February 2011

Feature Article: From Russia with Spam

Table of Contents

Feature Article: From Russia with Spam

Josep Albors, IT Security & Cybercrime Analyst, Ontinet.com

Sending out unsolicited email on a massive scale is a common practice for certain "businesses" located in Russia or in neighbouring countries. For years this approach has been working quite well for them: using botnets to send mails in question keeps the cost for these companies very low. In our laboratory we regularly monitor mail campaigns of this type, and basically, they basically consist of sending emails containing web links where the unsuspecting visitor is likely to be offered all kinds of dubious products and services.

But this week we have seen a change of pace in this type of campaign, which has started to feature many forums specifically created in order to publish posts that continually advertise such products. It all starts with an innocent email that may contain various topic and types of content but always invites us to follow a link.

After clicking on the provided link, we are redirected to a post published in a forum, where a beautiful young lady presents us with photos and personal information, with the alleged intention of finding a partner. Obviously, this is an example of the so-called Russian bride scam, where some poor innocent believes he has found a possible soul-mate, and an exchange of emails with the alleged Miss ensues, culminating in a request for money to enable "her" to travel to see him. Once "she" receives the funds, of course, the conversation is likely to die away abruptly.

However, being curious to see what kind of posts are published such a forum, we decided to investigate further and analyze what sort of material was being published. We soon realized that the Forum itself was being used to promote all kinds of spam.

During analysis and comparing it with other forums, we note that most of these forums were created last weekend, and the only content published offers these products and services of dubious provenance. Today we find many, many messages created with this type of post: in just one of the forums we investigated, over 50 pages of posts were published in only 3 days). To give just two examples of advertised products, there are classic products with effects similar to Viagra or luxury items such as handbags or replica watches.

The creators of this type of spam seem to have found a rich new vein to mine in the creation of such forums. It is now relatively easy for anyone to create their own forum, and with the ease of automation and the resources that are now available to those behind these criminal activities, we are likely to face the creation of thousands of forums of this type in a short space of time.

ESET's laboratory at Ontinet.com recommends that users who receive messages like this delete them without accessing the provided link. Also if you come across a similar message in a reputable forum, it is advisable to inform the maintainers of the forum so that they can remove malicious posts. Only in this way will we avoid an escalation in this type of campaign that might well evolve in a massive spread of malware.

Misplaced trust in trustworthy names?

UrbanSchrott, IT Security & Cybercrime Analyst, ESET Ireland

Just the other day a journalist commented to me, as so many have before, that "surely people can be relatively safe online, if they just avoid dodgy sites" (and by dodgy sites, they usually mean porn or piracy sites). After all the years of telling people about malicious code injections, about drive-by downloads, and about Trojans just about everywhere you look (or don't look), some still believe all they have to do to stay safe is to refrain from visiting dodgy sites. Well, just recently we have again been reminded that not only are troubles *not* limited to dodgy sites, but that even some sites we'd expect to be completely trustworthy can be compromised.

At the beginning of February, ESET researchers Aryeh Goretsky and Randy Abrams wrote about an infection that seems to have originated from Microsoft. In late January a customer reported that ESET NOD32 Antivirus had prevented a Trojan from infecting a mobile user's computer, but that the source of the infection was Microsoft's own Update Catalog. Though this was no direct fault of Microsoft, their driver updates page provides users with many third-party driver updates, and it is into one such that a Trojan sneaked (more in Aryeh's full story). Randy Abrams then followed up with a detailed breakdown how the third party updates function, how such occurrences are not unusual and why Microsoft didn't catch it.

Very soon after that came reports of BBC6 Radio's homepage being afflicted by a malicious link which was reported to carry various types of malware. In addition Lush cosmetics websites have been compromised and customer data stolen (more in ESET researcher David Harley's blog). David also reported that public access PCs in libraries have been found with hardware key-loggers attached, stealing people's log in data. (See also Keyloggers in the Library and Dan Raywood's article for SC Magazine on Keyloggers found plugged into library computers).

ESET's Marek Polesensky added his contribution to the growing list of reports on Facebook threats, with a report on a slew of worms, including Win32/Yimfoca.AA and Win32/Fbphotofake, where for a few weeks Win32/Yimfoca.AA has even ranked in the ThreatSense.Net Top Ten Threats in many European countries.

Financial institutions weren't spared either. In Ireland we're still seeing plenty of phishing emails using templates of well known Irish banks, as well as a recent phish purporting to be from the Revenue Commissioner, and indicating that the recipient is entitled to a tax rebate. Elsewhere Trusteer has reported of a Trojan that keeps online banking sessions open for crooks to exploit, even after the user has logged out.

