March 2013
Feature Article: Bank Fraud and Job Scams

ENJOY SAFER TECHNOLOGY™

Table of Contents

Bank Fraud and Job Scams

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

Today I found a particularly endearing example of the 419 (advance fee fraud) scam in my mailbox.

The sender, one 'Harry Cole' claims to represent a bank called the IFC (presumably that's the International Finance Corporation) and says that an 'inquest' (sounds like a matter of 'grave' concern) conducted by the bank turned up an 'inactive/dormant' account, and that I'm a 'potential beneficiary to an unclaimed sum.'

Sounds interesting? Not really: this is a terse variation on a type of 419 where the scammer claims that he can cut you in on a bank account belonging to someone who died suddenly and intestate or without any known heirs, and that otherwise the money will go to some undeserving party such as corrupt government officials or into the bank's own coffers. (That's supposed to allow you to justify to yourself the fact that you're agreeing to engage in a form of fraud. On the other hand, the fact that you know deep down that you would be defrauding the bank is also an effective way of discouraging you from reporting the scam when you realize you've been had.) If the recipient of the email is naïve enough to follow through, in due course he'll find himself required to make various payments before the money can be transferred (hence advance fee fraud), which of course will never happen.

What makes it somewhat endearing in a dopey sort of way is that the 'hook' for this scam is that 'the similarity in your name and email makes it possible for us to liquidate the deceased account in your favour. I wonder how they knew that my middle name is AskESET?

Yep. As interest in the new ESET blog and resources site at http://welivesecurity.com grows, so does the volume of scams and spams sent to our contact address askeset@eset.com. In fact, I used one of them as the basis for a recent blog: Job Scams: Nice Work If You Can Get It. A short extract:

"The new ESET blog format must be striking a real chord with people. At any rate, job offers are just pouring in. Except that they don't seem to be jobs for security bloggers, or for web developers like the team that maintains this site.

What qualifies us for an unspecified role in a hotel in Canada, I wonder? Perhaps they need someone to polish their emails. Some of the wording has a strong whiff of the West African 419, and after all, we're not short of editing talent round here. But as our colleagues at ESET Ireland pointed out recently, at a time when the global economy is in crisis, there are all too many people solving their own employment and financial problems by scamming the unemployed, and job scams are an obvious way of grabbing their attention"

Blots on the Threatscape

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

Recently, I was asked for some commentary on the effects of viruses in the enterprise. Finding myself writing far more than the journalist could possibly use, I thought you might find some of the content I produced interesting and/or useful. (Always the optimist...) Like many requests from journalists, this one took the form of some specific questions.

- What are the key virus threats?

  Strictly speaking, viruses in a technical sense – that is, self-replicating malware – are a pretty small blot on the threatscape, though from time to time something will come along and have a major impact. Stuxnet and its siblings, for instance, have had an impact out of proportion to the relatively small number of infections. But most people outside the security industry these days use the term as interchangeable with malware (malicious software). In fact, most malware nowadays is not self-replicating, but spread by other means such as spam campaigns.

  Some of the significant malware and related attacks we see today include:

  - Banking Trojans ranging from Zeus and its siblings to Carberp

- Ransomware (malware that encrypts your data or denies you access to your PC, then demands that you pay to get it back.
- Phishing, which may involve the use of some form of Trojan
- Bots that give the attacker the opportunity to control large groups of machines (botnets) for a variety of criminal activities: spam, phish and malware dissemination, Distributed Denial of Service attacks (often for purposes of extortion), captcha cracking.
- Targeted attacks (see below)

Our current top ten, which you'll find later in this document, gives you some idea about the most prevalent detections worldwide. However, some of our detections are highly generic, meaning that because of the use of advanced heuristics, a single detection might include specimens of malware that have common characteristics, but aren't necessarily related in the sense of belonging to the same family or originating with the same gang. For instance, in the list below:

- INF/Autorun includes all kinds of disparate malicious code that attempts to use the Windows Autorun/Autoplay mechanism to infect systems. While modifications to recent versions of Windows have severely curtailed the effectiveness of this infection vector, the figures indicate that there is still plenty of malware out there that includes code to misuse it.
- Kryptik detections don't describe a single Trojan family, but a wide range of malcode that shares certain coding techniques.
- ScrInject is a class of malware that redirects a browser to a malicious URL.
- Dorkbot is a bot that owes its position in the top ten to the fact that it's extraordinarily widespread in South America and has been since 2011.

