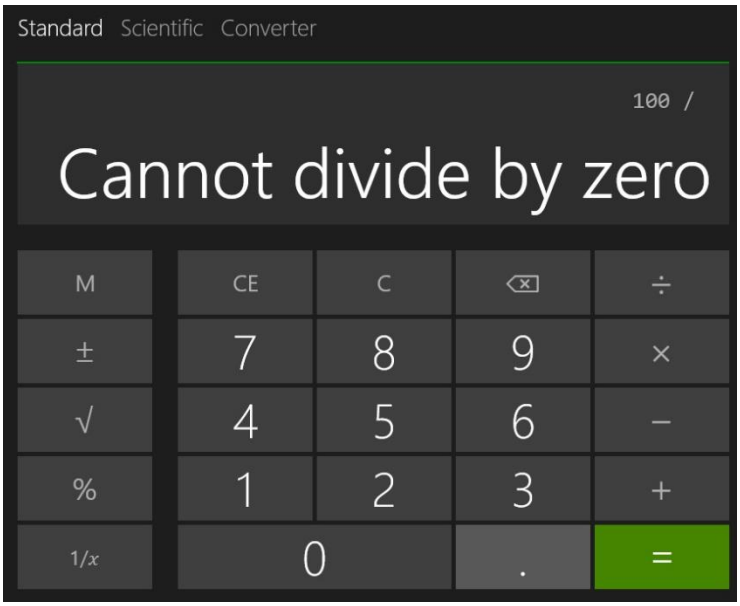
July 2015
Feature Article: Divide by Zero Cookie Intolerance

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Divide by Zero Cookie Intolerance



David Harley, ESET Senior Research Fellow

[A version of this article was previously published on the ITSecurity UK web site].

Once upon a time – I guess it was in the late 1980s – a band I was in got into a debate over what we should call ourselves. I'd fairly recently switched from the building industry to the IT industry, and had become totally hooked on programming, which may explain why my own slightly Zen suggestion was 'Division by Zero'. Yes, I know there is or was a Polish band with that name, but there wasn't then… Anyway, I was outvoted.*

Still, decades on I was fascinated to read that the internet is obsessed with what happens when you ask Siri "what's zero divided by zero?" It turns out that Apple's virtual personal assistant thinks that's a silly question and gives you an accurate enough but somewhat brusque response:

"Imagine that you have zero cookies and you split them evenly among zero friends. How many cookies does each person get? See? It doesn't make sense. And Cookie Monster is sad that there are no cookies, and you are sad that you have no friends."

Ouch! Well, maybe if you're easily offended by an automated response, you'd better not ask the question. But the chances are that people have been interested in seeing/hearing the meme of the week rather than the real answer to the question, which is (literally) indeterminate, mathematically speaking. I'm not going to attempt to explain it because, frankly, my understanding of calculus doesn't go much beyond being able to spell it.

However, 0/0 is actually a special case of division by zero. While Siri does offer a commonsense-ish explanation of why you can't divide zero by itself, and you can certainly argue that in terms of everyday arithmetic, there isn't much you can do with a number divided by nothing that you can't do with a number that isn't divided at all. However, there is actually a more formal reason why you 'can't' divide by zero.

From a programmer's viewpoint, though, there are practical issues. Calculators are normally programmed to return a 'Divide by Zero' error where a / is followed by a 0 followed by an =. In fact, many programming languages are specifically designed to prevent an illegal

'Divide by Zero' operation because the result of the operation is unreliable (to say the least). Sometimes, this will result in a compiled program grinding to a halt with an inscrutable error message along the lines of ' runtime error [numeric code] at [segment]:[offset]' which can be very embarrassing for the programmer, especially one who may have no idea what he's done to initiate an arithmetical operation. While I'm absolutely not a mathematician – and was never primarily a programmer – I did enough coding (some of it math-related) at that time to learn the hard way that sometimes you need to do some of your own exception handling in unexpected contexts. A program that crashes out with an error code is fine when you're debugging it, not so fine when it does so out in the real world.

What does this have to do with security? Well, the accuracy and integrity of data certainly concern those of us working in security, and an unreliable application – well, any application may fail if the right combination of the wrong circumstances arises – can certainly give you a nasty shock with a high impact. Reportedly, in 1997 the USS Yorktown suffered a systems failure due to a divide-by-zero error in a Windows NT application that left it dead in the water for two and three-quarter hours. One contributor to the RISKS digest observed that:

Ideally, the next few generations of operating systems will end up being so incompatible with legacy systems that no country anywhere will be able to wage war.

*I know you've only read this right to the end in the hope of finding out what we did call ourselves, so let me quench the fires of curiosity. We became the Flying Piglets. When I tell people that (not very often) they tend to say "Oh… you were quite famous then." Evidently I need to improve my enunciation: the Flying Piglets (not to be confused with Three Flying Piglets) weren't nearly as famous as the Flying Pickets.

ESET Corporate News

ESET Shares New Findings on Operation Potao Express

ESET has published a new research article concerning Operation Potao Express, an extensive analysis of the cyberespionage group behind the Win32/Potao malware family. An ESET white paper on the malware includes technical details on how the malware spreads and the most noteworthy campaigns since its first appearance in 2011.

Win32/Potao is a type of espionage malware that has been detected mostly in Ukraine and a number of other CIS countries, including Russia, Georgia and Belarus. The Potao family is a typical cyberespionage trojan that steals passwords and sensitive information in order to send them to the attackers' remote server.

Operation Liberpy: ESET sinkhole and destroy 2000-strong keylogging botnet

ESET has published an in-depth research article entitled 'Operation Liberpy: Keyloggers and information theft in Latin America'. Liberpy was a 2000-strong HTTP-based botnet that targeted Venezuelan users that employed keyloggers for the purposes of identity theft.

The operation kicked off with a malicious e-mail campaign that included infected attachments purporting to provide package-tracking details. Duped users who became infected were not only added to the botnet, but also became potential propagation nodes via attached or integrated USB devices.

Before moving to Windows 10, make sure you have the latest version of ESET

ESET announced that its home and business products for Windows are compatible with the newest version of Microsoft's operating system, Windows 10. However, users who still have older versions of ESET security products are advised to upgrade them to newer versions before updating their OS.

Businesses which have decided to upgrade their endpoints to Windows 10 are advised to make sure that ESET Endpoint Security and ESET Endpoint Antivirus are updated to the latest builds of versions 5 or 6. Older versions are not compatible with Windows 10.

For both home and business users, ESET has prepared a dedicated support web page that answers questions about moving to Windows 10: http://www.eset.com/us/windows10-compatibility-free-update

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 3.93%

Win32/Bundpil.A 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 C&C to receive new commands. The worm may delete files with the following file extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

2. SWF/Exploit.ExKit

Previous Ranking: N/A
Percentage Detected: 3.19%

SWF/Exploit.ExKit is a generic detection for exploits that take advantage of vulnerabilities in Flash software; usually associated with Exploit Kits.

3. Win32/Adware.MultiPlug

Previous Ranking: 2
Percentage Detected: 2.61%

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.

4. JS/Kryptik.I

Previous Ranking: 4
Percentage Detected: 1.79%

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.

5. LNK/Agent.AV

Previous Ranking: 5
Percentage Detected: 1.53%

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. LNK/Agent.BS

Previous Ranking: N/A
Percentage Detected: 1.51%

LNK/Agent.BS 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.

7. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.31%

Sality is a polymorphic file infector. When it is 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

8. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.24%

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.

9. HTML/Refresh

Previous Ranking: N/A
Percentage Detected: 1.13%

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.

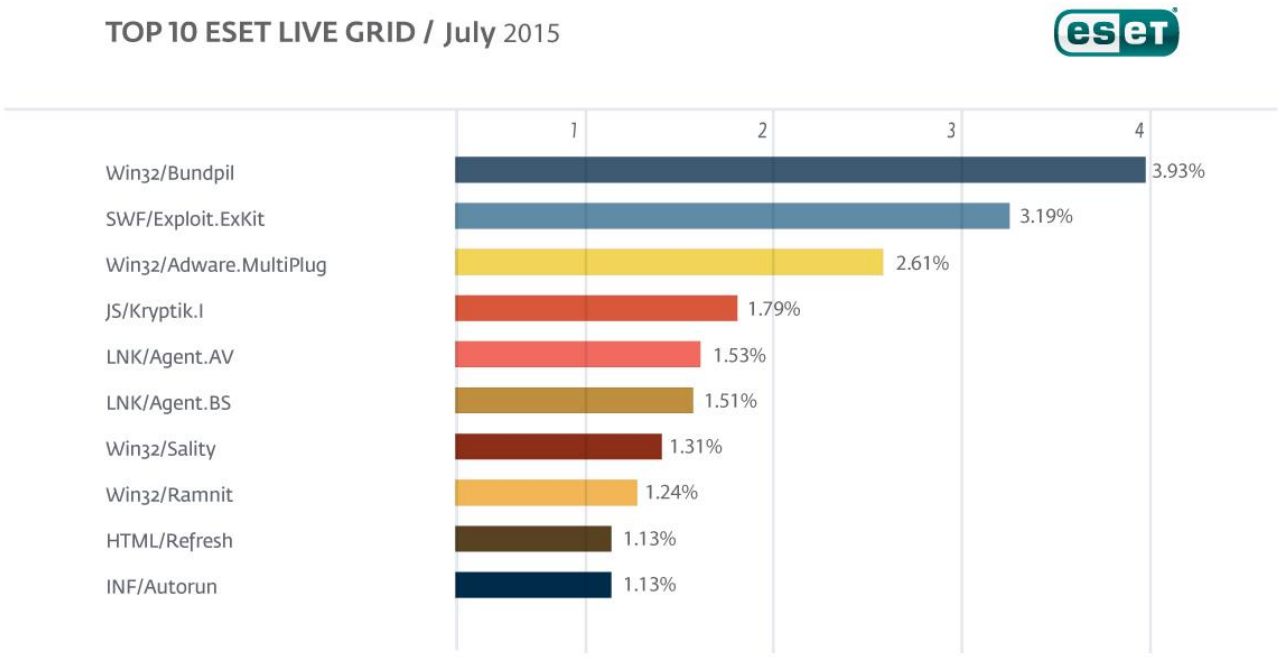
10. INF/Autorun

Previous Ranking: 9
Percentage Detected: 1.13%

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 malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malware executable when the infected drive is mounted. The 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 3.93% of the total, was scored by the Win32/Bundpil 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