Keeping a Close Watch

Trend Micro Specialized Cybersecurity Report for Latin America and the Caribbean

TREND MICRO™

In partnership with

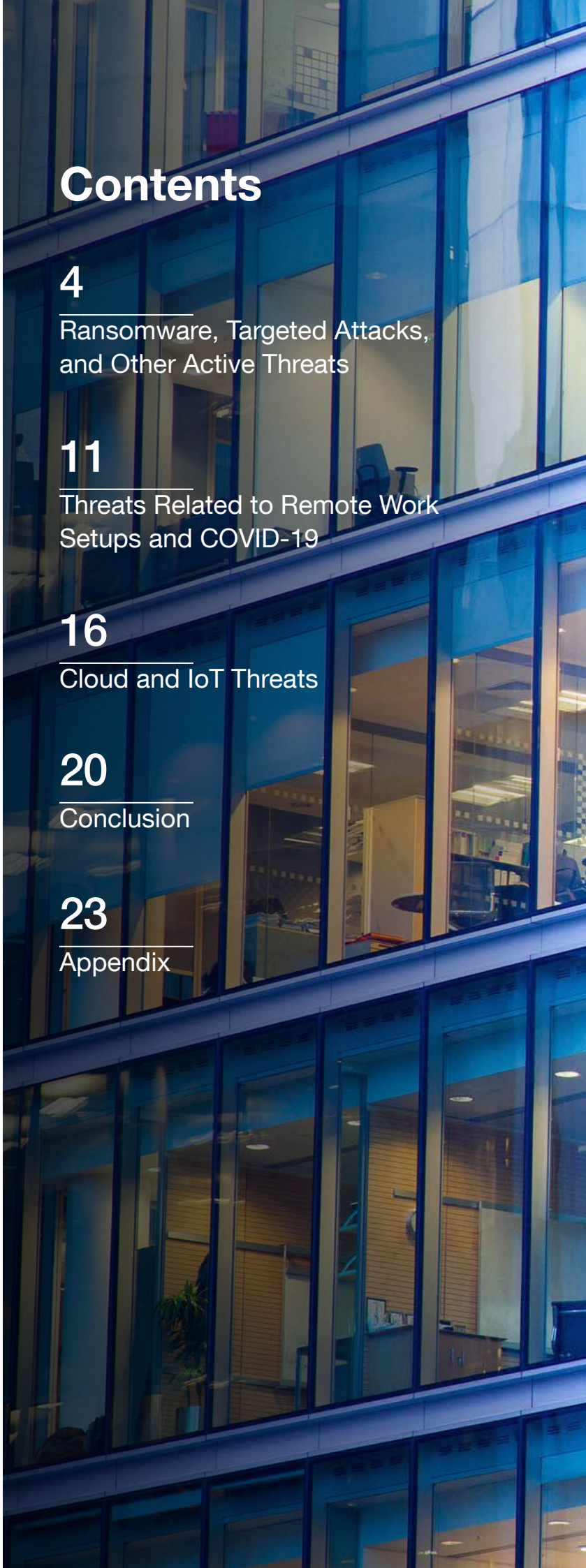
OAS More rights for more people

Written and published by

Trend Micro Research

Stock image used under license from Shutterstock.com

Contents



The Cybersecurity Landscape of Latin America and the Caribbean

In September 2021, Trend Micro released its 2021 midyear cybersecurity report, titled "Attacks From All Angles."[1] That report, aimed at helping organizations bolster their protection, gave a comprehensive view of the cybersecurity challenges that organizations and users around the world had been facing.

While that report took a global perspective of the cybersecurity landscape, a closer look can lend a more detailed view, as what happens when one peers through a microscope. For this reason, Trend Micro, in collaboration with the Cybersecurity Program of the Organization of American States Inter-American Committee against Terrorism (OAS/CICTE), examined the threat landscape data concerning member states of the OAS and compared the regional findings of the Americas with the identified global trends from the 2021 midyear cybersecurity report. This data was supplemented with responses to a survey distributed through CSIRTAmericas, a network of governmental computer security incident response teams (CSIRTs) of the member states of the OAS, in which data was collected from 22 respondents from members of the network across the region and other public officials.

The objective of the threat landscape regional analysis is to understand how entities from the region view ransomware, targeted attacks, scams, remote work setups, and the adoption of relatively new technologies as cybersecurity concerns, thereby adding valuable insights and a comprehensive perspective of common and differing threats across the region. (The details of the methodology and the full disclaimer on the data gathering process can be found in the Appendix section of this report.)

Our pertinent findings include the following:

- Online threats such as ransomware, targeted attacks, and scams were a top security issue, which is not surprising since these threats had been running rampant in 2021, particularly affecting high-profile organizations in critical industries.
- Adjustments due to COVID-19 and remote work setups were a pressing concern when the pandemic began. Although most companies had already adjusted more or less accordingly, some were still aiming to have more defined security measures.
- The COVID-19 pandemic catalyzed a more widespread adoption of new technologies, such as the cloud and the internet of things (IoT) or industrial internet of things (IIoT), but misconfiguration and the lack of user education for these technologies inadvertently left organizations vulnerable to data breaches, malware, and other cyberattacks.
- In terms of comparing the OAS member states data with global trends, some findings were similar. On the other hand, for some threats, other findings diverged, such as the most detected types or the most affected industries.

Throughout 2021, cyberthreats were coming in from all angles, necessitating connected protection that would provide protection across email, network, web, endpoints, and all other layers. The good news is, through a better understanding of Trend Micro's detections of these threats primarily through the Trend Micro™ Smart Protection Network™ infrastructure, entities can protect their systems through actionable steps, starting from the simple ones that could go a long way.

This report was prepared and published by Trend Micro in collaboration with the Cybersecurity Program of OAS/CICTE. The opinion and content expressed in this document are those of the authors, are presented exclusively for informational purposes, and do not represent the official opinion or position of the OAS, its General Secretariat, or its member states.

Ransomware, Targeted Attacks, and Other Active Threats

Ransomware, targeted attacks, and scams continued to proliferate and evolve, involving more advanced tools and going after bigger targets.

The survey asked the respondents to rank cyberthreats such as ransomware, targeted attacks, and scams based on the perceived level of importance and frequency with which their organizations faced such cybersecurity challenges. An overwhelming majority answered "a great deal," while the second most frequent answer was "a lot." As a result, cyberthreats including ransomware, targeted attacks, and scams were the highest-rated overall in the survey.

Figure 1. How online threats (ransomware, targeted attacks, scams, etc.) were ranked as a security challenge by the survey respondents

Ransomware

At this point, ransomware needs no introduction, especially with massive ransomware attacks making headlines in 2021. Worries over the threat's effect were reflected in the survey. "The constant increase in the number of ransomware attacks, as well as the high impact they cause on their victims," one of the respondents said, "is one of the fundamental concerns of every institution and organization." And in many cases, the security measures entities had were not able to keep up with the intensity of modern campaigns.

These worries were exacerbated by the rise in high-profile modern ransomware attacks,[2] as seen in major global events such as those launched by Sodinokibi (aka REvil)[3] and DarkSide on the meat processor JBS[4] and the fuel supplier Colonial Pipeline,[5] respectively. Both of these ransomware families were among the most detected in the first half of 2021.

