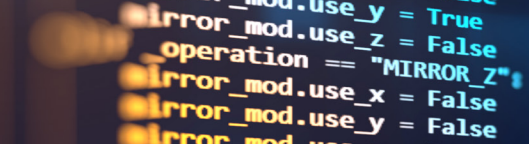
A Growing Risk Ignored: Critical Updates

EXPLORING THE PREVALENCE OF OUTDATED SYSTEMS AND THEIR LINK TO DATA BREACHES

BITSIGHT®
The Standard in SECURITY RATINGS



INTRODUCTION

On May 12, 2017, thousands of computers across the world were infected by a strain of ransomware known as "WannaCry" (also "WannaCryptor" or "WannaCrypt").[1] Estimates show that this massive attack impacted over 300,000 computers across banks, hospitals, telecommunications services, train stations, and numerous other critical services.[2, 3] The attack spread to more than 150 countries, including the United Kingdom, Spain, Germany, China, Turkey, Russia, the United States, and others.[4] Months before this attack, Microsoft had released a patch of all Server Message Block (SMB) vulnerabilities, including EternalBlue, which researchers believe is one of the vulnerabilities that criminals exploited to carry out the attack.[5] Despite the available patch, it appears that many companies neglected to install the critical update (MS17-010) from Microsoft prior to the attack.[6]

Many of the techniques used in this ransomware attack have been around for decades. For instance, the SQL Sapphire worm seen in 2003 exploited a buffer overflow vulnerability in computers running Microsoft SQL Server. Microsoft released a patch for the vulnerability long before the attack. However, many companies had failed to apply the update and as a result, thousands of machines were infected and the worm caused network outages, airline flight cancellations, and ATM failures.[7] Given the increasing number of endpoint devices connected to corporate networks, the ever-expanding supply chain, the complexity of cyber attacks, and the critical vulnerabilities that get patched through periodic updates, are companies adequately updating their operating systems and Internet browsers? What is the risk of running outdated systems? Furthermore, what is the risk to any company if members of their supply chain are falling behind in their patching process?

To answer these questions, BitSight researchers examined more than 35,000 companies from over 20 industries across the world to explore the use of outdated operating systems and outdated Internet browsers over the last year and their correlation to data breaches. As part of this study, researchers focused on operating systems from Apple and Microsoft, along with Internet browsers such as Firefox, Chrome, Safari, and Internet Explorer. As criminals continue to exploit outdated systems to carry out massive attacks, it has become important for companies to patch vulnerabilities and assess the number of outdated endpoints on their networks as well as the networks of their trusted third parties with access to sensitive data.

KEY FINDINGS

1. Over 2,000 organizations run more than 50 percent of their computers on outdated versions of an operating system, making them almost three times as likely to experience a publicly disclosed breach.

2. Over 8,500 organizations have more than 50 percent of their computers running an out-of-date version of an Internet browser, doubling their chances of experiencing a publicly disclosed breach.

3. More than 25 percent of the computers used in the Government sector were running outdated MacOS or Windows operating systems, with nearly 80 percent of these outdated systems comprised of MacOS.

4. In March of this year, two months before the WannaCry ransomware attack, nearly 20 percent of computers examined in this report that were running Windows were using Windows Vista or XP, both of which did not have a patch available and are no longer officially supported by Microsoft.

5. A month after each macOS Sierra point release is announced, more than 35 percent of companies fail to upgrade to the latest version, potentially exposing the systems to vulnerabilities during that time.

EXPLORING THE CORRELATION TO BREACHES

The recent WannaCry ransomware attack brought to light the link between outdated systems on corporate networks and the probability of cyber criminals gaining access to a company's data. However, the problem has existed for quite some time. For example, Conficker has existed since 2008 and continues to impact a large number of companies according to a recent report by Check Point Software Technologies.[8] The worm exploits a vulnerability in Windows XP, Windows 2000, and Windows 2003 (MS08-067), allowing a hacker to gain remote access without authentication.[9]

