Threat Radar

June 2016
Feature Article: Bank Fraud, Privacy and Passwords

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Bank Fraud, Privacy and Passwords

David Harley, ESET Senior Research Fellow

[A version of this article originally appeared on the IT Security UK site.]

Whose Fault, Whose Responsibility?

Owing to extra-curricular preoccupations and a houseful of grandchildren, I didn't give quite the same attention to security news towards the end of May as I do normally, so I nearly missed an article by John Leyden for The Register: Bank in the UK? Plans afoot to make YOU liable for bank fraud.

While I don't feel a lot of love for the banking industry- so ready to seek taxpayers' money, to recover the cost of its own mistakes and to maintain generous salaries and bonuses for its upper echelons, yet so ready to cut back on services and so ungenerous when it comes to paying interest on the money we lend them – it seems reasonable enough in principle that customers should be to some extent accountable for their own actions in cases of proven negligence. Yet I feel a definite frisson at the prospect of sanctions against undeserving 'hacking victims' with 'poor online security', as discussed in 'proposed changes mulled by banks, the UK government and GCHQ'. Who is considered competent and impartial enough to *evaluate* a victim's security?

The banks who for decades have told victims that they must have shared their PINS, else their cards couldn't have been used? The banks who have proved so expert at sending security-hostile messages to their customers that have groomed those customers into accepting phishing messages that defy common sense and logic? The banks who want us to use the security software they offer even though it conflicts with other security software?

What could possibly go wrong?

Let's hope that the effectiveness of the measures financial institutions take to protect their customers' accounts is scrutinized even more carefully…

Security, Privacy and Passwords

Interestingly, the Register's article refers to 'proposed changes mulled by banks, the UK government and GCHQ'. Interesting, because the latter government agency (or rather its Computer-Electronics Security Group (CESG) recently decided that it wants us not to change our passwords. Something of a switch from the sort of over-generic security advice we normally expect from official resources – 'use and update antivirus, don't open suspicious emails, use strong passwords and change them often…' While Kieren McCarthy can't resist a little political snidery – 'As for CESG, we cannot think of a single reason why the organization, which is part of the UK's spying organization GCHQ, would benefit from people not updating their passwords' – there is, in fact some sensible commentary behind the switch. Forced password expiry does tend to encourage end users into avoidance strategies that may even make them more vulnerable. And in fact, the CESG advice is to some extent about hardening other aspects of authentication from the system administrator's end, so that insecure user behaviour is less dangerous.

FBI Alerts

David Harley, ESET Senior Research Fellow
[This article was previously published as two articles on the AVIEN blog.]

Data breaches used as basis for extortion

Not ransomware, but related in that it clearly involves extortion/blackmail: the FBI has issued an alert about Extortion E-Mail Schemes Tied To Recent High-Profile Data Breaches. The threatening messages arrive in the wake of a flood of revelations of high-profile data thefts. The ready availability of stolen credentials is used by crooks to convince victims that they have information that will be released to friends 'and family members (and perhaps even your employers too)' unless a payment of 2-5 bitcoins is received.

The generic nature of some of the messages quoted by the FBI doesn't suggest that the scammer has any real knowledge of the targets or of information that relates to them.

'If you think this amount is too high, consider how expensive a divorce lawyer is. If you are already divorced then…'

This sounds more like mass mailouts in the hope that some will reach a target sufficiently guilt-ridden to pay up just in case. Other messages may well frighten some people, fearful of being 'doxed', into paying up in case their personally-identifiable information falls into the wrong hands.

Support scam alert

Another FBI alert, this time summarizing an increase in reports of tech support scams. While law-enforcement alerts are often behind the curve, there are several points well worth noting here:

- The addition of two approaches to initial contact that have been particularly noticeable recently:

- Via BSOD/locked screen

- Addition of an audio message urging the victim to report the issue to a fake support line

- An uptick in the variation where the scammer offers a ‘refund’ on ‘services’ previously paid for. This isn’t the technique much favoured by 419 scammers where the scammer takes advantage of the time it can take for a cheque to clear. Instead, the scammer persuades the victim to give the scammer remote access to the victim’s account as well as to his or her PC.

Stuxnet Revisited

David Harley, ESET Senior Research Fellow
[A version of this article was originally published on the ITSecurity UK blog.]

I’m not generally a fan of articles that revisit antique malware that ceased to matter years or even decades ago. However, it appears that – six years on from when it first came to everyone’s attention – Stuxnet still commands attention. And I’m not even talking about the recent wave of ‘Stuxnet revisited’ posts centred on FireEye’s analysis of malware that seems to owe something conceptually to Stuxnet’s targeting of Siemens systems but is intended ‘to manipulate a specific industrial process running within a simulated Siemens control system environment.’ Or the less-publicized issue of an unpatchable vulnerability in a web-based SCADA system used primarily in the US energy sector. (Affected sites *can* upgrade the component in question, fortunately, but they can’t patch it.)