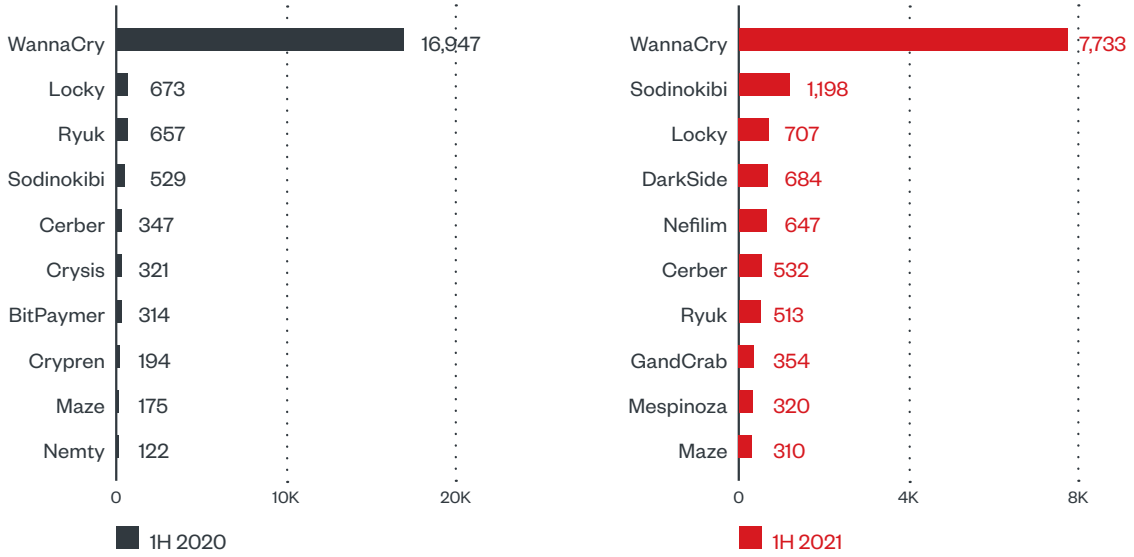


Figure 2. The top 10 ransomware families across OAS member states in terms of file-only counts of ransomware family detections in the first half of 2020 and in the first half of 2021

WannaCry was still the most detected ransomware family, maintaining the reign documented in Trend Micro's roundup reports from recent years. It remained as such even though it is a relatively old family considered as premodern ransomware and the malicious actors behind it had not been actively initiating attacks. The persistence of this family shows how a network worm can thrive if devices are not patched properly, if at all. However, similar to the findings of the 2021 midyear cybersecurity report, across OAS member states, WannaCry detections decreased by more than half from the first half of 2020 to the first half of 2021.

Beyond WannaCry, one of the most notable findings in the top 10 was the rise of detections of modern ransomware, which uses tools and techniques reminiscent of advanced persistent threats (APTs) for more advanced means of infiltration.

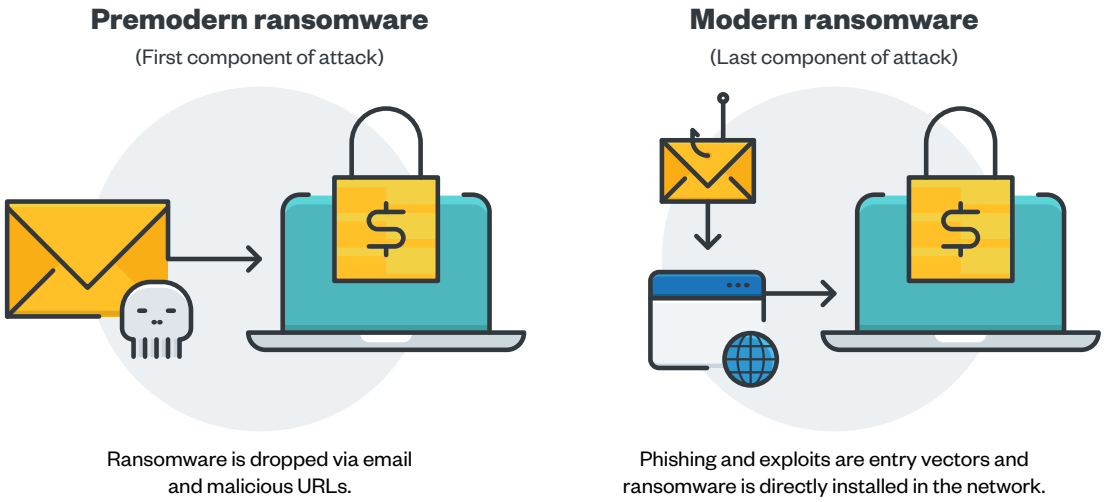


Figure 3. The differences between premodern and modern ransomware

Among the modern ransomware families, Sodinokibi roughly doubled its detections from the first half of 2020 and became the second most detected ransomware across OAS member states in the first half of 2021. Meanwhile, DarkSide entered the top 10. This rise in rankings was also seen in global trends, where Sodinokibi rose a rank higher in 2021 than in 2020, with 2,119 detections, and DarkSide infiltrated the top 10, with 830. This correlation might be attributed to the fact that over half of the total global detections consisted of detections in the Americas. Out of the 2,119 global detections of Sodinokibi, 1,119 were in the Americas, and out of the 830 global detections of DarkSide, 684 were in the Americas.

Besides the sophistication of modern ransomware attacks, what is also alarming is that attackers naturally go after critical industries, including government. Despite this, some of the survey respondents were not confident about how security measures were being implemented to combat these rapidly advancing campaigns.

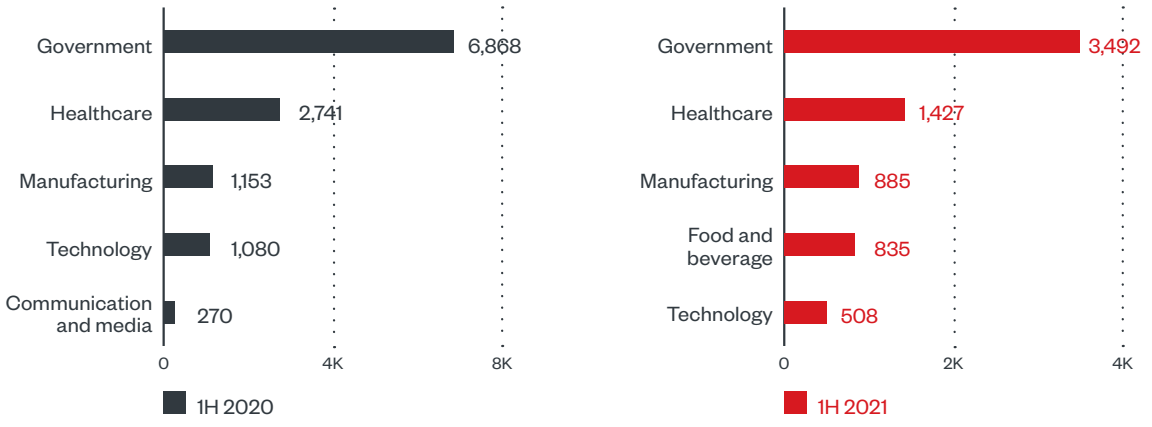


Figure 4. The top five industries affected by ransomware attacks across OAS member states in the first half of 2020 and in the first half of 2021

The top five industries affected by ransomware attacks across OAS member states in the first half of 2021 were mostly the same as those in the first half of 2020, with government remaining to be the industry with the most ransomware detections. However, these findings were slightly different from the detections across all regions in the 2021 midyear cybersecurity report, where banking, despite not being in the top five in the first half of 2020, overtook government as the industry with the most detections. The global top five were banking, government, manufacturing, healthcare, and food and beverage.

Targeted Attacks

Based on global trends, most targeted cyberthreat campaigns were aimed at entities in Asia. However, some global cyberattacks were not necessarily location-specific and instead went after certain platforms that were being used across borders. These included the attacks launched by the notorious TeamTNT group to target cloud vendor credentials[6] and Kubernetes clusters.[7] (We elaborate on these attacks in the cloud and IoT section of this report.) We also observed attacks wielding the PlugX loader,[8] a remote access tool (RAT), against entities in government and other industries.

To protect their systems against such targeted attacks, entities need to build robust and proactive cybersecurity measures. But this is easier said than done, as budgetary issues for acquiring skilled personnel and cybersecurity tools can be a roadblock for strengthening cybersecurity at the industry level. This was reflected in survey responses not only concerning online threats but also with regard to remote work adjustments and adoption of new technologies. An important factor was raised by a respondent who highlighted the possibility that such cyberattacks might be underreported, lending a false sense of cybersecurity to an enterprise.

Malware

For malware in general, the most detected family across OAS member states in the first half of 2021 was Webshell, which was the third most detected in the 2021 midyear cybersecurity report (with cryptocurrency miners being the first). Formerly at the top in terms of detections across OAS member states in the first half of 2020, WannaCry slid down to fifth place in the first half of 2021.

