December 2014
Feature Article: Bank Card Courier Scams

ENJOY SAFER TECHNOLOGY™

Table of Contents

Bank Card Courier Scams

David Harley, ESET Senior Research Fellow

Here's an elaborate scam I wrote about some time ago, but I've seen further reports of it in the UK recently, so here's an updated version for those who haven't come across it before. Some of these wrinkles would actually work in the US, but Chip and PIN is much less used there, which may account for the lack of reports from there that correspond exactly to the British reports.)

The essence of the scam as it has been reported is this: the scammer calls you posing as the anti-fraud department of your bank (or as a police officer) and tells you that suspicious activity has been detected on your bank card. It's not that unusual for your bank to ring out of the blue to ask you to verify a transaction, but what (reportedly) happens next is quite different.

It's not me, it's you

If your bank (or anyone else 'official') does ring you unexpectedly, you should bear in mind that it's more important for you to be able to verify their identity than vice versa. After all, they have your telephone number. Sometimes the scammer pre-empts that thought by suggesting that you ring the number on the back of your bank card to confirm, but doesn't put the phone down at his end, so that you're still connected to the number that they called from. (Telephone service providers do this to allow time for transferring legitimate calls between extensions, for instance.)

I guess that people who are caught this way don't like to insist that the caller puts the phone down, don't wait for the dial tone, don't realize that they're not actually able to call out, or aren't concerned that they don't hear a ringing tone before they hear someone speaking on the 'new' number. (However, some alerts state that the scammer will play a recorded dial tone to fool you into thinking that you have been disconnected.) If this is you, you might like to reconsider. If you're feeling really paranoid, you could ring a completely unconnected number and see if you get a response from 'your bank' or 'PC 49' rather than the real holder of that number. In fact, the line shouldn't remain open indefinitely if only one party hangs up, and in any case the scammer will not to want to tie his phone up longer than he needs to: things to do, other people to scam… Be aware, though, that it might take several minutes for the line to clear automatically where the phone hasn't been put down at the other end. That's 6-12 minutes according to some sources: I'd assume 12, which should cover calls made from other countries. If you're checking a number someone's given you in these circumstances, it's worth using a different line (if available) or a mobile phone.

The scammer may give you a different number, of course. If someone just says 'ring the following number' they could be directing you absolutely anywhere. If they suggest ringing a verifiable number, however, clearly they could be using the same technique for keeping the line open. In this instance of a different scam, all the scammer needs to do is stay on the line, having pressed the mute button on his handset, to convince the victim that his phone has been temporarily disconnected.

PINs and needles

The scammer may ask you for full details of your account and ask you to enter your PIN.

First of all, the bank doesn't need full details in order to verify who you are. Any bank worth your custom may well ask for something like the 2nd, 4th and last letters of your 'special

word', and slightly dubious old favourites like your mother's maiden name, and even the last four digits of your card number, and all that has some potential value to a scammer, if combined with information gleaned in other ways. But your bank already knows your account details, and doesn't need info like the card security code (the magic three digits on the back of the card) in this context. The only reason anyone should ask you for all that information is for fraudulent purposes, though there are still financial institutions that are genuine, yet persist in using insecure phone-call practices.

As for keying in your PIN, there is no legitimate reason why your bank should ask for it. They already have access to that information, and they certainly don't need it to cancel the card or to activate the new one: the point is that if you do key it in, the scammer can see what it is on his own phone display. (If they were sure your card had been used illegitimately, they'd almost certainly have cancelled or blocked it before they even talked to you.)

Your account number tells them which bank you're with, even if you haven't told them already. Did they tell you which bank they were at the beginning of the call, or did you assume that they were genuine and let slip the information as the call proceeded? Unfortunately, there are quite a few other ways in which they might have already known which company you bank with or whether you have an XYZ credit card. However it's more common for scam calls to be made more or less randomly, with the scammer relying on getting the information he needs from you and the telephone directory.

Sending the lads round

The next stage is that the scammer tells you he will come round or send a courier to collect your 'compromised' card. This is a dead giveaway: it would be a very expensive way for a bank to deal with a compromise: they could simply cancel your card without needing any information from you. Frankly, I suspect that most banks don't care about most of their customers enough to give you such instant service. They might, of course, want you to return it by post. If they send you a new card, they might want you to verify it by phone, but you should have a verifiable communication from them arriving with the card, in that instance. I am, of course, talking about a card sent in the normal way of business: if they offer to send a courier round to your address to pick up a compromised card and give you a replacement, that's part of the scam. It's really not difficult to take a bank card blank and add all the information that you have given them so that it looks like a genuine replacement card. Of course, it won't actually work. Even if the scammer has the ability to clone your card accurately from the information you give him, he won't: he certainly doesn't want you to have access to the account he's about to plunder.

