HACKING THE SYSTEM

Ransomware Attack on Costa Rica's Government

By

Natalia Rojas Chaverri

A Senior Honors Thesis submitted

for the English Honors course in

fulfillment of the requirements for

graduation

Berkeley Academy

Santa Ana

Costa Rica

22 May 2023

Table of Contents

Abstract

The exponential increase in the use of technology has exacerbated the threat of cybercrime worldwide. As technology evolves, cybercriminals obtain developed tools and methods to exploit vulnerabilities in computer systems. In the case of Costa Rica, weaknesses in governmental institutions' systems were exploited by two ransomware groups: Conti and Hive. Their cyberattacks affected the Costa Rican population's access to essential services and threatened the security of personal data. Conti's malware spread to various institutions, making it the first cyberattack against a government. The extensive research conducted for this thesis served to analyze the current state of cybersecurity in the country after the attacks and elaborate recommendations for increasing its digital security. Through quantitative and qualitative data gathered from information security experts (*n=2)*, the attraction factors that placed the country as a target for ransomware groups were identified. Furthermore, governmental decisions and responses regarding the attack were analyzed. The results revealed that there was negligence of cybersecurity protocols from institutions that have access to sensitive information and lack of regulations that enforce righteous procedures. This study also determined the vulnerabilities exploited that other countries may face as well, making this study of utmost importance for cybersecurity around the world. The data collected during this study showcase the importance of spreading awareness of cybersecurity measures and providing effective ways for the protection of private data.

***Keywords*:** attack, Conti, Costa Rica, cybersecurity, ransomware, systems, threats, vulnerabilities

Natalia Rojas Chaverri

Professor Peter J. Swing

English 12 Academic Research and Writing

22 May 2023

Introduction

This thesis will analyze the current vulnerabilities in Costa Rica's cybersecurity and the modifications to government policies and actions starting at the moment of the ransomware attack. However, first an overview of the sequence of events, the impact on citizens, institutions, and national security, and the response by the government must be understood. Analyzing this can help determine the actions that must change to protect a nation from falling prey to an attack of this magnitude. Disclosing the weaknesses targeted by Conti and Hive (the two responsible Russian-linked ransomware groups) and their consequences can influence governmental decisions in the future. This investigation will serve as an alert to recognize and take action on threats arising in an advancing-technological world, both from the perspective of the administration and each individual that plays an important role in its effectiveness. It will identify effective ways to protect sensitive information and increase cybersecurity in the country, and hopes to serve as a call for awareness of the dangers of an unprotected cyberspace.

A. Terms

"With the advent of the Internet and the development of computer systems, there is a new space of interaction between people called cyberspace, where the roles of the different agents develop, evolve and change day by day" (qtd. in "Plan General de Emergencia" 5). Cyberspace can be defined as:

> An artificial domain built by man, differentiated from the other four war domains (land, air, sea, and space). It is deeply linked and supported by physical means…[and] if this interconnection is attacked, it can have serious repercussions on…security strategies. (qtd. in Gamón 81)

The terms "cyberwar" and "cyberterrorism" remain unclear concepts due to their complex and constantly changing nature, but according to its general definition, describe the illegal aspects committed in cyberspace (Carlini 4; Gamón 82).

Cybercriminals can use various methods to attack people, companies, and institutions. However, this thesis will focus on ransomware, which is the method that cybercriminal groups employed to target the Costa Rican government. Ransomware is a "modality in which a cyber attacker limits access to different files of an operating system through malware and demands money to remove that restriction" (Summa). Ransomware groups "bypass standard cybersecurity structures such as firewalls and use highly skilled methods of phishing to gain access to networks" (Sangfor). According to the Costa Rican entity, Comisión Nacional de la Emergencia (CNE), this type of attack generally comes from an external source, often operating with the support of internal agents such as an employee or official of an institution or company who has access to the organization's computer programs to cause a serious security incident ("Plan General de Emergencia" 7).

Overview

On May 8, 2022, the same day Rodrigo Chaves was appointed Costa Rica's president, he declared a national state of emergency due to a ransomware attack on a crucial government entity, the Ministerio de Hacienda. This institution guards budgetary policies, formulates taxation, and manages operations systems (Ministerio de Hacienda). More than eight hundred servers were impacted, affecting all import and export services in the country, resulting in container shortages, extensive financial losses, and ceasing international commerce (Burgess). The attack spread to various government organizations, including and affecting the Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT),[1] Caja Costarricense de Seguro Social (CCSS),[2] and Ministerio de Trabajo y Seguridad Social (MTSS) ("Plan General de Emergencia" 10).[3] According to President Chaves, by May 16, 2022, the number of institutions impacted by the ransomware group grew to twenty-seven (Burgess).

The attacks were initiated on April 17, 2022, and two Russian-linked ransomware gangs held responsibility. The first and most impactful was executed by Conti, who demanded ten million dollars and threatened to release sensitive information from the Ministerio de Hacienda (Burgess). After the Costa Rican government refused to pay the ransom, 672 gigabytes of files from the institution were uploaded to Conti's website and the price demanded doubled (Burgess). Posts on Conti's blog stated, "I appeal to every resident of Costa Rica, go to your government and organize rallies," and, "we are determined to overthrow the government by means of a cyberattack," which is why this attack is said to be the first ever to target a nation's government explicitly through ransom (Burgess). With ninety-seven percent of the data published on Conti's

website, the group threatened to delete the recovery keys for the stolen information by May 23, 2022, unless the government paid the new price (Burgess).

Mid-attack on Costa Rican government institutions, Conti dismantled after a public statement supporting Russia's war on Ukraine (Sangfor). As a ransomware-as-a-service (RaaS) provider, Conti members code in separate hacker groups, many of which are located in Ukraine (Whittaker). Due to the public statement, some members located in Ukraine retaliated against the group by leaking source codes and internal chat logs (Whittaker). The publicized support for the Russian invasion made Conti lose public support, and international sanctions on Russian citizens, such as blocking money transactions, hampered their operations (Sangfor). On May 19, 2022, Conti's admin panel and negotiations server went offline and the rest of the infrastructure was reset (Burgess). Louise Ferrett, a threat intelligence analyst at Searchlight Security, stated Conti's behavior had become increasingly reckless, "so disbanding or rebranding [would allow] them to throw law enforcement off their tails, making their job even more complex and at the same time allowing them to rebuild their image" (Wadhwani).

Although Conti ceased its operations, Costa Rica's war was far from over. On May 31, 2022, the second attack started, "sending Costa Rica's health care system into a spiral" (Burgess). This time, a new Russian-linked ransomware group that calls themselves Hive was responsible. Conti is believed to have some links to the Hive group due to their history of targeting healthcare organizations, but Hive denied affiliation with Conti on their website (Burgess). On June 3, 2022, the CCSS declared an institutional emergency (Burgess).

A. Effects

The cyberattacks on Costa Rican entities prevented the development of the usual work of services to the public, affecting citizens' access to essential services and resulting in devastating consequences for the population and the governmental institutions involved. The economy suffered from the disruption in tax payments; estimated losses were $125 million in the first forty-eight hours (Burgess). Because of this, workers from public sectors, such as school teachers, could not obtain their payments on time, affecting them and their families (Fernandez). At least twelve thousand educators, which represent approximately fourteen percent of the total eighty-eight thousand employees from Ministerio de Educación Pública (MEP),[4] had their salaries affected and ninety-nine percent of vacation requests from employees were not processed (Fernandez).

