MICROSOFT SECURITY INTELLIGENCE REPORT

VOLUME 24
JANUARY – DECEMBER 2018

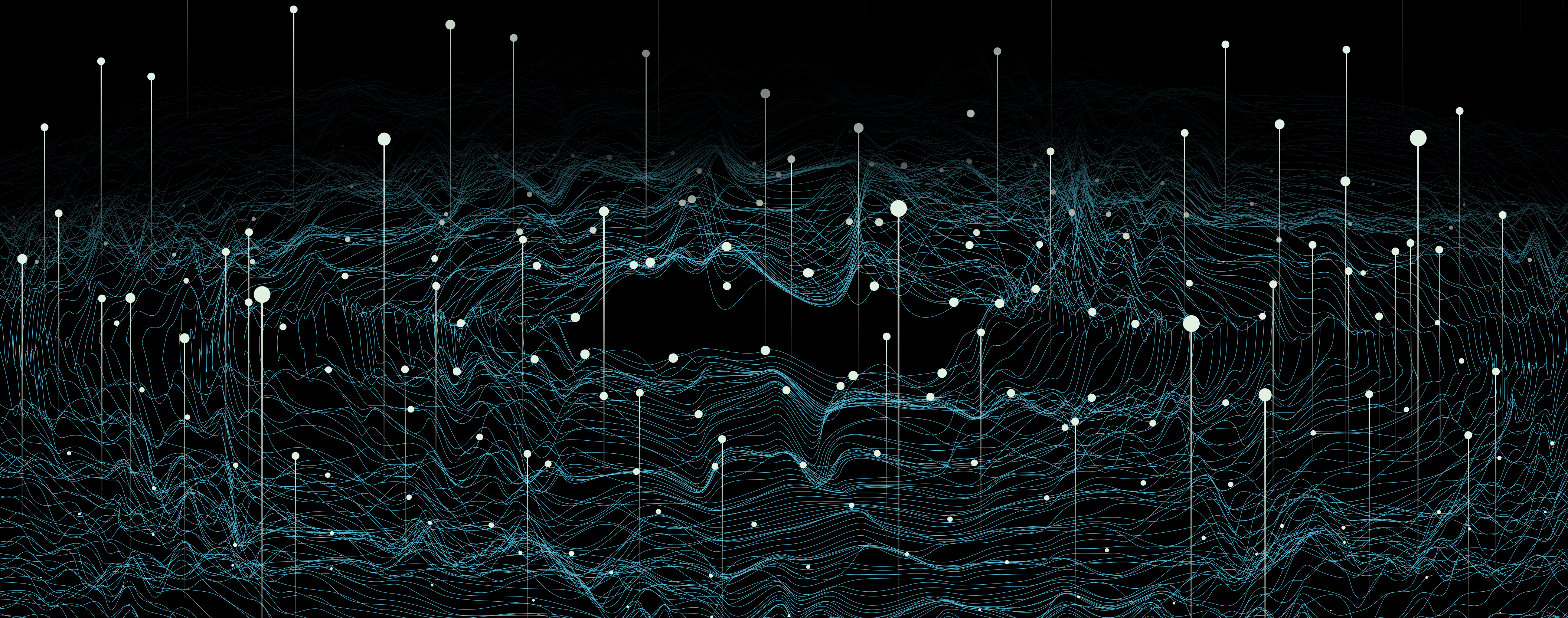


Table of contents

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Authors and contributors

Abhishek Agrawal
Information Protection

David Fantham
Information Protection

Debraj Ghosh
Microsoft Security Marketing

Diana Kelley
Cybersecurity Solutions 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

Jonathan Trull
Cybersecurity Solutions Group

Joram Borenstein
Cybersecurity Solutions Group

Karthik Selvaraj
Windows Defender Research Team

Kasia Kaplinska
Microsoft Security Marketing

Kristina Laidler
Security Incident Response

Matt Duncan
Windows Active Defense Data Engineering and Analytic

Mark Simos
Cybersecurity Solutions Group

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft Security Marketing

Ram Pliskin
Azure Security

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Cybersecurity Solutions Group

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender Research Team

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Foreword

Hello and welcome to the 24th edition of the Microsoft Security Intelligence Report (SIR). As a practitioner and security architect, I read reports like this hoping to understand the landscape a little better with the takeaway of practical advice about how to use that knowledge to defend and protect organizations more effectively.

The SIR team brings the spirit of education for improved cyber-resilience to this report and has sifted through a year of data to distill out the most important lessons.

What you're reading are insights culled from a year of security data analysis and hands-on lessons learned. Data analyzed includes the 6.5 trillion threat signals that go through the Microsoft cloud every day and the research and real-world experiences from our thousands of security researchers and responders around the world. In 2018, attackers used a variety of dirty tricks, both new (coin-mining) and old (phishing), in their ongoing quest to steal data and resources from customers and organizations. Hybrid attacks, like the Ursnif campaign, blended social and technical approaches. As defenders got smarter against ransomware, a loud and disruptive form of attack, criminals pivoted to the more "stealth", but still profitable, coin-miners.

That "pivot" can feel frustrating, like attackers are always one step ahead. But viewed through a different lens, the story here is a positive one. Defenders and cybersecurity professionals like you implemented defensive techniques that forced attackers to change their preferred payloads and move away from ransomware.

Another area where cyber criminals increased their activity is the supply chain. One of the most notable, the Dofoil coin-miner outbreak, which hit on March 6, 2018, was kicked off by a poisoned peer-to-peer app. Supply chain concerns went beyond apps and into the cloud and included malicious browser extensions, compromised Linux repositories, and multiple instances of back-doored modules. To address this threat, organizations are moving towards a transparent and trusted supply chain model.

Data is great, but sometimes it helps to find out what really happened at an organization. That's why we've included lessons learned in the field from our Detection and Response Team (DART). These include how a large manufacturing company was able to implement controls to block a multi-phased phishing campaign that had been plaguing them for months, and financial services organizations that were finally able to eradicate threat actors from their systems using advanced investigation tools and endpoint monitoring.

Last but not least, phishing clicks continued to go up – but machine learning models are getting better at catching phish before they hit user boxes and preventing harm after click if they do. More good news? An increasing number of companies are implementing multi-factor solutions to limit the success of credential theft phishing emails.

Attackers look for opportunities, so the more we know about their techniques and tradecraft, the better prepared we'll be to build defenses and respond quickly. Small important steps can make a huge difference in the overall cybersecurity health of an organization. That's why along with deep insights on the shifting malware and attack landscape, you'll find recommended steps and other best practice guidance in this report. Because when I was a practitioner that's exactly what I needed in my fight against the bad guys. We hope it's what you need too.

Diana Kelley
Microsoft Cybersecurity Field CTO

P.S. We're always looking to improve the SIR. If you've got feedback, please reach out and let us know how we're doing.

SECTION I

Ransomware, cryptocurrency mining, and money

The big security stories of 2017 mostly involved ransomware. High-profile worldwide outbreaks of WannaCrypt and Petya thrust ransomware —a type of malware that locks or encrypts computers, then demands money to restore access—into the general consciousness, and many speculated that the problem would only increase in the future. Instead, ransomware encounters declined significantly in 2018.

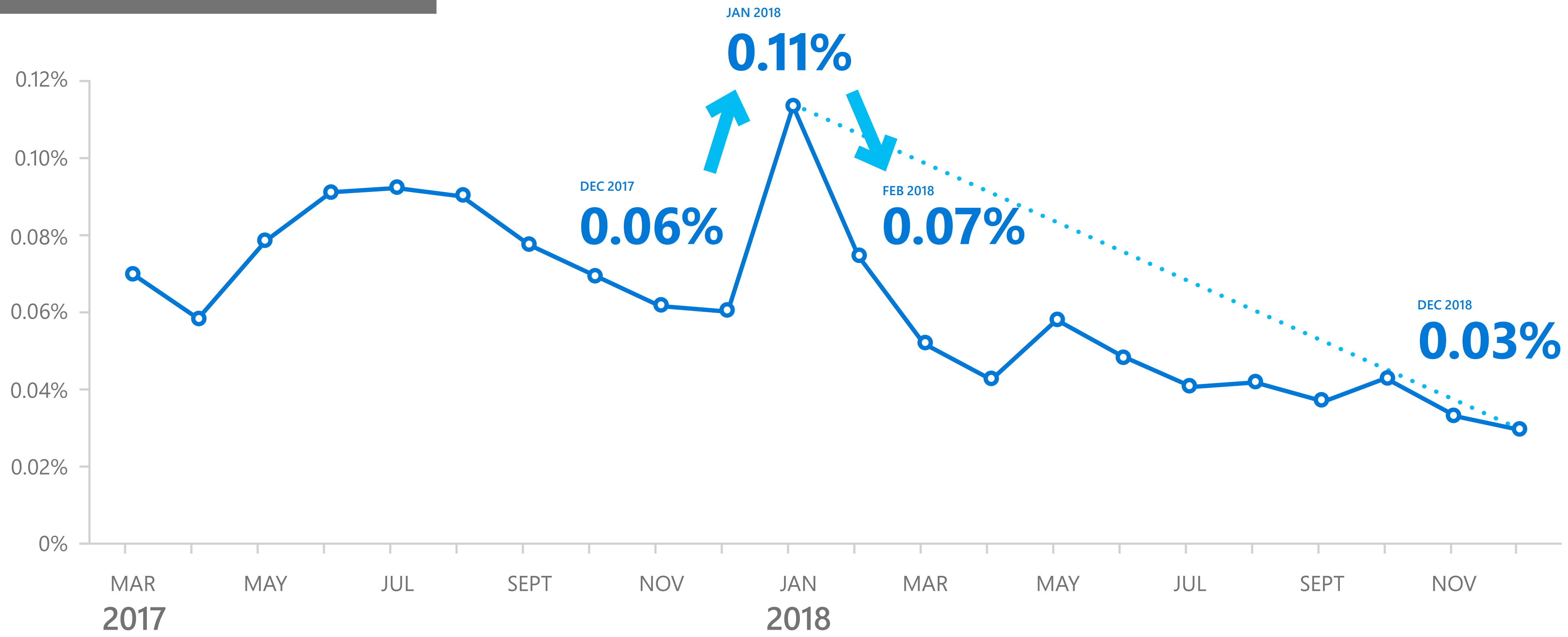
The decline in ransomware encounters was due in part to improved detection and education that made it more difficult for attackers to profit from it. As a result, attackers began to shift their efforts away from ransomware to approaches such as cryptocurrency mining, which uses victims' computing resources to make digital money for the attackers. The shift demonstrates the fundamentally opportunistic nature of most profit-oriented cybercriminals: they tend to chase the easiest money available, and when the economics of cybercrime change, they are quick to follow along.

RANSOMWARE ATTACKS ON THE DECLINE

More than a decade ago, the hackers and pranksters who dominated the early malware underground were supplanted by organized crime and other profit-oriented interests. Whereas early malware outbreaks were often flashy and obvious, profit-oriented malware was much more likely to operate quietly and avoid attracting attention, in order to continue performing its function—sending spam, stealing sensitive information, conducting denial-of-service attacks, and other malicious activity—as long as possible.

Ransomware bucked this trend. Instead of trying to remain undetected, ransomware openly denies victims access to their computers and important files until the victim pays the ransom (and often even afterward; attackers often do not release their control of computers even after the ransom is paid). As ransomware was peaking in 2017, it looked as though this style of open attack might represent a new phase in attacker techniques. But more recent data suggests that ransomware might be on the decline, with attackers increasingly returning to the stealthier mode of operation they've employed in the past, seeking to stay under the radar in order to more effectively conduct attacks like cryptocurrency mining. Although there has been a decline in the rate of ransomware encounters, this doesn't necessarily mean that the severity of attacks has declined.

Ransomware Encounter Rate



Ransomware encounter rates declined approximately 60 percent between March 2017 and December 2018, with intermittent increases across that period.

▲ **FIGURE 1.**

Ransomware encounters from March 2017 to December 2018

There are probably many causes for this overall decline, although Microsoft security researchers suspect that a primary factor is that both end users and organizations are becoming more aware of and dealing more intelligently with ransomware threats, including exerting greater caution and backing up important files so they can be restored if encrypted by ransomware. Also, as described earlier, cybercriminals are opportunistic.

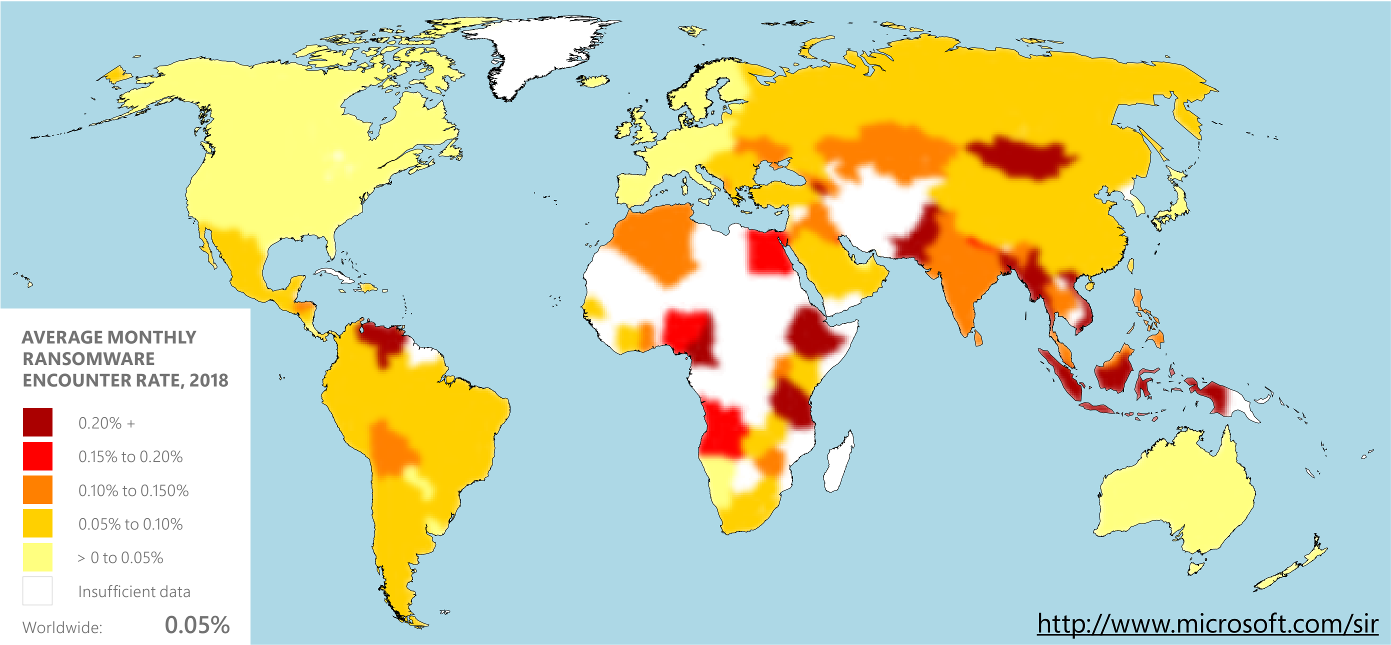
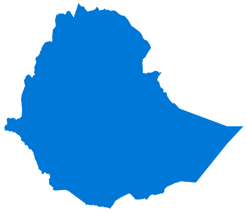


FIGURE 2.

Average monthly ransomware encounter rates worldwide by country/region in 2018

COUNTRY MOST IMPACTED BY RANSOMWARE: ETHIOPIA



Average monthly encounter rate: **0.77%**

The five locations with the highest average monthly ransomware encounter rates in 2018 were Ethiopia (0.77 percent average monthly ransomware encounter rate), Mongolia (0.46), Cameroon (0.41), Myanmar (0.33), and Venezuela (0.31), each of which had an average monthly ransomware encounter rate of 0.31 percent or higher during the period.1 A few years ago, ransomware encounters tended to cluster in wealthy countries and regions in Europe and North America, but as ransomware has started to fall out of favor with attackers the encounter pattern has come to more closely resemble that of malware as a whole.

The locations with the lowest ransomware encounter rates in 2018 were Ireland (0.01), Japan (0.01), the United States (0.02), United Kingdom (0.02), and Sweden (0.02 percent), each of which had an average monthly ransomware encounter rate of 0.02 percent or lower during the same period. Locations with low encounter rates tend to have mature cybersecurity infrastructures and well-established programs for protecting critical infrastructure and communicating with their citizens about basic security.

FOOTNOTES

[1] Encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter. 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.

CRYPTOCURRENCY MINING ON THE RISE

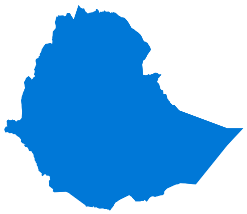
Cryptocurrency is virtual money that can be used to anonymously buy and sell goods and services, both online and in the physical world. Many different kinds of cryptocurrencies exist, but they are all based on blockchain technology, in which every transaction is recorded in a distributed ledger maintained by thousands or millions of computers around the world. New coins are created, or “mined,” by computers performing complex calculations that also serve the function of verifying blockchain transactions.

Mining coins can be very lucrative—in 2018, a single coin of Bitcoin, the oldest and most popular cryptocurrency, was worth several thousand US dollars—but performing the necessary calculations can be very resource intensive and becomes more so as each new coin is mined. For popular currencies such as Bitcoin, mining coins profitably is almost impossible without access to immense computing resources that are well out of reach for most individuals and small groups. For this reason, attackers seeking illicit profits have increasingly turned to malware that lets them use victims’ computers to help them mine cryptocurrency coins. This approach allows them to leverage the processing power of hundreds of thousands of computers instead of one or two. Even when a minor infection is discovered, the anonymous nature of cryptocurrency complicates efforts to track down the responsible parties.

In 2018, the average worldwide monthly cryptocurrency coin mining encounter rate was 0.12 percent, compared to just 0.05 percent for ransomware. Many factors contribute to the increased popularity of mining as a payload for malware. Unlike ransomware, cryptocurrency mining does not require user input: it works in the background, while the user is performing other tasks or is away from the computer, and may not be noticed at all unless it degrades the computer’s performance sufficiently. As a result, users are less likely to take any action to remove the threat, and it might continue mining for the benefit of the attacker for an extended period of time.

The availability of “off the shelf” products for covert mining of many cryptocurrencies is another driver of the trend. The barrier to entry is low because of the wide availability of coin mining software, which cybercriminals repackage as malware to deliver to unsuspecting users’ computers. The weaponized miners are then distributed to victims using many of the same techniques attackers use to deliver other threats, such as social engineering, exploits, and drive-by downloads. After the mining software is installed, it runs in the background on victim’s computers to perform the blockchain computations, with the attacker reaping the rewards.

AVERAGE MONTHLY ENCOUNTER RATES OF COUNTRIES MOST IMPACTED BY CRYPTOCURRENCY MINING



Ethiopia: 5.58%

Tanzania: 1.83%

Pakistan: 1.47%

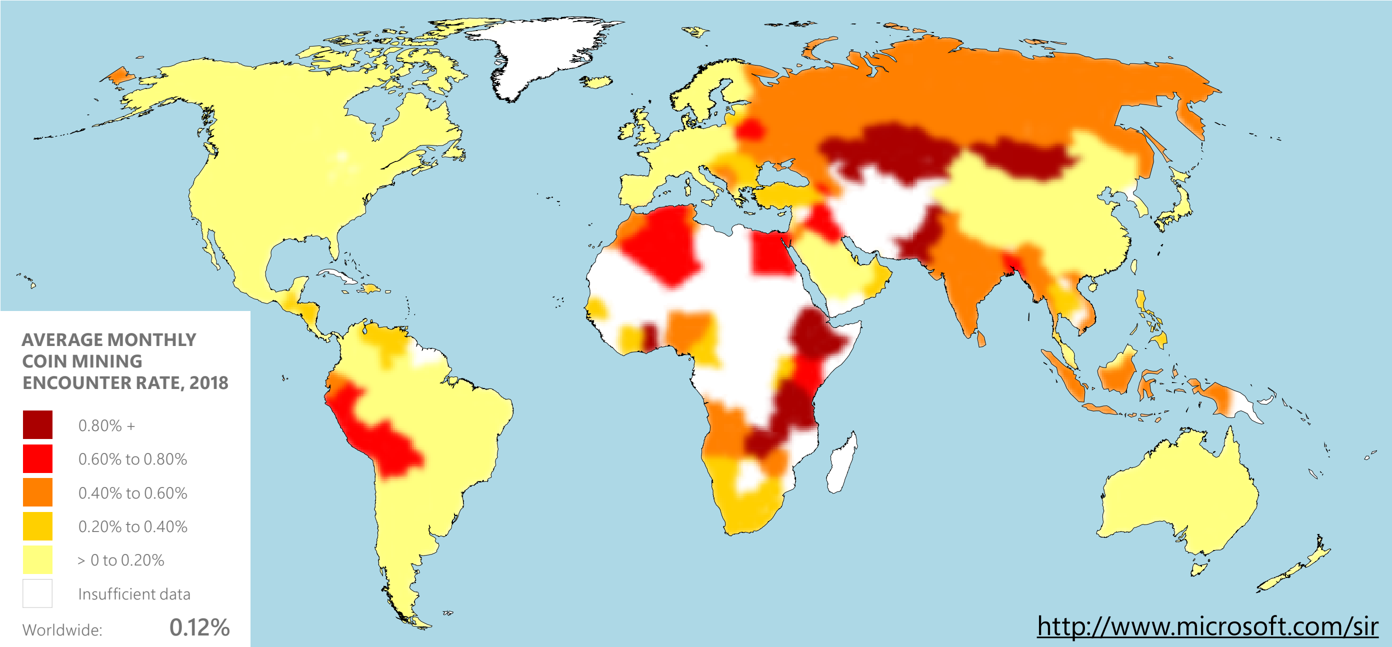
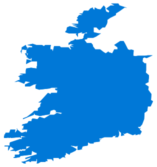


FIGURE 3.

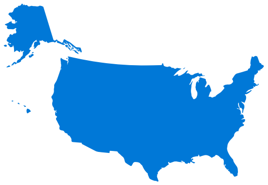
Average monthly coin miner encounter rates worldwide by country/region in 2018

AVERAGE MONTHLY ENCOUNTER RATES OF COUNTRIES LEAST IMPACTED BY CRYPTOCURRENCY MINING



Ireland: 0.02%

Japan: 0.02%



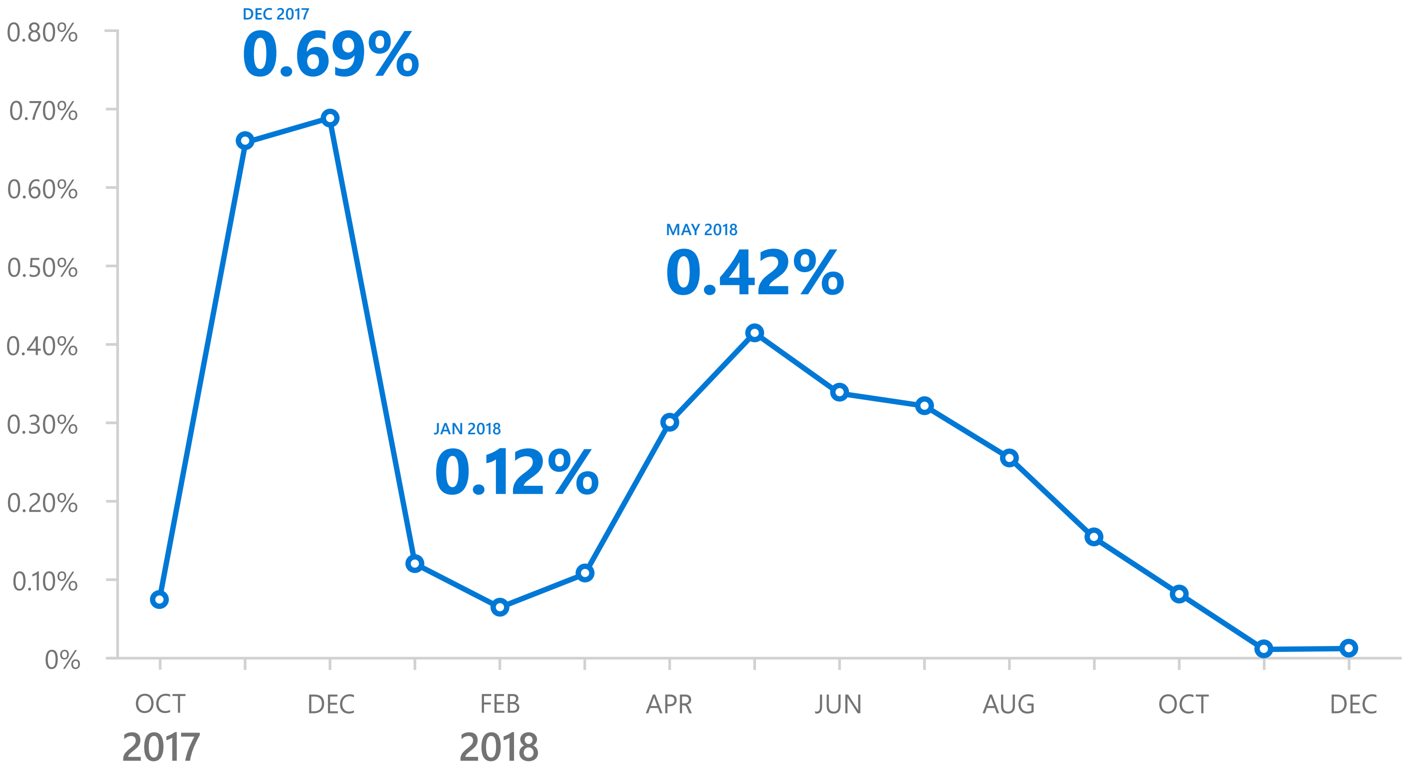
United States: 0.02%

The five locations with the highest cryptocurrency coin mining encounter rates in 2018 were Ethiopia (5.58), Tanzania (1.83), Pakistan (1.47), Kazakhstan (1.24), and Zambia (1.13), each of which had an average monthly coin mining encounter rate of approximately 1.13 percent or higher during the period. The locations with the lowest coin mining encounter rates in 2018 were Ireland, Japan, the United States, and China, each of which had an average monthly coin mining encounter rate of approximately 0.02 percent during the period.

BROWSER-BASED CRYPTOCURRENCY MINERS: A NEW KIND OF THREAT

The statistics presented in this section involve malicious cryptocurrency miners that are designed to be installed on victims' computers as malware. But some of the most significant cryptocurrency mining threats are based entirely within web browsers and never need to be installed at all. A number of services advertise browser-based cryptocurrency mining as a way for website owners to monetize traffic to their sites without relying on advertising. Site owners are supposed to add JavaScript code to their pages that mine cryptocurrency in the background while a user is visiting the site, with the proceeds split between the site owner and the service. Unfortunately, attackers have been quick to take advantage of these services to mine cryptocurrency without obtaining consent from the end users, often by

Brocoiner Encounter Rate



compromising legitimate websites and maliciously inserting the mining code into their source code. These browser-based miners don't require compromising the end user's computer at all, and will run on any platform with a JavaScript-capable web browser. Like cryptocurrency mining trojans, browser-based miners can significantly degrade computer performance and waste electricity while a user visits an affected web page.

FIGURE 4.

Encounter rate for Brocoiner, the most prevalent browser-based cryptocurrency miner

THE IMPACT OF UNSOLICITED CRYPTOCURRENCY MINING

The most obvious threat victims face from malicious cryptocurrency mining is consumption of computing resources, which can waste electricity and significantly degrade computer performance. Users and organizations also face other risks from coin mining, including:

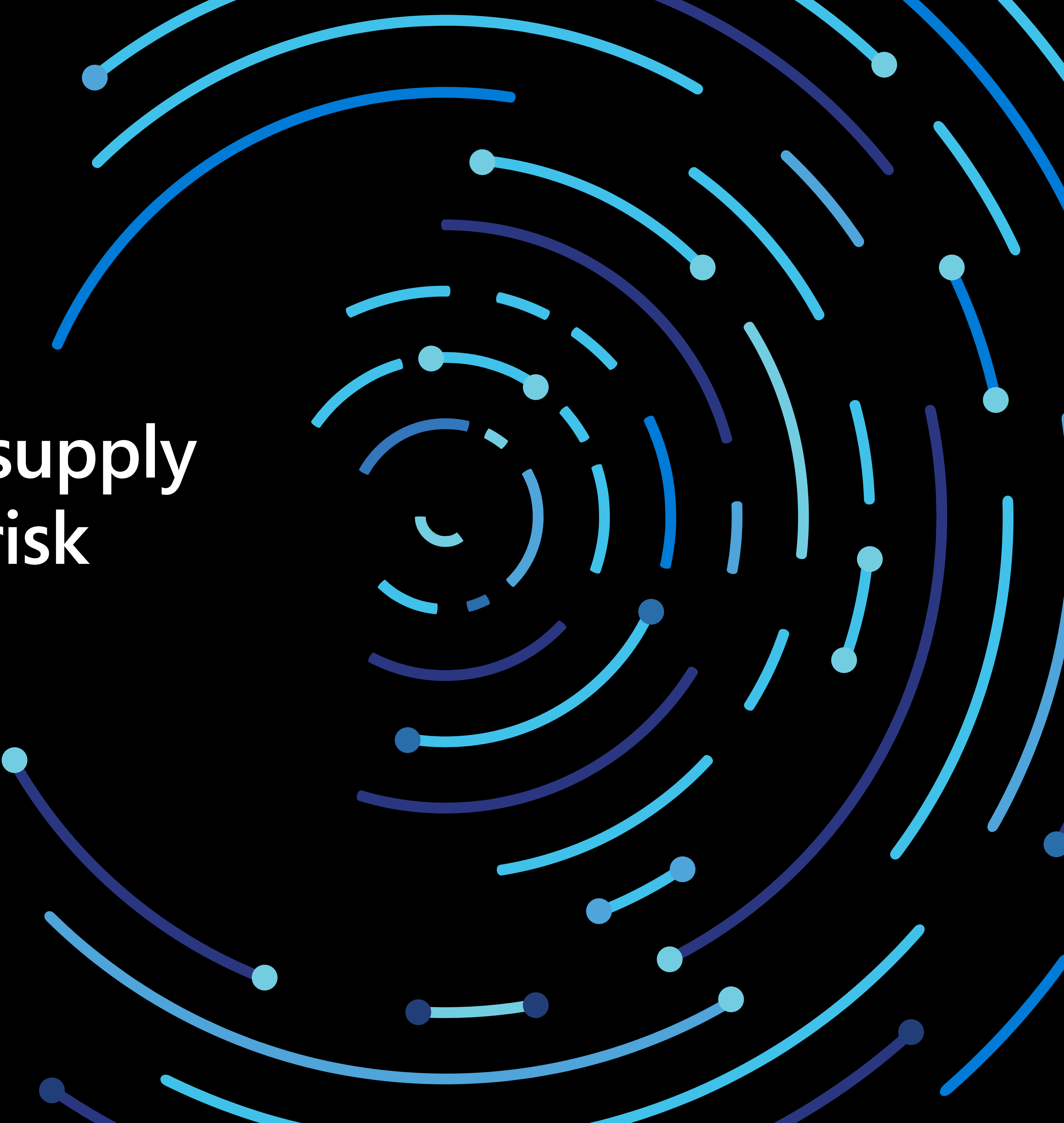
- **Gaining a foothold to do greater damage in the future.** Like other forms of malware, cryptocurrency mining can be an entry point for attackers. While the computer is mining cryptocurrency in the background, cybercriminals can learn about the environment and possibly uncover gaps in security to exploit for other purposes.

- **Internet-connected devices may be compromised and turned into bots for cryptocurrency mining.** Many such devices lack built-in security such as malware threat detection, which can make them desirable targets for attackers.

- **Harming machines.** Cryptocurrency mining software running continuously for months or longer can impair performance, and the heat generated by excessive power consumption and CPU utilization can damage computers.

SECTION II

Software supply chains at risk



For years Microsoft has been tracking threat actors who use supply chain compromise as an entry point for attacks. In a supply chain attack, the attacker concentrates on compromising the development or update process of a legitimate software publisher.

If successful, the attacker can incorporate a compromised component into a legitimate application or update package that then gets distributed to the software's users. The malicious code then runs with the same trust and permissions as the software. The increased number of software supply chain attacks over the past few years has become an important topic in many cybersecurity conversations and is a primary source of concern in many IT departments.

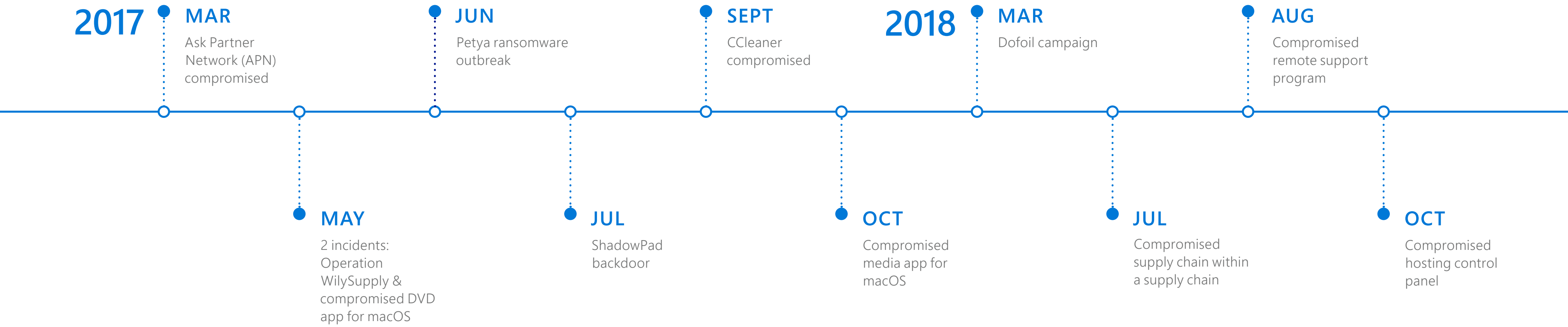

2017
MAR
Ask Partner Network (APN) compromised
MAY
2 incidents: Operation WilySupply & compromised DVD app for macOS
JUN
Petya ransomware outbreak
JUL
ShadowPad backdoor
SEPT
CCleaner compromised
OCT
Compromised media app for macOS
2018
MAR
Dofoil campaign
JUL
Compromised supply chain within a supply chain
AUG
Compromised remote support program
OCT
Compromised hosting control panel

FIGURE 5.

Software supply chain attacks in 2017 and 2018

MAJOR SOFTWARE SUPPLY CHAIN ATTACKS IN 2017

In 2017, supply chain attacks were responsible for a number of high-profile incidents, most notably the Petya ransomware outbreak in June, which was traced to initial infections from a compromised update process for a popular tax accounting application in Ukraine. In May, Operation WilySupply compromised a text editor's software updater to install a backdoor on target organizations in the financial and IT sectors. In July, a backdoor called ShadowPad was hidden in a server management software package, and allowed attackers to install additional malware payloads for data theft and other malicious activities. In September, the infrastructure of popular freeware tool CCleaner was compromised and a backdoored version was delivered to its userbase.

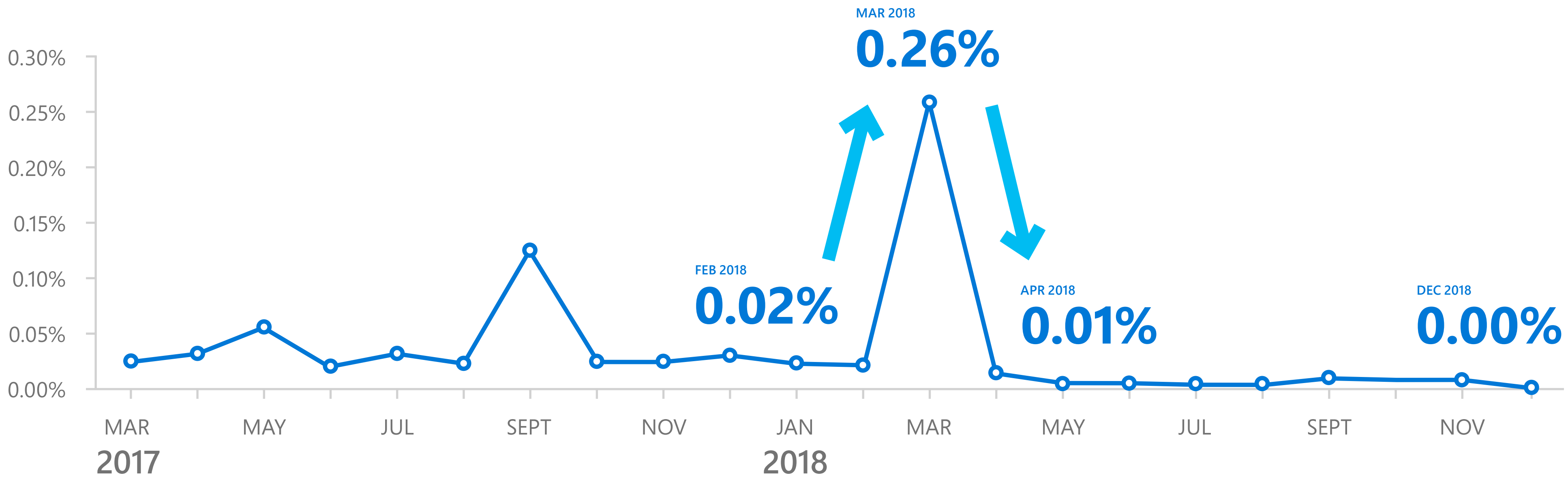
SOFTWARE SUPPLY CHAIN ATTACKS IN 2018 – ROOT CAUSES AND IMPACT

The first major software supply chain attack incident of 2018 occurred on March 6, when Windows Defender ATP blocked a massive campaign to deliver the Dofoil trojan (also known as Smoke Loader). The massive malware campaign was traced to a poisoned peer-to-peer application. The application's update package was replaced with a malicious one that downloaded compromised code, which later installed the Dofoil malware. The sophisticated trojan carried a coin mining payload, and exhibited advanced cross-process injection techniques, persistence mechanisms, and evasion methods.

▼ **FIGURE 6.**

Trending of Dofoil (Smoke Loader) encounters in 2018 shows spike of blocked instances in March

Dofoil Encounter Rate



In the first 12 hours of the campaign, Windows Defender Antivirus blocked more than 400,000 infection attempts worldwide. Russia accounted for 73 percent of global encounters, with Turkey and Ukraine registering 18 percent and 4 percent, respectively.

Several more attacks were detected using compromised software supply chains as delivery mechanisms in 2018, including those described in the following table:

Period	Attack	Description	Software affected
March 2018	Dofoil coin mining campaign (reported by Microsoft).	Attackers poisoned the update process of a peer-to-peer app to install Dofoil, which in turn installed coin mining malware.	Peer-to-peer app.
July 2018	Compromised supply chain within a supply chain (reported by Microsoft).	Attackers compromised the shared infrastructure between a PDF editor app vendor and one of its software vendor partners.	PDF editor app and third-party partner vendor.
August 2018	Compromised remote support program (Operation Red Signature, reported by Trend Micro and IssueMakersLab).	The update server of a remote support solutions provider was compromised to deliver a remote access tool called 9002 RAT.	Remote support program.
October 2018	Compromised hosting control panel solution (reported by ESET).	The installation script for a hosting control panel solution was altered to steal credentials.	Hosting control panel solution.

FIGURE 7.

Other software supply chain attacks in 2018

TRUST AT RISK

Supply chain attacks are insidious because they take advantage of the trust that users and IT departments place in the software they use. The compromised software is often signed and certified by the vendor, and may give no indication that anything is wrong, which makes it significantly more difficult to detect the infection. They can damage the relationship between supply chains and their customers, whether the latter are corporate or home users. By poisoning software and undermining delivery or update infrastructures, supply chain attacks can affect the integrity and security of goods and services that organizations provide.

Supply chain attacks have affected a wide range of software and targeted organizations in different sectors and geographic locations. The threat of supply chain attacks is an industry-wide problem that requires attention from multiple stakeholders, including the software developers and vendors who write the code, the system administrators who manage software installations, and the information security community that finds these attacks and creates solutions to protect people and software from them.

BEYOND SOFTWARE: SUPPLY CHAIN COMPROMISE THROUGH CLOUD OBJECTS

The ability of supply chain attacks to undermine trust is amplified and made even more complex in the cloud. Several incidents of compromised cloud objects, services, and infrastructure in 2018 highlight this complexity:

- Poisoned Chrome extensions that installed click-fraud malware (reported by ICEBRG)
- Various compromised Linux repositories (reported in a few online forums)
- Malicious WordPress plug-ins used for various malicious activities, including allowing attackers to publish content on WordPress sites (reported by Wordfence)
- Malicious Docker images that contained a script to download cryptocurrency coin mining malware and uploaded to Docker Hub account (reported by Fortinet and Kromtech)
- A typo-squatting malicious package in the official Python repository; the package contained a malicious script that downloads malware used to hijack coin mining addresses in the clipboard (reported on Medium)
- Compromised script in StatCounter that allowed attackers to inject a malicious script in websites that use StatCounter (reported by ESET)
- Multiple incidents of backdoored npm modules (The npm Blog, Medium) which, if exploited, could result in situations such as, for example, an attacker being able to input arbitrary code into a running server and execute it.

These incidents demonstrate how supply chain compromise can immensely widen an attack surface. If not secured, cloud objects can be unexpected entry vectors. For example, the Docker Hub incident involved a malicious account uploading Docker images that contained a hidden coin mining backdoor. The Docker images were hosted on Docker Hub for almost a year and were downloaded millions of times and used by unsuspecting administrators and users.

Supply chain risks extend to code in the cloud, open source, web libraries, containers, and other objects in the cloud. These risks, coupled with the high degree of variation among the software and hardware supply chain compromise incidents that have come to light, make supply chain attacks a broad category of threat. Although there is no single solution for the entire spectrum of these types of attacks, organizations need to build preventative protection and post-breach detection of supply chain attacks from compromised hardware and software suppliers, vendors and acquisitions, open source software suppliers, as well as cloud services and infrastructure suppliers.

Investigating cyber incidents with DART

The Microsoft Detection and Response Team (DART) is a global team of cybersecurity experts and incident responders that helps organizations with detection, investigation, and response to cybersecurity incidents. This section highlights some of the customer cases that DART handled in the last year; it illustrates common attacker trends and how Microsoft and customers were able to thwart them.

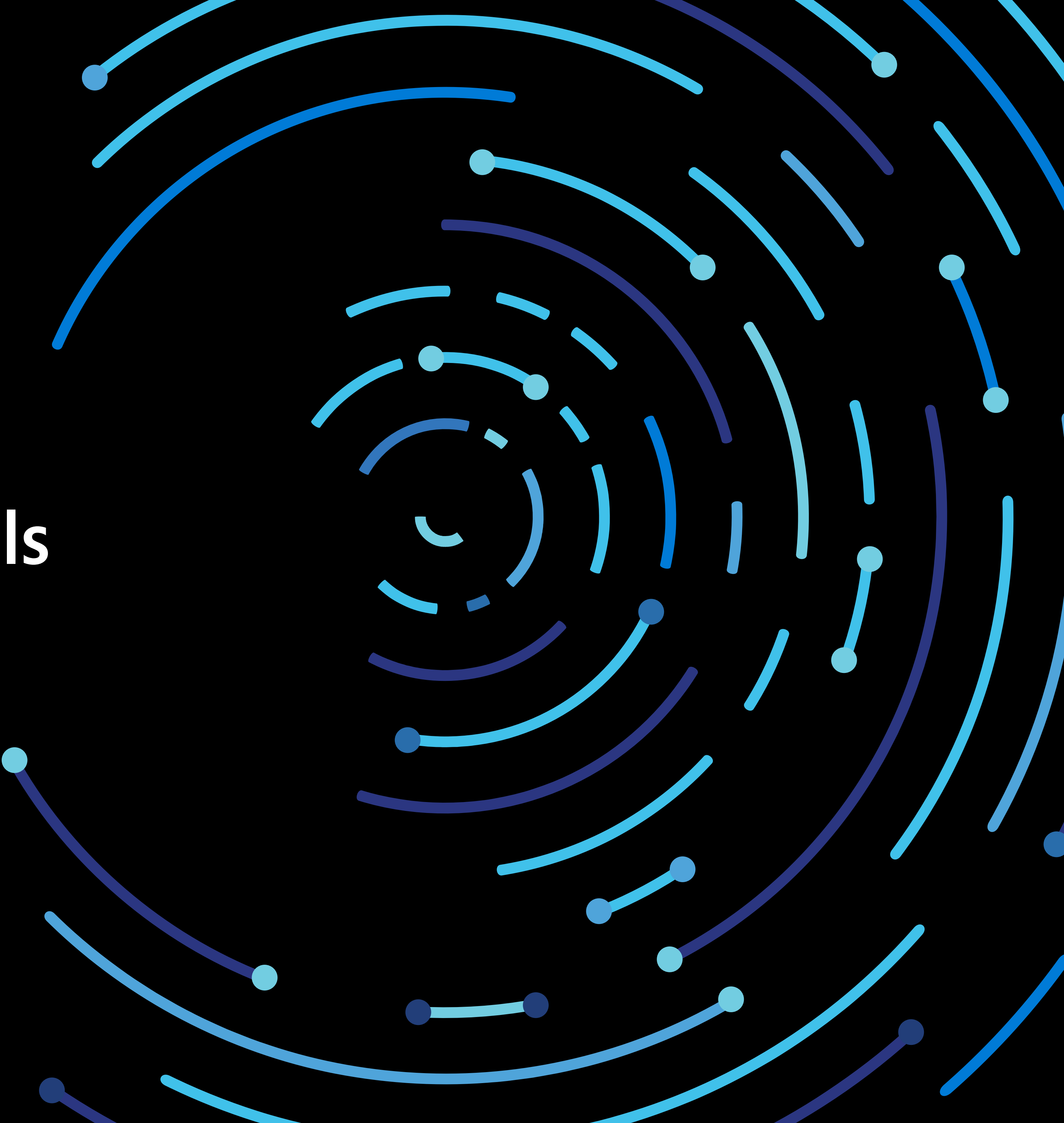
PROFESSIONAL SERVICES ORGANIZATION EXPERIENCED NATION STATE ATTACK THAT EXFILTRATED DATA

A professional services organization was affected by a sophisticated, state-sponsored advanced persistent threat (APT) that gained access to privileged credentials of the organization. The attackers gained access to the network using a password spray attack, in which they used a small number of weak or widely used passwords (such as "p@ssword" or "123456") to target a large number of user accounts and gain Office 365 administrative credentials. (Password spray attacks are used to avoid detection by limiting the number of login attempts for each account.) After infiltrating the network, the APT performed elaborate, automated exfiltration of data from employee mailboxes. Despite multiple in-house attempts to evict them, the adversary remained in the network for more than 200 days. As part of the attack, the adversary leveraged the organization's supply chain software and automated exfiltration of data.

Because they suspected a breach of their customer data, the organization engaged the DART team to investigate and help prevent further damage. DART identified targeted Office 365 mailbox searches, compromised accounts, and attacker command and control channels. Key customer lessons from this incident were to deploy controls to safeguard cloud services from identity-based threats and attackers. The organization adopted multi-factor authentication (MFA), conditional access policies for certain cloud apps, and Office 365 logging. To further protect itself against similar threats in the future, the organization may also adopt an endpoint threat detection and response (EDR) solution to detect attackers that may be trying to exploit its network. Furthermore, we have recommended that this organization appoint a cloud governance body or global identity team who will manage and enforce appropriate user authentication policies, so that the organization has oversight into their security posture and can more effectively mitigate risk.

SECTION III

Phishing still prevails



In 2018, Microsoft threat analysts have seen evidence that attackers continue to use phishing as a preferred attack method. Phishing promises to remain a problem for the foreseeable future because it involves human decisions and judgement in the face of persistent efforts by cybercriminals to make victims fall for their lures.

Phishing rates are still on the rise

Percentage of total inbound emails that are phishing emails

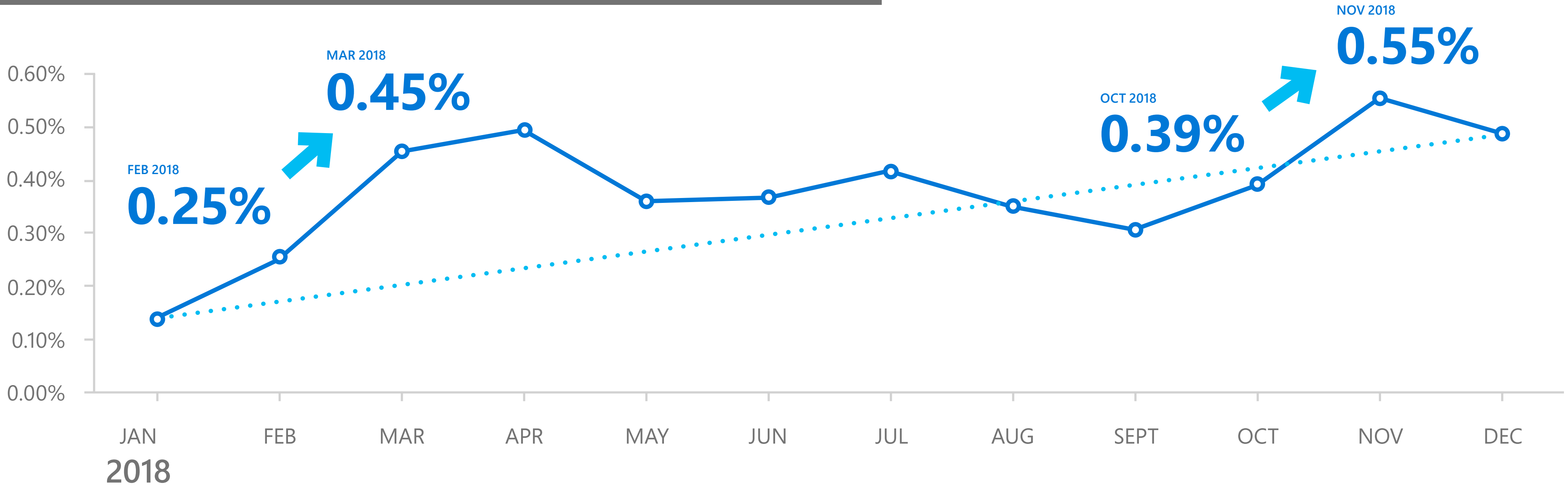


FIGURE 8.

Phishing emails in 2018

PHISHING CONTINUES TO BE A PREFERRED ATTACK VECTOR IN 2018

Microsoft analyzes and scans in Office 365 more than 470 billion email messages every month for phishing and malware, which provides analysts with considerable insight into attacker trends and techniques. The share of inbound emails that were phishing messages increased 250 percent between January and December 2018. Phishing remains one of the top attack vectors used to deliver malicious zero-day payloads to users, and Microsoft has continued to harden against these attacks with additional anti-phishing protection, detection, investigation, and response capabilities to help secure users.

Evolution in phishing attack methods

As the tools and techniques used to protect people from phishing become more sophisticated, attackers are forced to adapt themselves. Phishing attacks have become increasingly polymorphic, which means attackers don't use a single URL, domain, or IP address to send mail, but make use of a varied infrastructure with multiple points of attack. The nature of the attacks themselves has also evolved, with modern phishing campaigns ranging from short-span attacks that are active for just minutes to much longer high-volume campaigns. Others are serial variants attacks, wherein attackers send a short volume of mail on several successive days.

In addition, Microsoft has observed a trend toward attackers using hosted infrastructure and other public cloud infrastructure, which makes it easier to avoid detection by hiding among legitimate sites and assets. For example, attackers increasingly use popular document sharing and collaboration sites and services to distribute malicious payloads and fake login forms that are used to steal user credentials. There has also been an increase in the use of compromised accounts to further distribute malicious emails both inside and outside an organization.

Phishing campaigns vary from targeted to broad-based

As with malware distribution in general, phishing campaigns vary from targeted to broad-based, generic attacks. Although highly sophisticated attacks yield greater monetary gains per account phished, more generic attacks yield less money per compromised account but target a broader set of users.

An example of a sophisticated, targeted campaign is Ursnif, in which attackers localized the document file name to be specific to a familiar organization or the industry of the target. Such attacks are quite different from broad-based campaigns and appear to be more legitimate and trustworthy.

Some of the broad-based campaigns in 2018 were related to business email compromise (BEC) and impersonation of known brands, domains, or users within the target organizations and sophisticated spoofing campaigns. Domain impersonation is a common attack tactic used to lure organizations into believing that the email is trustworthy and should be opened.

Phishing lures come in many forms

Microsoft researchers have found that many different types of phishing lures or payloads are being employed in campaigns, including:

- **Domain spoofing** (the email message domain is an exact match with the original domain name)
- **Domain impersonation** (the email message domain is a look alike of the original domain name)[2]
- **User impersonation** (the email message appears to come from someone you trust)
- **Text lures** (the text message appears to come from a legitimate source such as a bank, government agency, or other company to impart legitimateness to their claims and typically asks the victim to provide sensitive information such as usernames, passwords or sensitive financial data)
- **Credential phishing links** (the email message contains a link to a page that resembles a login page for a legitimate site, so users will enter their login credentials)
- **Phishing attachments** (the email message contains a malicious file attachment that the sender entices the victim to open)
- **Links to fake cloud storage locations** (the email message appears to come from a legitimate source and entices the user to give permission and/or enter personal information such as credentials in exchange for accessing a fake cloud storage location)

This variety of lures that could potentially be employed by attackers increases the complexity of phishing threats that organizations must contend with.

FOOTNOTES

[2] Domain impersonation may resemble domain spoofing (exact match with the original domain name) in the exceptional case where the domain appears in the email display name.

Investigating cyber incidents with DART

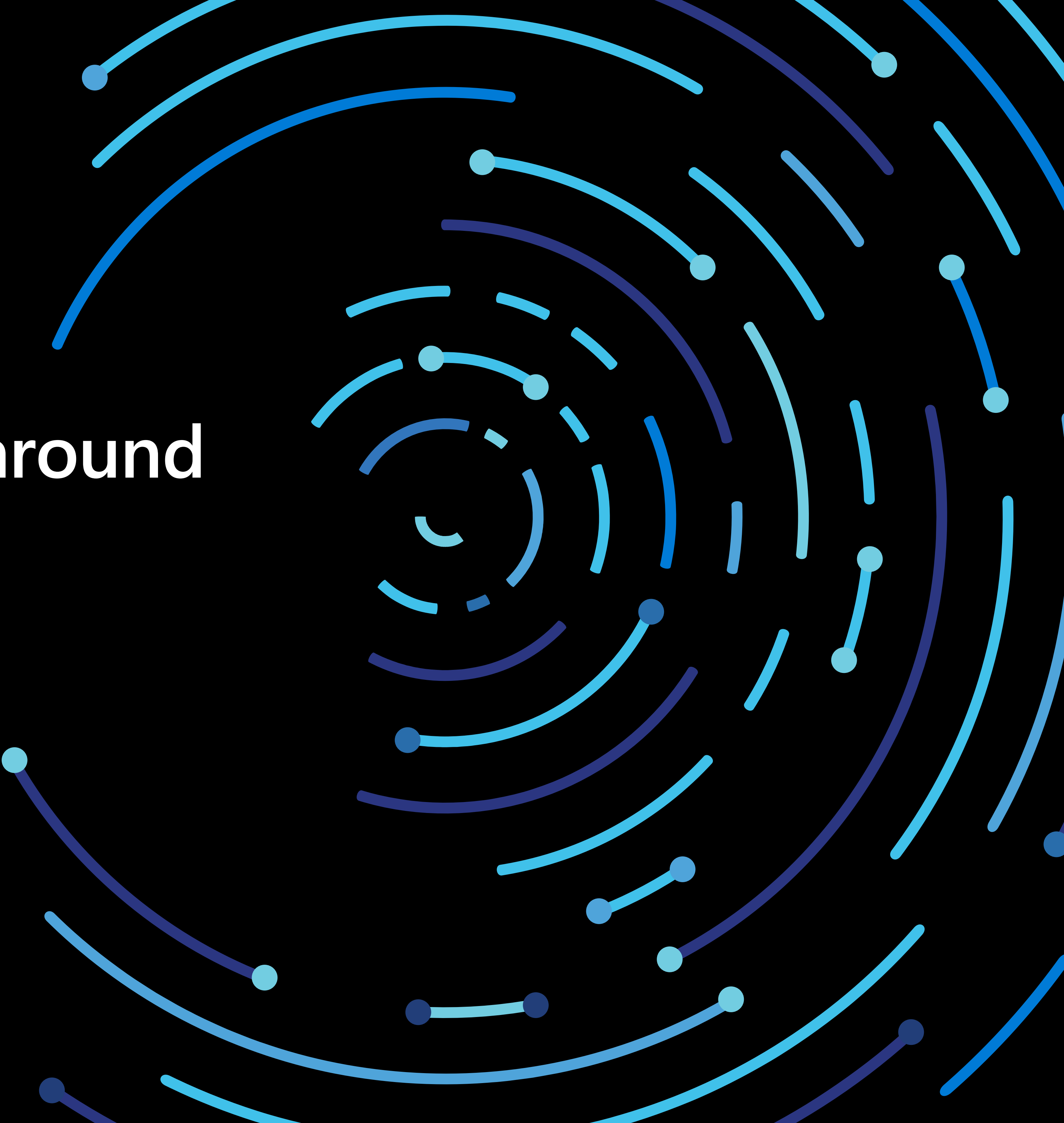
LARGE MANUFACTURING ORGANIZATION HIT BY TARGETED PHISHING INCIDENTS

A manufacturing organization experienced a multi-phased phishing campaign across a span of a few months. This approach is not unusual. During the first phase the attacker will perform reconnaissance and in the second phase will target high-value assets. The first phase of this campaign leveraged a well-known phishing scam that was based on a web page link embedded in an email sent to a small targeted group within the organization. The email claimed that the target had an important electronic document waiting to be reviewed, and all the recipient had to do was authenticate with their domain credentials to gain access. This fake landing page set up for the target to review the so called 'important document' actually harvested the credentials and allowed the attacker access to Office 365 accounts from anywhere in the world. The second phase of the phishing campaign was intended to send similar phishing emails to high value assets inside the target manufacturing organization, in hopes to gain access to more valuable data. Microsoft engaged with this client during the second phase of the phishing campaign. Key customer lessons from this incident were: phishing remains to be one of the most effective attack methods and users are still the weakest link. Training users to be wary of phishing scams, having tools in place to identify attackers and act, and regularly patching systems are all important; if the organization does not address even one of these, it can be vulnerable.

In this case, the most important concern of the customer was an immediate need to block access to the compromised accounts. In partnership with Azure Identity and Office 365 teams, DART devised a plan to eradicate the attacker from the network and monitor any traffic to the command and control channel by using the newly deployed Microsoft Azure Log Analytics solution. The team was able to help resolve the situation in just three hours. The attacker's access was blocked, and the organization could turn their attention to damage assessment and recovery. DART used the Azure Log Analytics tools to hunt for attacker behavior, which helped uncover many configuration challenges for the organization. For example, DART identified gaps in patching on critical servers, discovered computers on the network communicating with known bad hosts on the Internet, and also found several important servers without malware protection.

SECTION IV

Malware around the world



Malware poses risks to organizations and individuals in the form of impaired usability, data loss, intellectual property theft, monetary loss, emotional distress, and can even put human life at risk. Microsoft uses a broad array of tools and techniques to identify, block, and eradicate malware infections wherever they are found.

Malware encounter rates ranged from around 5 percent to more than 7 percent in 2017. In early 2018 they were elevated before decreasing throughout most of the year to just above 4 percent. Some potential reasons for the overall decrease in malware encounter rates in 2018 are the growth in adoption of Windows 10 and increased use of Windows Defender for protection. Encounter rate is the percent of computers running Windows Defender Antivirus that reported encountering malware during the month, including infection attempts that Defender blocked.

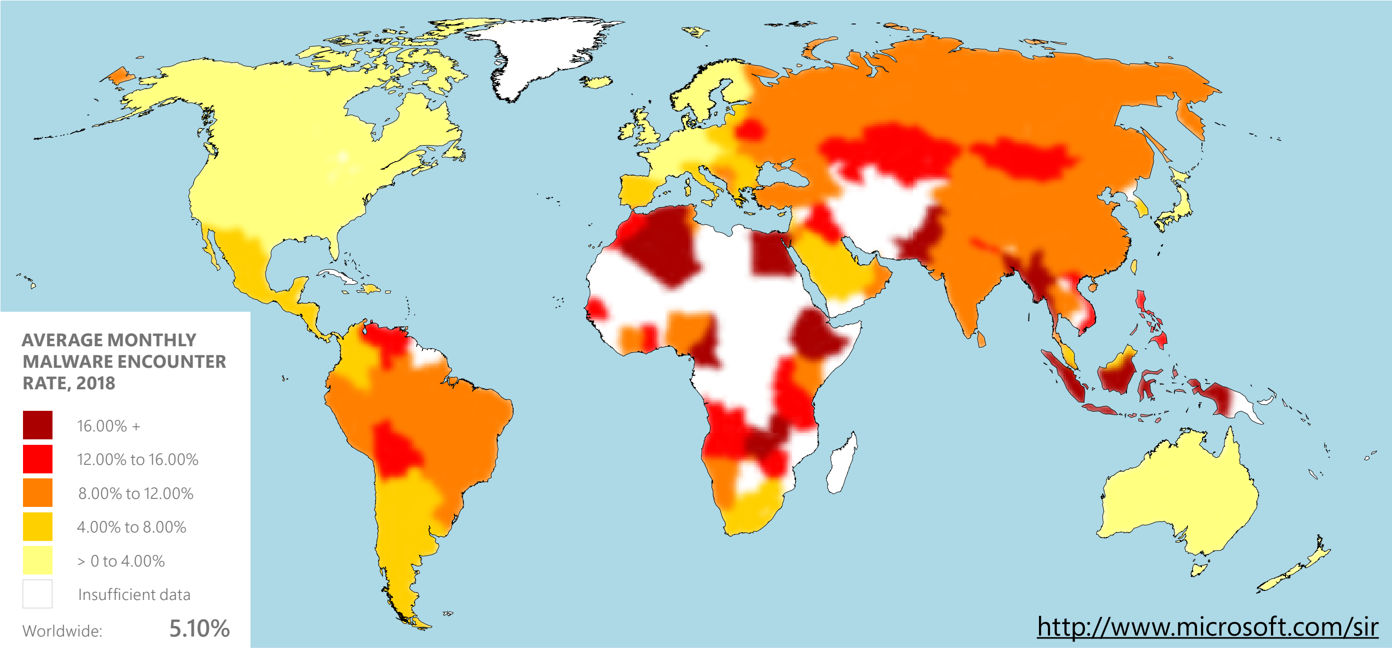


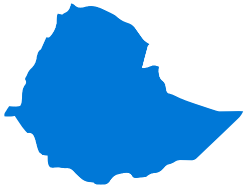
FIGURE 9.

Average monthly malware encounter rates worldwide by country/region in 2018

The five locations with the highest malware encounter rates during the January–December 2018 period were Ethiopia (26.33 percent average monthly encounter rate), Pakistan (18.94), the Palestinian territories (17.50), Bangladesh (16.95), and Indonesia (16.59), all of which had an average monthly encounter rate of approximately 16.59 percent or higher during the period. Infection rates tend to correlate strongly with human development factors and technology readiness within a society. All of the locations with the highest encounter rates in 2018 ranked in the bottom 40 percent of countries and regions in the 2017 Information and Communications Technologies (ICT) Index, published by the United Nations International Telecommunication Union (ICT).

The five locations with the lowest malware encounter rates during that same period were Ireland (1.26), Japan (1.51), Finland (1.74), Norway (1.79) and Netherlands (1.82), all of which had an average monthly encounter rate of 1.82 percent or less during the period. These locations tend to have mature cybersecurity infrastructures and well-established programs for protecting critical infrastructure and communicating with their citizens about basic security.

AVERAGE MONTHLY ENCOUNTER RATES OF COUNTRIES MOST IMPACTED BY MALWARE



Ethiopia: 26.33%

Pakistan: 18.94%

Palestinian territories: 17.50%

Investigating cyber incidents with DART

MULTIPLE FINANCIAL SERVICES ORGANIZATIONS EXPERIENCED NATION STATE ATTACKS THAT DISRUPTED OPERATIONS

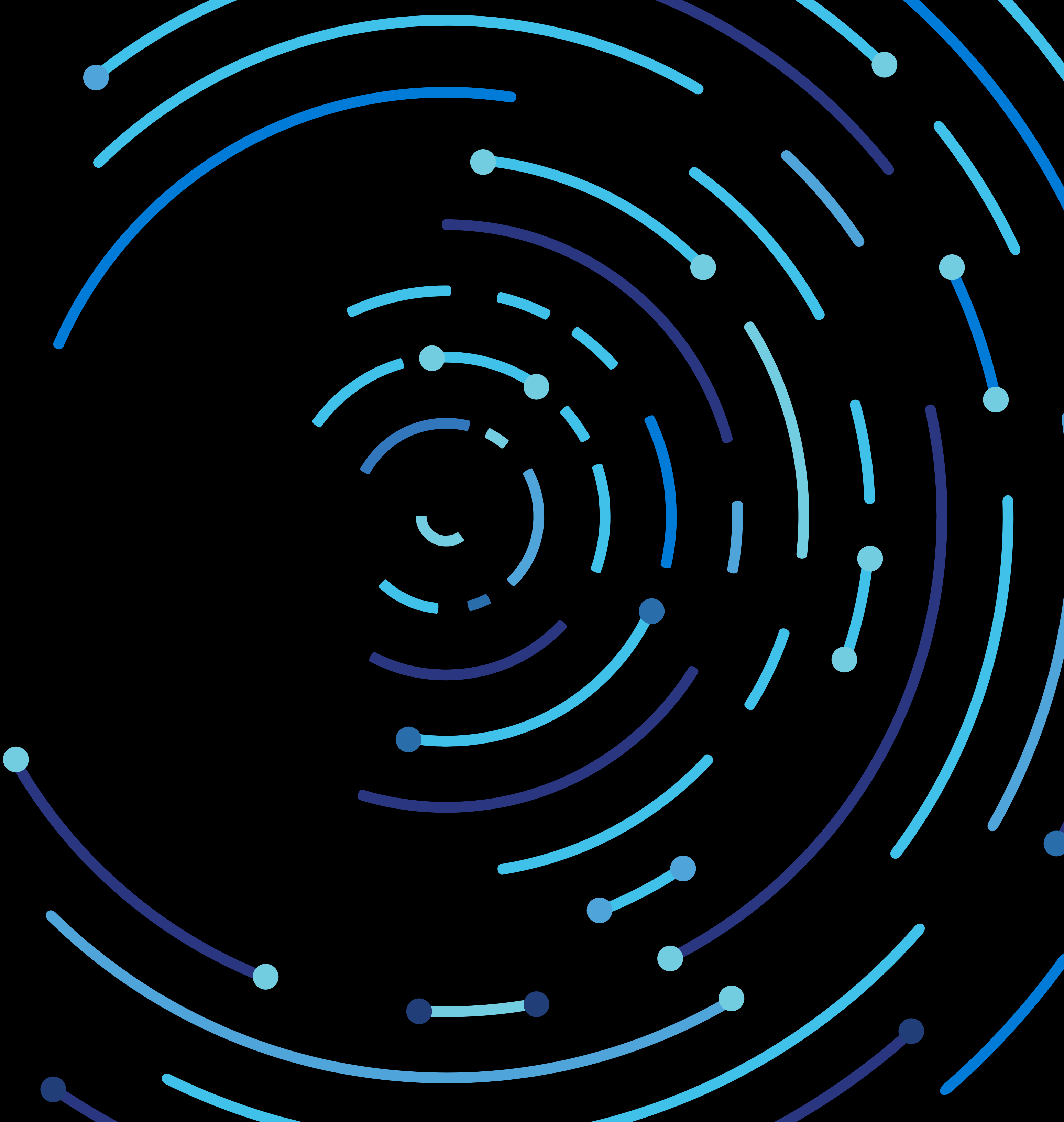
In one of the more destructive incidents DART has seen, several financial services organizations were targeted by a state-sponsored APT (a different group from the one that targeted the professional services organization referenced earlier) that played out similarly.

This APT gained administrative access after infecting a patient zero machine with a highly targeted, obfuscated backdoor implant, possibly delivered via a spear phishing email. Subsequently, the APT executed multiple fraudulent transactions, transferring large sums of cash into foreign bank accounts. In some cases, the attacker remained undetected for more than 100 days. After the attacker realized they were detected, the attacker rapidly deployed a pre-staged attack, delivering destructive malware to more than half of the systems in the environment; these customers' operations were shut down for several days.

There were a few key customer lessons from these incidents. The first was that software lifecycle management is especially important, which includes ensuring systems are being regularly updated (operating systems and security), patched, and audited. In one case, an organization's Linux system environment that had an exceptionally large number of workloads running on it was completely unmanaged, putting it at a remarkably high risk of attack. The second lesson was that it is important to maintain backups of system data in an offline location in case the primary data is lost. Another lesson was that traditional antivirus solutions may not suffice if you need to know about adversary activity.

Returning to normal operational mode was the highest priority for these organizations. DART helped restore services by first investigating the impact and then taking necessary mitigation actions, such as removing malware from the affected systems and getting them to a healthy state. The team also trained customers on how to use Microsoft threat investigation tools, including EDR and others, so that they could look for anomalous behavior and attacker activity in their network. DART emphasized that endpoint monitoring is critical for defending against sophisticated, targeted attacks that may go undetected by traditional antivirus solutions.

Guidance



Guidance

Building organizational resilience and meaningful risk reduction requires a security approach that includes prevention and detection and response. We have organized the following suggested security best practices and controls into those categories.

PREVENTION:

Preventive controls play a key role in an overall defense strategy as the right investments can increase the cost of attacks for cybercriminals and sustain those increased attack costs over time (without requiring an expert analyst to monitor and interpret the output). Preventive control investments should be targeted at the lowest cost techniques to steadily remove cheap and effective attack techniques.

Four things to consider for prevention are:

1. **Security hygiene is critical. As seen in some of the cyber incidents shared in this report, common hygiene issues can undermine advanced security capabilities, so following these tips can help mitigate risk:**

- Avoid using unfamiliar free and/or pirated software. Only use software from trusted sources.

- Mitigate credential theft risk, including securing privileged administrator accounts. To learn how, read this blog, which outlines some principles and tools Microsoft has used to guide and enhance our own security posture and some prescriptive roadmaps to help you plan your own initiatives.

- Apply secure configuration baselines provided by your software vendors.

- Keep machines up-to-date by rapidly applying the latest updates to your operating systems and applications, and immediately deploy critical security updates for OS, browsers, and email. Isolate (or retire) machines that cannot be updated or patched.

- Implement advanced email and browser protections. Deploy a secure email gateway that has advanced threat protection capabilities for defending against modern phishing variants.

- Enable host anti-malware and network defenses to get near real-time blocking responses from cloud (if available in your solution).

2. Implement access controls. Consider the following:

- Apply the principle of least privilege, which includes implementing network segmentation, removing local administrator privileges from end-users, and exerting caution when granting any permissions to applications running on the computer.
- Limit downloading of applications to only those from reliable sources (an official app store).
- Deploy strong code integrity policies, including restricting the applications that users can run. If possible, adopt a security solution that will restrict the code that runs in the system core (kernel) and can block unsigned scripts and other forms of untrusted code. Use application whitelisting.
- To learn about software supply chain attacks and how to protect against them, read this blog from Microsoft researchers.

3. Keep backups.

- Create destruction-resistant backups of your critical systems and data.
- Use cloud storage services for automatic backup of data online. For data that is on premises, regularly back up important data using the 3-2-1 rule. Keep three backups of your data, on two different storage types, and at least one backup offsite.

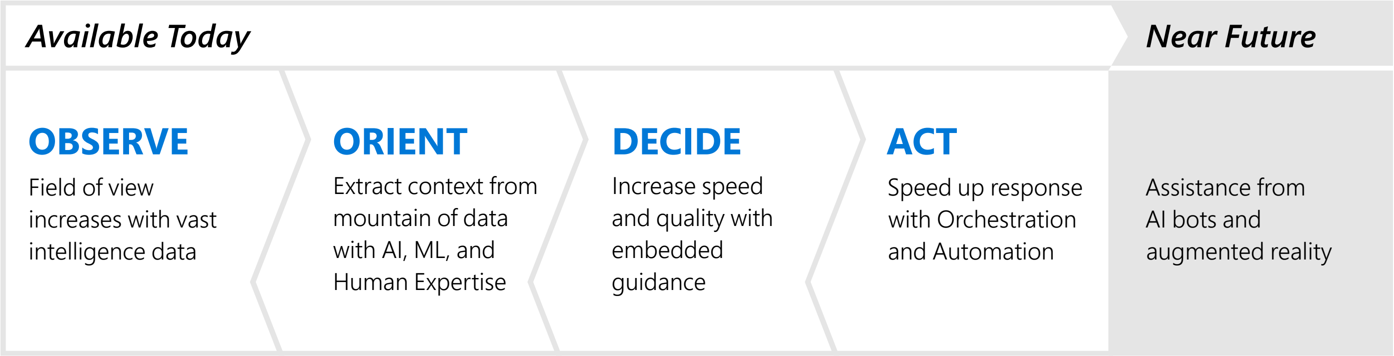
4. Be aware and act if you suspect anything.

- Teach employees to be wary of suspicious communications that request sensitive information and instruct them how to respond and report them to the organization's security operations team immediately. Training can also help mitigate social engineering and spear-phishing attacks.
- Be careful when clicking on web links. Practicing secure web browsing habits and using solutions that provide warnings about or block access to unsafe sites can help reduce the probability of encountering websites associated with cryptocurrency mining.
- If a computer is running exceptionally slow, look for any suspicious files that are running and feel free to submit a sample to the operating system vendor. You can submit files for malware analysis to Microsoft at https://www.microsoft.com/wdsi/filesubmission.

DETECTION AND RESPONSE:

Detection and response contribute to resiliency by limiting the time an attacker has access to your resources. This decreases attacker ROI by both increasing the attacker cost (they have to retry or modify their operations) and decreases return (limits probability of achieving their objective).

The same cloud technology that is enabling business organizations to better meet market needs can also help security operations better fight back against attackers.



Available Today

OBSERVE
Field of view increases with vast intelligence data

ORIENT
Extract context from mountain of data with AI, ML, and Human Expertise

DECIDE
Increase speed and quality with embedded guidance

ACT
Speed up response with Orchestration and Automation

Near Future

Assistance from AI bots and augmented reality

FIGURE 10.

Evolution trajectory of SOCs

As we look at the trajectory of Security Operations Centers (SOCs) evolution, we see technology continually increasing the speed and quality of SOC decisions and actions. Many of these innovations can be mapped to each stage of the Observe Orient Decide Act (OODA) "loop" that was documented by USAF Colonel John Boyd.[3]

OBSERVE – SOCs can tap into vast security intelligence available (from Microsoft and other sources) increasing their field of view dramatically within the organization and the external environment.

ORIENT – As these new data sources become available to already overloaded SOCs, machine learning (a subset of artificial intelligence) becomes a critical tool to reason over these massive datasets and identify anomalies worth investigating. Security vendors (including Microsoft) have adopted machine learning technology to quickly prioritize events (and help fuse these individual events into holistic incidents).

DECIDE – Because attack volume and complexity can quickly overload a SOC, analysts and incident responders need to make many decisions and act quickly in response to alerts and detections. Microsoft and other vendors have integrated automated investigation capabilities as well as guidance to help analysts quickly make good decisions (to isolate potentially infected or compromised devices, for example). For the moment, the automation is focused on quickly resolving low priority incidents so specialized skills can be applied to more complex problems.

ACT – Response requires rapid and accurate execution across many technologies and platforms, which is what security orchestration and response automation technologies enable. Microsoft and many others are continuing to invest in these technologies including modern threat detection and automated response solutions.

FOOTNOTES

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Some other trends that apply to a modern SOC are:

- **Quality over quantity of alert feeds** – As organizations shift from managing "not enough information" to managing "too much information", the time and attention of highly specialized SOC analysts becomes more and more valuable. This drives an increased need for quality in the alerts that require Tier 1 and 2 analyst engagement. While additional data feeds are always helpful for investigations and proactive hunting, Microsoft's Corporate IT SOC measures the true positive rate of alert feeds that require analyst response (and currently requires 90% or higher true positive rate).

- Data gravity – Analytics over large datasets (including security data) is difficult to do without access to the underlying raw data. As more security data is available, it becomes more economical and practical to perform the security analytics in the cloud vs. backhauling that data to an on-premises system. This will likely lead to evolution of SIEM and SOC architectures that may include hybrid SIEM approaches or adoption of native cloud SIEM as a service.

- **High context** – These types of detections are much more useful because of their ability to correlate datasets more effectively. While traditional network traffic based detections still provide some security value, raw network traffic typically lacks context to differentiate between legitimate activity and anomalous activity. We are seeing SOCs get a lot more value out of context rich detections like:

    - **Endpoint Detection and Response (EDR)** solutions that have deep context on the host activity
    - Identity based detections that include insight on normal user authentication patterns (locations, times, services accessed, etc.) and apply behavior analytics

These context rich detections are harder to evade by adversaries because they have to mimic a much more complex operation (vs. a few technical attributes of IP traffic).

Another lesson we have learned from major breaches at customers was the difficulty of rapidly responding to incidents when IT functions are partially or fully outsourced. We recommend reviewing your IT outsourcing contracts and service level agreements (SLAs) as well as supply chain vendors to ensure they are compatible with rapid security response. For more learnings from our incident investigations at customers, see the Incident Response Reference Guide (IRRG) at https://aka.ms/IRRG.

Data sources

Data sources

Microsoft has collected the data included in the Microsoft Security Intelligence Report through the course of providing a wide range of Microsoft products and services, as discussed in the Microsoft Privacy Statement. This data provides us valuable information about the security and operations of our products and services, as well as insights about the cybersecurity threat landscape generally. This data includes analytics from the following sources:[4]

- **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** is the search and decision engine that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users to help prevent infection.

- **Exchange Online** is the Microsoft-hosted email and productivity service. Exchange Online antimalware and antispam services scan billions of messages every year to identify and block spam and malware.

- **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 is not a replacement for an up-to-date real-time antivirus solution.

- **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.

FOOTNOTES

[4] Importantly, this data always goes through strict privacy and compliance boundaries before being used for security.

- **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 organizations and home users. Select subscription plans include access to Office 365 Advanced Threat Protection.

- Windows Security in Windows 10 provides real-time scanning and removal of malware and unwanted software. In addition, the latest version of Windows leverages rich contextual data such as machine configuration, device performance and health, and other such information to enhance security for customers. At the same time, we empower customers to be more informed about their privacy in Windows 10. Read this blog to learn about some of the ways Microsoft does so.

- **Windows Defender Advanced Threat Protection** is a service built into Windows 10 Anniversary Update and later versions 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.