Actually, I'm surprised that it's economical for courier card scammers to pay for a courier, but apparently it is. I suppose if the scammer gets to that point, he's reasonably sure he's going to get the card. It seems to be carried out exclusively by people who are geographically (fairly) close to the victim: this probably works well for the scammer, since many people are nowadays less likely to believe everything they're told by someone with a 'foreign' accent, due to the prevalence of phone scams originating in West Africa or India.

All cut up about it

A variation I've seen reported here is that the scammer advises you to cut up the card before you hand it over, but subsequently tapes it back together to use in an ATM. I'm not sure how reliably a sellotaped bank card works in an ATM (certainly if it's been cut into several pieces, as it should be if you want to render it unusable), but it could certainly be used

to get or confirm information about the card that hadn't already been captured over the phone and use that information to clone the card or use it over the internet or some other form of "Card Not Present" (CNP) fraud.

Variations on a rip-off

An alert from the Metropolitan Police (London's 'Met') reports some variations:

- The scammer wants you to withdraw lots of money from your bank and take it home as part of a 'police investigation', perhaps into a corrupt employee. At some point they will want to take the money off you so as to put it back into the banking system. Which may well be the case, but it will be the scammer's account that it goes into, not yours, and they certainly won't have marked the bank notes. Helping a police investigation is the last thing they're thinking about.

- Another variation is to ask you to purchase 'an expensive watch or other expensive items' and hand that/those over. I'm not sure how that works, but no doubt there is some convincing reason presented by the scammer.

Points to remember

- Banks don't usually do home visits.

- A compromised bank card can simply be cancelled: the bank probably doesn't need it at all, and certainly won't treat collecting it as a matter of urgency.

- Your bank doesn't need all your account data to authenticate your identity, and won't – or shouldn't – ask for your PIN. A single bank will normally use different authentication criteria for internet banking, for telephone banking, for ATM access and for counter transactions.

- The police don't offer a card replacement service, and they aren't likely to ask you to help with an undercover operation. They won't ask for your PIN either.

- Legitimate, honest couriers and taxi services can be used for dishonest purposes.

- When you put your phone down, it doesn't mean the line is immediately cleared. This may be changed at some point because of the ways in which this feature can be misused, but the system does have legitimate advantages: for instance, if the phone is put down on 999 call, it allows the operator to trace the call (for instance, where the caller has disconnected under duress). I can't say if the same is true with 911 calls in the US.

The scam has been referred to by some resources as a vishing scam, which is fair enough. However, it's only one type of vishing (Voice over IP or VoIP phishing), not an alternative term. Sometimes a phishing message will include a number to call rather than a web link, and of course that's no more to be trusted than an unsolicited URL.

Once again, my thanks to Martin Overton, Richard Clayton and the Anti-Phishing Working Group for help received when I first researched this issue.

ESET Corporate News

ESET Researchers Release 2015 Cybercrime Predictions and Trends

ESET® has compiled a summary of the top cybercrime trends and predictions for 2015. While internet privacy and Android malware dominated the industry in 2014, an increase of sophisticated cyber attacks and risks associated with the Internet of Things and mobile payments top the list of what ESET expects to see in 2015.

ESET Online Scanner Is Now Available Through Facebook

ESET® announced that Facebook is offering ESET Online Scanner for Facebook to all users as part of the social networking site's complimentary anti-malware initiative. ESET's solution scans users' Facebook accounts, identifies harmful malware and helps them quickly remove it from their devices.

When Facebook alerts users that a device they are using is behaving suspiciously and showing signs of a possible malware infection, ESET Online Scanner for Facebook is offered to help fix the issue. Users can run the software, see scan results, and disable the malware all without logging out of Facebook—making it seamless and easy to clean up an infected device.

The Top Ten Threats

1. HTML/Refresh

Previous Ranking: 1
Percentage Detected: 2.82%

HTML/Refresh 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.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 2.54%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address from which it tries to download several files. The files are then executed and HTTP protocol is used for comunication with the C&C to receive new commands. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. Win32/Adware.MultiPlug

Previous Ranking: 3
Percentage Detected: 2.39%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it's present into the users system might cause applications to displays advertising popup windows during internet browsing.

