Trends in Global Cybersecurity

Top 10 insights from the Microsoft Security Intelligence Report

Microsoft

For over 10 years, Microsoft has been studying and analyzing the threat landscape of exploits, vulnerabilities, and malware. We've used data gathered from more than 600 million computers worldwide to develop one of the most complete security data sets in the world. Our year-round research is then collected and published in the Microsoft Security Intelligence Report, a globally accredited, 160-page report that comprehensively addresses the security landscape.

We've distilled thousands of hours of research and taken these comprehensive insights into an abridged format that focuses on key insights and applications and is useful for readers to learn about the most important factors in the complex matrix of cybersecurity and for security teams to prioritize their IT safeguarding efforts.

In this eBook, we've captured the top 10 latest trends in security, based on data collected through the first half of 2016. Read on to learn critical information about vulnerability rates, exploits in key software programs, locations with the highest infection rates, and much more. With more than 6,000 vulnerabilities disclosed per year across the industry, it's extremely important to ensure that all the software in your IT environment is assessed and updated. Here are our top 10 findings to help increase your security level.

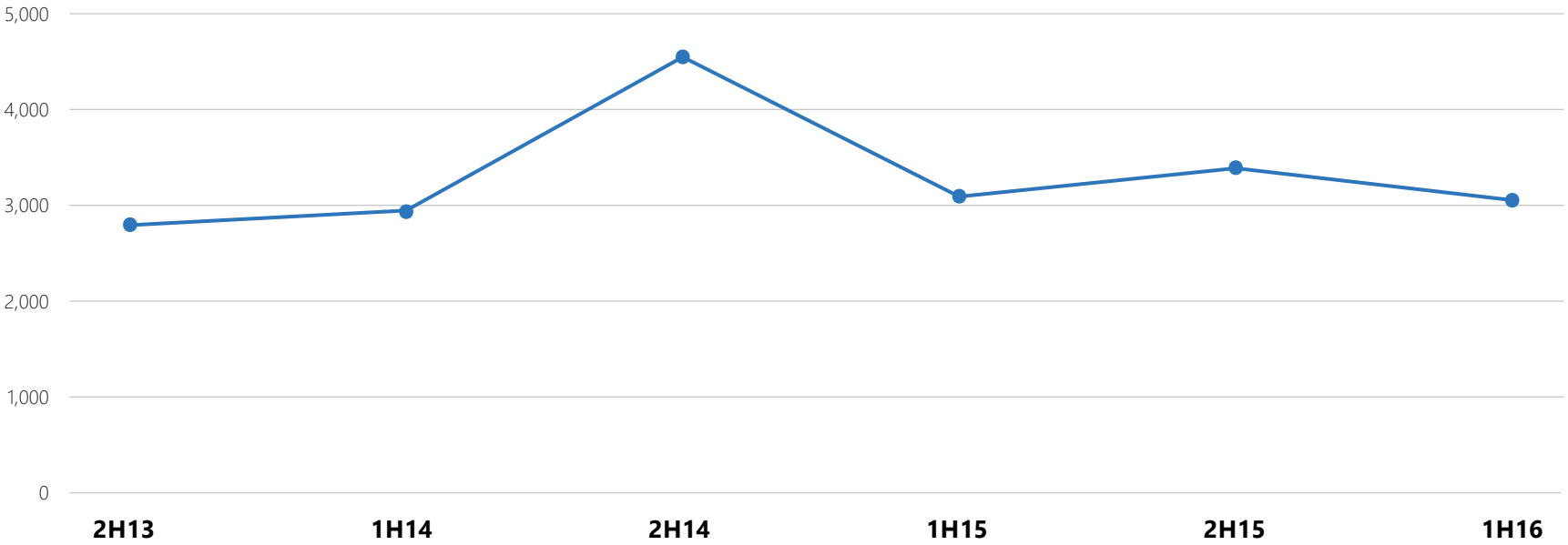
Table of contents

TREND 1

Severity of vulnerabilities

Vulnerability disclosures across the industry decreased 9.8 percent in the first half of 2016 to just over 3,000 disclosures, the lowest point in a year and a half.

Industry-wide vulnerability disclosures each half year, into the first half of 2016



WHY IT MATTERS

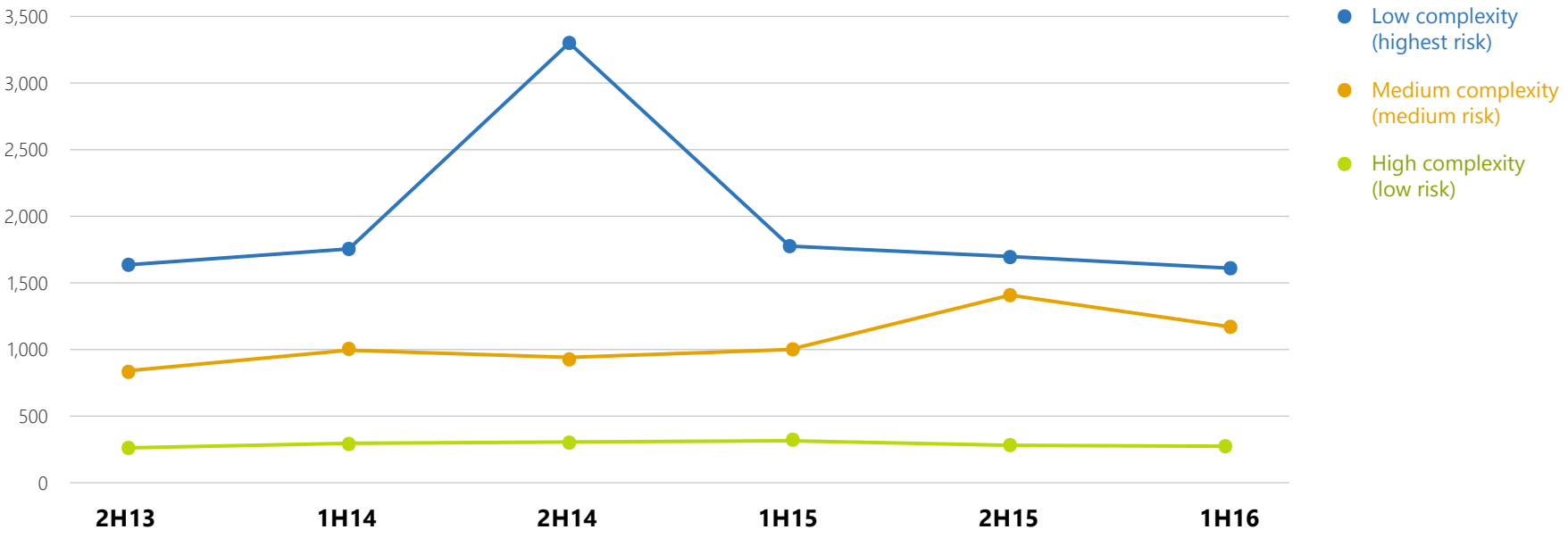
Vulnerability disclosures are revelations of software vulnerabilities to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, and even malware creators. Attackers and malware routinely attempt to use unpatched vulnerabilities to compromise and victimize organizations. While any decrease in vulnerability is a step in the right direction, publicly disclosed vulnerabilities still hover around 6,000 per year across the industry. It's extremely important that all software in your IT environment gets assessed and updated on a regular basis. Install software patches promptly, monitor networks for suspicious activity, and quarantine devices that exhibit unusual behavior.

TREND 2

Vulnerability complexity

Low-complexity vulnerability disclosures, which are at the highest risk for attack, decreased 13 percent since the last quarter of 2015, yet they still account for the most disclosures across the board.

