February 2017

Feature Articles: Key Card Ransomware-News versus FUD; When DIY Testing isn't DIY

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Key Card Ransomware: News versus FUD

By David Harley, ESET Senior Research Fellow. This article previously appeared on the ITSecurity UK site.

On the 28th January 2017, a news site reported that Hotel ransomed by hackers as guests locked out of rooms. The story initially claimed that a ransomware gang had been able to compromise systems in the Romantik Seehotel Jägerwirt in Austria including the key card registry system, even managing to lock guests into their rooms. The Local site later amended the article to explain that the claim that guests were unable to leave their rooms was 'due to a misunderstanding'.

Bleeping Computer's Catalin Cimpanu was rather more alert on the fact-checking front and pointed out that:

Fire code regulations all over the globe mandate that electronic key locks to open manually from the inside, which means no guest was locked inside their rooms. Additionally, electronic key systems are also created to handle power failures, so there was a way to open the doors from the outside, meaning no one was locked out either.

Graham Cluley also added a healthy dose of scepticism to the mix.

Why would a hotel announce that they had failed so spectacularly at securing their systems, and inconvenienced hundreds of their guests? Where were the quotes from aggrieved hotel guests who were locked in their rooms?

In fact, it appears that the hotel's reservation and cash desk systems were also hit: the hotel opted to pay the €1,500 ransom so that they could confirm bookings and arrivals, generate new key cards and so on. But also hardened its security systems so that a fourth attack failed, and is planning to replace its electronic room locks with traditional non-electronic door locks as part of its next refurbishment. There's a lesson there for anyone who hasn't yet noticed that the Internet of Things is at best a mixed blessing…

Several of the sites that originally uncritically accepted the story about guests being locked in have, fortunately, updated their stories to make them more accurate. I suspect, though, that there are 'fire and forget' journalists and bloggers who have simply moved onto the next media sensation. Enough, perhaps, to inspire a successor to the long-lived but wildly inaccurate claims that hotel key cards contain personal information about the guest and so pose a threat to their financial security, though I sincerely hope not. Still, in a post-truth age of alternative facts and fake news…

Graham goes further, suggesting that:

I wouldn't be surprised to hear computer security firms trotting the dubious anecdote out as evidence of the danger posed by ransomware for years to come.

Well, he has a point. Personally, I'm waiting for hype-happy next-gen vendors (or their partners) to claim that this is another failure of mainstream security products and we should be using their products instead. (That started out as a tongue-in-cheek remark, but given some of the outrageously deceptive marketing and inverted logic that comes out of one or two companies in that space I have a feeling it might just happen.)

When DIY testing isn't DIY

By David Harley, ESET Senior Research Fellow. A version of this article previously appeared on the Anti-Malware Testing blog.

For a while now I've been meaning to write about Carl Gottlieb's site TestMyAV. Well, not about that site so much as the pros and cons of companies setting up their own test labs.

It may surprise you to know that I actually started my career in security working for a medical research organization, and part of the job was, in fact, evaluating anti-malware products, even though in those days malware was nearly all viral. And yes, I did test with real malware. But long before I crossed the Great Divide and starting working with security companies rather than just using their products, I was scaling back on actual virus testing, as with the gradual escalation of the problem, I didn't have the resources to give it the attention it required.

Nowadays, since a sizeable proportion of my income comes from providing ESET with consultancy, I couldn't ethically set myself up as an independent tester, even if I had the time and resources. Clearly, I couldn't begin to compete with the sort of sample collection and validation that a security laboratory like ESET's has to carry out, and full-blown testing labs like those run by AV-Test or AV-Comparatives need extensive personnel and system resources. Not something that can be matched by an ageing, part-time author working from home.

TestMyAV worries me (a lot). It suggests that testing is simple enough that anyone can do it with the help of the resources that TestMyAV provides, including some high-level advice and documentation on setting up a lab, but also offering samples. And it seems to me that if newbie testers are reliant on samples from a site that doesn't disclose its sources, they have at least two problems. They have to assume that the samples are valid, in the absence of a documented validation process. And they don't know whether the samples are sourced from one of the companies they plan to test, which is a methodological disaster. As Simon Edwards, one of the most scrupulous testers I know, observed on Twitter:

'Testing anti-malware with malware provided by tested vendors (or related companies) is about as biased as testing can be. Don't do it!'

Clearly, he's referring to the fact that Carl Gottlieb is CTO of Cognition, which is a major Cylance reseller. And Cylance, like TestMyAV, persistently pushes the idea that independent testers are neither independent nor competent, and is reluctant to acknowledge the validity of external tests of its own product. TestMyAV states:

> Rather than trusting vendors, testing companies and sales people, we believe that testing isn’t hard and that everyone should have the ability to evaluate what solutions are best for their organisation.

You must have come across those 'Painting By Numbers' kits where the outline of a picture is marked out into numbered sections, where the number tells the aspiring artist what colour to use on that section. Well, TestMyAV sounds to me like 'testing by numbers', which isn't hard in that the site gives you several pages of instructions on how to set up a test lab, and then offers you the colours – sorry, samples – to use in your own tests. If you follow the instructions correctly, you should get exactly the results TestMyAV thinks you should get. But it's not clear to me why you should trust those results more than you would results from an independent tester.

I still intend to get back to this topic at greater length, though I'm making no promises about when or where. But in the meantime, it seems that Kevin Townsend has been worried about the site, too. In Anti-malware testing issues he lays stress on links between TestMyAV and Cognition. He emphasizes the number of pages there that offer an antivirus product recommendation. He summarizes the ongoing war of words between the mainstream used-to-be-antivirus industry and those companies that call themselves 'next generation'. And he suggests a less contentious way of testing products.

Kevin makes some very important points, but I don't agree with every word he says, of course: I think it's pretty harsh to suggest baldly that independent testers aren't independent, for instance, even though I'm not the testing industry's biggest fan, myself. The symbiotic relationship between testers and the mainstream security industry is complex and in some senses problematical, but both industries have - sometimes, at least - fought hard (in AMTSO and elsewhere) to strike the best possible balance in the interests of fair testing and the best outcome for the consumer, and their efforts have actually cleaned up the testing landscape dramatically.

Carl Gottlieb evidently disagrees vehemently with Kevin's entire article, but has chosen not to 'address the points publicly'.

ESET Corporate News

ESET Endpoint Security Wins the Highest Accolade in the Latest Anti-Malware Protection Tests.

ESET has broken an industry record with the number of awards earned, following a series of stringent industry tests by SE Labs, one of the world´s leading independent information technology security testing organizations.

In the latest series of SE Labs Anti-Malware Protection tests, ESET reaped three of the highest accolades- AAA Awards - by delivering 100% protection accuracy in tests for enterprise, small business endpoint, and consumer. This is the first time ESET has received three simultaneously AAA Awards since SE Labs' founding in 2016 and confirms its strongest features - zero false positives, low impact on system performance and 100% proactive protection.

"Now, more than ever before, protection is not only about blocking malicious URLs and having zero false positives, it is about the ability to handle more complicated, targeted attacks and being able to provide users with proactive protection without having an impact on their system. The SE Labs tests demonstrate these new, modern scenarios well and prove ESET products are functioning with 100% accuracy, for 100% peace of mind," said Juraj Malcho, Chief Technology Officer at ESET.

To learn more about the ESET product portfolio for home and business users, click here.
To read more about the SE Labs test results, please visit their website

ESET Researcher Named Executive Council Member of CompTIA IT Security Community

The CompTIA IT Security Community recently selected ESET Security Researcher Lysa Myers as an executive council member. She will now serve as an executive council member of the group, composed of industry leaders that collaborate to help the industry protect businesses. The group also provides guidance and leadership on the programs, education, and research offered by CompTIA, the non-profit trade association for the IT industry.

"We're extremely fortunate to have Lysa join our security community," said CompTIA's Lisa Person. "Her unique insights and perspectives on the security issues facing our industry assure that the programs we develop, the initiatives we support, and the positions we champion will have strong support across the industry."

Myers is a passionate security professional dedicated to educating businesses and individuals about security risks and how to avoid becoming a victim of emerging and common threats. Over the years, Myers has worked within anti-malware research labs and in testing organizations to help improve computer security products. Her role has enabled her to increase awareness around proper security practices and protocols. As a security researcher for ESET, and a frequent contributor to security publications, she continues to advocate for improvements to the security industry and greater training for all users.

The Top Ten Threats

1. Win32/TrojanDownloader.Wauchos

Previous Ranking: 1
Percentage Detected:5.81 %

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, including settings and the computer's IP address. Then, it attempts to send the information it has gathered to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

2. JS/Danger.ScriptAttachment

Previous Ranking: 6
Percentage Detected: 3.87%

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

3. LNK/Agent.DA

Previous Ranking: 4
Percentage Detected: 3.33%

LNK/Agent.DA is detection name for a *.lnk file that executes the Trojan Win32/Bundpil.DF. The LNK file is part of a Bundpil attack and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, convincing users that it's a link to drive content. It actually points to %system32%\rundll32.exe with a Bundpil DLL component as a parameter.

