

TOWARD A NEW MOMENTUM

TREND MICRO SECURITY PREDICTIONS FOR 2022



TOWARD A NEW MOMENTUM

TREND MICRO SECURITY PREDICTIONS FOR 2022



05

Cloud Threats

Enterprises will ensure that cloud security basics are employed to defend their environments against a slew of cloud security threats and achieve a managed level of risk



08

Ransomware Threats

To remain protected against evolving ransomware threats, enterprises will set their sights on protecting their servers with stringent server-hardening and application control policies



11

Vulnerability Exploits

Security teams will need to be well-equipped to contend with malicious actors intent on repurposing older vulnerabilities and exploiting newly found ones in a matter of days, if not hours



14

Commodity Malware Attacks

Malicious actors will continue to think of smaller businesses as easy prey, but cloud-heavy SMBs will come prepared with security measures that can fend off commodity attacks



17

IoT Threats

Enterprises will strive for improved network monitoring and visibility to safeguard their IT environments against threats arising from IoT adoption



20

Supply Chain Threats

As they focus on making their supply chains more robust via diversification and regionalization, enterprises will implement zero trust principles to keep their environments more secure



23

Full speed ahead for cybersecurity

Published by Trend Micro Research

Stock images used under license from Shutterstock.com

TOWARD A NEW MOMENTUM

TREND MICRO SECURITY PREDICTIONS FOR 2022

2021 marked a turning point for organizations big and small, as the ongoing lockdown drove many to expedite their digital transformations and embrace hybrid work models. Now, well over a year into the Covid-19 pandemic, these companies must prepare to shift gears once again as the world finds its footing in yet another new normal — one that prioritizes the hybrid work model and is, hopefully, at the tail end of the global health crisis.¹

Malicious actors are poised to move in on the opportunities arising from a business landscape still in flux. New pain points are bound to arise as the push for digital transformations continues to redefine organizations' attack surfaces. However, companies will be prepared to curb these threats by hardening their defenses with a multitude of tools and best practices.

Coming into 2022, emerging threats will continue to test the resilience of supply chains around the world. The fourfold extortion model that has been gaining popularity among malicious actors will spell operational disruptions with far-reaching impact not only on the victims themselves but on their customers and partners as well.

Cloud adopters will need to shore up their defenses on multiple fronts, especially if they are to weather attacks from actors intent on both using tried-and-true methodologies and innovating by following new technology trends. The introduction of new cryptocurrencies in 2022 will require security teams to stay on top of any cybercriminals attempting to infiltrate and abuse corporate resources for their cloud-computing capabilities. We also expect malicious actors to increasingly target build systems and developer credentials as points of entry to cloud services and applications. Consequently, developers will have to ensure that their credentials stay out of reach of attackers looking to compromise their systems.

We expect an unprecedented number of vulnerabilities to be unearthed in the year ahead as a result of more vulnerability hunters looking to collect big bug bounties and of increased media attention on vulnerabilities. We foresee this leading to a surge in zero-day exploits that will beat 2021's record-setting number of zero-day exploits in active use.² The patch gap will leave unprotected enterprises at the mercy of malicious actors eager to home in on any weak spots in IT infrastructures by stacking multiple vulnerabilities to create new, multiplatform threats.

We see two trends brewing in the ransomware ecosystem in 2022. Enterprises will have to steel themselves against modern ransomware threats, which are set to become even more targeted and prominent. And ransomware operators will be employing increasingly complex extortion methods, such as exfiltrating data in order to weaponize it. Their attacks will pose a challenge for security teams, as many enterprises have yet to invest in securing their servers as much as they have invested in securing their endpoints.

While enterprises will be busy fending off targeted attacks, malicious actors with updated toolboxes will have better success with smaller businesses, thanks in large part to malware brokers selling commoditized tools of the trade. The new wave of commodity malware set to arrive next year will likely include the introduction of a particularly insidious botnet-as-a-service model, capable of compromising multiple platforms.

Further developments in smart devices will fuel the cybercriminal underground's growing interest in the internet of things (IoT), expanding beyond the smart devices themselves. Instead, cybercriminals will cast their eyes on the ever-growing volume of connected car data, a sought-after commodity that promises to be a new revenue stream for automakers. This will present an opportunity for security vendors and car manufacturers to come together to write up the roadmap for a new class of secure smart cars.

Ultimately, 2022 will be a period of transition that will be rife with possibilities for companies and cybercriminals alike. This report details our threat experts' security insights and predictions for the coming year, with a view to helping organizations make more informed decisions on various security fronts.

CLOUD THREATS

Cloud Threats

Enterprises will ensure that cloud security basics are employed to defend their environments against a slew of cloud security threats and achieve a managed level of risk

▶▶▶

Cloud attackers will both pivot and stay put; they will shift left to follow technology trends and continue to use tried-and-true attacks to wreak havoc on cloud adopters

The cloud,³ with its seemingly endless capacity to store and process vast amounts of data, has enabled companies to transition to remote work with relative ease after the Covid-19 pandemic broke out.⁴ And in the coming year, cloud migration will remain to be a key aspect of the new business operations norm. Gartner predicts that global cloud services spending will reach over US\$482 billion in 2022, a 54% increase from 2020's US\$313 billion.⁵ And as users continuously migrate to the cloud, malicious actors are bound to follow suit.

To maximize their financial gain, malicious actors will make sure to cover all the bases. They will continue to wage tried-and-true types of attacks and at the same time carry out ones that use new trends in technology to stay ahead of the game.

Not only will enterprises continue to use software-as-a-service (SaaS) applications and solutions, but adoption is set to expand in the coming year. Gartner forecasts that SaaS users will spend about US\$172 billion in 2022, the highest spending among all public cloud services.⁶ And because the tactics, techniques, and procedures (TTPs) employed by malicious actors are still working — and will likely still work for a new crop of SaaS adopters — they will continue to use these in 2022.

