January 2017
Feature Article: Support Scams and Diagnostic Services

ENJOY SAFER TECHNOLOGY™

Table of Contents

Support Scams and Diagnostic Services 3
ESET Corporate News 5
The Top Ten Threats 6
Top Ten Threats at a Glance (graph) 9
About ESET 10
Additional Resources 10

Support Scams and Diagnostic Services

David Harley, ESET Senior Research Fellow

Every so often I get requests for help from people with a computer problem that may or may not be malware-related. Usually I'm unable to help directly because they don't give me enough information to identify the problem accurately, and I'm not in a position to offer worldwide one-to-one help in person, and anyway my helpdesk/support engineer days are long behind me. I don't have that range of expertise any more.

Finding a better 'ole

When I can't help, I try to refer the people concerned to a more appropriate person or forum, and to suggest they do what they can to ensure that the advice is from a reputable and competent source. I'm more cautious about recommending specific resources, even well-known commercial organizations, unless I'm in a position to confirm their competence and bona fides.

Unhealthy health checks

Sadly, this reluctance has been reinforced by accusations against Office Depot, which is alleged to have tricked customers into paying for unnecessary repairs to their systems. According to SC Magazine former technician employee Shane Barnett claims that:

'When computers were brought to Office Depot, staff were required to run ‘PC Health Check', a diagnostics scan which showed malware infections nearly every time.'

According to Bleeping Computer:

'KIRO 7 reporters tested the whistleblower's claims by taking six out-of-the-box computers to Office Depot centers in both Washington and Oregon. Office Depot employees diagnosed four of the six laptops with a malware infection and offered the reporter to fix it for an extra charge.'

Out-of-the-box and supply chain issues

As it happens, I remember back in the 90s routinely checking two out-the-box laptops that arrived in my office and discovering that both were infected with the Michelangelo boot sector virus, so I'm not about to assume that brand-new systems could not have been compromised by malware further back along the supply chain. However, the reporters had the KIRO 7 machines checked by security company IOActive, who were unable to find the merest sniff of malicious code.

Barnett claims that when running the software, sales people were required to ask the customer if they'd experienced 'strange popups, slow operating speeds, virus warnings and random shutdowns.' Well, popups and virus warnings could certainly signify a malcode problem, though they're not necessarily conclusive evidence. While below-par performance and random shutdowns can sometimes be associated with certain malicious programs, they may also arise from entirely different causes. However, Bleeping Computer asserts that:

'Barnett said that if the user answers positively to any of the questions, the scan would show a positive result.'

That, says an IT specialist at IOActive, is because the sales person is prompted to check a box within the program in that event, and if any one or more boxes are checked, the presence of malware is flagged.

Support scam? Poor diagnostics?

This has been likened by several commentators to the classic tech support scam. That may be a little harsh. It's possible that the software is simply 'over-sensitive', assuming that those four symptoms are conclusive proof of the presence of malware. Frankly, I suspect that a lot of technicians (who aren't necessarily security experts) might jump to the same conclusion. So I don't think that's proof of deliberate deception, but it doesn't indicate competence, either. Hence my caution when it comes to making specific recommendations. However, it turns out that the software was developed by support.com. According to Graham Cluley's post for Hot for Security blog, that's the company which:

'...was ordered, with partner AOL, to pay US $8.5 million in 2013 after being accused of using free malware scans to trick consumers into believing their PCs were infected.'

Which is disturbing. And, if the description of how the scans were used is accurate, far too close for comfort to the way that tech support scams work.

Fraud, incompetence and ethics

I think there's a question mark here, though. While the questions posed by Office Depot and the PC Health Check service don't constitute proof positive of the existence of malware, they do suggest the possibility of malware. Apart from that, they suggest some sort of problem with the system being checked. Did the reporters answer yes to any of those questions? If not, what reasons did they give for asking for the machines in question to be checked? What was the wording of the alert/warning?

