TURNING THE TIDE

Trend Micro Security Predictions for 2021

TURNING THE TIDE

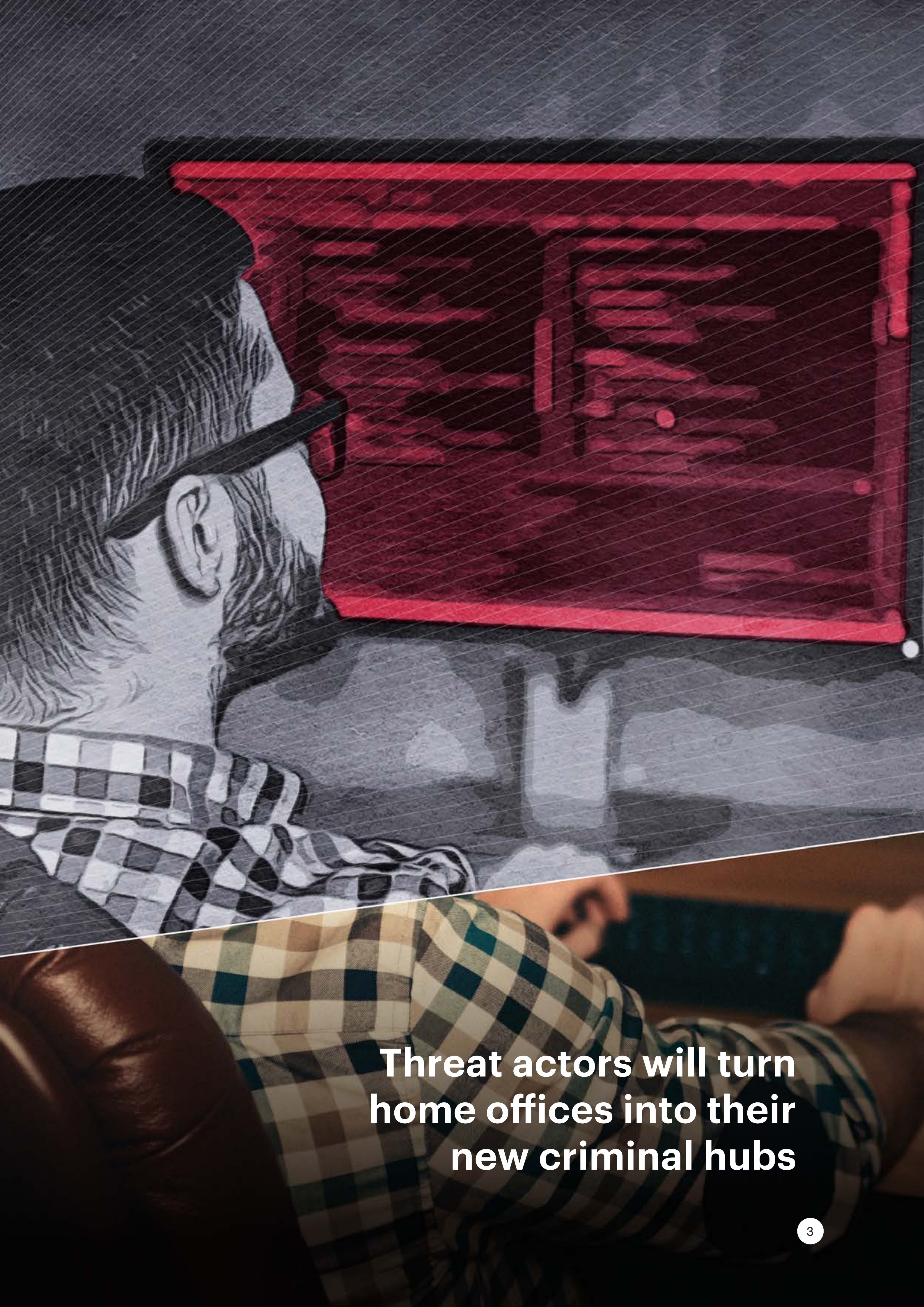
Trend Micro Security Predictions for 2021

The coronavirus (Covid-19) pandemic has changed the way many organizations operate as remote work has become the norm. However, moving from a customary office to a home-based workstation — potentially as a long-term arrangement — poses new security risks for businesses as more threat actors attempt to capitalize on Covid-19-related unease.