Malicious actors will still use low-effort but high-impact strategies in gaining access to cloud applications and services. Their use of phishing emails to steal credentials is one example of a method that will persist in the coming year. They will also continue to compromise SaaS applications and services via unsecured secrets,⁷ unrotated access keys, unsecure container images obtained from untrusted sources,⁸ and immature or poorly implemented identity access control management policies. Indeed, cybercriminals generally gravitate toward strategies that work. Malicious actors, for example, are still exploiting known vulnerabilities from past years because many environments are still not patched. On top of exploiting new vulnerabilities that will be discovered in the coming year, they will continue to use old ones that still work.

We expect to continue seeing cybercriminal groups such as TeamTNT targeting the cloud's computing power to illicitly mine cryptocurrency in the coming year.⁹ As more digital currencies emerge, cybercriminal units will continue to piggyback on victims' cloud computing resources using iterations of previously seen attacks.

On the other hand, cybercriminals will also be following technology trends. Any technology that gets widely adopted becomes a lucrative target for attackers, as in how malicious actors have targeted technologies such as Java,¹⁰ Adobe Flash,¹¹ and WebLogic.¹²

An interesting albeit nefarious side effect of the shift-left movement is that attackers will start to increasingly use this approach in their attacks. We are already seeing malicious actors targeting DevOps¹³ tools and pipelines in cloud integrated development environments (IDEs).¹⁴ We predict that cybercriminals will wage more campaigns using DevOps principles on supply chains, Kubernetes environments, infrastructure-as-code (IaC) deployments, and pipelines. We also predict that developers and build systems will serve as initial entry points for attackers looking to spread malware across multiple companies via supply chain attacks. Developers' tokens and passwords hold the keys to enterprises' operations, and using a compromised developer's credentials also increases an attacker's chances of deploying malware under the radar.

Cloud adoption is a fundamental element of digital transformation. Thus, it is important for enterprises to keep their cloud environments secure by going back to the basics of cloud security, which include understanding and applying the shared responsibility model,¹⁵ using a well-architected framework,¹⁶ encrypting, patching,¹⁷ and bringing in the right level of expertise. Enterprises will also need to enforce tighter security protocols around build systems and the code that developers check in, especially if the submitted code will have a hand in important production processes. To this end, security teams can apply measures such as including managing privileges with short-lived access tokens, developing an audit trail using command-line tools, and monitoring the pipeline by way of open-source security management software.

Ransom●ware Threats

To remain protected against evolving ransomware threats, enterprises will set their sights on protecting their servers with stringent server-hardening and application control policies



Servers will be the main ransomware playground

Like any insidious cyberthreat, ransomware¹⁸ survives and thrives by evolving steadily. Before, ransomware incidents usually involved endpoints as primary entry points, with victims falling prey to attacks by opening malicious emails or visiting malicious websites that surreptitiously deployed ransomware payloads.¹⁹ But when the pandemic happened, we saw an obvious shift in how ransomware operators carried out their attacks.

Malicious actors who want to gain access to target organizations are now focusing on exposed services and service-side comprises. And as hybrid work, a model wherein employees work both remotely and on-site, becomes the new norm for organizations,²⁰ we foresee this trend continuing in the coming year. The hybrid work model has many pros, such as increased flexibility and productivity, but it also comes with some undeniable cybersecurity cons. Because of the increased attack surface from less secure home-working environments and servers, it is difficult to pinpoint how malicious actors are coming in and waging attacks — and how cybersecurity teams can stop ransomware attacks at time zero.

Based on the security incidents we have observed this year, we also expect to see two major developments in ransomware in the coming year.²¹ First, ransomware attacks will become more targeted and highly prominent, making it harder for enterprises to defend their networks and systems against these attacks. Because modern ransomware is relatively new, it is very possible that enterprises have yet to make the same ransomware mitigation and defense investments for servers as they have made for endpoints. In addition, the continuing lack of skilled cybersecurity specialists is an aggravating factor with regard to securing organizations against ransomware threats.²² The TTPs used by ransomware operators will likely stay the same, but they will be used to go after more complex targets, ones that will possibly be bigger than the major targets of previous years.

The second development that we foresee is that ransomware operators will also use more modern and sophisticated methods of extortion that will resemble nation-state advanced persistent threat (APT) attacks.²³ Once attackers are able to infiltrate their victims' environments, they can opt to just exfiltrate sensitive data and go straight to extorting their victims, skipping the encryption or access blocking step altogether. In terms of the primary means of successful extortion, the focus will veer away from denial of access to critical data in favor of leaking and mining stolen data for weaponization. Attack vectors used by ransomware operators to target enterprises, such as virtual private networks (VPNs), spear-phishing emails, and exposed remote desktop protocol (RDP) ports, will remain at play. However, in 2022, the cloud will be targeted more often. As more enterprises migrate to the cloud,²⁴ they bring with them their sensitive data and resources, prompting cybercriminals to follow suit.²⁵

On top of employing security best practices to keep servers secure, enterprises will benefit from strict adherence to server-hardening guidelines for all pertinent operating systems and applications. Ensuring that servers are properly configured will help defend enterprises against ransomware attacks and other threats.

Since servers have a predictable set of applications based on their specific roles, it is also advisable for organizations to employ application control. This security practice allows applications to block or restrict applications except those that have been safelisted by IT teams.



Vulnerability Exploits



Security teams will need to be well-equipped to contend with malicious actors intent on repurposing older vulnerabilities and exploiting newly found ones in a matter of days, if not hours

Made more vigilant by dealing with the record high of zero-day exploits found in 2021, enterprises will be on high alert for potential patch gaps as more vulnerabilities are expected to be unearthed

The coming year promises to rival the all-time high of zero-day exploits that has helped shape the threat landscape of 2021: 66 zero-day exploits have been found in the wild at the time of writing of this report, which is higher than in any other year on record.²⁶ We foresee that even more in-the-wild zero-day exploits will be discovered in 2022, which will not necessarily suggest a drop in code quality, but rather will be fueled by various factors. These factors will include growing media interest in covering headline-making exploits, vulnerability hunters keen on bagging lucrative bug bounties²⁷ like those offered by Trend Micro's Zero Day Initiative (ZDI) in an effort to prevent zero-day attacks,²⁸ and implementation mistakes and oversights that will arise as more companies undergo digital transformations. It is possible that only a portion of actively exploited vulnerabilities will be found by the cybersecurity industry, so the discovery of more vulnerabilities will also point to increasingly effective detection methods and changing attitudes around disclosure.²⁹ Bug bounty programs have made great strides toward the early detection of vulnerabilities to the benefit of enterprises, as evidenced by how ZDI incentives contributed to the development of virtual patches for customers of the Trend Micro™ TippingPoint™ security solution, averaging 81 days ahead of a vendor's publicly released patch in 2020.³⁰

However, if the success of previous Pwn2Own hacking contests³¹ is any indication, the window for weaponizing vulnerabilities will be whittled down to a matter of days, if not mere hours, and exploits will be written for bugs fixed in beta before their patches can be released to the general consumer. The patch gap — the time between the discovery of a vulnerability and when a patch is rolled out to address it — will remain a gold mine for opportunistic actors, who will no doubt count on delays in the rollout of critical bug fixes to give them ample time to develop their exploits. Delays in the scheduled deployment of patches can occur when bug fixes need to undergo testing in software, as was the case when a fix for Google Chrome's V8 JavaScript engine was made available to browser users with the release of Chrome 77 in September 2019, a month after the V8 bug was already patched.³² This will leave enterprises in a tough position, as they contend with the two-pronged challenge of anticipating accelerated exploits during the waiting period for bug fixes and implementing them as soon as they are rolled out. Addressing these vulnerabilities is not a uniform process; for example, patching endpoints is more streamlined than patching servers, which often incurs more downtime costs.³³

Instead of actively studying swaths of code for flaws, malicious actors will start turning to patches as convenient pointers to holes in a system, after which they can tailor their malware code. In 2022, a dedicated segment of cybercriminals will be keeping a close eye on companies in anticipation of any disclosed vulnerabilities and deployed patches, which will help them expedite their attacks.

Bad actors are not just planning to take advantage of newly found vulnerabilities but will also continue to capitalize on older flaws. This will further underscore the need for enterprises and their partner vendors to prioritize patch management. Vulnerabilities found in previous years will stay relevant, as malicious actors will repurpose and combine these to beef up their attacks in the coming year.

Similarly, there will be an influx in blended attacks that will target multiple software products at once by daisy-chaining, for example, vulnerabilities in Google Chrome with vulnerabilities in Microsoft Windows, to gain privileged access to systems. An upside to this upcoming rise in attacks is that it will inevitably draw the attention of security analysts to lesser-explored attack surfaces. We expect to see more research dedicated to server-side technology that can shed light on weak spots in platforms like Microsoft Exchange and SharePoint, mitigating the impact of any future attacks on their end users.

Cloud-native security will also need to be a priority among enterprises, many of which have become cloud adopters after the pandemic hastened their digital transformations. The dependence of many cloud-native projects on libraries that are built on open-source software might leave them exposed to attacks that stack known vulnerabilities, as these libraries are not often kept up to date or routinely assessed for publicly disclosed flaws.³⁴ For security teams, finding trustworthy sources of cloud flaws will be instrumental in protecting cloud assets, as there remains a lack of cloud-related common vulnerabilities and exposures (CVE) reports relative to on-premises bugs.³⁵

More than ever, enterprises will need to ensure that their IT security teams are well-positioned to adapt and address this imminent surge in exploits. This will involve providing these teams with the support and resources they will need to take inventory of devices in an IT environment through asset management, monitor security updates from vendors so that they can respond as soon as vulnerabilities are publicly disclosed, and practice virtual patching³⁶ or machine isolation to protect any potential threat entry points.

Commodity Malware Attacks

Malicious actors will continue to think of smaller businesses as easy prey, but cloud-heavy SMBs will come prepared with security measures that can fend off commodity attacks



While all eyes are on ransomware, traditional commodity attacks and attacks-as-a-service will have time to innovate more sophisticated tools

Enterprises will remain to be profitable prey for ransomware operators looking for huge payouts, but the headline-making exploits of big-game hunters will only leave small and medium-sized businesses (SMBs) ripe for the picking among ransomware-as-a-service (RaaS) affiliates and small-time cybercriminals wielding commodity malware and keeping low profiles.³⁷

The public's attention has been firmly fixed on ransomware over the last few years, and ransomware is considered a type of commodity malware and an as-a-service model. But other off-the-shelf malware types such as remote access trojans (RATs), information stealers, cryptocurrency miners, droppers, and malware loaders will be circulating in cybercriminal circles. This will push the commodity malware market to grow into an insidious but formidable threat. Ransomware operators have taken advantage of commodity malware tools to make their attacks more effective,³⁸ while other malicious actors have used commodity attack tools to launch politically motivated campaigns.³⁹ Ransomware operators have also been observed using commodity malware tools like Cobalt Strike, Koadic, PowerShell Empire, and Metasploit⁴⁰ in concert with existing system administration utilities — a technique called “living off the land” — to avoid detection.⁴¹

These tools come with more advanced functionalities and affordable prices, making such malware accessible to malicious actors seeking to augment their toolbox.⁴² Many customized pieces of malware are eventually commoditized in the cybercriminal underground for other malicious actors to use,⁴³ which leads us to foresee the next generation of cybercriminals as being more innovative and better-equipped than the one responsible for the development of ransomware some 15 years ago.⁴⁴ We predict that the market around commodity attack tools will not only mature alongside novice malicious actors, but will also give them the means to expand their networks and connect with like-minded cybercriminals. After all, sellers have not only been providing ready-to-use malware, but have also been sweetening the deal with instructions, tips, and troubleshooting guides.⁴⁵

The service model, in which commodity malware is sold as part of service contracts rather than a one-time malware purchase, will be well-suited to lower-level actors, who are bound to graduate from needing malware tools to seeking reliable partners in crime as they grow into more experienced attackers. Such collaborations will lead to more resilient criminal activity, as evidenced by how malicious actors were able to rebuild the Emotet malware's botnet by using that of the banking trojan Trickbot, mere months after the takedown of Emotet's own infrastructure by law enforcement

authorities.⁴⁶ Because of this, we predict that commodity attacks will reach a point in 2022 where malicious actors will begin to have little need to develop bespoke malware, in which case such malware will be needed to better manage their affiliates in a complex targeted attack.

Considering this, the commodity malware space is long overdue for a more sophisticated offering with which malicious actors can upgrade their arsenal. The coming year will likely see the debut of a botnet-as-a-service designed to compromise and control both cloud-based and IoT platforms simultaneously, much like a souped-up version of the Zeus botnet.⁴⁷ It is possible that such a tool will come out of the Russian-speaking set of the cybercriminal underground, owing to its notoriously innovative malware scene,⁴⁸ but the FreakOut botnet is also shaping out to be a contender as it continues to evolve with additional features.⁴⁹

We foresee the commodity attack market, whose business model relies on the malware code doing the legwork instead of an attacker moving inside a network, being largely ineffective against the more robust defenses more commonly found in enterprise settings, such as security systems that use machine learning.⁵⁰ However, we predict that commodity malware tools will find more success in 2022 by targeting SMBs, employed as they will be by malicious actors hoping to encounter less security defenses from their targets and less competition from other cybercriminals. Specifically, we predict that IoT devices used by SMBs will be prime targets for such attacks. SMBs will therefore have to be more discerning when choosing vendors, purchasing their IoT devices from manufacturers that boast a solid patch history.

Rarely do SMBs have dedicated security teams, and when they do, these teams are likely constrained by limited funding, in which cybersecurity is merely an operating expense. Globally, cybersecurity expenditure is on track to exceed US\$150 billion by the end of 2021,⁵¹ but SMBs spend only over US\$40 billion annually on IT security solutions, remaining an underserved market in which only the more mature SMBs retain in-house security talent.⁵² Because of their budget constraints, we predict that many SMBs will make securing endpoints their top priority, followed by protecting their networks. Some SMBs might be even more prepared than others, however. Those that are more online-based, relying heavily on cloud-based services and platforms, will be more aware of the risks posed by commodity malware on their mission-critical operations, owing to the nature of their business. These companies are more likely to make security a part of their on-the-board agenda, writing in cybersecurity solutions as part of their cost of sales.

IoT Threats

Enterprises will strive for improved network monitoring and visibility to safeguard their IT environments against threats arising from IoT adoption



Information associated with the IoT will become a hot commodity in the cybercriminal underground, spurring enterprises on to mind security gaps that might lead to data leakage or tampering

Smart devices have long been tempting marks in the eyes of malicious actors banking on the fact that the limited computational capacity of most IoT devices leaves little room for built-in security.⁵³ Compromised IoT devices have been used in different kinds of attacks, such as distributed denial-of-service (DDoS) attacks.⁵⁴ With more organizations driven to undergo digital transformations to stay competitive or at least operational during the global lockdown, we predict that companies, particularly those in smart manufacturing, will be exposed to more cyberthreats as they transition to the hybrid work model and continue to use remote connection services.

To keep their operations airtight, more enterprises whose workforces rely on IoT devices will turn to intrusion prevention and detection systems (IPs/IDSs), network forensics tools (NFTs), network behavior anomaly detection (NBAD) tools, and network detection and response (NDR) tools that can help them keep close watch over the goings-on in their networks in the coming year. Cloud adopters that rely on third-party security vendors will have to vigilantly track their usage of cloud-based resources for any anomalous activity, safeguard their virtual private cloud (VPC) from attacks that might occur within their cloud-based infrastructure, and review the capabilities of prospective vendors to ensure that these suit their needs.

But in 2022, malicious actors will have loftier aspirations that will go beyond hijacking IoT gadgets as a convenient attack base for their criminal activity or as a means of moving laterally within a network. Cybercriminals will soon be joining the gold rush as more carmakers — including big-name players like General Motors, Honda, and Toyota⁵⁵ — cash in on the data traffic delivered by connected cars. These vehicles come equipped with an array of cameras, lasers, and other sensors that collectively log driving conditions and driver behavior, including a car's driving speeds and distances, and the kinds of entertainment media consumed by its passengers. These real-time insights have a myriad of business applications for commercial clients, such as measuring advertising success, gauging consumer demand, and determining discounts on auto insurance based on driving data.⁵⁶ For carmakers, this data could also be used to monitor the performance of vehicle components, which would enhance their own supply chains.⁵⁷

The demand for smart car information is set to become a booming new business that is predicted to be valued at around US\$450 to US\$750 billion by 2030,⁵⁸ with no signs of losing steam: 10 exabytes of data is forecast to come from connected cars monthly by 2025.⁵⁹ As more of these vehicles hit the road, malicious actors are geared up to turn a profit from the increased connectivity, which we expect will boost demand for illegal data filters that can block the reporting of risk data or hackers who can wipe bad driving from a smart car's records. Smart car architecture can also be further streamlined if its more complex data-collecting functions and processes are transitioned to the cloud — in fact, many applications and systems used by newer smart car models are already hosted on back-end cloud servers⁶⁰ — but doing so might open carmakers to other threats such as denial-of-service (DoS) and man-in-the-middle (MitM) attacks.⁶¹

If they are to future-proof their products, car manufacturers in 2022 will need to work closely with security vendors to collectively decide how they want to implement security. Examples of this partnership are already underway. There have been early initiatives like the Open EV Software Platform, spearheaded by the Mobility in Harmony (MIH) Consortium and its partners, Arm, Microsoft, and Trend Micro.⁶² There is also a collaboration between Volkswagen and Microsoft that seeks to create a cloud-based platform that carmakers can use to develop more advanced and secure automated driving solutions for connected cars.⁶³ More projects like these would lay the groundwork for the car industry to develop a dedicated operating system for smart vehicles, with the end goal of an automotive ecosystem built on a unified operating system that will make it possible for future models of connected cars to come equipped with standardized security features.