However, I have been asked a few times recently about Stuxnet, about which I wrote a great deal at one time. I suppose it was particularly important because it was one of the events moved the site-specific hardware-targeting malicious code from the realms of myth or semi-myth (the Iraqi printer virus, the Siberian oil pipeline explosion) to some verifiable fact. However, when I started to answer some of those questions, I realized that there is still a great deal of speculation being accepted as fact. So I went back to the speaker’s notes for a presentation I made at Infosec Europe a few years ago, essentially based on ESET’s Stuxnet report (though a lot shorter!), for what I hope is a more balanced and less speculative view. I’m not going to commit to a precise attribution (how very AV!), but there was certainly an agenda that differed drastically from the profit-driven criminal operations that capture most of our attention.

The Stuxnet report was just one of several papers and articles on which I worked directly with (among others) Alex Matrosov and Eugene Rodionov, then both with ESET’s team in Moscow. However, it was certainly the longest – apart from the 85 pages of the report itself, there were acres of preparatory and follow-up articles. But then, it was unusual in several respects.

- It made use of an astonishing array of 0-day or little-known exploits, taking advantage of issues in Windows (MS10-046, MS10-073, MS10-061, MS10-092, MS08-067. 0-days are commonplace, of course, but it’s unusual to use so many at once. That was actually one of the clues suggesting that it wasn’t the usual criminal gang approach: more like a collaboration between specialists. (Ironically enough, my own initial involvement was partly due to my being pulled into a hastily-assembled Tiger Team including SCADA sites, state agencies and other security vendors.)

- It was, in programming terms, extremely sophisticated, despite its comparatively promiscuous dissemination, increasing its chances of early detection. Though a less sophisticated version had managed to stay under the radar for a good while before that. Perhaps the 0.5 version had been so successful that staying under the radar was no longer a major concern. Or maybe the intention was to send a public message (whether it was accurate or mere misdirection) about the capabilities of the agencies and states rumoured to have been responsible.

- It was signed with stolen certificates. That's not a ubiquitous practice, but Stuxnet certainly helped make the approach more common.

- A very hardware-specific payload in an unusual control language: some of the code looked likely to have originated with a regular developer with knowledge of SCADA systems and Siemens control systems.

Another unusual feature is that quite a wide spread of security research teams (hat tip to VirusBlokAda, Symantec, Kaspersky, Microsoft etc.) unearthed pieces of the puzzle, though not in a formally aligned way like the Conficker Working Group. Still, it's a measure of the size of the problem. For instance, while some research focused very usefully on the PLC code (requiring access to specialized hardware), ESET focused on the 0-day attacks, from which we learned quite a lot. But it appears that so did the bad guys.

Stuxnet's legacy is harder to define than its initial impact and the general impressions it aroused. Of course, it 'lives on' in terms of other malicious code that bears a family resemblance, or at least borrowed techniques and even vulnerabilities. Not to mention those films and TV programmes where it's mentioned in the context of some imaginary supermalware. (However, the threat from direct re-use of Stuxnet SCADA-specific code was hugely exaggerated.)

What it *did* do was to bring to light the importance of potential problems with SCADA and ICS that aren't directly relevant to Stuxnet and its own targeting, and raised awareness of the potential vulnerability of Critical National Infrastructure (CNI) sites. To quote from myself (a bad habit, I know…):

The next such attack may be focused on a very different sector and use entirely different exploits. But it's unlikely that there will never be another attack of this type, even if it really was the first.

ESET Corporate News

ESET welcomes data loss prevention leader Safetica to its Technology Alliance

ESET announced that Safetica, a leading provider of data loss prevention solutions, has joined the ESET Technology Alliance. As a result of this relationship, existing ESET customers now have the option to add Safetica DLP (Data Loss Prevention) suite to their layered security strategy through their existing ESET reseller.

In EY's Global Information Security Survey 2015, 56% of respondents defined data loss prevention as a high priority and 33% as a medium priority for their organization over the next 12 months. Safetica solves this issue and provides a full DLP suite which covers a wide range of security threats that originate from a common source – the human factor. Safetica defends companies against planned or accidental data leaks, malicious insider actions, productivity issues, BYOD dangers and more.

ESET named as Internet security product with least impact on system performance

AV-Comparatives, an independent security software testing organization, has just published the results of its regular Performance test measuring the impact of internet security software on system performance. ESET Smart Security 9 was found to have less impact on system performance than all the other internet security products tested, and received an **Advanced+** badge.

