigerian scams or 419s (from the section of the Nigerian Criminal Code dealing with obtaining property by false pretences), though in reality the same type of lo-tech scam long ago ceased to be a uniquely African enterprise. Still, it's disconcerting that Nigeria recently failed to pass a Cyber Crime Bill. Admittedly, the fact that this bill had similar objectives to the recently-presented bill from the Economic and Financial Crimes Commission may have played a part in its demise.

Nevertheless, it seems that it joins a string of failed bills that attempted to address cybercrime in Nigeria going back as far as 2005's Computer Security and Critical Information Infrastructure Protection. According to Dr. Nnaemeka Ewelukwa, a Senior Teaching Fellow in International Trade Law at the University of London, the only law in Nigeria that deals specifically with Internet crime, the Advance Fee Fraud and other Fraud Related Offences Act 2006, does so only in terms of the regulation of ISPs and cybercafés. Better than nothing, but obviously not enough, in the light of his claims that hacking, spamming, online ID theft, and card-skimming-related offences are not punishable under Nigerian law.

ESET Researchers at Virus Bulletin

VB2011 - the 21st Virus Bulletin International Conference - will take place 5-7 October 2011 at the Hesperia Tower hotel, Barcelona, Spain; and ESET is a platinum sponsor.

You can take a look at the abstracts of ESET's accepted papers:

- 'Same Botnet, Same Guys, New Code' by Pierre-Marc Bureau: http://www.virusbtn.com/conference/vb2011/abstracts/Bureau.xml

- 'Fake but free and worth every cent' by Róbert Lipovský; Daniel Novomeský; Juraj Malcho: http://www.virusbtn.com/conference/vb2011/abstracts/Lipovsky-etal.xml

- 'Daze of Whine and Neuroses (But Testing Is FINE)' by David Harley; Larry Bridwell: http://www.virusbtn.com/conference/vb2011/abstracts/R-HarleyBridwell.xml

TDSS: the Next Generation

Win32/Olmarik (also known as TDSS, TDL, Alureon etc) continues to evolve in interesting and innovative ways. TDL4 is a case in point, with its ability to load its kernel-mode driver on systems with an enforced kernel-mode code signing policy (64-bit versions of Microsoft Windows Vista and 7) and perform kernel-mode hooks with kernel-mode patch protection policy enabled.

Eugene Rodionov and Aleksandr Matrosov, in a new ESET white paper on The Evolution of TDL: Conquering x64, look at the GangstaBucks gang that has been distributing TDSS since DogmaMillions shut up shop, then dive deeper into analysis of the installation and implementation of the bot, the kernel mode components and bootkit, with some extra information on its relationship to Win32/Glupteba.

You may also find their previous white paper TDL3: The Rootkit of All Evil? and Virus Bulletin article Rooting about in TDSS (made available by kind permission of Virus Bulletin, who hold the copyright) of interest. A series based on the same paper is due to appear at Infosec Institute shortly (probably week of

17th April). See also the blog on the remedial effect of the Microsoft patch at http://blog.eset.com/2011/04/15/kb2506014-kills-tdl4-on-x64.

Anti-Malware Testing Standards Organization

The Anti-Malware Testing Standards Organization (AMTSO, www.amtso.org), an international organization that promotes improved methodologies for testing security products, has launched a new online forum, follows its decision late last year to open up AMTSO membership with a new subscription model. ESET has been very active in AMTSO since its early days: ESET CEO Andrew Lee has been a member of the Board of Directors, and the same role is currently filled by ESET Senior Research Fellow David Harley.

AMTSO arose out of agreement between the vendor and tester communities that standards of testing for anti-malware products needed to be higher. However, it has always recognized that other communities (publishers, academia, and the user community) can provide valuable input into the developing of industry standards and guidelines for improving malware testing.

AMTSO's new subscription model encourages individuals and small organizations and everyone with an interest in testing to join in the sharing of information on anti-malware testing and the development of guidelines, at a fraction of the sum it would cost them for full membership. Subscription is now available for a 25 Euro fee via the Subscription tab at http://www.amtso.org.

AMTSO has also launched a forum where anyone may post and join in testing-related discussions, though only full members have voting rights.

The forum, which can be reached via a link on the www.amtso.org homepage, aims to provide a discussion point where anyone with a question or an opinion on the testing of anti-malware software can make their voice heard.

World Backup Day

Sebastian Bortnik, Awareness & Research Coordinator of ESET LA, blogged about an important initiative developed by a group of Web Hosting Companies. They decided to give to Backup Information an especific day as a way of recognize the importance that it has for all users. For this purpose, they have declared March 31st as the »World Backup Day« (http://worldbackupday.net/).

Backups are one of the corrective measures involved in security controls. In order to avoid the loss or damage of information, it is important to reflect about the importance of having a security copy and learn what it is and how it can be do it.