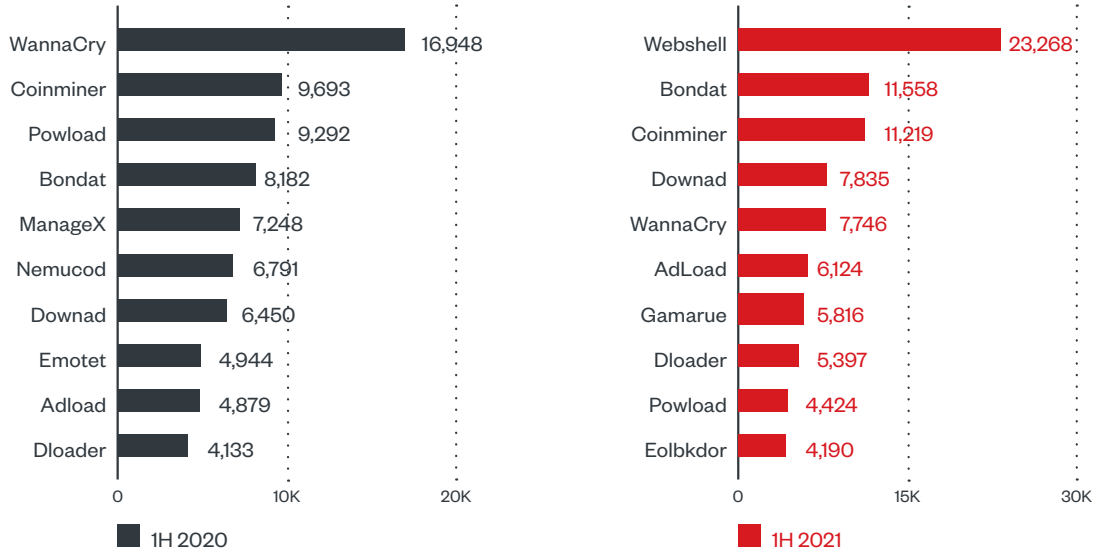


Figure 5. The top 10 malware families across OAS member states in terms of detections in the first half of 2020 and in the first half of 2021

The United States had the most malware detections, at over 163 million, while Brazil and Canada each had over 20 million detections.

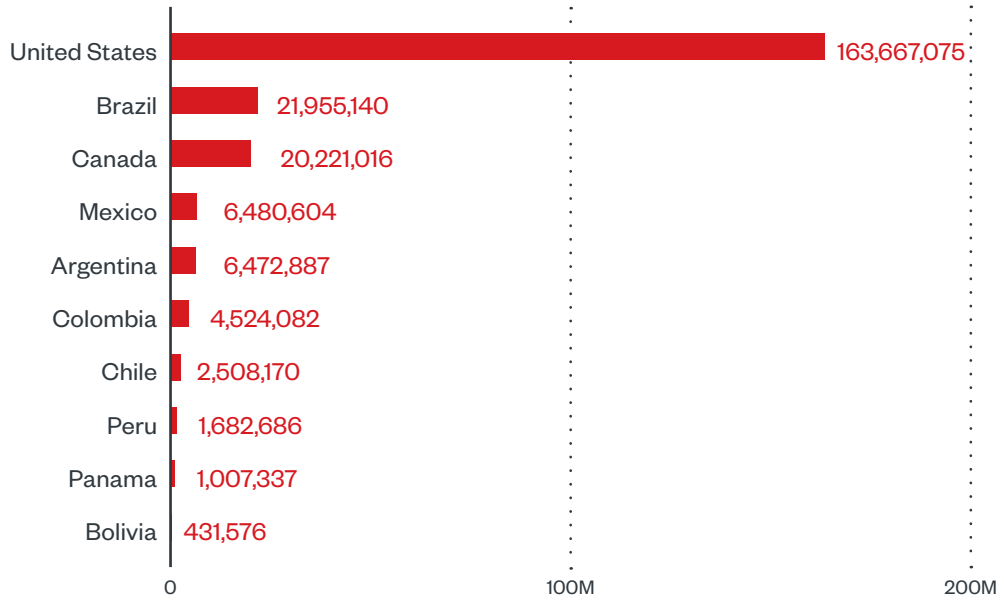


Figure 6. The top 10 OAS member states in terms of malware detections in the first half of 2021

Online Threats

Email threats and malicious URLs, which could be used as entry points for ransomware, targeted attacks, and scams, were persistent across OAS member states as well as around the world. Like those in terms of malware detections, the top OAS member states in terms of detections of email threats and malicious URLs included the United States, Brazil, and Canada, with detections in the United States vastly exceeding those in the other OAS member states.

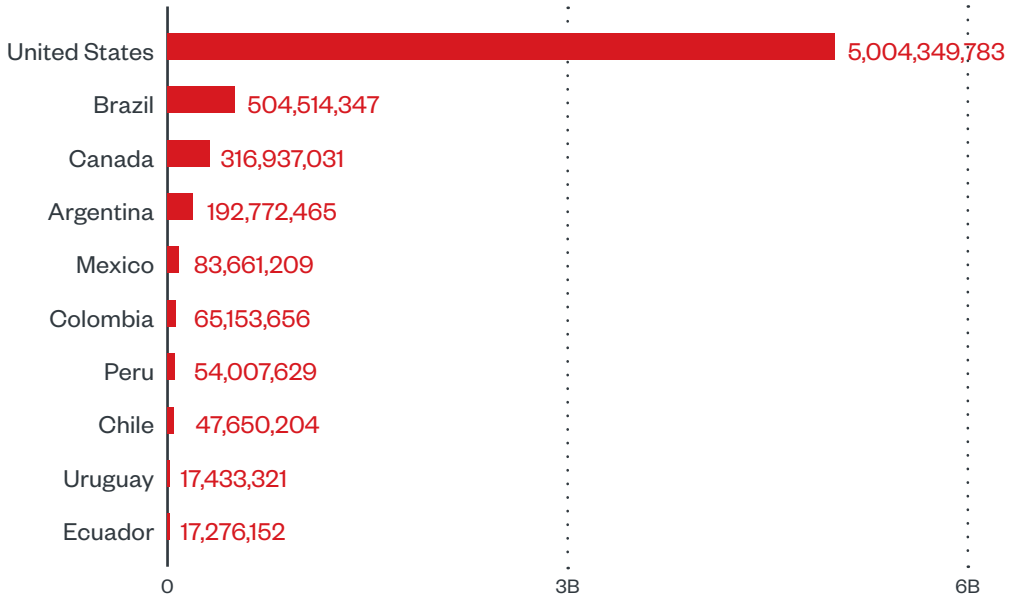


Figure 7. The top 10 OAS member states in terms of email threat detections in the first half of 2021

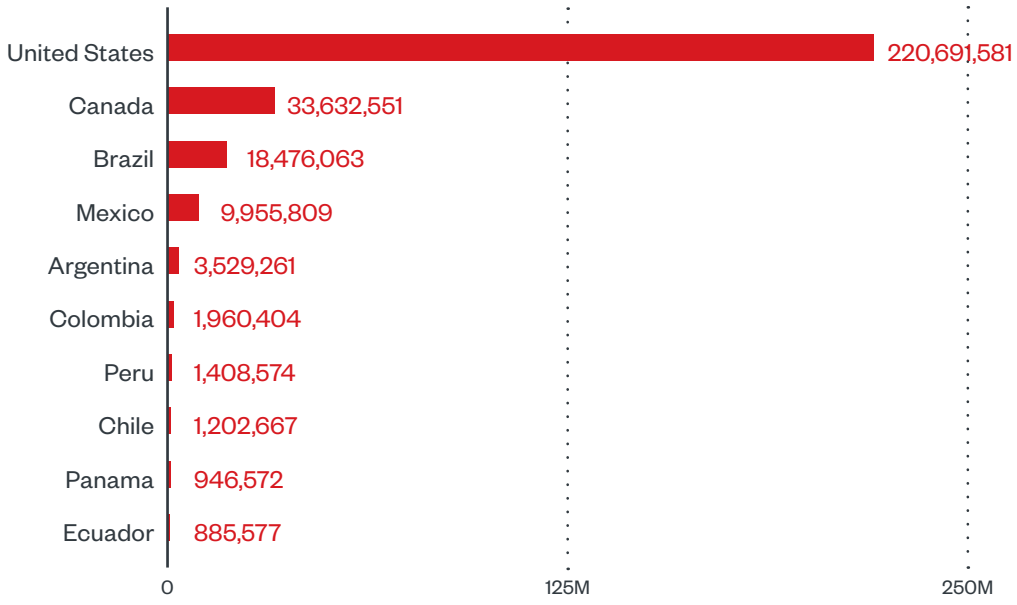


Figure 8. The top 10 OAS member states in terms of malicious URL detections in the first half of 2021

In avoiding these threats, ensuring that employees follow basic cybersecurity best practices can go a long way. This much was reflected in a significant number of survey responses that mentioned the necessity of launching campaigns for raising security awareness at the grassroots level. A respondent recognized how people with limited technical knowledge could be vulnerable and consequently compromise institutional security. Indeed, even simple mistakes by users — for example, those cited in the survey answers, such as bad internet browsing practices and lack of knowledge on how ransomware could get into a system — could negatively affect an entire organization.

