October 2015
Feature Article: 419 Special

ENJOY SAFER TECHNOLOGY™

Table of Contents

419s: This Time it's (not very) Personal

David Harley, ESET Senior Research Fellow

This article first appeared on the Chainmailcheck blog and is used by permission.

Urban Schrott's recent article describes how one of his colleagues, advertising his car on DoneDeal, was contacted directly by a scammer who quasi-personalized the scam by using the car sale as a hook. In fact, the reference to the car is pretty perfunctory.

> *'Hello. Thanks for your email concerning your offer. The offer is just a minor objective of my contacting you but am going to buy it at your selling price.'*

In fact, the car had already been sold, and you may notice that the article refers to 'the offer' rather than 'the car', suggesting that the message is actually boilerplate text sent out to multiple recipients. Still, it may well attract the attention of some recipients long enough to be drawn into the scam – not only are they promised 30% of nearly 20 million dollars, but they get to sell their car/furniture/whatever.

From that point on, the message is of a type you may be familiar with, purporting to be from an American soldier needing help in transferring funds from Afghanistan. The English isn't bad, though there are some errors 'I have summed up courage to contact you' that suggest that English wasn't the writer's first language. I particularly like the writer's description of the misfortunes he's experienced:

> *'No compensation can make up for the risk we have taken with our lives in this hellhole, and I have been shot, wounded and survived two suicide bomb attacks by the special grace of God.'*

Talk about guilt-tripping… Let us know next time you're shot or bombed, Tim, and we'll send you a bunch of grapeshot. Sorry, grapes.

Of course, if the recipient is naïve enough to fall for this tat, he or she will find that he needs to send various sums in advance so that the mythical money can be forwarded to him. There have been instances in the past where victims have spent hundreds of thousands of pounds or dollars (and more) but have (of course) never received a penny (or a cent).

Urban's earlier article expands on DoneDeal's own advice on scam avoidance and safety. If you're not familiar with 419s and the other scams associated with classified ad sites, Urban's article and DoneDeal's advice are all worth reading.

There are, of course, many scams directly associated with buying and selling on the internet, but clearly it's also worth looking out for other types of scam using sites like DoneDeal's to reach potential victims, using what might at first glance seem to be a personal(ized) message.

The 419: Mugs and Mugus

David Harley, ESET Senior Research Fellow

This article first appeared on the ITSecurity UK blog and is used by permission.

I was delighted to receive the following invitation recently from someone calling himself Heinz:

> *… I have an offer worth 23million if interested, please contact me*

I wonder what it's worth if I'm not interested? (And 23 million of what? If we're talking about bedbugs or Zimbabwean dollars I'm not *at all* interested.)

Grammatical pedantry apart, this is an obvious 419 scam email. Fortunately, I stopped believing in Santa Claus and something-for-nothing some years ago.

A 419? That's an example of 'Advance Fee Fraud' (AFF), a type of scam where the scammer hopes to persuade you to send him money in the expectation that you'll get goods or services or large sums of money that are never going to arrive. It's called a 419 because that's the section of the Nigerian Criminal Code Act that apparently covers:

> *Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.*
>
> *If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years.*
>
> *[…]*
>
> *419A. (1) Any person who by any false pretence or by means of any other fraud obtains credit for himself or any other person-*
>
> *a) in incurring any debt or liability; or*

b) by means of an entry in a debtor and creditor account between the person giving and the person receiving credit, is guilty of a felony and is liable to imprisonment for three years.

[…]

419B. Where in any proceedings for an -offence under section 419 or 419A it is proved that the accused-

(a) obtained or induced the delivery of anything capable of being stolen; or

(b) obtained credit for himself or any other person, by means of a cheque that, when presented for payment within a reasonable time, was dishonoured on the ground that no funds or insufficient funds were standing to the credit of the drawer of the cheque in the bank on which the cheque was drawn, the thing or its delivery shall be deemed to have been obtained or induced, or the credit shall he deemed to have been obtained, by a false pretence unless the court is satisfied by evidence that when the accused issued the cheque he had reasonable grounds for believing, and did in fact believe, that it would be honoured if presented for payment within a reasonable time after its issue by him.

Even this dry chunk of legalese implies the intention of covering a wide range of scams, and there are certainly many varieties of AFFs and 419-related scams, though they don't all come from this particular Heinz *or* from the noted purveyor of baked beans.