4. Win32/TrojanDownloader.Wauchos

Previous Ranking: 4
Percentage Detected: 1.87%

It is a trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer IP address. Then, attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

5. Win32/Sality

Previous Ranking: 5
Percentage Detected: 1.39%

Sality is a polymorphic file infector. When executed it starts a service and created/deleted registry keys related to security applications activite in the system and to ensure that the malicious process restarts at each reboot of operating system.
It modifies EXE and SCR files and disables services and processes implemented by and associated with security solutions.

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

6. LNK/Agent.AK

Previous Ranking: 6
Percentage Detected: 1.31%

LNK/Agent.AK is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat. This vulnerability became known at the time of discovery of Stuxnet, as it was one of four vulnerabilities that were executed by Stuxnet variants.

7. INF/Autorun

Previous Ranking: 8
Percentage Detected: 1.22%

INF/Autorun is a generic detection of versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to autorun a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in an attempt to hide the file from Windows Explorer.

8. LNK/Agent.AV

Previous Ranking: N/A
Percentage Detected: 1.21%

LNK/Agent.AV is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.

9. JS/Kryptik.ATB

Previous Ranking: N/A
Percentage Detected: 1.19%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

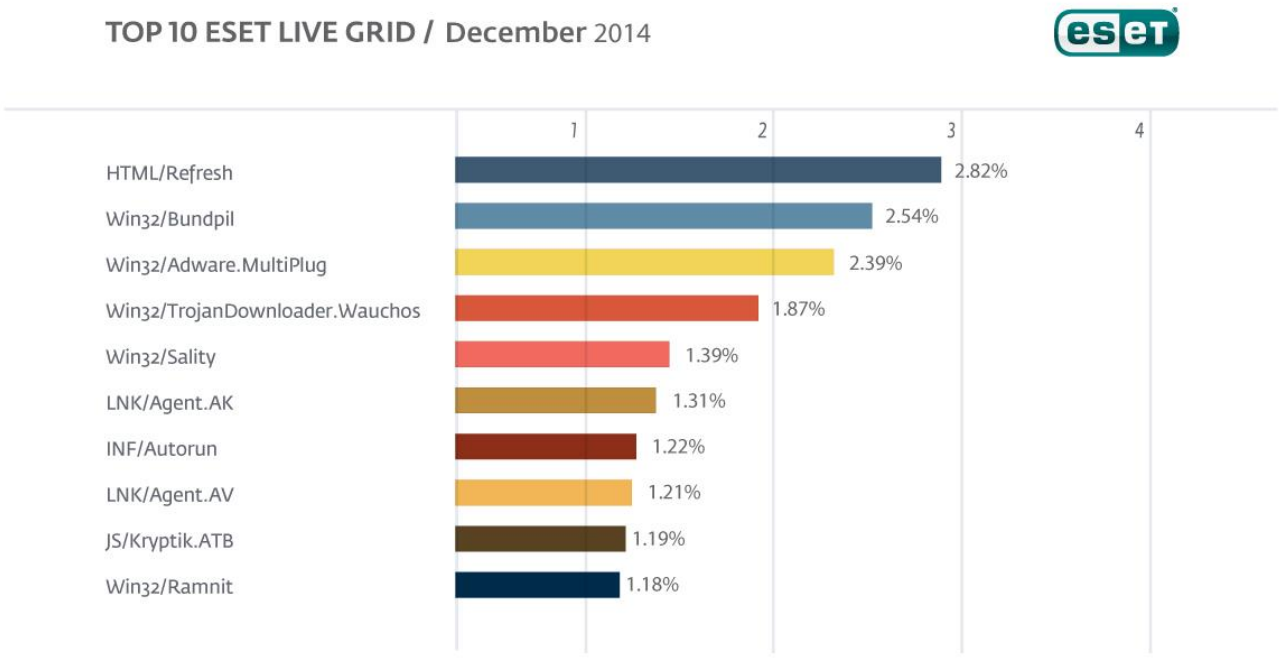
10. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.18%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. It exploits a vulnerability found on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remoteley to capture screenshots, send information it has gathered, download files from a remote computer and/or the Internet, and run executable files or shut down/restart the computer.

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 2.82% of the total, was scored by the HTML/Refresh class of treat.



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
- WeLiveSecurity
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation