



# Navigating New Frontiers

Trend Micro 2021 Annual Cybersecurity Report

## TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

**Trend Micro Research**

Stock image used under license from  
Shutterstock.com

# Contents

**4**

Modern Ransomware Actors Continue to Target Critical Industries

**9**

Cloud Adopters and Remote Workers Contend With Rising Threats to Cloud Environments

**16**

Targeted Attacks Take Aim at Bigger Game With Upgraded Arsenal

**20**

Rising Vulnerabilities Leave Unpatched Systems Exposed to More Risks

**26**

Pandemic-Related Threats Evolve and Continue to Plague Remote Workers

**30**

Increasingly Sophisticated Threats Call for Robust and Multilayered Defense

**32**

The Threat Landscape in Brief

A man in a checkered shirt is talking on a mobile phone in an office setting. The background is slightly blurred, showing other office equipment and a desk.

In 2021, the fast-tracked digital transformations that enabled the continuity of many organizations also opened them up to a slew of threats both old and new, as cybercriminals proved savvy to opportunities for abuse and attack, including those that had emerged since the onset of the Covid-19 pandemic.

Modern ransomware actors grew more ambitious and deliberate with their attacks, and set their sights on more profitable targets. Going beyond indiscriminately going after their victims, operators running ransomware families like REvil<sup>1</sup> and Conti<sup>2</sup> eschewed automated attacks in favor of a more hands-on, long-haul approach to carefully tailor their campaigns to entities in critical industries.

Targeted attacks gained popularity among different kinds of malicious actors, including those in cyberespionage and cybermercenary groups, who were armed with upgraded toolboxes that made their operations even more effective. Attacks from the likes of Void Balaur<sup>3</sup> and Tropic Trooper<sup>4</sup> demonstrated how these groups were capable of developing customized tools and were adept at red teamwork. Phishing scams remained a staple in these cyberattacks, in part because the influx of news about the global pandemic gave malicious actors ideas for new lures that resonated with a wider pool of potential victims.

Any cracks in an organization's security posture could be devastating for business continuity, as could be seen from the rise in and impact of critical vulnerabilities in 2021. The growth of the underground exploit market proved that, left unpatched, older flaws could still inflict as much damage on infected systems as newly discovered ones. Malicious actors continued to employ flaws both old and new in their campaigns, as in the Squirrelwaffle loader's use of the ProxyLogon and ProxyShell vulnerabilities,<sup>5</sup> and the Khonsari ransomware attacks that incorporated the Log4Shell vulnerability.<sup>6</sup>

Pressing security issues also continued to plague organizations-turned-cloud-adopters. Most of the challenges in cloud security in 2021 could be attributed to misconfigurations in the setup of cloud environments, as evidenced by how TeamTNT abused incorrectly configured servers to compromise Docker Hub accounts. TeamTNT was one of the first cybercriminal groups to focus primarily on cloud service providers (CSPs), signaling a growing interest in the cloud within cybercriminal circles.

From large-scale ransomware campaigns to high-risk vulnerabilities, the far-reaching impact of these security incidents showed that no user, enterprise, or industry was immune to compromise. The massive disruptions caused by high-profile attacks underscored the need for visibility over the ever-evolving attack surface across an organization's entire digital infrastructure. The defenses that might have sufficed in a prepandemic world stood to be reevaluated, if not redefined, in the face of mounting risks that could be averted only by an adaptive threat monitoring, detection, and response strategy with which organizations could continuously assess and enhance their security postures.

This annual cybersecurity report explores the notable events and emerging trends that shaped the cybersecurity landscape of 2021, during which Trend Micro protected its customers from over 94 billion threats. We hope that this roundup can provide organizations and end users alike with valuable insights they can use to make informed decisions about their security infrastructure and policies as they navigate and move forward in an ever-changing threat landscape.

# Modern Ransomware Actors Continue to Target Critical Industries

Over the years, we have observed how ransomware has evolved significantly. In 2018, a spray-and-pray strategy was the norm among malicious actors, who wanted to profit from as many victims as possible.<sup>7</sup> However, our researchers foresaw how ransomware operators would pivot away from such a quantity-based tactic and become more deliberate in their movements.<sup>8</sup> Notably, in 2021 ransomware operators staged attacks on more profitable targets, leading to business disruptions with real-world ramifications felt on a global scale.<sup>9</sup>

Already strained by the pandemic, healthcare organizations were hit hard by ransomware attacks in 2021, which were just behind the banking and government industries in terms of ransomware detections. A 2021 report suggests that because healthcare organizations are less likely to back up their data than those in other industries, they are more prone to paying the demands of ransomware actors.<sup>10</sup> Moreover, the healthcare industry has a trove of data that attackers seek to sell or use for extortion, including patient records with social security numbers, medical histories, and financial information.<sup>11</sup>

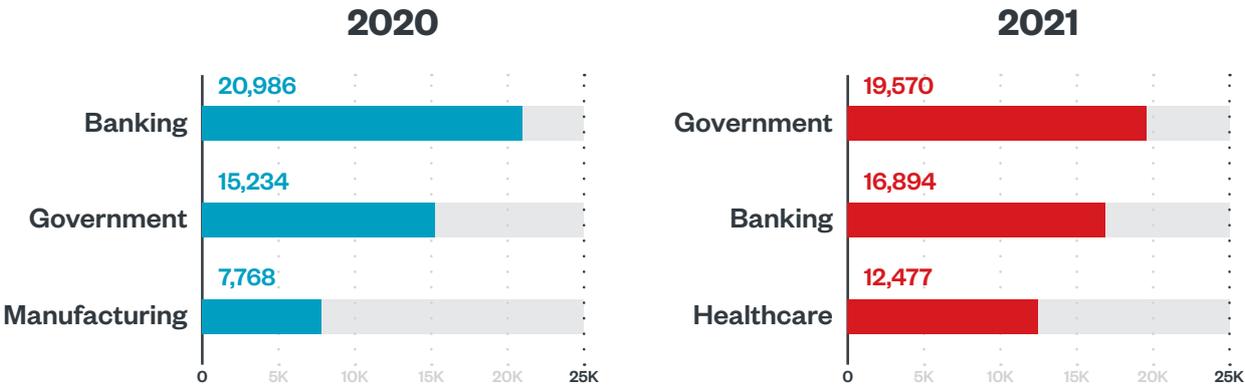


Figure 1. The top three industries in terms of ransomware file detections in 2021 and 2020

Source: Trend Micro Smart Protection Network

Attempted WannaCry infections topped the list of ransomware detections across all three of the most affected industries, outpacing other ransomware families by a wide margin. The spray-and-pray approach used by legacy ransomware like WannaCry might account for its large volume of attacks, but notably, modern ransomware gained ground.

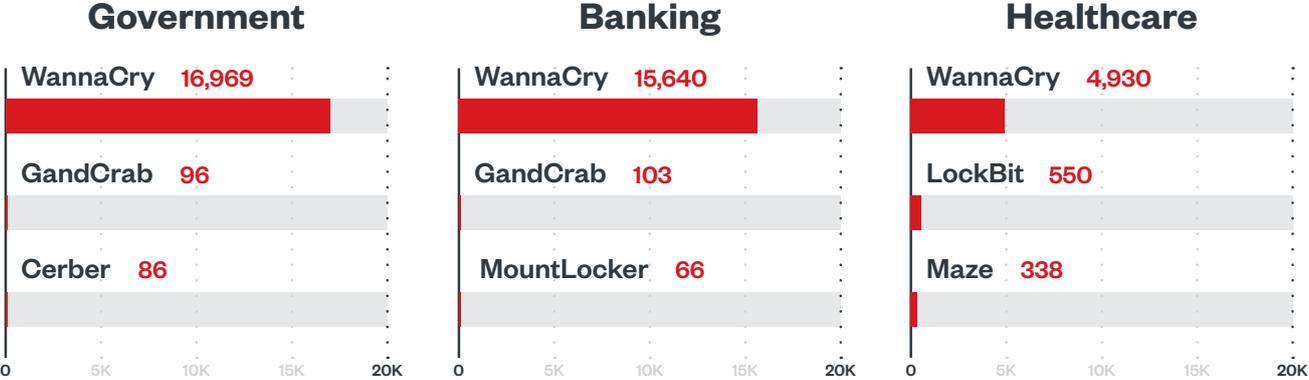


Figure 2. The top three ransomware families that affected the top three affected industries in 2021

Source: Trend Micro Smart Protection Network

Unlike their premodern counterparts, modern ransomware groups displayed erratic activity as they closed in on specific targets rather than cast a wide net,<sup>12</sup> which is most likely why we observed a 21% decrease in overall ransomware detections in 2021. We observed several modern ransomware groups ramp up their activities last year: Year-on-year detections of REvil (also known as Sodinokibi) soared by 143%, there were over 20 times as many detections of LockBit in 2021 as there were in 2020, and detections of Conti rose more than ninefold from the previous year.

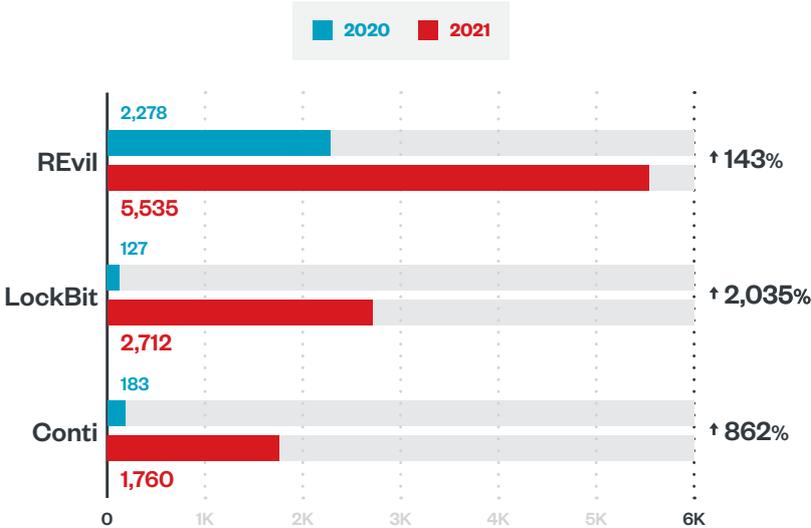


Figure 3. A year-on-year comparison of the top three modern ransomware families in terms of file detections in 2020 and 2021

Source: Trend Micro Smart Protection Network

Another factor that might have played into the decline in ransomware detections was the marked increase in our detections and blocking of malware tools like the Cobalt Strike beacon CoBeacon, the trojan Trickbot, and the information stealer BazarLoader. Our blocking of larger numbers of these affiliate tools might have prevented ransomware operators from staging full-blown attacks in 2021, as the presence of such tools is an early indicator of infection. In 2021, there was an eightfold rise in detections of CoBeacon, which had been abused by operators of ransomware families such as DoppelPaymer, Povlsomware, and Ryuk.<sup>13</sup> Detections of Trickbot, which had been linked to the Conti ransomware<sup>14</sup> as well as Ryuk,<sup>15</sup> saw a 23% year-on-year increase. Most notably, detections in 2021 of BazarLoader, which had been used to gain initial access to systems by the likes of Conti<sup>16</sup> and Ryuk,<sup>17</sup> were up by 2,468% from the previous year.

Because modern ransomware has more human involvement, collaboration among cybercriminals has gained traction in the underground, as evidenced by the rising trend of ransomware-as-a-service (RaaS). RaaS affiliate programs have been beneficial for all cybercriminal parties involved: By bringing partners onboard to divide the labor, ransomware actors can more efficiently profit from a victim's compromised assets.<sup>18</sup> The proliferation of RaaS has not only made ransomware more accessible even to malicious actors with limited technical knowledge but also given rise to higher specialization within the cybercrime ecosystem. In splitting the work among themselves, RaaS affiliates have been able to hone their skills and focus on certain specialties like penetrating networks or running the malware.<sup>19</sup>

The widespread use of RaaS is a result of the ongoing evolution of the flourishing cybercrime-as-a-service market, which continues to develop new business models for attackers. One such development is the growing demand for access-as-a-service (AaaS), with access brokers peddling stolen credentials in the criminal underground and finding reliable customers in ransomware actors, who use their wares to infect target systems.<sup>20</sup>

Another trend that has caught on within cybercriminal circles is the incorporation of double extortion, in which ransomware actors not only demand a sum to restore access to a victim's encrypted files but also threaten to release the sensitive data upon failure of payment. This tactic was first perpetrated in 2019 by the Maze ransomware and has since become even more widely used. As of June 2021, as many as 35 ransomware families employed double extortion. Some, including REvil and Conti, augmented their RaaS operations with this extortion technique to pursue big-name targets.<sup>21</sup>

Since it was discovered by Cisco Talos in 2019, REvil has become one of the most active RaaS families.<sup>22</sup> In 2021, it continued its use of double extortion on multinational enterprises like Apple,<sup>23</sup> JBS,<sup>24</sup> and Kaseya<sup>25</sup> to great effect. The bulk of REvil attacks took place in the US, but countries like Mexico and Germany were also affected.