For the Ministerio de Hacienda and the CCSS, the attack disabled their digital platforms for more than two months, impacting the service users, which, considering its relevance in the provision of public services, caused a serious impact on the national population ("Plan General de Emergencia" 10). Personal data logged into CCSS's online platforms affected by the ransomware was exposed and the healthcare systems went offline, causing delays in patients receiving treatment (Burgess). Furthermore, the CCSS warned parents, whose children were undergoing surgery, of trouble locating their children, and public health systems such as COVID-19 testing and tracking were not possible (Burgess; Sangfor). The CCSS reported more than thirty thousand medical appointments being rescheduled (which equals seven percent of the total appointments), 10,400 computers impacted, and 759 of the 1,500 servers compromised (Burgess).

According to a report made by MICITT, the existing cybersecurity measures in those institutions, in response to the actions of this specialized cybercrime group, made the presented consequences inevitable ("Plan General de Emergencia" 9). The crisis had significant repercussions on the socioeconomic dynamics of the country, the provision of basic services, and in turn, "on the exercise of the fundamental rights of the inhabitants and even beyond the country's borders" (11). The report also gathered damages by the eight most affected institutions (fig. 1), such as exfiltration of information published on Conti's website, information encryption, functionality affectation of computer systems, defacement (website modification), and theft of social media credentials (10). In other institutions, the technical measures deployed managed to detect and contain possible Conti attacks in their systems (10).

B. Response

Luckily for Costa Rica, the government was not completely unprepared for the cyberattack due to previous participation in relevant initiatives such as the Budapest Convention on cybersecurity, its Computer Security Incident Response Center (CSIRT-CR) established in 2015, and a National Cybersecurity Strategy implemented in 2017 (INPLP). In terms of data protection, a local data protection law was issued in 2011 and appointed a local agency for its supervision (INPLP).

After declaring a state of emergency, Costa Rican President Chaves reached out to advanced countries in cybersecurity, such as Spain, Israel, and the United States, to ask for support and advice (INPLP). Consequently, United States President Joseph Biden offered a fifteen million dollar bounty to anyone that provided useful information that could help identify and capture the criminals (Sangfor). Private companies in Costa Rica such as Microsoft, GBM,

and MICITT also helped defend the nation (Amerise). According to INPLP, “communication and coordination initiatives were carried out including high-level teams with members of the government and the private sector, the main business chambers of the country and all telecommunications service operators.” Furthermore, the government entity MICITT issued a new directive on the implementation of security measures that should be carried out immediately by the entire public administration for institutions to reinforce security (INPLP). The institutions received new policies, procedures, and controls to verify their digital platforms, and MICITT and the institutions linked to the CSIRT-CR started a process of rebuilding the National Cybersecurity Strategy 2022-2017 (INPLP).

Literature Review

When analyzing the current state of cybersecurity in Costa Rica, it is crucial to understand the increase in cyberthreats that the world has faced from 2018-23. Various works have sought to explain the cause of this rise in criminality, and understanding the trends will help find common vulnerabilities in less-developed countries. For this part of the investigation, research studies regarding the rise of ransomware and common vulnerabilities in legislation, public sectors, and lack of updated software, will be explained.

According to Harding and Ghoorhoo in *Hard Choices in a Ransomware Attack*, “Ransomware attacks started as a novelty but have now become a clear and present danger to entities of every size and function” (1). There has been a notable increase in the number of ransomware attacks and the price of demanded ransomware since 2018, but legislation and policy have not been updated (1). The authors explain this to be difficult as policymakers “are searching with incomplete information for the right combination of carrots and sticks that will

help victims and hurt attackers," whether it is due to a lack of technical knowledge or because they have never experienced an attack of this type (1). They also stated that many entities, such as schools or municipalities, have not taken the security steps needed to protect themselves, because they lack resources or knowledge, or because they have a misplaced sense of optimism that makes them believe they will not fall victim to cybercriminals (2). Their research identified vulnerable sectors to be hospitals, financial services, and universities due to the "sensitive nature of their customers' data" (3).

Harkins, Malcolm, and Freed further explain in *The Ransomware Assault on the Healthcare Sector* how this new era of ransomware has made everyone, "both individuals and organizations alike," a target with ransomware (148). This attack method is described as "inexpensive yet very impactful," due to its "wide array of attacks," and "real threat of data destruction" (148). As stated by the authors, "this ransom is typically paid in bitcoins, which provides the malware author with an untraceable form of instant payment," thus making this type of crime appealing (151-2). The problem with this attack method is aggravated by the proliferation of ransomware-as-a-service (RaaS). "RaaS is quickly becoming one of the most popular forms of cyberextortion," they explained, where "ransomware specialists can offer their code to novice hackers online for a nominal fee, or for no fee at all, or with a cut of any ransom obtained" (152). Therefore, this modality presents a danger that is unperceived by many organizations, and criminals take advantage of that.

Rodrigo Díaz presents an example of the threat of ransomware in *Estado de la ciberseguridad en América Latina y El Caribe*. The ransomware Maze, which started operating toward the end of 2019, became the first type of malware that extorts its victims by threatening

to divulge sensitive information (19). DopplePaymer, Sodinokibi, Netwalker, Conti, and Egregor followed in this modality (ransomware) and demonstrated an increase in diffusion speed and amount of ransom requested (20). For instance, Maze managed for fifty victims to pay ransom in six months of attacks and Egregor later targeted Cencosud in November 2020 and received ransom in just three weeks (20). The amount in ransom payments requested rapidly increased, as cyberattackers realized the value of sensitive information, and that techniques to access a small or medium company's systems did not differ greatly from a larger one that could also pay higher prices (20). By the third trimester of 2020, the value of ransom had tripled from the first trimester of the previous year (qtd. in Díaz 20). This evidences the need to continuously update software so that countries, institutions, and individuals can be safe from the rapid development of cyberattack methods.

When analyzing the vulnerabilities exploited in Latin America and the Caribbean during the first semester of 2020, the study found that five percent were vulnerabilities discovered from 2019-20 and fifteen percent in 2018 (Díaz 22). Therefore, eighty percent of exploited vulnerabilities had been known for at least two years before 2018, which meant that operative systems are failing to update their software for protection against cyberattacks, while cybercriminals continue to develop better techniques and tools to exploit them (qtd. in Díaz 22). This research should inform countries in Latin America of the threats in cyberspace and preventive measures should take priority to ensure the safety of their population.

Quantitative Analysis

Global digitalization has brought many advantages for the development of countries and advancement in all labor sectors. During the COVID-19 pandemic, it allowed for a shift to work

remotely, allowing many businesses to continue operating despite the sanitary restrictions forcing workers to remain in their homes. However, it also resulted in a dependency on technology, and that reliance is what cybercriminals utilize to thrive. "[As] the world continues to grapple with a lasting pandemic … [we notice how] threat actors opportunistically used a shifting landscape to adopt tactics and techniques to successfully infiltrate organizations across the globe" (IBM 3). This analysis categorizes the most predominant types of cybersecurity attacks in the world from 2019-21, showcasing the impact of Conti Group in different regions and identifying the most vulnerable areas in cyberattacks to contextualize these factors to some of the vulnerabilities that Costa Rica was facing during the ransomware attack.

