Microsoft Security Intelligence Report

VOLUME 23

Microsoft

Table of Contents

Foreword

Welcome to the 23rd edition of the *Microsoft Security Intelligence Report*, a bi-annual publication that Microsoft creates for customers, partners, and the industry. The purpose of this report is to educate organizations about the current state of threats, recommended best practices, and solutions.

What sets the *Microsoft Security Intelligence Report* apart from others is the volume and variety of Microsoft analysis. This analysis spans cloud services for businesses and individual consumers, from websites to identity, from email to endpoint. For example, there are 400 billion email messages scanned, 450 billion authentications, and 18+ billion webpage scans per month.

This edition focuses on three topics that emerge from data collected since February 2017: botnets, hacker methods, and ransomware.

Microsoft continues to develop new capabilities in its platforms that use machine learning, automation, and advanced real-time detection techniques. Our aim is to strengthen our customers' ability to not only protect against evolving, sophisticated threats, but also to quickly detect and respond when a breach occurs.

We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Microsoft Security

Executive Summary

Notable trends this year:

Looking beyond the headline-grabbing incidents of 2017, Microsoft has analyzed the threat intelligence gathered from its global customer base across 100+ countries and millions of computers. This analysis has exposed three interesting topics:

1. **Botnets** continue to impact millions of computers globally, infecting them with old and new forms of malware. This report provides information about the highly publicized disruption of the Gamarue botnet, which Microsoft helped with in 2017.

2. **Hackers went for the easy marks.** If cybercrime is a business, then low-cost attack methods with potentially high returns is what hackers focused on in 2017.

3. **Ransomware** is still a force to be reckoned with and doesn't look to be slowing down any time soon.

It was a busy year in security, of course, and this report is not meant to summarize all the news of the year. Instead, it discusses these three trends and provides context based on the threat intelligence Microsoft research teams glean from multiple sources, including on-premises and cloud solutions and services. We also share recommendations on how to defend against and respond to threats, and highlight other resources for additional information.

SECTION 1

Breaking botnets

Cyber criminals are continuing to relentlessly infect computers and engage in botnet activity with the intention to have a large infrastructure that they can then mine for sensitive data and possibly monetize, as is the case with ransomware threats. Defending against botnet activity is not a simple task and, as in years past, takes a massive effort by both private and public organizations working together.

A bot is a program that allows an attacker to take control of an infected computer. A botnet is a network of infected computers that communicate with command-and-control servers. Cybercriminals use botnets to conduct a variety of online attacks, such as send spam, conduct denial-of-service attacks on websites, spread malware, facilitate click fraud in online advertising, and much more.

There have been several botnet disruptions coordinated by the Microsoft Digital Crimes Unit (DCU) going back to the November 2008 Conficker botnet disruption. On November 29, 2017, the Microsoft Digital Crimes Unit (DCU) coordinated the disruption of the Gamarue botnet (also known as Andromeda).

Analysis and explanation

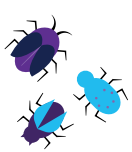
The Gamarue botnet disruption was the culmination of a journey that started in December 2015, when the Microsoft Windows Defender research team and Microsoft Digital Crimes Unit activated a Coordinated Malware Eradication (CME) campaign for Gamarue. In partnership with the internet security firm ESET, Microsoft Digital Crimes Unit security researchers and Windows Defender Security Intelligence teams performed in-depth research into the Gamarue malware and its infrastructure. Microsoft analyzed more than 44,000 malware samples, which uncovered the botnet's sprawling infrastructure. Detailed information about that infrastructure was provided to law enforcement agencies around the world, including:

1,214

domains and IP addresses of the botnet's command and control servers

464

distinct botnets



80+

associated malware families

The coordinated global operation resulted in the disconnection of the botnet's servers on November 29, 2017, disrupting one of the largest malware operations in the world.

The Gamarue botnet disruption was achieved through partnership of Microsoft with law enforcement agencies around the globe, including the United States Federal Bureau of Investigation, Germany's Luneburg Central Criminal Investigation Inspectorate, and Europol's European Cybercrime Centre.

Since 2011, Gamarue has evolved through five versions of malware and has distributed a plethora of other threats, including:

- Petya and Cerber ransomware
- Kasidet malware (also known as the Neutrino bot), which is used for DDoS attacks
- Lethic, a spam bot
- Info-stealing malware Ursnif, Carberp, and Fareit, among others

Up until its disruption, Gamarue was a very active malware family that showed no signs of slowing down. Since the disruption, Gamarue-infected devices have connected to the DCU sinkhole from 23 million IP addresses, highlighting the global pervasiveness of the Gamarue botnet (Figure 1).

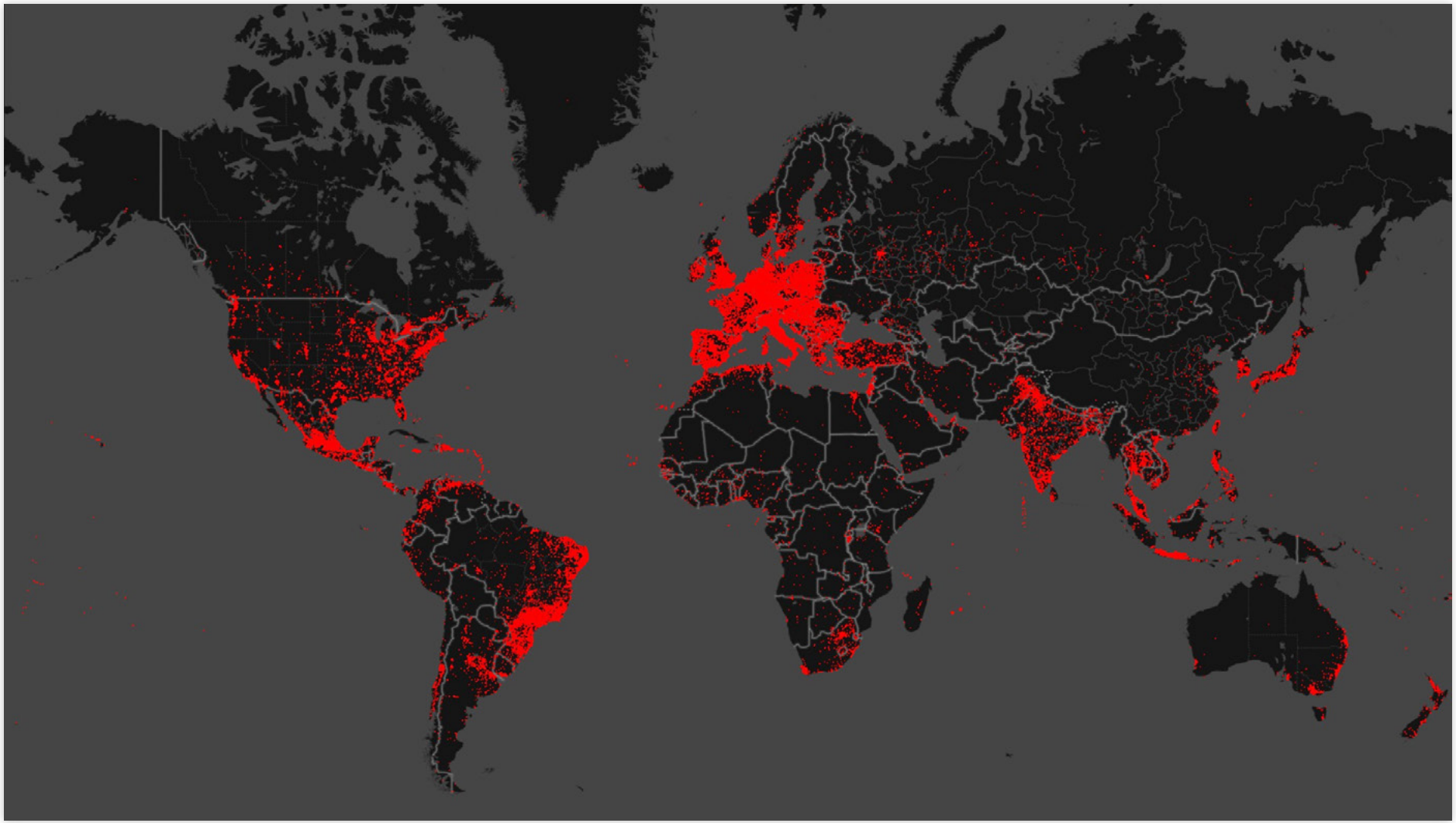


***Figure 1**. DCU telemetry demonstrates Gamarue's global prevalence of infected devices from December 2017 to January 2018*

The Gamarue botnet

Gamarue is known in the underground cybercrime market as the Andromeda bot. Like many other bots, Gamarue was advertised as a crime kit that hackers can purchase.

The Gamarue crime kit includes the following components:

- A bot-builder, which builds the malware binary that infects computers
- A command-and-control application, which is a PHP-based dashboard application that allows hackers to manage and control the bots
- Documentation on how to create a Gamarue botnet

The evolution of the Gamarue bot has been the subject of many thorough analyses by security researchers. At the time of disruption, there were five known active Gamarue versions: 2.06, 2.07, 2.08, 2.09, and 2.10. The latest and the most active is version 2.10.

Figure 2. Gamarue bot-builder Interface

Modular malware

Gamarue is modular, which means that its functionality can be extended by plug-ins that are either included in the crime kit or available for separate purchase. The Gamarue plug-ins include:

- **Keylogger ($150)**
  Used for logging keystrokes and mouse activity in order to steal user names and passwords, financial information, and so on.
- **Rootkit (included in crime kit)**
  Injects rootkit codes into all processes running on a victim's computer to give Gamarue persistence.
- **Socks4/5 (included in crime kit)**
  Turns victim's computer into a proxy server for serving malware or malicious instructions to other computers on the internet.
- **Formgrabber ($250)**
  Captures any data submitted through web browsers (such as Chrome, Firefox, and Internet Explorer).
- **Teamviewer ($250)**
  Enables attacker to remotely control the victim's computer, spy on the desktop, and perform file transfers, among other functions.
- **Spreader**
  Adds capability to spread Gamarue malware itself via removable drives (for example, portable hard drives or flash drives connected via a USB port); it also uses Domain Generation Algorithms (DGA) for the servers onto which it downloads updates.

Monetization: Pay for malware install

Gamarue's main goal is to distribute other prevalent malware families. The installation of other malware broadens the scale of what hackers can do with the network of infected computers. There are several ways hackers earn money using Gamarue. Because Gamarue's purpose is to distribute other malware, hackers can earn money by using a pay-per-install scheme. By using its plug-ins, Gamarue can also steal user information, and stolen information can be sold to other hackers in cybercriminal underground markets. Access to Gamarue-infected computers can also be sold, rented, leased, or swapped by one criminal group to another. Microsoft DCU noted at least 80 different malware families being distributed by Gamarue. The top three malware classes distributed by the Gamarue botnet were ransomware, trojan, and backdoor.

Figure 3. Classes of malware distributed by Gamarue

Anti-sandbox techniques

Gamarue employs anti-AV techniques to make analysis and detection difficult. Prior to infecting a computer, Gamarue checks a list of hashes of the processes running on a potential victim's computer. If it finds a process that may be associated with malware analysis tools, such as virtual machines or sandbox tools, Gamarue does not infect the computer. In older versions, a fake payload is manifested when running in a virtual machine.

```
analysis_prog_hash_list dd 99DD4432h    ; DATA XREF: chk_dbg+C8↓r
                                        ; chk_dbg+DD↓r
                                        ; vmwareuser.exe
                dd 2D859DB4h            ; vmwareservice.exe
                dd 64340DCEh            ; vboxservice.exe
                dd 63C54474h            ; vboxtray.exe
                dd 349C9C8Bh            ; sandboxiedcomlaunch.exe
                dd 3446EBCEh            ; sandboxierpcss.exe
                dd 5BA9B1FEh            ; procmon.exe
                dd 3CE2BEF3h            ; regmon.exe
                dd 3D46F02Bh            ; filemon.exe
                dd 77AE10F7h            ; wireshark.exe
                dd 0F344E95Dh           ; netmon.exe
```

Figure 4. Gamarue anti-sandbox assembly code

Operating system tampering

Gamarue attempts to tamper with the operating systems of infected computers by disabling the Windows Firewall, Windows Update, and User Account Control functions. These functionalities cannot be re-enabled until the Gamarue infection has been removed from the infected computer. However, the operating system tampering behaviors used by Gamarue do not work on Windows 10.

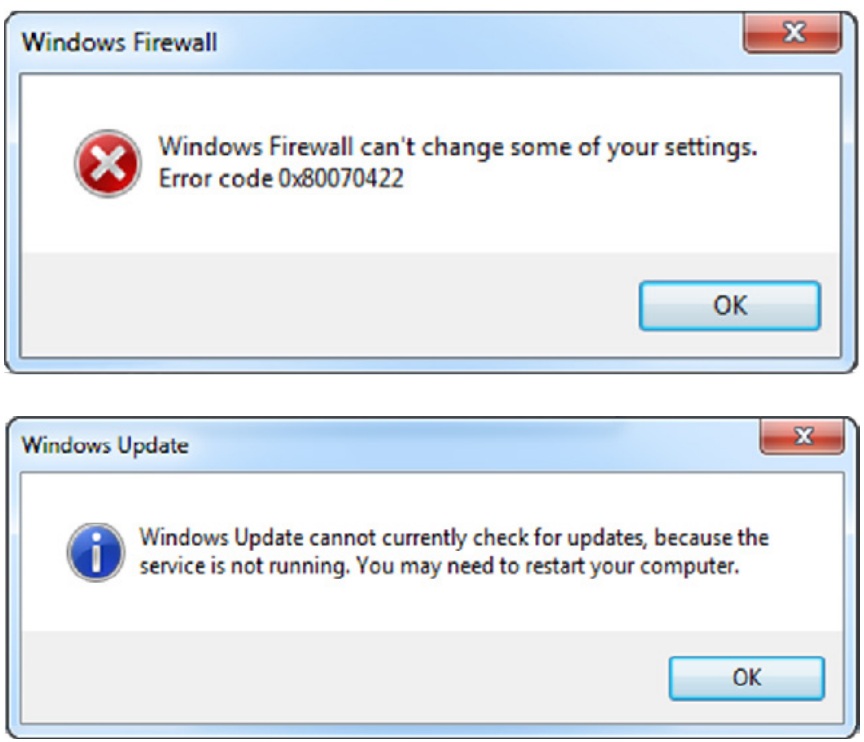


***Figure 5**. Disabled Windows Firewall and Windows Update*

The Avalanche botnet

The Gamarue botnet shared some common infrastructure with the Avalanche botnet for command and control of the two families of malware. Microsoft DCU assisted global law enforcement in the disruption of Avalanche by providing technical research and analysis. DCU collaborated with the Microsoft Windows Defender Security Intelligence team to develop the tools to detect and remove Avalanche and other malware propagating through the Avalanche botnet.

Impact of the disruption operation

Worldwide coordination of research and investigation efforts is key to disrupting a malware operation with the magnitude of Gamarue. As a result of such complexities, public/private partnerships between global law enforcement agencies and private industry partners are essential to a successful outcome.

A significant aspect of the Gamarue disruption was the kill chain effect that the operation had on the distribution of 80 additional malware families. By disrupting a major malware family like Gamarue, we are able to stop potential harm being caused to millions of users worldwide and begin the restoration of victims' devices.

Since the botnet disruption operation in November 2017, the sinkhole Microsoft created has experienced a 30% decrease in Gamarue victims worldwide, as shown in Figure 6.

Microsoft continues to collaborate with public and private industry partners to identify affected devices through the Microsoft Digital Crimes Unit Cyber Threat Intelligence Program to accelerate the remediation process.

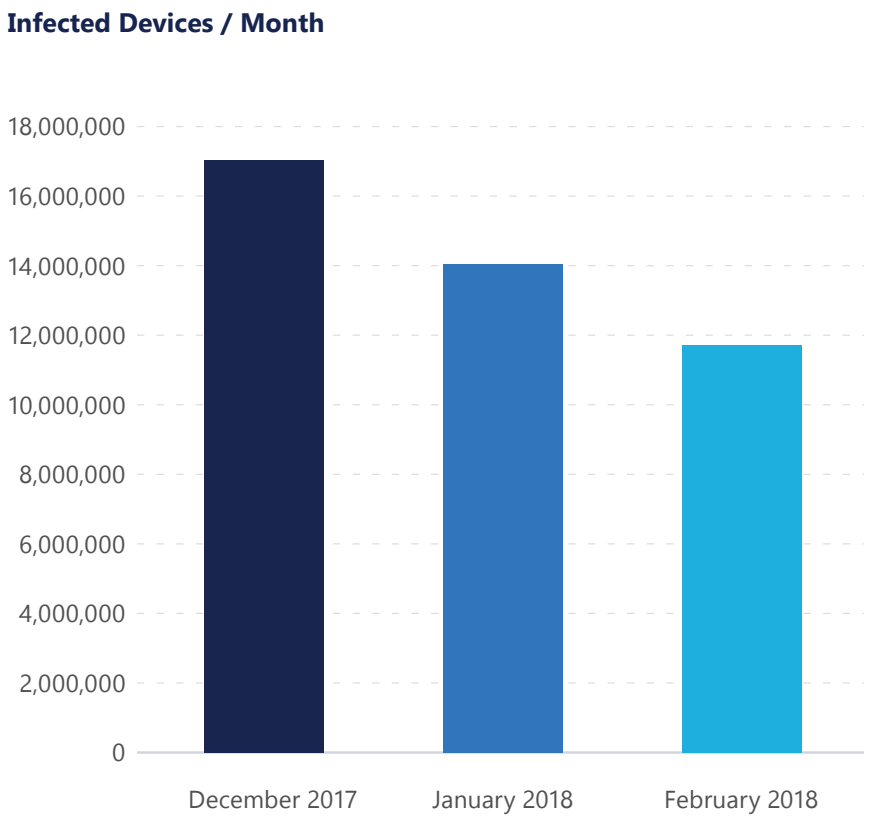


***Figure 6**. Gamarue malware infected devices have decreased after the botnet disruption*

Solutions and recommendations

To detect and protect computers from Gamarue and other malware, use security solutions that apply advanced machine learning models as well as generic and heuristic techniques. Microsoft is continuing the collaborative effort to help clean Gamarue-infected computers by providing a one-time package with samples (through the Virus Information Alliance) to help organizations protect their employees and customers.

SECTION 2

Hackers turning to easy marks

As the cost of circumventing security measures increases, hackers are taking advantage of "low-hanging fruit", such as infrastructure and apps used by organizations and consumers, with the intention of infecting computers and gaining access to sensitive data such as credentials. In this section, we share three of the low hanging fruit routes employed by cyber attackers: social engineering, poorly secured cloud apps, and legitimate software platform features.

Social engineering

As software vendors incorporate stronger security measures into their products, it is becoming more expensive for hackers to successfully penetrate software. By contrast, it is easier and less costly to trick a user into clicking a malicious link or opening a phishing email.

Microsoft Office 365 Advanced Threat Protection (ATP) detected a significant volume of phishing-based email messages at the very end of the year 2017. Phishing was the #1 threat vector (> 50%) for Office 365-based threats in the second half of calendar year 2017.

Top Threats (June - December 2017)

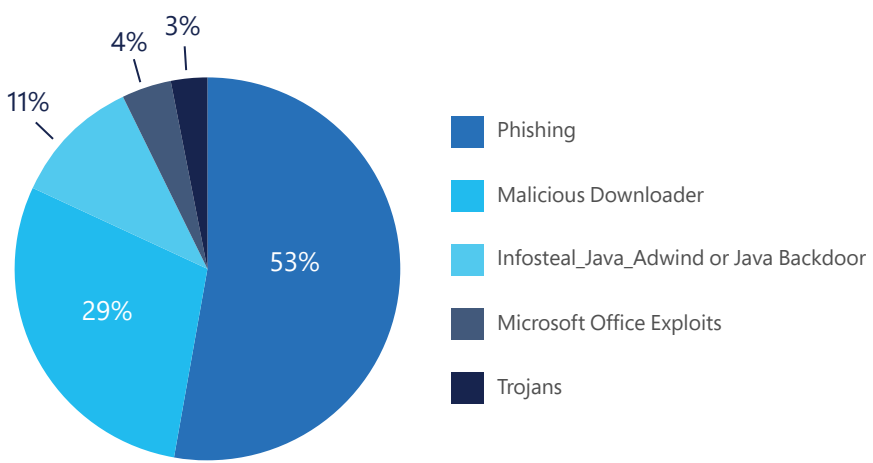


***Figure 7**: Top threats detected by Microsoft Office 365 ATP*

Analysis and explanation

By way of example, an attacker sending a phishing email in bulk to 1,000 individuals just needs to successfully trick one person to obtain access to that person's credentials. Consider a phishing campaign targeting online banking customers, as depicted in Figure 8. If users are distracted and quickly scan the seemingly legitimate but fake phishing email, they may accidentally click a link and share details such as entering their credentials, which are then logged/stored by the hacker for misuse. The point is that phishing and other social engineering tactics can be more simple and effective than other methods, and they work most of the time for more human beings. If successful, phishing is an easier way to obtain credentials as compared to exploiting a vulnerability, which is increasingly costly and difficult.

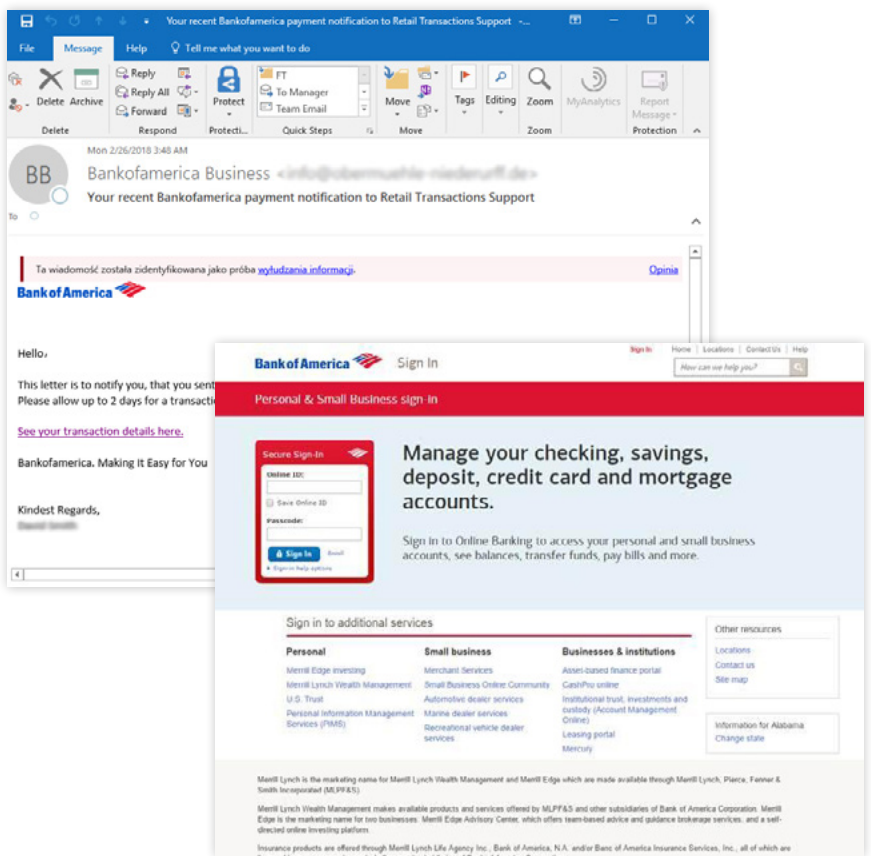


***Figure 8**: Phishing email example*

Phishing comes in many forms

Phishing as an attack vector spans a spectrum of attacks, from broad-based to targeted, as illustrated in Figure 9. The broad-based phishing scams aim to gain hold of personal information (for example, identity and financial information) at scale using techniques such as text lures and domain spoofing. As hackers start building more targeted campaigns that use spear phishing to target high-value accounts (for example, enterprise C-level accounts), we find that they often employ user or domain impersonation to lure users.

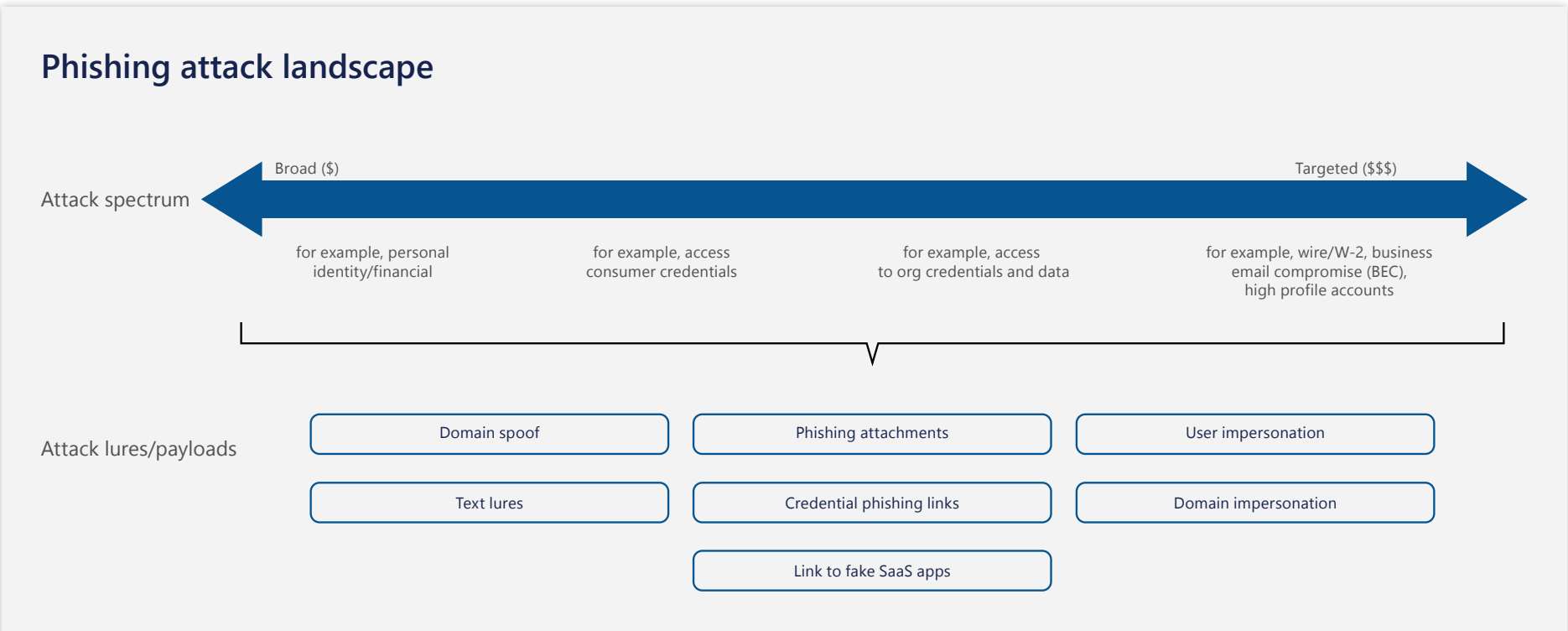


***Figure 9**: Phishing attack landscape varies from broad-based to targeted attacks*

Key phishing related findings

Based on threat intelligence from Office 365 Advanced Threat Protection and Exchange Online Protection across three months (November 2017 – January 2018), the Microsoft Office 365 security research team has been detecting approximately 180-200M phishing emails every month.

- The research team has seen about 30% of domain spoof attacks (based on Office 365 deployments).
- More than 75% of phishing mails include malicious URLs to phishing sites. Other variations include malicious phishing attachments and links in attachments.
- Phishing mails impersonate popular brands
  - Microsoft associated brands (for example, Office 365)
  - Other commonly abused brands include, but are not limited to, DocuSign, Dropbox, Apple, and Amazon.
  - Recent investigations show attacks that impersonate popular courier services such as FedEx, DHL, and UPS.
  - The research team also detected impersonation related to banks and government services.
- Although user impersonation and domain impersonation techniques were low in volume (# of instances in which techniques were used), they were high-severity attacks.

Lowest hanging fruit keeps changing

As an example of the downward trend of exploitation, the exploitation of macros was very prevalent until 2016. However, over time, the cost of such exploitation increased significantly. Not only did attackers need to have very fine-tuned skills to circumvent security measures, most vendors have since been offering more enhanced and effective email sandboxing technology to detect and defend against macro-based malware threats. As a result, when macro-based attacks became unsuccessful, adversaries turned to exploitation of PDFs. This trend was quite prevalent for a while, but as with detection of macros, vendors improved detection of PDF based exploits over time, and attackers moved toward phishing-based attacks.

Solutions and recommendations

Humans are often called the weakest link in cybersecurity, but with the right training and education they can also be the first line of defense. An employee that spots and reports a suspicious email could head off an extensive phishing campaign. And employees that note unexpected latency in systems can set off investigations that uncover lurking threat actors. Organizations can perform mock phishing exercises and can consider hiring third-party experts to obtain security awareness training, including education on phishing. Other resources to help train users:

Tips on recognizing phishing email messages, links or phone calls

Overview of phishing and security tips from US Federal Trade Commission

Phishing overview and resources to report and learn more from US CERT

Poorly secured cloud apps

As cloud (SaaS) apps (also known as cloud services) are increasingly adopted to support business productivity, efficiency, and even cost savings, it is imperative that the cloud apps be built securely so that they are not inadvertently opening the door to data compromise. Microsoft Cloud App Security R&D team has observed a lack of web session security and sound data encryption in SaaS storage and SaaS collaboration apps, based on our visibility and assessment of 30+ cloud apps.

Analysis and explanation

Poorly secured cloud apps can be low-hanging fruit for attackers. One reason is that a given app's lack of web session (HTTP headers session) security could enable attackers to execute application layer attacks (for example, cross-site scripting and cookie hijacking). Also, poor encryption could result in a scenario in which an attacker, after successfully compromising the cloud service or intercepting traffic, compromises the data within the service.

Building various security mechanisms into HTTP headers provides protection from various web session attack vectors, such as protocol downgrading, cookie hijacking, clickjacking, and cross-site-scripting.

The following HTTP headers description is taken from the OWASP website:

HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

The Microsoft Cloud App Security R&D team assessed web security and data encryption for multiple SaaS storage and SaaS collaboration apps. In the following graphs, you can see where the most common SaaS app weaknesses were observed.

Microsoft Cloud App Security assessed HTTP headers session protection of SaaS storage and SaaS collaboration apps. Figures 10 and 11 show results of this assessment.

Support for HTTP headers session protection

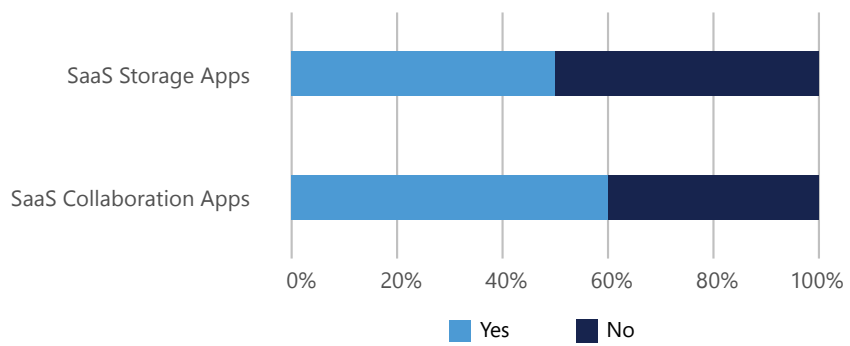


***Figure 10**: 50% of SaaS storage apps and 40% of SaaS collaboration apps do not support HTTP headers session protection*

Support for all HTTP headers session protection methods

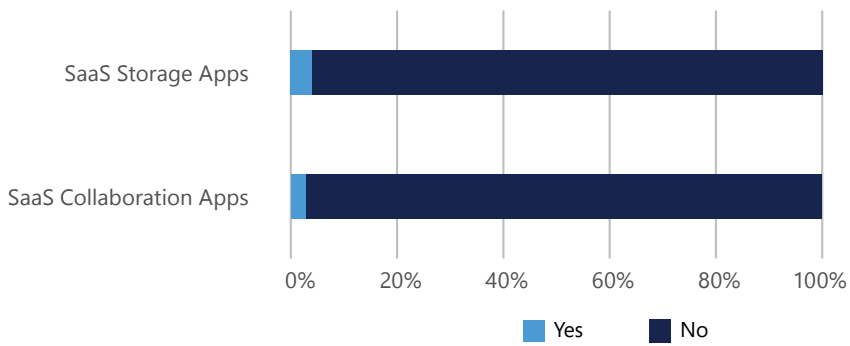


***Figure 11**: Only 4% of SaaS storage apps and 3% of SaaS collaboration apps support all HTTP headers session protection methods*

Microsoft Cloud App Security also assessed data encryption of SaaS storage and SaaS collaboration apps. Figures 12 and 13 show results of this assessment.

Support for some type of data encryption

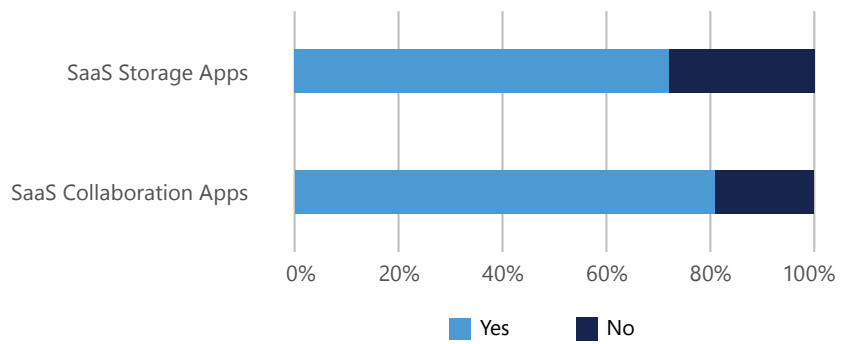


***Figure 12**: 28% of SaaS storage apps and 19% of SaaS collaboration apps do not support any type of data encryption method*

Encrypt data at rest and in transit

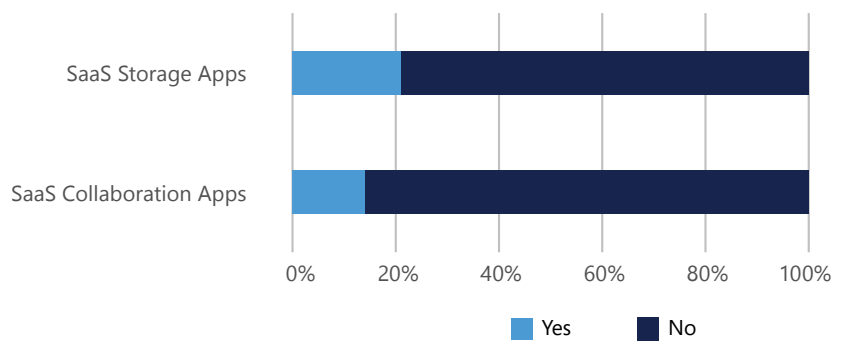


***Figure 13**: 79% of SaaS storage apps and 86% of SaaS collaboration apps do not encrypt data both at rest and in transit*

Solutions and recommendations

When adopting cloud apps, you should make sure that only apps with web session protection and encryption are allowed in your environment. Organizations should have a solution in place to have visibility into and control over all cloud apps usage. For example, some employees could be using unsanctioned SaaS apps for storing corporate or other forms of sensitive data. Using an enterprise cloud access security broker (CASB) security solution is the only way an organization can ensure that no such apps are used by employees.

Taking advantage of legitimate platform features

Business software usage is critical for productivity. Cyber criminals know this and take advantage of legitimate software platform features to infect computers. For example, during the last quarter of 2017, the Windows Defender Security Intelligence team detected some incidents in which hackers used legitimate business software to stay "under the radar" as they phished users and infected computers. The following is an example of this threat.

Microsoft Windows Dynamic Data Exchange (DDE) is a feature that facilitates the electronic transfer of Office files using shared memory and data. In early October 2017, it was publicly shared that a new variant of Locky ransomware is delivered through abusive use of DDE (Microsoft published a security update in December 2017 that disables DDE in all supported editions of Word and Excel by default.) The Microsoft Windows Defender Security Intelligence team also saw additional examples of this attack, and we share one such example in this report.

Analysis and explanation

From early October through November 2017, there was an emergence of hackers exploiting DDE by using techniques to execute malware on an unsuspecting end user's computer. In one particular case, a Word document was attached to a malicious spam email. After the user clicked to open the attachment and responded affirmatively to a series of pop-up dialog boxes prompting for an action to be taken by the software application, a DDE attack pulled in a malicious payload (such as Locky ransomware) and ran it on the computer. The problem lies in users interacting with content delivered via a legitimate software platform without realizing that there is malicious intent.

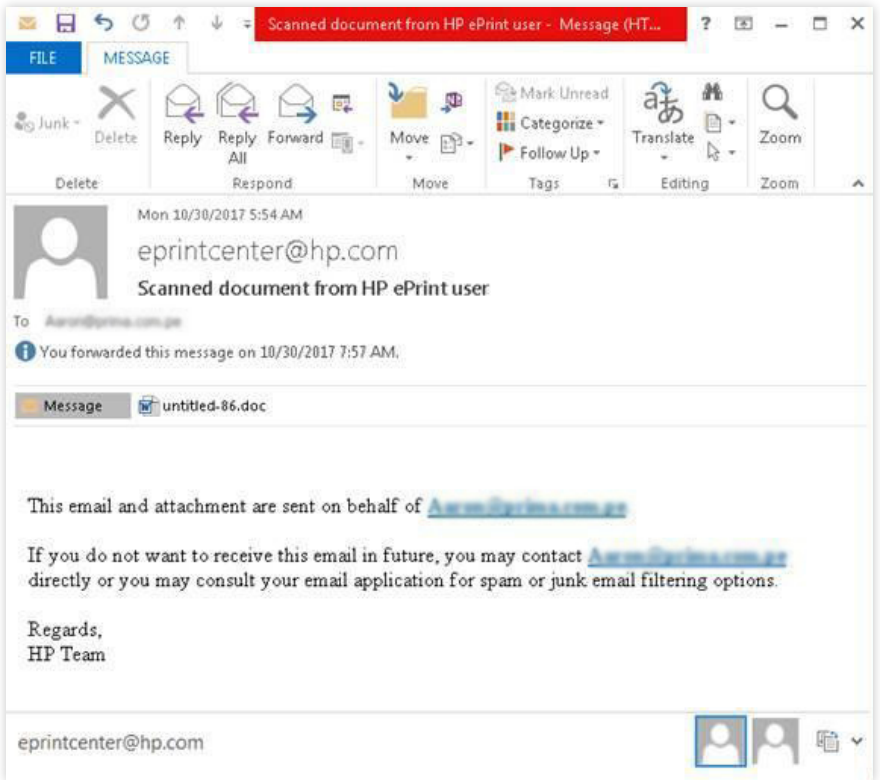


***Figure 14**: Example of a malicious spam email with attachment that delivers Locky ransomware by leveraging DDE functionality.*

Solutions and recommendations

Microsoft provides malware protection by default in newer versions of Windows, such as Windows 10, for the malicious payloads associated with DDE attacks. We also recommend the following best practices:

Protect your computer

We continue to encourage customers to follow the basic guidance to protect their computers by enabling a firewall, installing antivirus software and getting software updates (on-premise and cloud-based security updates).

Keep operating system software updated

You should apply the latest operating system software security updates to help make sure your computer is as protected as possible. If you are not sure whether the software is up to date, visit the vendor web site for viewing the latest software updates, scan the computer for available updates, and install any high-priority updates that are offered to you. Even if you have automatic software updates enabled and configured for your computer, and the updates are delivered to you when they are released, you should verify that they are installed.

SECTION 3

Wrestling ransomware

Cyber criminals run a business and for any business, money is a critical resource. Hence, ransomware continues to be a popular method used by cybercriminals to solicit and in several cases, successfully obtain money (bitcoin or other form) from victims. In exchange for the ransom, attackers typically offer to give the victim the private key necessary to decrypt the data, or otherwise restore the victim's access to the computer—a promise they frequently do not fulfill, even when paid. Ransomware was one of the most prominent types of malware being distributed by the Gamarue botnet described earlier in the report. Ransomware is also being used as an infection vector in some of the low-hanging fruit channels mentioned in the report, such as phishing emails and legitimate software platforms.

Analysis and explanation

The following ransomware trends were identified for the period February – December 2017:

- The geographical region with the greatest number of ransomware encounters was Asia.
- Three global outbreaks (WannaCrypt, Petya/NotPetya, and BadRabbit) showed the force of ransomware in making real-world impact. They affected corporate networks and brought down critical services such as hospitals, transportation, and traffic systems.
- The three most encountered ransomware families were Win32/WannaCrypt,Win32/LockScreen, and Win32/Cerber.
- Locations with the highest ransomware encounter rates include Myanmar (0.48 percent), Bangladesh (0.36 percent), and Venezuela (0.33 percent).
- Locations with the lowest ransomware encounter rates include Japan, Finland, and the United States, all of which had an average monthly ransomware encounter rate of 0.03 percent.

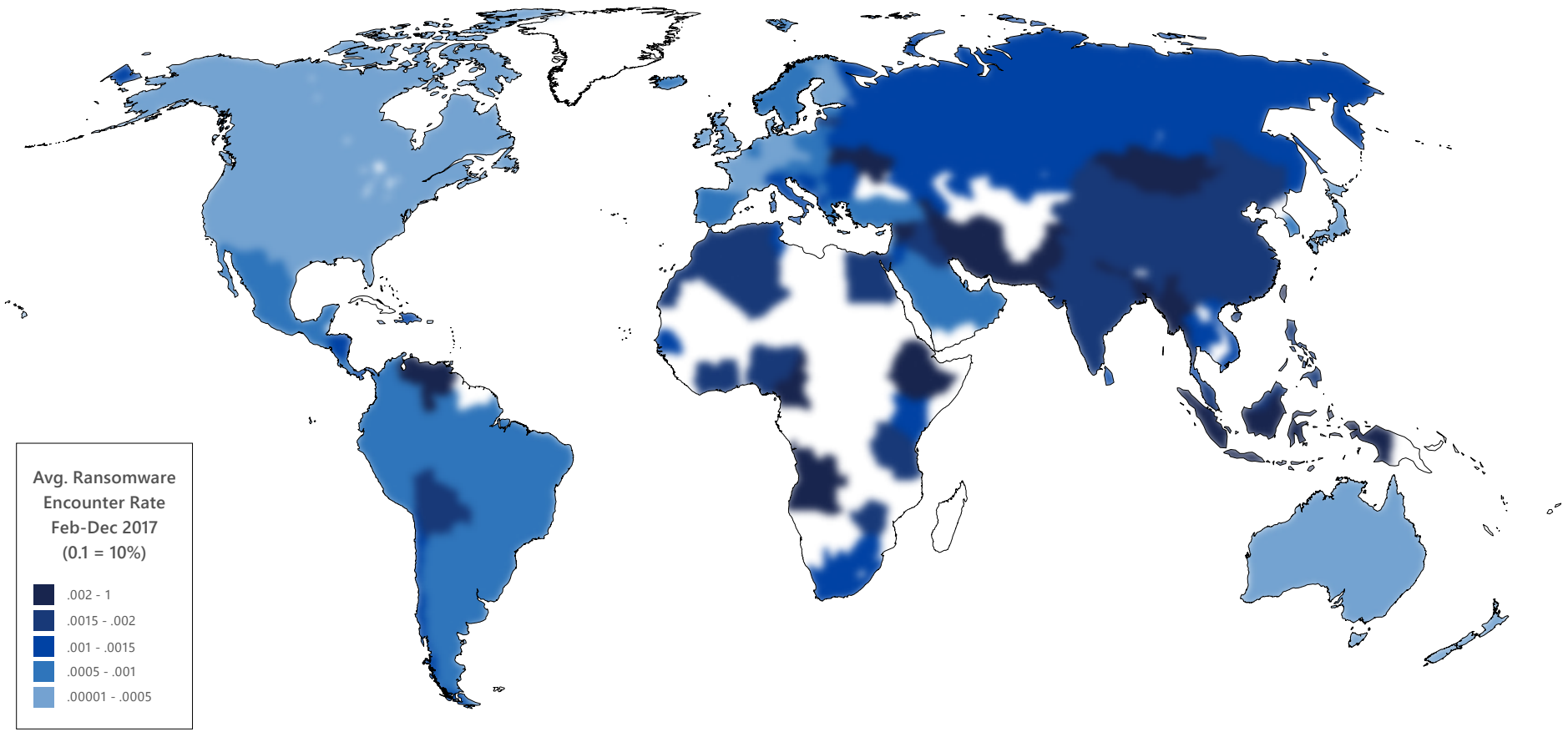


***Figure 17**: Encounter rates for ransomware families by country/region, February–December 2017*

- Win32/LockScreen, the most widely encountered ransomware family in 2017, displays a full-screen message that prevents the user from accessing the desktop, and demands that the user pay a fine in the form of an SMS message sent to a premium number in order to regain control of the computer. LockScreen primarily affects Android. We are finding Android malware on Windows machines. This can happen if, for example, Android users sync their phones or download Android applications in Windows and do side loading of the applications that are not sanctioned (for example, not sourced from the official Google Play store). The Southeast Asia region tends to have a higher adoption rate of Android, which would explain the greater number of encounters in that region.
- Win32/WannaCrypt (also known as WannaCry) emerged in early 2017 to target a vulnerability in Windows that Microsoft had previously addressed with Security Bulletin MS17-010.
- Win32/Cerber is often spread via the RIG (Meadgive) and Magnitude (Pangimop) exploit kits. Cerber is a ransomware-as-a-service family, sold to prospective attackers by its creators and designed to be easy to use by novices.

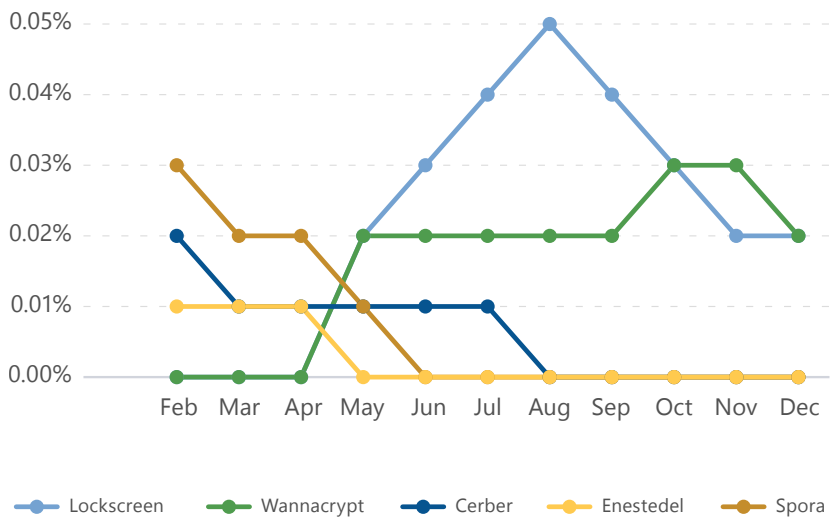


***Figure 18**: Trends for several commonly encountered ransomware families, February–December 2017*

The impact from rapid, destructive attacks such as WannaCrypt and Petya/NotPetya was unprecedented. Victims of either of these and of Bad Rabbit ransomware attacks will lose access to files, often indefinitely.

WannaCrypt used EternalBlue, an exploit for a previously fixed SMBv1 vulnerability, to propagate itself across networks rapidly, affecting a large number of computers in a short time. (Microsoft released Security Bulletin MS17-010 in March of 2017 to address the vulnerability.)

Petya (Ransom:Win32/Petya.B) used the same exploit that gave WannaCrypt its spreading capabilities, and added more propagation and infection methods to create arguably the most complex ransomware in 2017. Petya's initial infection vector was a compromised software supply chain, but the ransomware quickly spread using the EternalBlue and EternalRomance exploits, as well as a module for lateral movement using stolen credentials.

Bad Rabbit ransomware (Ransom:Win32/Tibbar.A) infected devices by posing as an Adobe Flash installer available for download on compromised websites. Like WannaCry and Petya, Bad Rabbit had spreading capabilities, albeit more traditional: it used a hardcoded list of user names and passwords. Like Petya, it can also render infected devices unbootable because it encrypts entire disks in addition to encrypting files.

Solutions and recommendations

Backup your data

The importance of backing up files to be able to recover in case of a ransomware attack cannot be overstated. Be sure to create destruction-resistant backups of your critical systems and data. There are many tools and services available for file backup, restoration (of previous file versions), and recovery. Also, be sure to regularly test that the backups are working.

Apply multi-layered security defenses

Use an email security solution/service that scans suspicious email attachments and ideally protects at the time a user clicks on an attachment, such as by quarantining a suspicious attachment for further investigation. At minimum, antivirus software can help detect and block the download and installation of some ransomware.
To detect and mitigate the impact of sophisticated ransomware, additional protection is required. Advanced threat protection that applies machine learning and artificial intelligence technologies to evaluate files to be able to detect suspected malware can help.

Keep all software up-to-date

To minimize the entry points for ransomware, be sure to keep all software updated, including operating system, web browser, web browser plug-ins (only use those that are required for business purposes), and security software. Also prioritize patching new releases to enable stronger protection from vulnerabilities.

Isolate or retire certain computers

If some computers cannot be patched or updated with the latest software, to minimize the footprint of exposure to a ransomware attack and infection, isolate or retire those computers.

Manage and control privileged access to data

To minimize risk of credential compromise and abuse, implement unique local administrator passwords on all systems, separate and protect privileged accounts, and reduce broad permissions on file repositories.

Additional noteworthy threat intelligence

The data that informs the proceeding topics comes in part from continued tracking of threats observed from Microsoft Azure cloud services and Windows endpoints worldwide. A broader look at that threat tracking information follows.

Cloud threat intelligence

Cloud services such as Microsoft Azure are perennial targets for attackers seeking to compromise and weaponize virtual machines and other services. In a cloud weaponization threat scenario, an attacker establishes a foothold within a cloud infrastructure by compromising and taking control of one or more virtual machines. The attacker can then use these virtual machines to launch attacks, including brute force attacks against other virtual machines, spam campaigns that can be used for email phishing attacks, reconnaissance such as port scanning to identify new attack targets, and other malicious activities. The following two figures show where incoming and outgoing attacks originate from.

Nearly two-thirds of incoming attacks on Azure services in 2H17 came from IP addresses in China, the United States, and Russia, at 31.7 percent, 18.0 percent, and 15.9 percent, respectively. France was fourth at 6.7 percent, with no other country or region accounting for more than 5 percent of the total.

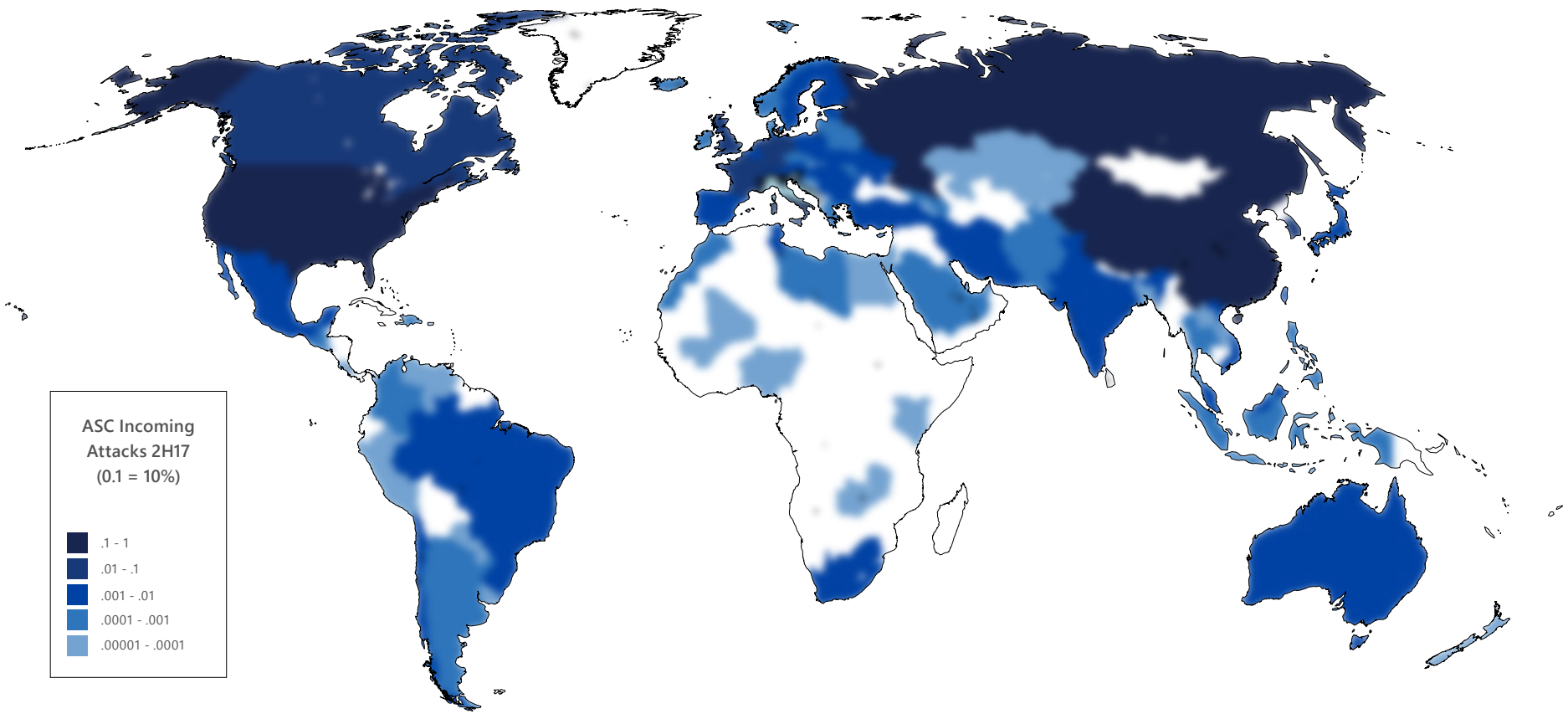


***Figure 19**: Incoming attacks detected by Azure Security Center in 2H17, by country/region of origin*

Compromised virtual machines often communicate with command-and-control (C&C) servers at known malicious IP addresses to receive instructions. 54 percent of the malicious IP addresses contacted by compromised Azure virtual machines in 2H17 were located in China, followed by the United States at 22 percent.

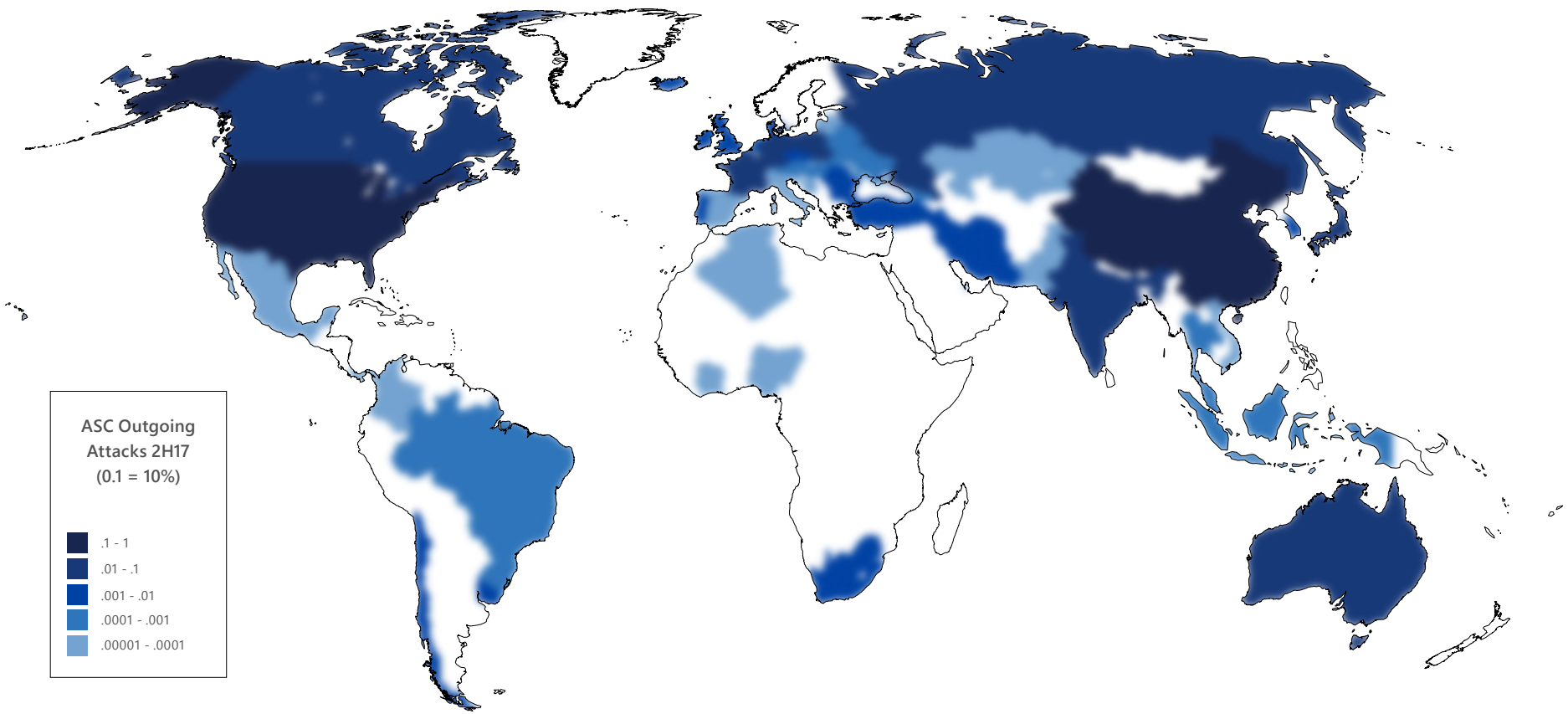


***Figure 20**: Outgoing communication to malicious IP addresses detected by Azure Security Center in 2H17, by address location*

Drive-by-download sites

Significant locations with high concentrations of drive-by download URLs included Taiwan, with an average of 6.4 drive-by URLs for every 1,000 URLs tracked by Bing; Iran, with 1.4; and the United Arab Emirates, with 1.3.

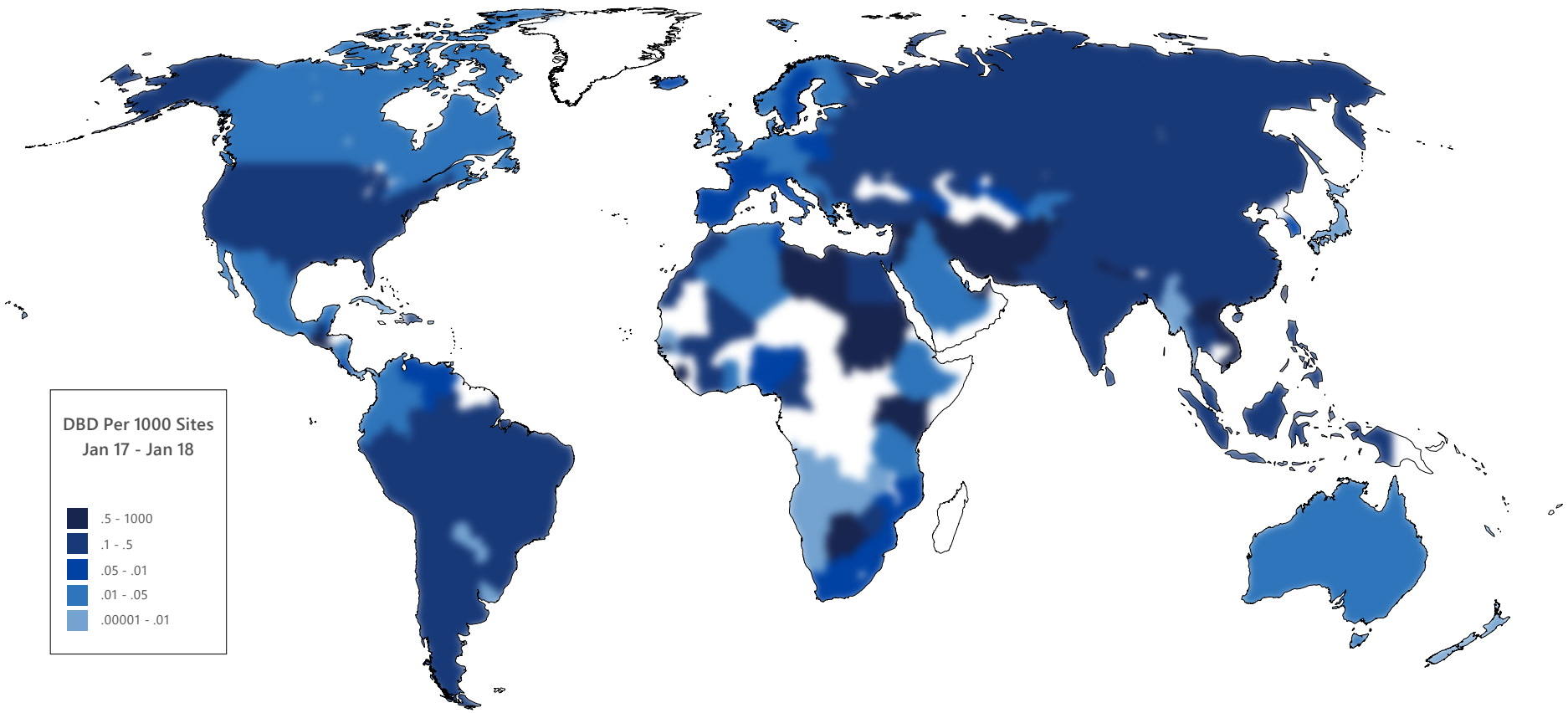


Figure 21: Monthly average number of drive-by download pages indexed by Bing from January 2017 through January 2018, per 1,000 URLs in each country/region

Endpoint threat intelligence

Malicious and unwanted software

Encounter rate, in the following figures, is the percentage of computers running Microsoft real-time security products that report a malware encounter.[1] For example, the average monthly encounter rate in Canada between February 2017 and January 2018 was 14.2 percent. This data means that, of the computers in Canada that were running Microsoft real-time security software during the period, 14.2 percent reported encountering malware, and 85.8 percent did not. Encountering a threat does not mean the computer has been infected. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.

[1]Encounter rate does not include threats that are blocked by a web browser before being detected by antimalware software. In particular, **IExtensionValidation** in Internet Explorer 11 enables security software to block pages that contain exploits from loading. For this reason, encounter rate figures may not fully reflect all of the threats encountered by computer users.

- Locations with high encounter rates included Pakistan, Nepal, Bangladesh, and Ukraine, all of which had an average monthly encounter rate of 33.2 percent or higher in 2017.
- Locations with low encounter rates included Finland, Denmark, Ireland, and the United States, all of which had an average monthly encounter rate of 11.4 percent or lower in 2017.

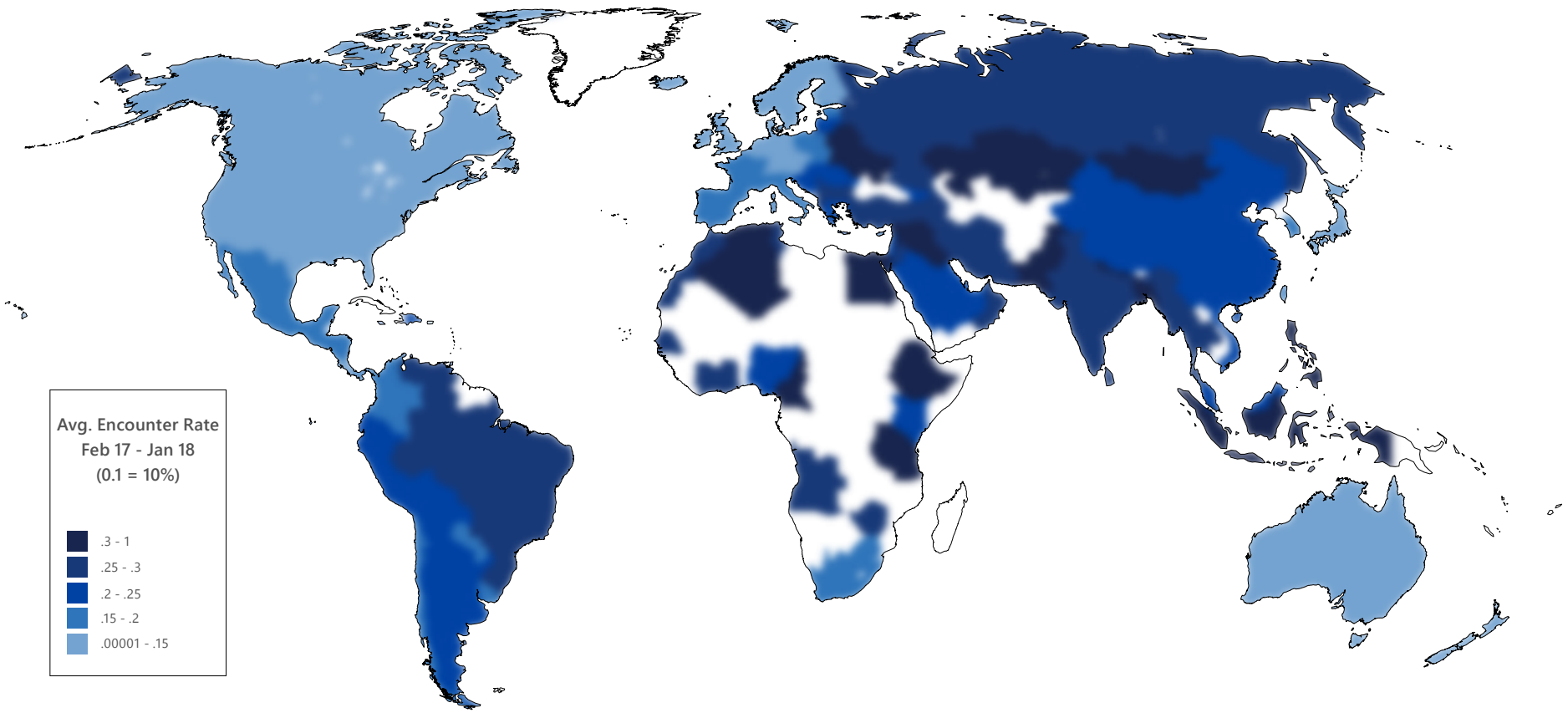


***Figure 21**: Encounter rates by country/region, February 2017–January 2018*

Windows Defender Security Intelligence (WDSI) classifies individual threats into types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the Microsoft Security Intelligence Report groups these types into categories based on similarities in function and purpose.

- Trojans were the most commonly encountered category of malicious software each month in 2017 by a large margin, led by several generic and cloud-based detections for a variety of threats.
- Encounter rates for other categories were much lower and more consistent from month to month.

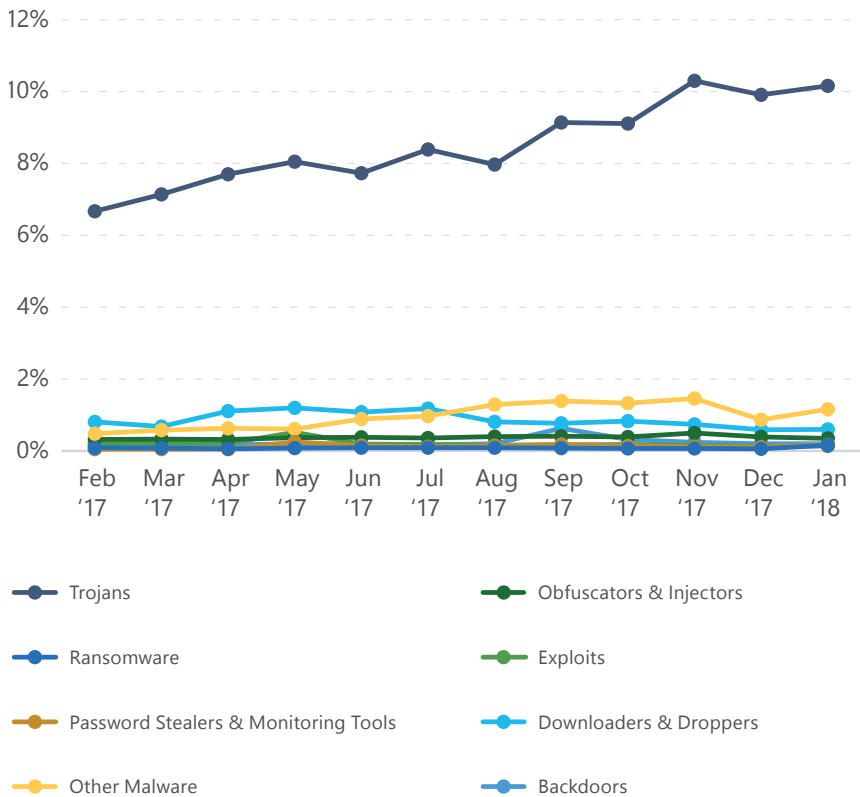


***Figure 22**: Encounter rates for malicious software categories, February 2017–January 2018*

- Browser modifiers were the most commonly encountered category of unwanted software for the period February 2017 – January 2018, led by Win32/Foxiebro and Win32/Obrypser.
- Software bundlers were the second most commonly encountered category of unwanted software for the period February 2017 – January 2018, led by Win32/Prepscram.
- Adware encounters were significantly less common than the other unwanted software categories, led by Win32/Adposhel.

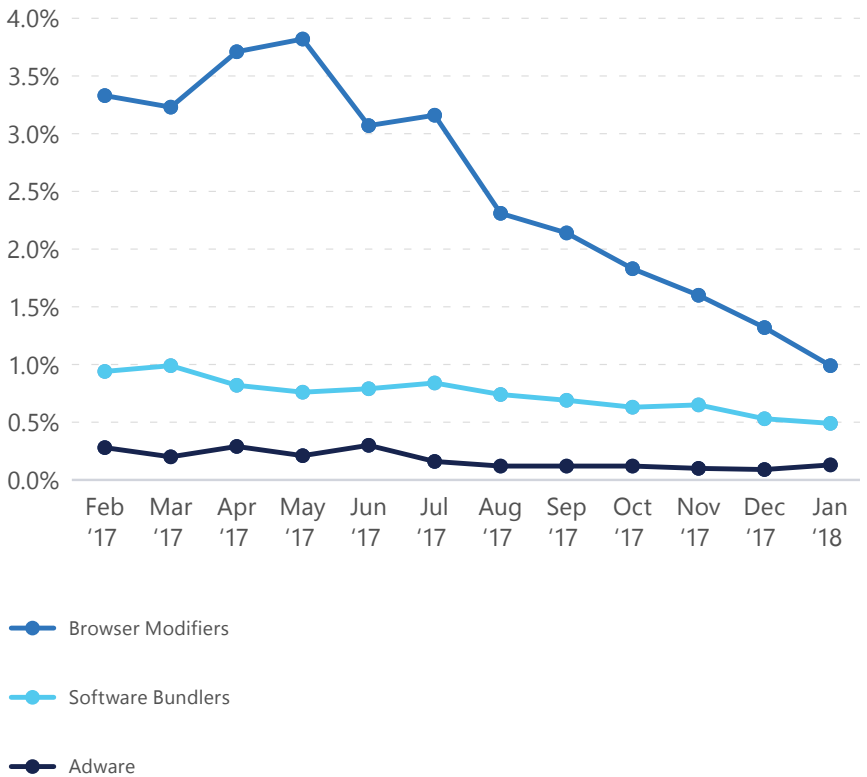


***Figure 23**: Encounter rates for unwanted software categories, February 2017–January 2018*

The next two figures show trends for the top malicious software families that were detected on computers by Microsoft real-time antimalware products worldwide.

- Win32/Fuery is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender. For more information about the feature and guidance for administering it in network environments, see the article "Block at First Sight" at technet.microsoft.com, and the entry "Windows Defender Antivirus cloud protection service: Advanced real-time defense against never-before-seen malware" (July 18, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc.
- Win32/Skeeyah and Win32/Dynamer are generic detections for a variety of trojans that share certain characteristics.
- VBS/Mutuodo, the most common malicious software family worldwide in November, is a trojan that launches executable files related to the Win32/Prifou family of browser modifiers.
- HTML/Brocoiner is a JavaScript cryptocurrency miner that has been found on both malicious and compromised websites, including sites that offer streaming videos, adult content, and online shopping. When a webpage containing the JavaScript is loaded, it automatically starts to mine for Monero or other cryptocurrency. This mining activity, often initiated without user consent, consumes resources and can slow down affected computers.

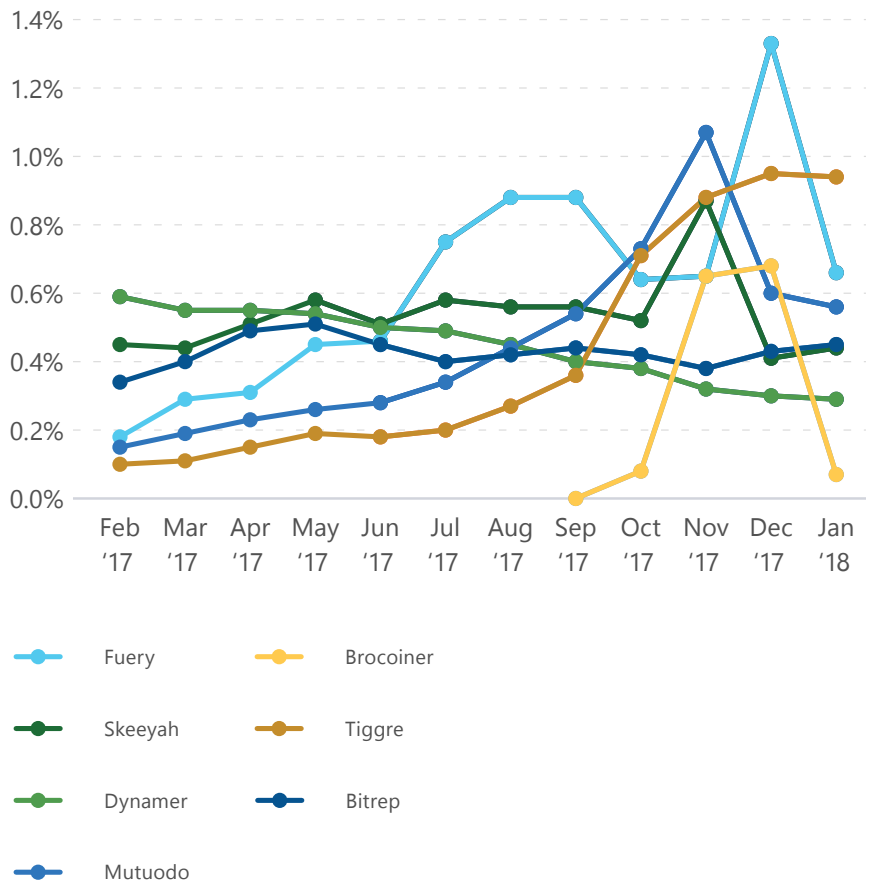


***Figure 24**: Encounter rate trends for the top malicious software families, February 2017–January 2018*

- The most commonly encountered unwanted software families were all browser modifiers.
- Win32/Prifou is a browser modifier that is installed when the user downloads other software from certain third-party websites. It displays ads while the user browses, attributed to "Price Fountain."
- Win32/Foxiebro is a browser modifier that can inject ads to search results pages, modify web pages to insert ads, and open ads in new tabs.

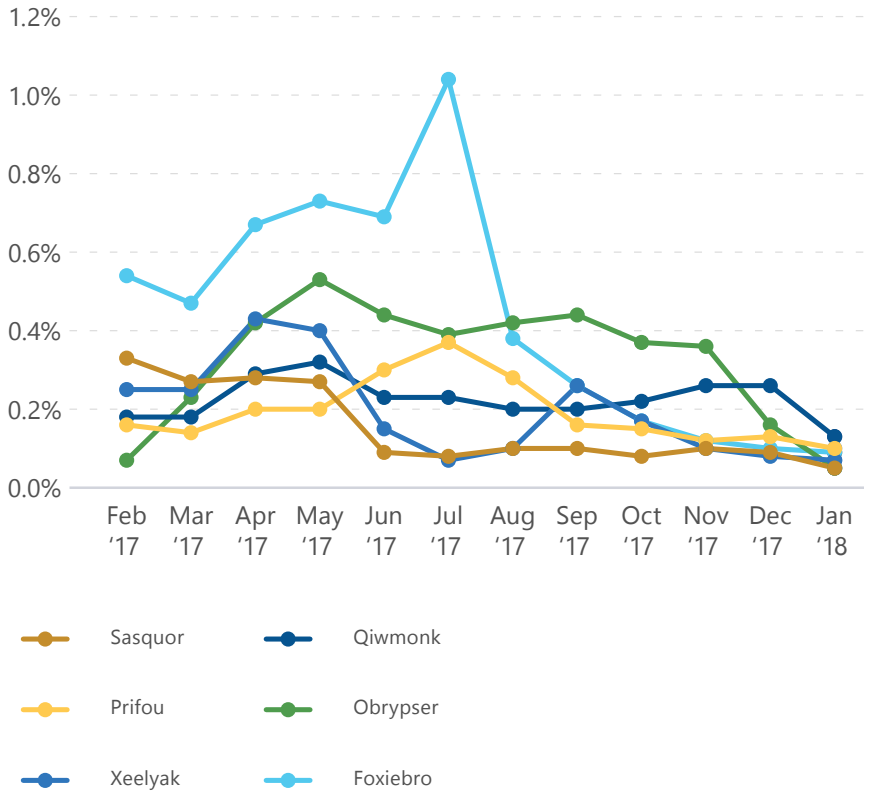


***Figure 25**: Encounter rate trends for the top unwanted software families, February 2017–January 2018*

Malicious websites

Microsoft Edge and recent versions of Microsoft Internet Explorer include SmartScreen Filter, a feature that checks web requests against a blacklist of known malicious websites and blocks access to them by default. Malicious websites include both phishing sites, which masquerade as legitimate sites to trick users into entering sensitive information, and sites that host and distribute malware.

An impression is a single instance of a user attempting to visit a known phishing site with SmartScreen Filter enabled and being warned, as shown in the Figure 26.

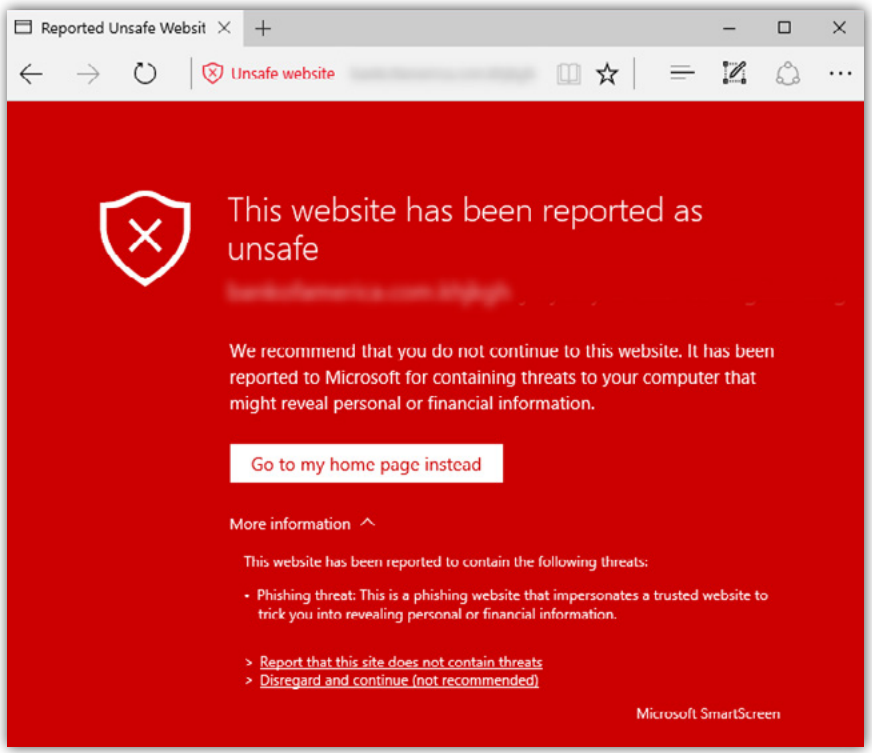


Figure 26: SmartScreen Filter in Microsoft Edge and Internet Explorer blocks reported phishing and malware distribution sites to protect users

- SmartScreen detected 5.8 phishing sites per 1,000 Internet hosts worldwide in 2H17.
- Locations hosting higher than average concentrations of phishing sites include Ukraine (19.1 per 1,000 Internet hosts in 2H17), Belarus (12.3), Bulgaria (12.2), and Indonesia (10.8). Locations with low concentrations of phishing sites included Taiwan (0.7), China (0.8), Mexico (0.8), and Korea (1.0).

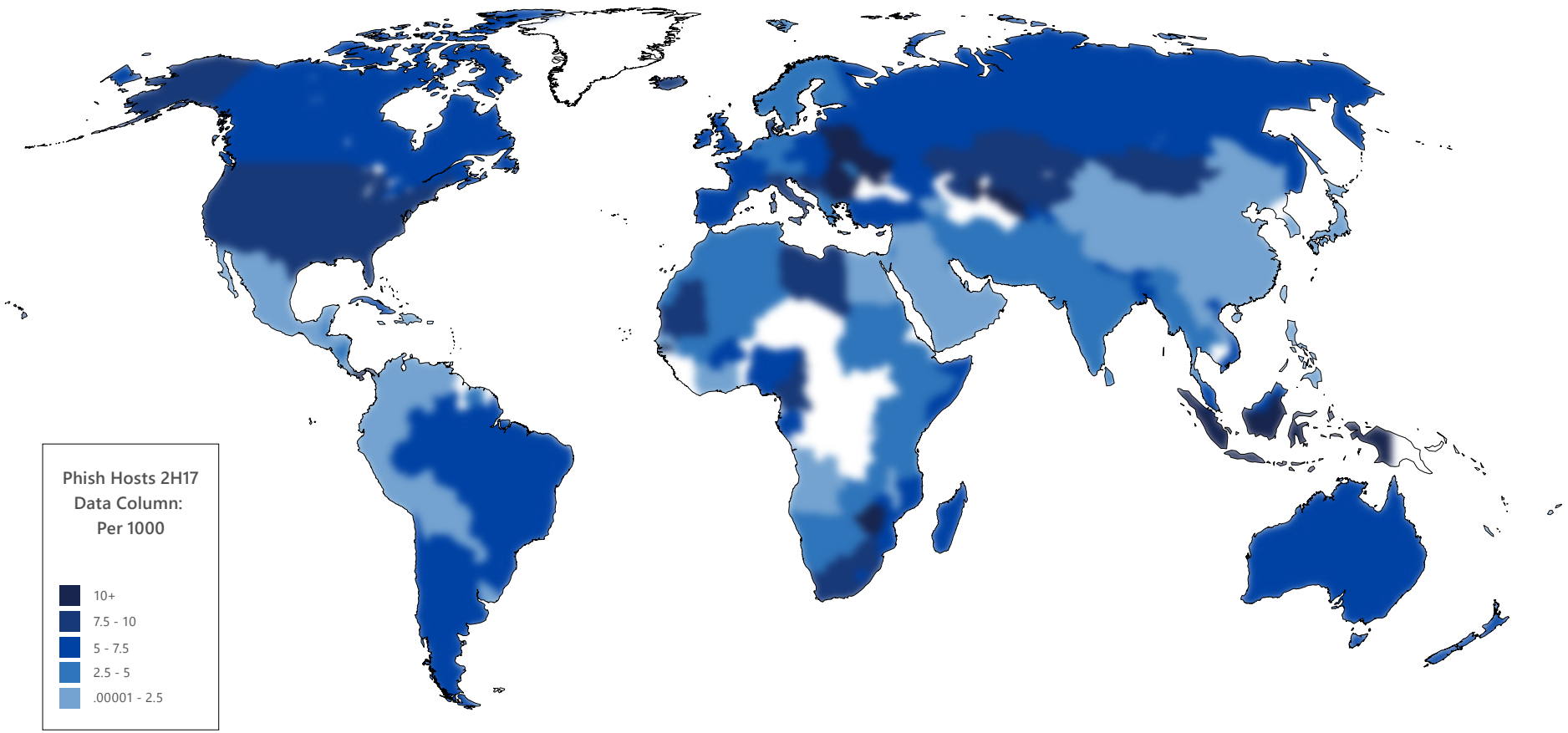


Figure 27: Phishing sites per 1,000 Internet hosts for locations around the world in 2H17

- SmartScreen reported 11.7 phishing impressions per 1,000,000 pageviews in 2H17.
- Locations with unusually high rates of phishing impressions included Albania (188.5 phishing impressions per 1,000,000 pageviews in 2H17), Armenia (186.5), and Iceland (77.9).
- Locations with unusually low rates of phishing impressions included Korea (1.0 impressions per 1,000,000 pageviews in 2H17), Japan (1.7), and China (1.9).

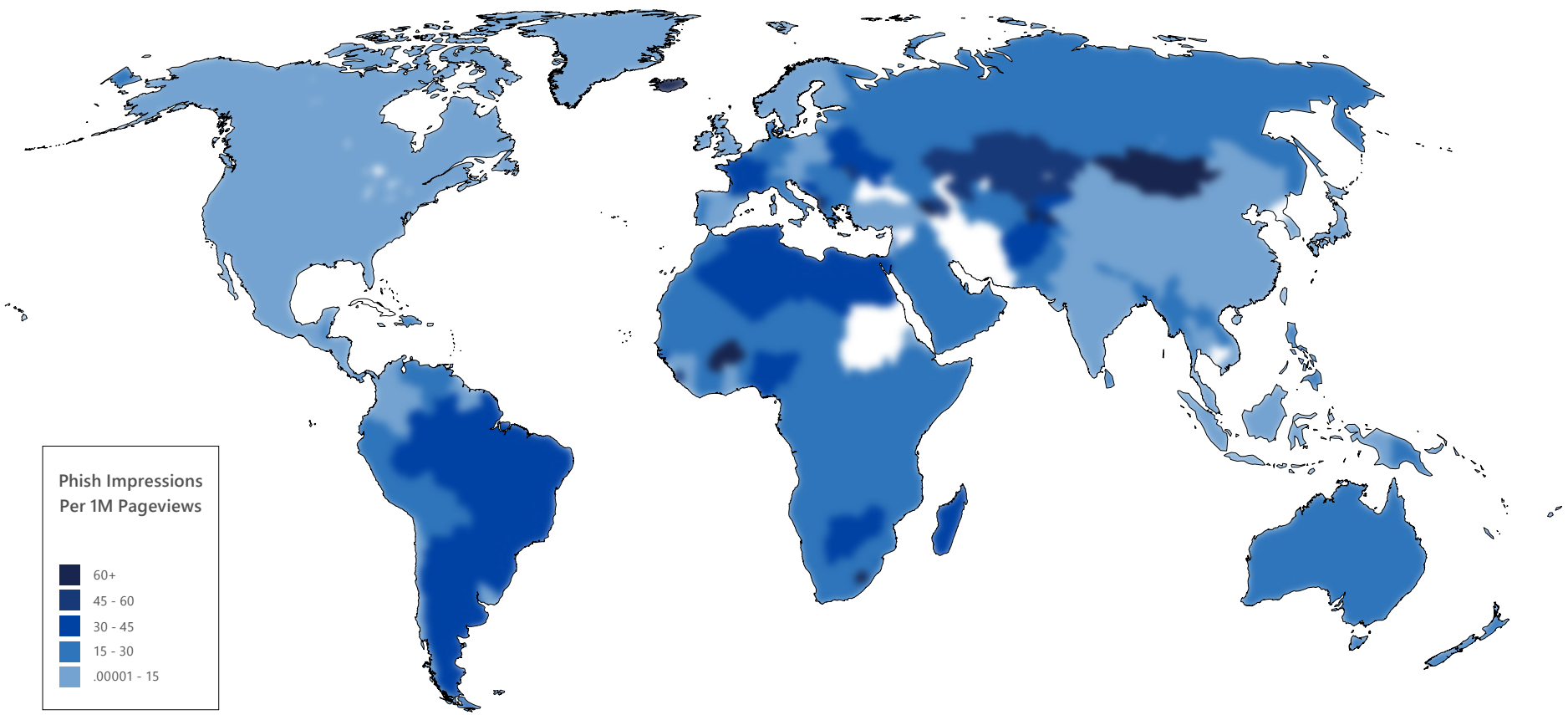


***Figure 28**: Phishing impressions by client location per 1,000,000 pageviews in 2H17*

- SmartScreen detected 12.1 malware hosting sites per 1,000 Internet hosts worldwide in 2H17.
- China, which had one of the lowest concentrations of phishing sites in the world (0.8 phishing sites per 1,000 Internet hosts in 2H17), had one of the highest concentrations of malware hosting sites (32.5 malware hosting sites per 1,000 hosts in 2H17). Other locations with high concentrations of malware hosting sites included Singapore (21.6), Russia (14.0), and Hong Kong SAR (14.0). Locations with low concentrations of malware hosting sites included Taiwan (3.4), Austria (3.4), and Mexico (3.5).

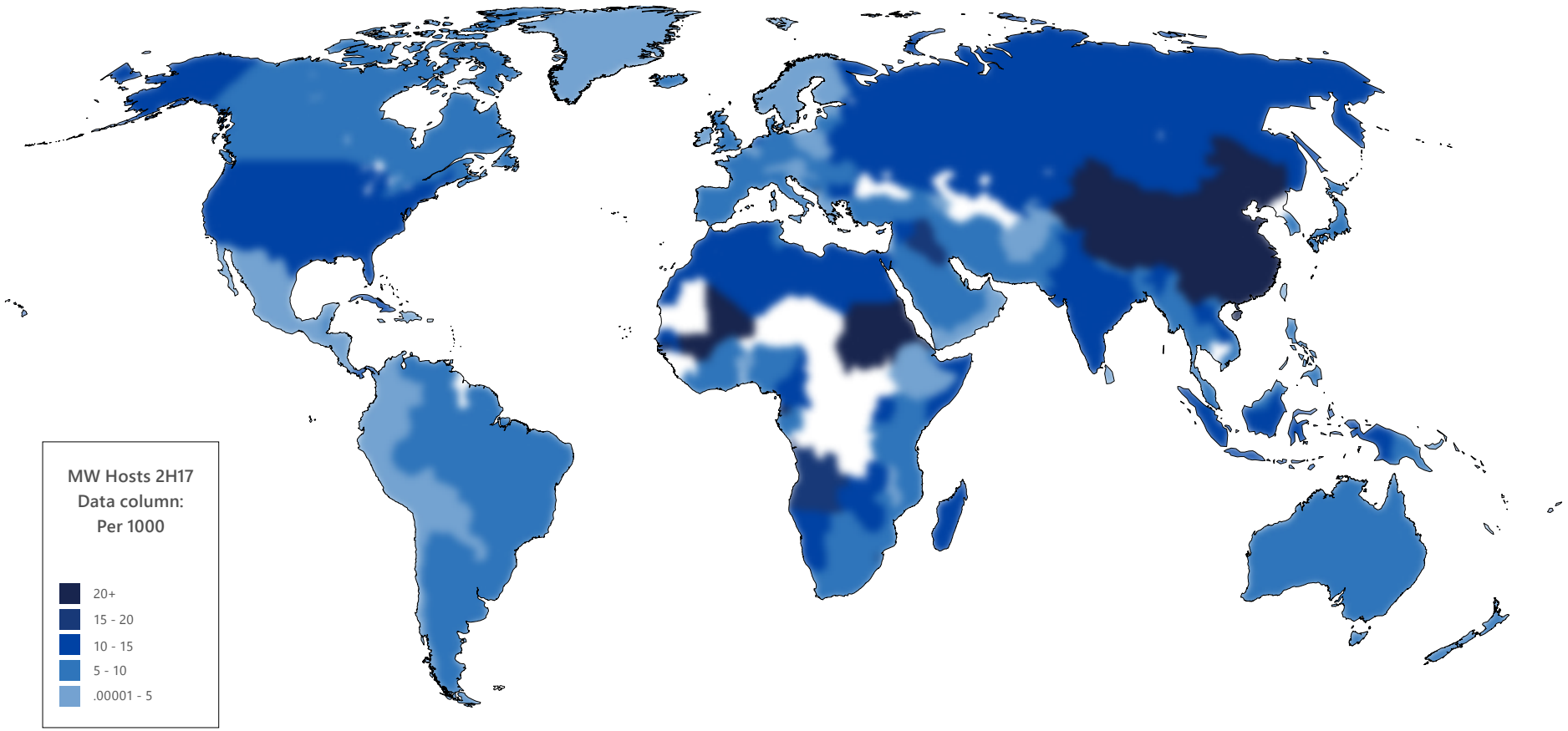


***Figure 29**: Malware distribution sites per 1,000 Internet hosts for locations around the world in 2H17*

- Malware impressions were much more common than phishing impressions in 2H17. SmartScreen reported 190.0 malware impressions per 1,000,000 pageviews in 2H17, compared to 11.7 phishing attempts per 1,000,000 pageviews.
- Locations that were heavily affected by malware impressions included Egypt (754.4 malware impressions per 1,000,000 pageviews in 2H17), Peru (680.2), and Hungary (623.5).
- Locations with unusually low malware impression rates included Korea (20.0), Japan (64.1), and Iceland (96.3).

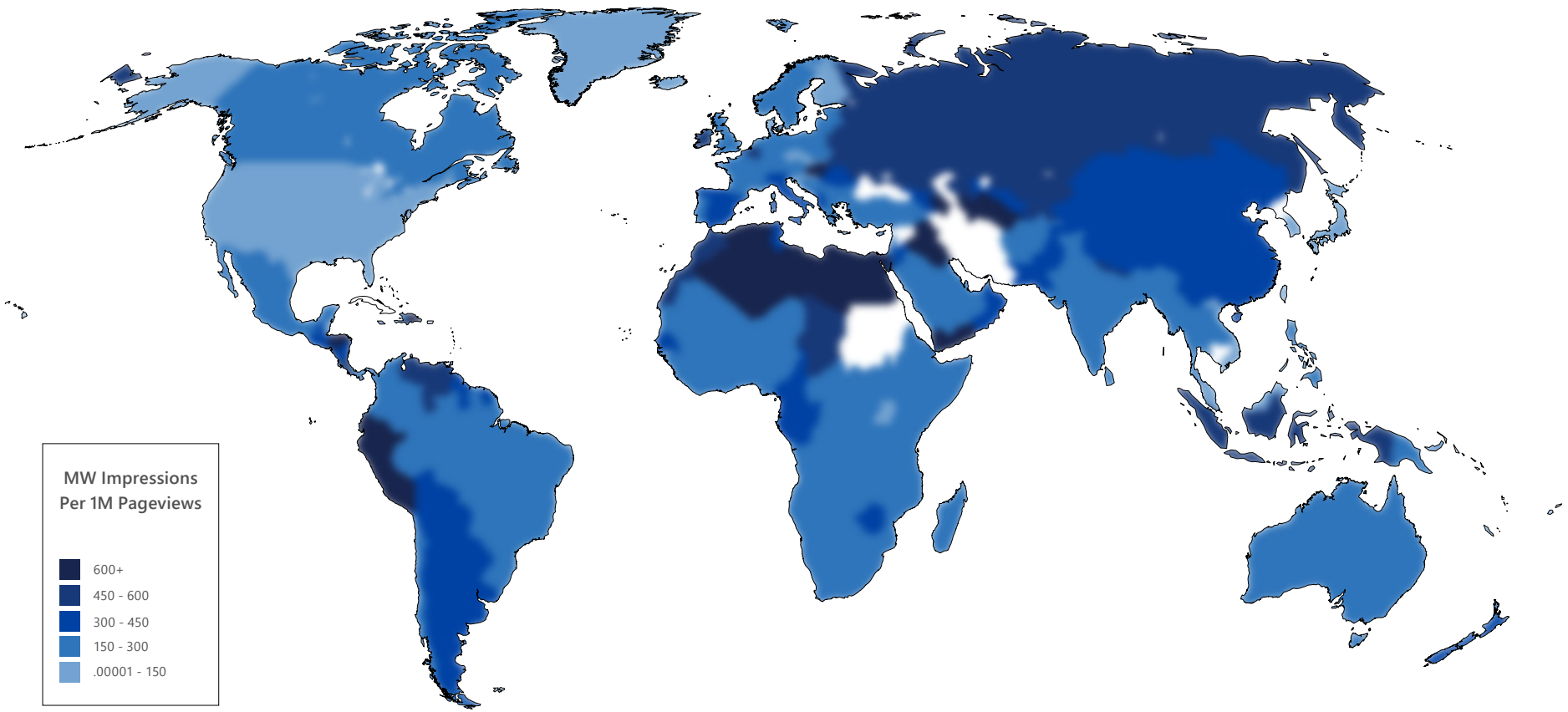


***Figure 30**: Malware impressions by client location per 1,000,000 pageviews in 2H17*

Conclusion

The past year has shown us the significant impact of the Gamarue botnet on computers worldwide; cyber criminals leveraging less sophisticated methods to infect machines and in some cases, extort ransoms from victims; and ransomware being used in a wide range of cybercrime activity, including email phishing campaigns and destructive attacks like WannaCrypt. Organizations that adopt security hygiene methods, security solutions, and best practices, have cyber resilience and incident response plans and employ the right mix of people and processes for dealing with the various threat scenarios and attacks described could at least minimize damage and impact from them.

Microsoft is a trusted security advisor and partner to large global organizations. To learn more about our security offerings, visit www.microsoft.com/security and check out the Microsoft Security Blog for our perspectives on additional trending threats and topics.

Authors and Contributors

Abhijeet Hatekar
Information and Threat Protection

Abhishek Agrawal
Information Protection

Christopher Coy
Digital Crimes Unit

Daniel Kondratyuk
Identity Security and Protection Team

Diana Kelley
Enterprise Cybersecurity Group

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender Research Team

Eric Douglas
Windows Defender Research Team

Francis Tan Seng
Windows Defender Research Team

John Dellinger
Microsoft Threat Intelligence

Jonathan San Jose
Windows Defender Research Team

Karthik Selvaraj
Windows Defender Research Team

Kasia Kaplinska
Microsoft Security Marketing

Mark Simos
Enterprise Cybersecurity Group

Matt Duncan
Windows Active Defense Data Engineering and Analytics

Meths Ferrer
Windows Active Defense

Paul Henry
Wadeware LLC

Prachi Rathee
Windows Active Defense Data Engineering and Analytics

Rodel Finones
Digital Crimes Unit

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Enterprise Cybersecurity Group

Tanmay Ganacharya
Windows Defender Research Team

Tim Kerk
Windows Defender Research Team

Tomer Teller
Azure Security

Vishant Patel
Digital Crimes Unit

Volv Grebennikov
Bing

Yiftach Keshet
Microsoft Cloud App Security Research Team

Yinon Costica
Microsoft Cloud App Security Research Team

Zheng Dong
Windows Defender ATP Research

Data sources

Data included in the Microsoft Security Intelligence Report is gathered from a wide range of Microsoft products and services whose users have opted in to provide usage data. The scale and scope of this telemetry data allows the report to deliver the most comprehensive and detailed perspective on the threat landscape that is available in the software industry:

- Azure Security Center is a service that helps organizations prevent, detect, and respond to threats by providing increased visibility into the security of cloud workloads and using advanced analytics and threat intelligence to detect attacks.
- Bing, the search and decision engine from Microsoft, contains technology that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users about it to help prevent infection.
- Exchange Online is the Microsoft-hosted email service for business. Exchange Online antimalware and antispam services scan billions of messages every year to identify and block spam and malware.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove specific prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed more than 600 million times each month on average in 2017. The MSRT is not a replacement for an up-to-date real-time antivirus solution.

- The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove malware and other malicious software. The Microsoft Safety Scanner is not a replacement for an up-to-date antivirus solution, because it does not offer real-time protection and cannot prevent a computer from becoming infected.
- Microsoft Security Essentials is a free, easy-to-download real-time protection product that provides basic, effective antivirus and antispyware protection for Windows Vista and Windows 7.
- Microsoft System Center Endpoint Protection (formerly Forefront Client Security and Forefront Endpoint Protection) is a unified product that provides protection from malware and unwanted software for enterprise desktops, laptops, and server operating systems. It uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.
- Office 365 is the Microsoft Office subscription service for business and home users. Select business plans include access to Office 365 Advanced Threat Protection.
- Windows Defender in Windows 8, Windows 8.1, and Windows 10 provides real-time scanning and removal of malware and unwanted software.
- Windows Defender Advanced Threat Protection is a new service built into Windows 10 Anniversary Update that enables enterprise customers to detect, investigate, and remediate advanced persistent threats and data breaches on their networks.
- Windows Defender Offline is a downloadable tool that can be used to create a bootable CD, DVD, or USB flash drive to scan a computer for malware and other threats. It does not offer real-time protection and is not a substitute for an up-to-date antimalware solution.
- Windows Defender SmartScreen, a feature in Microsoft Edge and Internet Explorer, offers users protection against phishing sites and sites that host malware. Microsoft maintains a database of phishing and malware sites reported by users of Microsoft Edge, Internet Explorer, and other Microsoft products and services. When a user attempts to visit a site in the database with the filter enabled, the browser displays a warning and blocks navigation to the page.

Product or service	Privacy statement URL
Azure/Azure Security Center	privacy.microsoft.com/en-us/privacystatement/
Bing	privacy.microsoft.com/en-us/privacystatement/
Exchange Online, Office 365	privacy.microsoft.com/en-us/privacystatement
Internet Explorer 11	privacy.microsoft.com/en-us/internet-explorer-ie11-preview-privacy-statement
Malicious Software Removal Tool	www.microsoft.com/en-us/safety/pc-security/msrt-privacy.aspx
Microsoft Edge	privacy.microsoft.com/en-us/privacystatement/
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/privacy.aspx
Microsoft Security Essentials	windows.microsoft.com/en-us/windows/security-essentials-privacy
System Center Endpoint Protection	www.microsoft.com/privacystatement/en-us/SystemCenter2012R2/Default.aspx#tilepspSystemCenter2012R2EndpointProtectionModule
Windows Defender in Windows 10	privacy.microsoft.com/en-us/privacystatement/
Windows Defender Offline	privacy.microsoft.com/en-us/windows-defender-offline-privacy

***Figure 31**: US privacy statements for the Microsoft products and services used in this report*

Glossary of Threat Definitions

To learn about some of the threat families described in this report and others, please visit:

https://www.microsoft.com/en-us/wdsi/threats