Threat Radar

January 2018
Feature Article: The Smiling Assassins (shaken not stirred)

eset ENJOY SAFER TECHNOLOGY™

Table of Contents

The Smiling Assassins (shaken not stirred)

David Harley, ESET Senior Research Fellow

[This article previously appeared on the AVIEN blog.]

I recently saw an article from Mark Stockley entitled *Ransom email scam from 'hitman' demands: pay up or die* and assumed - as I suspect many people will - that it was some particularly horrible example of ransomware. In fact, while it is pretty horrible in its way, it turns out that there's no real malware as such involved, just social engineering of the 419 persuasion, where the scammer claims to be an assassin ordered to kill the person who receives the email. In fact, I've written about this particular 419 sub-species several times before.

While the version noted by Mark Stockley rather more polished and up-to-date technologically (it wants payment in Bitcoin!) than most of the 419 scam messages I've seen that use a similar approach, it's not much different, fundamentally. Here's an extract from a particularly crass example I came across some years ago.

> I want you to read this message very carefully, and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i have being paid $50,000.00 in advance to terminate you with some reasons listed to me by my employers, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation.
>
> […]
>
> You will need to pay $15,000.00 to the account i will provide for you, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to), then the balance will be paid later.

Sometime later, my friend and colleague Urban Schrott drew my attention to a spam campaign that had been causing some hilarity over at ESET Ireland. The message had the subject "YOUR LIFE IS IN DANGER," and apparently came from someone calling himself Spike Dwaggin, though later he signs himself Dai Teatime. A commenter on one of my earlier blogs pointed out that Spike Dwaggin is a dragon from My Little Pony, that the name Dai features the

4th, 1st, and 9th letters of the alphabet (419 – geddit?), and told me that Dai Teatime is the assassin from Terry Pratchett's 'Hogfather'. (In fact, Pratchett's assassin is Jonathan Teatime, but close enough.)]

While it's not unusual for purveyors of 419 scams to use noms de plume reminiscent of famous people (real or fictional), this one is notably rich in popular cultural references. The article cited above references a few more, if you're interested. But here's the message from Spike/Dai.

As I sit here sipping a martini it is my regretful duty to inform you that you have been selected for assassination.

[Given the subsequent references to SMERSH, I can only assume that this would be a vodka martini (shaken not stirred).]

I am a professional assassin (I enclose my certificate of assassination as proof) and SMERSH have contracted me to assassinate you and have specifically paid extra for a particularly nasty death which makes it look like you died in a particularly bizarre sex game gone wrong; I had already bought the shire horse stallion (he's called Henry – picture attached), the lard and the dragon dildo (from Bad Dragon of course, I only use the very best tools) when I found out that you are innocent of the accuse, so I make out this time to contact you. Unfortunately international crime syndicates won't admit to mistakes and cancel the hit so I will be forced to carry out the assassination on you. Sorry about that old chap but rules are rules...

[Interestingly, the killer's modus operandi seems to have been influenced by a story relating to the Russian empress Catherine the Great, who was said (quite untruthfully) to have died as a result of being somewhat over-intimate with a horse. And could this particular horse be the Henry who 'of course dances the waltz' in the Beatles song 'Being for the benefit of Mr Kite'?]

There is an option for me to help you in other for you to know who had paid SMERSH for your DEATH and don't forget my men had been monitoring you for the past few days and daily record of your activities is been sent to me but I have refuse to order your DEATH.

[If your acquaintanceship with James Bond is limited to the movies, you may be unaware that a fictionalized version of SMERSH (a real Russian counter-intelligence agency that was wound up in 1946) plays a significant part in the very early novels. Oddly enough, a lot of commentary on 419-related forums relating to this particular example misses the fact that SMERSH and SPECTRE (a purely fictional criminal organization) are by no means the same thing, though there seems to be a certain amount of traffic from one to the other in terms of personnel. A bit like the AV industry… (And the word SPECTRE has acquired additional resonance recently in the security sector: see Aryeh Goretsky's article Meltdown and Spectre CPU Vulnerabilities: What You Need to Know for news of an altogether more serious threat.)]

Get back to me if you value your LIFE with all due speed or else I regret I will have to carry out my original contract to assassinate you and although he is quite charming for a horse I don't think Henry is the most sensitive of lovers.

Toodle Pip!