In the latest AV-Comparatives Performance test, ESET Smart Security was among 5 security products that achieved 75 points, the highest score; Avira, Bitdefender, Kaspersky Lab and Avast were the remaining. In the PC Mark test, ESET reached a score of 99.7 – along with AVG, Emsisoft and F-Secure.

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 6.72%

JS/Danger.ScriptAttachment is a generic detection of suspicious e-mail attachments.

2. Win32/Bundpil

Previous Ranking: 3
Percentage Detected: 5.14%

Win32/Bundpil 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

3. Win32/Agent.XWT

Previous Ranking: 4
Percentage Detected: 2.72%

Win32/Agent.XWT is a trojan that serves as a backdoor. It can be remotely controlled and is usually a part of other malware. It collects the operating system version and language settings, then attemps to send the gathered data to a remote machine using HTTP.

4. JS/Adware.Agent.L

Previous Ranking: 8
Percentage Detected: 1.68%

JS/Adware.Agent.L is the detection name for JavaScript code designed to deliver advertisements on an affected PC. When this code is injected into a webpage, it replaces advertisements it finds with new ones from hxxp://x.rafomedia.com. If ads found are already from rafomedia, the malware does not replace them.

5. HTML/Refresh

Previous Ranking: 10
Percentage Detected: 1.57%

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

6. JS/TrojanDownloader.FakejQuery

Previous Ranking: N/A
Percentage Detected: 1.40%

JS/TrojanDownloader.FakejQuery is usually located in legitimate HTML page and its main purpose is to load malicious content (from malicious source) into this page.

7. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.33%

Sality is a polymorphic file infector. When it is executed registry keys are created or deleted that are related to security applications in the system so as 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

8. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.32%

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 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.

9. HTML/ScrInject

Previous Ranking: 6
Percentage Detected: 1.31%

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

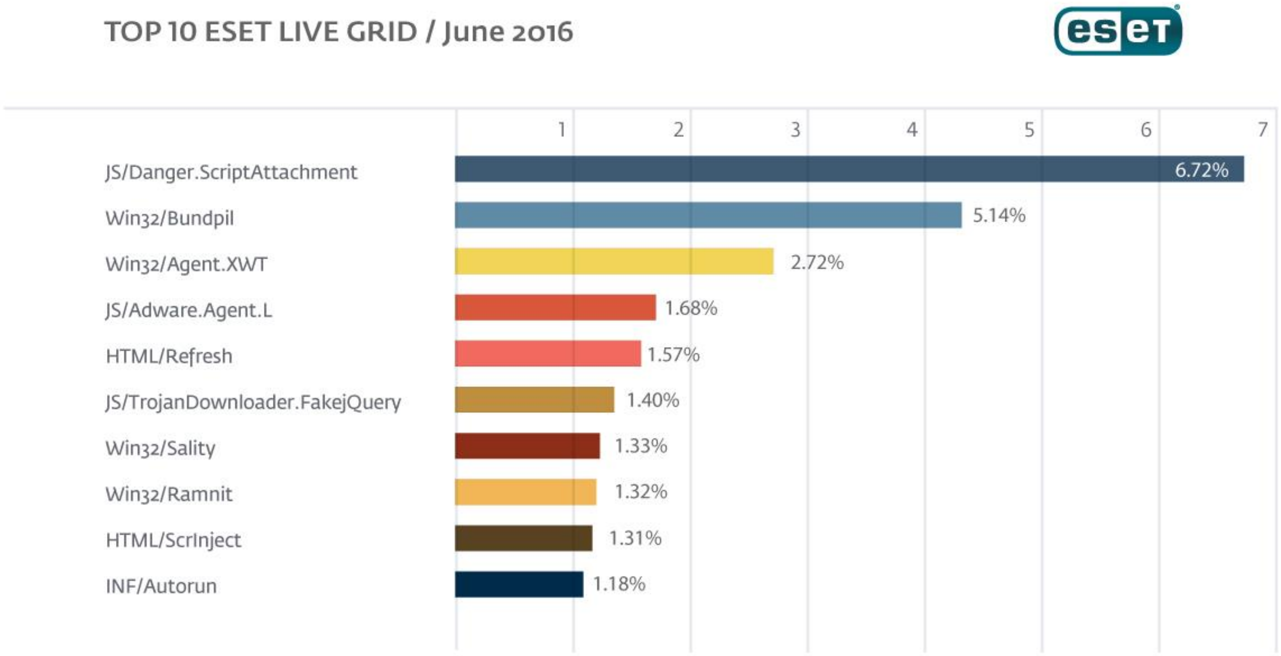
10. INF/Autorun

Previous Ranking: N/A
Percentage Detected: 1.18%

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.

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 6.72% of the total, was scored by JS/Danger.ScriptAttachment.



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 the United Kingdom, 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:

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

ENJOY SAFER TECHNOLOGY™