A. Predominant Cyberattacks in the World from 2019-21

According to a study by IBM Security X-Force, ransomware has been the most common cyberattack type for more than three years, resulting in twenty-one percent of all attacks in 2021 (7). Figure 2 shows the top attack types in 2021 compared to 2020.[5] The graph demonstrates there was a decrease in ransomware attacks compared to the twenty-three percent in 2020, but remains significantly higher than the percentage of other attack types in both years. IBM claimed the down-tick could have resulted from increased law enforcement activity in 2021 that in some cases forced ransomware groups to shut down (10). According to X-Force's research, the average time before ransomware groups shut down or rebrand is seventeen months, but the groups often continue their operations under new names (10). Therefore, a potential resurge of this type of cyberattack could be seen in the following years (10). This could exemplify the cause for Conti to shut down during their attack on the Ministerio de Hacienda and proves a current threat of them returning after having already tested their software.

Additionally, the data demonstrate an appeal for cybercriminals to utilize the sophisticated tools and methods that modern technology has allowed. This is why ransomware holds the higher percentage of attack types in both years, being so appealing to criminals due to their facility to rent a software and execute an attack while remaining hidden. Comparing the data from the two years, a higher percentage of ransomware attacks is identified in 2020, during which reliance on online platforms allowed for increased vulnerabilities in computer systems that cybercriminals could exploit. The research findings attribute the decrease in the percentage of ransomware attacks in the following year to the return to office after the pandemic, which diminished the usage of online platforms and data that cybercriminals could obtain. However, since some businesses decided to maintain the online modality, it is expected that the numbers continue rising.

B. Impact of Conti Group in Different Regions

Conti has been infamous in various Latin American countries in recent years. The attack on Costa Rica's government was one of the most notorious attacks in 2022, but the group also breached servers in Argentina and Peru, sometimes succeeding in obtaining sensible information and sometimes failing (Vanci). As of January 2022, according to the FBI, the hackers had targeted more than one thousand victims and retrieved more than 150 million dollars in ransom payments (Vanci).

Group-IB, one of the global leaders in cybersecurity and headquartered in Singapore, described Conti Group as "one of the most aggressive and organized ransomware operations," ("The Conti Enterprise"). Their report about ARMattack, one of the shortest yet most successful campaigns by Conti, found that in slightly more than a month, the ransomware collective

compromised more than forty companies worldwide, and in two years attacked more than 813 victims (“The Conti Enterprise”). Figure 3 shows the number of victims posted on Conti’s dedicated leak site (DLS) per quarter from 2020-22.

The study by IBM Security found the most common types of ransomware observed in 2021 (Fig. 4). Conti made up three percent of all the reported ransomware incidents, demonstrating its prevalence in worldwide cybersecurity. Although Conti was dismantled on May 19, 2022, a group with such a success rate in criminal activity can only be expected to reappear with greater power under new names, and only extreme precautionary action will stop it from further disrupting systems and threatening organizations. However, it is also important to note that there is a vast number of ransomwares that have also been effective in infiltrating their targets, so although this analysis on Conti’s operations will help build a better strategy for a country’s cybersecurity, they are not the only threat in cyberspace.

C. Vulnerable Areas

In 2021, Asia was the most affected continent, holding twenty-six percent of all cyberattacks that year (IBM 6). Currently, however, the world is seeing a shifted geographic focus of cyberoperations toward Latin America (15). As shown in Figure 2, Business email compromise (BEC) was the third most common attack type in 2020 but its percentage decreased in 2021 (15). It is theorized by the report from IBM Security X-Force, that the implementation of multifactor authentication (MFA) decreased the number of BEC attacks in 2021, but also resulted in a geographic shift to countries where MFA is not as widely implemented (15). Figures 5 and 6 show a breakdown of attacks by geography comparing the years 2020 and 2021, and the percentage of incidents that were BEC in 2021. The graphs demonstrate an increase in

cyberattacks on Latin American countries and a downward trend for Asia, probably due to their capacity to obtain technological protection such as MFA. Furthermore, the rate of BEC attacks against Latin America is higher than for any other region, and represents a sharp increase since 2019 (41).

The case of the ransomware attack in Costa Rica exemplifies how cybercriminals are targeting the weaker cybersecurity systems in Latin America. Speculation on the vulnerability targeted by Conti and Hive includes malicious links sent via email and opened by one of the workers from the Ministerio de Hacienda. The virus would have spread to the computer systems and retrieved the data that cyber criminals utilized for their attempted extortion. This event has and can be replicated in other systems and governments. The data from the graph (fig. 6) demonstrates this vulnerability is present in a worldwide aspect, and identifying the vulnerable areas may help analyze the factors that contribute to a weak cybersecurity system.

The rates of cyberattacks are often underestimated, especially when they are not publicized or the threat is contained. According to Bleeping Computer, in 2021, Costa Rica suffered over 1200 cyberattacks on a weekly basis (Sangfor). Nonetheless, the vulnerabilities in the country's cybersecurity were only brought up to the public's attention after the attack on the Ministerio de Hacienda (Vanci). CriptoNoticias also reported that the attack in 2022 was not the first time the country fell prey to a ransomware group. In May 2020, a hacker group named Maze Ransomware targeted Banco de Costa Rica to obtain sensitive financial data from the bank's clients (Vanci). These incidents demonstrate that it was until extensive damage was obtained by the cyber criminals, that the media pointed the lens to the issue. For that reason, the data gathered

during this thesis is of utmost importance to bring awareness to the protection that is needed as it relates to cyberspace.

Qualitative Analysis

Although the cyberattack on the Costa Rican government captured the attention of the media, the information provided for the general population remained superficial and many details on why and how this attack was conducted are still unknown. Therefore, a qualitative analysis was conducted in this section to find the vulnerabilities that made Costa Rica a target for criminal organizations. For this, two cybersecurity experts were interviewed: Mario Robles, CEO and founder of White Jaguars Cybersecurity, and Jorge Mora, ex-director of digital governance for the MICITT from August 2019 to May 2022.[6] The purpose of this analysis is to provide awareness to the problem that Costa Rica is currently facing, and note that the attack did not just occur once, but will certainly happen again if the necessary steps are not taken.

A. A Foreseen Disaster

To better understand the aspects that set Costa Rica as a target for these highly-organized ransomware groups, three important vulnerabilities in the world must be taken into consideration: today's digital era, the lack of education in digital matters, and the increased vulnerabilities during the pandemic. As explained by Mora, historically, technology has sought the facility of use from the person rather than focusing on a design for security (1).

> The internet boom has made this in, I believe, one of the most complex systems in planet Earth because we are talking about computers that connect to networks, those networks connect to systems [in an institution or a company] … and those systems are connected to other countries, and so we have a level of complexity

> that is very high because there is a dependency on the security that third parties have or don't have. (Mora 1)

Countries must make up for the lack of security by updating their software with anti-viruses and educating their employees on security measures. However, it is also up to the education system to teach the new generations on the correct usage of the digital tools.

Mora believes the education system has failed to update on these issues that are so important to make the best use of information technologies while being conscious of the security and correct use of data and information (1).

> It is common to hear people from different ages say, well, what does it matter that someone has my data, I am not a famous person or someone that has a lot of money, so what use will [cybercriminals] have with my information? Well, the problem is not what benefit can be obtained with the information of a specific individual, but the set of information of thousands or millions of individuals, that is what can generate statistical trends or information that can also be used for criminal acts. (Mora 1-2)

To achieve a state of high cybersecurity for the protection of the population's information, each individual plays a role and must follow the recommendations from cybersecurity experts.