For that reason, ESET gave some suggestions to consider while making a backup. There are some questions that all users need to ask themselves before doing a backup: Which information should be backed up?, How will the information be backed up? and When will the data be backed up?

To read more about this topic and the suggestions made, you can go to: http://blog.eset.com/2011/03/31/three-questions-on-world-backup-day-what-how-when

SC Magazine - Cybercrime Corner

David Harley, ESET Senior Research Fellow, and Randy Abrams, ESET Director of Technical Education, are contributing with the

edition of Cybercrime Corner, one of the sections of SC Magazine.
SC Magazine is an online resource center for IT security professionals and The Cybercrime Corner show the latest cyber security trends from acknowledged experts in the security industry.
Here is a list of some articles that David Harley and Randy Abrams have published there:

- Who are the cybercriminals?
- AV company, heal thyself
- Giving the cybercriminals a helping hand
- A tsunami is also a crime wave
- Supporters Club
- Poachers and Gamekeepers

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.62%

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

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

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

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

2. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 3.76%

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: 2.02%

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: 1.83%

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. Win32/Autoit

Previous Ranking: 9
Percentage Detected: 1.10%

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.

6. Win32/Autorun

Previous Ranking: 7
Percentage Detected: 0.96%

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.

7. HTML/Iframe.B.Gen

Previous Ranking: 15
Percentage Detected: 0.86%

Type of infiltration: Virus

HTML/Iframe.B.Gen is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

8. Win32/Bflient

Previous Ranking: 6
Percentage Detected: 0.85%

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.C

Previous Ranking: 8
Percentage Detected: 0.81%

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.

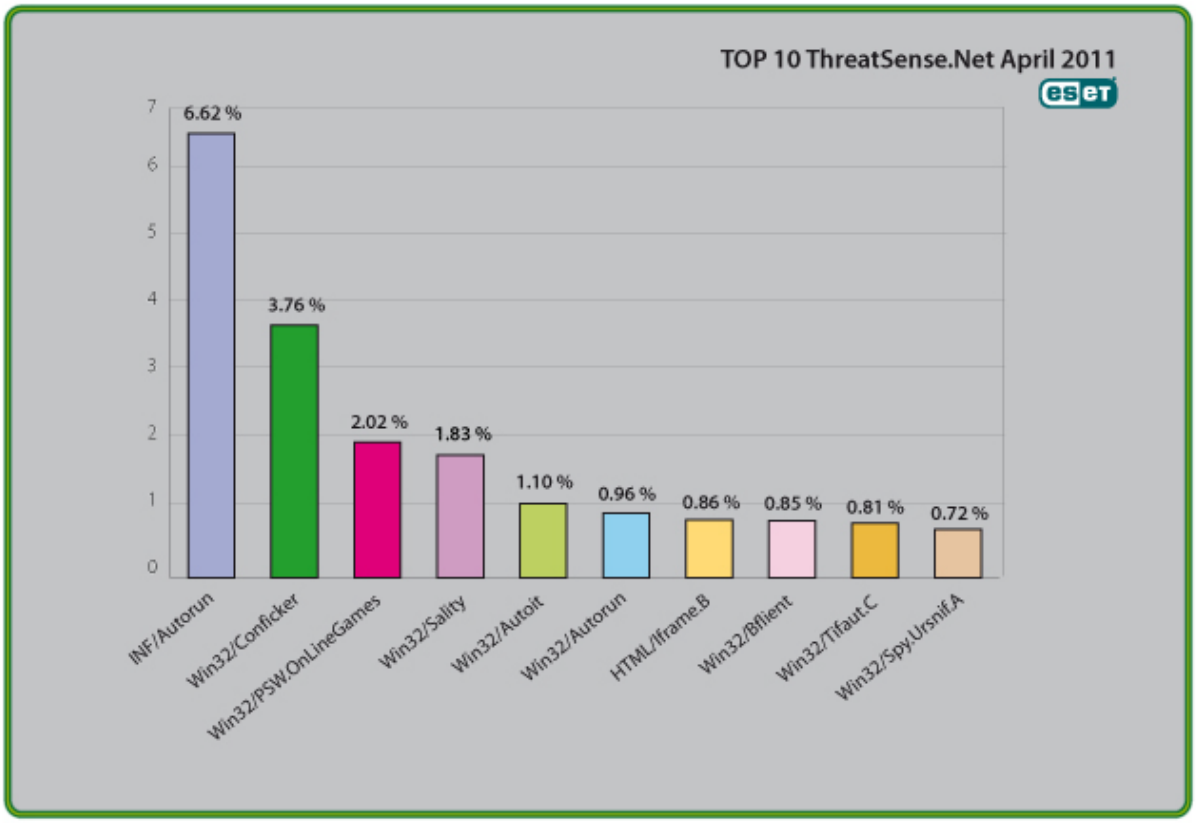
10. Win32/Spy.Ursnif.A

Previous Ranking: 10
Percentage Detected: 0.72%

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 6.62% 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