For instance:

- Lottery scams (where you're supposed to pay a tax and other expenses before you can receive an enormous cheque after you win a lottery you didn't actually enter and have never heard of).
- Cheque overpayment fraud, a variation on fake/bouncing cheque fraud.
- Assassination threats – paying off the assassin.
- Job scams where you pay an agency a fee for getting a job that doesn't exist.
- Inheritance fraud.
- Scams based on transferring funds from people claiming to be bank officials, US troops in the Middle East, even a Nigerian astronaut and the Pope.

- Business 'opportunity' scams.
- Dating scams.
- Political refugee appeals: a request for help from a political refugee to get their money out of the country and into yours.
- Philanthropic/Religious appeals: requests for help with the distribution of money for charitable purposes. Often appears to be from a private individual who is dying, or the representative of a religious or philanthropic organization, including the Vatican.
- Mule recruitment messages: messages that resemble classic phish-related "jobs" in money-laundering but have a decidedly "419". Most often, though, these turn out to be another variation on advance fee scams tied to job "opportunities."
- Disaster scams: Personal disasters and bereavements are often used as hooks for 419s, but so are armed conflicts, earthquakes and tsunamis. They may be used to supply spurious circumstantial detail to lend credibility to a scam story, but are also frequently used as the basis of false charitable/disaster relief appeals.

Of course, there are many more variations and sub-variations.

Believe it or not, this isn't the tersest 419 I've seen. Last year, I wrote:

> **Footnote. Or Foot in Mouth Note.**
>
> *And the award for the laziest 419 of the month goes to roselyngrey2, who sent me a message with the subject "I have a project. If interested. Reply". Yes, that's how it was punctuated. And there was no message body. I find it hard to imagine that anyone has ever fallen for that one…*

You might think that the point of this kind of brief message is that it's quite difficult to filter using software that looks for phrasing and phraseology that's characteristic of the elaborate stories that so many 419-scammers concoct. And I'm pretty sure that explains why some 419s are delivered as attachments, especially graphics files such as .JPGs (but also Microsoft Word documents, PDFs and so on). It's not by any means impossible to read text presented in a graphic using some form of optical character recognition software, but that's more resource-intensive than a simple text filter.

(It is worth remembering, incidentally, that Microsoft Office documents, PDFs *et al* are very commonly used to deliver malware via vulnerabilities in document formats. This type of attack is mostly associated with APTs and targeted phishing rather than AFF, but 419-scammers do try new approaches to monetization from time to time.)

All that said, some believe that there is a trend among 419 scammers towards more efficient targeting. The presumption is that most people are likely to be suspicious of any message offering grotesquely large financial rewards from Nigeria or elsewhere in West Africa because of the age of the scam and the fact that some of the messages are so stereotyped. While many scammers have therefore generated elaborate messages intended to avoid sparking recognition of the scam, Microsoft's Cormac Herley answers his own question [Why do Nigerian Scammers Say They are from Nigeria?] by suggesting that:

> *Far-fetched tales of West African riches strike most as comical. Our analysis suggests that is an advantage to the attacker, not a disadvantage. Since his attack has a low density of victims the Nigerian scammer has an over-riding need to reduce false positives. By sending an email that repels all but the most gullible the scammer gets the most promising marks to self-select, and tilts the true to false positive ratio in his favor.*

In fact, there's evidence that some 'Nigerian' 419s aren't from Nigeria at all: certainly we use the blanket term 419 for many types of message, but individual instances of messages in those categories might have been sent from anywhere.

What about these comically, telegraphically short messages? It does seem to me that they might actually fit into this model of increasing Return On Investment by allowing a potential victim to identify himself as what the scammers call a ***mugu*** (big fool) simply by responding to a message that makes promises most of us would consider laughable.

I don't believe that being naïve about scam messages is necessary foolishness – it's easy for people who've had access to the internet for decades to be condescending towards newbies, but I've seen IT professionals fall for scams and hoaxes – and I certainly don't think that gullibility on the part of the victim justifies fraud. Still, it's probably a good idea not to get into conversations with these guys. (Unless you're one of those people who enjoys baiting scammers and wasting their time by pretending to be a sucker, in which case why would I disapprove?)

