

EXHIBIT 8

Evaluating Microsoft's protection performance and capabilities

How the Microsoft Malware Protection Center evaluates its ability to keep customer computers secure.

Contents

Introduction.....	4
MMPC overview.....	4
Help protect customers and systems	5
Quickly respond to malware outbreaks.....	6
Advise customers on the threat landscape and protection.....	6
Build partnerships	6
The industry challenge	6
Addressing the challenge	7
Measuring up.....	7
Measuring up: Quality	7
Incorrect detections.....	7
Remediation failures.....	9
Measuring up: Customer experience	10
Performance.....	10
Usability	11
Measuring up: Protection	11
Active malware.....	11
Summary.....	12

Authors

Dennis Batchelder

Microsoft Malware Protection Center

Tim Rains

Microsoft Trustworthy Computing

Bill Pfeifer

Microsoft Malware Protection Center

Heather Goudey

Microsoft Malware Protection Center

Jaime Wong

Microsoft Malware Protection Center

Matthew Duncan

Microsoft Malware Protection Center

Georgeo Pulikkathara

Microsoft Trustworthy Computing

Holly Stewart

Microsoft Malware Protection Center

Joe Blackbird

Microsoft Malware Protection Center

Hong Jia

Microsoft Malware Protection Center

Katrin Totcheva

Microsoft Malware Protection Center

Jonathon Green

Microsoft Malware Protection Center

Iaan Wiltshire

Microsoft Malware Protection Center

Introduction

Both the volume and the complexity of the malware threats our customers face continue to increase every day. We understand that our customers need to periodically re-evaluate their chosen protection technologies to ensure they are effective at providing appropriate protection from these threats. We also understand the challenge faced by testers in trying to keep up with the fast moving ecosystem of malware threats, since new threats are constantly emerging and test organizations may not have access to the latest global telemetry. This means our customers must evaluate both a security provider's performance and its capability to respond as necessary to malware's volume and complexity.

This whitepaper helps customers with their performance and capability evaluation. It gives an overview into how the Microsoft Malware Protection Center (MMPC) works to help protect our customers and their systems. It describes how the MMPC measures its effectiveness, and it describes how long-term investments in gathering telemetry, automated processing of malware, and cloud-based protection are helping protect customers and their systems.

MMPC overview

The guiding vision at the MMPC is to keep every customer and their systems safe from malware.

The MMPC strives to provide world-class antimalware research and response capabilities that support Microsoft's range of security products and services. With research centers in multiple locations around the globe, the MMPC is able to respond quickly and effectively to new malicious and potentially unwanted software threats wherever and whenever they arise.

The MMPC has one of the most experienced senior malware research teams in the industry, and in particular, has a unique perspective into malware research and response on the Microsoft Windows Platform.

Microsoft has made significant progress over the years in helping protect customers from malicious and potentially unwanted software threats. However, these threats to business and consumers continue to evolve, as evidenced by MMPC analysis of the threat landscape, highlighted in the *Microsoft Security Intelligence Report*¹ (SIR) which is published twice yearly.

¹www.microsoft.com/sir

The MMPC breaks down its functions into the following four areas: help protect customers and systems, quickly respond to malware outbreaks, advise customers on the threat landscape and protection, and build partnerships within the antivirus industry.

Help protect customers and systems

Microsoft antimalware products and services help to protect more than a billion computers worldwide. The MMPC team works closely with the product and services teams at Microsoft to ensure they are protected, and that they can feed back accurate and actionable telemetry and malware samples—that can be used for further research.

The scanning tool that all these technologies use—the Microsoft antimalware engine—loads definition files that contain detection signatures for thousands of different families of malware and potentially unwanted software. These detection signatures are key aspects of security updates. They are continually updated in response to new research and telemetry.

Telemetry data generated by Microsoft security products includes information about the protected system, as well as the general geographical location of the computers (not their exact location or personal information). This data enables the MMPC to compare infection rates, patterns, and trends for systems in various locations around the world.

The Microsoft antimalware engine is employed in the following products²:

- [Microsoft Security Essentials](#)³
- [Windows Defender](#)⁴
- [System Center Endpoint Protection and Microsoft Forefront](#)⁵
- [Windows Intune](#)⁶
- [Malicious Software Removal Tool](#)⁷
- [Microsoft Safety Scanner](#)⁸
- [Windows Defender Offline](#)⁹

The MMPC also drives investments in antimalware technologies for other Microsoft services and products to ensure customers are protected, including:

- Outlook.com and Hotmail.com

² <http://download.microsoft.com/download/6%2f3%2fe%2f63f1806b-3faf-445a-b446-2d374bbe2918%2fintroducing%20Microsoft%20Antimalware%20Technologies.pdf>

³ <http://windows.microsoft.com/en-gb/windows/security-essentials-download>

⁴ <http://windows.microsoft.com/en-us/windows-8/windows-defender#1TC=t1>

⁵ <http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx>

⁶ <http://www.microsoft.com/en-us/windows/windowsintune/pc-management.aspx>

⁷ <http://www.microsoft.com/security/pc-security/malware-removal.aspx>

⁸ <http://www.microsoft.com/security/scanner/default.aspx>

⁹ <http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline>

- Bing
- SkyDrive

Quickly respond to malware outbreaks

By using advanced research and heuristics, and by continuously monitoring for malicious behaviors, the MMPC provides proactive detection for new threats. But evolving malware can break through this line of defense. This is where telemetry and samples from Microsoft's services and over a billion computers help: the MMPC team can identify and mitigate new threats within hours of their discovery. Labs in Redmond (Washington, United States), Munich (Germany), and Melbourne (Australia) ensure that a response team is always available.

Advise customers on the threat landscape and protection

The MMPC uses multiple channels to distribute malware research and security information to the public:

- MMPC website, www.microsoft.com/security/portal
- MMPC Blog, <http://blogs.technet.com/mmpc>
- *Microsoft Security Intelligence Report*, www.microsoft.com/sir

Build partnerships

The MMPC engages with the antivirus industry to share malware samples, prevalence data, and suspicious behaviors. It collaborates with security researchers, partners, and independent software vendors (ISVs) worldwide. It also collaborates with Microsoft's Digital Crimes Unit who work with law enforcement organizations that seek to apprehend attackers.

The industry challenge

The volume and complexity of threats that our customers face continue to increase. For example, in December 2012, the MMPC collected and analyzed 20 million new potential malware files. Just over 100,000 files were classified as new malware requiring new detection signatures. These new signatures prevented 3 million customers from getting infected, while existing signatures protected an additional 11 million customers.

The MMPC's automated systems are able to process most samples submitted to the MMPC and automatically add signatures for new malware. But for the more established malware families, the MMPC's security researchers need to look deeper and overcome the complex techniques that the family is using to evade the MMPC's protection measures. Dorkbot¹⁰ is an example of one such family. During December 2012, the MMPC protected 729,000

¹⁰ <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32/Dorkbot>

customers from Dorkbot infections; however, if the security researchers at the MMPC hadn't performed in-depth analysis and written 361 new signatures fast enough, 70,000 of Microsoft's customers would have been infected as a result of Dorkbot's evasions.

Prioritizing and scaling out the automated and in-depth human analysis of 20 million new files each month, in order to protect as many customers as quickly as possible, is a huge challenge for the MMPC. Though this is the same challenge faced by all antimalware vendors, with Microsoft's global telemetry, Microsoft is able to have a unique insight into the emerging malware landscape and leverage that knowledge to the benefit of our customers' protection.

Addressing the challenge

In order to handle the volume and complexity challenge, the MMPC prioritizes its work based on malware prevalence. This data is collected from over a billion customer computers providing telemetry, and from hundreds of millions of customer computers that have enlisted to help Microsoft identify and gather new malware files. This gives the MMPC clear visibility into which malware is actually affecting its customers, and which files should be prioritized.

Over the long term, the MMPC continues to invest in improving its automated processing of malware to handle the more evasive malware families. It is also continuing to invest in cloud-based protection for faster delivery of its protection.

Measuring up

The MMPC strives to provide protection coupled with the highest quality and best customer experience. It measures its level of quality, experience, and protection in order to assess its own effectiveness in achieving this balance.

Measuring up: Quality

The MMPC measures quality through two metrics: incorrect detections (when the product incorrectly detects a file as malware or when that file doesn't meet the MMPC's criteria for malware detections) and remediation failures (when the product detects malware, but fails to remove it completely).

Incorrect detections

A file wrongly detected is classified as an incorrect detection. The MMPC employs rigorous processes to prevent and respond to incorrect detections.