You don't have to be faced with a problem with your system before you give it some sort of health check, but I suspect that most people only take their systems out for a check if they do have a problem. If one of those check boxes also gets ticked, it's not unreasonable for the software, or salesman, to think that there's a possible problem, even if assuming a 'virus' is not a conclusion I'd leap to personally. After all, in the past 30 years I've seen far too many dubious reports of techs claiming that they were unable to restore a system due to an unnamed 'virus'. Not to mention the many people who've reported miscellaneous system problems to me because they think a misbehaving keyboard or problem with the file system 'must be a virus'. (My usual answer is "it's possible, but a virus is far from the likeliest cause".) I'd need a lot of persuading to pay $180 for a solution to an unidentified virus or Trojan, too.

Scam or support problem?

This isn't necessarily quite the same as a support scam. There's a significant difference between old-school tech support scams and the newer model. The classic old-school approach - still happening! - is to ring people more or less at random and claim to be ringing about a problem the owner doesn't know about, but the scammer somehow (magically) does. Many reports I see nowadays are designed to lure the victim into ringing a fake helpline to get help with an issue the scammers have actually engineered by generating fake alerts.

Sometimes, however, a victim has a problem and goes looking for a solution, but finishes up at a call centre where he gets bad advice, based on deceptive 'diagnostic information', and a big bill. In the latter case, the scammer might argue that the victim is getting a solution to a genuine problem, just as Office Depot might be able to claim. However, if that solution is based on the same snake oil that the old-school scammers use to 'prove' that a system is compromised (misrepresentation of CLSID, EventViewer and ASSOC output, and so on), that defence falls apart.

Hopefully, Office Depot isn't using deliberate deception to extort money for fake services, though some of the claims made by Barnett have been interpreted as suggesting that it was. If it isn't, but its own investigation of the software and the way in which it's used indicates bad/incompetent practice, I hope it will amend its practices accordingly, as good ethics would demand. It would certainly be helpful if the company were to make public its findings, which doesn't seem to have happened yet.

This article was previously published on ITSecurity UK

ENJOY SAFER TECHNOLOGY™

ESET Corporate News

ESET opens new research and development offices in Canada and Romania

ESET Canada Recherché, the Montréal-based research and development branch of global anti-malware company ESET, continues its expansion in Canada with the opening of its new office in downtown Montréal. The company expects to strengthen its researcher base by doubling its staff in the city.

“Montréal proved to have all the key characteristics to welcome a successful cybersecurity R&D center,” said Richard Marko, Chief Executive Officer of ESET. “Almost a quarter of a million post-secondary students are currently enrolled in the city’s six universities, which brings an innovative spirit in many disciplines and allows for a constant flow of talented candidates. Montréal also benefits from a very active and diverse cybersecurity community comprised of a mix of start-ups and larger companies.”

ESET has been present in Montréal since 2009. From its technological hub on the Polytechnique Montréal campus it has been conducting cutting-edge research projects with a specific focus on situational awareness of web-based threats and enhancing public understanding of malware through blogposts, whitepapers and presentations.

“The threat landscape ESET customers are facing is constantly evolving and that’s why we believe that investing heavily in R&D is the key to offering the best protection, not only today but also in the future,” said Marko. “The reason ESET is so active in the Montréal community is that we believe we have a responsibility to develop the next generation of cybersecurity professionals.”

Destructive KillDisk malware encrypts Linux machines, ESET reseachers discover

The new variant of KillDisk has encrypted Linux machines, making them unbootable with data permanently lost. Despite the fact that the malware’s design doesn’t allow the recovery of encrypted files, as encryption keys are neither stored nor sent anywhere, the criminals behind KillDisk demand 250 thousand USD in Bitcoins. Fortunately, ESET researchers found a weakness in the encryption employed which makes recovery possible, albeit difficult.

“KillDisk serves as another example of why paying ransom should not be considered an option. When dealing with criminals, there’s no guarantee of getting your data back – in this case, the criminals clearly never intended to deliver on their promises,” says Robert Lipovský, ESET senior researcher. “The only safe way of dealing with ransomware is prevention. Education, keeping systems updated and fully patched, using a reputable security solution, keeping backups and testing the ability to restore – these are the components of true insurance.”

Learn more about KillDisk targeting Linux machines in the blogpost published on ESET’s security news site, WeLiveSecurity.com.

The Top Ten Threats

1. Win32/TrojanDownloader.Wauchos

Previous Ranking: 2
Percentage Detected: 5.86%

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/ProxyChanger

Previous Ranking: N/A
Percentage Detected: 3.62%

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

3. Win64/TrojanDownloader.Wauchos

Previous Ranking: 5
Percentage Detected: 2.86%

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.

4. LNK/Agent.DA

Previous Ranking: 3
Percentage Detected: 2.77%

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.

5. Win32/Bundpil

Previous Ranking: 4
Percentage Detected: 2.57%

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

6. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 2.34%

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

7. HTML/FakeAlert

Previous Ranking: 6
Percentage Detected: 2.30%

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’.

8. Win32/Adware.ELEX

Previous Ranking: N/A
Percentage Detected: 1.37%

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.

9. HTML/Refresh

Previous Ranking: 7
Percentage Detected: 1.25 %

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.

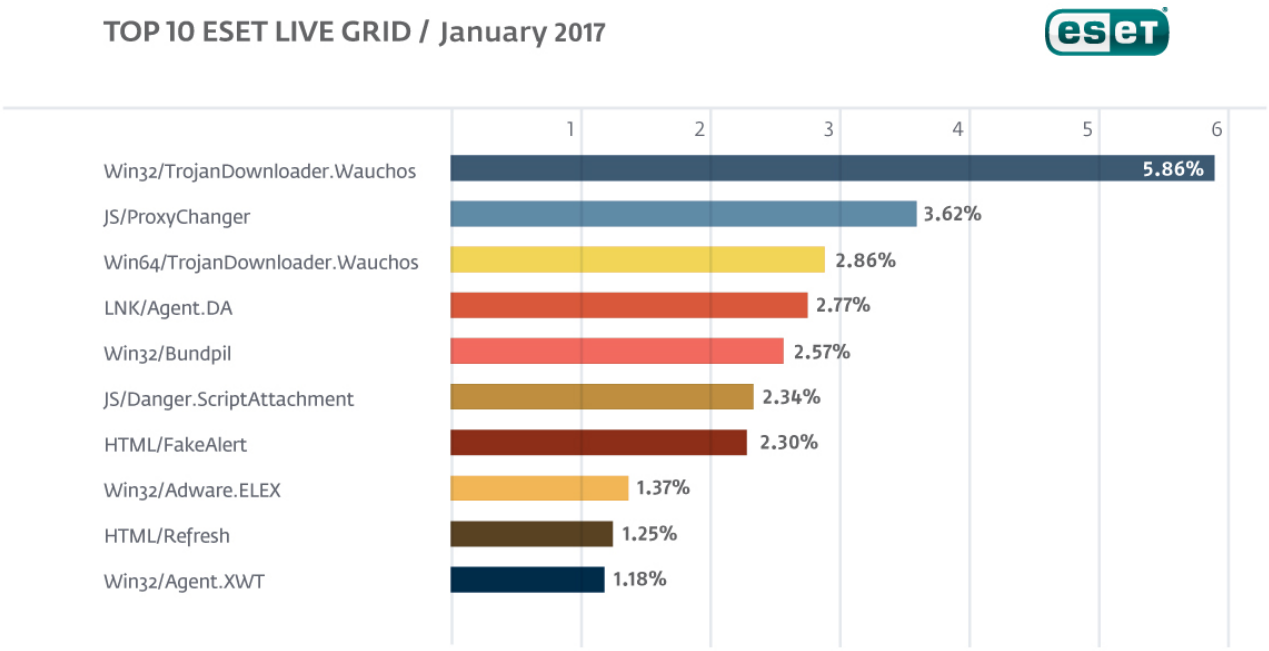
10. Win32/Agent.XWT

Previous Ranking: N/A
Percentage Detected: 1.18%

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.

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 5.86% 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