Unknown people who turn up in your mailbox wanting to give you something for nothing (sometimes we call these windfall scams) are not to be trusted. However, even 419s use other forms of social engineering as a lure: threats and humanitarian appeals, for example. Other scams such as phishing also use more than one form of social engineering, and while they are also often stereotyped in format – no personalization, threat of immediate loss of access to funds, and so on, that stereotyping may not be so easy to identify for the man in the street.

To quote a paper from 2007 by myself and Andrew Lee:

> There is no absolute, infallible test for discriminating between phishing mails and legitimate mails, either by eye or using automated software. Indeed, part of the problem is that occasionally, bad practice on the part of targeted organizations makes it easy for the scammer to generate mails that look very similar.

There are, however, a number of useful indicators.

- Email from a bank or other institution concerning an account with them that you don't actually have is obviously suspicious. It's almost certainly been sent to a number of email addresses the scammer got hold of, in the hope that in some cases, they'd strike lucky and someone with an account at that institution would get the message.

- There is, or should be, an obligation for any institution sending email relating to sensitive data to personalize it in some appropriate way so that you can be reasonably sure it comes from where it says it comes from.

But that's a topic that deserves addressing in its own right.

ESET Corporate News

ESET Launches Latest Version of Flagship Security Solution With New Banking and Payment Protection

ESET® announced the release of the latest versions of its flagship consumer security solutions – ESET Smart Security 9 and ESET NOD32 Antivirus 9. The new solutions employ advanced detection technologies to improve protection, usability and performance while maintaining its renowned light footprint.

The most prominent new security feature is **Banking & Payment Protection,** included in ESET Smart Security 9. This new feature provides protection when customers are using online banking sites or online payment gateways, and provides them with a protected browser ensuring all online financial transactions are processed in a secure environment. In addition, all the data the user enters, including credit card details and passwords, are encrypted.

ESET Smart Security 9 features security which also includes enhancements to proven technologies such as **Botnet Protection** and **Exploit Blocker.** Botnet Protection shields the user's computer from being taken over by a remote attacker and used as part of a network of infected computers for malicious purposes. Exploit Blocker is designed to fortify applications on the user's system, such as web browsers, PDF readers, e-mail platforms or Microsoft Office™ components. Building on technologies introduced on previous versions, ESET LiveGrid® is used as an advanced early warning system that allows for effective detection of emerging threats. Together, these advanced detection technologies are described in greater detail on the ESET Technology page.

The latest edition of both ESET Smart Security and ESET NOD32 feature a completely redesigned user interface based on extensive usability testing. The user experience is also improved through a completely new licensing framework that simplifies product purchases and activations. Access to online help content in ESET's Knowledge Base, as well as access to the gamified ESET Cybersecurity Education, remains free for ESET customers.

ESET's Next-Generation Business Products Called Outstanding by AV-Comparatives Annual Business Review

AV-Comparatives, an independent testing organization, published its annual IT Security Suites for Small Businesses Review. In this in-depth analysis of IT security solutions from nine vendors, it provides business customers with relevant evaluation of each vendor's security products. The following ESET next-generation business products were reviewed: ESET Remote Administrator, ESET Endpoint Security for Windows, ESET File Security for Windows and ESET Endpoint Security for OS X.

"ESET business products are exceptionally well designed, with important information and functions easily accessible," said Andreas Clementi, CEO at AV-Comparatives, and explained: "Two outstanding features of the product are its comprehensive, clear and well-illustrated documentation/help facilities, and the neatly designed endpoint protection software."

Moreover, according to AV-Comparatives, ESET Remote Administrator is suitable to manage networks not only of small businesses, but also at enterprise level and it is very straightforward to set up. *"All ESET next-generation business products are neatly designed and have easy-to-use protection software. The high degree of consistency among the versions for different platforms and also between the client software and the console can simplify the life of IT administrators,"* states the AV-Comparatives Review.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 5.80%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL from which it tries to download several files. The files are then executed and HTTP is used for communication with the command and control server (C&C) to receive new commands. The worm may delete files with the following file extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

2. LNK/Agent.BS

Previous Ranking: N/A
Percentage Detected: 2.62%

LNK/Agent.BS 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.

3. LNK/Agent.AV

Previous Ranking: 5
Percentage Detected: 1.74%

LNK/Agent.AV is another 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.