Lastly, during the pandemic, "just as companies implemented telecommuting for people to work from home, well, criminals also had to digitize," elaborated Robles, "and precisely [since ransomware] … is a service that someone else can hire, that means I don't need to have very deep technical knowledge to be able to hire that platform and run it" (7-8).

> So that makes these types of attacks available to people who are not so specialized and it is a good opportunity to have fewer risks. I no longer have to go rob a bank with a gun, it's easier to try to break into the systems and extract the money without them seeing my face. (Robles 8)

Therefore, these three aspects generated a series of vulnerabilities all around the world and, as Mora stated, "there was not enough time to implement the necessary security measures so that an institution [could] be 100% secure" (2). For this reason, cybersecurity experts were not surprised at the ransomware attack on the Costa Rican Ministerio de Hacienda. "What happened here in the country, let's say it was a song that had already been sung for a long time," stated Robles, and "it was only a matter of time" (1-2).

B. Inside the Minds of Cybercriminals

The question about why Costa Rica specifically became appealing to cybergroups was identified by another series of factors that were explained by the experts in cybersecurity. First, at the time when the attack started, all countries in Latin America were "considerably behind in technology," explained Mora, which made them "attractive … to be testing grounds for these cybercriminals" (6). Costa Rica, for example, started having great advancements in cybersecurity in 2019, but being a less-developed country could have made it the perfect place to test some new cybercriminal tools (6). This claim is supported if we take into account that Conti targeted more than 150 different countries during that time, and that same week the attacks in Costa Rica were happening, other countries in Latin America were also affected (7; Robles 6).

Mora also explained a theory elaborated by Tech Intelligence that states the possibility that Conti utilized the attack on Costa Rica's government as a smokescreen so that the group

could dismantle by distracting the authorities' attention with the attack (5). That would have not made the country a special target, but rather just a means to an end. Nonetheless, there are indicators that point toward the attack being a directed attack. As Robles indicated, "There are many theories so it will be very difficult to know [why the attack was really executed]" (7). Taking into consideration that Conti functions as a RaaS group, that means that anyone that had an interest in Costa Rica could have rented Conti's platforms to execute the attack, it was not necessarily them directly (Robles 7). However, there are two main areas of speculation on why Conti may have taken an interest in the country.

The first is support for Russia in the war against Ukraine, as it is known that Costa Rica is a close ally of the United States, which "could have touched some sensitive nerve [on Russian groups]" (Robles 6). Mora also elaborated on that topic, "we are a country that does not have an army and … by not having a physical army, we could understand that there are no virtual armies [either], so there [would be] no counterattack" (5). Additionally, Mora believes that at that time, the country had been in the international spotlight, as it had had a series of recognitions on environmental issues, so that would have placed Costa Rica in the world news (5).

The second is that the ransomware groups were attracted by Costa Rica's economy, because as stated by Robles, within the scope of Central America, Costa Rica's economy is the best positioned (6). "That means that suddenly we are a small country that does not have global levels of cybersecurity and suddenly it seems to be a place that has the money to potentially pay for one of these attacks," said Robles (6-7). Mora also elaborated, according to his personal criteria, that the Ministerio de Hacienda must have been identified as an institution that had money (7).

> In fact, the amount requested [by Conti] historically had been two to five million dollars, and [in this attack] this was quite high, they were asking for ten million dollars in their extortion process, so it seems to me that if it was a directed objective and studied. (Mora 7)

C. Attack Vector

Just as it is very difficult to know for certain the real reason for the attack, it is also complicated to identify the entry point. "There are very large third-party investigations involved to detect this kind of issue and a forensic analysis must be conducted, which [could] take months or even years depending on the volume of data," said Robles (4). However, based on the way ransomware normally operates, an idea of how the cybercriminals could have executed this attack can be inferred. "They sent an email, said something convincing, you clicked on a link, your computer was infected with malware, and it spread through the networks. That's the nightmare (Robles 4)." This is common knowledge for cybersecurity professionals, so that would make professionals in cybersecurity question why the institutional systems were unprotected from this type of attack.

Mora explained a vulnerability that he noticed in the public sector when he worked in digital governance:

> There was no regulation that made it obligatory to abide by the technical recommendations that were requested by the MICITT. … We found vulnerabilities in systems or security devices such as a firewall, switches, operating systems, the institutions were notified but there was no regulation that made the application of these recommendations mandatory. (3)

He added that there are also budget constraints in the public sector and a lack of workers with the necessary knowledge for the technology that there is, so that poses a great challenge to public institutions (2).

Furthermore, it was identified at the time that credentials from different public institutions were being sold on the dark web.

> These groups in Russia had information that was quite specific regarding how Costa Rica works and how it operates. That is something that normally these groups on the other side of the world usually do not know. So there are indications that suggest that there was someone collaborating from here. We are not saying that it was an expert, it could have been anyone with some technical knowledge that could have been collaborating. (Robles 5)

D. Call for Action

Evidencing the common and specific vulnerabilities in the country is hoped to serve as a call for action in better preparedness for future cyberattacks because, as Robles stated, "this is every day and it is always … The normal thing in private companies and other institutions is to see millions of attack attempts every day" (3). He suggests each individual to have their own security at home, "that is why we talk about wanting to have a society that is cyber resilient because we have to accept the fact that we are always going to be attacked and we have to be prepared with that" (3).

Regarding the government's response to the incident, according to Mora and Robles, it was better than expected. "Actually, I would say that the Ministerio de Hacienda was restored sooner than could have been anticipated," said Robles, "In some estimates it was thought that the

servers could have been down for six months due to the level of impact" (8). "I think there was a very good response with the resources that were available," commented Mora (8). However, Robles also stated that:

> There is definitely evidence of a lot of bad practices that exist and that must be learned. For example, in the case of the Ministerio de Hacienda, if the attack entered through an end user and that reached the servers, that means that we had a terrible architectural failure because that should have been isolated. … [Additionally], time goes by and one can still hear comments from people who say, well, we were unlucky last year. It's over. Now who knows until when it will happen to us. Until we heard what just happened to the MOPT. And right now the MOPT is in a situation very similar to that of the Ministerio de Hacienda. (8)

Current Situation

According to Mario Robles, the main problem with the lack of cybersecurity in Costa Rica is the absence of political will (3). There are few people, with the technical knowledge of the cybersecurity measures necessary to protect a country from cyberthreats, in power to implement the necessary policies (Robles 3). "The process is slow," Robles stated, and currently "there has been some willingness on the part of the government to inject a bit of capital … but the reality is that the MICITT … [does] not have the muscle to execute [effective measures]" (3). This means that the country is still vulnerable to cyberattacks; as Robles stated, "it could happen to other institutions at any moment (10)."

He also explained that some private companies have been proactively working with the municipalities that were affected during the ransomware attack to implement mechanisms for

defense against cyberthreats (3). Nonetheless, it has mostly been a decision of each company rather than an order from the government (3). For the Ministerio de Hacienda, which was the most affected institution during the attack, there is still some data that the response team has not been able to retrieve, and "we're still picking up the pieces," he explained (10).

Although the government's actualization in defense measures has been slow and small, some better practices have been evidenced since the attack, "more frequent reviews have been carried out and many institutions have undertaken the task of hardening their infrastructure a bit better," said Robles (9-10). The improvement in ways to detect and detain cyberattacks has been few but at least there is some advancement, which is the first step towards achieving cyber resilient security.

