Microsoft Security Intelligence Report Volume 23 Supplement

Malware at Microsoft

Microsoft

Table of contents

01.
Introduction

This report is a supplement to the main Security Intelligence Report Volume 23. It is focused on threats we see inside Microsoft. The information in this report comes from Microsoft Core Services Engineering (MCSE, formerly known as Microsoft Information Technology or MSIT). MCSE provides information technology services internally for Microsoft employees and resources.

The MCSE team manages more than **650,000 devices** for more than **165,000 users** across more than **150 countries** and regions worldwide. Safeguarding a computing infrastructure of this size requires implementation of strong security policies and technology to help keep malware off the network and away from mission critical resources. It also requires dealing with malware outbreaks swiftly and comprehensively when they occur.

In this report, we compared the potential impact of malware to the levels of antimalware compliance from more than **650,000 workstation** computers and devices managed by MCSE between January and December 2017.

This data is compiled from multiple sources, including Windows Defender Antivirus and Windows Defender Advanced Threat Protection (ATP), System Center Endpoint Protection (SCEP), Windows Event Forwarding (WEF), modern access, forensics, and manual submission of suspicious files.

Comparing the nature and volume of the malware detected on these computers to the level of protection they receive can illustrate significant trends and provide insights as to the effectiveness of antimalware software and security best practices.

650,000
devices and workstations

165,000
users

150
countries

02.

Malware detections

In this section, malware detections are defined as files and processes flagged by Windows Defender Antivirus and SCEP, regardless of the success or failure of automated containment or remediation. Malware detections are a measure of attempted malware activity, and do not necessarily indicate that a computer has been successfully infected.

Malicious and unwanted software detected

Trojans accounted for the largest number of detections, followed closely by Potentially Unwanted Applications (PUA). The large number of PUA detections is the result of Microsoft using the PUA-blocking features in Windows Defender Antivirus and SCEP to keep such programs out of enterprise networks.

See Detect and block Potentially Unwanted Applications at Windows IT Pro Center for more information about the enhanced PUA detection and blocking capabilities in Windows Defender Antivirus.

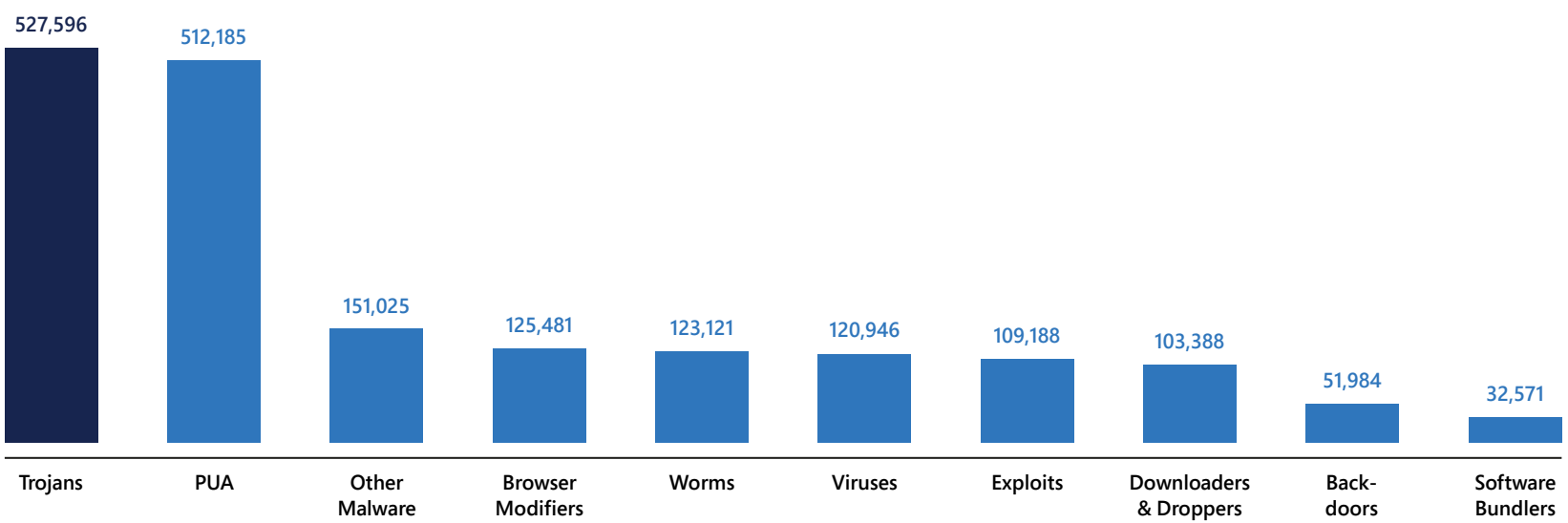

Figure 1. *Top categories of malicious and unwanted software detected by Windows Defender Antivirus and System Center Endpoint Protection at Microsoft in 2017.*

