October 2012

Feature Article: Ever received a “Londoning” scam?

Table of Contents

Ever received a "Londoning" scam?

Urban Schrott – ESET Ireland

The concept of the "Londoning" scam is far from new, but as it is still making the rounds and claiming victims, and we want to make sure that you're aware of it. The scam can arrive as an email, as a Facebook message, sometimes even as a mobile text message. Here's a recent example of such an email:

See Annex – Image 1

People generally like to help out a friend in need and cybercriminals were quick to start abusing that. The term "Londoning" originated from an epidemic of such scams circulating a couple of years ago, which often cited London as the place where your "friend" was mugged, but they may name any random destination. What they all have in common though, is that they ask the receiver to contact them and send them money. Straightforward, and in many cases quite effective too. Particularly if the scammers have gotten hold of some actual friend's of yours Facebook login and send you a message pretending to be them.

This type of scam is often compared to (and in some respects resembles) the infamous 419's or "advance fee frauds" (called 419s because of the article in the Nigerian criminal code which deals with such scams, as many of these we receive actually originate from Nigeria…) In fact, some examples of the scam actually named Lagos (the one in Nigeria) rather than London. However, David Harley, who has written extensively about these in the past, points out that whereas 419s are normally reliant on a social engineering message that tricks the victim into forwarding money, the 'London' scam may be a little more technically sophisticated. While spoofing an email to hide its true origins is not difficult, the so-called London scam is most effective if the scammer is able to hack the email or Facebook account (or something similar) of a real person as a means of deceiving his or her friends. This may, however, be carried out as part of a two-phase social engineering/phishing attack where the scammer first tricks the friend whose identity he steals into revealing his or her password, then uses the password to send fraudulent messages. However, some of these attacks may be more sophisticated than we think: some have suspected from conversations on Chat services that they might actually be talking to a bot rather than a live scammer.

So, how to spot such a scam?

- Well, you can be very suspicious of messages like this, however they arrive and wherever or whoever they come from. What constitutes "suspicious" in the email context? It's clear from the headers in the example above that it was sent to more than one person, doesn't indicate that the sender actually knows anything about the recipient other than their address (no personal touches) and so on.

- Don't even think of responding to the request by sending money until you've verified the source with extreme prejudice.

- Absence of personalization (personal touches in the message that actually indicates the sender knows you well) is a pretty good indicator of untrustworthiness (and characteristic of all generalized phish and 419 messages). If I was going to tap you for a few thousand quid, I think I'd probably ask after your spouse and children, for instance, however upset I was. However, bear in mind also that not all social engineering attacks are untargeted. Remember that someone who compromises your

Facebook account, for instance, has access to your profile and those of your friends, not just your account details and contact lists.

- If the way the message is expressed is uncharacteristic (especially if it sounds more "foreign" than you'd expect), that's a pretty good indication that you're not talking to the person you think you're hearing from.

- Be particularly sceptical when a "friend" (or, even more suspiciously, an acquaintance) wants you to send them cash by a scam-friendly channel such as Western Union.

- 419 scams are sometimes inventive in social engineering terms, but not necessarily hi-tech, so make sure you take reasonable precautions to avoid having your accounts (email, Facebook, other social networking sites) compromised. Use hard to break passwords, don't use the same password for multiple accounts, and be on the lookout for any attempt to trick you into giving your password away, and that will reduce your attack surface (no guarantees of invulnerability though!)

Quantum of Soullessness

David Harley, ESET Senior Research Fellow

Charlie Higson (@monstroso) has written a series of novels about James Bond as a teenager (no, I haven't read them). Which may well be why he was asked to compose a series of tweets summarizing twelve of the original James Bond novels in 140 characters or less, to mark the premiere of the latest James Bond movie, Skyfall. The UK free newspaper Metro (@MetroUK) – that's the one you're most likely find littering the seats in Tube trains – printed a couple of examples a day in advance: rather than describing a novel, one described the short story *Quantum of Solace*, first printed in a collection called *For Your Eyes Only*, and the other describes the movie also called *Quantum of Solace*. (Yes, I know *For Your Eyes Only* was also a movie.)

If you really want to, you can see those examples as published in Metro at http://e-edition.metro.co.uk/2012/10/22/index.html?p=5, though you'll have to subscribe to the magazine to do so, I think. You can read the tweets via the hashtag #BondTweets Metro also challenged readers to do better, so here, for what it's worth, is my summary of *Quantum of Solac*e:

Quantum of Solace: Fleming impersonates Somerset Maugham: 007 is passive audience to story of boring couple at Nassau dinner party

As a matter of fact, Somerset Maugham and Ian Fleming did have a certain amount in common: both did intelligence work (Maugham during the Great War, Fleming during World War II), and Maugham wrote a collection of stories about *Ashenden: or the British Agent* apparently based on his experiences as a spy – stories which in their turn influenced Fleming.