Many experts in cybersecurity have been upset with the lack of advancement in this field from the government. Policies that force institutions to uphold a certain standard in protection measures and investigations that analyze the situation and provide solutions for future reference are still missing. Mauricio París, from Fundación Privacidad y Datos (Privat), stated that "if in fifty years some historians were interested in understanding what the attacks that more than thirty institutions suffered during April and June of [2022] consisted of, it would be very difficult to understand what happened" (qtd. in Murillo).

Another expert in cybersecurity from Atticyber, Esteban Jiménez, stated:

> We have to learn from what happened because we suffered a direct attack from an incipient cybergroup … we are not prepared for the threats that are being detected in Costa Rica … they are threats that after Ukraine's invasion have been increasing in sophistication. (qtd in. Murillo)

Jiménez believes what is worse is that no one held responsibility (qtd. in Murillo). It is unknown who ignored the alerts, who was responsible for those alerts, or what was the chain of command (qtd. in Murillo). “This is especially curious when even the President of the Republic spoke that there were collaborators in the country of the criminal group that attacked us” (qtd. in Murillo).

Mora explained, on a similar topic, that during his time as director of governance, in January 2020, Servicio Civil had been asked to create cybersecurity positions to start improving the country’s safety, “because it was seen, at least at the time I was in charge, as an immediate need to try to strengthen the sector” (2).[7] However, “by May 7, [2022] … I hadn’t heard anything on the news that talked about [the positions being created]” (2).

Recommendations and Conclusion

The analysis of the ransomware attack toward the Costa Rican government will help develop strategies for increased cybersecurity in the country, but can also be viewed as an example for other countries to adopt these same measures and tools, to lower the rates of cyberattacks in the world. These recommendations take into account the specific vulnerabilities in Costa Rica’s public sector, as they are critical to the order of the nation, but also incorporate findings from cybersecurity experts, on measures that can apply to the protection of any system. It is paramount that governments, institutions, and individuals begin a process of cultural transformation and awareness in data protection, as data has more value than individuals often realize. In a system where everything is connected, the actions of one person can affect a subsequent chain of successors.

The path toward cyber-immunity begins with the education system. As Díaz stated, “The incorporation of adequate cognitive skills in educational settings at all levels can be a first step

that nations should consider" (32). Teaching the population about the protection of personal data will make them better digital citizens; knowing which sites are prone to be infected with malware can prevent the institutions where these people work from being infected as well. In Costa Rican universities, there are few careers that include cybersecurity lessons and that is something that should change because technology is used for almost every job. Even in the early years of education, at schools and at home, it is necessary to teach children how to use technology safely. As Robles said, the behavior that is learned at home is the behavior that you will have at your job, and if you are not taught to care for digital safety, and you work, say, for the public sector, you will affect them (6).

Research findings on *Estado de la ciberseguridad en América Latina y El Caribe*, concluded that two-thirds of the percentage of cybersecurity incidents are by the human factor (33). Therefore, on an individual level, every citizen must be informed of protection methods for their personal information such as information backups, protection, and actualization in software that contain anti-viruses. Furthermore, each institution should also be held responsible for educating their employees on these safety measures as well as incorporating mechanisms for early detection of vulnerabilities and keeping a monitoring system for their networks.

Regarding legislation and policies, there is a need for regulation from the Costa Rican government. Robles explained, "there is a law in a paper [for data protection] but there is no one to execute it and there is no one that will make it count … that goes in line with the things that should start to happen in subsequent years" (6). He suggested that there should be a sanction for institutions if there is a data breach that results in the divulgation of sensitive data from their users (6). That would help incentivize prioritizing data protection. Mora also recommended that

the government develop norms and procedures such as monitoring centers and incident response procedures (10). He believes institutions in the country need to work together to prevent future attacks because if an institution undergoes a cyberattack and they do not report it, other organizations would not have time to prepare and protect their own systems from a similar situation (10).

Response procedures should inform each institution of a strategy to not only minimize the impact in the light of a cyberattack, but also inform other institutions to beware of the same vulnerabilities. Constant monitoring from a team that could involve both the private and public sectors in the country can help generate early alerts to avoid cyberattacks. As Mora concluded, "We cannot stop future attacks from happening … I think the issue is more complex and integral, the first thing I would say is that we should not be alarmed by this" (10). Establishing a network of collaboration allows a country's organizations to defend themselves with anticipation and at a higher scale (Díaz 32). Governments need to update the security to conform to cyberspace and once there is a system for defense and a team that communicates the strategies to the vulnerable sectors, order will be reinstated.

Notes

1. MICITT (Ministry of Science, Innovation, Technology and Telecommunications) is a state-run organization that regulates, promotes, and boosts the development of favorable conditions for research, innovation, knowledge, and technology, to contribute to the country's economic growth (MICITT).
2. CCSS (Costa Rican Social Security Fund) "is in charge of most of the nation's public health sector. Its role in public health (as the administrator of health institutions) is key in Costa Rica, playing an important part in the state's national health policymaking (Development Aid)."
3. MTSS (Ministry of Labor and Social Security) "[is] the leading institution in the socio-labor framework aimed at citizens, vigilant of decent work, equity, social justice and the protection of fundamental labor rights (MTSS)."
4. MEP (Ministry of Public Education) "is the governing body that guarantees the country's inhabitants the fundamental right to quality education, with equitable and inclusive access, with pertinent and relevant learning, for the full and integral formation of people and coexistence (MEP)."
5. Other attacks include adware, banking trojans, botnets, cryptominers, defacements, fraud, DDoS, point-of-sale malware, spam, web scripts, web shells, and worms (IBM 8).
6. White Jaguars is a company that provides services on offensive security, which includes vulnerability detection, everything related to the exploitation of systems, fraud detection, and others. This private company worked with the MICITT on the early detection of vulnerabilities, and avoiding their spreading to other institutions (Robles 1).

7. Servicio Civil (Civil Service) “is a legal-administrative system, created to attract and keep the most deserving personnel in the public service. It is constituted by a set of institutions, people, norms and philosophical, doctrinal and technical principles; established in order to guarantee the efficiency of the Public Administration, protect the rights of its servants and preserve an orderly and equitable relationship in the administration of public employment (Servicio Civil).”