Dai Teatime
International Assassin

When I first saw the message on ESET Ireland's site, I assumed it was some kind of spoof intended to amuse rather than threaten. However, after checking on one or two scam-baiter forums, it seemed that Mr Teatime was probably quite willing to take money from anyone who appeared to have fallen for his shtick. As funny as this may seem to people who are security-savvy and all-too-well-acquainted with popular culture, it's possible that there are others who will find even this example genuinely frightening. And even more so with the crude threat exemplified in Stockley's article.

ESET Corporate News

Fancy Bear continues to spy in 2017, ESET researchers report

ESET has been committed to tracking Fancy Bear (also known as Sednit or APT28) – one of the most notorious cyberespionage groups in the world. A year after we brought out the most comprehensive whitepaper on the activities of this group, ESET researchers have uncovered a new version of Fancy Bear's flagship malware, Xagent, proving that the group remained very active in 2017, and continues to be in 2018.

Targeted tracking

Throughout its tracking of the group's activity, ESET has confirmed that Fancy Bear's main objective has been the theft of confidential information from specific, high-profile targets. The reported targets over the past few years include the French television network TV5Monde in April 2015, the German Parliament a month later, and the American Democratic National Committee (DNC) in March 2016.

When targeting individuals or groups, Fancy Bear uses two main attack methods to deploy its malicious software – typically by persuading someone to open an email attachment, or by directing an individual to a website that contains a custom exploit kit as the result of a phishing email. Once the group identifies an interesting target, it deploys its espionage toolkit, delivering long-term monitoring of compromised devices. Xagent is one of two backdoors delivered via this method and leveraged for spying.

An ever-evolving threat

In 2017, ESET discovered a new version of Xagent for Windows. As ESET reveals, Version 4 of Xagent comes with new techniques for string obfuscation and also featuresthe obfuscation of all run-time information. These techniques significantly improve the way in which strings are encrypted via methods unique to each binary.

The addition of new features and compatibility with all major platforms – Windows, Linux, Android and OS – makes Xagent the core backdoor used by Fancy Bear today.

Turla targets diplomats in Eastern Europe using fake Adobe Flash Player installers

ESET has identified and analyzed new malware used by Turla – the notorious state-sponsored cyberespionage group – to target high-value political organizations in Eastern Europe. This new tool, ESET reveals, attempts to trick victims into installing malware from what appears to be Adobe's website, with the goal of extracting sensitive information from Turla‘s targets.

While in the past the Turla group has relied on fake Flash installers to dupe users to install one of their backdoors, this is the first time that the malicious program has been downloaded from legitimate Adobe URLs and IP addresses. ESET is confident, however, that Turla's malware has not compromised any legitimate Flash Player updates, nor is it associated with known vulnerabilities in any Adobe product.

Analysis of Adobe Flash abuse

Having monitored the Turla group closely for many years, ESET found that this new malware is not only packaged with a legitimate Flash Player installer but also appears to be from adobe.com. From the endpoint's perspective, the remote IP address belongs to Akamai, the official Content Delivery Network (CDN) used by Adobe to distribute their legitimate Flash installer.

However, on closer inspection, ESET was able to see that the fake Flash installers were performing a GET request to extract sensitive information from the newly compromised systems. ESET telemetry can reveal that Turla installers have been exfiltrating information to get.adobe.com URLs since at least July 2016. Using legitimate domains for data exfiltration makes its detection in network traffic much harder for defenders, which highlights the Turla group's desire to remain as stealthy as possible.

Evidence of Turla involvement

ESET can be certain that this campaign is attributed to the Turla group for a number of reasons. First, some fake Flash installers drop a backdoor referred to as Mosquito, which has already been detected as Turla malware. Second, some of the Command and Control (C&C) servers linked to the dropped backdoors are using SATCOM IP addresses previously associated with Turla. Lastly, this malware shares similarities with other malware families used by the Turla group.

The Top Ten Threats

1. JS/CoinMiner

Previous Ranking: 1
Percentage Detected: 22.17%

The detection name JS/CoinMiner is applied to scripts that perform cryptocurrency mining without the user's knowledge. The scripts can be found on malicious sites, that you may be lured to via malvertising, or on legitimate sites that have been compromised to include the script.

2. HTML/ScrInject

Previous Ranking: N/A
Percentage Detected: 2.73%

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

3. JS/Adware.Imali

Previous Ranking: 2
Percentage Detected: 2.56%

JS/Adware.Imali is adware - an application designed to deliver unsolicited advertisements. The program code of the malware is usually embedded in HTML pages.