4. JS/TrojanDownloader.Iframe

Previous Ranking: 2
Percentage Detected: 1.69%

JS/TrojanDownloader.Iframe is a trojan that redirects the browser to a specific URL location serving malicious software. The malicious code is usually embedded in HTML pages.

5. HTML/ScrInject

Previous Ranking: 4
Percentage Detected: 1.63%

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

6. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.43%

Sality is a polymorphic file infector. When it is executed registry keys are created or deleted related to security applications in the system and to ensure that the malicious process restarts each time the operating system is rebooted.
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

7. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.39%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe (executable) files and searches for htm and html files into which it can insert malicious instructions. It exploits a vulnerability (CVE-2010-2568) found on the system that allows it to execute arbitrary code. It can be controlled remotely 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.

8. JS/IFrame

Previous Ranking: N/A
Percentage Detected: 1.31%

JS/IFrame is a trojan that redirects the browser to a specific URL location serving malicious software. The malicious code is usually embedded in HTML pages.

9. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.29%

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

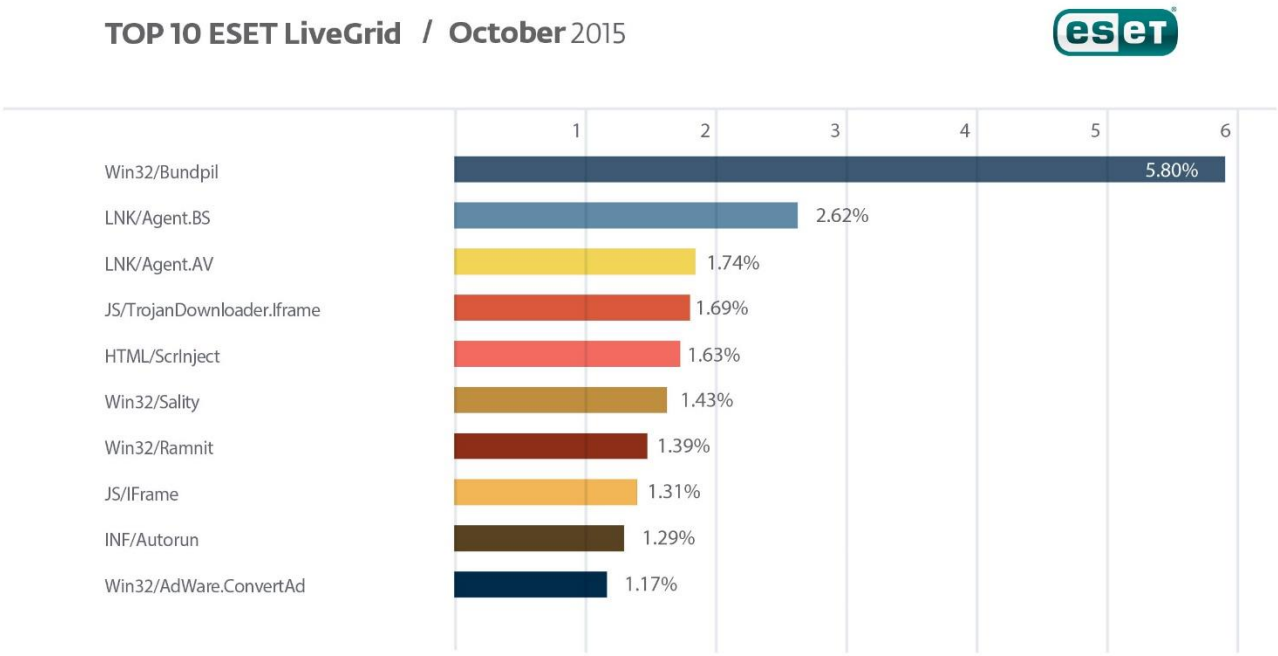
10. Win32/AdWare.ConvertAd

Previous Ranking: N/A
Percentage Detected: 1.17%

Win32/AdWare.ConvertAd is adware used for delivery of unsolicited advertisements. The adware is usually a component of other malware.

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 5.80% of the total, was scored by the Win32/Bundpil 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 has continued to lead the industry in proactive threat detection. By obtaining its 91st VB100 award in April 2015, 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 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