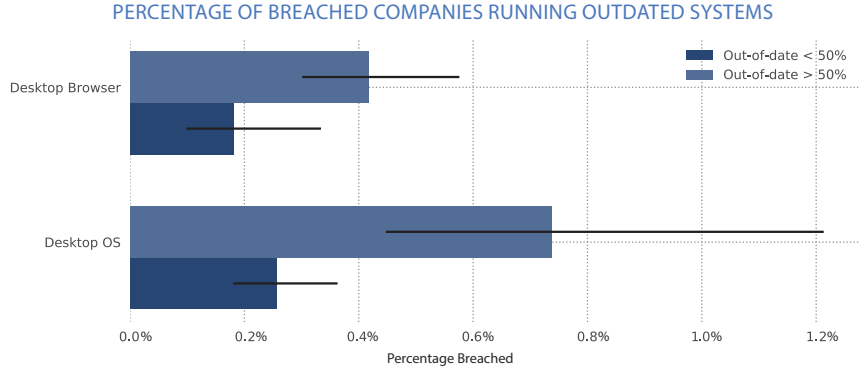
Through continuous patch management, organizations today can take a proactive approach to securing their networks by applying the latest patches and installing critical system updates.[10] Technology companies such as Apple, Google, and Microsoft frequently release software patches that fix major security vulnerabilities. For instance, a Google Chrome update from December 2016 addressed severe issues tied to universal cross-site scripting vulnerabilities in Chrome's "Blink" component, a web browser engine developed as part of the Chromium Project.[11] In another example, a recent update from March 2017 fixed vulnerabilities in macOS Sierra and iOS that could lead to arbitrary code execution, with root privileges in some cases.[12]

BitSight researchers examined more than 35,000 companies and found that over 8,500 of these organizations were running at least 50 percent of their computers on older Internet browsers (i.e. not the most up-to-date versions), making them more than twice as likely to experience a publicly disclosed breach compared to companies with less than 50 percent of their computers running out-of-date browsers. Researchers also found that when organizations had more than 50 percent of their computers running outdated versions of an operating system, they were nearly three times as likely to experience a breach than organizations with less than 50 percent of their computers on an outdated version of an operating system (Figure 1). In fact, over 2,000 organizations in this report were running at least 50 percent of their computers on outdated versions of an operating system.

Given the correlation between outdated systems and data breaches, organizations should consider taking a proactive approach to securing their networks before these vulnerabilities are exploited by cyber criminals. They should also be aware of the third parties with access to their data and whether they fall behind in their patching process. According to Bomgar's *Secure Access Threat Report 2017*, the average number of vendors accessing a company's network has doubled in just one year to 181 per week, with 67 percent of companies experiencing a data breach because of unsecured vendor access.[13] Companies with a growing vendor ecosystem should monitor whether their third parties leverage outdated systems and measure the risk that this presents to protecting their networks from cyber attacks.

FIGURE 1

The percentage of companies that experienced a cyber breach and their use of outdated operating systems and out-of-date Internet browsers over an eight-month period (95% confidence intervals displayed).



INDUSTRY PERFORMANCE

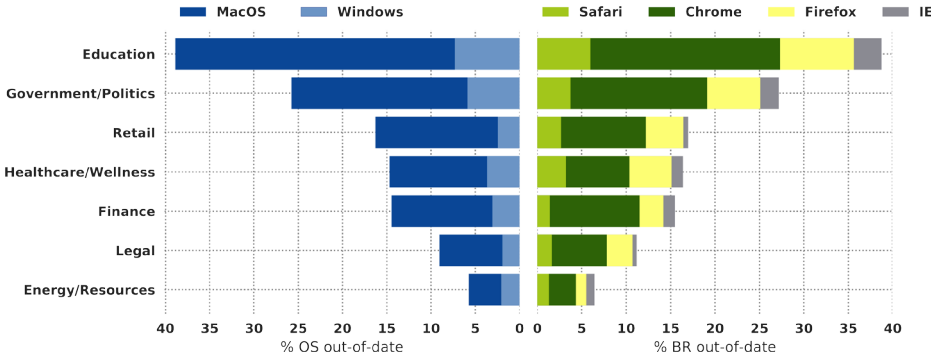
Today's cyber attacks not only steal data from organizations and their trusted third parties, but they also hold their data hostage and disrupt business operations through ransomware or DDoS (Distributed Denial of Service) attacks. In a recent report, *The Rising Face of Cyber Crime: Ransomware*, BitSight researchers found that the rate of ransomware attacks tripled, or in some cases increased tenfold, for many industries throughout 2016.[14] As the rate of complex cyber attacks continues to rise, experts agree that implementing the latest software and security updates is critical in the fight against cyber crime. According to Brad Smith, President and Chief Legal Officer at Microsoft, "as cyber criminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems. Otherwise they're literally fighting the problems of the present with tools from the past."[15]