Research and signature code review

When Microsoft researchers add detection for a file or program, they use the MMPC's criteria for malware detections and MMPC naming standards¹¹ to ensure the detection is intended and to determine the malware classification, risk level, and remediation recommendation. The researchers use specialized tools to ensure signature do not match against clean code segments from the MMPC's large repository of clean files and programs.

Post-mortems

The MMPC's researchers constantly review incorrect detections of the past, learn lessons from previous errors, and then document these case studies and build mitigations into future signature release processes.

Experimentation

If the MMPC's researchers are unsure of the accuracy of a new signature, they also have the option of releasing a heuristic, non-blocking detection that monitors detections and requests samples to confirm the signature is working as it should.

Prerelease signature quality testing

Before a new signature can be released to customers, it undergoes a series of quality tests to ensure that it only detects the malware it should detect—and not clean files. The MMPC's clean file collection is currently over 25TB in size.

Rapid response

After signatures are released, they continue to be monitored for quality. Special telemetry algorithms provide early warnings within minutes of an incorrect detection. When this happens, the case is treated with a high-priority response, and include an immediate cloud-based signature-disable notification. If the impact of the incorrect detection was widespread, the response process includes additional communications, both internal and external (on the MMPC website) to ensure that customers are aware of the issue and the update that corrects it.

Impact of incorrect detections

The following chart in Figure 1 shows how incorrect detectors have impacted customers over 2012.

¹¹ <http://www.microsoft.com/security/portal/shared/malwareNaming.aspx>

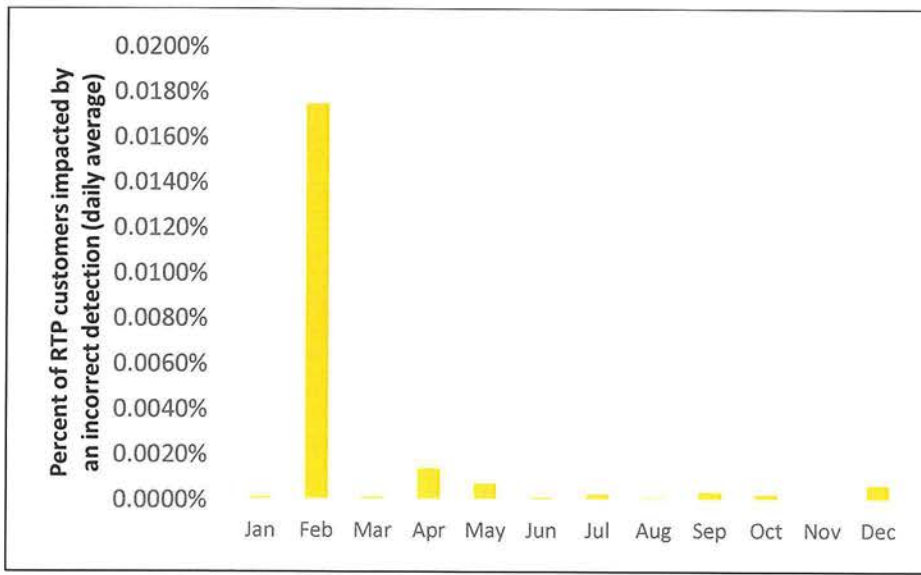


Figure 1

Remediation failures

If a threat is found infecting a customer system, remediation is used to remove it. The standard cleanup sequence is to stop and disable the malware's execution, delete related malware resources present on the disk that may cause reinfection, and undo malicious system changes made on the customer's computer. The MMPC tracks any failures to remediate.

Remediation triage process

The MMPC monitors remediation success and failure status on a weekly basis. Knowing which active malware threat is failing to be remediated over which product version helps the MMPC to reproduce the failure and design an appropriate fix in the product's engine. The MMPC monitors both Inactive Failures (threats that were not actively running on the computer, but did not have a clean removal) and Active Failures (threats that were actively running on the computer and were not successfully removed).

Impact of remediation failures

Microsoft's real-time protection products had the following remediation failures in 2012:

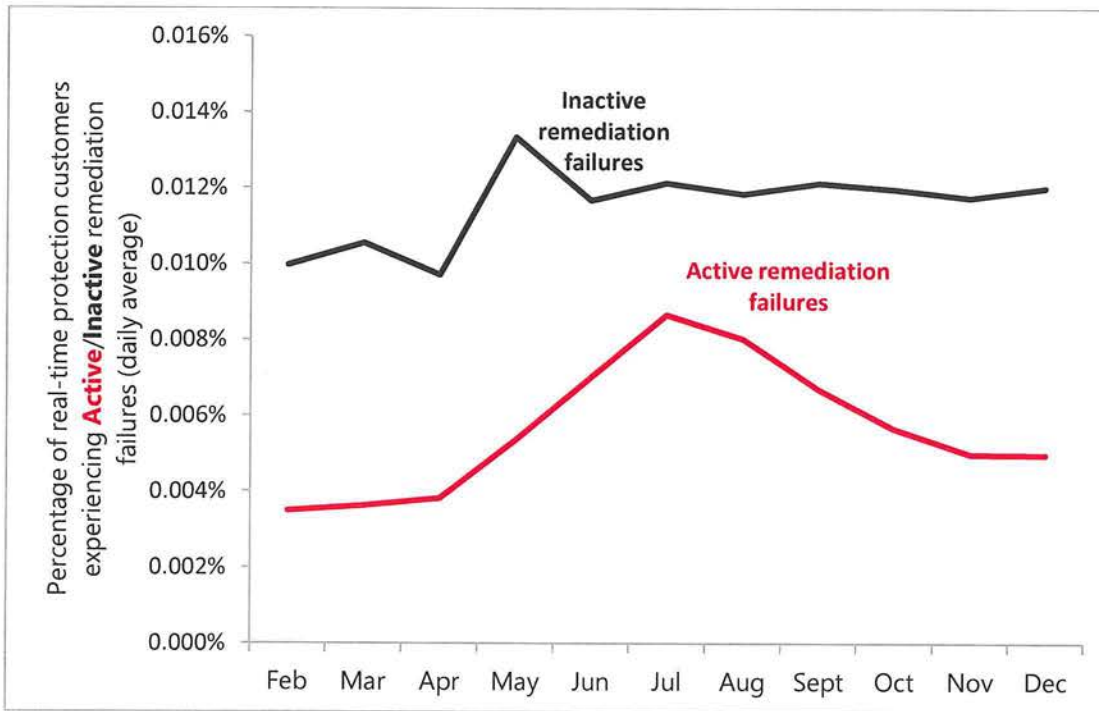


Figure 2

Measuring up: Customer experience

The MMPC measures customer experience through performance and usability. The goal is to provide quiet protection, with extra help only when the customer needs it.

Performance

The MMPC keeps system load to a minimum, and aims to eliminate all performance degradations caused by signature, engine and product updates.

All new signature update packages must pass the MMPC's signature release pipeline performance tests. Antimalware engine and product updates adhere to the same performance tests as the Windows platform.

Impact of performance

The following chart shows Windows Defender's performance impact on Windows 8:

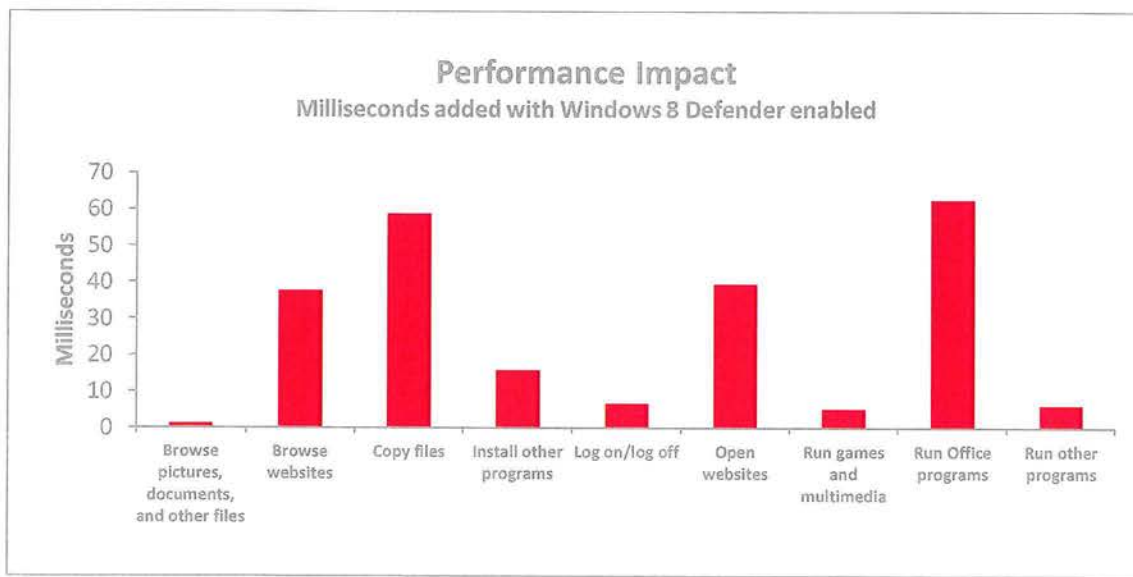


Figure 3

Usability

Because of the MMPC's philosophy to provide silent protection, most malware detections do not require a customer's attention. However, some cases do require customer action, and in these cases, Microsoft protection products will ask customers to reboot, perform offline cleaning, and reset their potentially-stolen passwords. The MMPC reviews these cases, and adds new capabilities into its protection to reduce the need for any customer involvement.

Measuring up: Protection

The MMPC measures its ability to provide adequate protection by tracking active malware infections.

Active malware

Malware threats that were able to bypass protection and infect a customer's computer are considered active.

The number of unique malware files encountered in the wild¹² increased from 60 million to 80 million per month in 2012.

To keep active infections to a minimum, the MMPC prioritizes its work by using prevalence data from its suspicious file telemetry. In addition, many members of the antimalware industry work together to share samples and telemetry, and the MMPC uses this to identify malware that wasn't reported by its own suspicious file telemetry.

¹² http://www.microsoft.com/security/portal/threat/encyclopedia/glossary.aspx#in_the_wild

Active malware impact

The following chart shows what percentage of customers reported active malware infections (daily average):

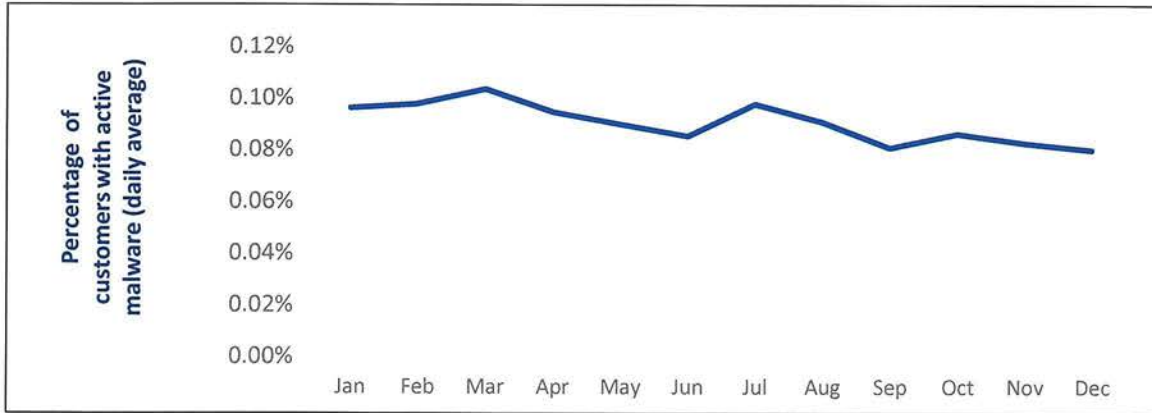


Figure 4


Summary

The MMPC is committed to providing an ideal balance of quality, experience, and protection to Microsoft's customers.

In order to adequately evaluate a protection provider, customers need to rely on more information than what external certifications and comparative tests can provide. The MMPC believes that the metrics, processes, and investments described in this paper provide a useful framework to evaluate any protection provider's performance and capability to respond to the evolving malware threat landscape.

For the most current numbers, visit the MMPC microsite [Microsoft real-time protection and performance metrics](http://www.microsoft.com/security/portal/shared/protection.aspx).¹³

¹³ <http://www.microsoft.com/security/portal/shared/protection.aspx>



Evaluating Microsoft's protection performance and capabilities - *How the Microsoft
Malware Protection Center works to keep customer computers secure*

© 2013 Microsoft Corp. All rights reserved.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Licensed under [Creative Commons Attribution-Non Commercial-Share Alike 3.0 Unported](#)