National Fraud Intelligence Bureau

Intelligence Debrief Report

February 2014

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the National Fraud Intelligence Bureau (NFIB) in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the NFIB. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998. The cover sheets must not be detached from the report to which they refer.

Welcome…

to the February 2014 edition of the NFIB Intelligence Debrief Report.

For those of you who are new to this publication, this document is compiled for you and as such your participation into its content is greatly appreciated. We target our research, analysis and with assistance from you we better identify areas and systems that are being exploited by fraudsters.

Regardless of the size of the fraud or its complexity, we actively seek to fill knowledge gaps on your behalf and produce an informative and worthwhile document for publication to as wide an audience as possible.

Some of you may have seen our December 2013 Newsletter on the dangers and weaknesses within free public Wi-Fi that are being exploited by the cyber criminal. The previous newsletter received very favourable feedback from our partners with some organisations even placing it on their public facing websites. Other organisations circulated it through their staff as an information document to try and initially prevent the fraud. If you didn't receive a copy and would like to please get in contact.

From 'spankers' to 'sniffers', in these publications we have introduced you to all sorts of new words and phraseology used by offenders.

This edition focuses on a new phenomenon that we have called 'SIM Splitters'.

This document is designed to inform both users and security advisors of the dangers of external security measures. With fully informed law enforcement and private industry then we can work together to target harden and protect the public and businesses from future fraud.

For future issues, if you do have areas you would like to be included, please email NFIBfeedback@cityoflondon.pnn.police.uk and we will tailor our enquiries to suit.

We hope you enjoy this edition and you find it useful.

Tonight Matthew I'd like to be the bloke that takes over your bank account ………

We have all probably seen or can visualise a television talent show where a hopeful contestant walks through a brightly lit, smoke-filled studio set and onto the stage to sing a cover of a famous song. Ahead of them is an eager audience waiting to see if their performance is so convincing that it's like watching the star themselves. At the end we applaud their efforts and pass comment on how they almost fooled us into believing they were someone else.

Well that's fine when its theatre or on a stage, but perhaps not so when it's your financial institution trying to make contact with you to confirm that you want your money transferred into someone else's account.

Let's just stop at this point and answer the question - how do fraudsters find out what they know?

Firstly, what we are told is - don't underestimate the power of the internet and with it the ability of likeminded people to readily communicate across the world. Forums are wonderful places because I can ask the question, 'how do I…?' or 'can someone help me please…? When they work it out, it's posted back for all to read. Straight-forward search engines will bring back an awful lot of information, probably the answers you want if you look hard enough. Almost without exception, everyone we speak to has done their homework. For those of you that read the Wi-Fi security document in December and searched the internet as we suggested, you will have seen publically advertised 'ethical hackers'. At the end of the day information is information; it's the use it is put to that is the problem. Have a go yourself, open search straight from the home page, type 'how do I hack….?' and let the predictive search help you out. You may be surprised.

Last month saw the release of the Government 'Cyber Streetwise' initiative. The campaign is part of the Government's National Cyber Security Programme and comes at a time when an increasing number of people use the web on laptops, tablets and Smartphones. Findings from the Government's most recent National Cyber Security Consumer Tracker suggest more than half the population are not taking simple actions to protect themselves online.

Figures from the www.gov.uk website show that while 94% of people believe it is their personal responsibility to ensure a safe internet experience, the research highlights:

- only 44% always install internet security software on new equipment;
- only 37% download updates and patches for personal computers when prompted – falling even further to a fifth (21%) for Smartphones and mobile devices;
- less than a third (30%) habitually use complex passwords to protect online accounts; and
- 57% do not always check websites are secure before making a purchase.

We researched the NFIB KnowFraud system to help with some stats. Between the 1st Feb 2013 and 1st Feb 2014 we received 18,420 individual reports that could be classed as online account takeover fraud. **That's 348 a week or just over 2 every hour of every day**. These figures are only what are reported obviously and they don't include any other type of ID fraud, this is purely account takeovers.

So where is it coming from?

I can't blame the whole of the problem on Trojans but …

'…….a Trojan is like a key logger, it records everything that you do. We used to use them years ago but at that time they were put between the keyboard and the machine, looked like a bullet. We had to put them and, take them off and download them. These are much better, they sit there doing their thing and no-one knows they are there. The best ones are tagged onto websites, doesn't matter which one……'

'…..I buy all my stuff from Russia; pay him a grand for a whole person's profile. When you get the info it's like a long text document, everything they've typed, everything they have accessed, the whole picture. Wherever they have been, everything about them. I only want their bank statement and mobile number. That gives me everything I need. Other people I know use it for other things because it's their life, all written down for you….'