Threats Related to Remote Work Setups and COVID-19

The COVID-19 pandemic posed certain cybersecurity challenges as it ushered in widespread adoption of remote work or work-from-home (WFH) setups, where employees work from their places of residence, rather than in their offices, using company-linked computers and other devices connected to their home networks. The survey also looked into how entities in the Americas region were adapting to the abrupt shift to remote work setups, in terms of both operations and securing systems.

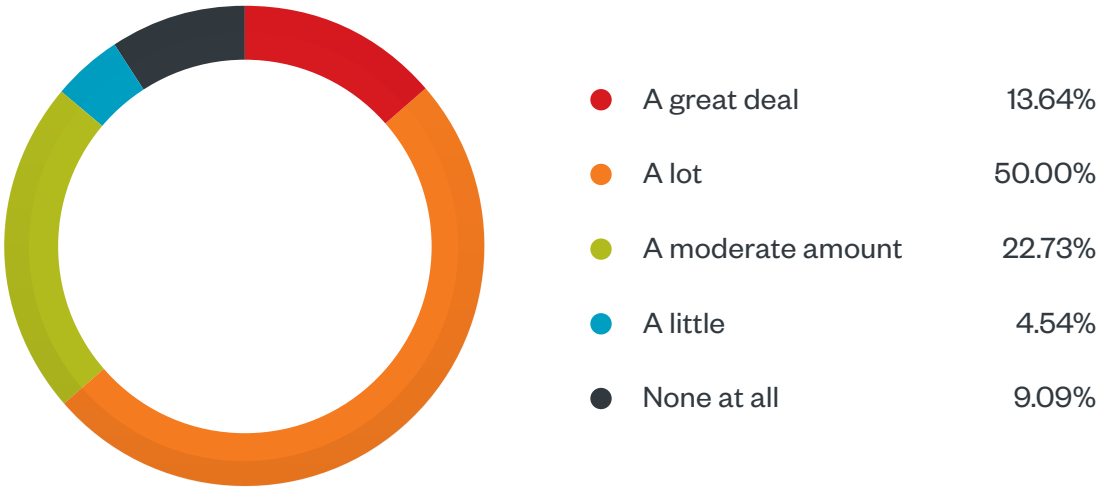


Figure 9. How adjusting to secure remote work setups due to COVID-19 (in terms of both operations and securing systems) was ranked as a security challenge by the survey respondents

To the survey question that asked respondents to rank how much they viewed remote work-related adjustments as a challenge, the majority of the respondents answered "a lot," the second highest ranking in the survey. This was followed by "a moderate amount," and then by "a great deal."

While the matter was still considered a top concern by the respondents, it was not rated as highly as online threats. Perhaps this could be attributed to the fact that it had been roughly 2 years since the COVID-19 pandemic began, during which many organizations might have adjusted or gotten used to remote work setups.

WFH Threats

While remote work–related issues might not have been perceived as a major concern by survey respondents, a study of the past year shows the security gaps in WFH setups. As noted in the 2021 midyear cybersecurity report, issues related to WFH setups continued to beset organizations. Since remote work systems brought on heavier reliance on online and mobile systems, this shift was taken advantage of by malicious actors through scams and malware that involved these systems.

One of the biggest challenges with regard to this matter, according to the survey, was the lack of thorough preparation for the transition. Since the pandemic urged an almost overnight shift to remote work, many entities were left with mere days to prepare. "Organizations have had to take a great leap toward remote work while not always being sufficiently prepared in processes or security controls, representing a high risk in terms of cybersecurity," a respondent said. And, as noted by the same respondent, with such a limited time, ensuring the continuity of operations might have been prioritized over securing systems. This was further illustrated by a survey answer that mentioned how the respondent's organization opted to prioritize ease of communication without thoroughly evaluating if the tools they were using were secure.

These might have resulted from several factors mentioned in the responses, such as the lack of previously established security measures, the need for antimalware tools and secure means for communication and access, and internal matters, including the challenge of raising awareness among high-level members of an organization of the importance of cybersecurity tools and cybersecurity at large.

And this in turn affects the level of the users' security awareness. As some of the respondents attested, users might not be entirely aware of the risk they are putting themselves and their organizations in when their remote work setups remain unsecured, or when they are too trusting of emails, platforms, or apps.

For example, in professional settings, business email compromise (BEC) persists, and because of remote work setups, it might prove more difficult to verify emails. As noted in the 2021 midyear cybersecurity report, one possible reason for the continued proliferation of BEC scams was that malicious actors might have been going after entities involved in COVID-19 vaccination programs.

Detections of BEC (specifically CEO fraud) attempts across OAS member states saw a 43% decline in the first half of 2021 compared to the same period in 2020. The United States had by far the highest number of BEC (CEO fraud) attempt detections, with Canada a far second.

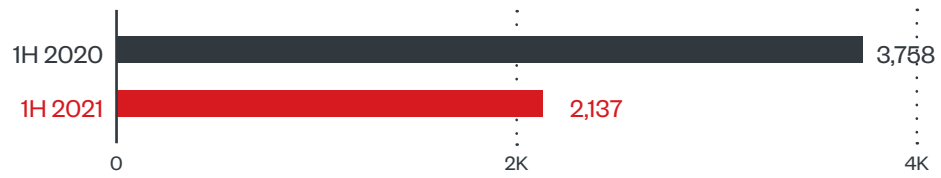


Figure 10. BEC (CEO fraud) attempt detections across OAS member states in the first half of 2020 and in the first half of 2021

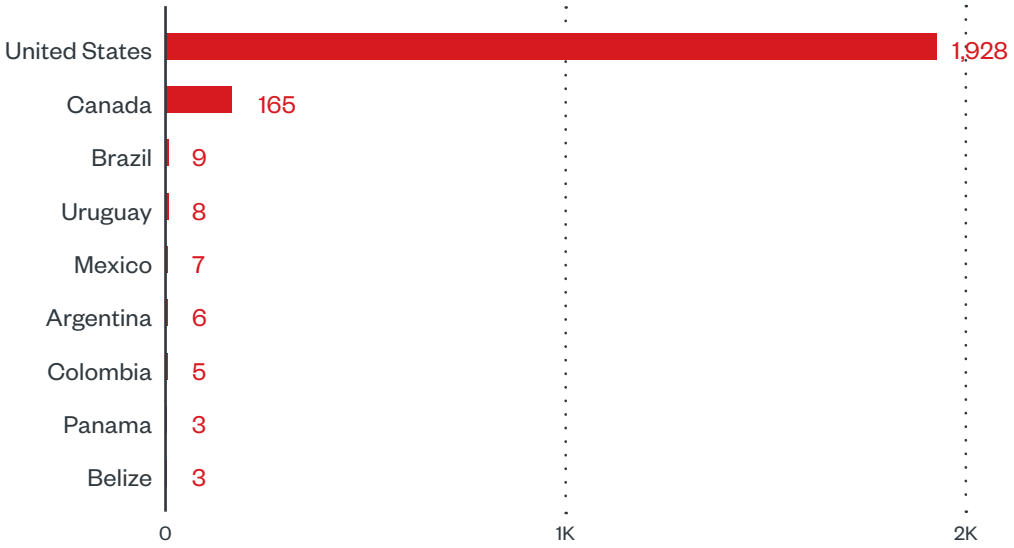


Figure 11. The top OAS member states in terms of BEC attempt detections in the first half of 2021

Systems that were heavily used during lockdowns, such as online banking platforms and applications, were also struck by cyberattacks. With regard to detections of online banking malware, the United States ranked first, with over 7,000 detections, while Brazil and Mexico each had approximately 3,000, and Canada had over 700.