Supply Chain Threats

As they focus on making their supply chains more robust via diversification and regionalization, enterprises will implement zero trust principles to keep their environments more secure

Global supply chains will be in the crosshairs of fourfold extortion techniques as companies evolve their supply chain operations

The Covid-19 pandemic has shone a hard spotlight on the fragility of supply chains. Massive economic shortages and delays have arisen because of several factors, including increased demand,⁶⁴ shipping container and worker shortages,⁶⁵ and yearslong dependence on leaner production systems, which is a result of the just-in-time manufacturing model.⁶⁶ When supply chain woes started becoming a worldwide burden, the value of supply chains also started becoming even more evident — not just to struggling businesses but also to crooked cybercriminals undeterred but rather fueled by a global pandemic. In particular, supply chain attacks have become increasingly interconnected with ransomware campaigns this year, as exemplified by the high-profile REvil/Sodinokibi⁶⁷ attacks on large organizations including Quanta Computer,⁶⁸ JBS Foods,⁶⁹ and Kaseya.⁷⁰

Further taking advantage of and exacerbating the great supply chain disruption, malicious actors will generate a surge in the quadruple extortion model⁷¹ in 2022. They will make the most of their cyberattacks by strong-arming big-name victims into paying large sums of money via a fourfold extortion technique: holding the victim's critical data for ransom, threatening to leak the data and publicize the breach, threatening to go after the victim's customers, and attacking the victim's supply chain or vendors.

This year, the cybercriminal group DarkSide targeted Colonial Pipeline, the largest refined oil pipeline system in the US. The group prevented the company from accessing its computer systems and stole over 100 GB of corporate data.⁷² It has been observed that the group has been constantly innovating their attack strategies by also offering both DDoS and call center services.⁷³ Doing so enables DarkSide affiliates to launch quadruple extortion techniques that can heavily affect supply chains. Consequently, malicious actors could deny access to critical data such as manufacturing secrets, withhold access to machines used in production, or contact customers and stakeholders to pressure victim organizations to pay up.

Supply chains will also be the focus of access-as-a-service (AaaS) brokers. Once vulnerable environments are compromised, AaaS brokers can sell company network access, administrative accounts, and authentication credentials to cybercriminals for varying prices.

Economic shifts prompted by the pandemic will push enterprises to invest in their supply chain development processes. They will focus on building more robust supply chain operations by means of diversification. For years, countries have favored globalization, which has been criticized as the cause of many countries' overreliance on obtaining supplies from a single geographical source.⁷⁴ Instead of globalization, supply chain operations will shift to regionalization, helping ensure that enterprises are able to address increased demands and volatile production costs. Diversification strategies will differ for all companies — some links in the supply chain will be local, while others will be in different countries or regions.

However, diversification is no easy feat to pull off properly and securely; it can be a costly and resource-intensive endeavor. As organizations look for vendors and suppliers that are closer to home to reduce economic risks and help keep business operations afloat, they might also be unwittingly opening their doors to security risks. Long-term suppliers that they have been working with for years will be replaced by new companies that they will need to assess. These new vendors might offer cloud applications and services with security policies that might not be up to par or might not prioritize cloud security at all.

The period during which two organizations align their processes is critical — and malicious actors can wage targeted attacks to take advantage of the changes and unfamiliarity associated with new partnerships. For example, an actor can pretend to be someone from a new supplier and send a spear-phishing email asking the recipient to fill out relevant company information on a malicious website.

To keep supply chains secure as companies evolve their strategies, they should apply the zero trust approach in their security practices.⁷⁵ The zero trust model helps secure the way in which organizations interact with other companies and exchange data via continuous verification throughout a connection's lifetime. Through this model, organizations can be sure that the health of the users, devices, applications, and services that they interact with is constantly monitored and assessed.

Full speed ahead for cybersecurity

Our security predictions for 2022 outline the threats and risks that have emerged from our security experts' research, observations, and insights on imminent security concerns and security technologies. In dealing with these issues, organizations will benefit from a holistic and multilayered cybersecurity strategy that involves the following security recommendations:

Go back to security basics. It may seem deceptively simple, but adhering to security best practices can help organizations combat the majority of old and new threats in the coming year. Malicious actors will continue to exploit old vulnerabilities in systems and applications, so it is important for organizations to be on top of their patch management policies. This will help them avoid data breaches and, subsequently, costly fines and reputational damage. Enterprises should also understand and apply the shared responsibility model and regularly encrypt critical data.

Apply the zero trust model to keep applications and environments secure. Enterprises can improve their security posture by applying the zero trust model, wherein any user or device that attempts to connect to applications and systems needs to be verified before being granted access and continuously thereafter — regardless of whether the user or device is inside the network or not.

Harden server security and employ access control. As organizations move toward a hybrid work model, it is imperative for organizations to craft and implement security policies that take into account the perimeterless nature of the postpandemic workplace. Access and application control can enable organizations to get a better handle of their overall security even as employees access sensitive or critical work applications and data from anywhere and from different devices.

Prioritize visibility. As employees continue to access cloud applications, services, systems, and databases remotely in the coming year, it is important for organizations to bring visibility to the fore to help fortify their cybersecurity defenses. Security teams must be aware of all cloud providers, accounts, and services in order to keep an eye on them and make sure that they are configured as securely as possible. This will help minimize the risk of unintended exposures and misconfigurations.

Shift to stronger security with the right solutions and level of expertise. To successfully protect their systems and environments from ever-evolving threats, organizations require flexible, automated, and advanced security solutions that efficiently detect attacks in emails, endpoints, networks, servers, and cloud workloads. Trend Micro provides thorough investigation details and security insights from a dedicated team of security analysts who have access to extensive security analytics, powerful security solutions, and its global threat intelligence.



References

1. Julie Steenhuisen. (Nov. 3, 2021). *Reuters*. "Analysis: Country by country, scientists eye beginning of an end to the COVID-19 pandemic." Accessed on Nov. 25, 2021, at <https://www.reuters.com/business/healthcare-pharmaceuticals/country-by-country-scientists-eye-beginning-an-end-covid-19-pandemic-2021-11-03/>.
2. Joe Devanesan. (Oct. 20, 2021). *TechHQ*. "2021 was a record-breaking year in zero-day exploits – that's both good and bad news." Accessed on Nov. 19, 2021, at <https://techhq.com/2021/10/2021-was-a-record-breaking-year-in-zero-day-exploits-and-thats-both-good-and-bad-news/>.
3. Trend Micro. (Oct. 24, 2019). *Trend Micro Security News*. "The Cloud: What it is and what it's for." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-what-it-s-for>.
4. Trend Micro. (Oct. 7, 2020). *Trend Micro Security News*. "CSO Insights: DataBank's Mark Houpt on Looking Beyond Securing Infrastructures in the New Normal." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal/>.
5. Bernard Marr. (Oct. 25, 2021). *Forbes*. "The 5 Biggest Cloud Computing Trends In 2022." Accessed on Nov. 10, 2021, at <https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/>.
6. Gartner. (Aug. 2, 2021). *Gartner*. "Gartner Says Four Trends Are Shaping the Future of Public Cloud." Accessed on Nov. 10, 2021, at <https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud>.
7. David Fiser and Alfredo Oliveira. (June 29, 2021). *Trend Micro Research, News, and Perspectives*. "Secure Secrets: Managing Authentication Credentials." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/21/f/secure_secrets_managing_authentication_credentials.html.
8. Chuck Losh. (May 18, 2021). *Trend Micro Research, News, and Perspectives*. "Container Security First Steps: Image and Registry Scanning." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/21/e/container-security-first-steps-image-and-registry-scanning.html.
9. Trend Micro. (July 20, 2021). *Trend Micro Security News*. "TeamTNT Activities Probed: Credential Theft, Cryptocurrency Mining, and More." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/teamtnt-activities-probed>.
10. Trend Micro. (Sept. 10, 2013). *Trend Micro Research, News, and Perspectives*. "How the Java Security Situation Quietly Got Much Worse." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/13/i/java-security-situation-quietly-got-much-worse.html.
11. Trend Micro. (Feb. 2, 2015). *Trend Micro Research, News, and Perspectives*. "New Adobe Flash 0-Day Exploit Used in Malvertisements." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/15/b/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements.html.
12. Catalin Cimpanu. (May 1, 2020). *ZDNet*. "Oracle warns of attacks against recently patched WebLogic security bug." Accessed on Nov. 10, 2021, at <https://www.zdnet.com/article/oracle-warns-of-attacks-against-recently-patched-weblogic-security-bug/>.
13. Trend Micro. (n.d.). *Trend Micro Security News*. "DevOps Definition Page." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/definition/devops>.
14. David Fiser. (March 4, 2020). *Trend Micro Research, News, and Perspectives*. "Security Risks in Online Coding Platforms." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/20/c/security-risks-in-online-coding-platforms.html.
15. Trend Micro. (May 14, 2020). *Trend Micro Security News*. "Cloud Security: Key Concepts, Threats, and Solutions." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions>.
16. Melissa Clow. (Dec. 16, 2020). *Trend Micro Research, News, and Perspectives*. "A Guide to the Well-Architected Framework." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/20/l/well-architected-framework-guide.html.
17. Trend Micro. (March 4, 2021). *Trend Micro Security News*. "Security 101: Virtual Patching." Accessed on Nov. 10, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>.
18. Trend Micro. (n.d.). *Trend Micro Security News*. "Ransomware Definition Page." Accessed on Nov. 8, 2021, at <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>.

19. Trend Micro. (Sept. 28, 2017). *Trend Micro Security News*. "Spam, BEC, Ransomware: The Continuing Abuse of Email by Old and New Threats." Accessed on Nov. 8, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/spam-bec-ransomware-the-continuing-abuse-of-email-by-old-and-new-threats>.
20. Dinesh Malkani. (June 4, 2021). *Forbes*. "Going Hybrid: The Future Of Work Is Here." Accessed on Nov. 8, 2021, at <https://www.forbes.com/sites/forbestechcouncil/2021/06/04/going-hybrid-the-future-of-work-is-here/>.
21. Trend Micro. (Sep. 14, 2021). *Trend Micro*. "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup>.
22. Robert Lemos. (Oct. 27, 2021). *Dark Reading*. "Cybersecurity Talent Gap Narrows as Workforce Grows." Accessed on Nov. 22, 2021, at <https://www.darkreading.com/careers-and-people/cybersecurity-talent-gap-narrows-as-workforce-grows>.
23. Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern Ransomware's Double Extortion and How to Protect Enterprises Against Them." Accessed on Nov. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransoms-ware-s-double-extortion-tactics-and-how-to-protect-enterprises-against-them>.
24. Trend Micro. (April 14, 2020). *Trend Micro Security News*. "Undertaking Security Challenges in Hybrid Cloud Environments." Accessed on Nov. 8, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/undertaking-security-challenges-in-hybrid-cloud-environments>.
25. Claudia Glover. (Oct. 11, 2021). *Tech Monitor*. "Ransomcloud: How and why ransomware is targeting the cloud." Accessed on Nov. 8, 2021, at <https://techmonitor.ai/technology/cybersecurity/ransomcloud>.
26. Patrick Howell O'Neill. (Sept. 23, 2021). *MIT Technology Review*. "2021 has broken the record for zero-day hacking attacks." Accessed on Nov. 5, 2021, at <https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons>.
27. Trend Micro. (July 13, 2021). *Trend Micro Security News*. "Trends and shifts in the underground N-day exploit market." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market>.
28. Trend Micro. (May 19, 2021). *Trend Micro Newsroom*. "Trend Micro's Zero Day Initiative Enhances Position as World's Largest Vulnerability Disclosure Player." Accessed on Nov. 25, 2021, at <https://newsroom.trendmicro.com/2021-05-19-Trend-Micros-Zero-Day-Initiative-Enhances-Position-as-Worlds-Largest-Vulnerability-Disclosure-Player>.
29. Clement Lecigne and Maddie Stone. (July 14, 2021). *Google*. "How we protect users from 0-day attacks." Accessed on Nov. 5, 2021, at <https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks>.
30. Jon Clay. (April 28, 2021). *Trend Micro Research, News, and Perspectives*. "How Trend Micro Helps Manage Exploited Vulnerabilities." Accessed on Dec. 3, 2021, at https://www.trendmicro.com/en_us/research/21/d/how-trend-micro-helps-manage-exploited-vulnerabilities.html.
31. Charlie Osborne. (July 14, 2021). *ZDNet*. "Microsoft July 2021 Patch Tuesday: 117 vulnerabilities, Pwn2Own Exchange Server bug fixed." Accessed on Nov. 5, 2021, at <https://www.zdnet.com/article/microsoft-july-2021-patch-tuesday-117-vulnerabilities-pwn2own-exchange-server-bug-fixed>.
32. Catalin Cimpanu. (Sept. 10, 2019). *ZDNet*. "Security researchers expose another instance of Chrome patch gapping." Accessed on Dec. 1, 2021, at <https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping>.
33. Trend Micro. (April 7, 2021). *Trend Micro Research, News, and Perspectives*. "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>.
34. Magno Logan. (Oct. 8, 2021). *Trend Micro Security News*. "Minding the Gaps: The State of Vulnerabilities in Cloud Native Applications." Accessed on Nov. 17, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications>.
35. Shaun Nichols. (Nov. 2, 2021). *TechTarget*. "Why cloud bugs don't get CVEs, and why it's an issue." Accessed on Nov. 17, 2021, at <https://searchsecurity.techtarget.com/news/252508948/Why-cloud-bugs-dont-get-CVEs-and-why-its-an-issue>.
36. Trend Micro. (March 4, 2021). *Trend Micro Research*. "Security 101: Virtual Patching." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>.
37. Trend Micro. (Aug. 28, 2018). *AP News*. "Trend Micro Report Reveals Criminals Increasingly Drawn To Low-Profile Attacks." Accessed on Nov. 5, 2021, at <https://apnews.com/press-release/pr-businesswire/7f2907b6661b426c855e4875511266e1>.

38. BSI Staff. (July 26, 2021). *The British Standards Institution*. "How your business can adapt to cybersecurity trends." Accessed on Nov. 21, 2021, at <https://shop.bsigroup.com/articles/how-your-business-can-adapt-to-cybersecurity-trends>.
39. David Agranovich and Mike Dvilyanski. (Nov. 16, 2021). *Meta*. "Taking Action Against Hackers in Pakistan and Syria." Accessed on Nov. 21, 2021, at <https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria>.
40. VMWare. (Oct. 11, 2021). VMWare Security Blog. "Moving Left of the Ransomware Boom." Accessed on Nov. 25, 2021, at <https://blogs.vmware.com/security/2021/10/moving-left-of-the-ransomware-boom.html>.
41. Lucian Constantin. (March 19, 2021). *CSO Online*. "Ryuk ransomware explained: A targeted, devastatingly effective attack." Accessed on Nov. 25, 2021, at <https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html>.
42. Jaromir Horejsi and Daniel Lunghi. (Sept. 13, 2021). *Trend Micro Research, News, and Perspectives*. "APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html.
43. National Cyber Security Centre. (Oct. 6, 2016). *National Cyber Security Centre*. "Common Cyber Attacks: Reducing The Impact." Accessed on Nov. 21, 2021, at <https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact>.
44. Trend Micro. (n.d.). *Trend Micro Security News*. "Ransomware Definition." Accessed on Nov. 21, 2021, at <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>.
45. Numaan Huq et al. (June 28, 2019). *Trend Micro Research*. "Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground." Accessed on Nov. 5, 2021, 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>.
46. Lawrence Abrams. (Nov. 15, 2021). *BleepingComputer*. "Emotet malware is back and rebuilding its botnet via TrickBot." Accessed on Nov. 22, 2021, at <https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot>.
47. Bernadette Caraig. (n.d.). *Trend Micro Threat Encyclopedia*. "The Zeus, ZBOT, and Kneber Connection." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection>.
48. Joshua Yaffa. (May 23, 2021). *The New Yorker*. "How Hacking Became a Professional Service in Russia." Accessed on Nov. 21, 2021, at <https://www.newyorker.com/news/news-desk/how-hacking-became-a-professional-service-in-russia>.
49. Catalin Cimpanu. (Jan. 19, 2021). *ZDNet*. "New FreakOut botnet targets Linux systems running unpatched software." Accessed on Nov. 5, 2021, at <https://www.zdnet.com/article/new-freakout-botnet-targets-linux-systems-running-unpatched-software/>.
50. Trend Micro. (n.d.). *Trend Micro Security News*. "Machine Learning." Accessed on Nov. 22, 2021, at <https://www.trendmicro.com/vinfo/us/security/definition/machine-learning>.
51. Gartner. (May 17, 2021). *Gartner*. "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021." Accessed on Nov. 22, 2021, at <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>.
52. Bharath Aiyer, Venky Anant, and Daniele Di Mattia. (March 24, 2021). *McKinsey*. "Securing small and medium-size enterprises: What's next?" Accessed on Nov. 22, 2021, at <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next>.
53. Trend Micro. (May 28, 2020). *Trend Micro Security News*. "Smart Yet Flawed: IoT Device Vulnerabilities Explained." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained>.
54. Trend Micro. (July 22, 2021). *Trend Micro Security News*. "IoT Security Issues, Threats, and Defenses." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses>.
55. Trend Micro. (Oct. 11, 2021). *Trend Micro Research, News, and Perspectives*. "Honda to Start Selling Smart Car Data." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/j/honda-to-start-selling-smart-car-data.html.
56. Kotaro Abe and Ryotaro Yamada. (Sept. 29, 2021). *Nikkei Asia*. "Honda joins \$400bn gold rush to monetize smart car data." Accessed on Nov. 5, 2021, at <https://asia.nikkei.com/Business/Technology/Honda-joins-400bn-gold-rush-to-monetize-smart-car-data>.
57. Anthony Spadafora. (Nov. 18, 2020). *TechRadar*. "Amazon and NXP team up on smart car cloud computing deal." Accessed on Nov. 17, 2021, at <https://www.techradar.com/news/amazon-and-nxp-team-up-on-smart-car-cloud-computing-deal>.

58. Mark Minevich. (July 13, 2020). *Forbes*. "The Automotive Industry And The Data Driven Approach." Accessed on Nov. 5, 2021, at <https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/>.
59. Toyota Motor Corporation. (Aug. 10, 2017). *Toyota Motor Corporation*. "Industry leaders to form consortium for network and computing infrastructure of automotive big data." Accessed on Nov. 5, 2021, at <https://global.toyota/en/detail/18135029>.
60. Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro Research*. "In Transit, Interconnected, At Risk: Cybersecurity Risks of Connected Cars." Accessed on Nov. 17, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars>.
61. Trend Micro. (Feb. 6, 2021). *Trend Micro Research, News, and Perspectives*. "Connected Cars, 5G, the Cloud: Opportunities and Risks." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/en_us/research/21/b/connected-cars-5g-the-cloud-opportunities-and-risks.html.
62. MIH Consortium. (Oct. 20, 2021). *MIH Consortium*. "MIH Unveils Open EV Software Platform and Announces key partnerships with Arm, Microsoft and Trend Micro." Accessed on Nov. 5, 2021, at <https://www.mih-ev.org/en/news-info/?id=695>.
63. Microsoft. (Feb. 10, 2021). *Microsoft News Center*. "Volkswagen Group teams up with Microsoft to accelerate the development of automated driving." Accessed on Nov. 17, 2021, at <https://news.microsoft.com/2021/02/10/volkswagen-group-teams-up-with-microsoft-to-accelerate-the-development-of-automated-driving>.
64. Garth Friesen. (Sep. 3, 2021). *Forbes*. "No End In Sight For The COVID-Led Global Supply Chain Disruption." Accessed on Nov. 25, 2021, at <https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain-disruption/>.
65. Elizabeth Harris. (Oct. 4, 2021). *The New York Times*. "'The Beginning of the Snowball': Supply-Chain Snarls Delay Books." Accessed on Nov. 25, 2021, at <https://www.nytimes.com/2021/10/04/books/book-publishing-supply-chain-delays.html>.
66. Peter S. Goodman and Niraj Chokshi. (June 1, 2021). *The New York Times*. "How the World Ran Out of Everything." Accessed on Nov. 25, 2021, at <https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html>.
67. Trend Micro Research. (Jan. 26, 2021). *Trend Micro Research, News, and Perspectives*. "Examining A Sodinokibi Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.
68. Michael Novinson. (April 23, 2021). *CRN*. "Apple Menaced After REvil Ransomware Attack Against Supplier." Accessed on Nov. 5, 2021, at <https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier>.
69. Trend Micro Research. (May 12, 2021). *Trend Micro Research, News, and Perspectives*. "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
70. Trend Micro Research. (July 4, 2021). *Trend Micro Research, News, and Perspectives*. "IT Management Platform Kaseya Hit With Sodinokibi/REvil Ransomware Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/g/it-management-platform-kaseya-hit-with-sodinokibi-revil-ransomwa.html.
71. Janus Agcaoili et al. (June 15, 2021). *Trend Micro Security News*. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Nov. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti>.
72. Trend Micro. (Sept. 14, 2021). *Trend Micro*. "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 25, 2021, at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup>.
73. Brian Krebs. (May 11, 2021). *Krebs On Security*. "A Closer Look at the DarkSide Ransomware Gang." Accessed on Nov. 25, 2021, at <https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/>.
74. Chad P. Bown and Douglas A. Irwin. (Oct. 14, 2021). *The New York Times*. "Why Does Everyone Suddenly Care About Supply Chains?" Accessed on Nov. 6, 2021, at <https://www.nytimes.com/2021/10/14/opinion/supply-chain-america.html>.
75. Trend Micro. (Aug. 13, 2021). *Trend Micro Research, News, and Perspectives*. "What Is Zero Trust and Why Does It Matter?" Accessed on Nov. 9, 2021, at https://www.trendmicro.com/en_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html.

TOWARD A NEW MOMENTUM



TREND MICRO SECURITY PREDICTIONS FOR 2022



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, 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 new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

©2021 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