Based on our telemetry, REvil attacks were aimed at critical industries. Most were levied against the transportation industry, followed by organizations in the financial and the oil and gas industries. In our report on ransomware activity during the first half of 2021, we posited that the transportation industry bore the brunt of REvil attacks likely because it played an important part in global supply chains and logistics.<sup>26</sup>

REvil’s customized attacks suggest that its operators have extensive knowledge of their targets’ IT environments. The efficiency of REvil can also be attributed to its diverse toolbox. This includes the use of Qakbot, AdFind, BloodHound, and other third-party sync tools, and the exploitation of vulnerabilities like CVE-2021-30116, which affects Kaseya VSA servers; CVE-2019-2725, a deserialization vulnerability in Oracle WebLogic; the FortiGate SSL VPN flaw CVE-2018-13379; and the Pulse Secure SSL VPN vulnerability CVE-2019-11510.<sup>27</sup>

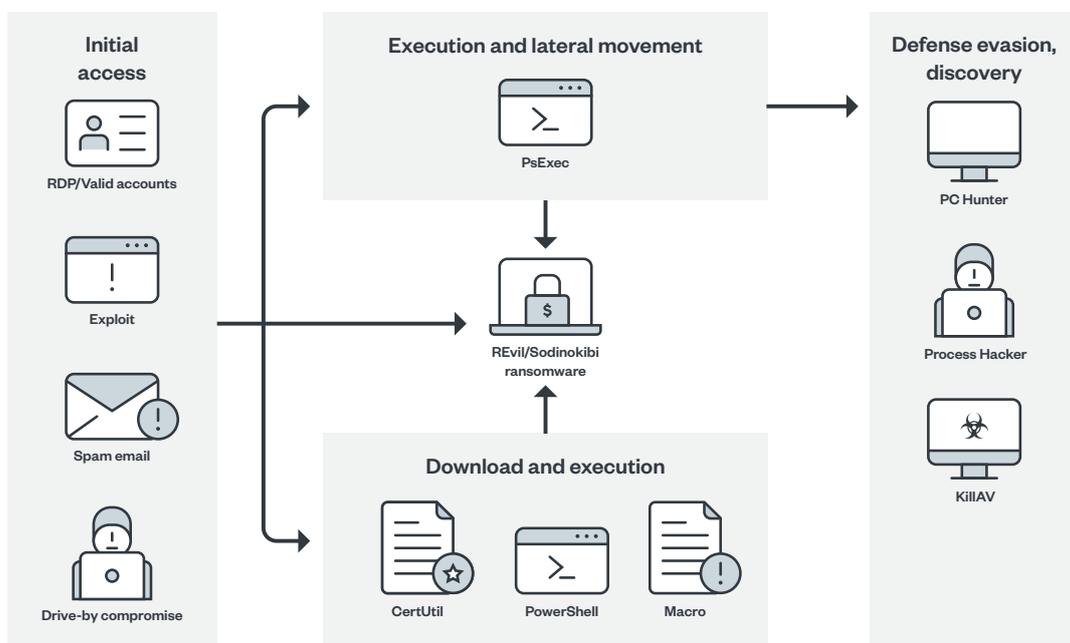


Figure 4. REvil’s infection chain

Another notorious RaaS, called Conti, which we believe to be a successor of Ryuk, was behind many debilitating attacks around the world in 2021.<sup>28</sup> In the US alone, there were more than a million Conti attacks between January 1 and November 12, 2021.<sup>29</sup> As noted in our 2021 midyear cybersecurity report, this modern ransomware family had the tenth highest number of attack attempts during the first half of 2021.<sup>30</sup> The bulk of these occurred in the US, followed by the Netherlands and Taiwan. Retail organizations experienced the most Conti attacks. The insurance, manufacturing, and telecommunications industries were also hit hard, but Conti’s high-profile attacks on healthcare organizations was what made major headlines last year.<sup>31</sup>

Like REvil's, Conti's operators also take advantage of double extortion, threatening to release stolen data and selling access to infected systems if their victims fail to pay the ransom. They employ a variety of exploits, such as those of the PrintNightmare and Zerologon vulnerabilities, and tools and malware, including familiar names like BazarLoader, Cobalt Strike, Mimikatz, and Rclone. Working in concert, these enable Conti operators to gain remote access to a targeted system, disable the system's security software, locate and exfiltrate valuable data, and encrypt files to make them inaccessible until the ransom demand is met.

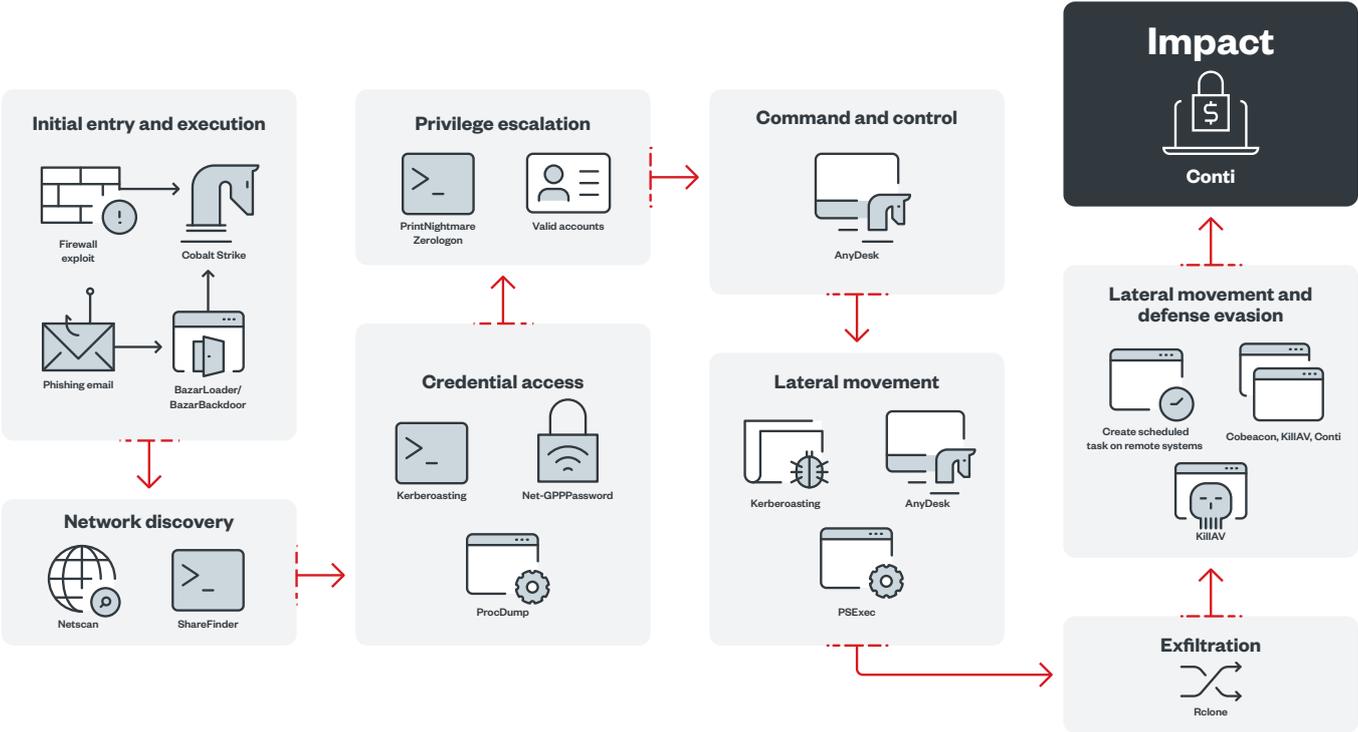


Figure 5. Conti's infection chain

# Cloud Adopters and Remote Workers Contend With Rising Threats to Cloud Environments

Threats to cloud security were among the most pressing IT infrastructure risks for organizations in 2021, according to the Cyber Risk Index for the first half of 2021.<sup>32</sup> Protecting their cloud architecture is a challenge for companies because many of the technologies that compose this architecture are regularly updated with new features.<sup>33</sup> On top of these complexities, defenders must keep up with the tools malicious actors use to target the cloud, which are also constantly changing. For instance, in 2019, steganography, or the practice of hiding code within an image, was a trend in cloud attacks.<sup>34</sup> The following year, malicious actors used valid and clean images that downloaded malware onto affected systems after deployment. And as detailed in our midyear cybersecurity report, in 2021 attackers reverted to using images with malicious content.<sup>35</sup>

## Malicious Actors Continue to Take Advantage of Cloud Misconfigurations

The cloud has helped many organizations accelerate their digital transformations and embrace remote work during the Covid-19 pandemic. Spending on cloud infrastructure, including cloud computing and storage solutions, saw a 6.6% year-on-year increase in the third quarter of 2021, which amounted to US\$18.6 billion, and 2021 saw an overall growth in cloud-related expenditure, according to the International Data Corporation.<sup>36</sup>

However, malicious actors were quick to capitalize on this push toward digitization, as securing the cloud comes with its share of complexities. Cloud environments continued to be at risk of compromise at the hands of cybercriminals who were out to abuse any misconfigurations, which proved to be major weak spots of cloud security even though CSPs had endeavored to make cloud services safer by recommending that all customers follow the shared responsibility model.<sup>37</sup>

Fortifying the security postures of cloud environments that use services like those of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) — the three biggest CSPs in the world<sup>38</sup> — should be a top priority for cloud adopters, for whom misconfigurations might not only lead to costly data breaches but also run up expenses from idle instances and unused storage.<sup>39</sup> According to 2021 data

from Trend Micro Cloud One™ – Conformity, Amazon Elastic Block Store, a block storage service, had the highest number of configuration failures among AWS services, with a misconfiguration rate of 29%. Virtual Machines had the most misconfigurations among Azure services, with a 65% misconfiguration rate, while Identity and Access Management (IAM) pulled in the most misconfigurations among GCP services, with a 98% misconfiguration rate.



Figure 6. The misconfiguration rates for the top three AWS services in terms of rule checks in 2021

Source: Trend Micro Cloud One™ – Conformity

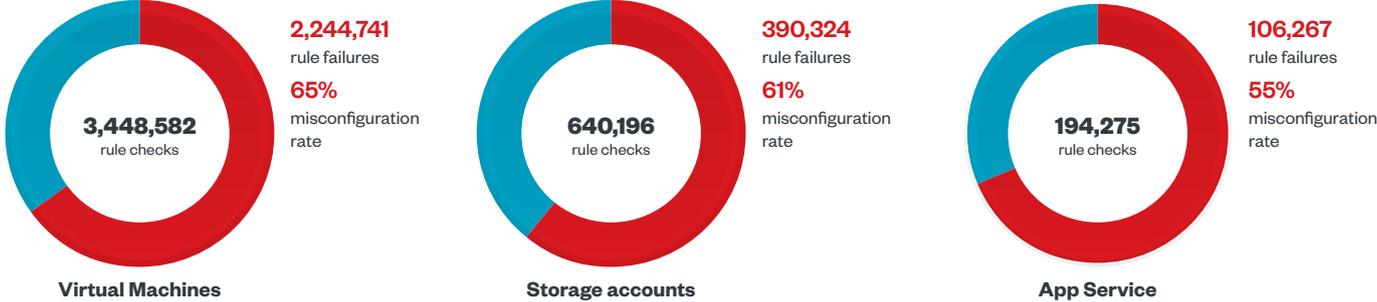


Figure 7. The misconfiguration rates for the top three Microsoft Azure services in terms of rule checks in 2021

Source: Trend Micro Cloud One – Conformity

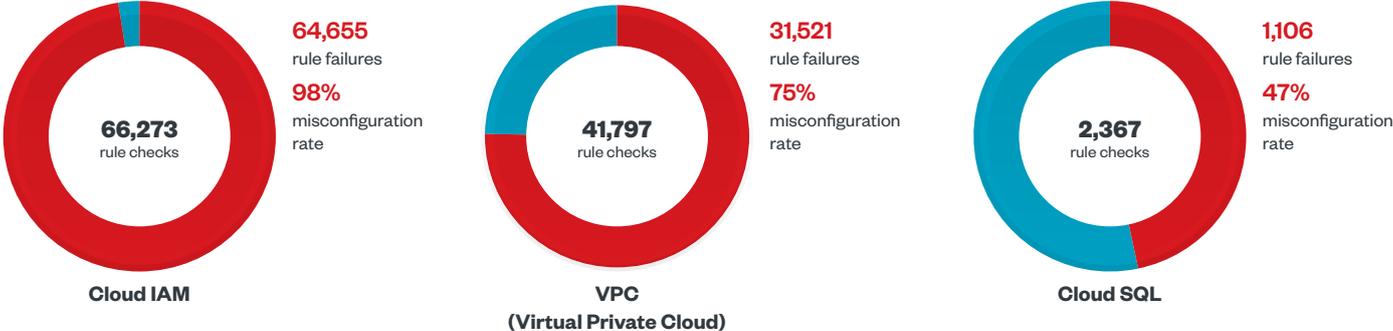


Figure 8. The misconfiguration rates for the top three GCP services in terms of rule checks in 2021

Source: Trend Micro Cloud One – Conformity

One misconfiguration that was frequently abused by malicious actors in 2021 was found in the REST APIs of Docker, a software platform used to build, test, and deploy software applications. Incorrectly configured servers with exposed Docker REST APIs became a prime target for the cybercriminal group TeamTNT, which abused the Docker REST APIs by using compromised Docker Hub accounts to deploy malware like cryptocurrency miners.<sup>40</sup>

The growing adoption of cloud-based software and services has put the cloud in the crosshairs of malicious actor groups like TeamTNT, which was among the first groups to target CSPs in their campaigns, primarily to steal CSPs' environmental metadata. Upon analyzing their recent campaigns, we found that the group had augmented its repertoire of tools, which enabled it to launch more modular attacks on specific victims.<sup>41</sup>

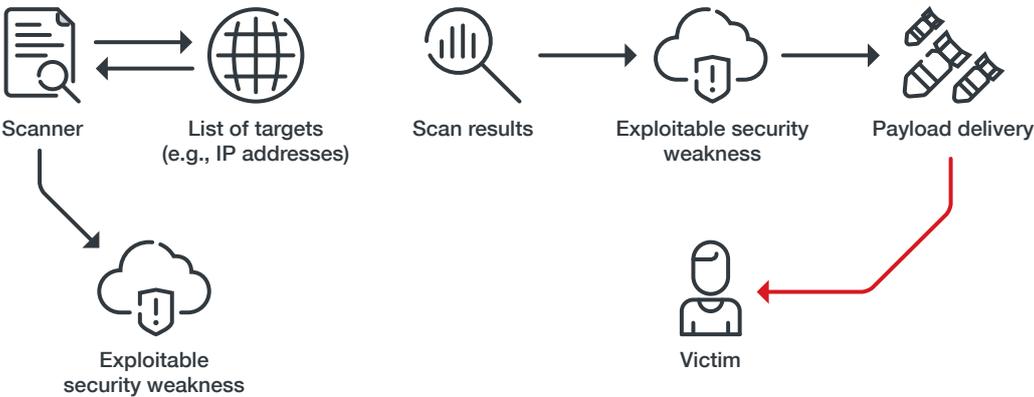


Figure 9. TeamTNT's attack chain

This group was also the perpetrator behind a cryptocurrency-mining and credential theft campaign that targeted Kubernetes, a widely used container management platform, from March to May 2021. By exploiting a role-based access control misconfiguration as an entry point for its attacks, TeamTNT was able to take over multiple Kubernetes clusters. This resulted in the compromise of nearly 50,000 IP addresses, most of which were in China and the US.<sup>42</sup>

# Email Threats Climb as More Organizations Adopt Remote Work

Since the onset of the pandemic, internet and email usage had been even more instrumental for business continuity and remote work. As email became an even more useful tool for people around the world who were working from home, malicious actors seized the opportunity to take advantage of remote workers' increased dependence on online communication. In 2021, Trend Micro Cloud App Security, an API-based solution that protects both users and organizations from threats to their cloud-based apps and services, detected and blocked more than 25.7 million email threats, a marked increase from the over 16.7 million threats that the solution detected and blocked the previous year.