Combine then the confidence that everything will be all right if one avoids dodgy websites, with the reality that the above threats are lurking everywhere, even in supposedly very known and safe institutions. We sort of expect such organisations to take care of security concerns for us: since this clearly isn't always the case, it comes as no surprise that one fifth of Irish businesses have experienced a data breach and UK business is losing over £20 billion to cyber crime, as reported in ESET Ireland's blog. And tying in with this data, EU statistical office reports that a third of EU computer users have caught a computer virus.

Antivirus vendors, such as ESET, have often been accused by media of fear-mongering in order to stimulate sales of our products, but all one really has to do is glance over news headlines to see that every day there can be found a different report about another breach, fraud, scam, item of malware, etc. And very few of these are harmless or easy to ignore. And most of these stories don't even come directly from antivirus vendors. Perhaps now, with names we have come to accept as trustworthy coming under attack, it is time for a less

complacent attitude in dealing with cyber threats on the part of both the media and the general public. Just as regular crime is no longer seen exclusively in the dodgier parts of towns, so cybercrime has long since stopped being the domain of dodgy websites. On the contrary: the more successful security types are at spotting and taking down malicious sites, the more the bad guys will try to compromise sites that you'd expect to be thoroughly respectable and clad in virtual armour.

Nothing Exceeds like Stuxnet

People might think that everything worth saying about Stuxnet has been said by now. However, the team responsible for the "Stuxnet under the Microscope" report has maintained a watching brief, and a flood of material of variable worth and interest continues to flow past their eyes.

On the first of February, novelist William Gibson drew a fairly dubious comparison between Stuxnet and the 25-year-old Brain virus. On the whole we prefer his fiction... As the month rolled on, Iran continued to maintain that reports of damage to its nuclear program are overstated and even malicious, but admitted that the issue deserved investigation in the light of the Russian Ambassador's contention that it could have caused another Chernobyl.

Lot of people related to the security world has been giving their opinions about this situation from different points of view:

Nima Bagheri, CEO of U0vd, offered a more balanced view from Iran (actually rather a good presentation)

There were certain rumours about the likelihood that the Anonymous hacktivist group has access to Stuxnet code (probably a disassembly). In fact, disassembled Stuxnet code is certainly available on the Internet, but doing something with it is something else. After all, security companies have samples and disassemblies too, and are monitoring and planning accordingly.

Symantec's substantial Stuxnet Dossier was updated in the light of the belief that five organizations in Iran were targeted, as summarized by Kim Zetters in Wired. Eric Byres, Andrew Ginter, and Joel Langill also produced a substantial document.

Tofino Security also updated a revised document by Eric Byres and Scott Howard on "Analysis of the Siemens WinCC / PCS 7 "Stuxnet" Malware for Industrial Control System Professionals". The site requires registration, but has some interesting material.

Joel Langill also maintains a Stuxnet resource at that you might find interesting.

And while it goes back to late January, it seems a pity not to mention the availability of Tom Parker's hefty presentation "Stuxnet Redux: Malware Attribution & Lessons Learned" for Black hat. You can also see the latest in a series of resource blogs.

David Harley, Senior Research Fellow at ESET will be talking about Stuxnet and its implications for the SCADA industry at Infosec Europe in April:

Infrastructure Attacks - the next generation?

Business Strategy Theatre
Tuesday April 19th, 12pm

AMTSO anticipation

AMTSO (Anti-Malware Testing Standards Organization) normally holds its first workshop of the year in the Bay area, close to the annual RSA conference in San Francisco. This year, the workshop was hosted by our friends at Webroot: particular thanks to Jong Purisima for his help on the organization. As ever, there was stimulating discussion, much of it centred on how AMTSO could get its message(s) out more effectively.

No guidelines papers were approved this time (a paper on the EICAR test file was withdrawn for the moment as AMTSO and EICAR are considering a joint initiative), but considerable progress was made on a paper that addresses some of the confusion around testing and statistics – what we mean by statistical validity is crucial to the usefulness or otherwise of a comparative test. Papers on sample selection, classification and validation, and another on ways in which vendors can facilitate testability are in good shape.

However, some of the most interesting discussions were about the new $20 subscription model and the open discussion forum, both of which should come into effect in the very near future.

The next AMTSO workshop is in Prague in May, to coincide (but not overlap) with the next CARO workshop.

RSA

ESET was also heavily engaged with the RSA conference and expo at the Moscone Center in San Francisco. ESET North America's shiny new stand attracted a lot of attention, as did Randy Abrams' presentation on "Learning from giant security blunders – remembering the past so that we don't repeat it," which focused on a few of the more embarrassing security slip-ups to have appalled and entertained us over the last couple of decades. David Harley subsequently cited it when talking to Dan Raywood of SC Magazine about incidents in the UK where keyloggers were found attached to internet-connected PCs in public libraries. When Raywood asked him how common such incidents are, David commented:

"As it happens, one of the ESET presentations at the RSA Conference highlighted a couple of not-unrelated incidents: in 2007, the RSA Conference itself made available common access kiosk computers running XP with full admin privileges and no protection except a free anti-virus product; while in 2010 IBM gave out Autorun-infected USB sticks at AusCERT. Wouldn't you expect better security in those cases?"