We affirmed in our security predictions for 2020 that the old paradigm, where networks are traditionally isolated behind a corporate firewall, would be behind us. Traditional setups and protections would no longer be adequate in an ecosystem that demands a wide range of services and platforms.

When the Covid-19 pandemic hit, organizations quickly had to reckon with this reality. It has put to the fore sobering reminders of perennial issues and neglected warnings that have beset cybersecurity for years. It also presented how organizations worldwide are at a significant risk of disruption by cyberattacks, global crises, and other eventual tipping points. While the risk has always been there, the pandemic only underlined the gravity of the issue: How are sectors equipped or prepared for such scenarios?

In 2021, organizations will scramble to deal with the far-reaching effects while striving to stay secure as online dependency grows. We discuss the developments that are not only plausible but ones that should also be anticipated. We look into the drivers of cybersecurity's near future and how organizations will have to adapt as threats and technologies exert their influence. Our report aims to empower organizations and decision-makers to frame a proper, strategic response that can withstand change and disruption.



Threat actors will turn home offices into their new criminal hubs

Turning the Tide

The ongoing pandemic and resulting lockdowns in many parts of the world have forced an influx of employees into unfamiliar territory — remote work, and in many cases, working from home full-time. As a result, many employees and companies are starting to realize the viability of working from home moving forward. In these circumstances, users and enterprises will have to protect work-from-home setups from threats — not only for IT teams who suddenly need to secure entire remote workforces but also for individual users who need to take precautions.

The boundaries between work and private lives have broken down as work is done over home internet service providers (ISPs), with possibly unpatched routers and machines, other connected devices in the background, and family members sharing computers while working for different organizations. While virtual private networks (VPNs) can secure connections with workplaces, housebound users will have to be wary of VPN vulnerabilities that could drive remote attacks.[1, 2]

Home networks will also become launch points for threat actors looking to hijack machines and jump to other devices in the same network, aiming to gain a corporate foothold. Malicious actors will either take advantage of installed software or “wormable” unpatched vulnerabilities — hopping from one remote worker’s machine to another until it finds a suitable target. This supply chain attack will spread to other users downstream. Employees who remotely access confidential and critical information (e.g., human resources, sales, and tech support) will also be actively targeted by data-stealing attacks in 2021. A lack of an intrusion detection system or a firewall in place, coupled with high-speed internet bandwidth, will make it especially easy for threat actors to move from one corporate network to the next.

Routers have always been viewed as sitting ducks for remote attacks on connected devices. Cybercriminals will offer hacked routers as a new service where they sell access to home networks. Access-as-a-service will emerge as a lucrative business model for criminals, who could establish persistent footprints and offer access to high-value home networks (such as those of executives or IT admins) to other threat actors. Organizations with converged networks will be prime targets for this — they will find themselves in the crosshairs of cybercriminals looking to profit by selling access to operational technology (OT) networks. An exploited weak point in the information technology (IT) space can become profitable for threat actors planning to cash in on OT network access in 2021.

Having detailed company security policies will help organizations ensure that the exchange of data between offices and employees working from home is protected adequately, and home office setups do not become a gateway for various forms of cybercrime. An incident response plan will have to outline how an organization would deal with security in a network with discrete machines. Companies should advise work-from-home employees on home router and internet of things (IoT) security, as well as the use of a virtual private network (VPN). This would include a briefing on the risks of password reuse and the use of default router and IoT passwords. We also recommend segmenting home networks to isolate company computers (i.e., using a virtual local area network [VLAN] and dedicating it for office work only).

The Covid-19 pandemic will upend cybersecurity priorities as it proves to be fertile ground for malicious campaigns

Turning the Tide

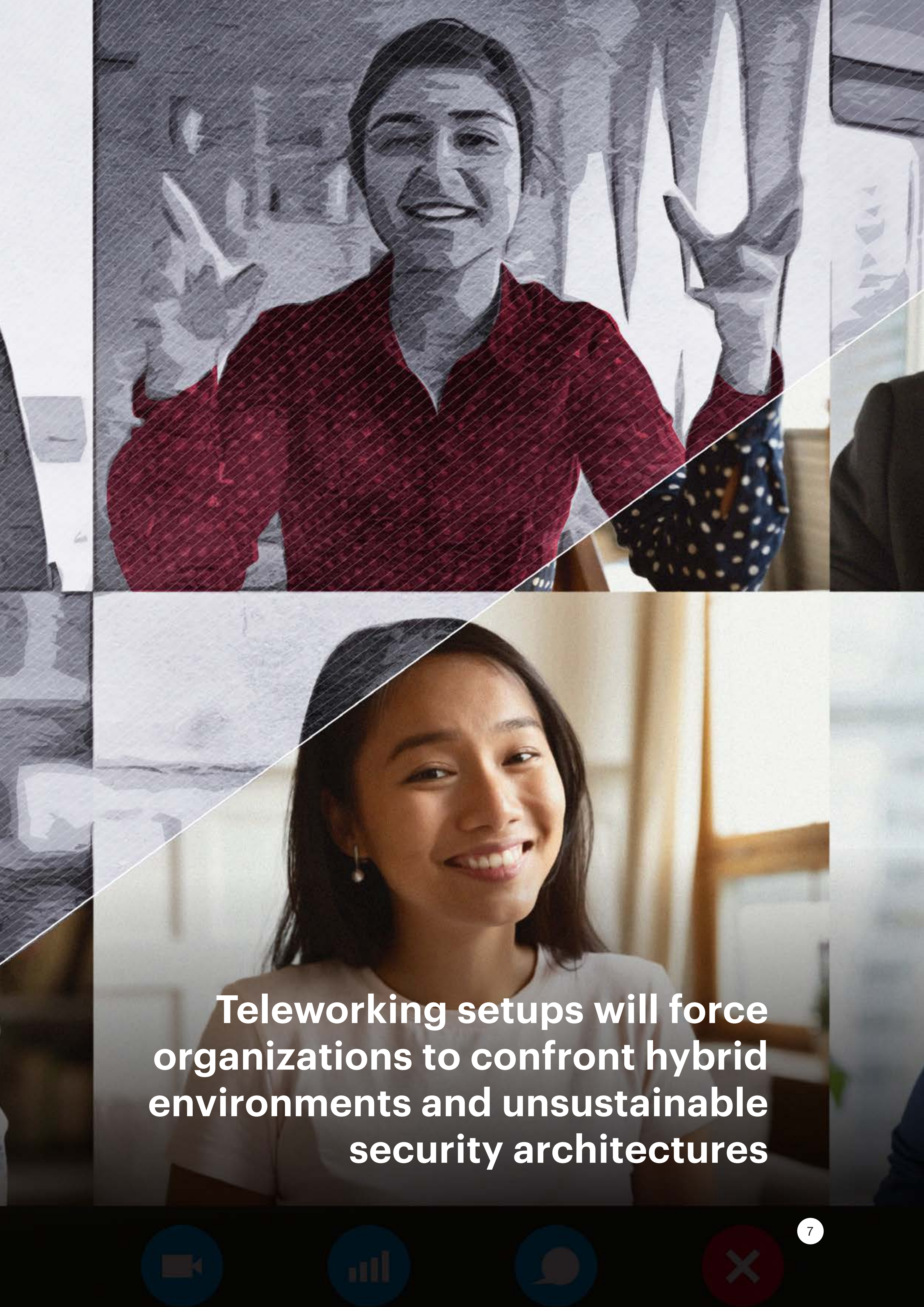
Threat actors see any major event as an opportunity for manipulation or sabotage, and it's no different for the coronavirus pandemic — they are shifting tactics and exploiting collective Covid-19-related fears. In our mid-year security roundup for 2020,[3] we noted a dramatic increase in Covid-19-related fraudulent emails, spam, and phishing attempts since the beginning of the public health crisis. Cybercriminals will continue to bank on social engineering opportunities and remain active with campaigns using coronavirus-themed lures.