Addenda

Figure 1: Affected institutions

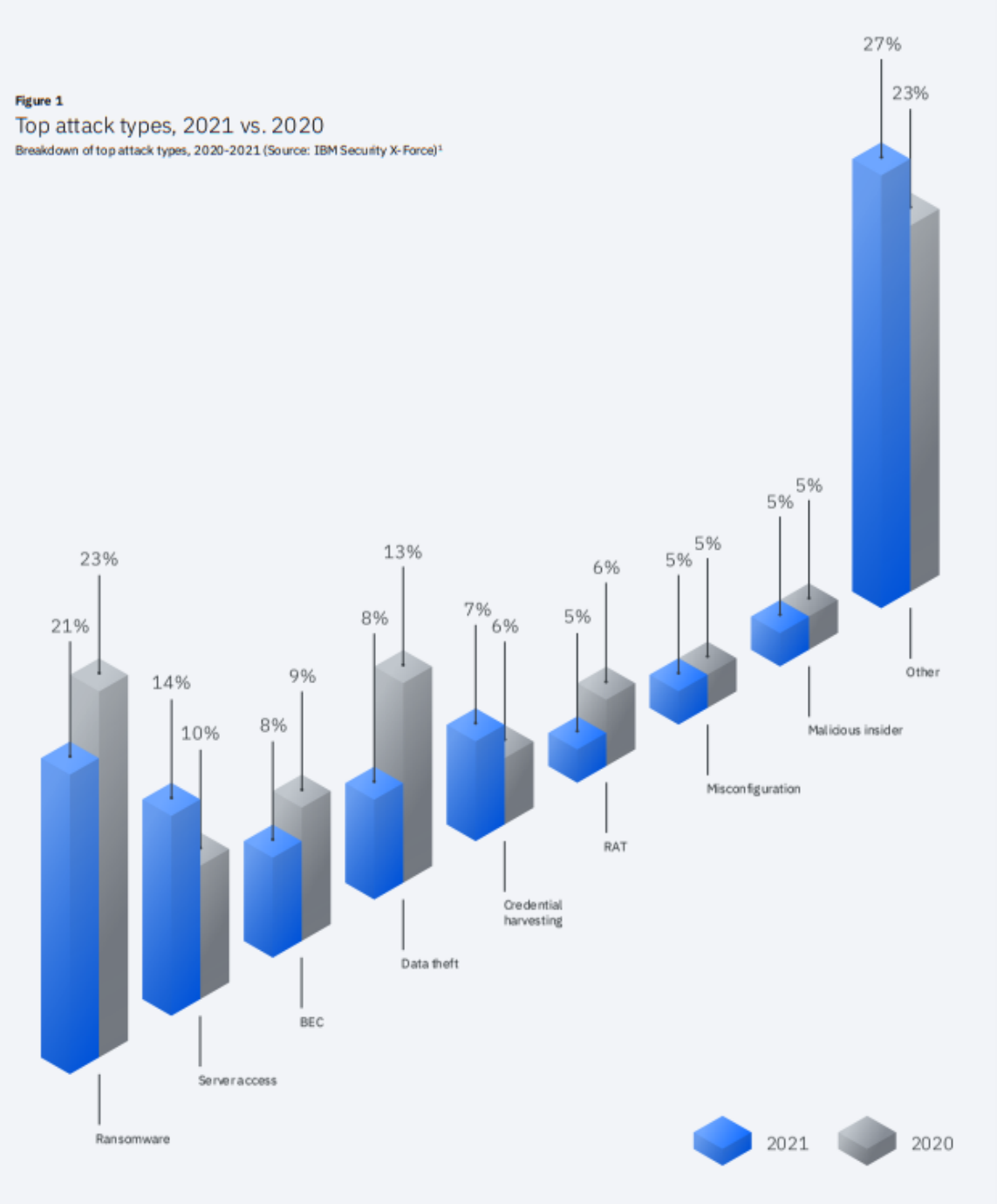
Instituciones afectadas por los Ciberataques

INSTITUCIÓN	FECHA	INCIDENTE
Ministerio de Hacienda	17 de abril	• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Cifrado de información • Afectación funcionalidad de sistemas informáticos
MICITT	18 de abril	• Defacement (modificación del sitio web) • Afectación de funcionalidad de sistemas informáticos
Instituto Meteorológico Nacional (IMN)		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación de funcionalidad de sistemas informáticos
RACSA		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación de funcionalidad de sistemas informáticos
Caja Costarricense del Seguro Social (CCSS)	20 de abril	• Robo de credenciales de RRSS • Ataque por medio de SQL inyección • Afectación de funcionalidad de sistema informático de Recursos Humanos de la CCSS • Exfiltración de información de una tabla con datos de bitácora, pero no datos sensibles
Ministerio de Trabajo y Seguridad Social (MTSS)	21 de abril	• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Cifrado de información • Afectación funcionalidad de sistemas informáticos
Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC)	23 de abril	• Cifrado de información • Afectación funcionalidad de sistemas informáticos
Sede Interuniversitaria de Alajuela (SIUA)		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación funcionalidad de sistemas informáticos
En las otras instituciones (Municipalidad de Golfito, Municipalidad de Turrialba, INDER, Municipalidad de Santa Bárbara, Municipalidad de Garabito, MEIC, Colegio Universitaria de Cartago, FANAL, Municipalidad de Alajuelita, CONAPE, Ministerio de Justicia y Paz) las medidas técnicas desplegadas logran detectar y contener el posible CONTI en sus sistemas.		

Fuente: MICITT, mayo, 2022.

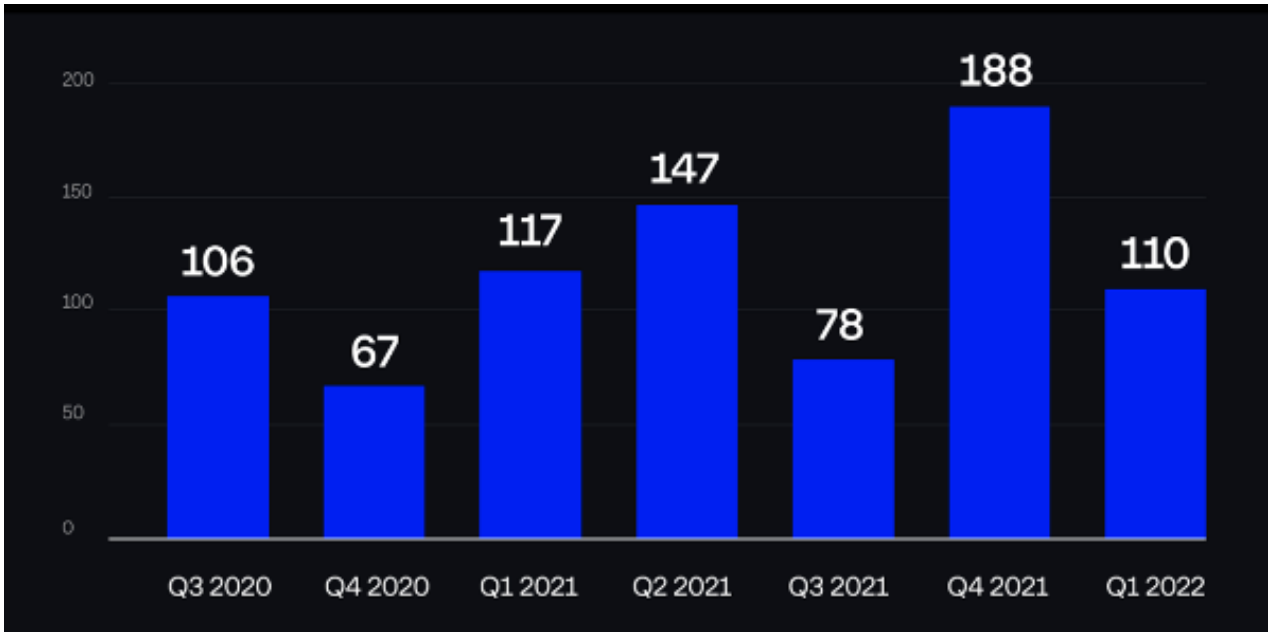
Data was gathered from Gobierno De La República de Costa Rica Comisión Nacional de Prevención De Riesgos y Atención De Emergencias' "Plan General de la Emergencia Ciberataques."