Most common file types detected

Executable program files with the .exe extension were the most commonly detected type of malicious file at Microsoft in 2017. Malicious executables can be found across multiple vectors/locations/environments (email, web browser, and so on). Malicious files with the .temp and .tmp extensions, typically used for temporary files, were the next most common type of threats, followed by files with the .dll extension.

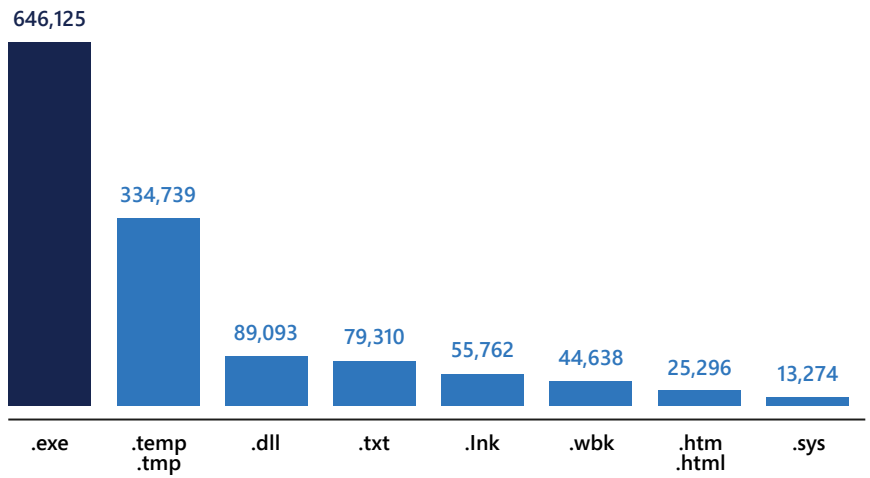

Figure 2. *Top file types used by threats detected at Microsoft in 2017.*

Rank	Process Description
01	Cloud Backup/Storage
02	Web browsing
03	File transfers in OS
04	Non-OS tasks
05	Security tools

Figure 3. *The top five transmission vectors used by malware encountered at Microsoft in 2017.*

Most common transmission vectors used by malware

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it.

The transmission vector most commonly used by infection attempts detected on Microsoft computers in 2017 involved files downloaded from cloud backup and storage services, followed by web browsing and file transfers made through File Explorer. Non-operating system tasks were fourth, followed by security tools.

03.
Malware infections

Because almost all the computers at Microsoft run real-time security software at all times, most infection attempts are detected and blocked before they can infect the target computer. When Windows Defender Antivirus or SCEP do disinfect a computer, it is usually because the software's signature database has been updated to enable it to detect a threat that it did not recognize when the computer first encountered the threat.

This lack of recognition may be because the threat is a new malware family, a new variant of a known family, a known variant that has been encrypted or otherwise repackaged to avoid detection, or because of some other reason. Windows Defender Security Intelligence (WDSI) constantly analyzes malware samples submitted to it, develops appropriate detection signatures, and deploys them to customers who use Windows Defender Antivirus, SCEP, and Microsoft Security Essentials.

Categories of malware and unwanted software infections

Detection (shown in Figure 1 on page 6) and infection (shown in Figure 4 below) statistics were significantly different in 2017. For example, Trojans, which accounted for more than 500,000 detections at Microsoft in 2017, were only removed from 28 computers internally during the year.

Meanwhile, ransomware accounted for the most detections and removals in the wake of the WannaCry attacks in May, but was only the twelfth most commonly detected category at Microsoft during the year. Most of the other categories also show clear differences between Figure 1 and Figure 4, although the ordering in the latter chart is significantly influenced by the low volumes involved.