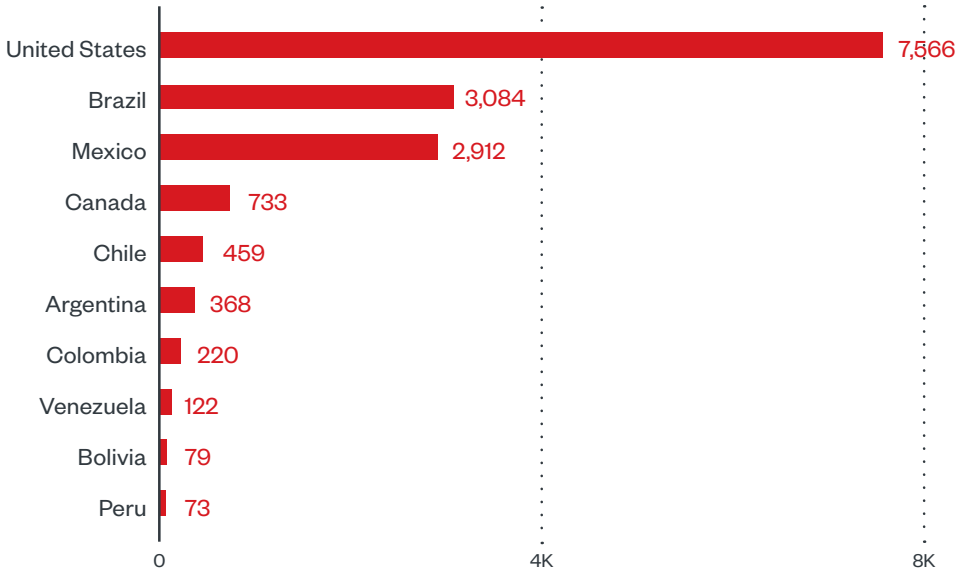


Figure 12. The top 10 OAS member states in terms of online banking malware detections in the first half of 2021

In terms of blocked malicious Android apps across OAS member states in the first half of 2021, there was an almost twofold increase compared to the corresponding number from the first half of 2020. The vast majority of the blocked malicious Android apps were observed in the United States, which had over 750,000, while Brazil had over 66,000 and Mexico and Canada each had over 20,000. Global trends also showed a rise in blocked malicious Android apps, although the increase was not as significant as in the Americas region.

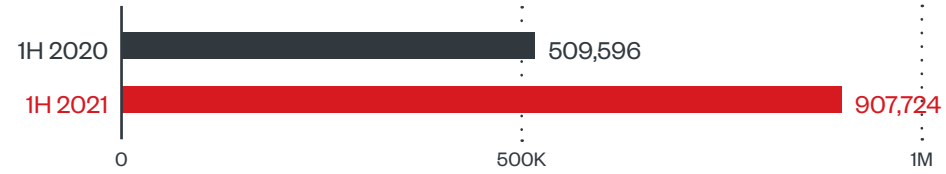


Figure 13. The number of blocked malicious Android apps across OAS member states in the first half of 2020 and in the first half of 2021

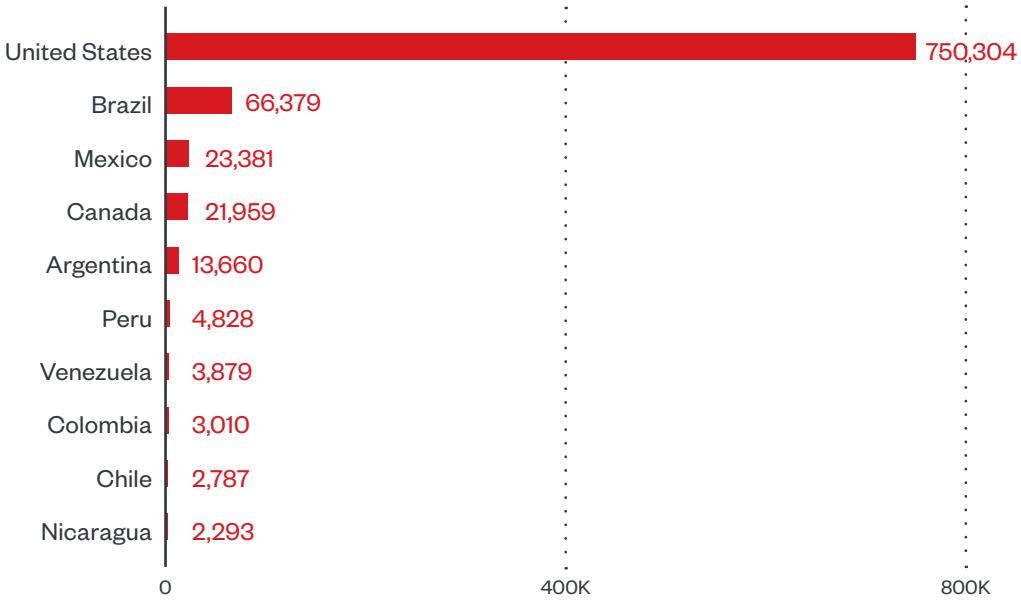


Figure 14. The top 10 OAS member states in terms of blocked malicious Android apps in the first half of 2021

COVID-19-Related Threats

News and issues surrounding the COVID-19 pandemic, such as vaccine updates and lockdown restrictions, were used by malicious actors as a social engineering lure, bringing additional threats to remote work setups.

In both global trends and the Americas region-specific data, the United States had the most COVID-19-related threat detections in the first half of 2021, although the detections decreased by over half from the same period in 2020. Meanwhile, some member states' numbers, particularly that of Colombia, increased significantly from the first half of 2020 to the first half of 2021, which might be indicative of additional efforts from malicious actors toward deploying COVID-19-related attacks in these member states.[9]

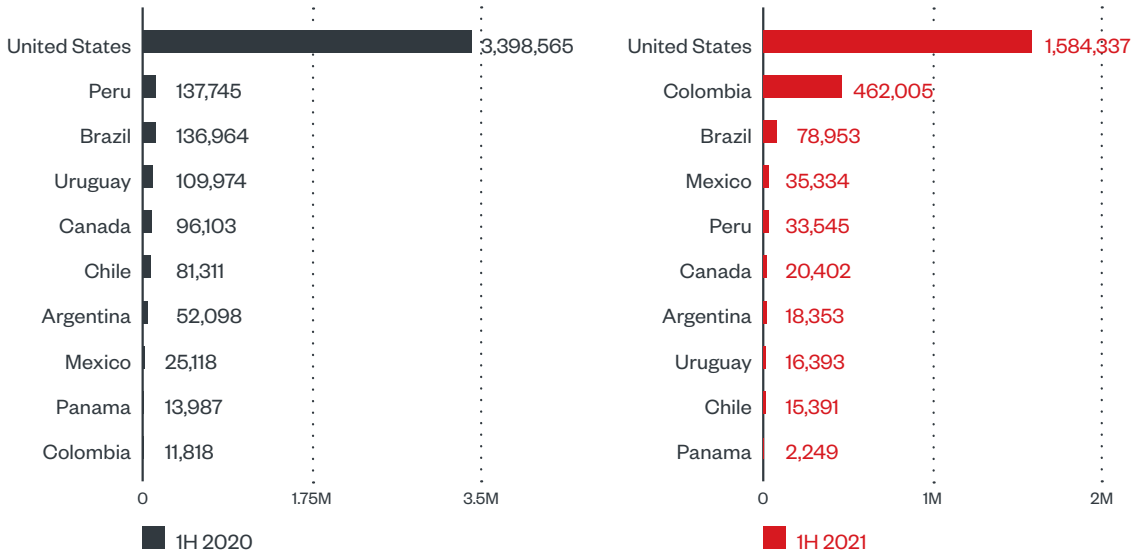


Figure 15. The top 10 OAS member states in terms of detections of COVID-19-related threats (malicious spam emails, malicious URLs, and malware) in the first half of 2020 and in the first half of 2021

As noted in the 2021 midyear cybersecurity report, misinformation had served as a catalyst for scams related to the pandemic, and vaccination programs and testing registrations had been among the most used lures.

Cloud and IoT Threats

Even before the COVID-19 pandemic and the large-scale transition to remote work setups began, many entities were already adopting relatively new technologies, such as cloud-based platforms and IoT or IIoT systems. This shift also came with its own set of concerns for most organizations. The adoption of such technologies should be managed to ensure that the benefits of using them far outweigh the risks.

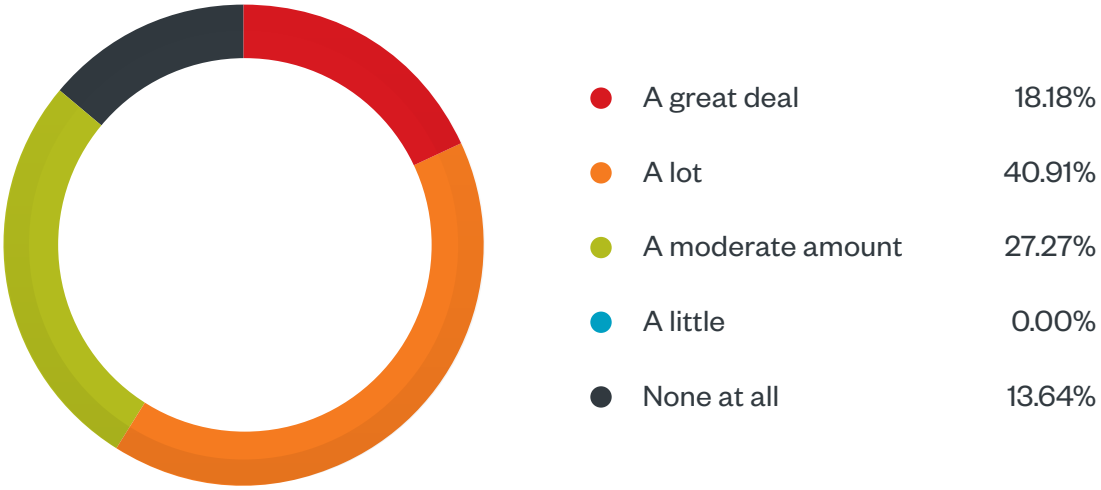


Figure 16. How adjusting to relatively new technologies such as the cloud and the IoT or IIoT was ranked as a security challenge by the survey respondents

In the survey, when asked to rank the shift to relatively new technologies in terms of the challenge they posed, most respondents rated it as something that concerned them "a lot." The option with the next highest number of responses was "a moderate amount," followed by "a great deal," and then "none at all."

Cloud Threats

Some entities had taken the security of these platforms for granted. As emphasized by a survey respondent, some might maintain their systems with default passwords and security settings, not knowing the dangers of leaving these platforms in such a state.

Misconfiguration and failure to patch and update systems have been among the most common causes of successful system infiltration. In 2021, misconfigured cloud systems were consistently targeted by malicious actors. As previously mentioned, TeamTNT targeted cloud platforms in its campaigns in 2021.

In March, Trend Micro tracked TeamTNT's activities and found a binary containing a hard-coded shell script used for harvesting cloud credentials. In this campaign, the group compromised a cloud instance, executed its script, and then looked for credentials deployed through the cloud metadata service. The script created a file and then uploaded it to a remote web server, which was intended by the group to be set as an open directory, which in turn allowed Trend Micro researchers to access the uploaded files. The server, besides being a repository of stolen data, also contained Linux cryptocurrency-mining tools that the group deployed on affected systems. Trend Micro detected more than 4,000 infected instances in this campaign.

In May, Trend Micro found that TeamTNT continued to target cloud credentials, this time by compromising clusters on Kubernetes, a widely used open-source platform for managing containerized applications, and exploiting them for cryptocurrency mining. Trend Micro confirmed that close to 50,000 IP addresses were compromised across multiple clusters.

Consistent across these cybersecurity incidents in March and May was the presence of cryptocurrency-mining elements. Cryptocurrency miners, which were the most detected malware type globally, were the third most detected malware type across OAS member states in the first half of 2021. As was the case with global trends, MalXMR was the most detected malware family, with its detections across OAS member states increasing twofold from the first half of 2020.

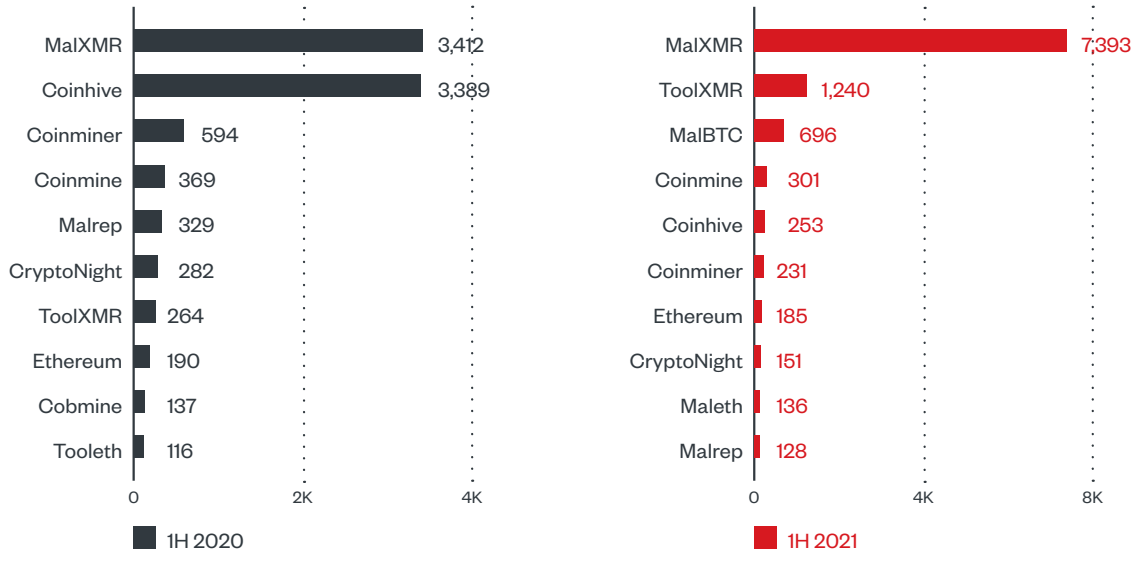


Figure 17. The top 10 cryptocurrency-mining malware families in terms of detections across OAS member states in the first half of 2020 and in the first half of 2021

IoT Threats

The IoT and the connections it enabled were likewise abused by malicious actors. One of the means whereby malicious actors take advantage of the IoT is through botnets.[10] A botnet is a network of hijacked computers and devices, or bots, remotely controlled by a hacker through the botnet malware implanted in the infected systems.

Botnet-related detections across OAS member states consisted mostly of those from the northern hemisphere. Detections from this subregion also made up a notable portion of global botnet detections: over 10% for botnet connections and over 30% for botnet command-and-control (C&C) servers.

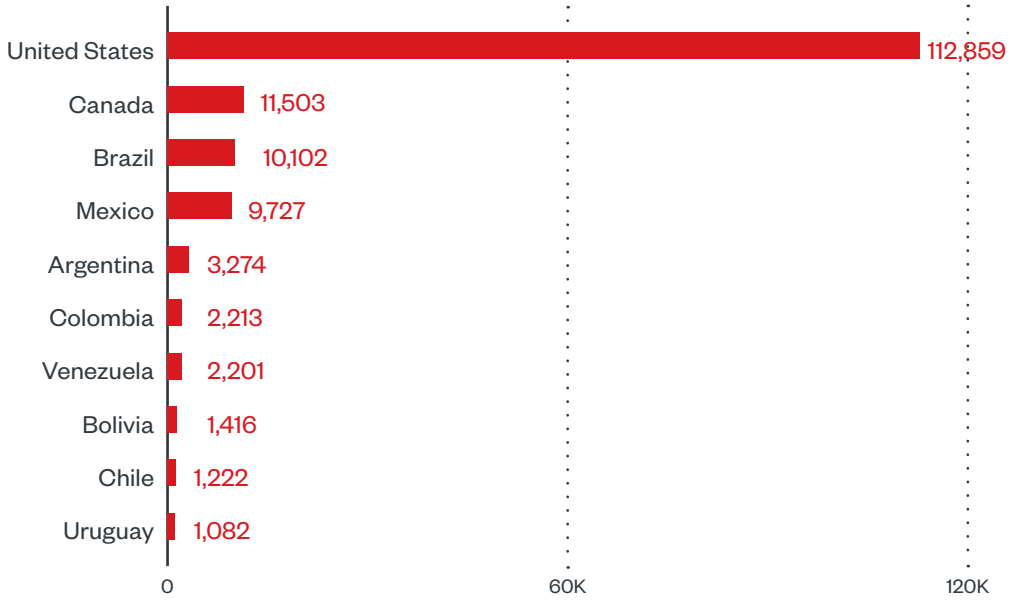


Figure 18. The top 10 OAS member states in terms of detections of botnet connections in the first half of 2021

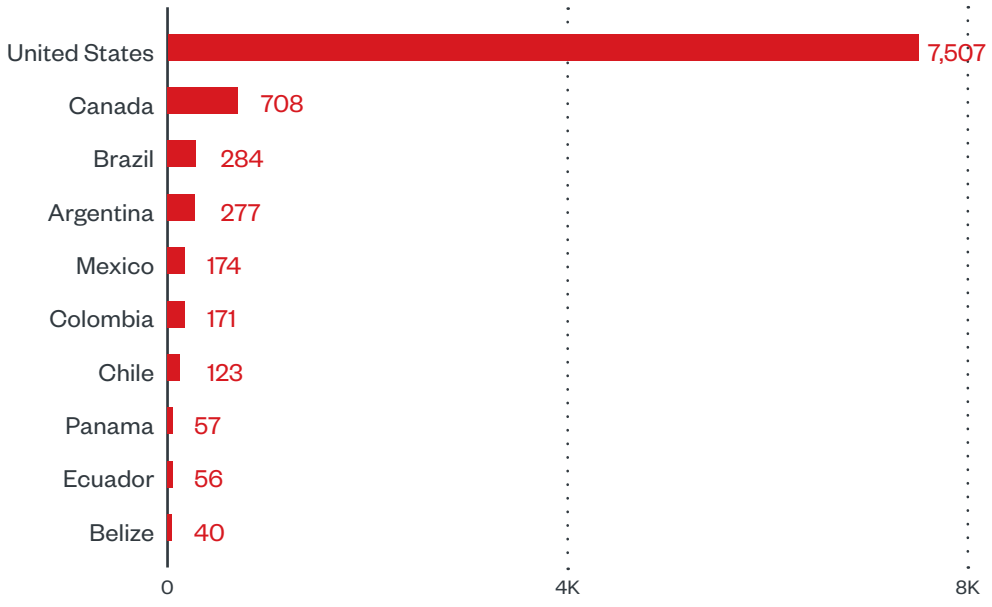


Figure 19. The top 10 OAS member states in terms of detections of botnet C&C servers in the first half of 2021

One of the IoT botnet malware families Trend Micro observed in 2021 was VPNFilter,[11] an older cyberthreat that remains active to this day. This malware compromises routers and storage devices via backdoor accounts and exploits devices from known vendors.

New technologies do offer promising benefits, but as some of our respondents acknowledged, they are not without risks. These risks include the expanded attack surface: "New technologies such as the IoT and 5G pose a high risk to security, since they significantly expand the attack surface and give way to new threats that are getting more sophisticated every day," one of the respondents said.

Aside from the threat brought about by botnets, Trend Micro also identified risks and cyberattack scenarios in other IoT technologies such as 5G campus networks[12] and LoRaWAN.[13] Increased knowledge and tools for assessing security, such as the LoRaPWN tool[14] for LoRaWAN, can help prevent damage resulting from threats.

But the lack of experience and confidence among users could sometimes hinder secure facilitation. This learning curve, while an inevitable part of the process, might also unintentionally expose systems and, in turn, the entire organization to risk.

To mitigate risks, according to a respondent, the importance of enforcing cybersecurity technical policies especially geared toward these platforms should be emphasized. Established policies, including proper configuration and timely updates, can help in the secure adoption of new technologies.

Conclusion

As in the rest of the world, a plethora of cyberthreats affected entities in the Americas region during the first half of 2021. While some findings based on the data collected were similar to those for global trends, others showed different results. This could perhaps be attributed to how malicious actors, influenced by lucrative targets, a particular country or region's cybersecurity policies, and other motivations, adjusted the tactics and tools they used depending on the country or region they were seeking to infiltrate.

With a better understanding of the cyberthreats that have affected OAS member states, the question now is: How can this knowledge be used to prepare for the future?

In the survey, the respondents were asked how they anticipated their industry or country to deal with the challenges as they would develop in the next 6 to 12 months. The respondents could indicate that they believed that either these challenges would become bigger challenges or the challenges would be better managed. A majority chose the former.

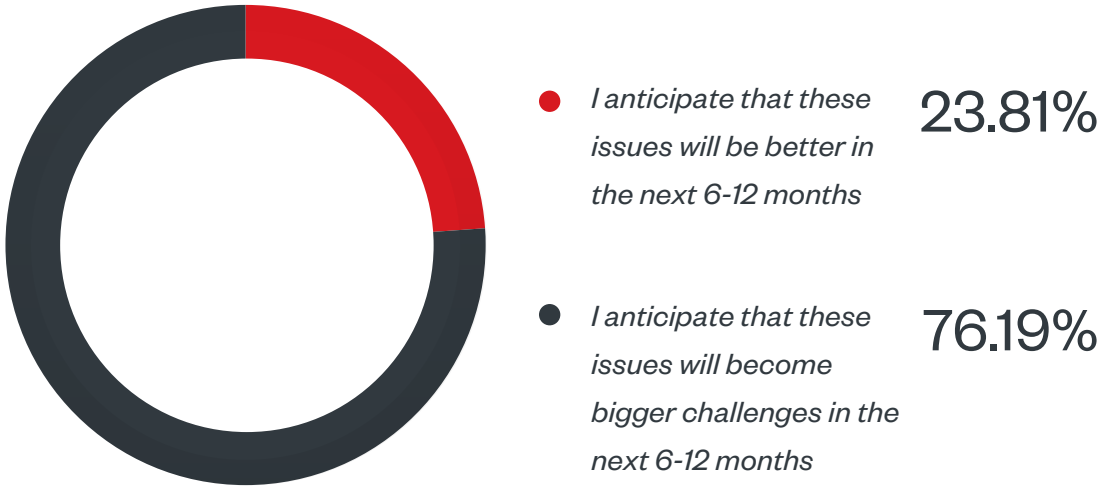


Figure 20. How the survey respondents anticipated their industry or country to deal with the developing challenges in the next 6 to 12 months

One of the main reasons most respondents expected the challenges to become bigger was the struggles that could come with attempting to keep up with new technologies, as well as updates with existing ones, especially in remote or hybrid work setups where more technologies were being onboarded. "The speed with which technology and interconnected solutions are developed and implemented is not the same as the application of controls," one respondent said. "There is still a lack of awareness about the risks at a general level."

Even more concerning was how cyberthreats continued to evolve, as expressed by a respondent: "Threats are going to become more sophisticated precisely because criminals are going to take advantage of the new environments." Lack of budget was also cited in some answers as one of the reasons.

On the other end of the spectrum, some respondents believed that cybersecurity concerns would be better managed in the next 6 to 12 months. This was mostly due to being able to adjust months into the pandemic, as well as the implementation of cybersecurity standard strategies, such as national cybersecurity strategies (NCSs), and security tools.

As for security concerns (besides the ones mentioned in the survey questions) that the respondents were anticipating to escalate in the next 12 months, the respondents mentioned the following: cyberthreats such as virtual private network (VPN) abuse and phishing, the current situation in the country such as an upcoming election that might urge cybercriminals to go after public services, and inadequate personnel and resources for cybersecurity.

A Look Toward the Future

The uncertainty and concerns regarding cyberthreats are not unfounded, as cyberthreats continue to evolve rapidly. Trend Micro's cybersecurity predictions report for 2022, titled "Toward a New Momentum,"[15] forecasts what malicious actors will focus on this year, with a view to equipping entities with the knowledge on what to watch out for. The cybersecurity issues highlighted in the predictions report echo those that had emerged in the Americas region:

- Ransomware operators will focus on extortion over encryption, and unprotected company servers will serve as breeding grounds for ransomware attacks.
- With security teams' focus on ransomware, traditional commodity attacks and attacks-as-a-service will take the opportunity to improve tools.
- Malicious actors will continue to repurpose older vulnerabilities as well as exploit new ones, including flaws found in platforms used for remote work setups.
- IoT data, especially connected car information, will be the target of cybercriminals, and enterprises will need take measures against data leakage.
- Botnet-as-a-service, designed to compromise and control both cloud-based and IoT platforms simultaneously, will emerge as a rampant threat.

The Importance of Preparedness in the Cybersecurity Landscape

In 2021, entities in OAS member states and countries all over the world had to defend themselves from threats coming from all angles. Now that these threats have been identified, what can entities do moving forward? The good news is, by knowing which threats are prevalent in the cybersecurity landscape, entities can perform actionable steps to boost the security of their systems.