As a part of this study, *A Growing Risk Ignored: Critical Updates*, BitSight researchers examined seven major industries, including Education, Government, Retail, Healthcare, Finance, Legal, and Energy. They found that among these industries, Education and Government had the highest usage rate of outdated operating systems and Internet browsers. In fact, more than 25 percent of the computers used in the Government sector (including state and local government) were running outdated versions of MacOS or Windows operating systems, with nearly 80 percent of these systems being out-of-date MacOS. This industry also had a high rate of outdated Internet browsers. More than 25 percent of the Internet browsers in this industry were not the most up-to-date versions, with Chrome representing the majority of these systems (70.4%).

FIGURE 2

The percentage of outdated operating systems and out-of-date Internet browsers across seven industries, over an eight-month period. Each bar depicts the total percentage of outdated operating systems or browsers. Each bar then shows a breakdown of the percentage of Windows, MacOS, Safari, Chrome, Firefox, or Internet Explorer (IE).

PERCENTAGE OF OUTDATED OPERATING SYSTEMS AND BROWSERS ACROSS INDUSTRIES



President Trump's recent Executive Order on Cybersecurity highlights similar findings, noting that the executive branch has for too long accepted antiquated and difficult-to-defend IT.[16] The order specifically addresses the issue, calling for government agencies to update their outdated systems. According to Tim Bossert, US homeland security adviser, "The trend is going in the wrong direction in cyberspace and it's time to stop that trend and reverse it on behalf of the American people."[17]

Although Finance has been a top performer in previous research, this new study found that the financial sector performs in line with Healthcare and Retail when it comes to outdated operating systems and Internet browsers. An estimated 15 percent of computer operating systems and browsers are out of date in each of these industries. These are important findings because they suggest that although Healthcare and Retail companies have made most of the headlines for their exposure to recent ransomware attacks, the Financial sector may be vulnerable to similar cyber attacks in the future as a result of their use of outdated systems.

Companies in the Legal and Energy sectors demonstrated the lowest rate of outdated operating systems and Internet browsers. Given that the Energy sector provides critical infrastructure services, organizations in this sector should maintain their proactive approach to security. Despite its top performance, researchers found that more than 120 companies in this sector were running out-of-date or unsupported operating systems and more than 400 companies were observed to have greater than 33 percent of Internet browsers out-of-date. This represents a gap in security and presents an opportunity for hackers to exploit weaknesses in this critical sector.

TIME LAPSE BETWEEN UPDATES

When large technology companies such as Google, Apple, and Microsoft release software updates, they not only provide patches for security vulnerabilities, but they also help end-users to protect their systems against cyber attacks. For example, with macOS Sierra (10.12) Apple changed the behavior of its GateKeeper feature by deleting the download-from-anywhere option from the "Security and Privacy" settings. This aims to ensure that users only download applications from the App Store and identified developers rather than from anywhere on the Internet, where applications may come with vulnerabilities and backdoors that cyber criminals can exploit to carry out attacks. Older operating systems such as Yosemite (10.10) are not equipped with these safety features.[18]

Despite the known value of maintaining updated systems, BitSight researchers found that organizations take months to upgrade to the latest software versions. Most of the organizations examined by BitSight as part of this study take, on average, more than a month to implement the latest point releases of macOS Sierra (Figure 3). For example, on March 27, 2017, more than two months after Sierra 10.12.3 was released, over 40 percent of companies using computers with macOS Sierra, were running an older version of the operating system. During that same month, more than 10 percent of computers on OS X were running 10.9 or older (Figure 4), which Apple released four years ago in June 2013.[19]

FIGURE 3

The percentage of ccompanies with computers running a particular point version of macOS Sierra (10.12) over an eight-month period.

