

# 2016 Trends in Cybersecurity:

A Quick Guide to  
the Most Important  
Insights in Security



For 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.

This year, in an effort to drive awareness of key insights and trends, we've also developed A Quick Guide to the Most Important Insights in Security, an abridged, to-the-point resource that readers can use to learn the important factors in the complex matrix of Cybersecurity.

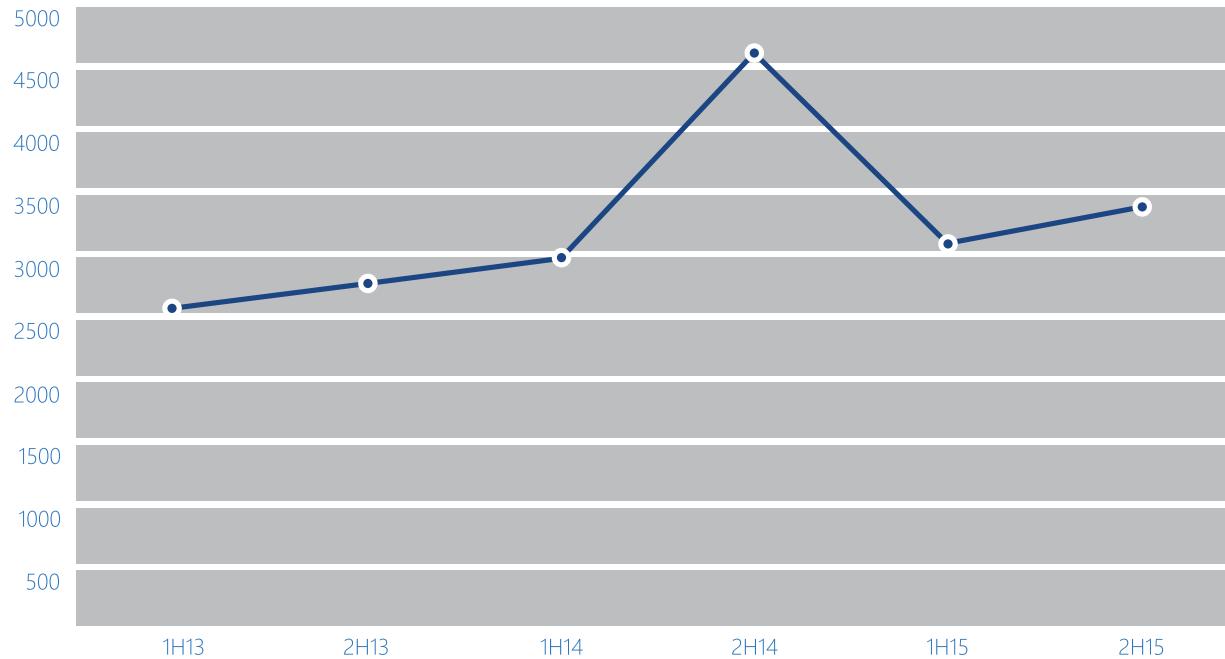
In this eBook, we've captured our Top 10 key findings. Read on to learn critical information about vulnerability rates, exploits in key software programs, the locations with the highest infection rates, and much more. With more than 6,000 vulnerabilities disclosed per year across the industry, it's extremely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

# The Trends

- 4** Severity of Vulnerabilities
- 6** Declining Java Exploits
- 8** Stronger Enterprise Protection
- 10** Global Security Concerns
- 12** Extent of Exploits Kit
- 14** Most Commonly Detected Objects
- 16** New Application Vulnerabilities
- 18** Increased Trojan Levels
- 20** Continued Complexity of Threats
- 22** Platform Agnostic Vulnerabilities

41.8 percent of all  
vulnerability disclosures  
are rated as highly severe  
—a three-year high.