Based on the survey results and the data presented in this report, entities will benefit from taking the following measures for improving their overall cybersecurity posture:

Heightening user awareness on the best practices to avoid threats. Simple steps such as never clicking links or downloading attachments in emails from unfamiliar sources, keeping software and applications patched and updated, and using multifactor authentication, among other best practices, can go a long way toward protecting entities from cyberthreats. It is therefore imperative to ensure that employees are aware of these steps, as such measures can be easily overlooked.

Establishing specific and actionable cybersecurity policies and strategies. On the administrative level, entities should prioritize the establishment of cybersecurity policies and standards. For example, entities can implement the zero trust model, an architectural approach that assumes that any unfamiliar user or device attempting to connect to an organizations' applications and systems, regardless of whether the user or device is already inside the network or not, needs to be verified before being granted access and trusted over time.

Assessing the cyber risks and properly configuring new technologies. The COVID-19 pandemic has indefinitely changed work setups, and more tools will continue to be adopted for either fully remote work or hybrid work models. Entities should therefore keep assessing the risks of incorporated technologies and ensure that they are properly configured. Entities should also employ access and application control especially if their employees access critical applications and data outside the office.

Allocating resources to procuring the necessary tools for providing enhanced protection. Entities should adopt cybersecurity solutions that can help provide visibility for proactive monitoring, advanced threat detection for spotting cyberthreats earlier, and correlated data across multiple layers (email, endpoints, servers, cloud workloads, and networks) for providing a broader perspective on findings, among many other benefits. These can help entities ensure round-the-clock security against persistent cyberthreats.

Overall, a cybersecurity approach that is connected across all layers, with the optimization of cybersecurity tools that can detect and deflect the diversification of cyberattacks, can enable the protection of an entity from malicious actors' schemes that can infiltrate systems from different entry points.

Appendix

Methodology

The data presented in this report takes into account data from the Trend Micro Smart Protection Network infrastructure. The data covers the date range from Jan. 1 to June 30, 2021, and includes the following countries in the Americas region:

- Antigua and Barbuda
- Argentina
- Bahamas
- Barbados
- Belize
- Bolivia
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Cuba
- Dominica
- Dominican Republic
- Ecuador
- El Salvador
- Grenada
- Guatemala
- Guyana
- Haiti
- Honduras
- Jamaica
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and the Grenadines
- Suriname
- Trinidad and Tobago
- United States
- Uruguay
- Venezuela

Data Disclaimer

The data analyzed for and presented in this report is from Trend Micro's Smart Protection Network (SPN) sensors, Philippines Threat Hunting team, Mobile App Reputation Service (MARS) team, Smart Home Network (SHN) solution, IoT Reputation Service (IoTRS), and researchers.

The data is a snapshot of the data gathered from sensors and parameters the research team had during the report's creation. The data might change retrospectively because of any future enhancements applied to the sensors and parameters.

Most data is from products and solutions Trend Micro has deployed in the market. A small percentage of the data is from external sources (via setting up honeypots or exchanging data with other companies). Therefore, the data presented can be considered customer data.

The detection numbers are derived from the coverage of the SPN sensors distributed globally. Thus, the data strongly correlates with how many products Trend Micro sells and deploys in each country, and how many customers turn on the feedback mechanism, which allows Trend Micro to collect threat data.

As a hypothetical example, if Trend Micro has a 50% market share in Malaysia and only a 20% market share in Thailand, the sensors would naturally pick up more cyberthreats in Malaysia than in Thailand, simply because there are more sensors in Malaysia. However, it would not necessarily mean that there are more cyberthreats in Malaysia than in Thailand.

The sensors are by default turned off. Customers can choose to turn them on for better protection. Once cyberthreats are detected, they are removed from the customers' IT environments.

There is no normalization applied to the data.

Regional Survey

To complement the data from the Americas region, a survey was distributed and disseminated to public officials and other sectors in the region through the CSIRTAmericas network of the OAS/CICTE. This qualitative data on their current state of cybersecurity went beyond the numbers and gained insights from the people in key positions in organizations based in OAS member states.

Disclaimer

The OAS and Trend Micro distributed an online survey to various organizations based in OAS member states. The results of this questionnaire are not representative of the 35 member states; it cannot be assumed that the results reflect the institutional views of each stakeholder. Nevertheless, while a more comprehensive study is required to provide a deeper understanding of the topics in question as they are perceived in the region, it is hoped that the analysis of the data collected through the survey might still shed some light toward a thorough understanding of the cybersecurity challenges in the region.

Some of the responses were translated to English.

The survey was sent out in September 2021. 22 responses were gathered from this survey.

Regional Questionnaire

Trend Micro OAS Specialized Report

1. How would you rank the following concerns in terms of the challenge they pose to your industry/country?
   - Dealing with online threats (ransomware, targeted attacks, scams, etc.)
   - A great deal
   - A lot
   - A moderate amount
   - A little
   - None at all

   Please provide specific details on the challenges that you encounter.

2. Adjusting to secure remote setups due to COVID-19 (both in terms of operations and securing organizations)
    - A great deal
    - A lot
    - A moderate amount
    - A little
    - None at all

    Please provide specific details on the challenges that you encounter.

3. Shifting to new technologies (cloud-based platforms, IoT/IIoT, etc.)
    - A great deal
    - A lot
    - A moderate amount
    - A little
    - None at all

    Please provide specific details on the challenges that you encounter.

4. How do you anticipate that your industry/country will deal with these challenges to develop in the next 6-12 months?
    - I anticipate that these issues will become bigger challenges in the next 6-12 months
    - I anticipate that these issues will be better managed in the next 6-12 months

    Aside from the ones discussed, is there a big threat or security concern that you are anticipating to escalate in the next 12 months? Please expand on the cybersecurity threat identified.

References

1. Trend Micro. (Sept. 14, 2021). *Trend Micro.* "Attacks from All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup.
2. Mayra Fuentes et al. (June 8, 2021). *Trend Micro.* "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.
3. Trend Micro Research. (Jan. 26, 2021). *Trend Micro.* "Examining A Sodinokibi Attack." Accessed on March 7, 2022, at https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.
4. Ericka Pingol. (June 4, 2021). *Trend Micro.* "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/f/meat-supply-giant-jbs-suffers-cyberattack.html.
5. Trend Micro. (May 12, 2021). *Trend Micro.* "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
6. David Fiser and Alfredo Oliveira. (March 9, 2021). *Trend Micro.* "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/c/teamtnt-continues-attack-on-the-cloud--targets-aws-credentials.html.
7. Magno Logan and David Fiser. (May 25, 2021). *Trend Micro.* "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html.
8. Gilbert Sison, Abraham Camba, and Ryan Maglaque. (Jan. 20, 2021). *Trend Micro.* "Investigation into PlugX Uncovers Unique APT Technique." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/xdr-investigation-uncovers-plugx-unique-technique-in-apt-attack.html.
9. Jared S. Hopkins, Kim Mackrael, and Giovanni Legorano. (Aug. 12, 2021). *The Wall Street Journal*. "Covid-19 Vaccine Scammers Target Authorities in Dozens of Countries Including Italy and Colombia." Accessed on Nov. 3, 2021, at https://www.wsj.com/articles/covid-19-vaccine-scammers-target-authorities-in-dozens-of-countries-including-italy-and-colombia-11628760600.
10. Trend Micro. (n.d.). *Trend Micro.* "Botnet." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/botnet.
11. Stephen Hilt, Fernando Merces. (Jan. 19, 2021). *Trend Micro.* "VPNFilter Two Years Later: Routers Still Compromised." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.
12. Philippe Z Lin et al. (May 27, 2021). *Trend Micro.* "The Transition to 5G: Security Implications of Campus Networks." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-transition-to-5g-security-implications-of-campus-networks.
13. Sébastien Dudek. (Jan. 26, 2021). *Trend Micro.* "Low Powered and High Risk: Possible Attacks on LoRaWAN Devices." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.
14. Sébastien Dudek. (Feb. 19, 2021). *Trend Micro.* "Gauging LoRaWAN Communication Security with LoraPWN." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/b/gauging-lorawan-communication-security-with-lorapwn.html.
15. Trend Micro (Dec. 7, 2021). *Trend Micro.* "Toward a New Momentum: Trend Micro Security Predictions for 2022." Accessed on Dec. 17, 2021 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022.

TREND MICRO™ RESEARCH

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

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research