Industry-wide vulnerability disclosures, by access complexity, 2H13–1H16

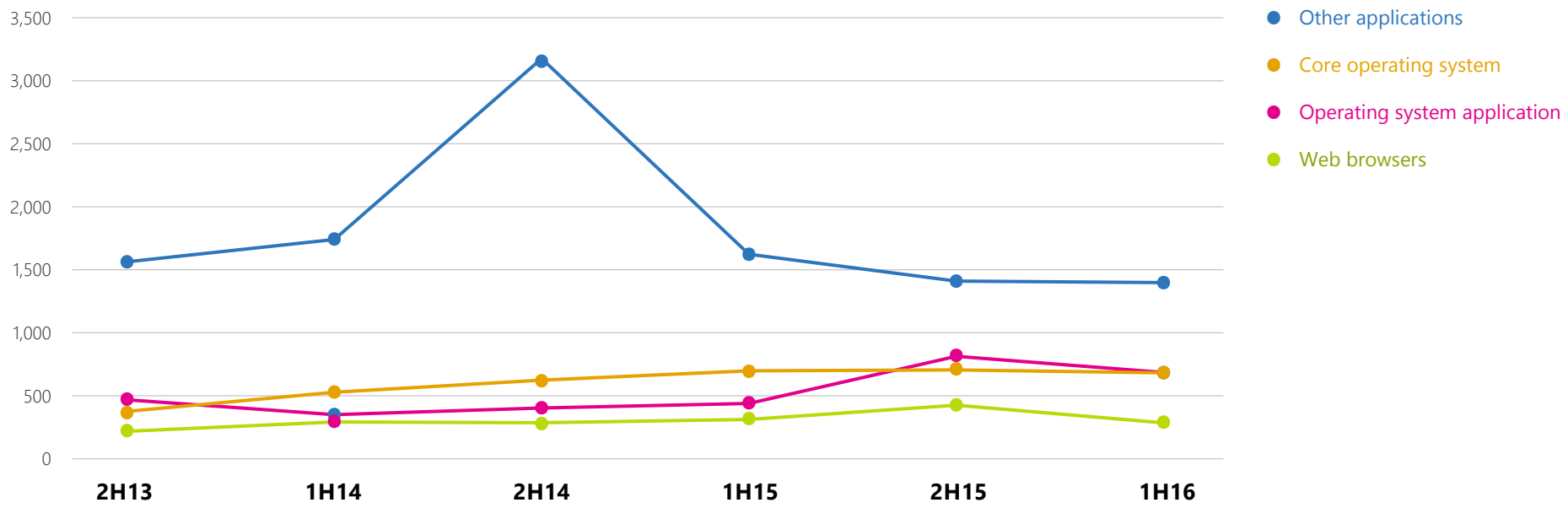


WHY IT MATTERS

Some vulnerabilities are easier to exploit than others and thus pose a higher threat. A low-complexity vulnerability represents a simpler and more readily available target to an attacker than a high-complexity vulnerability that can only be exploited under very specific and rare circumstances. Disclosures for low-complexity vulnerabilities decreased by 13 percent in the first half of 2016, reversing a multi-year growth trend. However, low- and medium-complexity vulnerabilities taken together still represent over 95 percent of all vulnerability disclosures, and they should remain a high priority for security teams.

Although a lot of security attention is given to guarding browsers and operating systems, 45.8 percent of all disclosed vulnerabilities are actually found in applications other than web browsers and operating system applications.

Industry-wide operating system, browser, and application vulnerabilities, 2H13–1H16



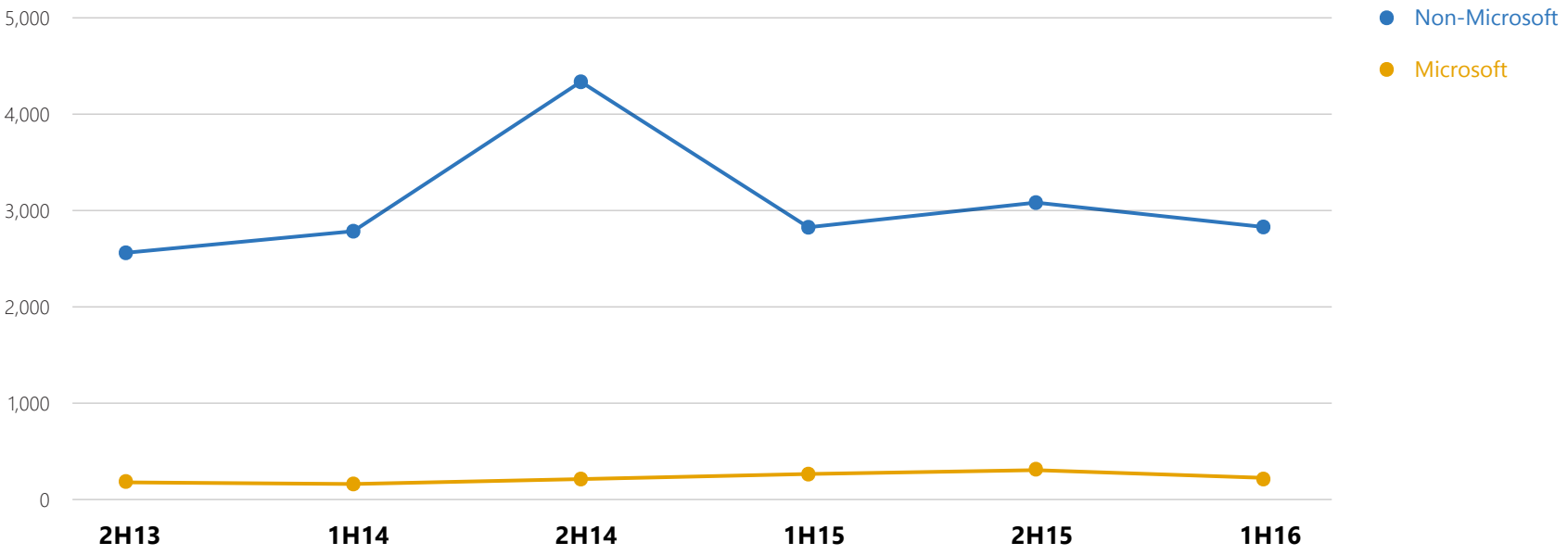
WHY IT MATTERS

Many security teams focus their efforts on patching operating systems and web browsers. But vulnerabilities in those two types of software usually account for a minority of the publicly disclosed vulnerabilities. The majority of vulnerabilities are in other applications. Other applications, although a necessity to do business and perform needed functions, are yet another attack vector for threat actors.

Security teams should spend appropriate time assessing the risks of applications already in use or ones being considered for their organization. Patching and updating existing software on a regular basis is foundational to minimizing risk to your organization.

In any six-month period, less than 10 percent of vulnerability disclosures are found in Microsoft software.

Vulnerability disclosures for Microsoft and non-Microsoft products, 2H13–1H16



WHY IT MATTERS

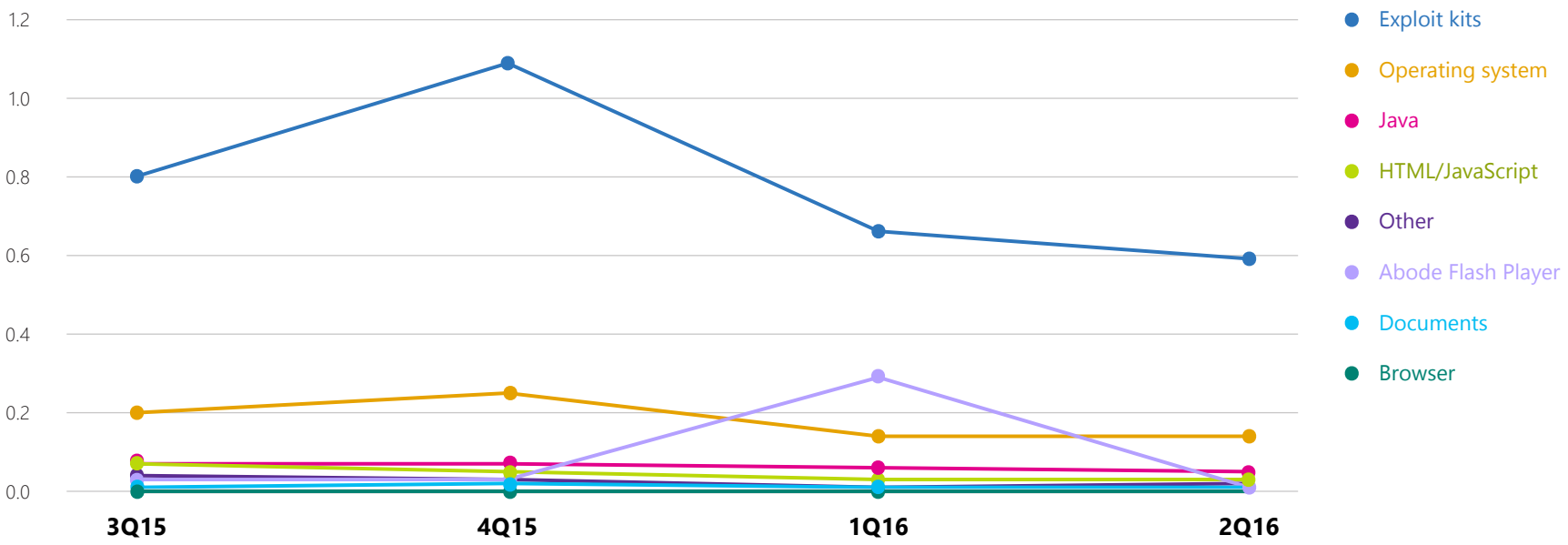
If your organization only focuses on patching vulnerabilities in your most commonly used software, you likely are not managing all the vulnerabilities present in your IT environment. It's important to know if you need to take action on any of the other nearly 3,000 vulnerabilities that could be lurking outside of widely used Microsoft applications.

Device encryption and consistent compliance with IT rules can help reduce the odds of a breach. If you detect suspicious behavior, block and quarantine the device off the network until you identify and remove the threat.

Declining Java exploits

Encounters with Java exploits have continued to decline over the last four quarters, allowing security teams to focus on higher priority risks such as exploit kits and operating system exploit encounters.

Trends for the top Java exploits, detected and blocked by Microsoft real-time antimalware products in the 2H15–1H16



WHY IT MATTERS

Attackers used to favor Java exploitation, but that is no longer the case. The continued decrease is likely the result of several important changes in the way web browsers evaluate and execute Java applets. Security teams can now prioritize their efforts on higher-priority risks. Java users should continue to install security patches as they become available, to continue guarding against potential future attacks.

TREND 6

Extent of exploit kits

Exploit kits remain the most commonly encountered exploits, at 40 percent. Notably, Axpergle exploit kits fell sharply in 2016, which some experts have linked to a major cybercrime ring breakup.

Quarterly encounter rate trends for the exploit families most commonly detected and blocked by Microsoft real-time antimalware products in 2H15 and 1H16, shaded according to relative prevalence

EXPLOIT	TYPE	3Q15	4Q15	1Q16	2Q16
JS/AXPERGLE	Exploit kit	0.71	0.92	0.53	0.40
SWF/NETIS	Adobe Flash Player	0.00	0.00	0.27	0.00
CVE-2010-25 68 (CPLLNK)	Operating system	0.18	0.24	0.13	0.13
HTML/MEADGIVE	Exploit kit	0.07	0.17	0.08	0.10
JS/NEUTRINOEK	Exploit kit	0.01	0.11	0.04	0.10
HTML/IFRAMEREF	Generic	0.04	0.05	0.03	0.02
SHELLCODE	Adobe Flash Player	0.01	0.03	0.02	0.02
SWF/DLCYPT				0.01	0.01
JS/ANGRE	Exploit kit	0.01	0.01	0.01	0.01
WIN32/PDFJSC	Documents	0.01	0.01	0.01	0.00

WHY IT MATTERS

Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets, and they can enable lower-skilled attackers to perform more sophisticated attacks. A typical kit comprises a collection of webpages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons. When the attacker installs the kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of having their computers compromised through drive-by download attacks.

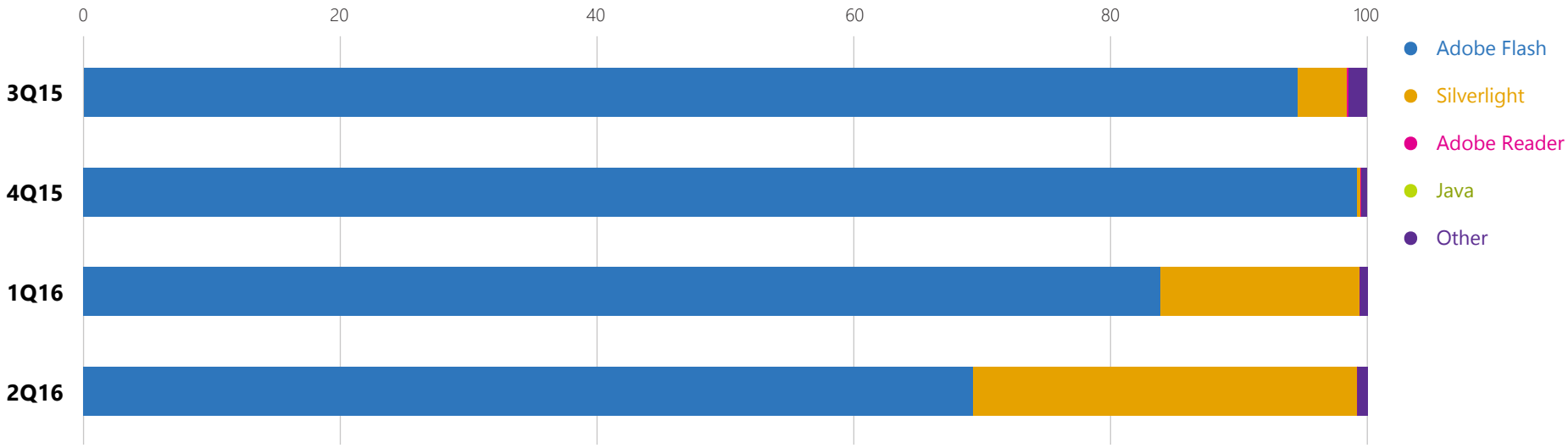
The sharp decrease in Axpergle exploit kits over the first two quarters of 2016 could potentially give rise to competing exploit kits, such as HTML/Meadgive or JS/NeutrinoEK, later in the year.

TREND 7

Most commonly detected objects

While Adobe Flash Player continues to be the most commonly detected object on malicious webpages, it has decreased over the first half of 2016, while Microsoft Silverlight has climbed to nearly 30 percent of all detections.

ActiveX control detected on malicious webpages through IExtensionValidation, 3Q15–2Q16, by control type

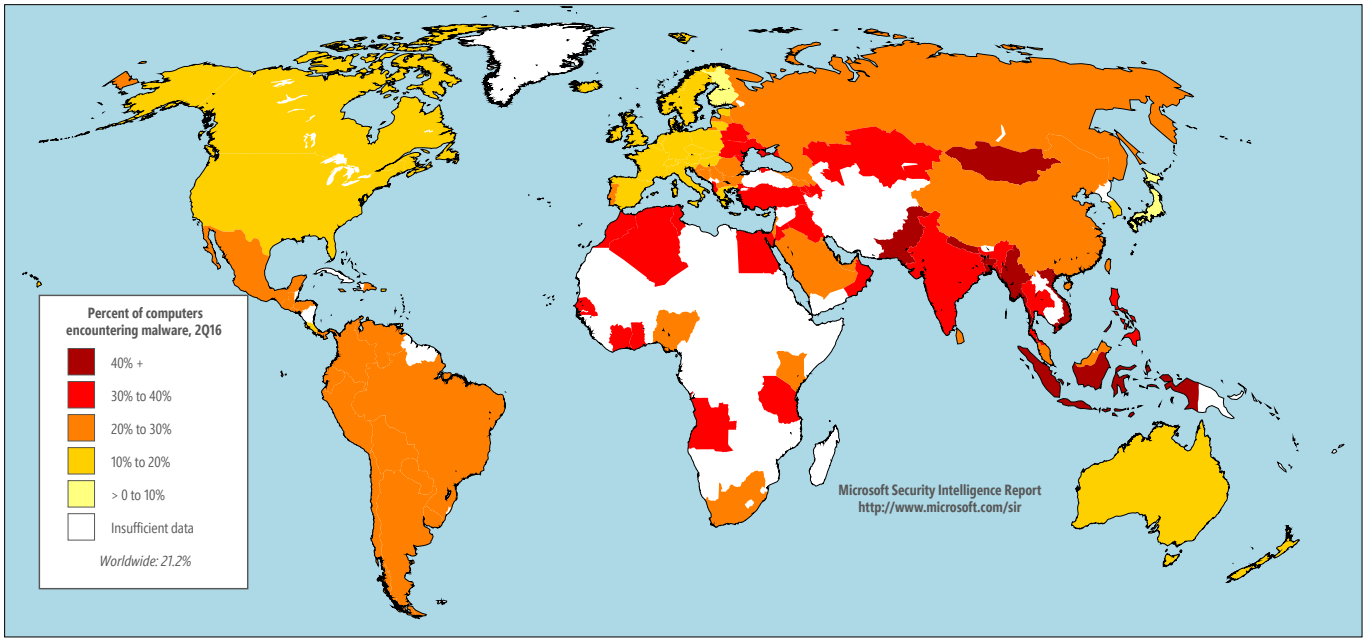


WHY IT MATTERS

This data tells security teams that attackers shifted their attacks hosted on malicious web pages from Java to Flash Player in 2015, and they are increasingly targeting Microsoft Silverlight in 2016. Knowing this makes it easier to plan mitigations for malicious webpages. It also illustrates the importance of keeping Adobe Flash Player and Silverlight updated. Users should prioritize installing security updates for these applications to help protect against this rising threat. Microsoft published Security Bulletins MS15-044 in May 2015 and MS16-006 in January 2016, respectively, to address the vulnerabilities.

The locations with the five highest malware infection rates in the first half of 2016 were: Libya, Iraq, Mongolia, the Palestinian territories, and Oman.

Infection rates, by country/region for 2Q16



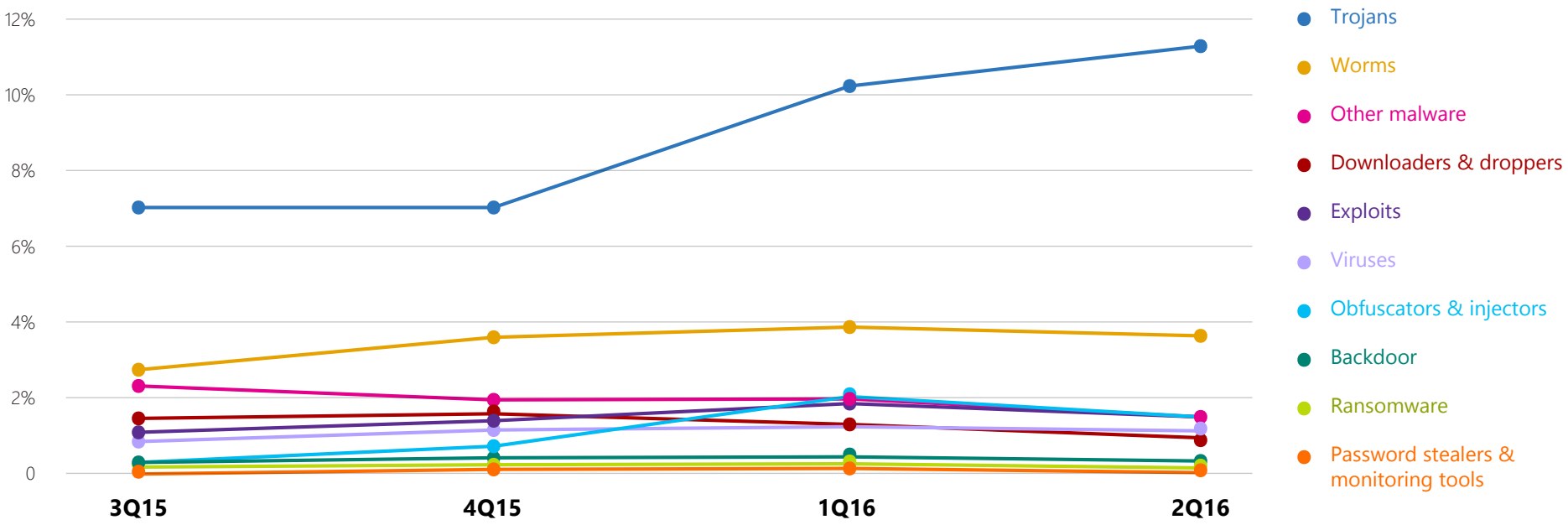
WHY IT MATTERS

Malware is unevenly distributed around the world, and each location has its own mix of threats. By studying the areas of the world that are highly impacted with malware and comparing them to the least-infected parts of the world, we can try to discover what technical, economic, social, and political factors influence regional malware infection rates. This information might help to inform future public policy that, in turn, could lead to reduced malware infection rates in highly impacted parts of the world.

Increased Trojan levels

Encounters with Trojans, a prevalent category of malware that uses social engineering to trick users, increased by 58.3 percent over the last four quarters and remained at elevated levels.

Encounter rates for significant malware categories



WHY IT MATTERS

Knowledge is power! Understanding which types of threats people in your organization are most likely to encounter helps organizations prioritize mitigations, including training people to identify such threats.

Trojans claim to be one thing, like a document or video, but are really a tool that attackers use to trick people into taking some action that isn't in their best interest, like installing malware on their systems or lowering their security settings. As evidenced by the large spike in encounters over the past three quarters, Trojans continue to be a favorite tool among attackers.

Educate your workforce about common Trojan tricks, including fake web headlines with provocative titles and spoofed emails. Encourage workers to use personal devices for social media and web surfing instead of devices connected to your corporate network.

The prevalence of any particular threat can vary dramatically, depending on the country and the nature of the threat. Although there is no absolute solution for achieving "perfect" security, knowing regional trends can help guide your security approach.

Threat category prevalence worldwide and in 10 locations with the most computers reporting encounters

CATEGORY	WORLD-WIDE	US	CHINA	BRAZIL	RUSSIA	INDIA	TURKEY	FRANCE	MEXICO	UK	GERMANY
TROJANS	11.3	5.1	13.5	21.9	19.2	26.6	31.6	6.0	16.0	4.7	5.3
BROWSER MODIFIERS	4.1	2.2	6.8	8.4	7.0	7.6	5.5	4.0	4.6	1.7	3.1
SOFTWARE BUNDLERS	3.9	1.9	0.2	6.0	12.1	8.8	5.3	3.8	3.0	2.6	4.6
WORMS	3.8	0.5	2.9	4.6	1.9	21.0	8.1	1.0	9.6	0.6	0.4
OTHER MALWARE	1.6	1.0	1.5	3.3	2.2	2.5	3.0	1.0	1.8	0.8	0.8
DOWNLOADERS & DROPPERS	1.6	1.0	1.6	5.1	1.4	2.9	1.1	1.7	2.0	1.2	0.9
EXPLOITS	1.5	1.0	0.7	0.9	0.4	1.3	1.1	1.9	0.7	2.0	1.5
VIRUSES	1.3	0.2	4.5	1.1	0.6	3.5	2.7	0.2	0.6	0.2	0.1
OBFUSCATORS & INJECTORS	1.1	0.3	1.3	1.5	2.3	3.0	2.4	0.6	1.1	0.4	0.4
ADWARE	1.0	1.0	0.0	1.0	1.3	1.1	1.0	1.7	0.9	1.4	1.5
BACKDOORS	0.4	0.2	0.6	0.8	0.4	1.1	1.0	0.3	0.3	0.2	0.2
RANSOMWARE	0.3	0.4	0.0	0.1	0.3	0.2	0.4	0.2	0.2	0.2	0.2
PASSWORD STEALERS & MONITORING TOOLS	0.2	0.1	0.2	0.2	0.2	0.3	0.3	0.1	0.2	0.1	0.1

WHY IT MATTERS

Understanding the strategies and tactics that attackers are using in parts of the world where you have operations will allow you to better protect those operations. For example, Turkey has a 31.6 percent encounter rate for Trojans but only a 1.1 percent encounter rate for downloaders & droppers; Russia has one of the highest prevalence rates for worms but is low on exploits. Use the data in the Security Intelligence Report to understand the threats your organization is most likely going to encounter and to inform your security plan.

To learn more about these and other findings, download the Security Intelligence Report at **www.microsoft.com/sir** or visit **www.microsoft.com/security**.

Microsoft