All very amusing, and if you're really interested in Higson's tweets, Twitter has conveniently aggregated them all at http://blog.uk.twitter.com/2012/10/tweeting-bond-novels.html, but what does it have to do with security? (IT security rather than national security, that is, though these days there's a close relationship between the two: just google cyberwar, cyberespionage and so on...)

Well, maybe the connection has more to do with authoring than security per se. It sometimes seems that the shoehorn is

mightier than the word-processor.

When I left the NHS in 2006, one of the first jobs I took on as an independent consultant was generating short security-related articles for a company in the US. (Actually, the brevity of the articles was less of a challenge than some of the restrictions on the *type* of content.) Recently I joined a panel of experts (ok, experts plus me...) whose role is to find 50 words or less on a current topic for inclusion in an occasional blog. Professional writers are often expected to keep to a word limit, but limits like these are hard work. You probably don't seriously expect a single tweet to give much of the flavour of a full-length novel, though in the case of an author you don't like much, maybe you'll prefer the tweet. [Insert your own suggested author names here...] But how feasible is it to distil useful security advice into 50 words? Well, the first one to which I contributed my (50) words of wisdom is at http://blogs.technet.com/b/mediumbusiness/archive/2012/09/27/don-t-duck-byod-culture-embrace-it.aspx, so you can judge for yourselves, if you want. (And by the way, if I'd had a few more words to play with, I'd have included a hat tip to Righard Zwienenberg, from whom I stole the CYOD acronym – his presentation at http://www.virusbtn.com/pdf/conference_slides/2012/Zwienenberg-VB2012.pdf will make the connection clearer.)

I don't feel too unhappy with that format: it's probably as useful as other articles that largely consist of short quotes from a range of (hopefully) knowledgeable people. The trick is to bear in mind the 11th law of Data Smog: "Beware stories that dissolve all complexity." (Data Smog: Surviving the information glut, by David Shenk: Abacus, 1997.) Sometimes it's more satisfying to ignore limits and use as many words as it takes (though hopefully not more than it needs).

It's not all about support scams

David Harley, ESET Senior Research Fellow

Recently, I've been hearing about and receiving phone calls from people with Indian accents about something a little different from the classic 'your PC is virus-infected but you can pay me to get it fixed' support scam. Craig Johnston, a friend (and former colleague at ESET) who was one of my co-presenters at Virus Bulletin this year (yes, it was a paper about support scams) recently received a call from someone claiming to be from something called the Australian Refund Agency, and that Craig was entitled to a refund of fees and taxes to the value of 5,349.27Australian dollars. All he had to do was write down a reference number and contact the scammer's supervisor on a local phone number, and the supervisor would organize the refund. Being a security guy from way back, Craig wasn't about to fall for that one, even if he hadn't met with the exact scam before. A quick Google search came up with a web site that described very similar scams: http://www.scamwatch.gov.au/content/index.phtml/itemId/792988. He still hasn't called that supervisor, even though he keeps getting calls urging him to do so.

The calls I've been getting have been slightly different (apart from the fact that I live in the UK, not Australia, of course). Most of them have started off by asking me to participate in a spurious survey, but I've also been getting calls that offer me refunds on a mortgage I don't have, or a way to save money by registering for a consumer group. In a little more detail:

- Offers of products and services benefiting from a fake government grant. I've had several of these, ranging from mortgage offers to grants for building work. I'm fairly sure

our cash-strapped government is not giving away money for kitchen extensions and conservatories.

- Refunds for overpaid tax, bank fees, mortgage refunds and so on. I'm trying to remember when I last got a tax refund: probably in the 1970s... Perhaps people really do get such refunds occasionally even in the present climate of "We shouldn't have taken your money but we can't afford to give it back", but I'm pretty sure that that agencies and institutions don't spend a lot of time and money ringing round people who might be entitled to restitution, still less paying Indian call centres to ring round.

- Here's another variation I came across recently when an elderly and somewhat easily confused relative rang me to find out if my wife and I were OK, as someone had rung her to say that we'd been involved in a serious accident. At least, that's what she believed they were telling her. If so, maybe it's a scam variation that I'm not aware of. I think, though, that it's more likely that she misunderstood a known scam where the scammer tells you that he or she represents the Accident Investigation Bureau and can get you recompense for an accident previously sustained by you or a family member.