Industry-wide vulnerability disclosures each half year into the second half of 2015



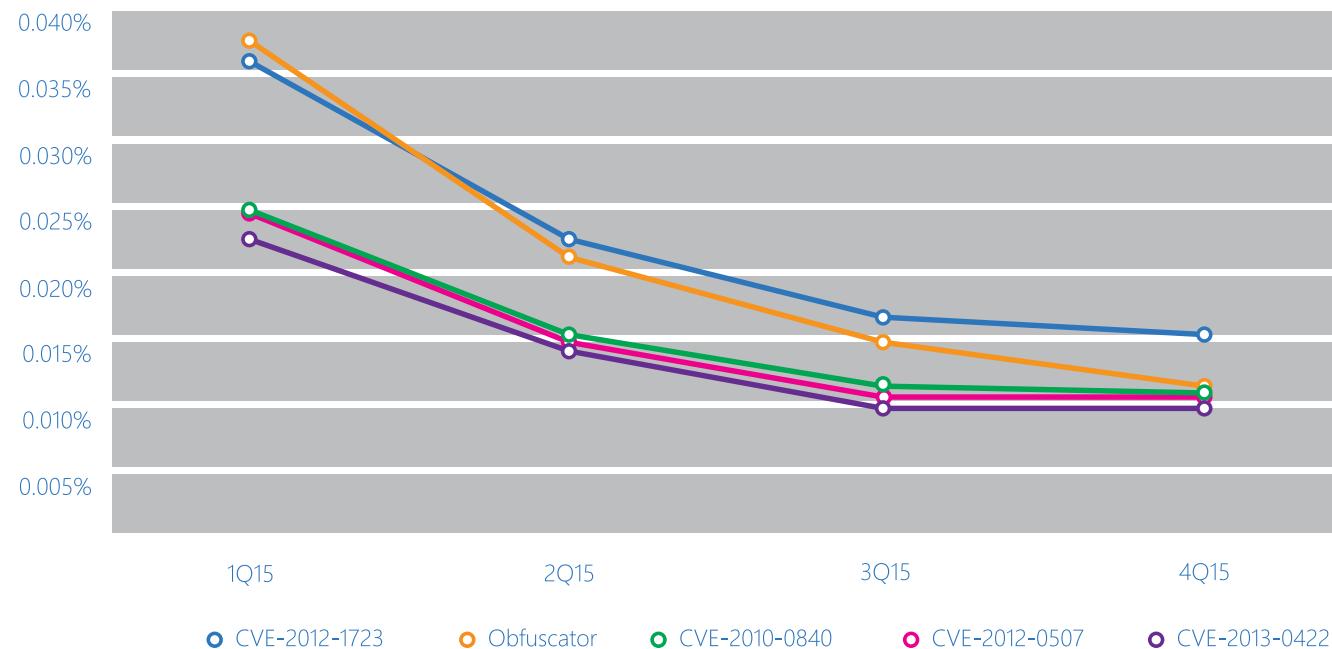
## Why it matters

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. Vulnerability disclosures across the industry increased 9.4 percent between the first and

second halves of 2015, to just above 3,300. These are the high-severity vulnerabilities that security teams dread as they might enable remote attackers. With more than 6,000 vulnerabilities publicly disclosed 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.

# Encounters with Java exploits are on the decline.

Trends for the top Java exploits detected and blocked by Microsoft real-time antimalware products in the second half of 2015