Figure 2: Top Attack Types, 2021 v. 2022



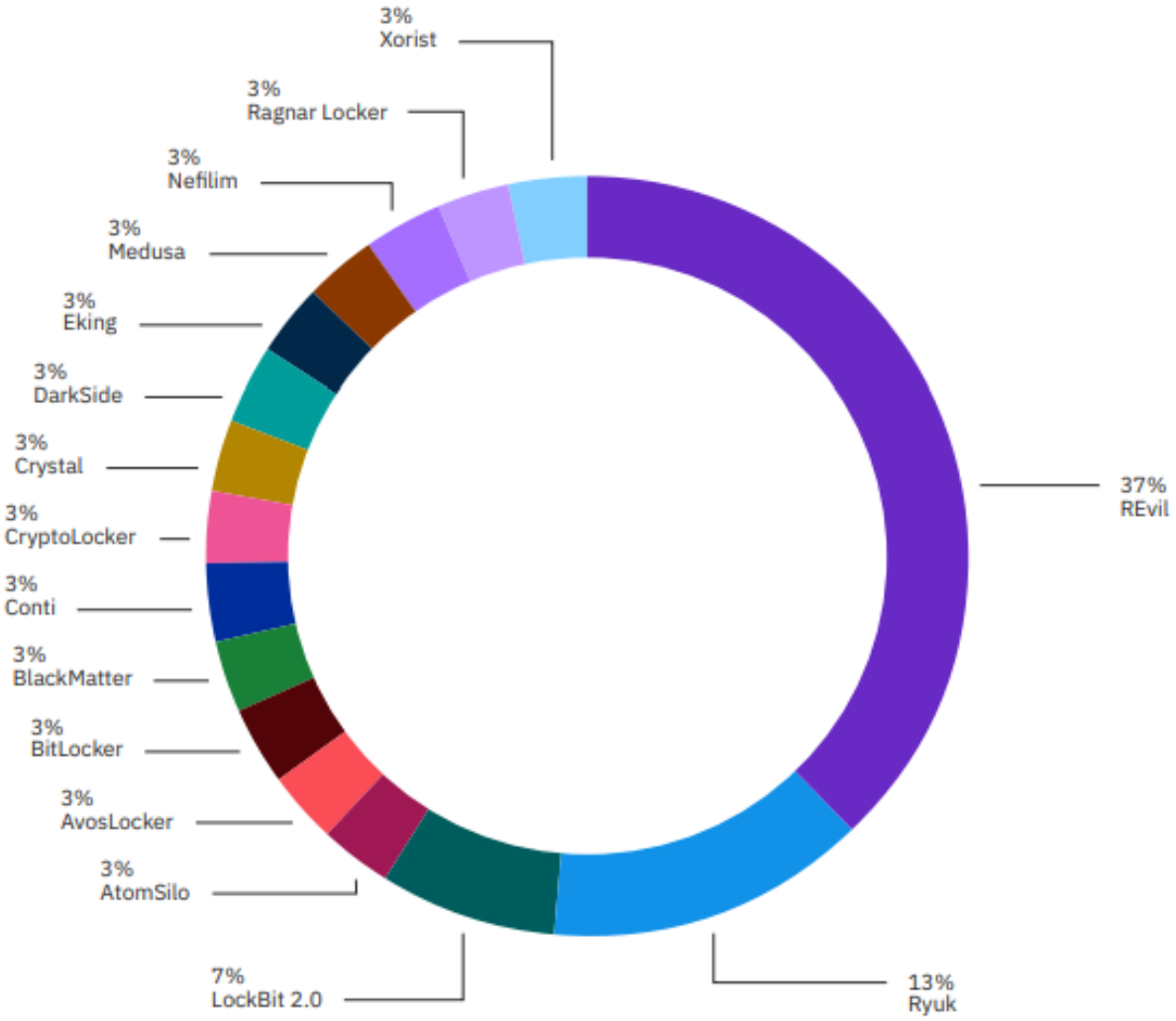
Data was gathered from IBM Security's "X-Force Threat Intelligence Index 2022."

Figure 3: Number of Victims Posted on DLS by Conti per Quarter



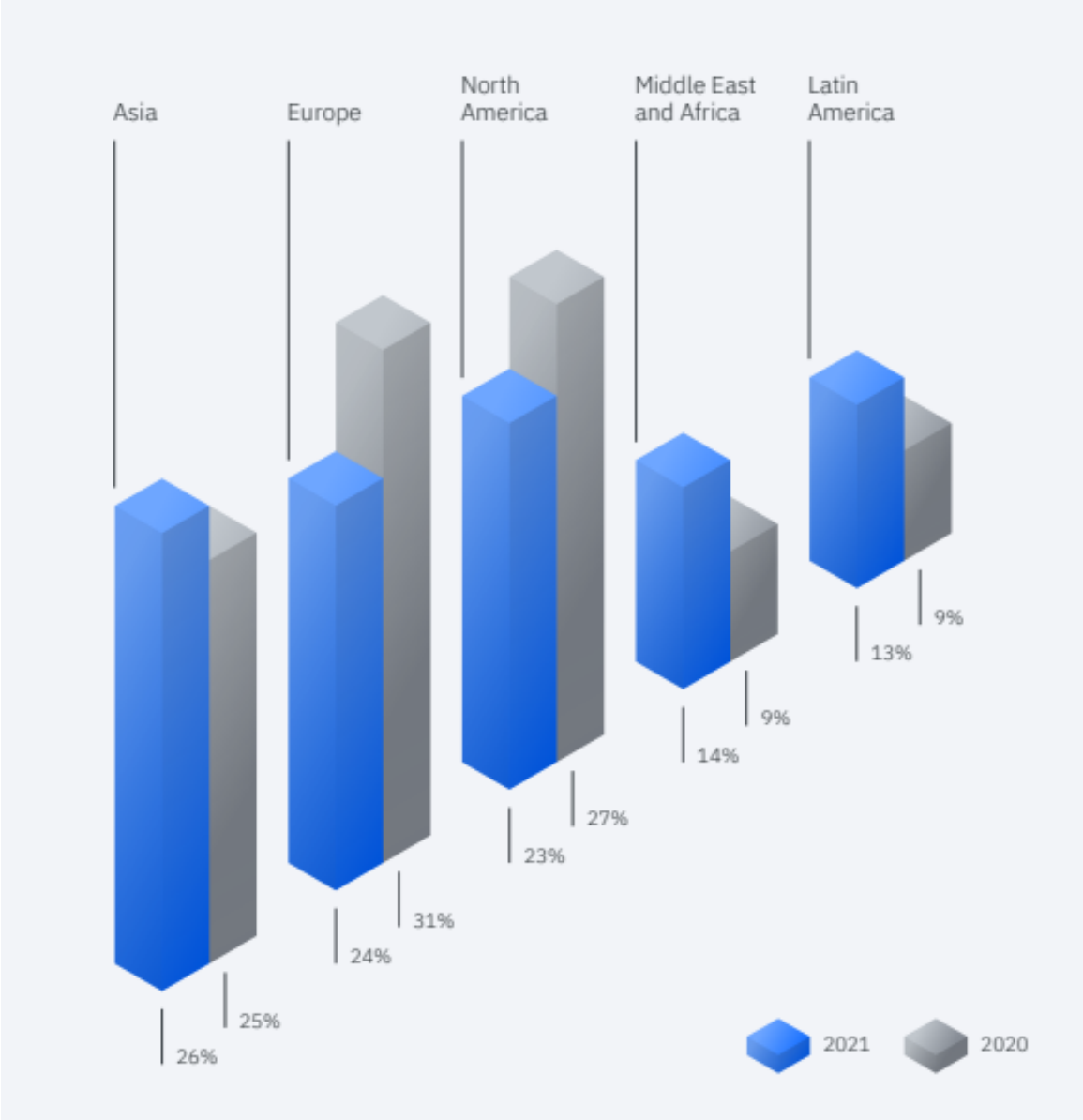
Data was gathered from Group-IB's "The Conti Enterprise: Ransomware Gang That Published Data Belonging to 850 Companies."

