December 2016:
Top 10 Worldwide Threats 2016

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Top Ten Threats at a Glance (graph) 3

The Top Ten Threats 4

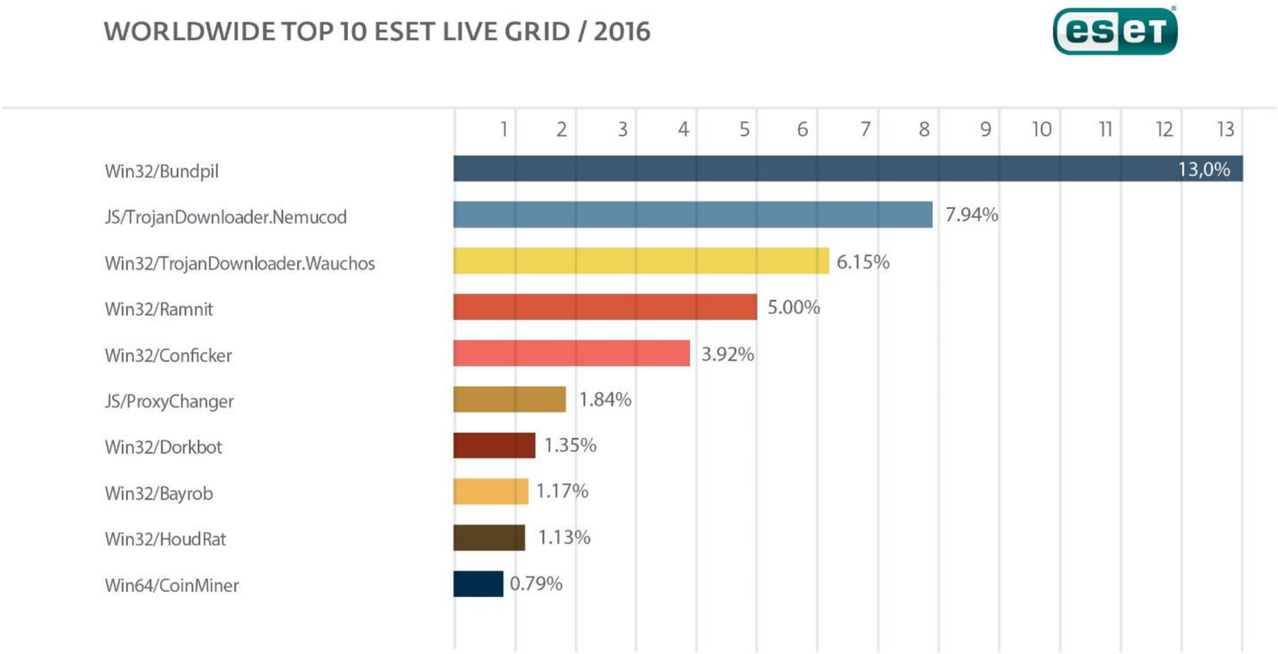
ESET Corporate News 6

About ESET 8

Additional Resources 8

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 year, with 13% of the total, was scored by Win 32/Bundpil.



The Top Ten Threats

1. Win32/Bundpil

Percentage Detected: 13%

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

2. JS/TrojanDownloader.Nemucod

Percentage Detected: 7.94%

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 associated with ransomware.

3. Win32/TrojanDownloader.Wauchos

Percentage Detected: 6.15%

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.

4. Win32/Ramnit

Percentage Detected: 5%

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 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.

5. Win32/Conficker

Percentage Detected: 3.92%

Win32/Conficker.X is a worm that repeatedly tries to connect to various web pages. It tries to download several files from the addresses. It can be controlled remotely.

6. JS/ProxyChanger

Percentage Detected: 1.84%

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

7. Win32/Dorkbot

Percentage Detected: 1.35%

Win32/Dorkbot is a worm that spreads via removable media. The worm serves as a backdoor. It can be controlled remotely.

8. Win32/Bayrob

Percentage Detected: 1.17%

Win32/Bayrob is a trojan that serves as a backdoor and can be controlled remotely. When executed, the trojan registers itself as a system service, in order to be executed at every system start. It collects the following information: operating system version, computer name and IP address, information about the operating system and system settings, MAC address, and a list of running services. The trojan can then send the information to a remote machine using HTTP.

9. Win32/HoudRat

Percentage Detected: 1.13%

Win32/HoudRat Is a worm that serves as a backdoor. It can be controlled remotely and it is written in AutoIt.

10. Win64/CoinMiner

Percentage Detected: 0.79%

Win64/CoinMiner malware family (trojan) designed to use the hardware resources of the infected computer for mining the digital currency (for example Bitcoin, Litecoin, Darkcoin or other).

Usually, within the malware body there is stored legal application used for mining the digital currency. This application is dropped by malware to victim's computer, then executed with proper command line parameters (without the knowledge of the affected user).

ESET Corporate News

2017 cybersecurity predictions from ESET security experts

ESET released its annual security forecast report written by ESET security researchers from around the globe. This year's report entitled, "Trends 2017: Security Held Ransom," predicts and explores the latest cyber threats that will take shape in the coming year.

According to ESET researchers, some of the key systems that may become increasingly targeted by cybercriminals include gaming consoles, internet connected devices (IoT), critical infrastructure and mobile devices.

Many of the insights and predictions are based on intelligence gathered by ESET's research labs across the globe. The report suggests that ransomware will continue to be prominent in 2017, and we may see an emergence of the "Ransomware of Things" (or RoT), the hijacking of internet-connected devices. Also, increasing frequency of attacks on large infrastructure and internet services puts critical infrastructure security as a top concern.

Download the entire "ESET Trends 2017: Security Held Ransom" report, and/or read its digested version on WeLiveSecurity.com.

ESET makes history with 100th Virus Bulletin Award

ESET has reached a monumental milestone in the security industry: its core product, ESET NOD32, is the first-ever security solution to receive 100 Virus Bulletin Awards (VB100). The 100th award was presented to ESET CEO Richard Marko by John Hawes, Virus Bulletin's Chief of Operations, at a ceremony on December 16th, 2016.

"We are honored to be the first to receive 100 VB100 Awards for a single product," said Marko, the ceremony. "Since the first VB100 Award in 1998, we have grown from a small, dynamic company made up of a few technologists, into an established endpoint security vendor with over 100 million users in more than 200 countries and territories."

Virus Bulletin, an independent testing organization, presented its first VB100 in 1998, and to this day it is considered to be the most coveted accolade in the industry. To earn an award, an anti-malware product must detect all current "in-the-wild" viruses without producing any false positives.

To learn more about ESET security solutions for home and business users, visit www.eset.com, or, to see the latest VB100 comparative testing, visit www.virusbulletin.com.

Patch management and compliance leader joins ESET Technology Alliance

Often overlooked as part of a comprehensive cybersecurity strategy, patch management helps secure and monitor networks, allowing companies to verify licenses and software updates and reduce risk to the network via outdated or compromised software. In order to ensure the best protection to our users, ESET has welcomed Flexera Software as the newest member of the ESET Technology Alliance.

Flexera's patch management suite, Corporate Software Inspector (CSI), will help ESET customers cover a wider range of potential security threats. In particular, CSI addresses the serious risks that come with the intensive adoption of multiple software and application types, and their need for regular updates. As a result of this newly established relationship, ESET customers now have the option to add CSI as part of their security strategy via their existing ESET reseller.

Launched in 2013, the ESET Technology Alliance is an integration partnership that aims to better protect businesses by offering a range of complementary IT security solutions. All members of the ESET Technology Alliance are carefully vetted against a set of established criteria to extend "best-in-class" business protection across IT environments.

For more details, please visit https://www.eset.com/us/business/endpoint-security/patch-management

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 the 97th award in July 2016, 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