Email remained an oft-used avenue for cybercriminals to stage their attacks. In fact, 92% of malware was delivered through email in 2021.<sup>43</sup> Phishing emails in particular were responsible for 90% of 2021’s data breaches.<sup>44</sup> Phishing campaigns persisted as an effective means to spread malware, especially ransomware, in 2021, as proved by the enduring success of Emotet, the notorious botnet-malware-turned-RaaS. Authorities took down Emotet in November 2021, but its absence was short-lived, as it resurfaced toward the end of the year.<sup>45</sup> Its yearslong use by ransomware groups like Ryuk and trojans like Trickbot showed how much the underground economy had grown and continued to evolve, to the point that it eventually developed its own supply chain.<sup>46</sup>

Phishing attempts that were detected and blocked by Trend Micro Cloud App Security in 2021 nearly doubled from those in 2020. Of these, 62% were from spam emails, which increased nearly sevenfold from the previous year. The remaining 38% were credential-phishing attempts, which grew by 14% from 2020. (Credential phishing involves cybercriminals’ use of fake login pages to gull potential victims into handing over their account credentials, whereas phishing by spam email is a broader category that aims to get user information.) The finance industry experienced the most phishing attempts, followed closely by the healthcare and education industries.

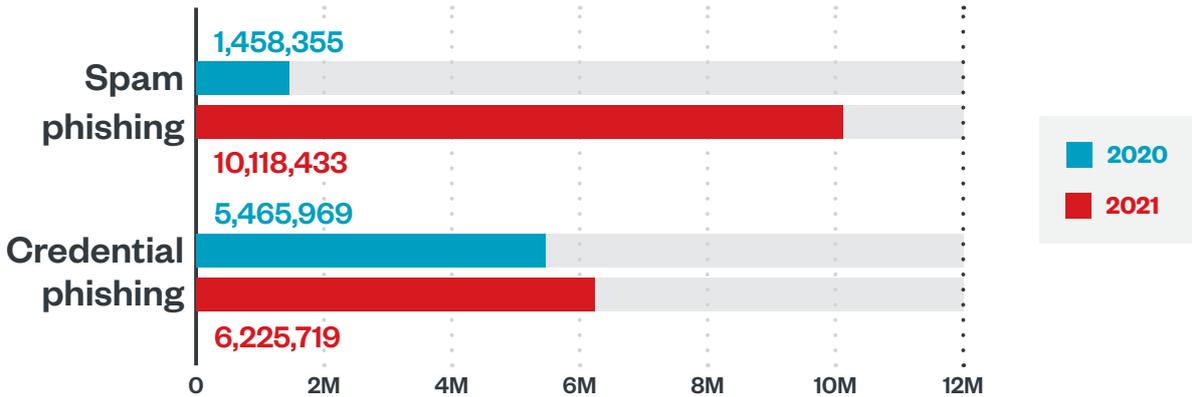


Figure 10. A comparison of the detections of spam phishing and credential-phishing attempts in 2020 and 2021

Source: Trend Micro Cloud App Security

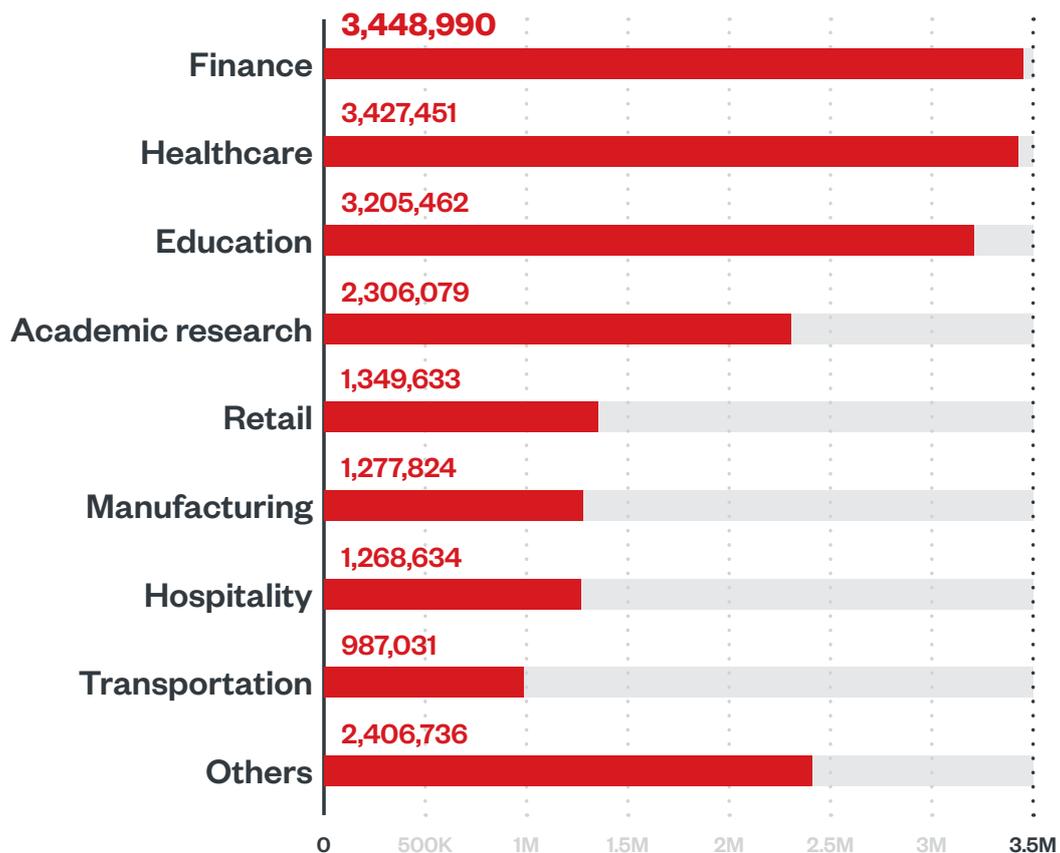


Figure 11. The industries with the highest detections of spam phishing and credential-phishing attempts in 2021

Source: Trend Micro Cloud App Security

Despite a slight increase during the first half of the year, possibly as a result of more attacks on businesses and supply chains related to vaccine production,<sup>47</sup> detections of attempts at business email compromise (BEC) totaled 282,775 in 2021, dropping 11% from the previous year's BEC detections.

Malicious actors turned to increasingly sophisticated BEC attempts, focusing on improving the quality of their email content rather than on churning out a high volume of attack attempts. Though there were fewer BEC attempt detections in 2021, Trend Micro Cloud App Security found and blocked 133,541 BEC emails using authorship analysis, while the remaining 149,234 were detected using behavior and intention analysis. The former, which could be detected only by comparing the spoofing email with the writing style of the supposed sender, made up 47% of all BEC attempts in 2021, whereas the 73,210 that were detected in 2020 composed only 23% of all BEC attempts found that year.

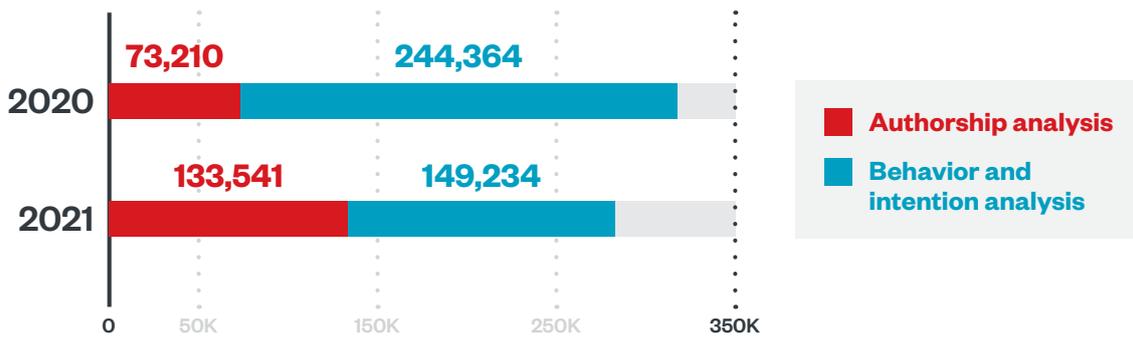


Figure 12. A comparison of the proportions of BEC attempts blocked based on authorship analysis and BEC attempts blocked based on behavior and intention analysis in 2020 and 2021

Source: Trend Micro Cloud App Security

The greatest numbers of BEC attempts were aimed at the retail and consulting industries. The retail industry remained an appealing target for financially motivated cybercriminals, especially phishing fraudsters, owing to the wealth of customer payment data, credentials, and other personal information that retailers held.<sup>48</sup>

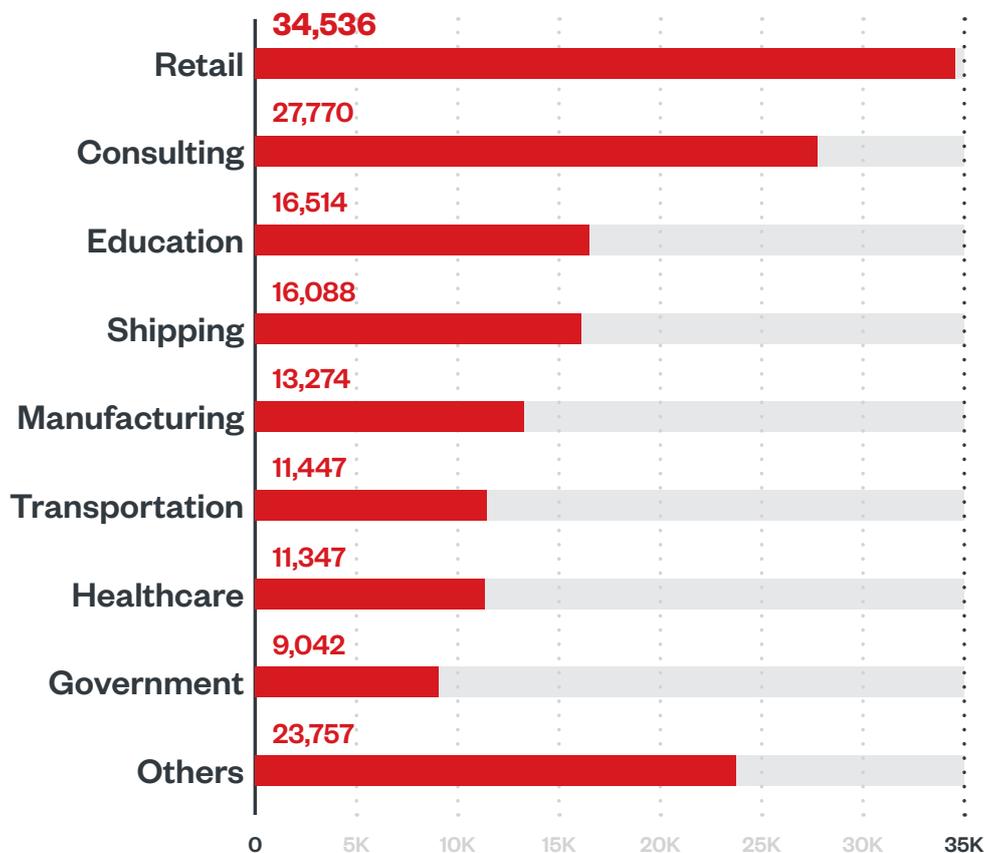


Figure 13. The industries with the highest detections of BEC attempts in 2021

Source: Trend Micro Cloud App Security

In 2021, the information and communication industry was the most common target of malware-laden emails. While many businesses struggled during the pandemic, this industry continued to grow and is expected to be valued at over US\$11.9 trillion by 2025, which might explain why it had been in the crosshairs of attackers.<sup>49</sup> Retail companies were also on the receiving end of many emails with malware. Retailers drew the attention of more attackers after the industry experienced rapid growth when online sales surged as a result of the pandemic.<sup>50</sup> Malicious email attachments were also a common means for cybercriminals to carry out attacks on construction firms, which were appealing targets because of their valuable intellectual properties, such as blueprints, that could be used to bypass buildings' security.<sup>51</sup>

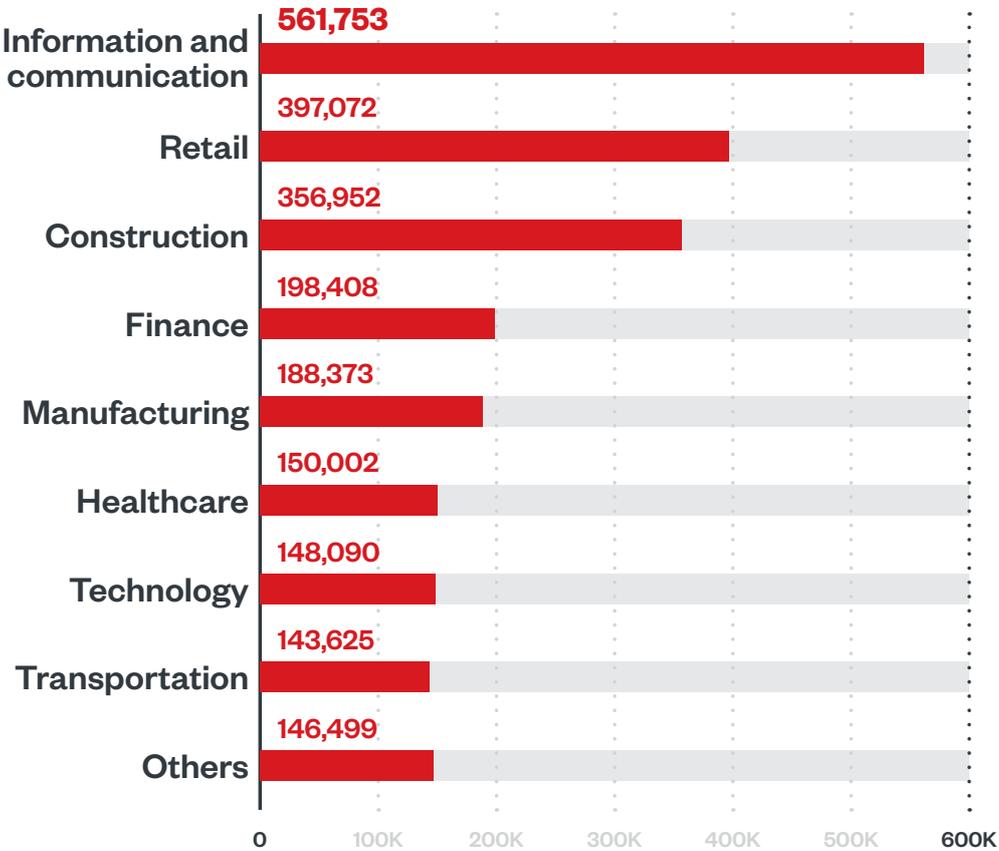


Figure 14. The industries with the highest detections of malware files in emails in 2021

Source: Trend Micro Cloud App Security

# Targeted Attacks Take Aim at Bigger Game With Upgraded Arsenal

With more malicious actors moving past the indiscriminate distribution of their malware, 2021 saw certain industries fall prey to targeted attacks. An enduring threat that has plagued organizations as far back as 2012,<sup>52</sup> targeted attacks require a high level of technical expertise and a plethora of resources on the part of threat actors, because the tools and techniques involved need to be tailored to the intended victims' systems.<sup>53</sup>

During the first half of 2021, we observed a shift to more targeted modern ransomware that veered away from quantity-based attacks and toward more profitable prey,<sup>54</sup> as more cybercriminals resorted to increasingly advanced tools and techniques that pointed to a targeted approach. Not only can this kind of attack have a direct impact on the targeted organization, but its effects can also be felt by the victim's customers because of any resulting business disruption or customer information leakage.<sup>55</sup> The threat actors behind a targeted attack may be financially motivated, but its main goal is data theft.<sup>56</sup>

## Void Balaur Stages Attacks on Government Entities and Other Targets

Also known as Rockethack, Void Balaur is a cybermercenary group that deals largely in data theft and cyberespionage, advertising its services in the Russian-speaking cybercriminal underground through forums and websites like Darkmoney and Probiv. In past years, we observed this group launch attacks on the telecommunications, retail, financial, medical, and biotechnology industries. They continued pursuing telecommunications organizations in 2021, when we discovered that Void Balaur had been targeting engineers and management officers of various Russian and UK telecommunications outfits.<sup>57</sup>

Although the hackers-for-hire behind the group are driven by monetary gain, they have also frequently targeted journalists, human rights activists, and government officials. For instance, in September 2021, we found Void Balaur targeting a former head of an intelligence agency, two members of the national parliament, and five active government ministers of an Eastern European country. This suggests that their activities might play into a larger campaign on multiple fronts to cause widespread disruption. Many of their targets are based in Russia and its neighboring countries, although Void Balaur activity has also been spotted in other European countries, the US, Japan, and Israel.

Among Void Balaur's main services is hacking into email and social media accounts. For a higher fee, the group can also supply the complete copies of stolen email inboxes without the users' knowledge. In 2019, it began selling the confidential information of Russian individuals, such as their criminal records, credit histories, bank statements, text messages, and passport and flight data. Void Balaur uses specialized malware like Z\*Stealer and DroidWatcher, capable of remote tracking, accessing location information, and stealing user credentials for different apps and digital currency wallets.<sup>58</sup>

## Tropic Trooper Returns to Attack the Transportation and Government Industries

The cyberespionage group Tropic Trooper, which now goes by Earth Centaur, has been active since 2011 but it resurfaced in July 2020 with new tools, including modified remote access trojans (RATs). Toward the end of 2020 and continuing in 2021, we observed it using these tools to target transportation businesses and transport-related government organizations.<sup>59</sup> Its attacks commonly involve information theft — including that of financial documents, search histories, and flight schedules — from compromised systems. Based on our analysis, we predict that Tropic Trooper will continue gathering confidential data while waiting for the opportune time to capitalize on it.

Tropic Trooper usually breaches its victims' systems by exploiting vulnerabilities in their Microsoft Internet Information Services and Exchange servers, and then installing web shells that execute backdoors such as ChiserClient and SmileSvr. The group uses a customized variant of Gh0st RAT to discover and collect information from active sessions on an infected host, which it then exfiltrates using the victim's compromised intranet.

The threat actors behind Tropic Trooper have proved themselves talented at red teamwork. By using open-source frameworks, they have developed various backdoors with different protocols, which they have used to bypass their victims' security settings. They also employ reverse proxies to avoid detection by network security systems.

# More Malicious Actors Use BazarLoader as an Arrival Mechanism

During the third quarter of 2021, we observed an uptick in the use of BazarLoader, an information stealer and loader that we detected as TrojanSpy.Win64.BAZARLOADER and Backdoor.Win64.BAZARLOADER. The highest detections of BazarLoader took place in the Americas region.<sup>60</sup>

Since it was first observed in 2020,<sup>61</sup> BazarLoader has been used by cybercriminals to gain initial access for data theft or to deploy second-stage malware like ransomware. Between January and October 2021, BazarLoader campaigns that used malicious spam emails as an arrival mechanism primarily targeted the US, followed by select European and Asian countries. Most of these emails took the form of fraudulent order invoices and notices of service plan termination. On the other hand, campaigns that used JavaScript droppers to deliver BazarLoader over the same period focused on targets in the US and Australia.

Notably, malicious actors use different arrival mechanisms to deliver BazarLoader as part of their attacks. In one method, BazarLoader is bundled with a legitimate program and deployed using a software installer, such as that for VLC and TeamViewer. Its delivery mechanism possibly involves social engineering as a means of tricking victims into downloading the compromised installer. A BazarLoader executable is then dropped while the installer is loading. The installer creates a process that runs the BazarLoader executable and then establishes a connection with a command-and-control (C&C) server using Microsoft Edge.

Other malicious actors favor a method that involves delivery by way of an ISO file that contains a Windows LNK (link) file. The LNK file is disguised as a folder icon to trick a victim into clicking it, which runs its BazarLoader dynamic-link library (DLL) payload.

## Qakbot Reemerges With an Improved Variant

Discovered in 2007,<sup>62</sup> the information stealer Qakbot, which is detected by Trend Micro as TrojanSpy.Win32.QAKBOT, has become popular among ransomware operators as a piece of malware-installation-as-a-service botnet malware for their campaigns. In 2019, Qakbot infections were used in the deployment of manually operated ransomware families like MegaCortex, PwndLocker, Egregor, ProLock, and, most recently, REvil/Sodinokibi.<sup>63</sup>

Following a three-month hiatus, Qakbot operators resumed their email spam run in September 2021. Their campaign returned with a new version of Qakbot that uses Visual Basic for Applications (VBA) macros as well as Excel 4.0 macros. Over the past years, we observed that spam campaigns linked to Qakbot operators mainly targeted the telecommunications, technology, and education industries. Among the top countries affected by these campaigns were the US, Japan, and Germany.

# Buer Loader Becomes Better at Evading Detection

Buer Loader's competitive pricing made it the malware loader of choice for many threat actors when it was introduced in the underground market in 2019. It remains active to this day and has been used by threat actors to deploy well-known malware such as Ryuk, Wizard Spider, and the Cobalt Strike beacon as part of targeted ransomware attacks.<sup>64</sup> We found that Buer Loader was most active in India, followed by Israel, and that detections of the loader were highest among organizations in the healthcare, banking, and telecommunications industries.

In 2021, a new variant of Buer Loader, written in Rust, was used in spam runs that involved emails with malicious attachments containing the loader. One campaign used emails that masqueraded as DHL shipping notices, while succeeding campaigns mentioned Covid-19 in their emails as a lure or referenced both DHL and Covid-19. The Buer Loader variant used in these emails retains most of the same code as in previous variants, but it was likely rewritten in a new programming language to avoid detection. This updated variant also uses signed XLL (Excel add-in) files as another way to stay under the radar of their victims' IT teams.

# Water Basilisk Uses New Crypter Tool to Flood Systems With RATs

August 2021 saw the height of activity for a fileless attack campaign called Water Basilisk, which bombards its victims' systems with RATs — including BitRat, NjRat, LimeRat, Warzone, QuasarRat, and Nanocore RAT — through a new HCrypt variant.<sup>65</sup> The operators behind Water Basilisk use this crypter-as-a-service to make obfuscated VBScript and PowerShell scripts that deploy their malicious payloads. We have observed Water Basilisk incidents that involve PowerShell scripts containing as many as seven RATs.<sup>66</sup>

Water Basilisk actors have been hosting their malware and phishing kits on publicly accessible file-hosting services and compromised WordPress websites. They use these WordPress websites or phishing emails to disseminate a malicious ISO image. This image has an obfuscated VBScript stager that downloads and executes next-stage VBScript content into an infected system. Finally, PowerShell scripts deobfuscate and deploy their payload RATs in a given process.

The HCrypt version that Water Basilisk uses to propagate its malware is sold in underground markets for US\$199. Our analysis suggests that more variants of this crypter tool, which continues to be updated by its developers, will be introduced in the future, and these can contain even more RATs and have an updated obfuscation algorithm to evade detection more effectively.

# Rising Vulnerabilities Leave Unpatched Systems Exposed to More Risks

The intricacies of modern IT infrastructures make patch management essential for business operations to run smoothly, but this is easier said than done: On average, it takes 200 days to fix a vulnerability, and 256 days if the flaw is rated severe.<sup>67</sup> In an ideal world, organizations routinely update the software they rely on and their own security policies. But this is a tall order for IT teams that are already spread thin, especially because tracking updates is but one of their many everyday tasks.<sup>68</sup>

## Older Flaws Stay Relevant as Malicious Actors Bank on Unprotected IT Environments

In 2021, Trend Micro™ Zero Day Initiative™ (ZDI), a part of Trend Micro Research, released advisories on 1,604 vulnerabilities, which was 10% higher than the corresponding number from the previous year. Among these, 54 were rated with critical severity, a significant decrease from the 173 critical vulnerabilities of 2020. However, 2021 did see an increase in those rated with high severity, rising to 1,138 from the previous year's 983.

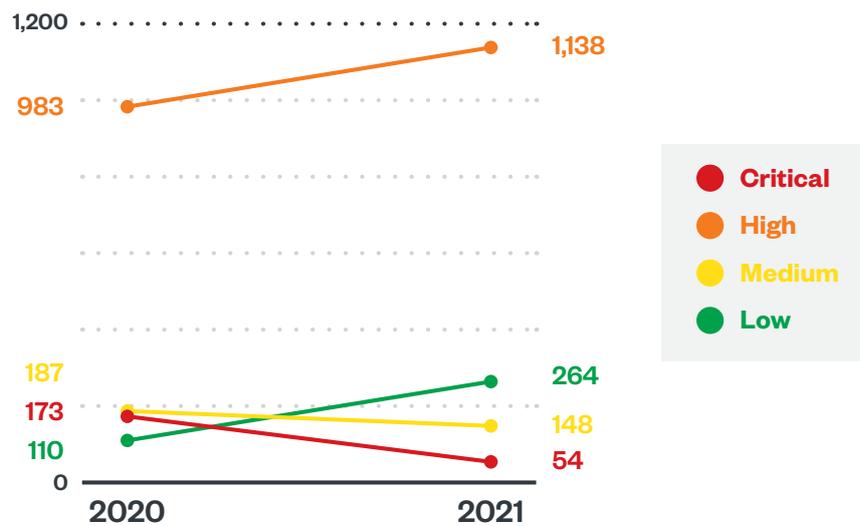


Figure 15. A comparison of the proportions of Common Vulnerability Scoring System (CVSS) ratings among vulnerabilities disclosed by Trend Micro’s ZDI program in 2020 and 2021

Source: Trend Micro™ Zero Day Initiative™

Many legacy vulnerabilities have stayed in use, as there remains a demand for them in the underground exploit market. In fact, our 2021 study found that 22% of the exploits sold in the underground were over three years old.<sup>69</sup> Such exploits have been a reliable source of income for malicious actors, who can sell them in underground forums, with prices starting at US\$1,000.<sup>70</sup>

Data from Trend Micro™ TippingPoint® Threat Protection System, a network security platform deployed at some of the largest organizations in the world, shows that malicious actors also exploited relatively new vulnerabilities alongside older ones, with some dating as far back as 2005, despite the availability of patches for these flaws. There are familiar names in the list of vulnerabilities with the highest exploit counts in 2021; seven of these have been extensively abused by cybercriminals and have ranked among the most exploited flaws since 2017.

Far and away the highest number of exploit detections in 2021 was of CVE-2019-1225, which amounted to over 75 million found by Trend Micro. CVE-2019-1225 is a memory disclosure flaw in Microsoft’s Remote Desktop Services that was disclosed in August 2019.<sup>71</sup> Successful exploits of this vulnerability allow attackers to gather information that they can use to further compromise victims’ systems. Coming in second was the critical vulnerability CVE-2017-14100. Found in Asterisk, a software implementation of a private branch exchange from Digium, this flaw accounted for more than 20 million detections in 2021. Exploits of this flaw, which was disclosed in September 2017, allow unauthorized users to remotely perform arbitrary shell command injections.<sup>72</sup>

CVE ID number	Affected product	Rule ID	Hits
CVE-2019-1225	Windows RDP server	DV-36042	75,267,406
CVE-2017-14100	Asterisk 11	DV-29739	20,846,194
CVE-2011-1264	Microsoft Windows Server	DV-3886	4,831,951
CVE-2010-0817	Microsoft SharePoint server		
CVE-2014-6271	GNU Bash	DV-16798	1,860,228
CVE-2014-6277			
CVE-2014-6278			
CVE-2014-3567	OpenSSL	DV-17056	1,622,083
CVE-2005-1380	BEA Admin Console	DV-2023	1,054,890
CVE-2010-3936	Microsoft Forefront Unified Access Gateway		
CVE-2010-0817	Microsoft SharePoint server		
CVE-2017-0068	Microsoft Edge		
CVE-2003-1138	Apache	DV-11984	1,032,998
CVE-2017-5638	Apache Struts	DV-27410	784,031
CVE-2018-13379	Fortinet FortiOS	DV-36087	631,799
CVE-2018-10562	Dasan GPON home router	DV-31936	588,763

Table 1. The top vulnerabilities in terms of exploit detections in 2021

Source: Trend Micro™ TippingPoint® Threat Protection System

## Log4j Flaw Log4Shell Leads to Exploit Outbreak

2021 was peppered with noteworthy incidents that resulted from unpatched security gaps, such as the high-severity vulnerability CVE-2021-44228. First reported privately to Apache in November 2021<sup>73</sup> and dubbed Log4Shell, this flaw affects Apache Log4j, a Java-based logging tool.<sup>74</sup> Although the open-source Apache community had released a patch for it in December, the vulnerability still led to a slew of exploits that malicious actors developed for a variety of illicit activities, including data theft, malware deployment, and unauthorized cryptocurrency mining or cryptojacking. Notably, the operators of the Khonsari ransomware began using Log4Shell in their attacks in December 2021.<sup>75</sup>

Log4j is a widely used utility in both in-house and third-party applications for enterprises. Log4j's dependence on Java makes it difficult to detect when the tool is running across an enterprise's environments. This explains why Log4Shell is not easily addressed, despite the availability of a patch. Log4Shell could allow attackers to send crafted log messages that execute arbitrary code, effectively weaponizing compromised machines to launch different kinds of attacks.

As of December 2021, Log4Shell affected only 7% of Trend Micro customers, scattered across the Americas, the AMEA (Asia, Middle East, and Africa) region, Europe, and Japan, with the US having experienced the highest number of incidents.<sup>76</sup> Among our customers, the organizations most affected by this vulnerability belonged to the government, retail, and manufacturing industries.

# Attackers Exploit ProxyLogon and ProxyShell Flaws

Other prominent flaws that made waves in 2021 included the ProxyLogon and ProxyShell vulnerabilities in Microsoft Exchange Server, which were disclosed in late 2020. Microsoft released patches for ProxyLogon (CVE-2021-26855) in March 2021 and for the ProxyShell vulnerabilities (CVE-2021-34473 and CVE-2021-34523) in May and July 2021.<sup>77</sup> Despite the availability of patches, however, our telemetry showed that ProxyLogon had been part of many 2021 attacks by different malware families, such as the LemonDuck cryptocurrency miner, the BlackKingdom ransomware, and the Prometei botnet malware.<sup>78</sup>

In September 2021, researchers reported on spam campaigns employing a new loader called Squirrelwaffle.<sup>79</sup> We found that these campaigns also used ProxyLogon and ProxyShell exploits in their spam campaigns, and in doing so, they were able to send malicious emails posing as replies in existing email threads to trick potential victims.<sup>80</sup> In November 2021, our investigation into Squirrelwaffle intrusions in the Middle East showed that publicly available ProxyLogon exploits were used to gain access to, search through, and even download a victim’s email messages. The ProxyShell vulnerabilities were also abused by Squirrelwaffle’s operators to impersonate a local administrator, enabling them to perform PowerShell commands and deliver email replies containing a malicious Excel file.<sup>81</sup>

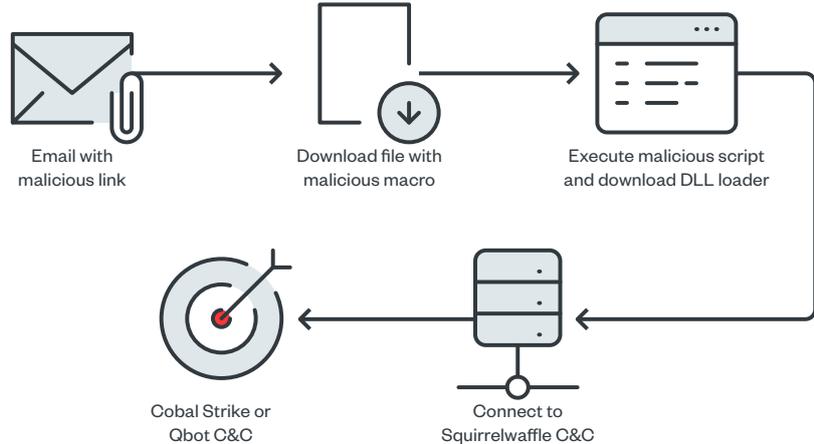


Figure 16. The infection chain of the malicious Excel file in a Squirrelwaffle spam email

# Unpatched VPN Vulnerabilities Threaten At-Home Work Setups

The pandemic has bolstered usage of virtual private networks (VPNs) among organizations whose geographically dispersed employees need to connect to secure corporate networks as part of their work-from-home setups. For organizations that have embraced remote working, scalable corporate VPNs and internal applications accessible through their VPNs have become pressing priorities.<sup>82</sup> Globally, VPN usage soared in 2021, during which VPN downloads reached 785 million.<sup>83</sup>

But like any security technology, VPNs could be abused by malicious actors for their attacks. In 2021, one of the most exploited vulnerabilities in VPN products was CVE-2018-13379, which accounted for more than 631,000 detections, even though a patch for it had been available since May 2019.<sup>84</sup> This is a path traversal flaw in Fortinet FortiOS that unauthorized users could abuse to create custom HTTP resource requests to vulnerable FortiGate SSL VPN endpoints, allowing them to read and download files from affected systems.<sup>85</sup> In early 2021, we discovered the use of CVE-2018-13379 in Sodinokibi<sup>86</sup> and Conti<sup>87</sup> ransomware attacks, exploited in conjunction with other vulnerabilities to help attackers get a foothold in victimized systems. This flaw is among the notable VPN vulnerabilities in 2021, according to Japan's Information-Technology Promotion Agency and the Japan Computer Emergency Response Team Coordination Center.

CVE		Jan	Feb	Mar	Apr	May	Jun
Total		198,777	139,165	158,372	138,181	114,727	98,577
Fortinet	CVE-2018-13379	113,330	77,853	75,785	68,651	70,083	61,467
Pulse Secure	CVE-2019-11510	45,937	15,627	27,876	21,440	15,230	9,558
		787	488	566	956	508	301
	CVE-2019-11539	0	0	1	0	0	11
	CVE-2021-22893	0	0	0	107	27	0
Citrix Systems	CVE-2019-19781	1,388	579	713	988	650	418
		3	761	158	5	5	15
Palo Alto	CVE-2019-1579	0	0	0	0	0	0
F5	CVE-2020-5902	37,332	43,857	53,038	36,493	24,493	24,378
		0	0	0	0	0	1
	CVE-2021-22986	0	0	2	12	66	19
		0	0	12	12	29	39
		0	0	221	9,517	3,636	2,370

CVE		Jul	Aug	Sep	Oct	Nov	Dec
Total		61,950	43,963	185,374	103,444	34,139	59,124
Fortinet	CVE-2018-13379	24,735	16,668	53,467	31,496	15,545	22,719
Pulse Secure	CVE-2019-11510	9,146	7,717	29,343	13,719	5,266	8,296
		274	451	3,629	4,919	487	951
	CVE-2019-11539	35	1	0	5	0	12
	CVE-2021-22893	0	0	17	3	0	0
Citrix Systems	CVE-2019-19781	631	695	9,265	5,347	472	1,268
		17	63	24	32	16	11
Palo Alto	CVE-2019-1579	0	0	0	10	0	12
F5	CVE-2020-5902	23,333	15,899	79,272	41,841	10,863	21,671
		6	0	0	0	0	5
	CVE-2021-22986	160	0	0	0	0	970
		251	151	223	309	30	86
		3,362	2,318	10,134	5,763	1,460	3,123

Table 2. A monthly comparison of the detections of attempts to exploit notable VPN vulnerabilities in 2021

Sources: Trend Micro TippingPoint Threat Protection System, Japan's Information-Technology Promotion Agency, and the Japan Computer Emergency Response Team Coordination Center

# Pandemic-Related Threats Evolve and Continue to Plague Remote Workers

The Covid-19 pandemic has driven organizations to rethink their own operations. In the midst of it, many have adopted a hybrid work model that is dependent on remote connection and cloud computing to adapt to and stay afloat through the seismic changes it has precipitated.<sup>88</sup> However, research showed that in 2021, 72% of organizations in the US still struggled to defend themselves against attacks that aimed to infiltrate their corporate networks through their employees' work-from-home setups.<sup>89</sup>

Home offices had expanded the attack surfaces of enterprises, as demonstrated at Pwn2Own Austin 2021, a hacking competition organized by Trend Micro's ZDI program.<sup>90</sup> The event highlighted how the remote-working staples that many teleworkers relied on could be subjected to attacks. The participating security researchers carried out collision hacks on devices like printers, routers, and network-attached storage (NAS) devices by using previously disclosed vulnerabilities or discovering new ones. Collectively, the participants at Pwn2Own Austin disclosed 61 new bugs.<sup>91</sup>

Malicious actors have typically used the latest events and news stories in phishing attacks, but these emails could be used only in the short term. The pandemic, though, has provided them with an abundance of information around which they could theme their phishing emails. Daily Covid-19 news coverage and updates have given them a steady supply of guises that have helped them better tailor their techniques to potential victims.<sup>92</sup>

Throughout 2021, we observed various scams and malware attacks that used social engineering tactics to entice potential victims into providing personal information. One trend was the increasing phishing attacks on the vaccine cold chain, likely because employees involved in any link of the chain had access to valuable sensitive data. Another was the proliferation of fake mobile apps and websites that impersonated government entities, nongovernmental organizations, and companies involved in vaccine distribution, which malicious actors used to target people seeking aid, work opportunities, or more information on how to acquire vaccines.<sup>93</sup>

We detected more than 8 million threats related to Covid-19 in 2021, about half as many as those in the previous year. As in 2020, most of these threats were from the US and Germany, which were likely targeted because of the important part they played in the cold chain as the base countries of major vaccine researchers and manufacturers.

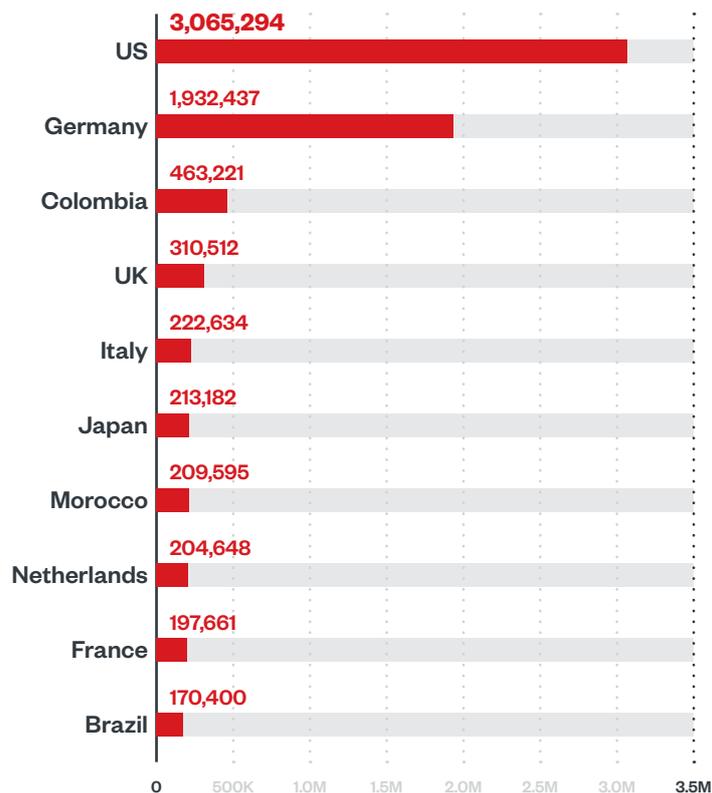


Figure 17. The top 10 countries in terms of detections of Covid-19-related threats in 2021

Source: Trend Micro Smart Protection Network

Threats that revolved around Covid-19 largely consisted of emails, which accounted for 94% of all our Covid-19-related threat detections in 2021; these saw a 45% year-on-year decrease over 2020. There was also a drop, of 82%, in detected malicious URLs from 2020 to 2021. On the other hand, malicious files more than quadrupled from 2020 to 2021; most of these were detected in Indonesia and Brazil.

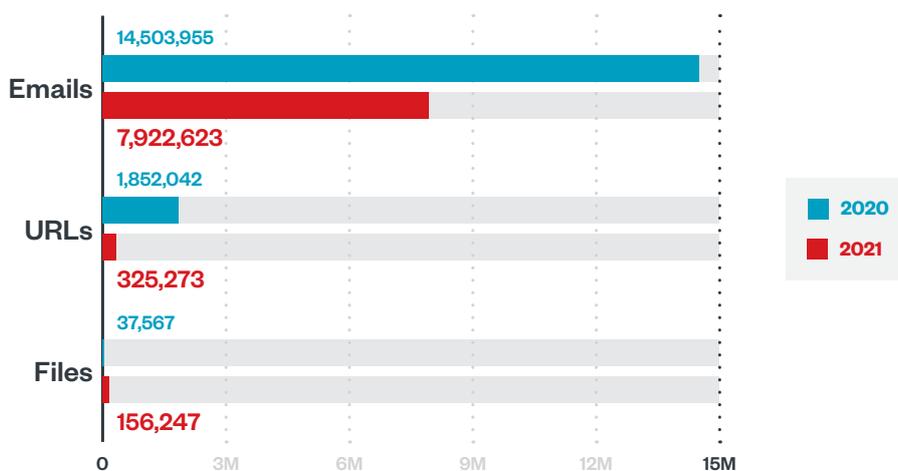


Figure 18. A comparison of the detections of Covid-19-related threats, consisting of malicious emails, URLs, and files in 2020 and 2021

Source: Trend Micro Smart Protection Network

Pandemic-related threats in 2021 peaked in May, which was an eventful period for cybercrimes against the healthcare industry. In that month, Ireland’s public healthcare system, the Health Service Executive, fell victim to a debilitating Conti attack, resulting in the largest ever known cyberattack on a health service computer system.<sup>94</sup> Additionally, a 2021 report showed that there were two or more data breaches in the healthcare industry per day for five consecutive months, from March to July, which might account in part for the substantial surge in Covid-19-related threats in May.<sup>95</sup>

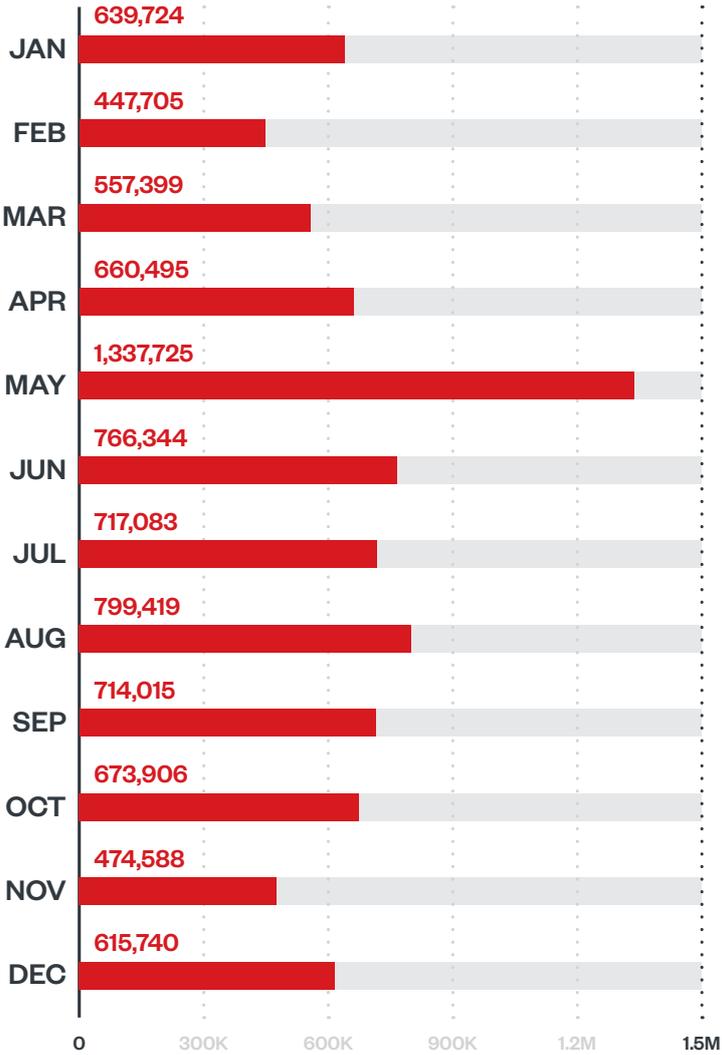


Figure 19. A monthly comparison of the detections of Covid-19-related threats in 2021

Source: Trend Micro Smart Protection Network

In 2021, there was a 49% year-on-year decline in Covid-19-related threats, which could be explained by different factors. Malicious actors might have been lying in wait for new pandemic-related trends and news that they could abuse. However, these threats were concentrated in two countries, so cybercriminal interest in Covid-19-themed lures could have been waning elsewhere. While media consumption was strong in certain countries, especially in Western Europe, the same could not be said of countries whose media agencies were not as preoccupied with the Covid-19 crisis.<sup>96</sup> Additionally, the working hours lost because of widespread lockdowns were equivalent to 255 million full-time jobs in 2020,<sup>97</sup> but that number receded to 125 million jobs the following year, as more people returned to work after mass vaccination rollouts and declines in Covid-19 cases.<sup>98</sup> As the world gradually adjusted to this new normal and the labor market made return-to-office plans, Covid-19-themed threats began to lose their efficiency. Heightened awareness of these threats might have also pushed more enterprises and individual users to employ software solutions that improved their security postures.

Still, constant vigilance of scams surrounding the pandemic is necessary for all organizations if they are to steer clear of costly losses. The World Economic Forum reports that since the pandemic began, cybercrime has evolved in step with the global digital economy: Organizations have had to fend off an average of 270 attacks each in 2021, and a single successful attack attempt can run up as much as US\$3.6 million in losses.<sup>99</sup>

# Increasingly Sophisticated Threats Call for Robust and Multilayered Defense

2021 was marked by attacks that grew in number and complexity, and whose repertoire of advanced tools and techniques underscored the necessity of a more strategic, risk-focused approach to security. Sudden shifts in business operations, like the mass migration to remote work and a growing dependence on online environments, brought about a shift in the attack surface and a multitude of security gaps that malicious actors were only too eager to exploit. Companies had grown more reliant on technologies like the internet of things (IoT) and added more connected devices to their corporate network, which in turn widened their attack surfaces.<sup>100</sup>

The changing face of cybercrime means that conventional defense practices are no longer as effective as they once were. An organization needs to focus on managing risk throughout the life cycle of its attack surface, with a focus on discovering an ever-changing attack surface, assessing risk, and then mitigating that risk. This enables the organization to ensure a secure working environment for its physical offices and be on the lookout for threats that can undermine its virtual workspaces as well. Modern-day distributed workforces do not access company resources the way they did on-premises, and the security needs of enterprises across the board have outgrown the password-based authentication processes that were built on binary login scenarios.<sup>101</sup>

New security paradigms like zero trust, which assumes that attackers exist both within and outside a system, are more suited to managing transformed attack surfaces. This is not achieved by any one product; zero-trust environments are governed by a philosophy of constant validation and monitoring, so the trustworthiness of every device and user is properly assessed before any device or user is granted permissions to any company resource. By practicing stringent access management policies that are grounded in zero trust, organizations can be better equipped to protect themselves against attackers attempting credential dumping to access their systems or steal their sensitive data.<sup>102</sup>

Investments in advanced security technologies should not be the sole focus of an organization's defense strategy. These also need to be paired with policies that can stand up to increasingly elaborate scams and lures that elevate overall risk. The social engineering tactics and human errors that have allowed attacks to make inroads year after year stress the crucial role that individual users play in a company's security profile. A workforce that has access to the resources it needs to stay alert and well-informed of potential threats can help cut off potential entry points for attackers.

Since the pandemic started, the need to secure at-home work setups has also put additional strain on cybersecurity teams, 61% of which are already understaffed,<sup>103</sup> as the shift to hybrid work arrangements has added to the complexity of enterprise networks and left security personnel scrambling to assist remote employees. Until this talent gap can be addressed, organizations should work alongside security vendors to automate processes and provide advanced analytics to lessen the load on their overworked cybersecurity workforce.<sup>104</sup>

Companies need security solutions that can assist in the discovery, assessment, and mitigation of persistent and emerging risks across the enterprise. It is important for enterprises to understand their growing attack surfaces to determine the security risks of their digital assets if they are to stay agile and adapt quickly to a changing threat landscape. Discovering the ways in which their attack surfaces are continuously changing and expanding will help enterprises gain the insights they need to accurately assess and apply the right security solutions to thwart threats.

However, this is beyond the capability of siloed tools or any single layer of protection. To manage the risk of evolving threats, decision-makers need to derive insights from high-quality data. As more organizations undergo digital transformations, they come up against the daunting task of breaking down data silos, which are usually borne of business units that are accustomed to collecting information separately and of siloed technology and legacy systems built over time as companies grow.<sup>105</sup>

Data gathered in silos from different products makes it a challenge for organizations to act on security incidents swiftly. Without a means to correlate all this information, security leaders are left to piece together different perspectives of an attack, often with varying levels of detail, from different technologies.<sup>106</sup> Having solutions in place that can assess, cross-check, and consolidate output from systems helps centralize data and results in a more detailed picture of an organization's risk posture.

On top of the complex threats bearing down on organizations, they also must keep pace with the rising number of data privacy and security compliance rules. However, only 4% of a compliance officer's time goes toward actually updating policies or implementing new measures to stay abreast of regulatory developments, whereas 26% of their time on the job is spent liaising with different teams within their organization.<sup>107</sup> A compliance team should be able to access accurate reporting of its company's IT infrastructure if it is to be more agile and productive, instead of having to interface with different departments to manually collect the information it needs.

Organizations can put themselves in a better position to map out their expanding attack surfaces by employing a unified cybersecurity platform that can monitor and address the different needs of their endpoint, email, network, and cloud environments simultaneously. In doing so, they can achieve transparency over the goings-on in their entire digital ecosystems, anticipate new threats, and plan countermeasures accordingly.

# The Threat Landscape in Brief

In 2021, Trend Micro Smart Protection Network, including Mobile App Reputation Service, IoT Reputation Service, and Smart Home Network, protected Trend Micro customers from more than 94 billion threats. Our year-on-year data shows an increase in blocked threats and reputation queries across most metrics compared to 2020, most notable of which is the substantial 382% spike in blocked malicious files.

# 94,289,585,240

Overall blocked threats in 2021

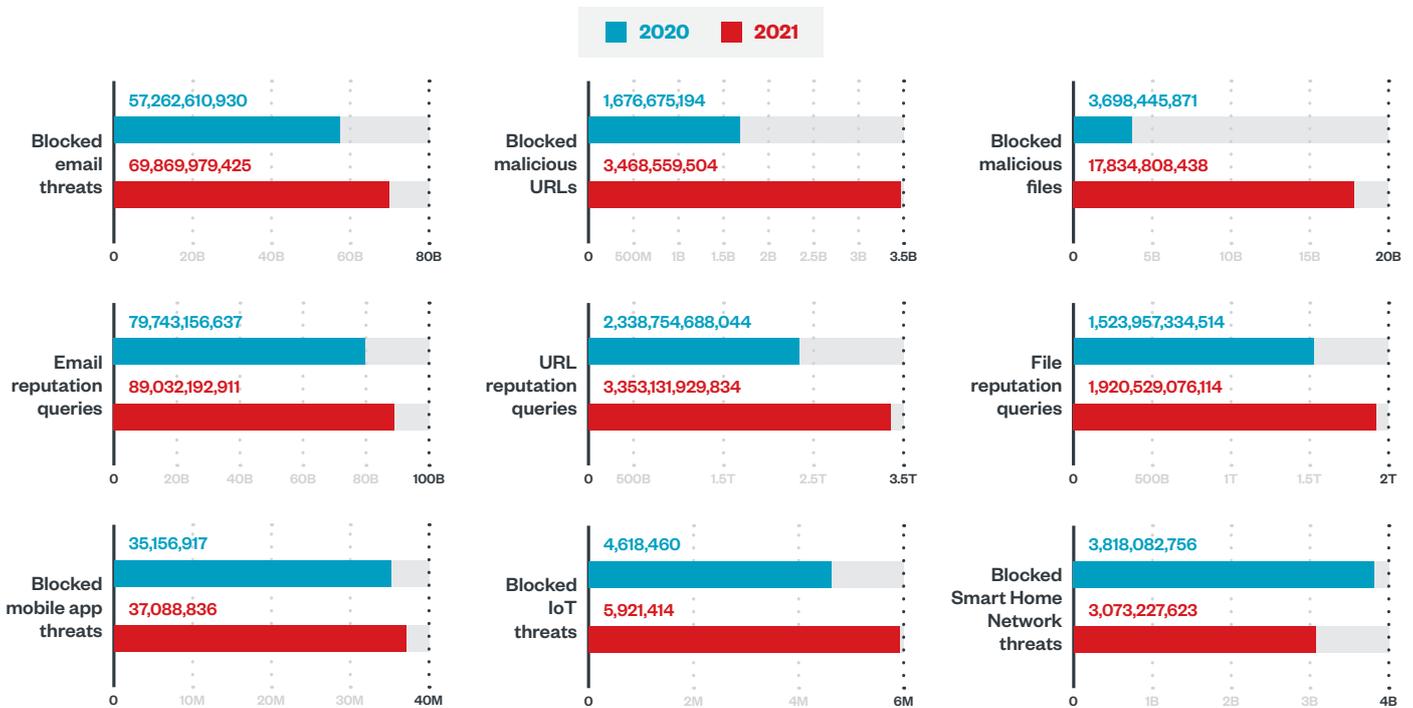


Figure 20. A comparison of the numbers of blocked email, URL, and file threats, of email, URL, and file reputation queries, and of blocked mobile app, IoT, and Smart Home Network threats in 2020 and 2021

Source: Trend Micro Smart Protection Network, including Mobile App Reputation Service, IoT Reputation Service, and Smart Home Network

The malware families that dominated the threat landscape of 2021 were led by cryptocurrency miners, followed closely by web shells and the trojan Ulise. WannaCry, which topped the list in 2020, continued to be the only ransomware among them. We detected 78 new ransomware families in 2021, a 39% year-on-year decrease.

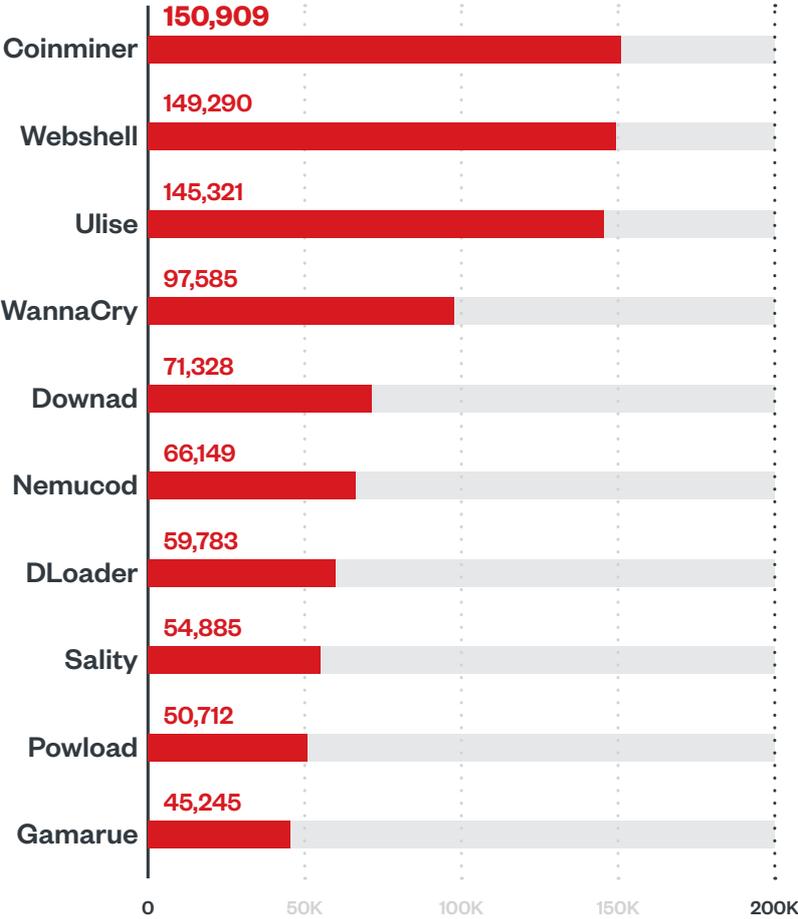


Figure 21. The top 10 malware families in terms of detections in 2021

Source: Trend Micro Smart Protection Network

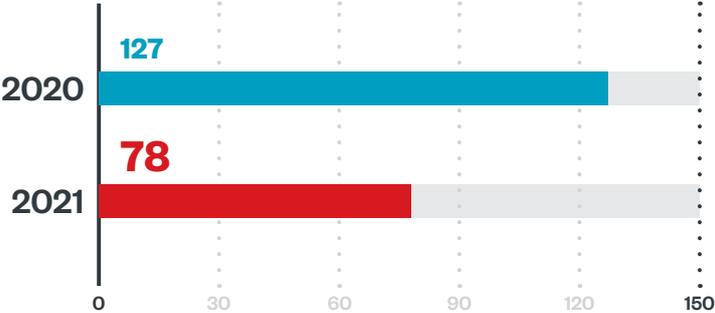


Figure 22. A comparison of the detections of new ransomware families in 2020 and 2021

Source: Trend Micro Smart Protection Network

Jan	Feb	Mar	Apr	May	Jun
Amjixius	IziCrypt	TrojanLock	BlackHole	Apostrius	DarkRadiation
SophCrypt	Cryng	VoidCrypt	Nitro	Venus	Babuk
SharpCrypter	HDLocker	HogLocker	AstroLocker	Hades	FakeRyuk
Cicada	SickRansom	OnCrypt	Hanta	QLocker	LegionLocker
Crysis.Tibggh	Lucifer	DadiCrypt	WhiteBlackCrypt	FiveHands	GonnaCrypt
BlueCrab	Butwo	Assist		Taihenchan	
Judge	Flamingo	HelpYou		Networm	
Mijnal	CNHCrypt	ThunderCrypt		NoCry	
Namaste		GangBang			
Gunshot		DarkWorld			
GaryTest					
Moloch					
Psixtin					

Jul	Aug	Sep	Oct	Nov	Dec
Grief	Hive	Ransomart	KCry	Polaris	Splinjok
GoFive	Cyrat	Diavol	LokiLocker	QuantumLocker	BlackCat
RedDot	CalCrypt	Sanwai	TimeCrypt		Rook
HKitty	AvosLocker	AtomSilo	HQCrypt		
Epsired	BlackMatter	MorrisCrypt	Colossus		
	LockFile				
	Rantu				
	ChaosBuilder				
	Chaos				

Table 3. The new ransomware families detected in 2021

Source: Trend Micro Smart Protection Network

In 2021, there was a 14% year-on-year increase in mobile device–related malicious samples. There was also an uptick in the number of blocked Android mobile apps, which were 5% more than in the previous year.

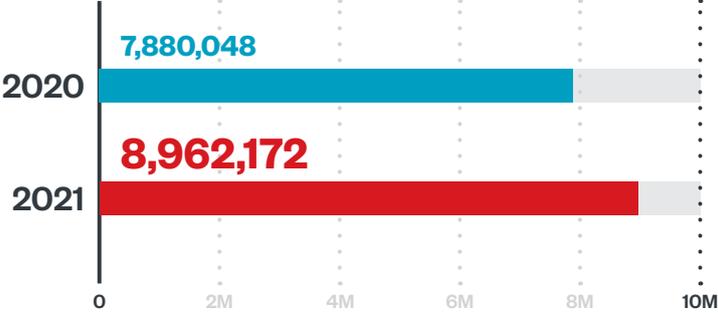


Figure 23. A comparison of the detections of mobile device–related malicious samples in 2020 and 2021

Source: Trend Micro Mobile App Reputation Service

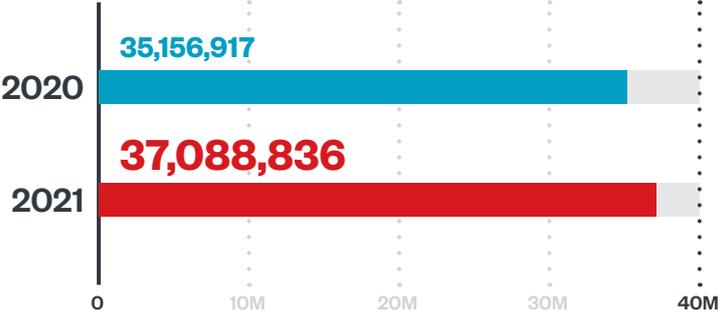


Figure 24. A comparison of the numbers of blocked malicious Android apps in 2020 and 2021

Source: Trend Micro Mobile App Reputation Service

# References

- 1 Trend Micro. (Dec. 20, 2021). *Trend Micro*. “Ransomware Spotlight: REvil.” Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil>.
- 2 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti.” Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 3 Trend Micro. (Nov. 10, 2021). *Trend Micro*. “Void Balaur and the Rise of the Cybermercenary Industry.” Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html](https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html).
- 4 Nick Dai, Ted Lee, and Vickie Su. (Dec. 14, 2021). *Trend Micro*. “Collecting In the Dark: Tropic Trooper Targets Transportation and Government.” Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html](https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html).
- 5 Mohamed Fahmy, Sherif Magdy and Abdelrhman Sharshar. (Nov. 19, 2021). *Trend Micro*. “Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains.” Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html](https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html).
- 6 Ranga Duraisamy, Ashish Verma, Miguel Carlo Ang, and Nitesh Surana. (Dec. 13, 2021). *Trend Micro*. “Patch Now: Apache Log4j Vulnerability Called Log4Shell Actively Exploited.” Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html](https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html).
- 7 Trend Micro. (Aug. 28, 2018). *Trend Micro*. “Trend Micro Report Reveals Criminals Increasingly Drawn To Low-Profile Attacks.” Accessed on Feb. 22, 2022, at <https://newsroom.trendmicro.com/2018-08-28-Trend-Micro-Report-Reveals-Criminals-Increasingly-Drawn-To-Low-Profile-Attacks>.
- 8 David Sancho. (Jan. 30, 2018). *Trend Micro*. “Digital Extortion: A Forward-looking View.” Accessed on Feb. 22, 2022, at [https://www.trendmicro.com/en\\_us/research/18/a/digital-extortion-forward-looking-view.html](https://www.trendmicro.com/en_us/research/18/a/digital-extortion-forward-looking-view.html).
- 9 Trend Micro. (June 8, 2021). *Trend Micro*. “Modern Ransomware’s Double Extortion Tactics and How to Protect Enterprises Against Them.” Accessed on Jan. 30, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransoms-doubles-extortion-tactics-and-how-to-protect-enterprises-against-them>.
- 10 Puja Mahendru. (May 17, 2021). *Sophos*. “The State of Ransomware in Healthcare 2021.” Accessed on Feb. 21, 2022, at <https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021>.
- 11 Stephane Duguin. (Nov. 8, 2021). *World Economic Forum*. “If healthcare doesn’t strengthen its cybersecurity, it could soon be in critical condition.” Accessed on Feb. 22, 2022, at <https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity>.
- 12 Trend Micro. (Nov. 23, 2021). *Trend Micro*. “Examining Erratic Modern Ransomware Activities.” Accessed on Jan. 30, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/examining-erratic-modern-ransomsactivities-ransomware-in-q3-2021>.
- 13 Abraham Camba, Catherine Loveria, Ryan Maglaque, and Buddy Tancio. (July 5, 2021). *Trend Micro*. “Tracking Cobalt Strike: A Trend Micro Vision One Investigation.” Accessed on March 11, 2022, at [https://www.trendmicro.com/en\\_us/research/21/g/tracking\\_cobalt\\_strike\\_a\\_vision\\_one\\_investigation.html](https://www.trendmicro.com/en_us/research/21/g/tracking_cobalt_strike_a_vision_one_investigation.html).
- 14 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti” Accessed on March 11, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 15 Trend Micro. (Nov. 4, 2020). *Trend Micro*. “Ryuk 2020: Distributing Ransomware via TrickBot and BazarLoader.” Accessed on March 11, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader>.
- 16 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti” Accessed on March 11, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 17 Trend Micro. (Nov. 4, 2020). *Trend Micro*. “Ryuk 2020: Distributing Ransomware via TrickBot and BazarLoader.” Accessed on March 11, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader>.
- 18 Trend Micro. (Sept. 7, 2016). *Trend Micro*. “Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises.” Accessed on Jan. 25, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises>.

- 19 Fyodor Yarochkin. (Oct. 5, 2021). *Trend Micro*. “Ransomware as a Service: Enabler of Widespread Attacks.” Accessed on Jan. 25, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks>.
- 20 Trend Micro. (Nov. 30, 2021). *Trend Micro*. “Investigating the Emerging Access-as-a-Service Market.” Accessed on Feb. 22, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market>.
- 21 Janus Agcaoili, Miguel Ang, Earle Earnshaw, Byron Gelera, and Nikko Tamaña. (June 15, 2021). *Trend Micro*. “Ransomware Double Extortion and Beyond: REvil, Clop, and Conti.” Accessed on Jan. 25, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti>.
- 22 Pierre Cadieux, Colin Grady, Jaeson Schultz, and Matt Valites. (April 30, 2019). *Cisco Talos*. “Sodinokibi ransomware exploits WebLogic Server vulnerability.” Accessed on Feb. 22, 2022, at <https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html>.
- 23 Michael Novinson. (April 23, 2021). *CRN*. “Apple Menaced After REvil Ransomware Attack Against Supplier.” Accessed on Feb. 18, 2022, at <https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier>.
- 24 NPR. (June 3, 2021). *NPR*. “REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says.” Accessed on Feb. 18, 2022, at <https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says>.
- 25 Brian Fung. (July 3, 2021). *CNN*. “New ransomware attack targets key IT vendor.” Accessed on Feb. 18, 2022, at <https://edition.cnn.com/2021/07/02/tech/ransomware-cybersecurity-attack-kaseya/index.html>.
- 26 Trend Micro. (Dec. 20, 2021). *Trend Micro*. “Ransomware Spotlight: REvil.” Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil>.
- 27 Trend Micro. (Dec. 20, 2021). *Trend Micro*. “Ransomware Spotlight: REvil.” Accessed on Feb. 22, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil>.
- 28 Alvin Nieto, Mark Vicente, RonJay Caragay, Miguel Carlo Ang, McJustine De Guzman, Emmanuel Evangelista, Divina Chua, and Marco Dela Vega. (March 19, 2021). *Trend Micro*. “Trend Micro Vision One: Tracking Conti Ransomware.” Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/research/21/c/vision-one-tracking-conti-ransomware.html](https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html).
- 29 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti.” Accessed on Feb. 22, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 30 Trend Micro. (Sept. 22, 2021). *Trend Micro*. “Cyberattacks from all Angles: 2021 Midyear Report.” Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html](https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html).
- 31 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti.” Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 32 Trend Micro. (Sept. 22, 2021). *Trend Micro*. “Cyber Risk Index (CRI): Trend Micro and the Ponemon Institute investigate cybersecurity gaps.” Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/security-intelligence/breaking-news/cyber-risk-index.html](https://www.trendmicro.com/en_us/security-intelligence/breaking-news/cyber-risk-index.html).
- 33 Jon Clay. (Sept. 14, 2021). *Trend Micro*. “1H’2021 Security Review Shows Active Cloud Attacks.” Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/research/21/i/1h-2021-security-review-shows-active-cloud-attacks.html](https://www.trendmicro.com/en_us/research/21/i/1h-2021-security-review-shows-active-cloud-attacks.html).
- 34 Trend Micro. (March 10, 2020). *Trend Micro*. “Trend Micro Cloud App Security Report 2019.” Accessed on Feb. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019>.
- 35 Trend Micro. (Sept. 22, 2021). *Trend Micro*. “Cyberattacks from all Angles: 2021 Midyear Report.” Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html](https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html).
- 36 Business Wire. (Jan. 13, 2022). *Business Wire*. “The Most Common Cloud Misconfigurations That Could Lead to Security Breaches.” Accessed on Jan. 30, 2022, at <https://www.businesswire.com/news/home/20220113005919/en/Cloud-Infrastructure-Spending-Increased-in-Third-Quarter-of-2021-with-Overall-Growth-Expected-for-2021-According-to-IDC>.
- 37 Trend Micro. (Oct. 25, 2021). *Trend Micro*. “The Most Common Cloud Misconfigurations That Could Lead to Security Breaches.” Accessed on Jan. 30, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches>.

- 38 Larry Dignan. (Dec. 22, 2021). *ZDNet*. "Top cloud providers: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players." Accessed on March 14, 2022, at <https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas>.
- 39 Aaron Ansari. (Nov. 30, 2021). *Trend Micro*. "What You Can Do to Mitigate Cloud Misconfigurations." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/what-can-you-do-to-mitigate-cloud-misconfigurations.html](https://www.trendmicro.com/en_us/research/21/k/what-can-you-do-to-mitigate-cloud-misconfigurations.html).
- 40 Trend Micro. (Nov. 9, 2021). *Trend Micro*. "Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html](https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html).
- 41 David Fiser and Alfredo Oliveira. (Nov. 11, 2021). *Trend Micro*. "TeamTNT Upgrades Arsenal, Refines Focus on Kubernetes and GPU Environments." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html](https://www.trendmicro.com/en_us/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html).
- 42 Magno Logan and David Fiser. (May 25, 2021). *Trend Micro*. "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html](https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html).
- 43 PurpleSec. (n.d.). *PurpleSec*. "2021 Cyber Security Statistics." Accessed on March 1, 2022, at <https://purplesec.us/resources/cyber-security-statistics>.
- 44 Cisco. (n.d.). *Cisco*. "2021 Cybersecurity threat trends: phishing, crypto top the list." Accessed on March 1, 2022, at <https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list>.
- 45 Trend Micro. (Dec. 7, 2021). *Trend Micro*. "Malware Awareness - EMOTET resurges with new detections." Accessed on Jan. 30, 2022, at <https://success.trendmicro.com/solution/1118391-malware-awareness-emetet-resurgence>.
- 46 Erin Johnson. (March 2, 2021). *Trend Micro*. "Emotet One Month After the Takedown." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/c/emotet-one-month-after-the-takedown.html](https://www.trendmicro.com/en_us/research/21/c/emotet-one-month-after-the-takedown.html).
- 47 Trend Micro. (Sept. 14, 2021). *Trend Micro*. "Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats." Accessed on Jan. 28, 2022, at <https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats>.
- 48 Ali Neil. (Nov. 23, 2021). *Dark Reading*. "Don't Help Cybercriminals Dash With Your Customers' Cash This Black Friday." Accessed on Feb. 21, 2022, at <https://www.darkreading.com/vulnerabilities-threats/don-t-help-cybercriminals-dash-with-your-customers-cash-this-black-friday>.
- 49 Business Wire. (Sept. 9, 2021). *Business Wire*. "Information Technology Global Market Report 2021: IT Services; Computer Hardware; Telecom; Software Products - Forecast to 2025 & 2030 - ResearchAndMarkets.com." Accessed on March 8, 2022, at <https://www.businesswire.com/news/home/20210909006056/en/Information-Technology-Global-Market-Report-2021-IT-Services-Computer-Hardware-Telecom-Software-Products---Forecast-to-2025-2030---ResearchAndMarkets.com>.
- 50 Sally Adam. (Aug. 31, 2021). *Sophos*. "The State of Ransomware in Retail 2021." Accessed on March 7, 2022, at <https://partnernews.sophos.com/en-us/2021/08/resources/the-state-of-ransomware-in-retail-2021>.
- 51 Katie Kuehner-Hebert. (Dec. 13, 2021). *Constructor Magazine*. "An increasing dependency on technology demands better asset protection." Accessed on March 8, 2022, at <https://www.constructormagazine.com/site-security>.
- 52 Trend Micro. (April 10, 2018). *Trend Micro*. "A Historical Overview of Proactive Incident Response Strategies and What They Mean to Enterprises." Accessed on Feb. 11, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/historical-overview-of-proactive-incident-response-strategies-and-what-they-mean-to-enterprises>.
- 53 Trend Micro. (Nov. 9, 2015). *Trend Micro*. "Understanding Targeted Attacks: Six Components of Targeted Attacks." Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attacks-six-components>.
- 54 Trend Micro. (Sept. 22, 2021). *Trend Micro*. "Cyberattacks from all Angles: 2021 Midyear Report." Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html](https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html).
- 55 Trend Micro. (Oct. 8, 2015). *Trend Micro*. "Understanding Targeted Attacks: The Impact of Targeted Attacks." Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-impact-of-targeted-attacks>.
- 56 Trend Micro. (Sept. 24, 2015). *Trend Micro*. "Understanding Targeted Attacks: What is a Targeted Attack?" Accessed on Jan. 28, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack>.

- 57 Trend Micro. (Nov. 10, 2021). *Trend Micro*. "Void Balaur and the Rise of the Cybermercenary Industry." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html](https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html).
- 58 Trend Micro. (Nov. 10, 2021). *Trend Micro*. "The far-reaching attacks of the Void Balaur cybermercenary group." Accessed on Jan. 29, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group>.
- 59 Nick Dai, Ted Lee, and Vickie Su. (Dec. 14, 2021). *Trend Micro*. "Collecting In the Dark: Tropic Trooper Targets Transportation and Government." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html](https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html).
- 60 Ian Kenefick. (Nov. 23, 2021). *Trend Micro*. "BazarLoader Adds Compromised Installers, ISO to Arrival and Delivery Vectors." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html](https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html).
- 61 Raphael Centeno, Don Ovid Ladores, Lala Manly, Junestherry Salvador, and Franklynn Uy. (April 12, 2021). *Trend Micro*. "A Spike in BazarCall and IcedID Activity Detected in March." Accessed on Feb. 18, 2022, at [https://www.trendmicro.com/en\\_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html](https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html).
- 62 Homeland Security. (November 2010). *Homeland Security*. "Sector Open Source Digest." Accessed on Feb. 21, 2022, at [https://www.fbiic.gov/public/2010/dec/FS\\_Nov\\_2010\\_PDF.PDF](https://www.fbiic.gov/public/2010/dec/FS_Nov_2010_PDF.PDF).
- 63 Ian Kenefick. (Nov. 13, 2021). *Trend Micro*. "QAKBOT Loader Returns With New Techniques and Tools." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html](https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html).
- 64 Christopher Boyton. (Nov. 5, 2021). *Trend Micro*. "A Review and Analysis of 2021 Buer Loader Campaigns." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html](https://www.trendmicro.com/en_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html).
- 65 Aliakbar Zahravi and William Gamazo Sanchez. (Sept. 20, 2021). *Fortinet*. "Water Basilisk Uses New HCRypt Variant to Flood Victims with RAT Payloads." Accessed on Jan. 27, 2022, at [https://www.trendmicro.com/en\\_us/research/21/i/Water-Basilisk-Uses-New-HCRypt-Variant-to-Flood-Victims-with-RAT-Payloads.html](https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCRypt-Variant-to-Flood-Victims-with-RAT-Payloads.html).
- 66 Aliakbar Zahravi and William Gamazo Sanchez. (Sept. 20, 2021). *Trend Micro*. "Water Basilisk Uses New HCRypt Variant to Flood Victims with RAT Payloads." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/i/Water-Basilisk-Uses-New-HCRypt-Variant-to-Flood-Victims-with-RAT-Payloads.html](https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCRypt-Variant-to-Flood-Victims-with-RAT-Payloads.html).
- 67 Kaseya. (Feb. 22, 2022). *Kaseya*. "Patch Management Policy Features, Benefits and Best Practices." Accessed on Feb. 22, 2022, at <https://www.kaseya.com/blog/2022/02/22/patch-management-policy>.
- 68 Trend Micro. (April 7, 2021). *Trend Micro*. "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on Feb. 21, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>.
- 69 Trend Micro. (July 13, 2021). *Trend Micro*. "Nearly a Quarter of Exploits Sold on Cybercriminal Underground Are More Than Three Years Old." Accessed on Jan. 29, 2022, at <https://newsroom.trendmicro.com/2021-07-13-Nearly-a-Quarter-of-Exploits-Sold-on-Cybercriminal-Underground-Are-More-Than-Three-Years-Old>.
- 70 Trend Micro. (July 13, 2021). *Trend Micro*. "Trends and shifts in the underground N-day exploit market." Accessed on Jan. 29, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market>.
- 71 Microsoft Security Response Center. (Aug. 13, 2019). *Microsoft Security Response Center*. "Remote Desktop Protocol Server Information Disclosure Vulnerability: CVE-2019-1225." Accessed on Jan. 28, 2022, at <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2019-1225>.
- 72 CVE report. (Sept. 2, 2017). *CVE.report*. "CVE-2017-14100." Accessed on Jan. 29, 2022, at <https://cve.report/CVE-2017-14100>.
- 73 Ranga Duraisamy, Ashish Verma, Miguel Carlo Ang, and Nitesh Surana. (Dec. 13, 2021). *Trend Micro*. "Patch Now: Apache Log4j Vulnerability Called Log4Shell Actively Exploited." Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html](https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html).
- 74 Trend Micro. (Dec. 22, 2021). *Trend Micro*. "The Log4j story, and how it has impacted our customers." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21/l/the-log4j-story-and-how-it-has-impacted-our-customers.html](https://www.trendmicro.com/en_us/research/21/l/the-log4j-story-and-how-it-has-impacted-our-customers.html).

- 75 Ranga Duraisamy, Ashish Verma, Miguel Carlo Ang, and Nitesh Surana. (Dec. 13, 2021). *Trend Micro*. "Patch Now: Apache Log4j Vulnerability Called Log4Shell Actively Exploited." Accessed on Jan. 29, 2022, at [https://www.trendmicro.com/en\\_us/research/21//patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html](https://www.trendmicro.com/en_us/research/21//patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html).
- 76 Trend Micro. (Dec. 22, 2021). *Trend Micro*. "The Log4j story, and how it has impacted our customers." Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/research/21//the-log4j-story-and-how-it-has-impacted-our-customers.html](https://www.trendmicro.com/en_us/research/21//the-log4j-story-and-how-it-has-impacted-our-customers.html).
- 77 Lisa Vaas. (Nov. 22, 2021). *ThreatPost*. "Attackers Hijack Email Threads Using ProxyLogon/ProxyShell Flaws." Accessed on Feb. 21, 2022, at <https://threatpost.com/attackers-hijack-email-threads-proxylogon-proxyshell/176496>.
- 78 Arianne Dela Cruz, Cris Tomboc, Jayson Chong, Nikki Madayag, and Sean Torre. (May 6, 2021). *Trend Micro*. "Proxylogon: A Coinminer, a Ransomware, and a Botnet Join the Party." Accessed on Feb. 21, 2022, at [https://www.trendmicro.com/en\\_us/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html](https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html).
- 79 Edmund Brumaghin, Mariano Graziano, and Nick Mavis. (Oct. 26, 2021). *Cisco Talos*. "Squirrelwaffle Leverages malspam to deliver Qakbot, Cobalt Strike." Accessed on Feb. 22, 2021, at <https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html>.
- 80 Jon Clay. (Dec. 13, 2021). *Trend Micro*. "This Week in Security News - December 3, 2021." Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/research/21//this-week-in-security-news-dec-3-2021.html](https://www.trendmicro.com/en_us/research/21//this-week-in-security-news-dec-3-2021.html).
- 81 Mohamed Fahmy, Sherif Magdy and Abdelrhman Sharshar. (Nov. 19, 2021). *Trend Micro*. "Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains." Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html](https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html).
- 82 Melanie Tafelski. (Nov. 9, 2021). *Trend Micro*. "Cybersecurity Trends from the Global Pandemic." Accessed on Jan. 28, 2022, at [https://www.trendmicro.com/en\\_us/devops/21/k/cybersecurity-trends-from-the-global-pandemic.html](https://www.trendmicro.com/en_us/devops/21/k/cybersecurity-trends-from-the-global-pandemic.html).
- 83 Atlas VPN. (n.d.). *Atlas VPN*. "Global VPN Adoption Index." Accessed on Jan. 28, 2022, at <https://atlasvpn.com/vpn-adoption-index>.
- 84 Fortinet. (Aug. 28, 2019). *Fortinet*. "FortiOS and SSL Vulnerabilities." Accessed on Jan. 27, 2022, at <https://www.fortinet.com/blog/psirt-blogs/fortios-ssl-vulnerability>.
- 85 National Vulnerability Database. (June 4, 2019). *National Vulnerability Database*. "CVE-2018-13379 Detail." Accessed on Jan. 27, 2022, at <https://nvd.nist.gov/vuln/detail/CVE-2018-13379>.
- 86 Trend Micro. (Jan. 26, 2021). *Trend Micro*. "Examining A Sodinokibi Attack." Accessed on Jan. 27, 2022, at [https://www.trendmicro.com/en\\_us/research/21/a/sodinokibi-ransomware.html](https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html).
- 87 Trend Micro. (Dec. 1, 2021). *Trend Micro*. "Ransomware Spotlight: Conti." Accessed on Feb. 21, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 88 Trend Micro. (Dec. 16, 2021). *Trend Micro*. "Addressing Cloud-Related Threats to the IoT Addressing Cloud-Related Threats to the IoT." Accessed on Jan. 30, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/addressing-cloud-related-threats-to-the-iot>.
- 89 Trend Micro. (n.d.). *Trend Micro*. "How to Reduce the Risk of Phishing and Ransomware: Osterman Research White Paper." Accessed on Jan. 30, 2022, at <https://resources.trendmicro.com/Osterman-Email-Security-WP.html>.
- 90 Zero Day Initiative. (Nov. 1, 2021). *Zero Day Initiative*. "Pwn2Own Austin 2021 - Schedule and Live Results." Accessed on March 1, 2022, at <https://www.zerodayinitiative.com/blog/2021/11/1/pwn2ownaustin>.
- 91 Eduard Kovacs. (Nov. 5, 2021). *Security Week*. "Device Exploits Earn Hackers Over \$1 Million at Pwn2Own Austin 2021." Accessed on March 1, 2022, at <https://www.securityweek.com/device-exploits-earn-hackers-over-1-million-pwn2own-austin-2021>.
- 92 Jon Clay. (July 21, 2021). *Trend Micro*. "Reduce Instances of Covid-19 Phishing Email Attacks." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/g/reduce-instances-of-covid-19-phishing-email-attacks.html](https://www.trendmicro.com/en_us/research/21/g/reduce-instances-of-covid-19-phishing-email-attacks.html).
- 93 Paul Pajares. (July 8, 2021). *Trend Micro*. "Threats Ride on the Covid-19 Vaccination Wave." Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html](https://www.trendmicro.com/en_us/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html).
- 94 US Department of Health and Human Services. (Feb. 3, 2022). *US Department of Health and Human Services*. "Lessons Learned from the HSE Cyber Attack." Accessed on March 7, 2022, at <https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf>.

- 95 IntSights. (n.d.). *IntSights*. "Building Immunity: The 2021 Healthcare and Pharmaceutical Industry Cyber Threat Landscape Report." Accessed on March 7, 2022, at <https://wow.intsights.com/rs/071-ZWD-900/images/Building%20Immunity-Healthcare-Pharma%20Report-2021.pdf>.
- 96 Nic Newman. (n.d.). *Reuters Institute for the Study of Journalism*. "2021 Digital News Report: Executive summary and key findings of the 2021 report." Accessed on Feb. 11, 2022, at <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/dnr-executive-summary>.
- 97 Felix Richter. (Feb. 4, 2021). *World Economic Forum*. "COVID-19 has caused a huge amount of lost working hours." Accessed on Feb. 11, 2022, at <https://www.weforum.org/agenda/2021/02/covid-employment-global-job-loss>.
- 98 International Labour Organization. (Oct. 27, 2021). *International Labour Organization*. "ILO: Employment impact of the pandemic worse than expected." Accessed on Feb. 11, 2022, at [https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS\\_824098/lang--en/index.htm](https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_824098/lang--en/index.htm).
- 99 World Economic Forum. (Jan. 18, 2021). *World Economic Forum*. "Closing the Cyber Gap: Business and Security Leaders at Crossroads as Cybercrime Spikes." Accessed on Jan. 30, 2022, at <https://www.weforum.org/press/2022/01/closing-the-cyber-gap-business-and-security-leaders-at-crossroads-as-cybercrime-spikes>.
- 100 Trend Micro. (Sept. 28, 2021). *Trend Micro*. "IoT and Ransomware: A Recipe for Disruption." Accessed on March 1, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-and-ransomware-a-recipe-for-disruption>.
- 101 Rajat Bhargava. (Feb. 9, 2021). *Forbes*. "Why The 'New Normal' Requires Zero Trust." Accessed on Jan. 30, 2022, at <https://www.forbes.com/sites/forbestechcouncil/2021/02/09/why-the-new-normal-requires-zero-trust>.
- 102 Trend Micro. (Feb. 9, 2021). *Trend Micro*. "What Is Zero Trust and Why Does It Matter?" Accessed on Jan. 30, 2022, at [https://www.trendmicro.com/en\\_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html](https://www.trendmicro.com/en_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html).
- 103 Security Magazine. (May 4, 2021). *Security Magazine*. "Cybersecurity workforce minimally impacted by pandemic, but still grappling with persistent hiring challenges." Accessed on Feb. 11, 2022, at <https://www.securitymagazine.com/articles/95123-cybersecurity-workforce-minimally-impacted-by-pandemic-but-still-grappling-with-persistent-hiring-challenges>.
- 104 Danny Palmer. (Aug. 2, 2021). *ZDNet*. "The cybersecurity jobs crisis is getting worse, and companies are making basic mistakes with hiring." Accessed on Feb. 11, 2022, at <https://www.zdnet.com/article/the-cybersecurity-jobs-crisis-is-getting-worse-and-companies-are-making-basic-mistakes-with-hiring>.
- 105 Michael Paladino. (April 16, 2021). *Forbes*. "Breaking Down Data Silos Takes A Cultural Shift." Accessed on Feb. 11, 2022, at <https://www.forbes.com/sites/forbestechcouncil/2021/04/16/breaking-down-data-silos-takes-a-cultural-shift>.
- 106 Trend Micro. (Oct. 29, 2020). *Trend Micro*. "The Real Frontiers for 2021 in XDR." Accessed on Feb. 11, 2022, at [https://www.trendmicro.com/tr\\_tr/ciso/20/j/the-real-frontiers-for-2021-in-xdr.html](https://www.trendmicro.com/tr_tr/ciso/20/j/the-real-frontiers-for-2021-in-xdr.html).
- 107 Scott Ikeda. (Feb. 17, 2021). *CPO Magazine*. "Balancing the Challenges: Fear and Cost in Compliance With Regulations." Accessed on Feb. 11, 2022, at <https://www.cpomagazine.com/cyber-security/balancing-the-challenges-fear-and-cost-in-compliance-with-regulations>.



## 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](http://www.trendmicro.com)



| research 