"The real problem is that people expect someone else to protect their privacy and security in all sorts of contexts. Not everyone who makes available a common access PC or access point is responsible enough or expert enough to take adequate precautions to protect the people who use it."

David's own blogs on the subject can be found at Keyloggers in the library and Public Access PCs Booby Trapped. He has commented since: "While I don't have full details of the incident, I have to wonder whether it points to a particular problem in small organizations and sub-branches of larger organizations, where there is often no on-site tech support. One of the devices disappeared after it was noticed, but before the library itself removed it. Was it just lost? Or did the criminal come in and remove it while someone working in the branch was asking someone else what they should do about it?"

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 2
Percentage Detected: 5.53%

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: 1
Percentage Detected: 3.78%

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: 2.20%

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: 1.72%

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: 1.24%

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/Tifaut.C

Previous Ranking: 6
Percentage Detected: 1.09%

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.

7. Java/TrojanDownloader.OpenStream

Previous Ranking: 35
Percentage Detected: 1.02%

Java/TrojanDownloader.OpenStream.NAU is a Trojan written in Java, which tries to download other malware from the Internet. It may be invoked when visiting a malicious website by referencing a malicious Java class file within a Java archive file (.JAR).

When the malicious .JAR archive is processed, the Java class component gets the URL of the file to download from the malicious website.

8. Win32/Spy.Ursnif.A

Previous Ranking: 9
Percentage Detected: 0.77%

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.

9. HTML/ScrInject.B

Previous Ranking: 8
Percentage Detected: 0.73%

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.

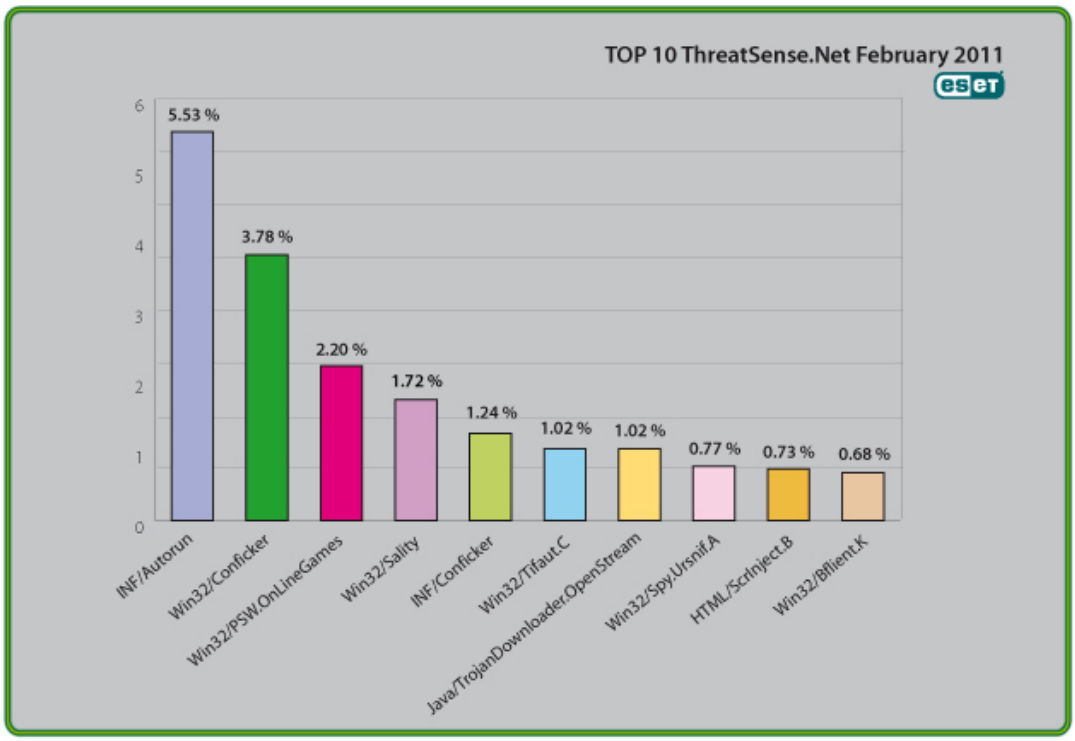
10. Win32/Bflient.K

Previous Ranking: 6
Percentage Detected: 0.68%

Win32/Bflient.K 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.

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 5.53% 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