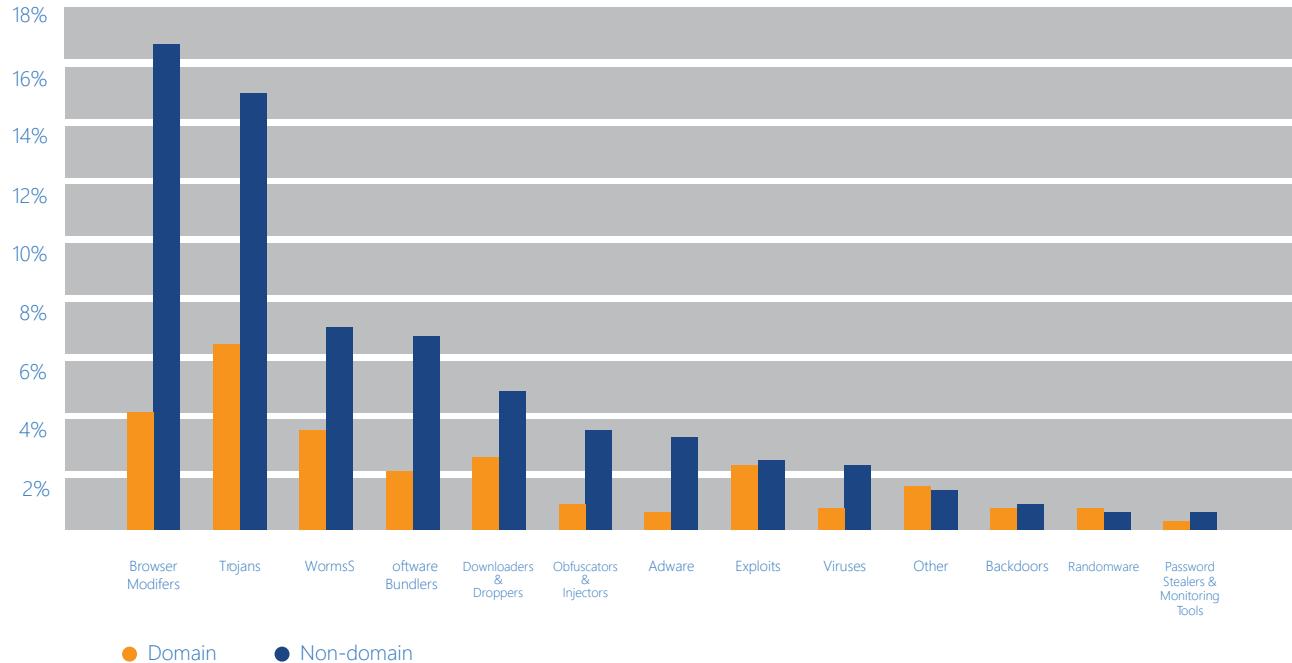
## Why it matters

Attackers used to favor Java exploitation, but that is no longer the case. This decrease is likely the result of several important changes in the way web browsers evaluate and execute Java applets. Security teams can prioritize

their efforts now on higher priority risks. Java users should continue to install security patches as they become available to continue guarding against potential future attacks.

Consumer computers encounter 2X the number of threats as compared to enterprise computers.

Malware and unwanted software encounter rates for domain-based and non-domain computers.