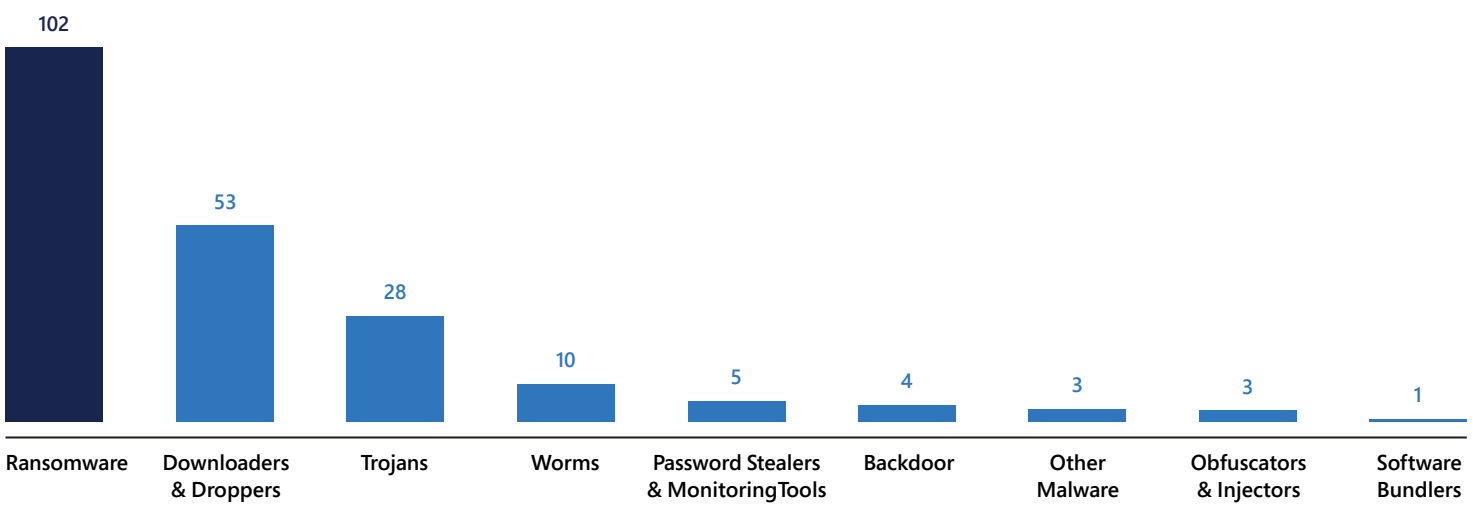

Figure 4. *Infections and removals at Microsoft in 2017, by category.*

Top file types infected by malware

Figure 5 is important because it provides information about threats that Windows Defender Antivirus and SCEP did not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. Almost half of the malicious files removed from computers at Microsoft by Windows Defender Antivirus and SCEP in 2017 had the extension .exe, which is used by executable files. Almost all the rest were code library files using the .dll extension, with small numbers of .js, .scr, .html, and .vbs files accounting for the rest.

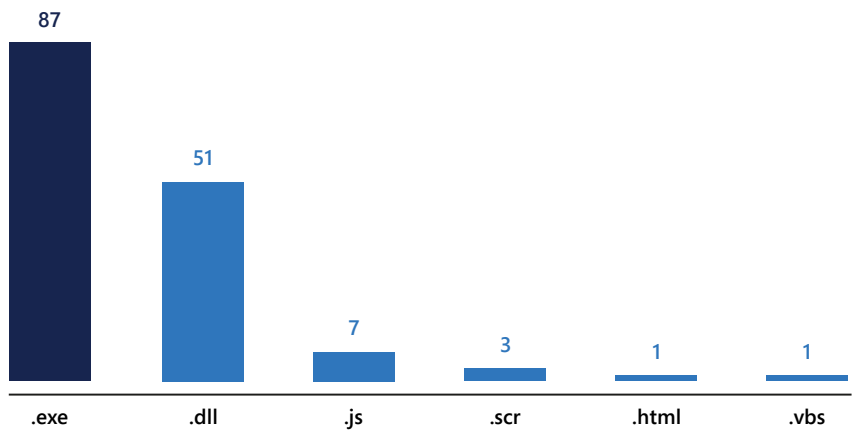

Figure 5. *Infections and removals at Microsoft in 2017, by file type.*

04.

What IT departments can do to protect their users

To help IT departments protect their users, this section has a number of recommendations from Microsoft on how to safeguard devices and workstations.

Sofware evaluation, management and updates:

- Evaluate commercially available management tools, develop a plan, and implement a third-party update mechanism to disseminate non-Microsoft updates.
- Ensure that all software deployed on computers in the environment is updated regularly. If the software provider offers an automatic update utility like Microsoft Update, ensure that it is enabled by default. See Windows Update: FAQ at support.microsoft.com for instructions on enabling automatic updates of Microsoft software.