Since I don't really want to spend the whole of my working day in fruitless discussions with scammers, I've taken to simply pointing out that my phone number is registered with the Telephone Preference Service (the UK's Do Not Call list) to get them off the line. (Though I have in the past had heated – if short – discussions with scammers who denied the existence of such a list or argued that it didn't apply to them, whereupon I've made short sharp references to UK law and European Community directives before putting the phone down.) However, there have been scams that actually try to exploit Do Not Call lists. (Some of these actually predate the current spate of Indian call-centre scams by several years.)

The most common variation is to offer to register your phone number: for a fee, of course. In fact, such lists are usually free, so if you give your credit card details in response to such a phone call, you not only waste your money and expose your credit card to further misuse, the chances are that you still won't be signed up to anything. In fact, our readers in the US should note that the Federal Trade Commission doesn't allow third parties to register telephone numbers for the National Do Not Call Registry. Unfortunately, I can't guarantee that this applies to all such lists, or that registration is free on all such lists and always will be. However, US readers might want to check the National Do Not Call Registry's page at https://www.donotcall.gov/, rather than pay attention to random phone calls. That page also makes an indirect reference to a scam variation suggesting that you have to re-register your number (for a fee), and assures subscribers that their registration does not expire.

- "INTERNATIONAL" or "WITHHELD" on the caller-ID display is a bad sign. Personally, I don't do business with anyone who hides his or her number of origin. However, an apparently local number isn't a guarantee of good faith.

- Evasiveness about what company the caller represents is a huge danger sign. Even if he or she is apparently forthcoming, ask for a name, company or governmental agency contact details and telephone number. If they really have anything to do with you, you should be able to verify those details independently and contact them directly by ringing back. Don't take anything for granted about the real identity of someone who rings you out of the blue.

- If you follow this blog regularly, you'll have a pretty good idea of how to spot a support scammer. If you read this far, you'll also be sceptical about claims to represent a Do Not Call service, and insist on verifying the service independently. And it's a pretty safe assumption that any unsolicited offer of refunds and rebates, free holidays and the like, is likely to end in an expensive disappointment.

- Do not ever give your financial details over the phone to someone who has rung up out of the blue. Verify, verify, verify!

In God we trust. All others pay ~~cash~~ by credit card

David Harley, ESET Senior Research Fellow

The ESET North America team was asked recently for our thoughts on whether we're moving towards a cashless society. Well, the US certainly is. I hear that only 5-10% of transactions there are carried out with real money nowadays. However, even ignoring all the security issues, there's still the question of what happens with those people who don't qualify for some form of credit or virtual cash, especially in a declining global economy. The last 10% will probably be more difficult than the other 90%, because there are people who simply cannot get credit.

'Real' cash is essentially a token: it represents a hypothetically redeemable fraction of a concrete object (a gold bar) representing a hypothetically standard unit of value. (Hypothetical because $1 represents a very different material value in the third world to what it represents in even the poorest neighbourhood in the US. Cashlessness doesn't (just) represent currency, though: it represents credit, which is essentially trusting the individual to retain his financial standing. In general, creditors don't intentionally give credit to people they don't know anything about, so they build up comprehensive financial profiles of individuals: initial acceptance is based on their history of past transactions, where they live, reputation in the financial community, police records, medical records and so on. But the more you use the facilities extended to you by a financial institution, the more they know about you, because they know what you buy, where you buy, and how dependable you are when it comes to repayment. The detail and reliability of those profiles may vary, but that's the essential mechanism.

This isn't automatically a bad thing, security-wise. It's harder to counterfeit (successfully and consistently, at any rate) coins and banknotes than it is to get illicit credit, or to steal someone else's credit. Of course a barter economy based on the exchange of material objects is even harder to game. On the other hand, stealing cash is, in some contexts easier than stealing credit or identity, and unless we're talking about transactions where bank note numbers are recorded, harder to trace back. However, bartering for services is harder to maintain without credit, and advanced societies are based as much on service as on the transactions involving material objects.

You can - within limits - test a coin or a banknote by its physical characteristics. You may be able to test a credit card by analogous mechanisms, but in a (largely) cash-free economy it's not only the validity of the card that's at stake, but the creditworthiness of the customer. For the customer, it's equally problematical to ensure that his creditworthiness is not compromised when his card is out of his sight, or when he gives his details to a web site or over the phone. Unfortunately, being aware of these issues isn't the same as being able to do something about them.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 5.30%

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. HTML/Iframe.B

Previous Ranking: 3
Percentage Detected: 4.41%

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.

3. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 3.29%

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.

4. HTML/ScrInject.B

Previous Ranking: 2
Percentage Detected: 3.09%

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

5. Win32/Sirefef

Previous Ranking: 5
Percentage Detected: 1.81%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

6. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.78%

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.

7. Win32/Qhost

Previous Ranking: 8
Percentage Detected: 1.48%

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.

8. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 9
Percentage Detected: 1.36%

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.