Note that the percentages relate only to instances of malware flagged by our telemetry – our software includes an option to report it to the ESET lab when an attempt to infect the machine it protects is detected. This gives us some feel for prevalence and – perhaps more importantly – the opportunity to refine our detections, but doesn't say anything about the absolute numbers of infected machines worldwide. We don't publish absolute numbers because they can be misleading.

However, some very significant malware doesn't get anywhere near the top ten. The kind of stealthy, targeted threat that the security industry sometimes calls an APT (Advanced Persistent Threat) may remain undetected for long periods because of its very limited spread. Stuxnet was an interesting example of malware that finally got noticed because infections suddenly started to accelerate. ESET at first detected it heuristically, then developed Stuxnet-specific detections because there was a spike in infections. But the term 'spike' is relative: the numbers behind the percentages we see in the top ten are usually much higher than Stuxnet ever reached.

- How do they weasel their way in and what can you do about it?

Most malware relies partly or completely on social engineering. Spam campaigns via email, the social media and so on, try to lure victims to sites booby-trapped with malicious code. Sometimes the site is legitimate but has been compromised by some form of hacking. The malicious code may be self-launching (drive-by downloads) or may be in the form of a malicious binary passed off as something desirable or useful. Targeted threats often exploit vulnerabilities in certain types of document (often PDFs, nowadays), and may be delivered as an attachment to mail or instant messaging. Email filters and similar defences are more likely to let a document through as an attachment than a program, especially if they use some form of 0-day exploit. However, they still rely on fooling the victim into opening the attachment. Criminal gangs use a variety of techniques to make it harder to detect malware, such as using legitimate programs and services like AMMYY to open a backdoor into an infected machine, or chaining together software components and web redirections where the unequivocally malicious code is at the end of the chain, so that even where the malcode is known, it won't necessarily be seen by an antivirus

scanner unless it's able to step through the entire chain of steps.

This may seem like a weird thing for an AV researcher to say, but don't rely on antivirus software. Multi-layered protection such as that used by well-protected corporates fills many of the gaps that AV can't reach: even if it doesn't recognize malware as such, it blocks some of the avenues that malware uses to get a foothold. Some ISPs and mail providers also use some of the tools that a large corporate uses (firewalling, intrusion detection and prevention, and so on) but a home user can also benefit from some similar technologies on the desktop using a proper security suite. Free antivirus programs are a lot better than nothing, but they don't offer the same protection or support. When so many people are using their own devices at work, or working from home at least some of the time on their own PCs or other devices, it's important that organizations take the protection of those devices into account when they consider the security of the organization as a whole.

- Prevention is still better than cure, but what can you do if the worst happens?

Sometimes it's easier to rebuild a system than to clean it, especially in a corporate environment, but it's probably not necessary nearly as often as some sectors of the security industry will tell you. In fact, under these circumstances a good support contract is a welcome return on investment (apart from its value in terms of installation and maintenance support). Some large companies (Lockheed Martin and Boeing spring to mind) invest in trained professionals with very specific expertise in dealing with malware, reflecting the fact that such companies are often the first to see certain kinds of new threat family. Even small companies sometimes have in-house expertise – my own reputation, such as it is, was originally based on managing anti-virus for a medical research organization with less than 2,000 users. But sometimes significantly larger companies don't have an in-house expert on malware or security on tap, and not all system administrators have the knowledge to deal with a serious local infection situation. So it makes sense to evaluate a security product's support structure, not just its unit cost. Or consider outsourcing some security support, or factoring in the cost of training internal IT staff.

- How can a virus infection harm the reputation of a company?

It would be unprofessional to discuss specific companies whose management of a breach I've been involved with personally, and discussion of other incidents is often speculative. I would say, though, that the most embarrassing virus incidents are those where the malware is well-known enough that you'd expect a well-protected organization to recognize and deal with an attack earlier than actually happened. However, a less well-protected organization may not be able (or willing) to identify the exact cause of a breach. In many countries, legislation exists that obliges a company to inform its customers when a breach endangers customer data, but not necessarily to give other details of the breach. When a company says, in effect, that it was attacked using an APT, there are often grounds for suspecting that what it means is “we screwed something up and we're not sure how, but we don't want you to think it's our fault.” In an era where targeted attacks are increasingly frequent and inflicted on a wide range of organizations, my feeling is that those organizations limit reputational damage better if they can say “we got something wrong, here's what happened, and here's what we're doing to reduce the chances of its happening again.” It doesn't have to be incredibly detailed – in fact, it may be bad security practice to give away too much information – but it does have to show that the company is genuinely managing the security problem, not just the PR problem.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 3.59%

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/Sality

Previous Ranking: 3
Percentage Detected: 2.19%

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

3. HTML/ScrInject.B

Previous Ranking: 4
Percentage Detected: 2.10%

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

4. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 2.09%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

5. Win32/Ramnit

Previous Ranking: 6
Percentage Detected: 1.79%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

6. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.42%

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.