Identity, rights management and access control:

- Implement strong password policies and require employees to change their passwords periodically.
- Strengthen authentication by using smart cards. See Smart Cards at technet.microsoft.com for more information.
- Strengthen the security of user access by implementing a multifactor authentication method. See Validate and Deploy Multifactor Authentication Services (MFA) at Windows IT Pro Center for more information.
- Create and implement access controls and rights management models.

Web protection:

- Ensure that Windows Defender SmartScreen is enabled in Microsoft Edge and Internet Explorer. See Windows Defender SmartScreen at support.microsoft.com for more information.
- Promote Microsoft Edge for browsing the web. The deep integration with Windows security features makes Microsoft Edge the most secure browser on Windows 10. With its multiple layers of security, Microsoft Edge is safer than Google Chrome and Mozilla Firefox, offering the best phishing and social engineered malware protection, as tested by NSS Labs.

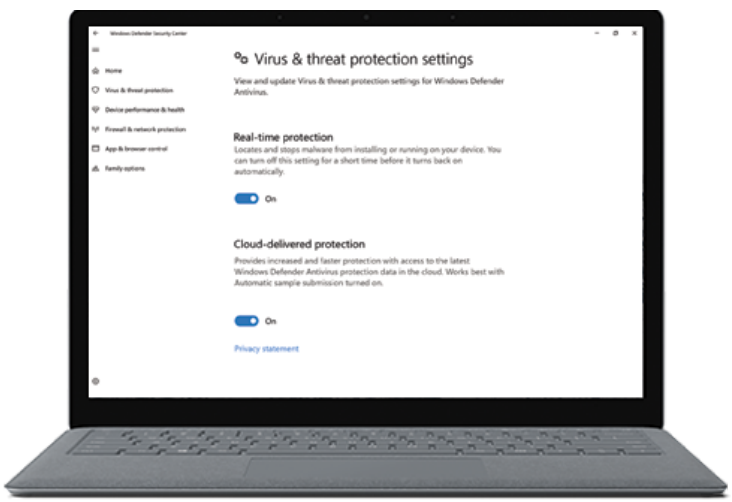

Figure 6. *Enabling cloud-delivered protection for Windows Defender Antivirus in Windows 10.*

Device/workstation policies:

- Use Group Policy to enforce configurations for Windows Update, Windows Firewall, and Windows Defender SmartScreen. See Knowledge Base article KB328010 at support.microsoft.com, and Windows Defender Firewall with Advanced Security Deployment Guide and Available Windows Defender SmartScreen Group Policy and mobile device management (MDM) settings at Windows IT Pro Center for instructions.

- As shown in Figure 6, from the Windows Defender console, in the Virus & threat protection settings, set the default configuration for antimalware to enable real-time protection across all drives, including removable devices.

- Enable the Windows Defender Antivirus cloud protection service in Windows 10 to automatically send information about suspicious files and behaviors to the Windows Defender Cloud, which can help identify and block threats during the first critical hours of an attack. For information about using Group Policy to enable cloud-delivered protection throughout your organization, see Deploy, manage, and report on Windows Defender Antivirus at Windows IT Pro Center.

- Use Windows Defender Advanced Threat Protection (ATP) to defend the network against advanced threats using endpoint behavioral sensors, cloud security analytics, and Microsoft threat intelligence. See Windows Defender Advanced Threat Protection at Windows IT Pro Center for more information.

- Use AppLocker to block the installation and use of unwanted software such as Java or peer-to-peer (P2P) applications. See AppLocker at Windows IT Pro Center for more information.

- Use Windows Defender Exploit Guard to minimize exploitation of vulnerabilities in all software in your environment. See Windows Defender Exploit Guard at Windows IT Pro Center for more information.

- Enable the following Windows PowerShell v5 security features via Windows Management Framework 5.1:

  - Script block logging.

  - System-wide transcripts.

  - Constrained PowerShell.

  - Antimalware Scan Interface (AMSI) integration in Windows 10.

For more information about how Microsoft Core Services Engineering works to ensure a trusted computing environment, see the following articles at the Microsoft IT Showcase:

- Microsoft uses Windows Defender ATP antivirus to boost malware protection
- Using Windows Defender telemetry to help mitigate malware attacks

Keep up with the evolving threat landscape by reading the main Microsoft Security Intelligence Report, Volume 23 today: www.microsoft.com/sir