4. HTML/FakeAlert

Previous Ranking: 7
Percentage Detected: 2.97%

HTML/FakeAlert is 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 user's data. The user is usually urged to contact fake technical support hotlines or 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’.

5. Win64/TrojanDownloader.Wauchos

Previous Ranking: 3
Percentage Detected: 2.9%

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer's IP address. Then, it attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

6. JS/ProxyChanger

Previous Ranking: 2
Percentage Detected: 2.7%

JS/ProxyChanger is a Trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses.

7. Win32/Bundpil

Previous Ranking: 5
Percentage Detected: 2.29%

Win32/Bundpil is a worm that spreads via removable media. The worm contains a 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

8. JS/TrojanDownloader.Nemucod

Previous Ranking: N/A
Percentage Detected: 1.54%

JS/TrojanDownloader.Nemucod is a trojan that uses HTTP to try to download other malware. It contains a list of URLs and tries to download several files from those addresses. The files are then executed. This Trojan is now frequently associated with ransomware attacks.

9. HTML/Refresh

Previous Ranking: 9
Percentage Detected: 1.41 %

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.

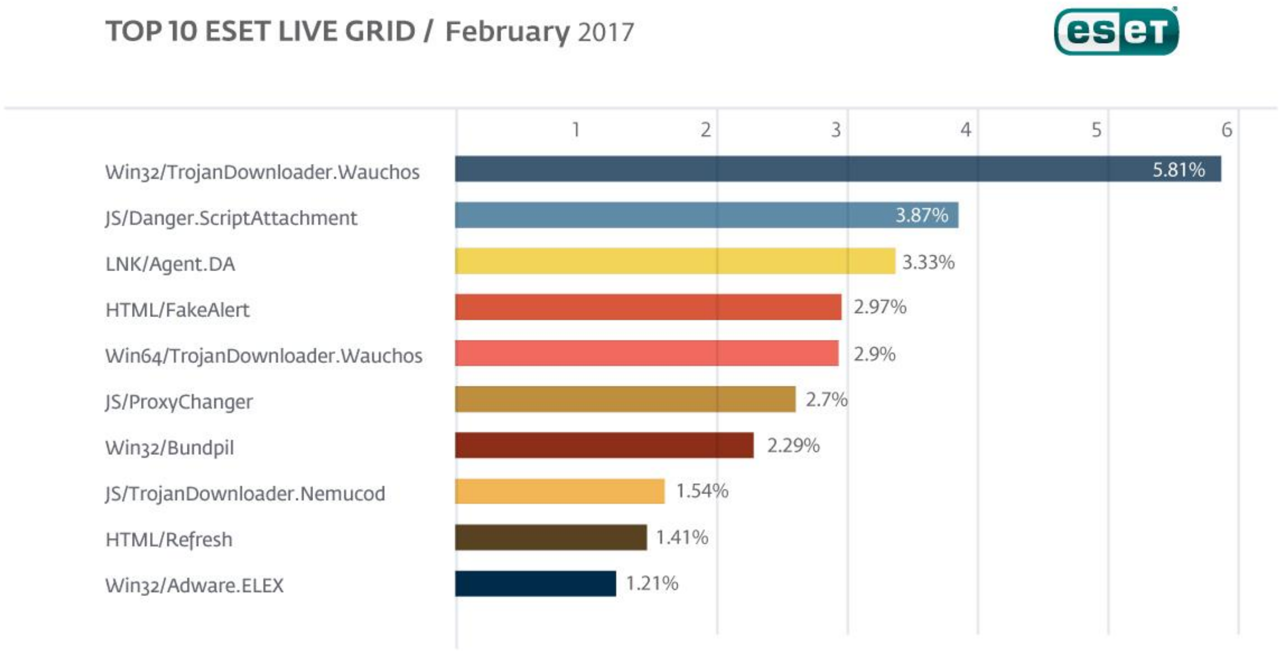
10. Win32/Adware.ELEX

Previous Ranking: 8
Percentage Detected: 1.21%

Win32/Adware.ELEX is an application designed for delivery of unsolicited advertisements to an affected computer. Usually, it alters the behavior (settings) of an Internet browser (for example adware sets its own “homepage” and setting back this value to original value is no easy task - the adware or a component of the adware is protecting this setting). Then the adware displays small windows with advertisements within the browser.

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 5.81% of the total, was scored by Win32/TrojanDownloader.Wauchos.



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