Covid-19 will continue to present global businesses with cybersecurity challenges. E-commerce, for instance, has seen sustained growth in recent years, and the pandemic has reinforced it. Organized crime will attempt to break into logistics as online shopping further increases and more parcels get delivered. Crimes such as production sabotage, trafficking, and transporting counterfeit goods will emerge as their modi operandi amid the pandemic.

The healthcare sector, in particular, will be thrust under the spotlight. As many physicians have since moved to telemedicine and the provision of medical services has become even more critical, the IT security of healthcare systems will be put to the test. Security teams will not only need to address security risks that are associated with patient data and malware attacks,[4] but also the possibility of medical espionage.

Threat groups will reconnoiter coronavirus vaccine laboratories, particularly targeting those institutions that have publicly identified themselves as working on Covid-19-related research. Malicious actors will attempt to gain intelligence on response efforts and steal ongoing research on vaccines and related remedies. This potential medical information theft can slow down their research efforts and jeopardize the delivery and supply of treatment options.

Misinformation campaigns will also make it difficult for users to cut through the murk of the pandemic's many uncertainties. Threat actors will pivot to using misinformation to lure users into clicking on malicious attachments and links in fraudulent transactions. These scams will be sent through emails, fake apps, malicious domains, and social media, purporting to provide health information, supposed vaccines, and corresponding waitlists.[5] Conversely, the topic of vaccines will be used as a phishing lure when they become available.



Teleworking setups will force organizations to confront hybrid environments and unsustainable security architectures

Turning the Tide

As telecommuting further takes hold in 2021, hybrid environments — where work and personal data commingle in a single machine — will pose a significant challenge to organizations having less control over employee use. Mixing personal and work-related tasks (i.e., using one machine to do various online activities) blurs the lines concerning where the data is stored and where it is processed. If a work device is infected, how will personal data be considered in the cleanup? Is there a way to track printed or exported data? This decreased visibility of enterprises into what is happening on devices is exacerbated when employees access personal apps from the devices.

As various technologies used in remote work made the headlines for security issues, zero trust models will gain momentum in 2021 as an effective approach for empowering distributed workforces. By eliminating implicit trust on anything inside or outside the network, everything is verified.[6] Through micro-segmentation, a zero-trust architecture gives users access to only specific resources needed within certain perimeters. Such enforcement will ensure a robust security posture by making it more difficult for threat actors to penetrate the network. The zero-trust approach easily integrates with the cloud-backed secure access service edge (SASE), giving security teams critical visibility on all inbound and outbound traffic.

In the wake of the pandemic, organizations have modified their IT infrastructure and fast-tracked their move to the cloud. Infrastructures that would normally stumble over upgrading technologies are accelerating transformation programs. Those who rely on traditional on-premise solutions will not be able to keep up with the current demands that secure cloud-based software and applications can undertake. It will be organizations' goal, regardless of sector or industry, to ensure that they are versatile and agile enough to meet the challenges ahead.

From virtual travel to remote entertainment, there will be a continued emergence of new business models as various entities break new ground on digital platforms. Emerging technology solutions will help with daily routine work in home offices through AI-enabled apps. Before inevitably facing forms of digital criminal schemes, these apps will first find it tricky to get off the ground and market.

In response to the ongoing pandemic, organizations have grasped the need to reorient their security and cover remote workers for business continuity. IT teams will have to overhaul security approaches to accommodate remote-working setups for the long-term. Organizations would be wise to outline work-from-home policies (including coordinating with managed service providers), data handling, and, to every extent possible, enforce the line between personal and business use of devices.

The unprecedented need for contact tracing will have malicious actors directing their attention to users' gathered data

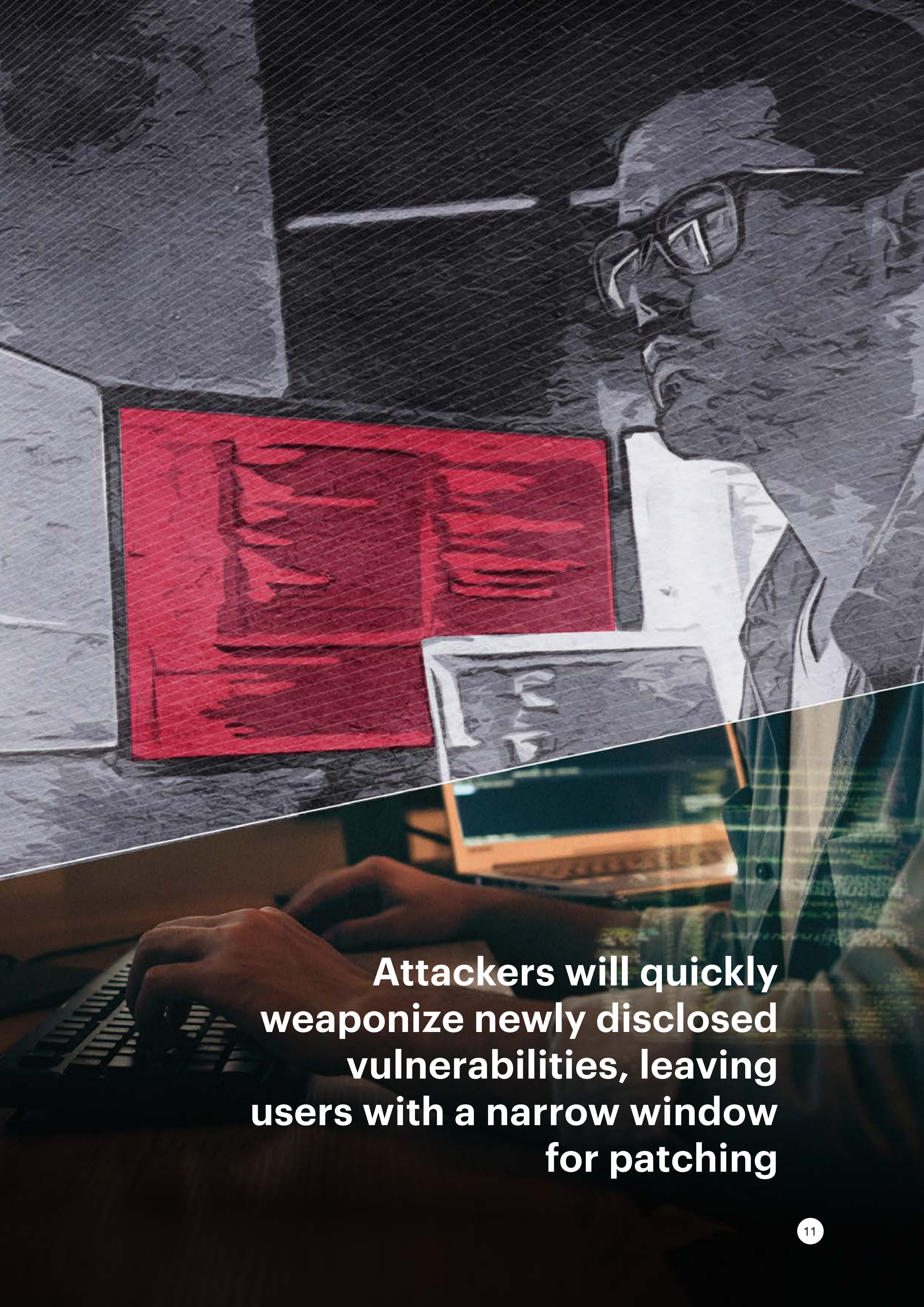
Turning the Tide

Unprecedented levels of data gathering[7] in efforts to monitor individuals' health statuses will attract criminals and political activists attempting to obtain that data. The rush to implement these measures will increase the risk of exposing or leaking user data.

Rapid access to data could be crucial in fighting the outbreak, but easing data privacy measures leads to problems of its own. Big databases, along with hasty implementations, are rich targets for malicious actors looking to compromise collected and possibly retained data. Cybercrime groups can abuse this in different ways, including extracting identity information and selling it in the underground.

A lack of strict protocols and protections leaves servers or databases vulnerable to exploitation. Governments will have to prepare and take appropriate steps to secure the data from hackers.

Efforts to slow the spread of the disease could also include lockdowns, which will have economic implications on several supply chains. The economic and operational impact will create budgetary constraints in organizations' security operations, challenging security teams to maintain (or increase) coverage under tighter financial allocations.



Attackers will quickly weaponize newly disclosed vulnerabilities, leaving users with a narrow window for patching

Turning the Tide

While zero-day vulnerabilities tend to steal the limelight when it comes to attacks, known or n-day vulnerabilities will raise significant concerns in 2021. Whereas zero-day vulnerabilities refer to flaws or bugs that have just been disclosed but remain unpatched, n-day vulnerabilities are those that have been publicly known and may have patches rolled out. There are innumerable known vulnerabilities today, and many organizations will find that they have considerable exposure in their respective digital footprints.

In 2021, there will be a quick adoption of n-day vulnerabilities and exploits released by the research community. Attackers will actively weaponize newly disclosed flaws in their attack frameworks. In Operation Poisoned News, the threat actors lifted code from an n-day proof of concept (POC) and took advantage of several privilege escalation bugs released by Google's Project Zero.[8] Earth Kitsune actors had a similar modus: They modified exploits released by Project Zero and Trend Micro's Zero Day Initiative (ZDI).[9]

N-day vulnerabilities will prove to be a goldmine for threat actors seeking weaknesses that are readily available for their use. Exploits reported in attacks may also have public disclosure documents for perusal, as opposed to zero-days that are time-consuming and arduous to find and exploit.

We predict n-day vulnerability marketplaces will also spring up for trading or selling exploitable known bugs — where vulnerability findings are modified accordingly to the threat actor's needs. It is not far-fetched to conjecture that sellers will also offer exploit customization depending on the attack. While this will enable relatively inexperienced actors to craft attacks, it will be particularly appealing to threat actor groups that are known for taking advantage of existing zero-day and n-day flaws in high-value targets. Sophisticated attacker groups, moreover, will ramp up their use of penetration testing tools, including the widely used Cobalt Strike, which had its source code allegedly leaked in November 2020.[10]

Exposed APIs will be the next favored attack vector for enterprise breaches

An application programming interface (API) is a software intermediary that allows communication between any application — from data sharing and functionality delivery to streamlining operations and system connectivity, providing protocols, routines, and tools for deploying services and software in devices, including the IoT. Many businesses rely on APIs to provide access to internal systems and interact with customers via apps.

The caveat is they are also ripe for the picking for threat actors looking for an entry point into an organization's networks. As APIs become more prominent in the enterprise space, so will their attack surface. APIs will become a preferred target as they also act as conduits for third-party integration, and we predict that API security will be a new focus area for adversaries in 2021.

APIs, while already ubiquitous, have security that is still nascent. They introduce several weaknesses that could be vectors for data breaches in enterprise applications. Some recent cases have reported gaining access to users' personal information[11, 12] and finding exposed source code and access to backend services.[13]

APIs also are relatively easy to discover, have many parameters open for compromise, and are inherently unsecure. Traditional defense mechanisms involving Captchas, JavaScript, or mobile SDK instrumentation cannot be effectively used to prevent an automated attack,[14] which means APIs are only partially protected, if at all. We recommend configuring access control and authentication mechanisms with a defense-in-depth approach and regularly monitoring access logs.

Enterprise software and cloud applications used for remote work will be hounded by critical class bugs

We expect top software and services used in distributed work will run into more publicly disclosed vulnerabilities due to increased research. Using publicly available vulnerability details, users can check their systems for security problems while allowing researchers and threat actors to look into similar holes in systems — especially if the discovered flaws are relatively new. Researchers will be particularly on the lookout for critical class bugs and similar variants in enterprise software and other remote-working technologies. Both cybercriminals and threat actor groups will favor weaknesses in popular software as part of their campaigns.

Vulnerabilities related to Microsoft Teams, as well as SharePoint, Office 365, and Exchange, will be sought-after in 2021. Processing potentially sensitive information in these collaboration software platforms will be a major concern for organizations with increased remote workforces, particularly in regulated industries such as financial services and healthcare.

With a renewed push to move to cloud environments and use collaboration tools, cloud security is talked about more than ever. To gain system visibility and meet scaling needs, organizations gather and store massive data across multiple sources and environments. These clouds of logs, however, will be central to modern, high-profile cybercrimes. Cloud environments often keep troves of valuable and sensitive data that criminals can use to find initial access points into networks.

The uptake of cloud technology use in 2020 will press on in 2021 to address the pandemic’s effect on operations. We expect this trend to continue to grow even when the pandemic recedes. Toward the end of 2021, the majority of workloads will be running in the cloud. Organizations that moved quickly and haphazardly will grapple with the security implications. We predict that data breaches and exponential compromise in cloud infrastructures will be caused not by cloud providers but by misconfigurations and missteps of unwitting users.

Other concerns for cloud adopters are hackers attempting to take over cloud servers and deploy malicious container images. We expect a sprawl of vulnerable images running in various architectures as users put unfettered trust in container services and depositories. These images will be aimed at hijacking repositories and poisoning resources.[15] Exposed data will be a common pitfall that leads to cloud-based breaches and attacks in organizations.

Forging Ahead with Cybersecurity

Trend Micro’s security predictions for 2021 reflect our security experts’ research and insights on emerging technologies and security issues. Stay ahead of the threats we outlined with these security recommendations for proactive global threat intelligence and response:

Foster user education and training. Threat actors will continue to capitalize on the fear surrounding Covid-19, and users must be informed of the tactics and possible attack vectors. Organizations should reinforce knowledge on threats and extend corporate best practices into the home. Directly share the do’s and don’ts of telecommuting and advise against using personal devices.

Maintain strict access control on the corporate network and home office. Organizations should focus on creating security-based company policies and an incident response plan that covers the perimeter of their operations. This will harden services, workstations, and corporate data while empowering businesses to work remotely. Refrain from putting implicit trust in assets or user accounts regardless of the location.

Reiterate basic security measures and patch management programs. Weak points will only crop up throughout the next several months of remote-working arrangements. It will be imperative to regularly update and patch applications and systems that are more vulnerable than ever.

Augment threat detection with security expertise. Ensure advanced, round-the-clock threat detection and incident handling in cloud workloads, emails, endpoints, networks, and servers with the help of dedicated security analysts. Gain better insights into attacks and prioritize security alerts through comprehensive threat intelligence and industry-leading solutions.

References

1 Cybersecurity and Infrastructure Security Agency. (January 10, 2020). *US-CERT.* “Continued Exploitation of Pulse Secure VPN Vulnerability.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-010a.

2 Charlie Osborne. (July 17, 2020). *ZDNet.* “Cisco releases security fixes for critical VPN, router vulnerabilities.” Accessed on Nov. 10, 2020, at https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/.

3 Trend Micro. (August 26, 2020). *Trend Micro.* “Securing the Pandemic-Disrupted Workplace.” Accessed on Nov. 10, 2020, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report.

4 Cybersecurity and Infrastructure Security Agency. (October 28, 2020). *US-CERT.* “Ransomware Activity Targeting the Healthcare and Public Health Sector.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

5 Trend Micro. (April 24, 2020). *Trend Micro.* “Developing Story: COVID-19 Used in Malicious Campaigns.” Accessed on Nov. 10, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

6 Mary K. Pratt. (January 16, 2020). *CSO Online.* “What is Zero Trust? A model for more effective security.” Accessed on Nov. 12, 2020, at https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

7 Elizabeth Beattie. (April 3, 2020). *Al Jazeera Media Network.* “We’re watching you: COVID-19 surveillance raises privacy fears.” Accessed on Nov. 11, 2020, at https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raisesprivacy-fears.

8 Elliot Cao et al. (March 24, 2020). *Trend Micro.* “Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links.” Accessed on Nov. 12, 2020, at https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/.

9 Nelson William Gamazo Sanchez et al. (October 19, 2020). *Trend Micro.* “Operation Earth Kitsune: Tracking SLUB’s Current Operations.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations.

10 Lawrence Abrams. (November 11, 2020). *BleepingComputer.* “Alleged source code of Cobalt Strike toolkit shared online.” Accessed on Nov. 17, 2020, at https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/.

11 Zack Whittaker. (August 20, 2020). *TechCrunch.* “Fearing coronavirus, a Michigan college is tracking its students with a flawed app.” Accessed on Nov. 11, 2020, at https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app/.

12 Guy Rosen. (September 28, 2018). *Facebook.* “Security Update.” Accessed on Nov. 11, 2020, at https://about.fb.com/news/2018/09/security-update/.

13 Danny Palmer. (April 2, 2019). *ZDNet.* “Security flaws in banking apps expose data and source code.” Accessed on Nov. 11, 2020, at https://www.zdnet.com/article/security-flaws-in-banking-apps-expose-data-and-source-code/.

14 Edward Amoroso. (June 5, 2020). *Help Net Security.* “Understanding cyber threats to APIs.” Accessed on Nov. 11, 2020, at https://www.helpnetsecurity.com/2020/06/05/api-security-threats/.

15 Trend Micro. (May 14, 2019). *Trend Micro.* “Container Security: Examining Potential Threats to the Container Environment.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

TURNING THE TIDE

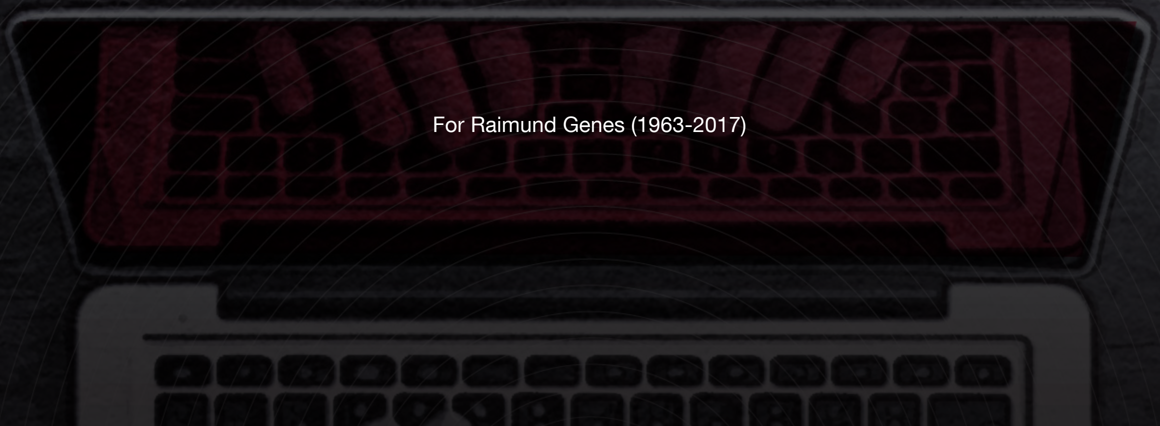
Trend Micro Security Predictions for 2021

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 threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



For Raimund Genes (1963-2017)