Note: The prevalence of point releases observed prior to an announcement date is likely due to Apple beta users testing each new release.

MAC OS SIERRA RELEASES AND PREVALENCE OF USE BY ORGANIZATIONS

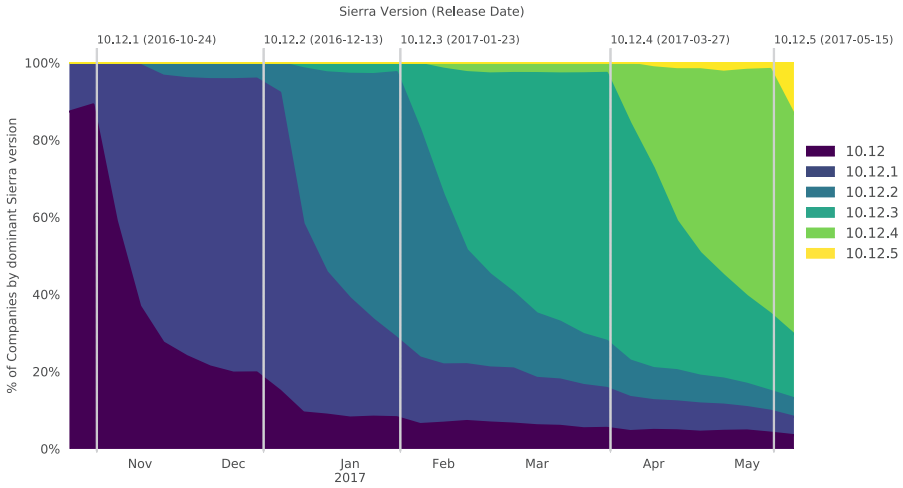
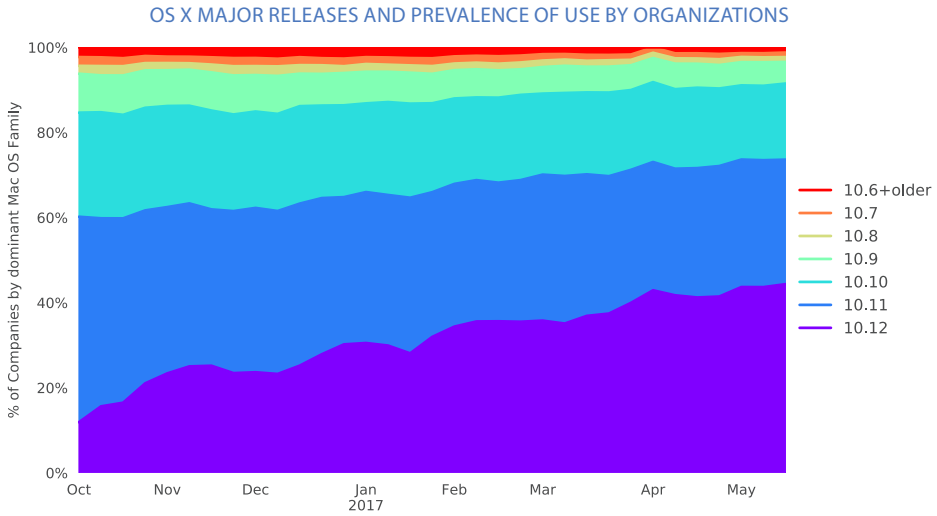


FIGURE 4

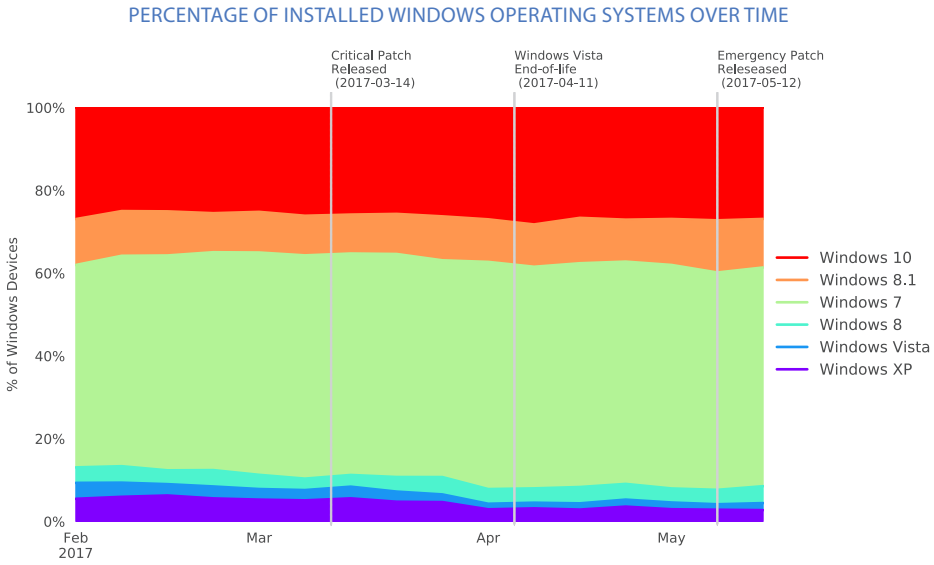
The percentage of computers and the version of MacOS that they used over an eight-month period.



BitSight researchers also found that as of March 2017, nearly 50 percent of the computers examined in this report that were running a Windows operating system, were on Windows 7 instead of the latest version, Windows 10 (Figure 5). More surprisingly is that nearly 20 percent of these Windows computers were running Windows XP or Vista, which Microsoft no longer supports. According to Markus Nitschke, head of Windows at Microsoft Germany, "Windows 7 does not meet the requirements of modern technology, nor the high security requirements of IT departments."[20] Meanwhile, Windows 10 includes new sensors to detect in-memory malware and tools to isolate infected machines from the rest of the network.[21]

FIGURE 5

The percentage of computers and the version of Windows operating systems that they used over a four-month period in 2017.



The widespread impact of the WannaCry attack should be considered a wakeup call for security teams to upgrade their operating systems and Internet browsers. In fact, a previous study by BitSight found that Windows 7 was hit especially hard by the WannaCry attack: over 67 percent of machines on IP addresses impacted by this attack were running Windows 7.[22] Will companies transition to Windows 10 as a result of the ransomware attacks? It will be interesting to examine whether the use of Windows 10 increases over the next few months.

RECOMMENDATIONS

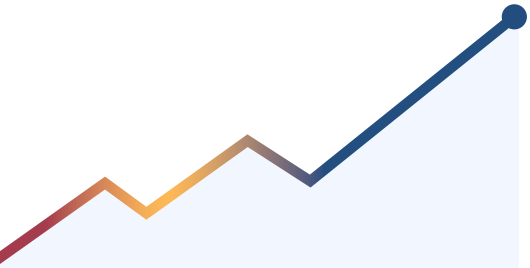
The WannaCry attacks have been a wakeup call for security teams, revealing the large number of organizations that use outdated systems and ignore critical updates. Some of these organizations may be trusted third or fourth parties in a company's supply chain. Below are recommendations for organizations to approach cybersecurity with a sense of urgency to secure their networks and collaborate with third and fourth parties to protect their sensitive data.

- **Apply critical system updates and monitor your attack surface from the outside**. Large technology companies such as Google, Microsoft, and Apple frequently update their software and communicate the vulnerabilities that get patched with each release. Although it may be difficult for large companies to update every computer on their networks, IT teams should at least examine whether any computers on their networks are using outdated versions of operating systems. This can be done from outside the network without solely relying on penetration tests or network scans.
- **Update Internet browsers**. With the growing adoption of tools such as Google Drive and Box, which allow employees to access company data through web browsers, organizations must maintain up-to-date Internet browsers to protect their sensitive data. Some browsers offer automatic updates, but because employees across the company may use different browsers to access the Internet, information security teams cannot solely rely on these automated features. Instead, they must proactively monitor their network and consider installing updates on systems with outdated browsers.
- **Continuously monitor and evaluate your third parties**. Organizations should confirm that their data is not managed by third parties with outdated endpoints connected to their network. If organizations cannot determine whether their critical vendors are using outdated operating systems or Internet browsers, they should consider restricting the vendor's access to the company's sensitive data so that the company's data is not at risk in the event of a breach.
- **Understand the business impact of cybersecurity decisions**. Cybersecurity should be an important part of business discussions with the board of directors and senior executives. When a company considers engaging a critical third party, cybersecurity has to be an integral part of the decision. Knowing whether a potential vendor is using outdated systems can help the organization better understand the vendor and the level of risk that they present to the business.

