

Report

Black Hat 2015: State of Security

Endpoint Risk Overshadows All Others

Table of Contents

Summary	3
Beginning With the Endpoint, the Greatest Security Risk	3
A Flash in the Pan? Security Professionals Pan Flash	4
Critical Infrastructure at Risk—All Eyes on Financial Services	7
Mixed Reaction to Windows 10—Slow Adoption in First Year	8
Conclusion	10
Methodology	10
About Bromium	11

Summary

Every year, thousands of the brightest and most determined information security professionals meet at the Black Hat Conference to discuss the latest and greatest security research. Bromium® surveyed many of these security professionals about their opinions on a variety of security trends, including the recent launch of Windows 10, the risk of cyber attacks on critical infrastructure and the source of the greatest security risk: the endpoint.

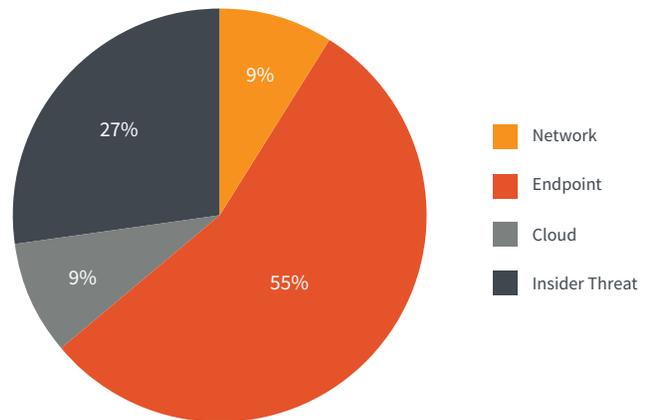
The majority of information security professionals cited the endpoint as the source of the greatest security risk. In this report, we will explore some of the trends that contribute to this risk, including issues with Flash and patching zero-day vulnerabilities.

Beginning With the Endpoint, the Greatest Security Risk

Bromium asked more than 100 information security professionals attending Black Hat to identify the source of the greatest security risk. Fifty-five percent selected the endpoint and 27 percent selected insider threats, displaying a cynical (yet pragmatic) view that end users introduce the most security risk. By contrast, only 9 percent selected the network and only 9 percent selected the cloud meaning there is five times more risk on the endpoint than on the network or the cloud, underscoring the need to prioritize endpoint solutions.

Humans are just one element that makes the endpoint the source of the greatest security risk. Another major factor is vulnerable software, a trend Bromium continued to explore in this research.

WHAT IS THE SOURCE OF THE GREATEST SECURITY RISK?
(PERCENT OF RESPONSES)

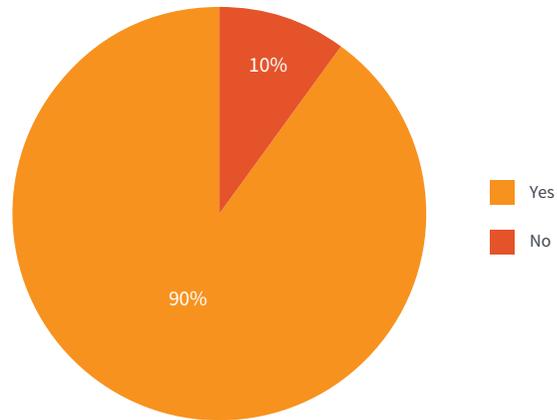


A Flash in the Pan? Security Professionals Pan Flash

Ninety percent of information security professionals believe their organization would be more secure if it disabled Flash. Recently, Bromium Labs published “Endpoint Exploitation Trends 1H 2015,” which found Flash was responsible for more exploits than any other popular software in the first six months of 2015. Flash vulnerabilities have become so problematic that Mozilla temporarily blocked Flash from Firefox, YouTube has switched to HTML5 and Facebook has called for the end of Flash.

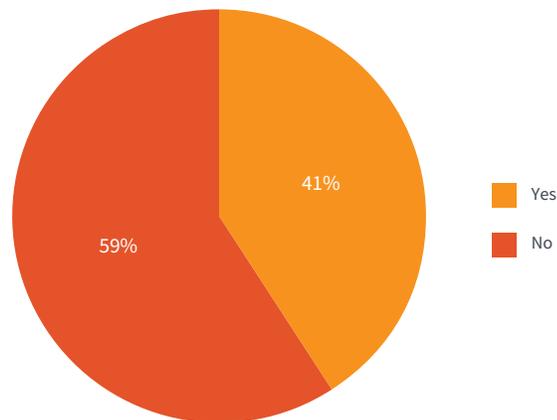
The reason that so many Flash exploits exist is because Flash is so popular (it was only a few years ago that Java exploits were so common for the same reason). The problem for information security teams is that they are often at odds with operations teams.

WOULD YOUR ORGANIZATION BE MORE SECURE IF IT DISABLED FLASH?
(PERCENT OF RESPONSES)



Information security professionals are challenged because disabling Flash is not always an option. Forty-one percent of organizations would become less productive or “break” critical applications if they disabled Flash. Ironically, one Black Hat attendee relayed an anecdote that the only application in his organization that required Flash was its security awareness training videos.

WOULD YOUR ORGANIZATION BECOME LESS PRODUCTIVE OR “BREAK”
CRITICAL APPLICATIONS IF IT DISABLED FLASH? (PERCENT OF RESPONSES)



The struggle to disable Flash is a frequent dilemma for information security professionals that must find alternatives to address zero-day vulnerabilities. One best practice is to urgently implement patches, but even that can be a challenge.

HOW QUICKLY DOES YOUR ORGANIZATION IMPLEMENT PATCHES FOR ZERO-DAY VULNERABILITIES? (PERCENT OF RESPONSES)



The majority of information security professionals implement patches for zero-day vulnerabilities in applications such as Flash, Java and Internet browsers as soon as they are available; 10 percent in the first day and an additional 50 percent in the first week.

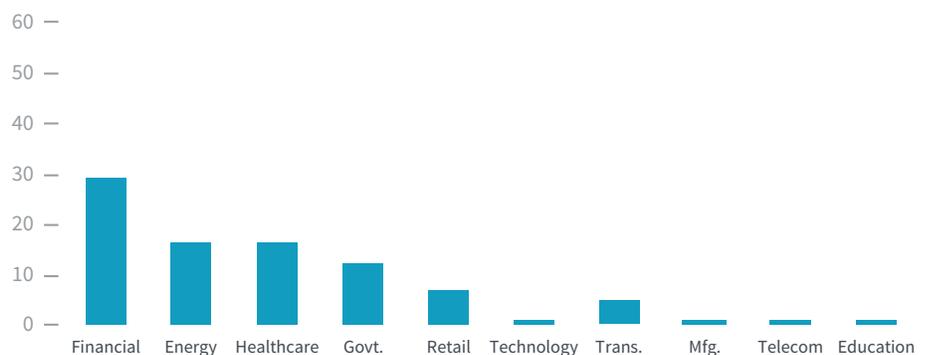
It should be concerning that 22 percent of information security professionals take more than a month to patch zero-day vulnerabilities. If an organization is running a vulnerable version of Flash, then it can be compromised by the majority of popular exploit kits, such as Angler. Once again, this demonstrates the tension between security and operations since security teams may be limited in their ability to implement zero-day patches.

Critical Infrastructure at Risk—All Eyes on Financial Services

At a macro level, Black Hat attendees believe critical infrastructure is at the most risk of cyber attacks. Specifically, Bromium surveyed Black Hat attendees to identify which industry is at the most risk of cyber attacks. At a micro level, risk of cyber attacks can be broken down into financial services (30 percent), energy (17 percent), healthcare (17 percent) and government (12 percent). The risk of cyber attacks on tech companies, retail and transportation was noticeable, but not significant. Information security professionals see virtually no risk to education, telecom and manufacturing.

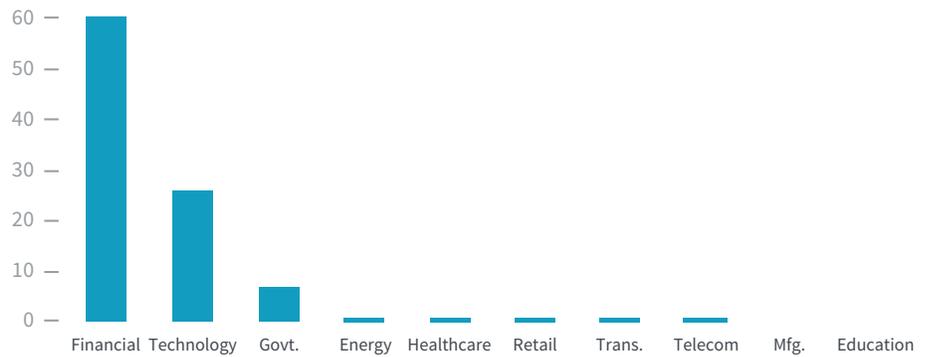
Financial services was singled out as the most at risk of cyber attacks, but was also singled out as having implemented the best security practices. Sixty percent of Black Hat attendees believe financial services have implemented the best security practices with an additional 27 percent selecting technology.

WHICH VERTICAL/INDUSTRY DO YOU BELIEVE IS AT THE MOST RISK OF CYBER ATTACKS? (PERCENT OF RESPONSES)



It makes sense that financial services were singled out as being at the most risk because they provide the most reward. As a result, financial services tend to be more security conscious and technically savvy, willing to make greater investments in security solutions and becoming early adopters of new technology.

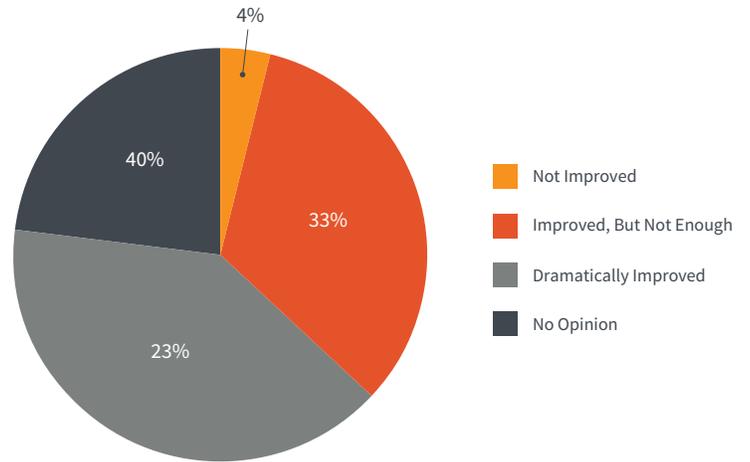
WHICH VERTICAL/INDUSTRY DO YOU BELIEVE HAS IMPLEMENTED THE BEST SECURITY PRACTICES? (PERCENT OF RESPONSES)



Mixed Reaction to Windows 10—Slow Adoption in First Year

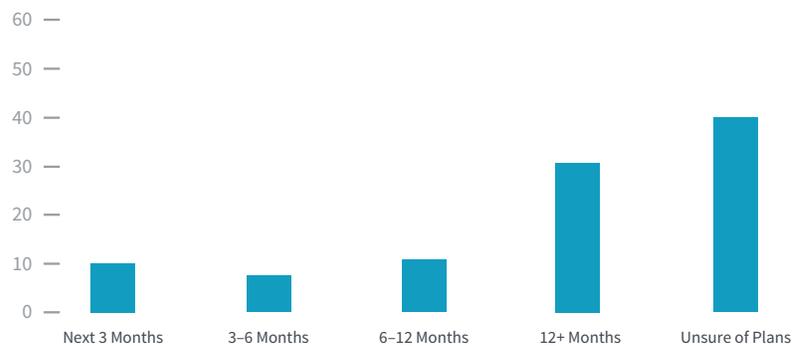
Many information security professionals had no opinion of Windows 10, which was released just days before Black Hat; however, a majority still believe that security has improved. The opinion of 23 percent of information security professionals is that Windows 10 is dramatically improved; however, 33 percent believe that while security has improved, it is not enough.

WHAT IS YOUR OPINION OF THE SECURITY FEATURES IN WINDOWS 10?
(PERCENT OF RESPONSES)



When asked to discuss plans to upgrade to Windows 10, a vocal minority expressed excitement for the new operating system, but most had no plans (40 percent) or would be waiting more than a year (31 percent) to upgrade. For Windows 10, the first year appears to be an early adopter market, but it will be interesting to see if deployments begin accelerating in 2016.

WHEN DOES YOUR ORGANIZATION PLAN TO UPGRADE TO WINDOWS 10?
(PERCENT OF RESPONSES)



Conclusion

The results of this survey indicate that endpoint security risk is more than five times greater than network or cloud. A challenge exacerbated by issues with Flash and delays with critical patches. The human element increases endpoint risk because of their tendency to connect to untrusted networks in hotels, airports or coffee shops and their inability to identify malicious content in email or on the Internet. This problem increases the risk of cyber attack because detection-based security solutions, such as antivirus, have also proven they are unable to identify malicious content in email or on the Internet.

Bromium has pioneered a new approach to endpoint protection: threat isolation to prevent breaches. Bromium vSentry® utilizes micro-virtualization to isolate every user task, such as opening documents and browsing the Internet, which contains untrusted content from accessing the host system (and by extension, the network).

Methodology

Bromium “Black Hat 2015: State of Security” surveyed 101 information security professionals at Black Hat Conference in Las Vegas, Nevada, August 5-6, 2015.

For more information

For more information, contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.



Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information refer to www.bromium.com
or contact sales@bromium.com

Copyright ©2015 Bromium, Inc. All rights reserved.
RPT.BLACKHAT.SURVEY.US-EN.1508