4. SMB/Exploit.DoublePulsar

Previous Ranking: 5
Percentage Detected: 2.43%

SMB/Exploit.DoublePulsar is our name for a detection preventing the exploitation of vulnerable systems by Win32/Exploit.CVE-2017-0147.A and Win32/Filecoder.WannaCryptor malware.

5. JS/Redirector

Previous Ranking: 4
Percentage Detected: 2.37%

JS/Redirector 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.

6. JS/Adware.Revizer

Previous Ranking: N/A
Percentage Detected: 1.84%

JS/Adware.Revizer is adware - an application designed to deliver unsolicited advertisements. The program code of the malware is usually embedded in HTML pages.

7. Win32/CoinMiner

Previous Ranking: N/A
Percentage Detected: 1.78%

The detection name Win32/CoinMiner is applied to scripts that perform cryptocurrency mining without the user's knowledge. The scripts can be found on malicious sites, that you may be lured to via malvertising, or on legitimate sites that have been compromised to include the script

8. Win64/CoinMiner

Previous Ranking: N/A
Percentage Detected: 1.6%

The detection name Win64/CoinMiner is applied to scripts that perform cryptocurrency mining without the user's knowledge. The scripts can be found on malicious sites, that you may be lured to via malvertising, or on legitimate sites that have been compromised to include the script

9. HTML/FakeAlert

Previous Ranking: 7
Percentage Detected: 1.53%

HTML/FakeAlert is a generic detection name for an HTML page showing a made-up, fake alert message, usually about a fictional virus infection or some other problem which is supposed to harm the computer or the computer user's data. The user is usually urged to contact fake technical support hotlines or to download and execute a fake security solution from the Internet to prevent "damage". This kind of page is usually used as a starting point for support scams.

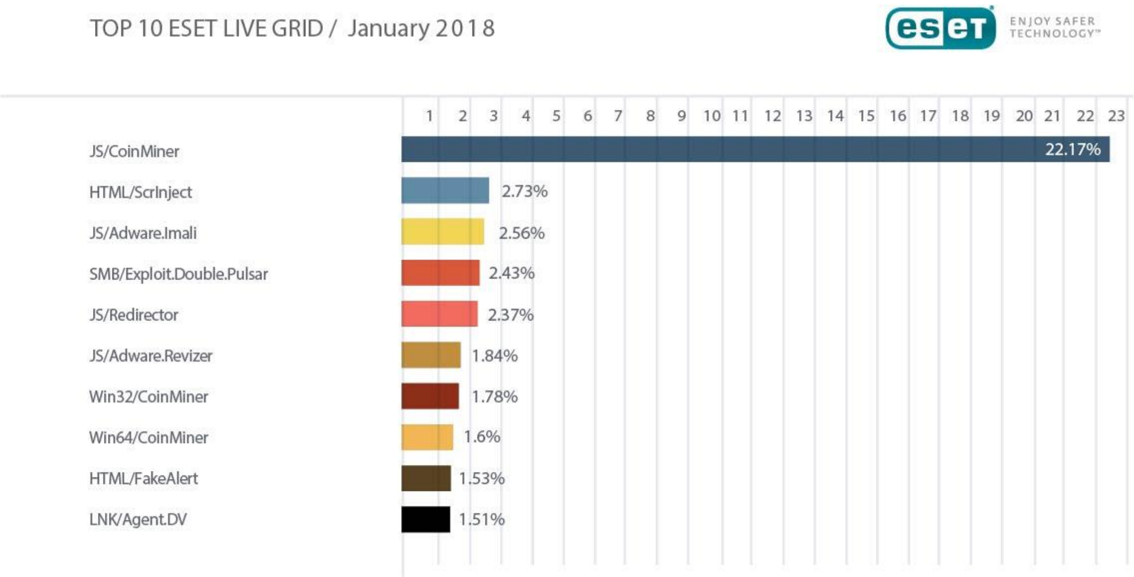
10. LNK/Agent.DV

Previous Ranking: 6
Percentage Detected: 1.51%

LNK/Agent.DV is a detection name for a *.lnk file that executes other malware and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, tricking users into believing that it's a link to drive content.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the most-detected malware this month, with **22.17%** of the total, was JS/CoinMiner.



About ESET

For 30 years, ESET® has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn 100 Virus Bulletin VB100 awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

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:

- VirusRadar
- ESET White Papers
- ESET Conference Papers
- WeLiveSecurity
- ESET Podcasts
- ESET Videos
- Case Studies