April 2015
Feature Article: Emerging Malware

ENJOY SAFER TECHNOLOGY™

Table of Contents

Emerging Malware

David Harley, ESET Senior Research Fellow

This article is a lightly edited version of some of the responses by members of ESET North America's research team to a number of queries posed in 2014 by an Information Assurance student working on a research paper on 'emerging malware threats.' In some instances, multiple researchers responded to the same question, so we have noted this in our responses.

--0--

What are your thoughts on operating system vendors moving towards a closed software distribution system such as the Mac App Store or Windows Store, as a solution to reduce exposure to malware?

Answer 1

Apple OS X and Microsoft Windows have probably moved as far in that direction as they can. I can't see them trying to force their customer-base to use only whitelisted versions of approved apps at this point: they are already using squillions of applications that have never been approved, and the OS vendors aren't going to push them through an approval process now. I realize that some will be approved in some sense (*e.g.* OS version compatibility), but they aren't exhaustively tested in the way that iOS apps and (some, and to some extent) Android apps are supposed to be.

Apple iOS and Google Android are different in that they started from scratch and were engineered to avoid some of the intrinsic security weaknesses of earlier operating systems, though you could certainly argue that Google fluffed it by not mandating a closed system where apps were only available from a regulated source. Also, you can argue that the devices are comparatively limited in their range of functionality. At any rate, I have yet to see one that would be an adequate replacement in all respects for a laptop.

What can the consumer should reasonably be able to expect from a closed environment? For the vendor to:

- Maintain the integrity of the model without letting applications through that started to pose some form of threat. Most of the problems with the closed distribution systems we associate with mobile devices aren't with unequivocal malware, but with apps in the grayware/PUA zone.

- Withstand the pressure to loosen the reins that's bound to come from those who come to realize they want more choice than they're given. (Jailbreaking/rooting happens for a reason, irrespective of whether it's a good idea…) That doesn't necessarily mean I'm in favor of a totally closed environment: it means that if your customers think that they're in such an environment, you have a duty to try to maintain it as such.

- Resist the temptation to assume that it can maintain perfect security on behalf of its customers at all times, or else in the worst case write off all breaches as the customer's fault.

- Take responsibility for the customer as well as for the system. Especially when it comes to dissuading the customer from believing that he never has to think about his own security.

—David Harley

Answer 2

First off, I think one has to understand that malware is largely these days a matter of organized crime, and that makes it a kind of business for these "dark-side entrepreneurs." They are accustomed to making money—or, to put it more correctly, *stealing money from others*—and simply because an operating system vendor has changed the software distribution model for their platform is not going to prevent them from finding ways to make money off it. In particular, they will look not just for vulnerabilities in the store system, but also for new "opportunities" in the store ecosystem to engage in new methods of criminality.

For example, we regularly see various fake apps which used to steal credentials for the legitimate app, pirated games which steal assets from original games, apps which claim to be a company's official app but just load its mobile web page, and so forth. All of which often bundle various forms of privacy-invasive add-ons such as adware and spyware in order to further monetize the app. We have even seen FakeAV apps appear on Android, a problem that in the past has been limited mostly to desktop operating systems such as Microsoft Windows and Apple OS X.

Now, these kind of malicious programs are not new on the desktop side of things—we've been dealing with a whole class of software called Potentially Unwanted Applications (PUAs) for over a decade now— but they tend to have slower growth rates because of the decentralized nature of where people get software. With app stores to "concentrate" software distribution into just a few sources, it becomes easier for even a small-time criminal to generate (read: steal) money.

When Windows Phone 8 was announced, I did take a look at what sort of problems we could expect in that gated ecosystem. That article may be found at http://www.welivesecurity.com/2012/02/24/windows-phone-8-security-heaven-or-hell/

There are also examples of categories of malware crossing over from mobile devices normally gated by app stores to the desktop. A prime example of this is *ransomware*. Historically, ransomware had never been more than a curiosity on PCs, however, the success of locking people's smartphones in Russia (and the CIS) and charging owners a small amount of money to unlock it (usually around $20-25USD) has led to the rise of malware like Cryptolocker under Windows, which targets businesses and requires hundreds of dollars in ransom payment.

So, in a nutshell, while closed software distribution models may discourage existing forms of malicious software, they also encourage criminals to find new avenues for theft.
—Aryeh Goretsky

--0--

Microsoft has been very outspoken about the security features built into Windows 8. Have your researchers noticed new techniques used by malware authors to infect Windows 8 (and 8.1) systems?

Windows 8, 8.1 (and 8.1 Update) do contain a great deal of improvements to prevent certain types of malware. For example, when running on modern hardware (*e.g.*, UEFI firmware-based), Windows can provide Secure Boot, a mechanism which is very effective in blocking bootkits, rootkits and malicious filter drivers that attempt to load early while the operating system is still initializing. But such techniques don't

protect against all malware, and in particular, they're not going to be very effective against malware that is (1) deployed through social engineering; and (2) runs within the context of the local user's account (*i.e.*, it doesn't try to do anything exceeding the permissions of the currently-logged in user).

For additional information on Windows 8.*x*'s defenses (and attacks on them), I refer you to the following articles I wrote on our We Live Security site:

- Windows 8 (security at RTM):blog • paper • podcast
- Windows 8 (RTM+6 months): blog • paper • podcast
- Windows 8.1 (RTM+12 months): blog • paper • podcast

They go quite a ways towards answering your question, above.
—Aryeh Goretsky

--0--

What tools does your company employ to combat such vast amounts of new malware created on a daily basis?

Many of the tools we use at ESET are going to be familiar to you from your malware reverse-engineering courses at university, including debuggers such as IDA Pro and OllyDbug; tools to decrypt or emulate JavaScript; multiple virtual (and real!) machines; tools like curl, PEiD and wget; packet sniffers, proxies, virtual machines and so forth. Sometimes we use tools "off the shelf," and at other times we may customize them to varying degrees.

Like all anti-malware companies, though, many of our tools are developed in-house and designed to handle very high transaction volumes (there are times when we have receive tens of new malware samples a second), while allowing connections from multiple users and locations. Without getting into specifics, such programs are designed to run on very fast computers with very high-resolution displays in order to maximize the amount of information displayed on screen. They also tend to display text with minimal or no graphics and rely on the keyboard for navigation, because that is much faster to use than a mouse. They are also universally very ugly, since they are designed by programmers for other programmers.
—Aryeh Goretsky

--0--

There are some security professionals that are especially critical of anti-malware software, because they are reactive and malware authors always find ways of evading detection. What do you say to these individuals with that viewpoint?

Answer 1

I've been hearing this over and over and over since at least the early 1990s, and it keeps rearing its ugly head. That leads me to believe that there is a fundamental misunderstanding about the issue -- both on the part of the general public (perfectly reasonable-- it's not their duty) and on the part of those aforementioned security professionals ("No comment"):

- First: are anti-malware scanners sufficient? No, and perhaps they never have been.
- Are anti-malware scanners necessary? Yes, but they're only part of the defenses that should be in place. [Other aspects include firewalls, regular and

automated software patching, host hardening, IDS and IPS, spam and phishing email filters, and the far-too-often-neglected user education]

- To those security professionals who say, in effect, that anti-malware software is a thing of the past, I ask them these questions:
    - What software is most prevalent on endpoint computers, and what security software is most frequently added to that already provided by the OS? It's clearly scanners. That in and of itself does not say that scanners are most important -- but it does indicate that there is at least a perceived value.
    - Do you advocate discarding all effective medicines for known maladies?
    - Do you advocate releasing all incarcerated violent felons?
- In effect, anti-malware scanners are like the prison system: they lock up the known bad guys. Moreover, the anti-malware research labs keep finding new bad guys and locking them up too; they also try to keep an eye on the neighborhood so that new "bad actors" are apprehended quickly. Like our police departments, though, crime usually is not prevented. While there is some aspect of proactive defense, there is a large element of reaction against the known bad operators.
- Anti-malware scanners provide something that the public may not realize or understand: they do not promise complete protection; instead, they promise:
    - Protection against the threats they recognize.
    - Commitment to search for and add speedy recognition (and protection) against new threats as they are discovered.

Very similar to our prison system in conjunction with law enforcement.

- Hence: yes, malware authors will sometimes find ways around anti-malware software, and those brand new variants will have a brief window of success, against some portion of the anti-malware scanners out there. But once discovered, the game is up -- unless, of course, you don't have mechanisms to recognize the attack. Scanners are a -- and perhaps for all practical purposes, THE -- time-tested way to provide that recognition and protection.

—Bruce P. Burrell

Answer 2

The following links might prove useful.

http://www.welivesecurity.com/2013/01/03/imperva-virustotal-and-whether-av-is-useful/
http://antimalwaretesting.files.wordpress.com/2013/05/dharley-feb2013.pdf
http://www.welivesecurity.com/2012/12/04/why-anti-virus-is-

not-a-waste-of-money/
http://www.welivesecurity.com/wp-content/uploads/2013/12/avar-2013-paper.pdf

Here's a lightly edited extract from the conclusion to that AVAR paper:

Personally (and in principle) I'd rather advocate a sound combination of defensive layers than advocate the substitution of one non-panacea for another, as vendors in other security spaces sometimes seem to. Actually, a modern anti-virus solution is already a compromise between malware-specific and generic detection, but I still wouldn't advocate anti-virus as a sole solution, any more than I would IPS, or whitelisting, or a firewall [still less a highly-specialized APT detection system]…

… if there's any single security solution (not just AV) that offers 100% detection and/or blocking of all malware and is still easy and convenient to use, totally transparent to all business processes, and never, ever generates some form of false positive, perhaps someone would tell us what it is so we can go and buy a copy…

… A major justification for malware-oriented security software is that it provides OS vendors and the vendors behind competing technologies with an incentive to try to keep ahead of malware (and antimalware). If all the researchers in AV labs retired or went to social media startups, the long-term impact on the overall detection (and therefore blocking) of malware would be considerable.

Those free products are effectively subsidized by commercial products – though they constitute a loss leader that may help to sell those same commercial products – and considerable resources and expertise are needed to maintain a quality anti-malware product.

We don't see how … effective but free anti-malware technology – as opposed to less effective products maintained by enthusiastic amateurs or as a 'value-add' to a different kind of security product – could survive.

…would the same companies currently dissing AV while piggybacking its research be able to match the expertise of the people currently working in anti-malware labs?

—David Harley

--0--

If you are an educator or student and have questions about emerging malware or anti-malware technologies, please feel free to contact us at AskESET@ESET.COM.

ESET Corporate News

ESET Welcomes Data Backup and Disaster Recovery Leader StorageCraft to the ESET Technology Alliance

ESET® announced that StorageCraft®, a leading provider of data backup and disaster recovery solutions, has joined the ESET Technology Alliance. As a result of this relationship, ESET customers now have the option to add StorageCraft backup and disaster recovery to their layered security strategy through their existing ESET reseller.

StorageCraft offers award-winning backup software and disaster recovery, data protection, and migration solutions for physical, virtual, and hybrid Windows and Linux IT environments. The company's solutions enable users to maintain business continuity during times of disaster, computer outages, or other unforeseen events by reducing downtime, improving security and stability for systems and data, and lowering the total cost of ownership.

By offering StorageCraft through ESET, customers and channel partners will receive an enhanced ordering experience, and easy access to high caliber products that cover a multi-layered security solution. In addition, partners will receive competitive pricing on ESET products when purchasing ESET and StorageCraft together.

ESET Selected as Finalist for 2015 Best of Interop Award

ESET announced its selection as a finalist for Interop Las Vegas' 2015 Best of Interop Awards in the Security category. The Best of Interop Awards recognize exhibitors for innovation and technological advancements in nine technology categories. Award winners will be announced from Interop Las Vegas 2015, which takes place April 27-May 1 at the Mandalay Bay Convention Center.

Interop Las Vegas, the industry's premier technology event focusing on the present and future innovations driving the IT community forward, is where ESET will showcase its completely redesigned and reengineered line-up of security solutions including the ESET Remote Administrator.

Before building the product, ESET conducted numerous in-depth interviews with customers and IT professionals around the world to learn more about the specific security challenges businesses of all sizes deal with every day. Real-world customer feedback underscored the importance of ease of integration, practical features without bloat, and an emphasis on simplicity in order to increase adoption, improve security, and lower overall cost of implementation and management. These findings are at the heart of ESET's new business products, providing improved usability and reduced IT resource requirements.

The Top Ten Threats

1. Win32/Adware.MultiPlug

Previous Ranking: 1
Percentage Detected: 3.57%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it gets a foothold on the users system might cause applications to display pop-up advertising windows during internet browsing.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 1.81%

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

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. JS/Kryptik.I

Previous Ranking: 7
Percentage Detected: 1.70%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

4. Win32/TrojanDownloader.Waski

Previous Ranking: 3
Percentage Detected: 1.67%

Win32/TrojanDownloader.Waski is a Trojan that uses HTTP to try to download other malware. It contains a list of two URLs and tries to download a file from the addresses. The file is stored in the location %temp%\¬miy.exe, and is then executed.

5. LNK/Agent.AV

Previous Ranking: 6
Percentage Detected: 1.35%

LNK/Agent.AV 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.

6. Win32/Sality

Previous Ranking: 4
Percentage Detected: 1.27%

Sality is a polymorphic file infector. When 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: 1.20%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. 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. HTML/ScrInject

Previous Ranking: N/A
Percentage Detected: 1.19%

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

9. Win32/AdWare.ConvertAd

Previous Ranking: N/A
Percentage Detected: 1.17%

Win32/Adware.ConvertAd is an adware used for delivery of unsolicited advertisements. The adware is usually a part of other malware.

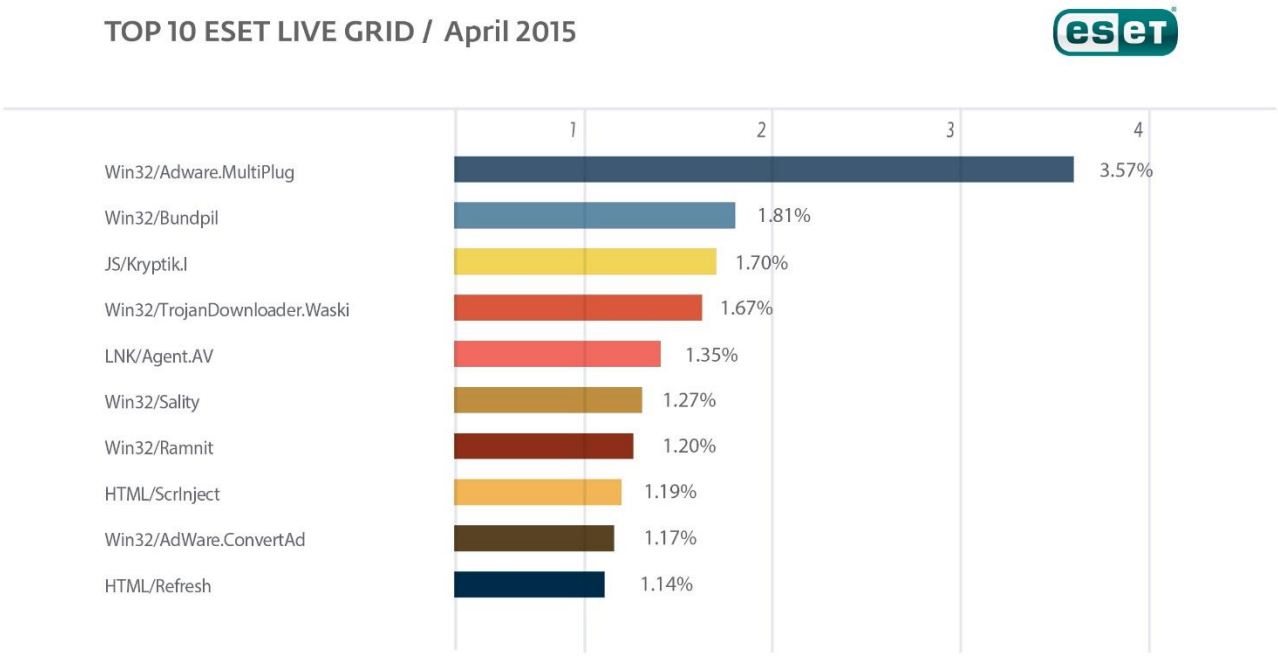
10. HTML/Refresh

Previous Ranking: 5
Percentage Detected: 1.14%

HTML/Refresh 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.

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 3.57% of the total, was scored by the Win32/Adware.MultiPlug 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 continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, 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 the 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