9. Win32/Sality

Previous Ranking: 10
Percentage Detected: 1.33%

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

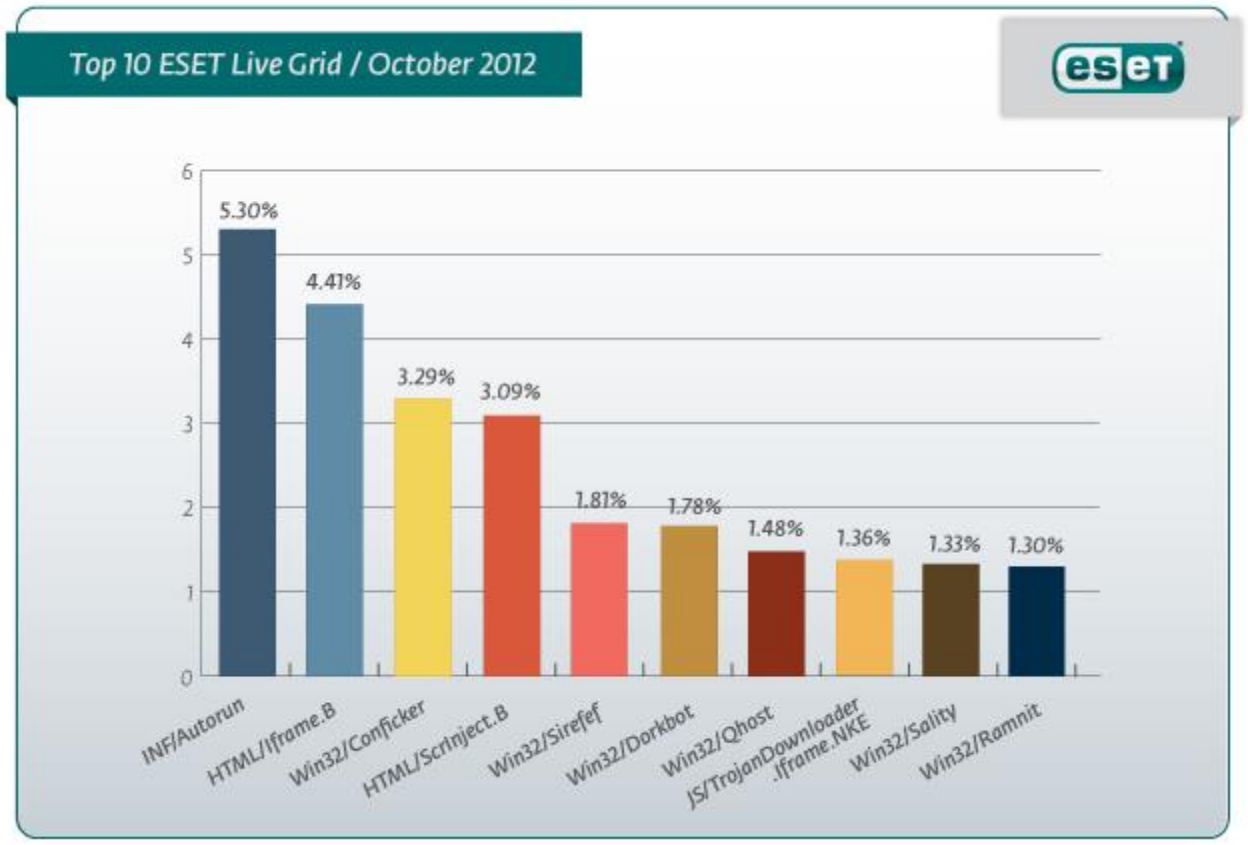
10. Win32/Ramnit

Previous Ranking: 28
Percentage Detected: 1.30%

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

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 5.30% of the total, was scored by the INF/Autorun class of threat.



Annex

-------- Original Message --------
Subject: My Milan Trip.Patricia Durney
Date: Wed, 24 Oct 2012 07:57:25 +0100 (BST)
From:patricia Durney
Reply-To:
To:undisclosed recipients: ;

I'm in some terrible and horrible situation,I came down here to Milan,Italy for a program and I was robbed at gun point last night, I misplaced my wallet on my way back to my hotel after I went for sight seeing. The wallet contained all the valuables I had. Now, my passport is in custody of the hotel management pending when I make payment.

I am sorry if i am inconveniencing you, but i have only very few people to run to now. i will be indeed very grateful if i can get a loan of 1,000 Euros from you. this will enable me sort my hotel bills and get my sorry self back home. I will really appreciate whatever you can afford in assisting me with. I promise to refund it in full as soon as I return. let me know if you can be of any assistance. Please, let me know soonest. Thanks so much.

Write me so I can let you know how to send it.

Thanks..
Trish

Image 1

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