So let's specifically talk Trojans.

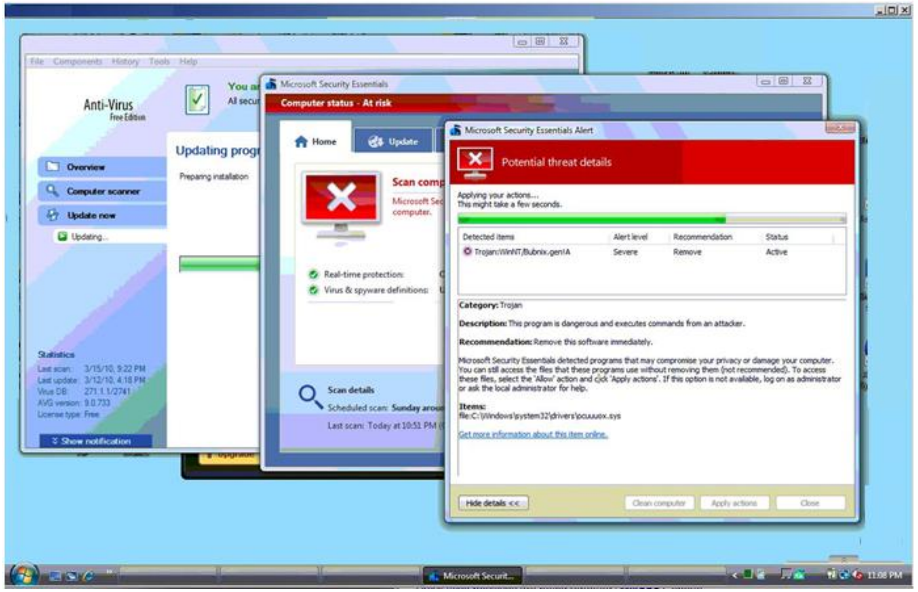
A Trojan virus is a piece of non-self-replicating malware which appears to perform a desirable function but instead performs a malicious action, often allowing unauthorised access to the victim's computer[1].

A typical example would be a 'free' antiviral program, such as the example diagram below. It manifests as a pop-up window and is alerting the victim to a malware attack, when it is actually the problem. It then 'scans' the computer looking for any infected files and 'finds' many fictitious threats with urgent messages urging the victim to click enter and to have them removed. During this time the virus has scanned the computer and removed the personal data stored there and sent it to a hacker. Viruses can be targeted towards specific pieces of data such as: usernames and passwords, emails, documents, account details, internet history and other sensitive information.

Trojan Horses, as in the Greek myth, are a bit different insomuch as once inside, they can change settings, spread further viruses and create back doors for the hacker to gain remote access to the system.

[1] NFIB. May 2013. *2013-04-30_Cyber Enabled Fraud – The Threats.pdf.*

As a final twist the Trojan anti-virus programme even offers to remove the fictitious infections for you. All you have to do is register, give them your bank details, name, address etc. etc. and voila problem ‘gone’……..



Applying your actions...
This might take a few seconds.

Detected items	Alert level	Recommendation	Status
Trojan:WinNT/Bubnix.gen!A	Severe	Remove	Active

Category: Trojan

Description: This program is dangerous and executes commands from an attacker.

Recommendation: Remove this software immediately.

Microsoft Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the 'Allow' action and click 'Apply actions'. If this option is not available, log on as administrator or ask the local administrator for help.

Items:
file:C:\Windows\system32\drivers\pcuuuox.sys

Get more information about this item online.

This type of malware does not spread through infected machines or replicate like Worms or other viruses; instead they must be activated on a machine by a user – like in the example above or by some form of social engineering by appearing to perform a legitimate function. This can be done either by downloading an infected file from the internet or opening an email attachment[2] (perhaps in a file with .zip or .exe after the file name) rather than just simply visiting an infected website. Recent examples have been emails purporting to be from Land Registry, banks and other institutions including online banking, social media, online auction sites to name a few. In fact it could be anything from anyone that, as a recipient, you are interested or curious enough to open.

With expanding technology Trojans are now expanding beyond PCs and are being downloaded onto Smartphones disguised as popular apps. Recreations or spoofs of the popular apps are appearing to take advantage of the craze. Some have now been removed from the App Store but these malware-hiding replicas are now available in a bid to be downloaded to people’s Smartphones.

From the fraudsters that we visited it became apparent that the hacking side of the fraud has been undertaken by Organised Crime Groups (OCGs) based in Russia. Their business model is solely to steal personal data through hacking and malware. This data, namely a bank statement, is then sold onto other OCGs based here in the UK. They then take on the next parts in the scam.

So back to the account take over.

The Russian OCG’s have somehow got the Trojan into your computer and they’ve retrieved the data they need, so what do they do now? As we know the bank monitors payments from an account to identify suspicious activity. So the last thing they want to do is go straight into the account and start transferring money. What they do now is open a business account or second account that sits parallel to the original. This account is in your name, your details and opened using a bank statement obtained

[2] Cisco. NA. *What Is the Difference: Viruses, Worms, Trojans, and Bots?* http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#6. Accessed 31.01.2014.

from the Trojan. It requires a lot less security than opening an initial account and is usually done on the same day.

'….opening an extra parallel account lets it sit next to the original without the real owner actually knowing. Bear in mind the bank thinks I'm the genuine person…..'

Once the account has been opened, the banking and personal details are then sent to the 'SIM Splitter', a master of their trade and with the fraudsters we spoke to, it's their day job.

Remember, phone companies are not designed to be a security or identity verification service; they provide phones therefore their checking procedure is perhaps not as robust as that of a financial institutions.

The SIM Splitter examines the information, checking to see if the victim has any payments for a contract mobile phone. The details will probably be on an email, either at the bottom of one you've sent or in an invoice, in your contacts or on a social networking site. (Remember that depending on what Trojan you have depends on what details they have gathered). He will then identify the phone provider from the internet. **Try it for yourself.** Put your number in and there you go, third click, www.ukphonenumber.net - don't forget all they want is the carrier or service provider. Our Splitter then conducts simple, open source checks on the victim i.e. Ancestry.com in order to obtain maiden names because they tend to be a security question, copies of birth certificates and marriage certificates.

Once this is done a simple process is followed:

- Using the bank statement obtained through the hacking establish the mobile network the victim belongs to;
- Obtain a blank SIM card, either through an insider at a phone company or purchase one for usually around £10;
- Use open source to establish the mobile phone network;
- Go to the phone provider and let them know that the mobile phone has been lost / damaged. Provide them with the details, namely the account number;
- Have new SIM card activated. (With some providers this only takes 10 minutes);
- As soon as the SIM card is activated transfer money from the victims account into the business account; and
- The banks will then make a call to the phone number on the account to confirm the transaction is genuine. (Some sends a text, and others phone asking if it is ok to transfer the funds, the Splitter just has to say yes).

'…….Once I get a SIM card, I have a very small window of opportunity. Usually get the fraud done within an hour. I tell the bank fraudster that the SIM is up and running and they then transfer money from the victim's current account to the business account. I then sit there and wait for the banks to either call or text me asking for confirmation. I always say yes and as soon as the transfer takes place I dump the SIM making it difficult for others to find me……..'

'………..I used to have a job, but this makes so much more money. I just sat at home with an old phone, putting different SIM cards in all day ready to authorise different payments from victim's accounts. We were doing 10 to 12 different accounts a week. I would then earn 20% of the takings or take an upfront fee. I'd clear £25 grand a week. But now I don't get to see my daughter……..'

'……I've got a mate in a phone shop who gets me 50 blank SIM cards at a time and I only pay him a grand. All you have to do is look at those shops that have huge numbers of SIM only transactions or lost phone reports. The flaw in this system is that you can't keep hitting the same place with the same person; they will spot you very quickly unless of course they are in on it. I used to have boys working for me to change the faces…'

'…..best bit comes when I have all the phone details, they think I'm the account holder. So I say, 'as I've lost the phone, do you think I should change my settings?', 'yes' says the phone company 'that's a good idea', so I change everything, contact details, security questions everything. Then when the victim finds out there phone is done the company won't even talk to them 'cos they can't answer the questions. By the time that is sorted out, I'm long gone…….'

So how do we know this goes on?

We completed some research through Action Fraud and here are some examples of how this type of crime is reported to us:

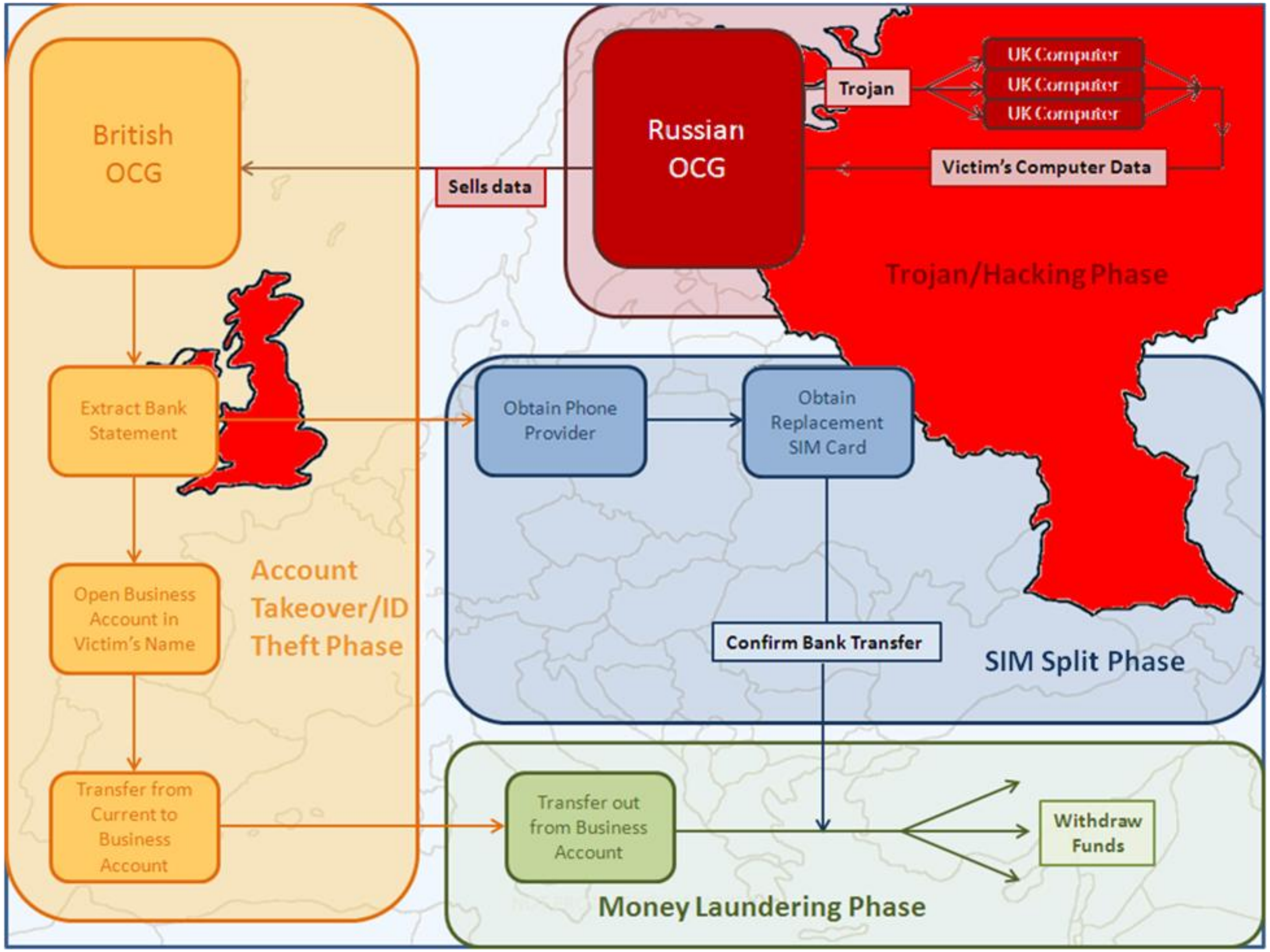
'Victim reports again that they received a text message from the bank to authorise the transfer then the mobile phone cut out. The victim called the bank the next day and they have suspended all accounts. Shortly after the victim received the text from the bank the mobile turned off with no coverage and now the phone provider do not believe that the victim is the account holder of the telephone from them.'

'The victim was paid from his employer and on the same day the suspect transferred a large sum of money into an account in the victim's name that the victim did not open. The bank have not refunded the money at this stage. The suspect also increased the victim's overdraft and on the same day his phone provider account was hacked online and the suspect requested a new SIM card for the account.'

'Victim was contacted by bank and advised that suspect had attempted to transfer money from victim's deposit account to his current account in order to transfer the same amount to suspect's bank account. The bank became suspicious and contacted victim about this and the transaction was stopped. It has transpired that victim's mobile phone had been authorised without victim's knowledge and accounts had been hacked. Suspect contacted mobile provider and asked for an upgrade for victim s mobile phone, following this the SIM card was cancelled and a new SIM card arranged. Suspect has also diverted victim's landline to another phone number. '

'On previous weekend the victim had a fraudulent transaction made to their bank account. Bank is dealing with this, however, at the same time the victim's phone stopped working. She took phone to supplier who stated her SIM had been hacked. They have reset everything so phone ok.'

On the next page is a diagram of the process of 'SIM Swapping'.


British OCG
Sells data
Russian OCG
Trojan
UK Computer
UK Computer
UK Computer
Victim's Computer Data
Trojan/Hacking Phase
Extract Bank Statement
Obtain Phone Provider
Obtain Replacement SIM Card
Open Business Account in Victim's Name
Account Takeover/ID Theft Phase
Confirm Bank Transfer
SIM Split Phase
Transfer from Current to Business Account
Transfer out from Business Account
Withdraw Funds
Money Laundering Phase

Lastly we completed some research with the providers to unveil what kind of security they hold around arranging for a new SIM card. Despite the know levels of risk surrounding identity fraud the results were quite shocking:

One company stated that in order to gain a replacement SIM the customer would require the phone number and PIN/Security code. If they did not have the PIN/Security Code they would require a photo ID. Despite not knowing what the genuine customer looks like, they would still accept this. This did not take into account a phone shop insider. A replacement SIM would then be issued free of charge and would take from immediate effect to 24 hours to activate.

Another told us that they require the phone number and a copy of the bank statement or any proof of address. It appeared to be up to the discretion of the staff member and this did not take into account a phone shop insider. There would be a £10 charge and would be activated anytime between then and 24 hours, but usually within 15 minutes.

The last provider we visited showed us a system specific to SIM swaps and the shop assistant does not know what questions will be asked until the security screen comes up. A demonstration was provided and they required the phone number, PIN and answers to the security questions (mother's maiden name, etc). A text is then sent to the original phone asking them to contact O2 customer service if they are unaware of any changes being made to their account. If the PIN is not known then ID is required namely a Driving Licence or Passport. This did not take into account a phone shop insider. A SIM is issued immediately and takes from 10 minutes to be activated. However, if the genuine customer were to contact O2 after receiving the security text then it would take around 15 minutes to get through to them. This provides a small window of opportunity for the fraudsters to confirm any transactions.

Some mobile phone providers do not hold copies of photographs or photo IDs of their customers when they sign up to a contract. This allows the SIM Swappers the opportunity to create false identity documents using their own photographs and the victim's details obtained through the stolen online bank statements, hacked personal data and open source searches. No guessing is involved as everything they need is right there in front of them and tailor made ID can be made for each victim transaction. In the case of some providers the Swappers only need to click 'PRINT' and hand in the stolen bank statement without the added cost of obtaining a fake ID each time.

We are hoping you have found this document useful. Is so, please let us know. We've shown you how the various stages of the fraud take place, so show us in return how you've used it please. We'd love to hear examples of how you've used it in particular cases or how it's been used to educate those new to the fraud arena.

Ok, that's it from us. Hope you enjoyed it. Be in touch soon.

The NFIB Proactive Debrief Team

Practical Guidance for PROTECT documents

This document is classified **PROTECT**. In government and law enforcement this determines the security measures that are required to protect it. This means:

- Only permit members of your staff who have a genuine ‘Need to Know’ to see the contents of the document;
- Do not copy the document or any of its pages without written approval of the Director of Intelligence NFIB;
- Do not pass on the document, or disclose any information contained in it, to any third party (outside of your business) without written approval of the Director of Intelligence NFIB;
- Do not read or work on this document in public areas;
- Lock the document in a secure cabinet when it is not being used; and,
- Only dispose of this product by shredding, pulping or incineration.

Protective Marking:	**PROTECT**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	V 0.1
Storage File Location:	H:/OPERATIONAL/Fraud_Intel/Intelligence
Purpose:	Quarterly Intelligence Debrief
Owner:	NFIB Management
Author:	DS Adams
Review By:	John Unsworth

The NFIB welcomes feedback from our readers to evaluate the quality of our products through continuous improvement and to inform our priorities. Please would you complete the following NFIB feedback survey through:
http://www.surveymonkey.com/s/AnalyticalProductsFeedback

This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send this to NFIBfeedback@cityoflondon.pnn.police.uk

NFIB – Intelligence Debrief Report February 2014

National Fraud Intelligence Bureau
21 New Street
London
EC2M 4TP

Phone: 020 7601 6875
Email: NFIBOutputs@cityoflondon.pnn.police.uk