7. HTML/Iframe.B

Previous Ranking: 2
Percentage Detected: 1.29%

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.

8. HTML/Fraud

Previous Ranking: 45
Percentage Detected: 1.06%

HTML/Fraud is a trojan that steals sensitive information, like

telephone numbers and e-mail addesses, and attempts to send the data to a remote machine. The trojan displays a dialog window asking the user to take part in a short survey, in order to persuade him to fill in personal information. The trojan contains a list of URLs and the HTTP protocol is used.

9. Win32/Qhost

Previous Ranking: 8
Percentage Detected: 0.98 %

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

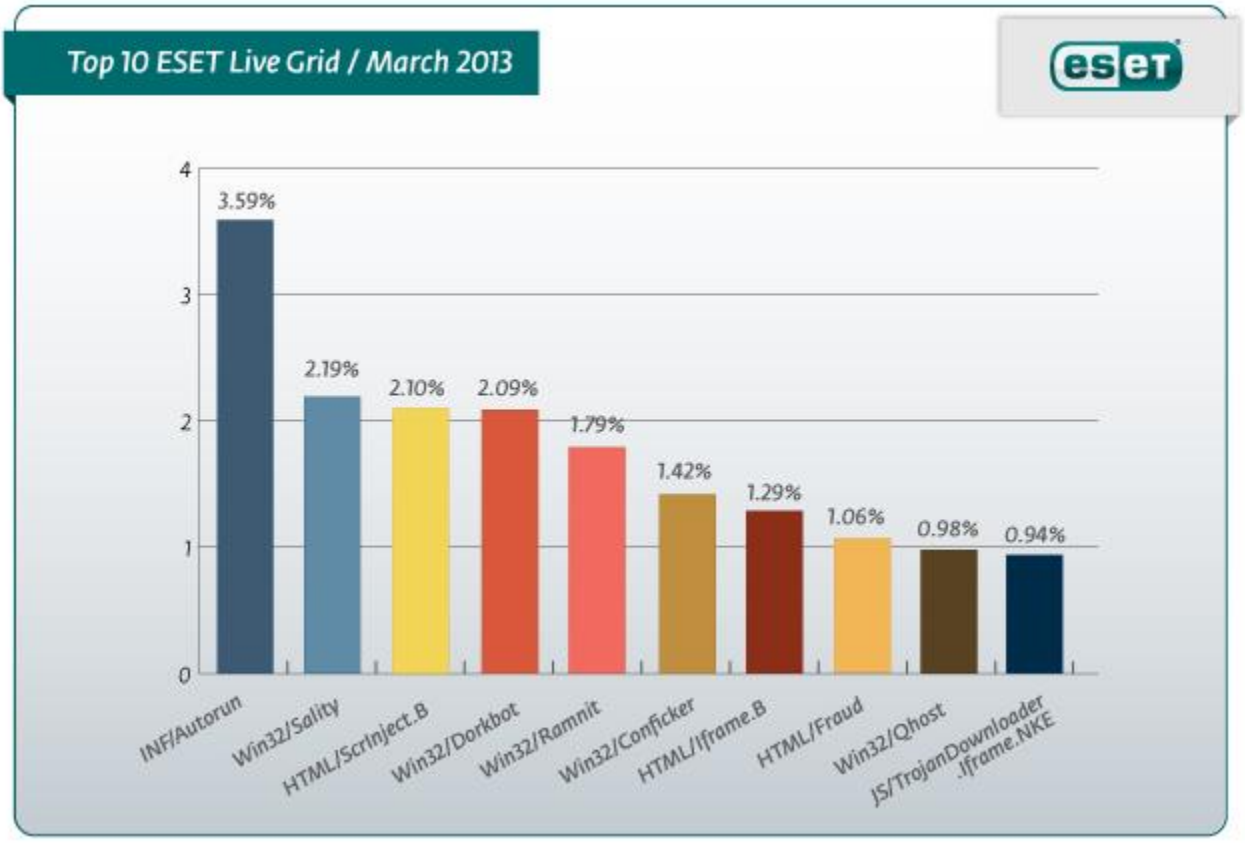
10. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 9
Percentage Detected: 0.94%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 3.59% of the total, was scored by the INF/Autorun class of threat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

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 (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation