THE NEW NORM

Trend Micro Security Predictions for 2020

TREND MICRO™ | research

THE FUTURE IS

Published by Trend Micro Research
Stock images under license from Shutterstock.com

THE NEW NORM

Trend Micro Security Predictions for 2020

The year 2020 marks the transition to a new decade, and recent notable events and trends signify a similar changeover in the threat landscape. Cybersecurity in 2020 and beyond will have to be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to advancing technological developments and global threat intelligence — only so defenders can keep up with and anticipate cybercrime mainstays, game changers, and new players.

The old paradigm, where networks are isolated behind a company firewall, is behind us. Gone are the days of using a limited stack of enterprise applications. The current paradigm demands a wide variety of apps, services, and platforms that will all require protection. Layered security that is applied to various implementation efforts and keeps up with ecosystem shifts will be crucial in tackling the broad range of threats.

Tried-and-tested methods — extortion, obfuscation, phishing — remain successful in attacks we see today, but new risks will inevitably emerge. The increased migration to the cloud, for instance, exacerbates human error: Misconfigurations contribute to the possibility of exponential compromise. The sheer number of connected assets and infrastructures further creates a slew of issues that opens doors to threats. Enterprise threats will be no less complex, mixing traditional risks with new technologies, like artificial intelligence (AI) in business frauds.

Our security predictions for 2020 reflect our experts' opinions and insights on current and emerging threats and technologies. The scenarios and developments described are of the possible future, where technological advances and evolved threats will be key drivers for landscape changes. This report intends to empower enterprises in making informed decisions in specific security focus areas that will present challenges and opportunities in 2020 and the coming decades.

THE FUTURE IS COMPLEX

D H G C I R
I A N O N I
F R I M T S
F D L P R K
I P Z L I Y
C U Z E C E
U L T X A T

The way the threat landscape has evolved over the years proves that threat actors remain undeterred from compromising systems for their own gain. They shift and adapt in their choice of attack vectors and tactics — prompting the need for users and enterprises to stay ahead.

Attackers will outpace incomplete and hurried patches.

System administrators will need to be vigilant when it comes to not only the timeliness of patch deployments but also the quality of the patches they deploy. Applying a patch of poor quality to critical systems could break important functionalities or lead to failure due to patch defects. Delaying the application of a patch, on the other hand, puts systems at risk of compromise due to an attack on a known vulnerability.

Patch-related issues leave open windows of exposure that attackers will use as points of entry. We anticipate more cases of patch bypass when the patch released is insufficient. For example, an attacker can trigger an exploit by changing a couple of lines to the fix's code. Last year, a patch for a then zero-day vulnerability in the Microsoft Jet Database Engine was found to be "incomplete," that is, the flaw was only limited and not eliminated.[1] This year, hackers exploited vulnerabilities in Cisco routers that were later found to have incomplete fixes.[2]

Attackers will count on users of open-source libraries to overlook fixes released by the library maintainers. They will also take advantage of patch gapping, wherein a vulnerability is exploited before the actual patch is shipped to the users of the downstream product that uses the vulnerable library.[3]

In cases where the patch does not eliminate the vulnerability or a gap exists in patch implementation, virtual patching can help by providing immediate protection and shielding from known and unknown vulnerabilities.

Cybercriminals will turn to blockchain platforms for their transactions in the underground.

The underground ecosystem will continue to evolve as cybercrime activities further proliferate. Trust will play a more critical role in underground markets, as evidenced by the implementation of vetting and escrow payments in high-risk transactions.[4] Blockchain will be seen as a new means to establish a distributed trust system among buyers and sellers; smart contracts will enable cybercriminals to formalize cryptocurrency payments and record them on the blockchain. To maintain anonymity and reduce the risk of exit scams, cybercriminals will turn to blockchain marketplaces that offer a decentralized way to facilitate transactions.[5]

Commodity malware like ransomware and the crime-as-a-service business model will still be perennial options for cybercriminals looking to easily profit from attacks.

Banking systems will be in the crosshairs with open banking and ATM malware.

Operators of mobile malware dedicated to attacking online banking and payment systems will be prolific in 2020. Online payments in Europe will see more activity as more banks confirm their support for mobile payments.[6] With the Revised Payment Service Directive (PSD2) now in effect in the European Union (EU), and other countries following suit with their own regulations,[7] "open banking" is not far from wider adoption. However, this also means several more security implications will affect the banking paradigm, from flaws in banking APIs to new schemes for phishing campaigns.[8] Industry players old and new must employ measures ranging from developing software that is secure by design to conducting regular security audits.

The commoditization of ATM crimeware will further gain ground. Variants of Cutlet Maker, Hello World, and WinPot have already been found being advertised for sale. We expect these ATM malware families to compete for dominance in the underground.[9]

Deepfakes will be the next frontier for enterprise fraud.

For years, email-based scams with evolved techniques[10] have been largely perpetrated by fraudsters in West Africa[11] — and we do not expect this to change. We do foresee fraud advancing in 2020 with new technologies, specifically artificial intelligence (AI). AI technology is being used to create highly believable counterfeits (in image, video, or audio format) that depict individuals saying or doing things that did not occur — commonly referred to as "deepfakes."[12] The rise of deepfakes raises concern: It inevitably moves from creating fake celebrity pornographic videos to manipulating company employees and procedures.

News of cybercriminals using an AI-generated voice in social engineering surfaced in 2019. An energy company was reportedly defrauded of US$243,000 by scammers who used AI to mimic the voice of the firm's CEO.[13] More attempts will exploit the technology, using deepfakes of decision-makers to deceive an employee into transferring funds or making critical decisions. There will be a shift from traditional business email compromise (BEC)[14] and technical support scams. Malicious actors will no longer rely solely on spoofing email addresses and will take advantage of the audiovisual element of deepfakes to lend more credence to their schemes. C-level executives will be prime targets for this kind of fraud since they are often in calls, conferences, media appearances, and online videos.[15]

Google has already released a vast dataset of deepfake videos to aid researchers in detecting forgeries.[16] While "deepfake scams" may be in their nascent stages, employees will have to learn to identify telltale signs of deepfakes, such as a different intonation, slow speech, and artificial-looking skin in videos. Additional verification steps in finance-related processes will also be crucial.

Managed service providers will be compromised for malware distribution and supply chain attacks.

Companies are increasingly relying on outsourcing for their day-to-day activities and needs. With that come apprehensions that attacks via the supply chain will bypass and jeopardize business processes[17] and security measures. The risk lies in putting unfettered trust in third parties like managed service providers (MSPs).

Supply chain attacks over the years have taken many forms, including hijacking a software update and compromising third-party services to get malicious code to target companies.[18] The latter is what we foresee will most affect small- to medium-sized businesses (SMBs) in 2020. If SMBs outsource parts of their infrastructure or operations, these third parties can become springboards for compromise.

Compromise in an MSP's supply chain can spread to other parties downstream. Malicious actors will target third-party service providers and load malicious code into their sites with the aim of harvesting customers' sensitive data, among others. Attackers will find distributors or suppliers with weak security postures to spread malware to customer organizations. For instance, a breach in a software provider's infrastructure allowed hackers to deploy ransomware on hundreds of dental offices' systems.[19] This trend will continue, if not pick up pace.

To prevent being hit by such malware attacks, enterprises should perform regular vulnerability and risk assessments and implement preventive measures, including thorough checks on providers and employees who have system access.

Attackers will capitalize on 'wormable' flaws and deserialization bugs.

In May, Microsoft released a fix for a critical remote code execution (RCE) vulnerability designated as CVE-2019-0708 and nicknamed BlueKeep. Since then, the company has rolled out similar updates for vulnerabilities that affect Remote Desktop Services in Windows. As the flaws are "wormable,"[20] any malware that exploits them can spread as quickly as WannaCry, which rapidly leapfrogged across the world and took down hundreds of thousands of computer systems in its wake in 2017. Developing an exploit to take advantage of BlueKeep, however, is a complex task that requires a high level of technical know-how. For instance, a Metasploit module that exploits the vulnerability was released but proved to be unwieldy, unlike the EternalBlue exploit.[21]

We will hear more of BlueKeep, and exploitation attempts on other known high-severity vulnerabilities will be forthcoming. Widely used protocols, such as Server Message Block (SMB) and Remote Desktop Protocol (RDP), will be in the spotlight for attackers seeking to exploit unprotected systems. The SMB protocol was notably the vehicle for the infamous WannaCry and NotPetya attacks. RDP is no stranger to security issues as well. Aside from being accessed by BlueKeep to run, it is also a common entry vector for ransomware;[22] attackers behind the SamSam ransomware scan for devices with exposed RDP connections.[23]

Other flaws that we expect to become a major concern for enterprises are deserialization bugs. Flaws involving deserialization of untrusted data are a highly critical class of vulnerabilities that, when exploited against enterprise applications, can modify data assumed safe from modification and allow the possible execution of attacker-controlled code.[24] Serialization is a technique that many programming languages use to translate an object into a format that can be stored or transmitted. Deserialization is the reverse of that process. One of the risks lies in how applications that accept serialized objects do not validate untrusted input before *deserializing* it. Skilled attackers will continue to take advantage of this by inserting a malicious object into a data stream and executing it on the app server.

Rather than finding several flaws to chain together for code execution, attackers can exploit deserialization bugs instead to easily gain complete remote control and execute code automatically even in complex environments. Serialization and deserialization are important concepts in Java applications and are common to many web applications and middleware products. Enterprises that use platforms supporting these mechanisms should practice immediate patching and virtual patching[25] as well as have awareness of system or software exploitability.

THE
FUTURE
IS

EXPOSED

The converged future ushers in old and new attacks and techniques that expose information technology (IT) and operational technology (OT) assets.

Cybercriminals will home in on IoT devices for espionage and extortion.

We foresee cybercriminals and threat actors using machine learning and AI to listen in on connected devices in enterprise settings, such as smart TVs and speakers. They can use language recognition and object identification to snoop on personal and business conversations. From there, they can identify a set of targets for extortion or gain a foothold for corporate espionage.

As for other forms of monetization for attacks against the internet of things (IoT), cybercriminals have yet to find a scalable business model that takes advantage of the wide attack surface the IoT affords, not to mention landscape changes like 5G networks. IoT attack monetization, while still in its infancy, will be tested in different ways by cybercriminals. Digital extortion[26] is the likeliest of these methods.

In underground communities, cybercriminals have been discussing how to compromise various types of connected devices for their moneymaking schemes. These schemes will be tried on consumer devices at first, with connected industrial machinery as the next logical target. We have already seen related discussions on vital programmable logic controllers (PLCs) that are used to control large-scale manufacturing equipment.[27]

IoT devices like routers will be monetized through botnets, which can be used subsequently as a distributed network for services offered to cybercriminals. It is not far-fetched to conjecture that router hacking will also come in the form of botnets used for Domain Name Server (DNS) hijacking, peddled as either crimeware or a service, primarily for phishing. Other offerings in the underground include access to webcams' video streams and smart meters with modified firmware. Such exposed devices will further put conversations on IoT security front and center — particularly how not all IoT devices have built-in security and are equipped to be properly protected against various attacks.

5G adopters will grapple with the security implications of moving to software-defined networks.

As 5G rollout gains momentum in 2020, we expect a variety of vulnerabilities simply on account of the newness of the technology, including its codes and dynamic switching between environments. Even with automation, the technology will still pose challenges not only because of inevitable code defects — vendors are also ill-equipped to address threats related to the technology.

Given that the 5G environment is a software-defined network that enables high-bandwidth and low-latency connectivity for users and connected devices, it is expected that the networks will service a wide range of applications and verticals. Threats related to 5G networks will stem from vulnerable software operations (i.e., the 5G network is managed by a potentially vulnerable software or supplier) and the distributed topology they afford (i.e., wider avenues for attacks, a large number of connected IoT devices). Attackers will seek to gain control of the software managing 5G networks to control the network itself. Additionally, upgrades involving 5G will be much like the software updates to smartphones and will entail vulnerabilities.[28] Researchers have already demonstrated how 5G vulnerabilities can be exploited in different ways using low-cost hardware and software platforms,[29] and it is safe to assume that cybercriminals are not far behind. Lack of security in 5G networks will also aggravate potential threats related to confidentiality (e.g., spying on data/traffic), integrity (e.g., modification of data transmitted), and availability (e.g., network disruption affecting interdependent sectors).[30]

The current measure of success for countries and vendors appears to be who gets to build 5G first, sacrificing security for speed. Putting 5G security as an afterthought, due to hasty migration and poor configurations, will pose challenges especially as more services become dependent on the technology. Applying security to 5G-enabled infrastructures post-deployment will be more complex than incorporating security from the start.[31] Mitigating consequences of inadequate protections will necessitate security professionals capable of identifying problems specific to software-defined networks.[32] If the network functions allow for dynamic shifting, then security must also be dynamic. For instance, in dynamic deployment of network services via network function virtualization (NFV) and application virtualization, security must also be able to keep up with rapid application deployment.

Critical infrastructures will be plagued by more attacks and production downtimes.

Utilities and other critical infrastructures (CIs) will still be viable targets for extortionists in 2020. Extortion through ransomware will still be cybercriminals' weapon of choice as the risk for companies is high. Prolonged production downtime translates to hefty monetary losses; production lines can be debilitated for weeks, depending on how long system restoration takes. Attackers can also assemble a botnet to mount a distributed denial-of-service (DDoS) attack against operational technology (OT) networks. Manufacturing companies that employ cloud service providers will be at risk of supply chain attacks; unsecure providers could serve as jumping-off points for threat actors to attack and immobilize production. Cyberattacks jeopardize availability, which is the top priority in these infrastructures, and the pressure to tighten cybersecurity for companies employing the industrial internet of things (IIoT) will only increase.[33]

Over the past years, different threat actors have targeted several energy facilities across the world in reconnaissance campaigns.[34] These activities for targeted ransomware attacks focus on getting access to credentials for industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems and gathering information on how the facilities operate. The impact of these compromises will propagate not only within the affected CI system but also across its interdependencies, with widespread consequences (e.g., disrupting local power plants and affecting energy supplies[35]).

This is not to say that system failure due to attacks will affect only the utilities industry. Food production, transportation, and manufacturing facilities will also be at risk as they increasingly use IoT applications and human-machine interfaces (HMIs) as their main hub for managing diagnostic and controller modules.

Public CIs and government IT infrastructures will find themselves open to attacks for longer than private industrial environments, as these areas of the public sector tend to be underfunded. Information gathered in reconnaissance campaigns will give threat actors opportunities for more coordinated attack attempts to disrupt not just infrastructures but also public services and political processes.

Home offices and other remote-working setups will redefine supply chain attacks.

Organizations will have to be wary of risks introduced by work-from-home arrangements and internet-connected home devices that blur the lines in enterprise security. After all, working in home environments is not as secure as being in the corporate network. Furthermore, weak Wi-Fi security compounds risks in remote work arrangements like shared or public workspaces. An open network leaves sensitive files and information exposed for snooping by other users in the same network.[36] Remote devices can be infected with malware that can get into the corporate network and make off with valuable information.

Today's mobile workforce is no longer tethered to a computer in a traditional office setting. Unlike in a bring-your-own-device (BYOD) setup, employees working from home can move between multiple connected devices to access cloud-based apps and communication software. Connected home devices serving as a gateway for enterprise attacks is an unavoidable development considering how employees may find these devices (e.g., smart TVs, speakers, and assistants) convenient for work use as well. Enterprises will have to decide on what information security policies to implement to deal with such scenarios.

Using the troves of personal information they have already amassed, cybercriminals will design enterprise attacks using home and public networks by impersonating employees. These increasingly sophisticated attacks will extend business email and process compromise well past simple redirection of funds or malware infection. The employee's home environment will become a launch point for supply chain attacks.

THE FUTURE IS MISCONFIGURED

Cloud and DevOps migrations present risks as well as rewards to adopters, underscoring the need for security throughout the deployment pipeline.

Vulnerabilities in container components will be top security concerns for DevOps teams.

The container[37] space is fast-paced. Releases are quick, architectures are continually integrated, and software versions are regularly pushed. Traditional security practices will not be able to keep up.

This highlights the importance of DevSecOps principles for DevOps teams as containers upend more conventions and shoulder more roles that are critical to organizations. Rapid development cycles may leave only little room for security and vulnerability testing. An application may now require an organization to secure hundreds of containers spread across multiple virtual machines in different cloud service platforms. Organizations will have their hands full with issues in different components of the container architecture, including vulnerabilities in runtimes (e.g., Docker, CRI-O, Containerd, and runC[38]), orchestrators (e.g., Kubernetes), and build environments (e.g., Jenkins). Attackers will find ways to take advantage of any weak link to compromise the DevOps pipeline.

Vulnerabilities in widely used container images have a detrimental effect on the enterprise pipeline if they are subsequently downloaded. Patching containers will be particularly tricky if organizations rely on a third party for the image fix, trusting that it is secure. Vulnerabilities in containerized applications will affect not only the container code or engine but also many other elements across the stack, which malicious actors can move in on for access and control.

Serverless platforms will introduce an attack surface for misconfiguration and vulnerable codes.

More enterprises are embracing serverless platforms to integrate cloud applications and reduce costs. Gartner projects that more than 20% of global enterprises will have serverless computing technologies deployed by 2020.[39] Serverless platforms offer "function as a service," allowing developers to execute codes without the organization having to pay for entire servers or containers.[40] However, going serverless does not mean immunity from security problems.

We expect outdated libraries, misconfigurations, and known and unknown vulnerabilities to be threat entry points to serverless applications. Attackers can take advantage of these to gather sensitive information or penetrate enterprise networks.[41]

Serverless platforms also include containers, serverless functions, and other dependencies, further underscoring the complexity of where a threat may originate from. Since serverless computing renders functions, especially those that are open-source, as stateless, monitoring permissions and storing sensitive data will additionally be top concerns in 2020. Besides increasing network visibility, improving processes and documenting workflows will be essential to running serverless applications.

As it is in container-based applications, DevSecOps should also be at the forefront of the serverless deployment. Serverless environments will also benefit from the continuous integration and ease of use that DevSecOps aspires to.[42] Security tools that tackle serverless infrastructures, including open-source application dependencies and vulnerabilities, will be important in serverless adoption and deploying specific functions.

User misconfigurations and unsecure third-party involvement will compound risks in cloud platforms.

An organization can still be at risk despite regularly updating systems and putting up appropriate measures if there are misconfigured applications and authentication issues in the deployment. Basic security controls that are not implemented properly will be a huge security threat to organizations' data.

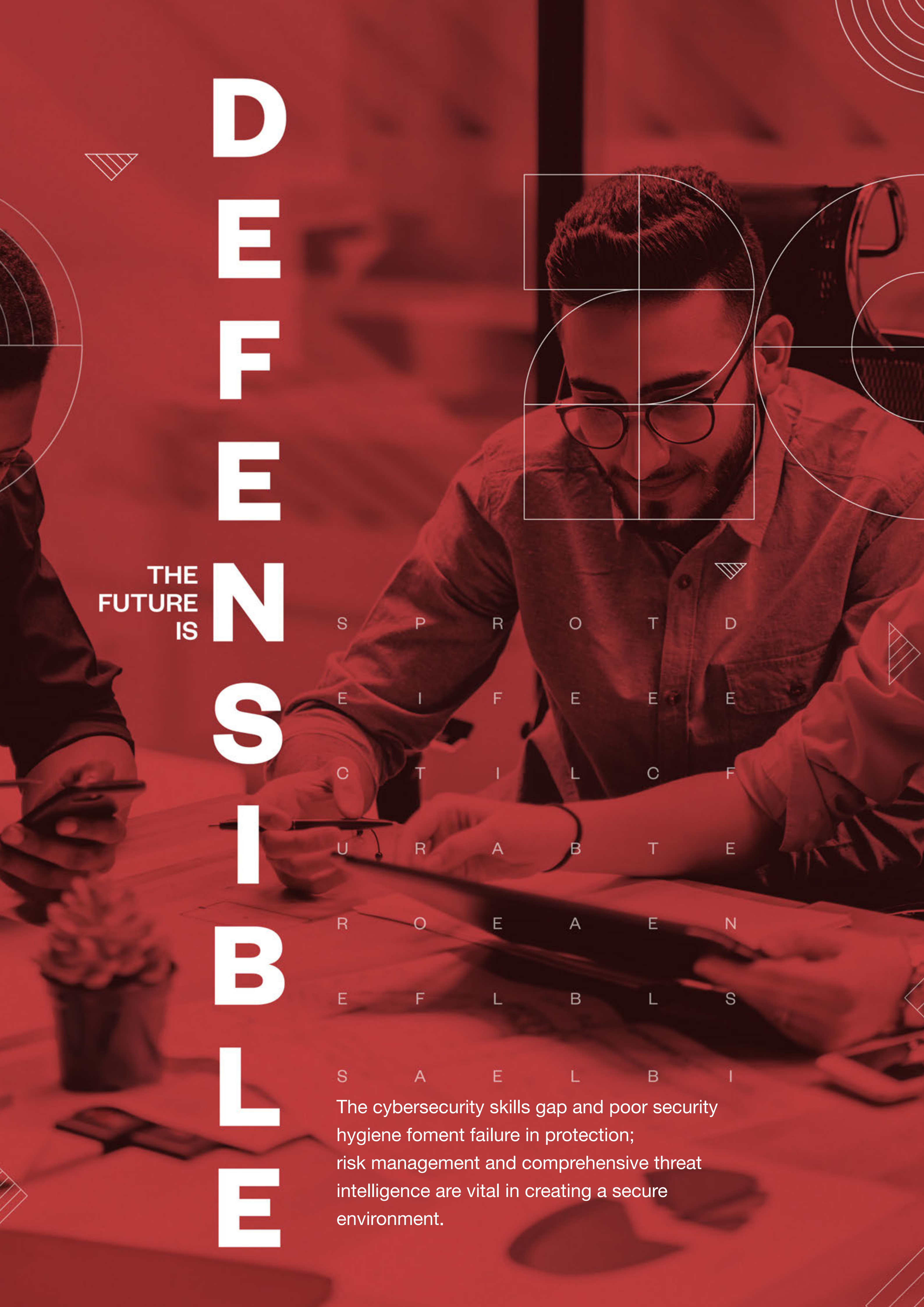
We foresee more incidents of compromised networks due to cloud services' weak points. Misconfigurations in cloud storages that cause data leakage will still be a common security issue for organizations in 2020. Insufficient access restrictions, mismanaged permission controls, negligence in logging activities, and publicly exposed assets are only a few of the missteps companies will make as they set up their cloud networks. Mistakes and failures involving cloud services will expose a significant number of company records and even lead to incursion of fines and penalties. These risks can be curbed by improving the overall cloud security posture (i.e., properly configuring and deploying infrastructures) and ensuring that best practices and industry standards are upheld.

As more companies and productions (e.g., manufacturing facilities)[43] move to the cloud, third-party service providers will be increasingly involved. However, there also lies the risk that these vendors may not be experienced with the cloud (i.e., used to traditional processes and systems) and equipped to protect the infrastructure. Attackers will be motivated to perform DDoS attacks against service providers via botnets to disrupt cloud services.

Cloud platforms will fall prey to code injection attacks via third-party libraries.

More compromises in cloud platforms will happen in 2020 by way of code injection attacks, either directly to the code or through a third-party library. Malware injection can be done in an attempt to eavesdrop or take control of a user's files and information on the cloud. Common forms of such attacks in cloud services' web applications are cross-site scripting attacks and SQL injection attacks. Successful attacks allow hackers to remotely retrieve sensitive data and manipulate database content. On the other hand, attackers can go in a different route with third-party libraries that, when downloaded by users, execute injected malicious code.[44]

Meanwhile, we foresee more attackers following data to the cloud. Cloud breaches will be expected as software-, infrastructure-, and platform-as-a-service cloud computing models are being widely adopted. The more corporate data resides in the cloud, the more malicious actors get interested. Preventing cloud compromises will require due diligence from developers, careful consideration of providers and the platforms offered, and improvements in cloud security posture management.



THE FUTURE IS DEFENSIBLE

S P R O T D

E I F E E E

C T I L C F

U R A B T E

R O E A E N

E F L B L S

S A E L B I

The cybersecurity skills gap and poor security hygiene foment failure in protection; risk management and comprehensive threat intelligence are vital in creating a secure environment.

Predictive and behavioral detection will be crucial against persistent and fileless threats.

Threats that "live off the land" will continue to evade traditional blacklisting techniques.[45] Enterprises will have to consider solutions with behavioral indicators, sandboxing, and traffic monitoring. Given that these threats are planted in the registry, reside in a system's memory, or abuse normally whitelisted tools like PowerShell and Windows Management Instrumentation (WMI), tracking non-file-based indicators such as specific execution events or behaviors will be important for detection. Fileless techniques will also continue to be notable for other forms of attacks that deploy banking trojans,[46] cryptocurrency-mining malware,[47] and ransomware.[48]

Aside from Linux threats that focus on infecting IoT devices to make them part of a DDoS botnet,[49] Linux-based malware will also experience a sustained upsurge as the open-source system becomes an important, if not the primary,[50] component in enterprise platforms. In addition, malware variants with information-stealing capabilities will increase, as these are reliable for gathering information that can be used to penetrate more deeply into networks. We expect these threats to persist in enterprise systems through various means — including fileless techniques — ready to respawn their processes for further attacks.

The MITRE ATT&CK Framework will play a bigger role in how enterprises assess security.

The MITRE ATT&CK Framework provides a comprehensive matrix for security evaluation. Its public knowledge base uses known attacks to classify and explain adversary tactics and techniques.[51] We expect more enterprises to assess threat models, security products, and organizational risks through the lens of the framework. Aside from threat hunters getting a better grip on attacks and patterns, defenders will also benefit from gauging the effectiveness of mitigations and security tools. The MITRE ATT&CK knowledge base can act as a common resource for security managers and cybersecurity providers, streamlining how intelligence on attacker techniques and defensive measures is shared.

Threat intelligence will need to be augmented with security analytics expertise for protection across security layers.

We anticipate attacks in 2020 and beyond to be more thoroughly planned, spread out, and varied in terms of tactics. Threat intelligence and security analyses will help organizations to defend their environments proactively by identifying security gaps, eliminating weak links, and understanding attacker strategies. Comprehensive threat intelligence infused into security and respective risk management processes will be invaluable to organizations looking to mitigate risks before any attacks occur.

Compromise through advanced threats, persistent malware, common phishing, potential zero-days, and other attacks can be prevented if insights and protection are readily available. Having complete environment visibility enables organizations to have an effective prevention methodology for detecting threats and deflecting attacks in real time. This means having better context beyond the endpoint, encompassing email, server, cloud workloads, and networks as well.

Organizations will acknowledge that the cybersecurity skills gap and poor security hygiene are still significant factors in the 2020 threat landscape. Decision-makers and IT managers will recognize the need for a bigger picture of what is happening in their enterprise environments. Security experts like security operations center (SOC) analysts will help get that consolidated point of view and correlate findings with global threat intelligence.

CYBERSECURITY IN 2020

Collaborating with security experts will be essential in mitigating risks in all areas of the enterprise cyber infrastructure. This will allow defenders and developers to gain further visibility and control over their connected devices and address their weak points. Real-time and zero-hour detection will also be crucial in proactively identifying known and unknown threats.

The ever-shifting landscape will require a cross-generational blend of multilayered and connected defense powered by security mechanisms such as:

- **Complete visibility.** Provides prioritized and optimized examination of threats with tools and expertise that mitigate impact and remediate risks.
- **Threat prevention with effective mitigation.** Automatically mitigates threats once visualized and identified, alongside antimalware, machine learning and AI, application control, web reputation, and antispam techniques.
- **Managed detection and response.** Provides security expertise that can correlate alerts and detections for threat hunting, comprehensive analysis, and immediate remediation using optimized threat intelligence tools.
- **Behavior monitoring.** Blocks advanced malware and techniques proactively and detects anomalous behaviors and routines associated with malware.
- **Endpoint security.** Protects users through sandboxing, breach detection, and endpoint sensor capabilities that prevent attacks and secure data.
- **Intrusion detection and prevention.** Deters suspicious traffic like command-and-control (C&C) communication and data exfiltration.

References

1. Catalin Cimpanu. (13 October 2018). *ZDNet.* “Microsoft JET vulnerability still open to attacks, despite recent patch.” Last accessed on 8 October 2019 at https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/.
2. Ionut Arghire. (29 March 2019). *Security Week.* “Cisco Improperly Patched Exploited Router Vulnerabilities.” Last accessed on 30 October 2019 at https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnerabilities.
3. Catalin Cimpanu. (9 September 2019). *ZDNet.* “Security researchers expose another instance of Chrome patch gapping.” Last accessed on 8 October 2019 at https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/.
4. Vladimir Kropotov, Fyodor Yarochkin, and Michael Ofiaza. (7 January 2019). *Trend Micro Security News.* “Your Word is Your Bond: Trust and Ethics in Underground Forums.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/your-word-is-your-bond-trust-and-ethics-in-underground-forums.
5. Europol. (9 October 2019). *Europol.* “Cybercrime Is Becoming Bolder With Data At The Centre Of The Crime Scene.” Last accessed on 11 October 2019 at https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene.
6. Apple. (1 October 2019). *Apple.* “Apple Pay participating banks in Europe and the Middle East.” Last accessed on 8 October 2019 at https://support.apple.com/en-gb/HT206637.
7. PwC. (n.d.). *PwC Italia.* “Open Banking… so what?” Last accessed on 28 October 2019 at https://www.pwc.com/it/en/industries/banking/future-open-banking.html.
8. Feike Hacquebord, Robert McArdle, Fernando Mercês, and David Sancho. (17 September 2019). *Trend Micro Security News.* “The Risks of Open Banking.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.
9. Numaan Huq, Vladimir Kropotov, Mayra Rosario, David Sancho, and Fyodor Yarochkin. (28 June 2019). *Trend Micro Security News.* “Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
10. Europol. (2018). *Europol.* “Internet Organised Crime Threat Assessment 2018.” Last accessed on 16 October 2019 at https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
11. The United States Department of Justice. (10 September 2019). *US Department of Justice.* “281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes.” Last accessed on 16 October 2019 at https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds.
12. J.M. Porup. (10 April 2019). *CSO Online.* “How and why deepfake videos work — and what is at risk.” Last accessed on 11 October 2019 at https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
13. Catherine Stupp. (30 August 2019). *The Wall Street Journal.* “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case.” Last accessed on 11 October 2019 at https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
14. Trend Micro. (n.d.). *Trend Micro.* “Business Email Compromise (BEC).” Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec).
15. Liam Tung. (4 September 2019). *ZDNet.* “Forget email: Scammers use CEO voice ‘deepfakes’ to con workers into wiring cash.” Last accessed on 16 October 2019 at https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/.
16. Nick Dufour and Andrew Gully. (24 September 2019). *Google AI Blog.* “Contributing Data to Deepfake Detection Research.” Last accessed on 23 October 2019 at https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html.
17. Trend Micro. (n.d.). *Trend Micro.* “Business Process Compromise (BPC).” Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise.
18. Chaoying Liu and Joseph C. Chen. (16 January 2019). *Trend Micro Security Intelligence Blog.* “New Magecart Attack Delivered Through Compromised Advertising Supply Chain.” Last accessed on 11 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.
19. Catalin Cimpanu. (29 August 2019). *ZDNet.* “Ransomware hits hundreds of dentist offices in the US.” Last accessed on 24 October 2019 at https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.
20. Simon Pope. (13 August 2019). *Microsoft Security Response Center.* “Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182).” Last accessed on 8 October 2019 at https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/.
21. Dan Goodin. (7 September 2019). *Ars Technica.* “Exploit for wormable BlueKeep Windows bug released into the wild.” Last accessed on 24 October 2019 at https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/.
22. Jay Yaneza. (9 February 2017). *Trend Micro Security Intelligence Blog.* “Brute Force RDP Attacks Plant CRYSIS Ransomware.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/.
23. Trend Micro. (23 March 2018). *Trend Micro Security News.* “SAMSAM Ransomware Suspected in Atlanta Cyberattack.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack.
24. MITRE. (19 September 2019). *Common Weakness Enumeration.* “CWE-502: Deserialization of Untrusted Data.” Last accessed on 8 October 2019 at https://cwe.mitre.org/data/definitions/502.html.
25. Trend Micro. (25 October 2018). *Trend Micro Security News.* “Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited.” Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited.
26. Trend Micro. (n.d.). *Trend Micro.* “Digital Extortion.” Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion.

27. Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho. (10 September 2019). *Trend Micro Security News.* “Uncovering IoT Threats in the Cybercrime Underground.” Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground.

28. Tom Wheeler and David Simpson. (3 September 2019). *The Brookings Institution.* “Why 5G requires new approaches to cybersecurity.” Last accessed on 16 October 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

29. Altaf Shaik and Ravishankar Borgaonkar. (2019). *Black Hat.* “New Vulnerabilities in 5G Networks.” Last accessed on 16 October 2019 at https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf.

30. Trend Micro. (14 October 2019). *Trend Micro Security News.* “EU Report Highlights Cybersecurity Risks in 5G Networks.” Last accessed on 17 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks.

31. Tom Wheeler and David Simpson. (3 September 2019). *The Brookings Institution.* “Why 5G requires new approaches to cybersecurity.” Last accessed on 6 November 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

32. Craig Gibson, Vladimir Kropotov, Philippe Lin, Rainer Vosseler, and Fyodor Yarochkin. (4 April 2019). *Trend Micro Security News.* “Securing Enterprises for 5G Connectivity.” Last accessed on 16 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity.

33. Trend Micro. (15 August 2019). *Trend Micro Security News.* “Securing the Industrial Internet of Things: Protecting Energy, Water and Oil Infrastructures.” Last accessed on 30 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures.

34. Trend Micro. (11 April 2019). *Trend Micro Security News.* “New Critical Infrastructure Facility Hit by Group Behind TRITON.” Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton.

35. Trend Micro. (22 December 2017). *Trend Micro Security News.* “TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems.” Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/.

36. Alfred Ng. (19 September 2019). *CNET.* “WeWork’s weak Wi-Fi security leaves sensitive documents exposed.” Last accessed on 31 October 2019 at https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/.

37. Trend Micro. (n.d.). *Trend Micro.* “Container.” Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/container.

38. Trend Micro. (28 February 2019). *Trend Micro Security News.* “CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine.” Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine.

39. Gartner, Inc. (4 December 2018). *Gartner.* “Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019.” Last accessed on 24 October 2019 at https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.

40. Scott Fulton III. (9 April 2019). *ZDNet.* “What serverless computing really means, and everything else you need to know.” Last accessed on 24 October 2019 at https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.

41. Guy Podjarny. (15 May 2018). *The Register.* “Hey cool, you went serverless. Now you just have to worry about all those stale functions.” Last accessed on 10 October 2019 at https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.

42. Trend Micro. (13 April 2018). *Trend Micro Security News.* “Serverless Applications: What They Mean in DevOps.” Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.

43. Willem Sundblad. (18 July 2019). *Forbes.* “Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy.” Last accessed on 10 October 2019 at https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.

44. Trend Micro. (29 November 2018). *Trend Micro Security News.* “Hacker Infects Node.js Package to Steal from Bitcoin Wallets.” Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets.

45. Trend Micro. (29 July 2019). *Trend Micro Security News.* “Risks Under the Radar: Understanding Fileless Threats.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.

46. Henry Alarcon Jr. and Raphael Centeno. (4 March 2019). *Trend Micro Security Intelligence Blog.* “Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/.

47. Augusto Remillano II and Arvin Macaraeg. (12 April 2019). *Trend Micro Security Intelligence Blog.* “Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/.

48. Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhat, and Joelson Soares. (29 March 2019). *Trend Micro Security Intelligence Blog.* “Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/.

49. Mark Vicente, Byron Galera, and Augusto Remillano II. (3 April 2019). *Trend Micro Security Intelligence Blog.* “Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/.

50. Steven Vaughan-Nichols. (1 July 2019). *ZDNet.* “Microsoft developer reveals Linux is now more used on Azure than Windows Server.” Last accessed on 30 October 2019 at https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server.

51. The MITRE Corporation. (n.d.). *MITRE.* “ATT&CK.” Last accessed on 11 October 2019 at https://attack.mitre.org/.

For Raimund Genes (1963-2017)

Trend Micro Security Predictions for 2020

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com