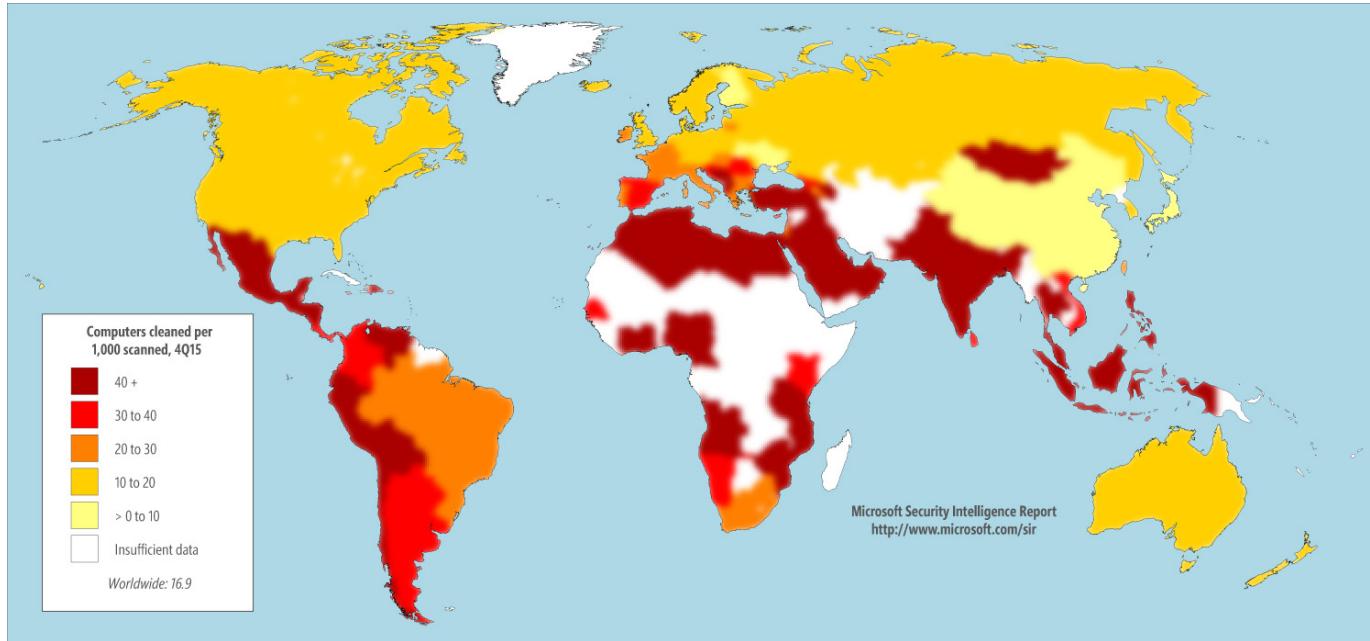
## Why it matters

Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls, that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers. The encounter rate for consumer computers was about 2.2 times as high as the rate for enterprise computers. Meanwhile, enterprise (domain-based) computers encountered exploits nearly as often as consumers' computers (non-domain), despite encountering less than half as much malware as non-domain computers overall. This tells CISOs that exploits are

an issue for organizations and staying up-to-date with security updates and the latest software is their best defense. Despite these trends, you can secure your company's assets by understanding the threat landscape and devising a security strategy across all fronts, including: identity and access credentials, apps and data, network devices and infrastructure. By adopting a proactive security stance and taking advantage of the latest in multi-factor authentication, machine learning and analytics technologies, you can harden your company's defenses against cyberattacks, and be equipped to respond in the event of a breach.

Locations with the highest malware infection rates were Mongolia, Libya, the Palestinian territories, Iraq, and Pakistan.

## Infection rates by country/region



# 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 re-

gional 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.

[A previous study is also available](#)

Exploit kits account for 40 percent of the most commonly encountered exploits.

Quarterly encounter rate trends for the exploit families most commonly detected and blocked by Microsoft real-time antimalware products in the second half of 2015, shaded according to relative prevalence

Exploit	Type	1Q15	2Q15	3Q15	4Q15
Axpergle	Exploit kit	0.86%	0.66%	0.71%	0.92%
CVE-2010-2568 (cpILnk)	Operating system	0.30%	0.23%	0.18%	0.24%
HTML/Meadgive	Exploit kit	0.06%	0.05%	0.07%	0.17%
JS/NeutrinoEK	Exploit kit	0.06%	0.03%	0.01%	0.11%
HTML/IframeRef	Generic	0.07%	0.05%	0.04%	0.05%
JS/Neclu	Exploit kit	0.03%	0.15%	0.05%	0.01%
ShellCode	Other	0.01%	0.02%	0.01%	0.03%
Win32/Sdbby	Other	0.00%	0.09%	0.02%	0.01%
CVE-2012-1723	Java	0.04%	0.02%	0.02%	0.02%
Java/Obfuscator	Java	0.04%	0.05%	0.02%	0.01%

# Why it matters

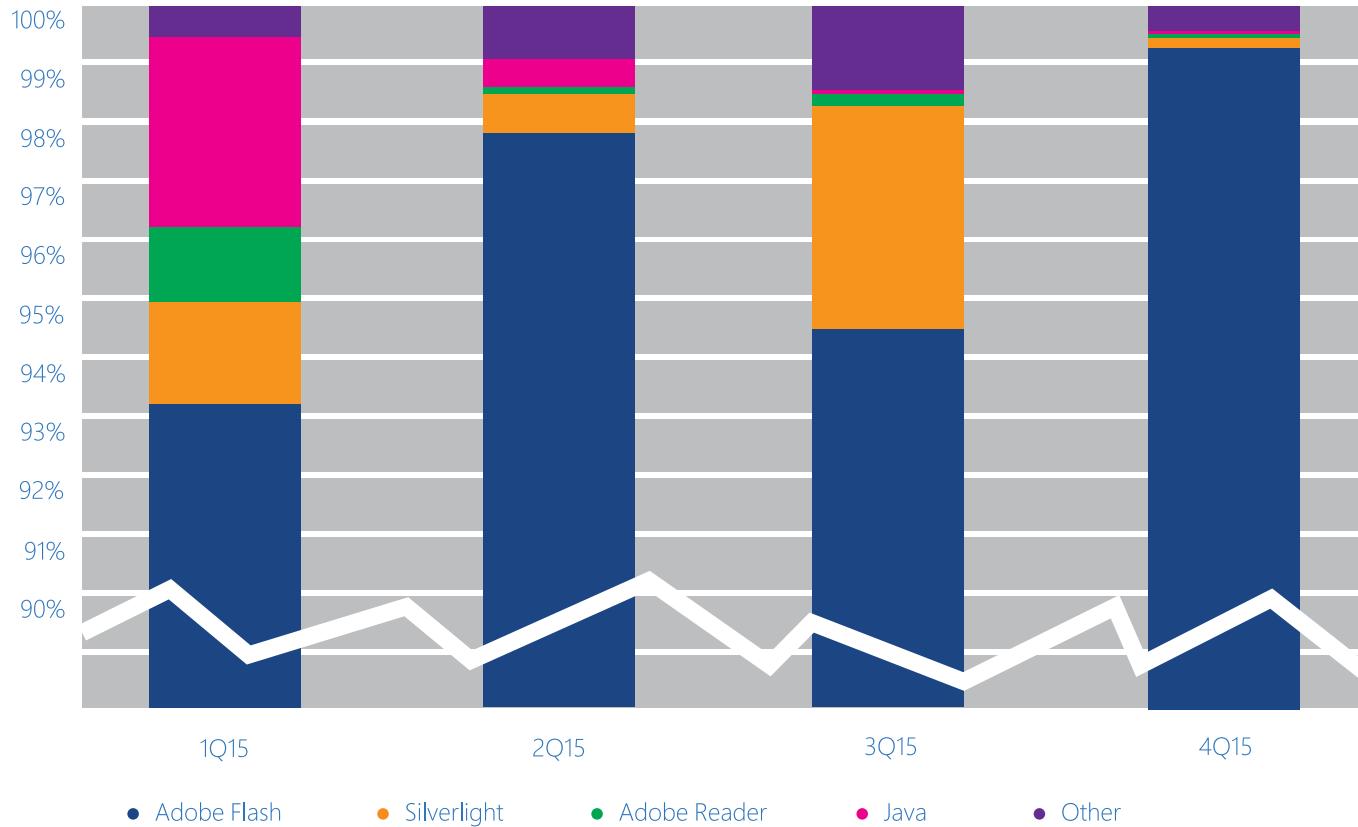
Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit comprises a collection of webpages that contain exploits for several 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. Exploit kits enable lower skilled attackers to perform more sophisticated attacks.

Understanding which exploits and exploit kits are being used by attackers helps security teams protect their organizations.

Adobe Flash Player objects were the most commonly detected type of object, appearing on more than 90 percent of malicious pages over a one-year period.

ActiveX controls detected on malicious webpages through IExtensionValidation in 2015, by control type



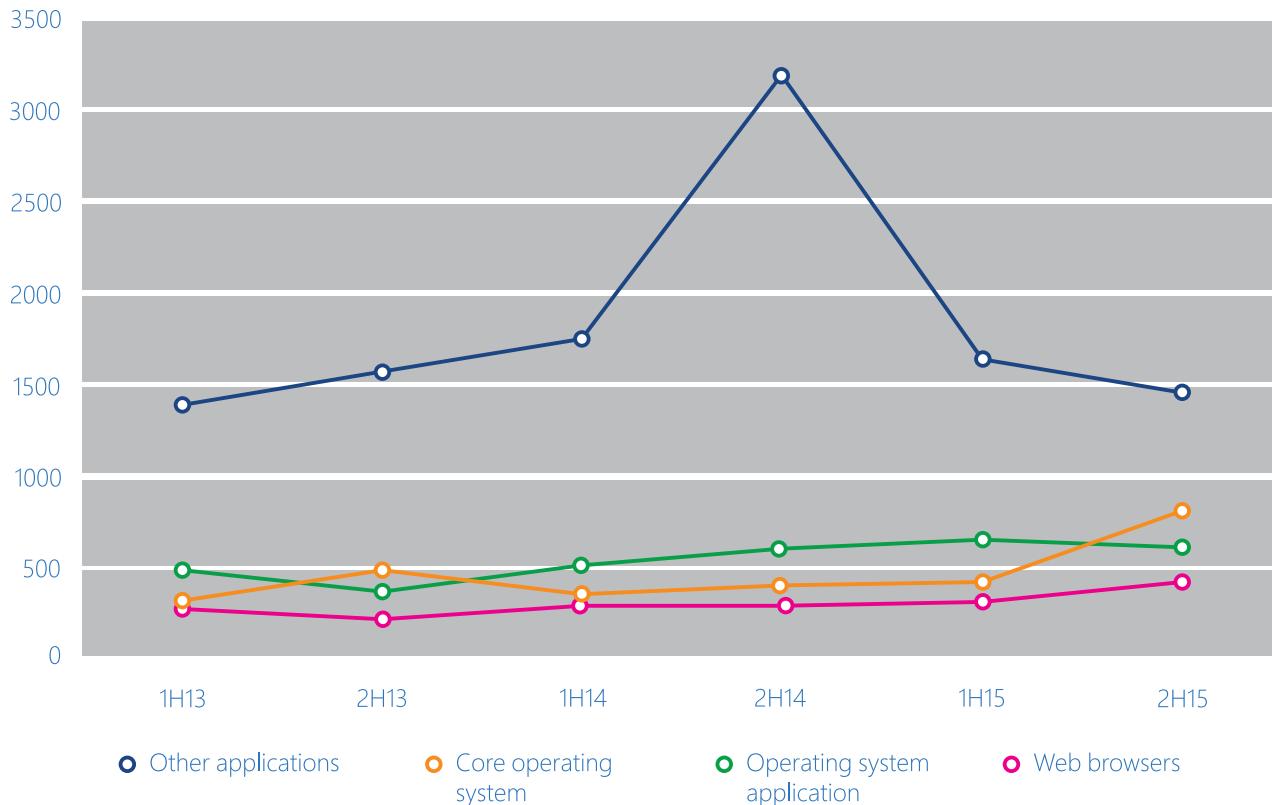
## Why it matters

This data tells security teams that attackers have shifted their attacks hosted on malicious web pages from Java to Flash Player. Knowing this makes it easier to plan mitigations for malicious

webpages. It also illustrates the importance of keeping Adobe Flash Player updated. Users should prioritize installing Flash security updates to help protect against this rising threat.

44.2 percent of all disclosed vulnerabilities are found in applications other than web browsers and operating system applications.

## Industrywide operating system, browser, and application vulnerabilities, 1H13–2H15



# Why it matters

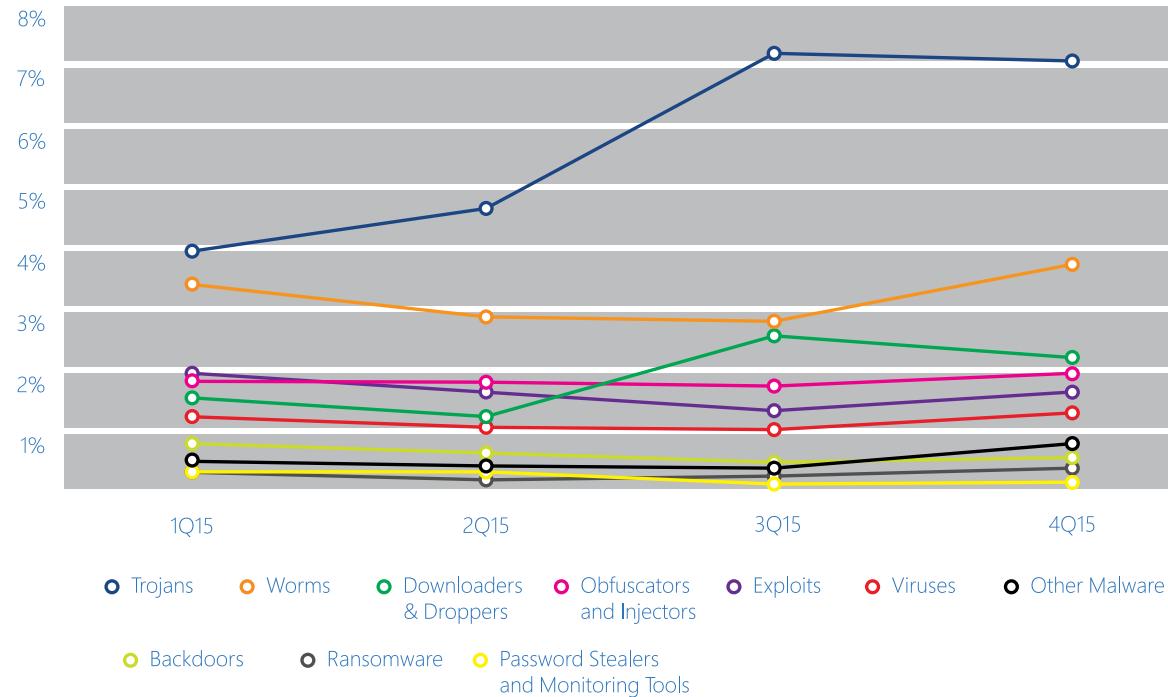
Many security teams focus their efforts on patching operating systems and web browsers. But vulnerabilities in those two types of software usually account for a minority of the publicly disclosed vulnerabilities. The majority of vulnerabilities are in applications. Security teams need to spend appropriate time on assessing and patching these vul-

nerabilities. Otherwise, they could be missing the bulk of vulnerabilities in their environments.

To increase protection on the network, identify unsanctioned apps and enforce your corporate policies regarding cloud resources, and monitor activity for anything unusual.

Encounters with Trojans, a prevalent category of malware that uses social engineering to trick users, increased by 57 percent, 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 system or lowering their security settings. This makes Trojans one of attackers' favorite

tools. Knowing this, and looking at how the top Trojans in your area of the world behave, will help you protect your organization better. 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, which is one of the reasons why there's no silver bullet for achieving "perfect" security. For example, Russia and Brazil had nearly triple the worldwide average encounter rates for some types of threats.

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

Category	Worldwide	USA	Brazil	China	Russia	France	Germany	UK	Italy	Canada	Japan
Browser Modifiers	7.6%	9.1%	11.8%	0.6%	7.0%	14.3%	8.7%	10.9%	15.3%	11.3%	4.2%
Trojans	7.1%	4.2%	12.7%	10.2%	20.8%	5.7%	4.3%	4.4%	7.0%	5.1%	1.5%
Worms	3.3%	0.6%	8.9%	5.6%	4.6%	1.9%	1.1%	0.8%	3.9%	0.6%	0.7%
Software Bundlers	3.1%	1.7%	1.5%	0.2%	0.5%	2.2%	0.9%	2.3%	2.5%	2.5%	0.5%
Downloaders & Droppers	2.2%	2.3%	6.5%	3.2%	6.6%	2.8%	1.5%	3.2%	3.1%	3.3%	0.4%
Obfuscators & Injectors	1.7%	1.0%	5.3%	5.2%	7.3%	1.9%	1.6%	1.7%	2.8%	1.6%	0.6%
Adware	1.6%	4.5%	7.1%	0.2%	5.2%	7.8%	4.1%	4.7%	7.2%	5.3%	2.0%
Exploits	1.4%	3.4%	2.4%	1.7%	1.3%	2.5%	3.2%	4.4%	4.3%	5.7%	3.2%
Viruses	1.1%	0.4%	2.2%	7.4%	1.5%	0.4%	0.3%	0.3%	0.8%	0.4%	0.2%
Other	0.6%	0.9%	0.3%	1.2%	0.3%	0.5%	0.5%	0.6%	0.7%	1.5%	0.2%
Backdoors	0.5%	0.7%	1.4%	1.8%	2.0%	0.9%	0.6%	0.9%	1.0%	0.7%	0.3%
Ransomware	0.3%	0.6%	0.5%	0.0%	0.6%	0.7%	0.6%	0.4%	1.4%	0.7%	0.4%
Password Stealers & Monitoring Tools	0.2%	0.4%	1.0%	0.5%	0.8%	0.3%	0.4%	0.4%	0.6%	0.6%	0.3%

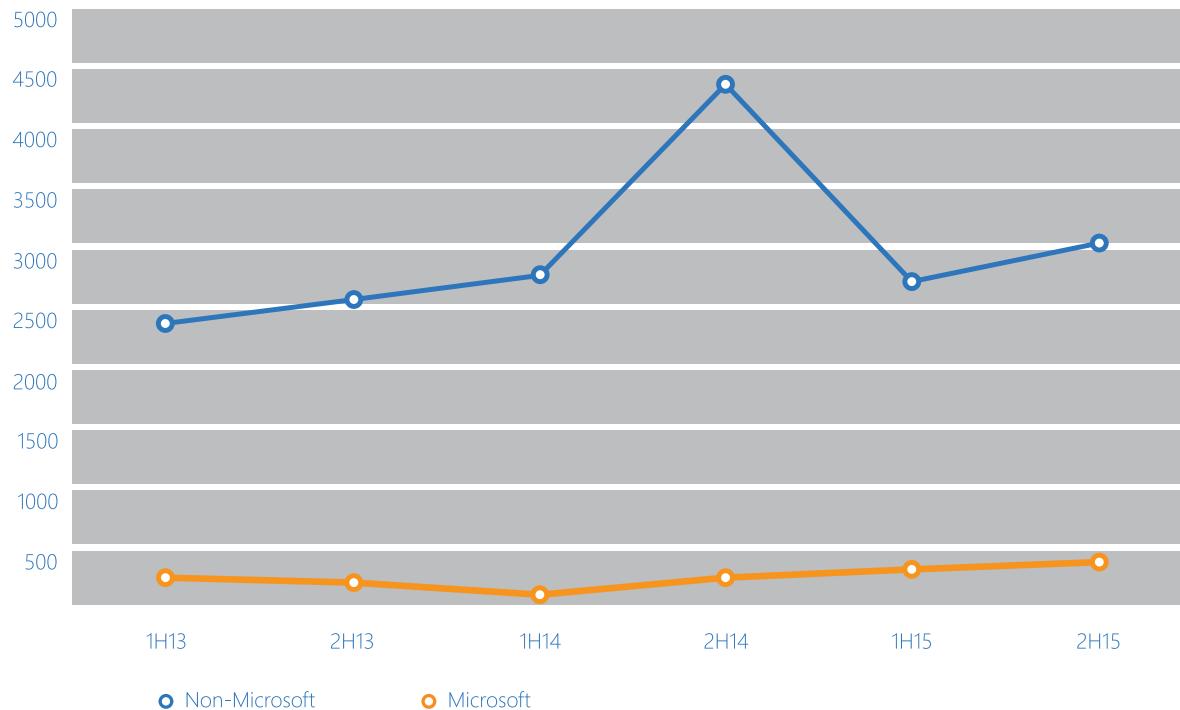
## Why it matters

Understanding what strategies and tactics attackers are using in parts of the world where you have operations will allow you to better protect those operations. There are parts of the world where ransomware is encountered far more than other locations;

similarly, with Trojans, and exploits, and other malware. 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.

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, 1H13–2H15



# Why it matters

If your organization only focuses on patching vulnerabilities in your most commonly used software, you are likely 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 in your organization's environment.

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 the threat is identified and removed.

To learn more about these and other findings, download the [Security Intelligence Report](#), or visit:  
[www.microsoft.com/security](http://www.microsoft.com/security)

© 2016 Microsoft Corporation. All rights reserved. This document is for informational purposes only. Microsoft makes no warranties, express or implied, with respect to the information presented here.