Figure 4: Types of Ransomware Observed in 2021



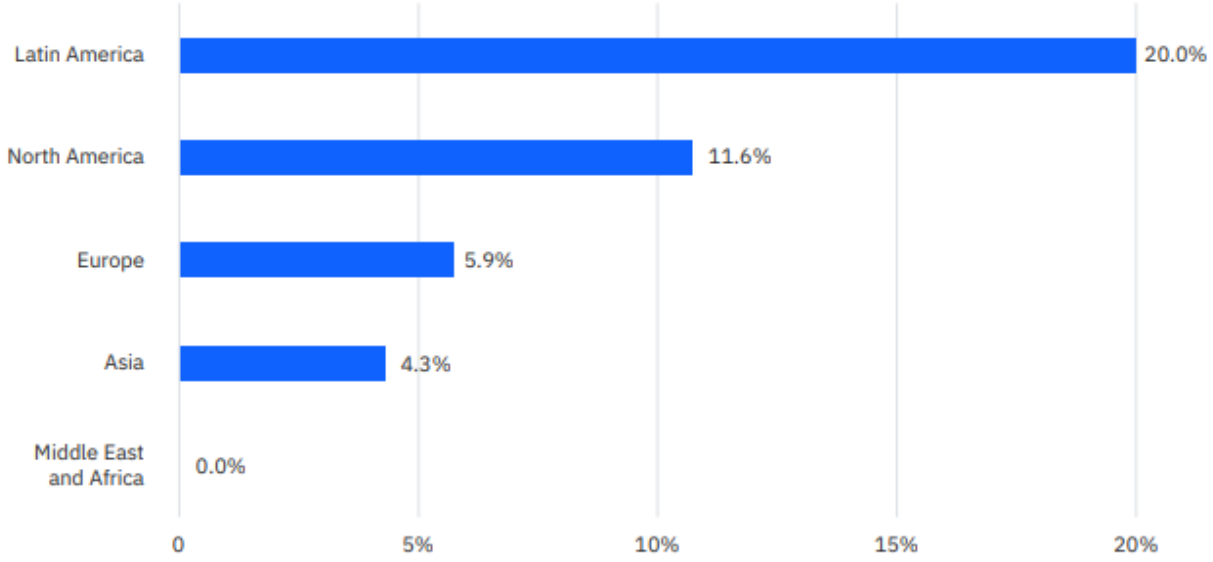
Data was gathered from IBM Security's "X-Force Threat Intelligence Index 2022."

Figure 5: Breakdown of Attacks by Geography, 2021 v. 2022



Data was gathered from IBM Security's "X-Force Threat Intelligence Index 2022."

Figure 6: Percentage of Incidents That were BEC, 2021



Data was gathered from IBM Security's "X-Force Threat Intelligence Index 2022."

Works Cited

Amerise, Atahualpa. *"Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia.* ["We are at war": 5 keys to understanding the cyberattack that has Costa Rica in a state of emergency]. BBC News Mundo, 20 May 2022. Web.

Burgess, Matt. *Conti's Attack against Costa Rica Sparks a New Ransomware Era*. WIRED UK, 12 June 2022. Web.

Carlini, Agnese. *Ciberseguridad: Un Nuevo Desafío Para La Comunidad Internacional*. [Cybersecurity: A New Challenge for the International Community]. Instituto Español De Estudios Estratégicos. 4 July 2016, pp. 1-16. PDF.

Conti Ransomware Attack Throws Costa Rica into a National State of Emergency. SANGFOR, 28 June 2022. Web.

Development Aid. *Costa Rican Social Security Fund (Caja Costarricense de Seguro Social)*, 14 June 2022. Web.

Díaz, Rodrigo, M. *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* [State of cybersecurity in logistics in Latin America and the Caribbean]. Repositorio CEPAL, 2021, pp. . PDF.

El Ransomware Ataca a Costa Rica: ¿Cómo Prevenirlo En Las Organizaciones? [The Ransomware Attacks Costa Rica: How to Prevent In Organizations?]. Revista Summa, 14 July 2022. Web.

Fernandez, Ileana. *Conti Group Hacking Affects Costa Rican Teachers*. The Tico Times, 20 May 2022. Web.

—. *Costa Rica Disables Servers Due to Cyber-Attack Threat*. The Tico Times, 21 July 2022. Web.

Gamón, Vincente. *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad.* [Internet, the new era of crime: cybercrime, cyberterrorism, legislation, and cybersecurity]. Revista Latinoamericana de Estudios de Seguridad. 26 April 2017, pp. 80-93. PDF.

Gobierno De La República de Costa Rica Comisión Nacional de Prevención De Riesgos y Atención De Emergencias. *Plan General De La Emergencia Ciberataques.* [General Cyber Attack Emergency Plan]. June 2022, pp. 1-32. PDF.

Harding, Emily, and Harshana Ghoorhoo. "The Core Issue." *Hard Choices in a Ransomware Attack*, Center for Strategic and International Studies (CSIS), 2022, pp. 1–4. *JSTOR*, PDF.

Harkins, Malcolm, and Anthony M. Freed. "The Ransomware Assault on the Healthcare Sector." *Journal of Law & Cyber Warfare*, vol. 6, no. 2, 2018, pp. 148dia–64. *JSTOR*, PDF.

Largest Cyber Attack in the History of Costa Rica: Does the State of Emergency Continue? International Network of Privacy Law Professionals (INPLP). Web.

MEP. *Marco Filosófico*. [philosophical framework]. May 8 2023. Web.

Mora, Jorge. Personal interview with the subject. Berkeley Academy, March 17 2023.

MTSS. *Visión y Misión.* [Mission and Vision]. January 1 2023. Web.

Murillo, Erick. *Especialista: A UN año de los ciberataques, "No se sabe qué fue lo que pasó."* [Specialist: ONE year after the cyberattacks, "It is not known what happened"]. Crhoy, 10 April 2023, Web.

MICITT. *"¿Qué Es MICITT?"* [What is MICITT?]. Ministerio De Ciencia Innovación Tecnología y Telecomunicaciones (MICITT), Web.

Robles, Mario. Personal interview with the subject. Berkeley Academy, March 09 2023.

Servicio Civil. *¿Qué es el Régimen del Servicio Civil?* [What is the Civil Service Regime?]. March 2023. Web.

The Conti Enterprise: Ransomware Gang That Published Data Belonging to 850 Companies. Group-IB, 23 June 2022, Web.

Vanci, Marianella. *Emergencia Nacional En Costa Rica Por Ataque De Ransomware*. [National Emergency in Costa Rica for Ransomware Attack]. CriptoNoticias, 11 May 2022, Web.

Wadhwani, Sumeet. *Conti Ransomware Gang Shuts Shop amid Attack on Costa Rica. Spiceworks*, 20 May 2022. Web.

Whittaker, Z. *Conti Ransomware Gang's internal chats leaked online after declaring support for Russian invasion.* TechCrunch, 28 Feb 2022, Web.

X-Force Threat Intelligence Index 2022. IBM Security, Dec. 2021, pp. 1-59. PDF.