CONCLUSION AND LOOKING AHEAD

Although companies have advanced their approach over the years, BitSight researchers have found that thousands of companies are using outdated operating systems and Internet browsers, increasing their chances of experiencing a publicly disclosed data breach. As more devices are connected to their networks, companies without robust endpoint security controls or mature third party risk management programs will likely be exposed to more cyber attacks in the future.

Looking ahead, could mobile devices become the next target for hackers? A 2016 survey from Gartner found that two-thirds of survey respondents used a personally owned device for work.[23] Criminals are already developing mobile worms.[24] Given the way that cyber criminals have exploited outdated systems to carry out massive attacks, outdated mobile devices may pose the next big cyber threat for companies. Further research should shed light on this issue and arm companies and their third parties with the necessary insight to protect their networks from the next attack.



METHODOLOGY

BitSight collects and processes vast amounts of data in order to provide the industry standard in Security Ratings. The foundation of this research is built on our ability to accurately identify machine compromises, network diligence details, and user behavior across the Internet, and attribute the information to companies. We determine this attribution by identifying the CIDR (Classless Inter-Domain Routing) blocks, domains, and AS (Autonomous System) numbers that organizations own. Customer research shows that our team constructs maps with greater than 95% accuracy, even for companies with hundreds of thousands of IP addresses.

In this report, unsupported operating systems are defined as those that have reached end-of-life and no longer recieve regular security updates. This includes Windows 8, Windows Vista, and Windows XP or earlier. Out-of-date operating systems and browsers are defined as installations that are still supported but not on the latest available version. To look at the spread of operating systems and Internet browsers, researchers studied over 1.5 billion observations over a period of eight months, from October 2016 to May 2017. A section of this report focused on seven industries, including 12,831 organizations across Finance (3,864), Healthcare (2,935), Education(1,908), Government/Politics(1,001), Energy/Resources (1,054), Retail (970), and Legal (1,099).

ABOUT BITSIGHT

BitSight pioneered security rating services and over the years has relentlessly executed on its mission, transforming how organizations evaluate risk and security performance by employing the outside-in model used by credit rating agencies. The BitSight team understands the increasing demands that have made third party cyber risk management a focus area for boards of directors and senior leaders. The company believes that the only way to effectively scale third party risk management programs is through automated, continuous monitoring. For more information, please visit www.bitsighttech.com, read our blog, or follow @BitSight on Twitter.

REFERENCES

1. "Ransomware cyber-attack threat escalating - Europol," *BBC News*, May 14, 2017. Retrieved on May 17, 2017 from http://www.bbc.com/news/technology-39913630

2. "WannaCry Ransomware: What We Know Monday," Bill Chappell, NPR, May 15, 2017. Retrieved on May 24, 2017 from http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday

3. "An NSA-derived ransomware worm is shutting down computers worldwide," Dan Goodin, *Ars Technica,* May 12, 2017. Retrieved on May 17,2017 from https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/

4. "The WannaCry ransomware attack has spread to 150 countries," Andrew Liptak, The Verge, May 14, 2017. Retrieved on May 25, 2017 from https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

5. "Understanding the Effect of DoublePulsar and Wannacry Across Industries is the Key to Protecting Your Supply Chain," Dan Dahlberg, BitSight Technologies, May 15, 2017. Retrieved on May 19, 2017 from https://www.bitsighttech.com/blog/understanding-doublepulsar-wannacry-across-industries-is-key-to-protecting-supply-chain

6. "Microsoft Security Bulletin MS17-010 - Critical," Microsoft, March 14, 2017. Retrieved on May 17, 2017 from https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

7. "The Spread of the Sapphire/Slammer Worm," David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver, 2003. Retrieved on May 18, 2017 from https://www.caida.org/publications/papers/2003/sapphire/sapphire.html#1

8. "Top Malware Families Found in January 2016 Show DDoS on the Rise," Check Point Software Technologies, March 8, 2016. Retrieved on June 6, 2017 from http://blog.checkpoint.com/2016/03/08/top-malware-families-found-in-january-2016-show-ddos-on-the-rise/

9. "Microsoft Security Bulletin MS08-067 - Critical," Microsoft, October 23, 2008. Retrieved on June 6, 2017 from https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

10. "Patch Management," Techopedia. Retrieved on May 26, 2017 from https://www.techopedia.com/definition/13835/patch-management

11. "Google Releases Security Updates for Chrome," United States Computer Emergency Readiness Team, December 1, 2016. Retrieved on May 17, 2017 from https://www.us-cert.gov/ncas/current-activity/2016/12/01/Google-Releases-Security-Updates-Chrome

12. "macOS Sierra: Protect your Mac from malware," Apple, March 28, 2017. Retrieved on May 17, 2017 from https://support.apple.com/kb/PH25087?locale=en_US&viewlocale=en_US

13. *The Secure Access Threat Report 2017*, Bomgar, May 2017. Retrieved on June 2, 2017 from https://www.bomgar.com/assets/documents/Bomgar_Secure_Access_Report.pdf

14. "The Rising Face of Cyber Crime: Ransomware," BitSight Technologies, September 21, 2016. Retrieved on May 17, 2017 from https://www.bitsighttech.com/blog/rising-face-of-cybercrime-ransomware

15. "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack," Brad Smith, Microsoft, May 14, 2017. Retrieved on May 17, 2017 from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.000h5ryr51brsd7epy9190b3sw7e7

16. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Office of the Press Secretary, The White House, May 11, 2017. Retrieved on May 30, 2017 from https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

17. “President Trump signs cybersecurity executive order,” David Jackson and Elizabeth Weise, USA Today, May 11, 2017. Retrieved on May 30, 2017 from https://www.usatoday.com/story/news/politics/2017/05/11/president-trump-signs-cybersecurity-executive-order/101556518/

18. “Apple Fixes 223 Vulnerabilities Across Mac OS, iOS, Safari,” Chris Brook, Threat Post, March 28, 2017. Retrieved on May 18, 2017 from https://threatpost.com/apple-fixes-223-vulnerabilities-across-macos-ios-safari/124599/

19. “Apple Releases Developer Preview of OS X Mavericks With More Than 200 New Features,” Apple, June 10, 2013. Retrieved on May 17, 2017 from https://www.apple.com/pr/library/2013/06/10Apple-Releases-Developer-Preview-of-OS-X-Mavericks-With-More-Than-200-New-Features.html

20. “Windows 7 Support endet in drei Jahren,” Markus Nitschke, Microsoft, January 16, 2017. Retrieved and translated via Google Translate on May 17, 2017 from https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=https%3A%2F%2Fblogs.technet.microsoft.com%2Fwindowsfurunternehmen%2F2017%2F01%2F16%2Fwindows-7-support-endet-in-drei-jahren%2F&edit-text=&act=url

21. “Windows Defender Advanced Threat Protection,” Microsoft, May 3, 2017. Retrieved on May 17, 2017 from https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection

22. “Assessing the Global Impact of WannaCry Ransomware,” Dan Dahlberg, BitSight Technologies, May 26, 2017. Retrieved on May 26, 2017 from https://www.bitsighttech.com/blog/assessing-the-global-impact-of-wannacry-ransomware

23. “Gartner Survey Shows That Mobile Device Adoption in the Workplace Is Not Yet Mature,” Gartner, November 29, 2016. Retrieved on May 17, 2017 from http://www.gartner.com/newsroom/id/3528217

24. Internet Security Threat Report, Symantec, April 2016.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu