2023

White paper series
Issue 10

Challenges and Strategies:

Considerations on Ransomware Attacks in the Americas

OAS More rights for more people

aws

Credits

Luis Almagro
Secretary General of the Organization of American States (OAS)

OAS Technical Team
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Mariana Jaramillo

AWS Technical Team
Abby Daniell
Melanie Kaplan
Camilo Gonzalez
Arturo Cabañas
Jordana Siegel

Editor
Jeimy Cano

Table of Contents

Definitions

Botnet (The word botnet comes from "robot network")
This is a network of infected computers (via malicious code) that are controlled remotely and can be forced to send spam, spread malware, or carry out a DDoS attack, all without the device owner authorization[1].

Useful Load (Payload)
Part of malware (malicious code) that performs the adverse or harmful action on the target system, after having made a successful intrusion.

Cyber Hygiene
This is the adoption of a security-focused mindset and daily usage habits that help individuals and organizations mitigate potential online breaches[2].

Data Encryption
Any procedure used in cryptography to convert plaintext to ciphertext, in order to prevent anyone other than the intended recipient from reading said data[3].

Backup Copy
A copy of the files and/or programs, made to facilitate recovery, if required[4].

DDoS
A service-blocking technique employed when numerous computers carry out an attack[5].

Doxing
The action or process of searching for and publishing private or identifiable information about a particular individual on the internet, typically with malicious intent[6].

Malicious Link
A malicious link is a link that leads to a fraudulent site. It usually consists of a connection that appears to lead to a legitimate website but is actually a fake website[7].

Information Exfiltration or Information Leakage
This is the illegal copying, transfer, or recovery of data or information from a server that ends up in the hands of an unauthorized third party.

Malware
A program inserted into a system, usually via covert means, with the intent to compromise the confidentiality, integrity, and/or availability of a victim's data, applications, or operating system, or to cause disruption to the victim[8].

Ransomware
This is a type of malware that typically hijacks and encrypts files on a storage system, then demands a ransom, usually through cryptocurrency payments, with no guarantee that all files can be decrypted or returned in their original condition.

1 https://www.avast.com/es-es/c-botnet (link in Spanish)
2 https://www.kaspersky.es/resource-center/preemptive-safety/cyber-hygiene-habits
3 https://csrc.nist.gov/glossary/term/encryption
4 https://csrc.nist.gov/glossary/term/backup
5 https://csrc.nist.gov/glossary/term/ddos
6 Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. ESET. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/
7 https://www.mundopc.es/links-maliciosos-como-detectar-una-url-fraudulenta-484.html (link in Spanish)
8 https://csrc.nist.gov/glossary/term/malware

Introduction

Recent news from various reports, issued by both information security technology providers as well as law enforcement agencies, report that **"ransomware"**[9] has become one of the most relevant risks and threats to global security, not only due to its versatility and capacity for action, but also because of its expansion and impacts, both financial and reputational, at the organizational level (Interpol, 2020). Within this context, the digital threat known as ransomware becomes a relevant point of reflection for both the public and private sectors.

When an organization is affected by ransomware, a key question arises: ***When an organization is affected by ransomware, a key question arises: "How should we respond to and mitigate a ransomware security event?"***[10], In both the public and private sectors, this question creates tensions of varying magnitudes, as well as implications on attributing responsibility within an organization. It also implies certain considerations, such as revealing detractors to cybersecurity investments, as well as countless implications – collaterals that commonly fulfill the adversary's purpose to create confusion, confrontation, and the responsibility game, thus allowing them more time for action and positioning during critical moments, which in turn enables them by extension to motivate payment, which is their ultimate goal. Therefore, both the public and private sectors must mitigate ransomware's impact on data and reputation during a ransomware event that can present uncertainty on its handling and on whether to respond to the ransom demand.

When an organization's executive level is informed of a ransomware event, a common first response is to question what type of information has been compromised and then, to request technical explanations on how this security event impacts operations, as well as any potential legal implications that this entails and whether said information is subject to legal protections. With this data, organizations usually try to establish, via all those involved internally, an overview of what has happened and then define a basic position for action, in response to ransomware.

In certain situations, these security events can severely affect organizations. For example, data extortion is a type of cybercrime based on the adversary's developed intelligence, deception, and distraction, and which is linked to a pattern of behavior based on the needs and expectations of individuals. In this sense, by identifying what may be of interest to the target of a ransomware attack – for example, an expected promotion, granting a bonus, paying a fine, or a call from the police, among others – and linking it to the dynamics of the current context (the specific context that the target experiences, based on their expectations), adversaries are able to make their actions mimic a specific social context to thus approach their potential victims without their noticing.

9 Definition, page 1.
10 International best practices currently suggest not paying. Refer to The European Union Agency for Cybersecurity (ENISA) Landscape for Ransomware Attacks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

In part, unauthorized users' success is due to a target's lack of understanding on security controls that govern technical services. If, in addition to the above, targets are identified to have low IT hygiene – this is commonly referred to as *cyber hygiene* – within the digital context, as well as a naive trust in available media and technologies, then this, paired with an increase in the digital products and services deployed with limited security and control measures, presents aggressors with the ideal mobilization scenario to achieve their actions and plans with little margin for action.

This publication seeks to provide recommendations and reflections based on international best practices for decisionmakers at public and private sector organizations, regarding both the reality of a ransomware attack and its implications, to illustrate the process that occurs during an event and thus, provide spaces to examine how to address this challenge, what margin of action can be achieved, and how to discover certain patterns that indicate a possible evolution of this type of threat within an organization.

Data Hijacking: What Happens at an Organization?

Data hijacking deprives a person or organization of one of their most important assets: data and information, whose hijacking currently represent a direct affront that endangers the rights and prerogatives of organizations and human beings in their free performance in social dynamics. The hijacking of data, and then its subsequent extortion by third parties, comprises a criminal action that, in due course, must be addressed by all jurisdictions and through legislative actions to be incorporated into national and international legal systems. (Grimes, 2022).

When an organization is affected by a ransomware event, dilemmas arise and typically, there are few legal maneuvers that can be activated in an attempt to contain any possible adverse effects. (Leo et al., 2022).

On the one hand, an organization can deploy cybersecurity policies, which, according to their scope and exclusions, can support entities in confronting this challenge. On the other hand, the organization can engage in negotiations with an attacker who has captured the data, with the knowledge that, even if they have a way to restore the information, it is likely that they will not be able do so. However, it is important to emphasize that international best practices and recommendations do not advocate negotiating with an aggressor.[11] The choice to pay is not an option recommended by best practices in the treatment of ransomware (and is openly illegal in certain national and international jurisdictions). Any conventional actions taken will result in making the organization more resilient to the occurrence of ransomware, without prejudice to the fact that at some point, an adversary may succeed. Additionally, these types of actions must be adjusted to a legal framework (with the exception of extortion payments), which, in turn, will give executives peace of mind in their compliance and reporting frameworks to control entities.

Finally, informing and involving the competent authorities[12] during an investigation can help provide information on the threat, to then use different strategies to find the attacker, disable the encryption mechanism, and utilize diplomatic channels,[13] if applicable, and so on, thus adjusting to the standards established by law. These are just some of the ways in which you can choose to address a data hijacking event.

11 https://www.nomoreransom.org/en/ransomware-qa.html
12 Supervisors for a particular sector, police authorities or law enforcement.
13 When compromised data has been is found or transferred to other countries and jurisdictions, and it is necessary to use diplomatic channels to coordinate police and judicial actions to advance the actions to recover or eliminate the information.

Ransomware takes information security professionals, corporate lawyers, and decisionmakers out of their comfort zones, given that whether the compromised information or data is subject to specific protection and due care conditions, the method of response to the situation must be clearly established for the various affected interest groups. Consequently, the affected organization will be subject to a crossroads where it will be evaluated based on its security measures, privacy practices, and standards of control, and how these have been developed and applied. On the other hand, there are also legal tensions, and their respective sanctions (generally economic), to contend with, which can end up impacting the organization's reputation in its field or industry.

This issue of addressing a ransomware attack goes beyond the technological phenomenon of its occurrence; it entails enabling a systemic examination of any problems connecting security practices, institutional relations, legal frameworks, insurers, technological vulnerabilities and, above all, human behavior (Sittig & Singh, 2016).

> Ransomware takes information security professionals, legal departments, and decisionmakers out of their comfort zones. To be resilient, it is important for each organization to have a proactive plan to respond to an emerging situation – for example, by following the NIST preparedness process.[14]

14 Ransomware | NIST

Ransomware Materialization: Two Sides of the Same Coin

The actions that follow a data hijacking event have a specific type of motivation (not always economic) and lead to either direct or indirect contact with the victim's interest groups, to initiate a game of pressures and tensions that seek to break down the affected party. For this, survival tests, threatening calls, and visible manifestations (photos, symbols, or belongings) to create uncertainty serve as fundamental pieces to create need and stimulate the necessary actions that lead to fulfilling the aggressor's objective.

In the digital world, ransomware has at least two views today. Hijacking information or data (generally, sensitive data), for which a ransom must be paid (based on the threat that not doing so will incur its destruction or disappearance); and access to sensitive or compromising information that may be exposed (and possibly affect reputation), if the digital criminal does not receive payment (Baykara & Sekin, 2018). In both cases, criminals will seek to provide evidence to their victims that the threat of any of these actions is real and serious, for which actions are carried out to intimidate and create pressure, including visible countdowns, modified voice messages to intimidate organizations or individuals, and means of contact based on anonymous or burner email accounts. When analyzing the occurrence of a ransomware event, it is necessary to evaluate both sides of the coin: the organization (or person), as well as the attacker.

On the individual or organizational side, analyzing the possible materialization and scope of damages on behalf of a ransomware attack may include the following aspects:

- Level of assurance in security and control practices;
- Level of refinement and use of available security and control technologies;
- Evidence and lessons learned from evaluating and monitoring recovery and business continuity plans;
- Analysis of browsing behavior and internet usage;
- Development level of the organization's or individual's information security culture (including personal cyber hygiene);
- Prospective analysis of latent and/or emerging risks relevant to the organization's industry, within the context of its operations and strategies; and
- Defining business (or personal) risk appetite[15] (Herrera Silva, Barona López, Valdivieso Caraguay & Hernández-Álvarez, 2019).

15 The share of risk that an organization is willing to accept and bear in achieving its mission/vision. Source: Quinn et al. (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. NIST. NISTIR 8286A. https://doi.org/10.6028/NIST.IR.8286A

Any deficiency or result that does not correspond to that expected from each of these above-mentioned elements will be associated with a limited risk management capacity, for both an organization and an individual, in view of the due care that must be taken to protect the information or data in its charge or of its property. Additionally, negligence could also be deduced and then verified via audit exercises or independent verification.

From the aggressor's perspective, analyzing capacities and support available to them, in or to achieve their objectives, may include, among other things, the following:

- Level of specialization and ability to develop intelligence;
- Specific motivations that lead to action(s);
- Use of known or specialized tools;
- Connections with other criminal groups;
- Payments based on cryptocurrencies, or monetization in other ways;
- Previous patterns of action; and
- Background information available at the national or international level (Cano, 2020).

Any information to be considered, based on the above list, will offer orientations and clues to follow the attacker's trail. Each of these will help shape the puzzle that involves connecting the offender's various actions, in order to find consistent patterns that give clarity to reconstruct a criminal action and thus, in the best of cases, pinpoint the attacker's location and achieve their capture. This is not always accomplished, and therefore, the more reliable and relevant the information that can be obtained, the better the maps that can be drawn over the uncertain territory that the adversary poses (El-Kosairy & Azer, 2018).

In the digital world, ransomware has at least two views today: *Information or data hijacking* (generally, sensitive data), for which a ransom is demanded (based on the threat that not doing so will proceed to its destruction or disappearance); or access to *sensitive or compromising information* that may be exposed (and possibly affect reputation), if there is no payment to the digital offender.

Recommendations/Best Practices Against a Ransomware Attack: *Conventional Ideas*

When an organization suffers a ransomware attack, it must consider both sides of the equation, and not focus only on the damage that it creates internally, to include the natural consequences that this entails from the standpoint of individual and collective responsibilities; it must also consider the possible impact on individuals within the organization.

Various agencies provide information to better equip organizations to handle these incidents. In this sense, certain conventional actions are proposed for organizations or individuals to apply when data hijacking and extortion has taken place. For example, in the case of the United States, the Federal Bureau of Investigation (FBI) encourages organizations to report rescue incidents to the police. The Internet Crime Complaint Center (IC3) accepts online reports of Internet crime, either from the actual victim or from a third party to the complainant, and will work with them to determine the best course of action for the future. In this case, the following information is essential to proceed:

1. Any relevant information deemed necessary to support the complaint;
2. Email header(s);
3. Financial transaction information (account information, transaction date(s) and amount(s), recipient details, etc.);
4. Name of the subject, address, telephone, email, website, and IP address;
5. Specific details regarding how the victim has been affected; and
6. Name, address, telephone, and email address of the victim.

The following recommendations are provided, based on currently available international best practices[16] :

• Hire or seek specialized services to restore any data that has been compromised. These types of services are expensive and involve the use of specific tools that attempt to find patterns and establish alternative methods of accessing data; note that this desired result is not always achieved.

• Contact security and control tool providers, or their contacts, to establish alternatives that allow for finding ways to recover the information (or part of it). Typically, this option generates discrete successes; there exist associated research centers that can contribute in this regard.

• Use any information backups that the organization or individual has, which generally do not respond to a systematic and/or validated practice. This strategy usually works partially, since updating the supported information defines the level of scope and maneuverability that the organization or individual can have. The use of this information as a form of recovery may create deficiencies and differences when used, since it depends on the reliability of the storage media used, the support technology to create backups, and the strategy used: daily backups, incremental or full backups, or cloud storage usage.

• Develop and update the business continuity plan, which extends to any information subject to legal protections (as a top priority, for example, any databases that store personal information) to maintain due care and regulatory compliance with a sector's supervisory agency(ies) at the national and international levels.

• Keep the data encoded (encrypted while not in use) via the storage media established by the organization/person (for double extortion cases: exfiltration and encryption).

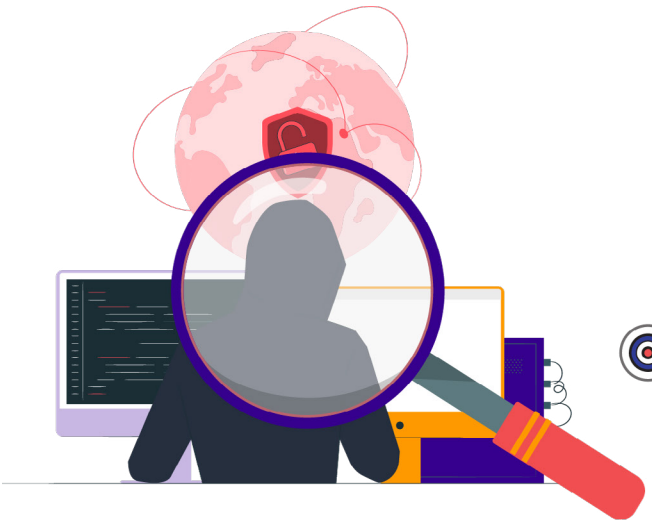
• Apply critical patches or adjustments, released by vendors, to programs or operating systems available to the organization and/or the individual.

• Ensure periodic training and simulation for individuals regarding the strategies used by attackers to create deceptions and motivate actions that enable ransomware materialization.

• Encourage people to report suspicious behavior on the devices they use (for example, disabling services, rebooting, and antivirus system alerts, among others).

16 U.S. Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov/stopransomware/ransomware-guide
The European Union Agency for Cybersecurity (ENISA) Landscape for ransomware attacks - https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
Australian Cyber Security Centre (ACSC) - Ransomware Attacks Emergency Response Guide - https://www.cyber.gov.au/sites/default/files/2021-07/11515_ACSC_Emergency-Response-Guide_Accessible_08.12.20.pdf

Case Study: Guacamaya and Conti: *Threats Present in the Region*



Considering the previous analyses carried out around ransomware, it is important to recognize and analyze the possible adversaries behind these actions. In this sense, a brief characterization of two case studies – and the impacts of their actions throughout the region – are described below.

GUACAMAYA

According to Vicens (2022), Guacamaya is a group of Central American activists whose main goal is to infiltrate mining and oil companies, the police, and various Latin American regulatory agencies to reveal general injustices and criminal offenses against the population, the local region, and the planet. They openly criticize "U.S. imperialism" and its aggression against the peoples of the Americas.

This hacktivist group targets governments, states, military, and extractive entities to allegedly motivate greater information transparency regarding governmental or institutional initiatives and, thus, provide citizens with details that have not been directly disclosed.

The group's primary mode of operation is to identify common or typical vulnerabilities in the infrastructure at target institutions, such as failures to update or configure an operating system or specific applications; these are then exploited to gain privileged access to information residing on technological devices, which information they then reveal and publish to various publicly accessible media. Additionally, they have a web portal[17] where they keep a record of their actions and statements.

Among its most notable actions are attacks on the public sector in Chile, Mexico, Peru, El Salvador, and Colombia, where, due to this ransomware attack, sensitive information from governments, military institutions, and extractive sector companies was revealed.

17 https://enlacehacktivista.org

CONTI

Unlike the Guacamaya group, CONTI is a transnational organized crime organization that allegedly originates in Russia. They were first detected in 2020 and are believed to be the successor to the Ryuk ransomware group. According to Chainalysis (2022), this ransomware group was the top-grossing group in 2021, with estimated revenues of at least $180 million.

According to Tavella (2021), CONTI usually uses the double extortion modality, also known as doxing, which consists of exfiltrating confidential information from their victims prior to encryption, and then extorting them by threatening to publish exfiltrated information unless paid the amount of money demanded. In this way, they increase pressure, since it's not only about recovering the encrypted files, but also about avoiding a possible information breach that could harm the victim in various ways.

CONTI's modus operandi extends to the following activities:

- Phishing campaigns with malicious attachments;
- Recruiting internal personnel from an affected company to solidify and expand their illegal activity;
- Exploiting known vulnerabilities on internet-connected exposed computers; and
- Attacks on computers with the "Remote Desktop Protocol – RDP" service)[18].

The CONTI criminal group works like any company in the world: It has multiple departments, from human resources and administrators to coders and researchers. They have policies regarding how hackers should process their code, and as a counterpart, best practices for keeping group members hidden from law enforcement (Burguess, 2022).

CONTI has been involved in numerous high-profile attacks, including those against the City of Tulsa, Broward County Public Schools, and Advantech in the United States of America. However, it wasn't until they attacked Ireland's Health Service Executive (HSE) and the Department of Health (DoH), knocking out the country's computer systems for weeks, that they gained notoriety (Abrams, 2022).

CONTI has recently been operating in Latin America where its most recent action, revealed by the international media, was the attack carried out on April 12, 2022, against the databases of the Costa Rican Ministry of Finance and other public institutions throughout the country, which led to the declaration of the "State of National Emergency for the entire public sector of the State of Costa Rica," in accordance with the provisions of Decree No. 43542-MP-MICITT on May 8, 2022.

As can be seen, both Guacamaya and CONTI form specific threats to stability in the region, given that their strategies and methods, although they vary in their manner of achieving objectives, are based on a limited application and assurance of best practices and standards in cybersecurity/security at the business and state levels, thus demanding the development and creation of joint capacities to strengthen a vigilant posture that allows not only for response, but also for deterrence, delay, or confusion of these adversaries.

18 Protocol that allows a remote user to have full access to a device, so that they can move the mouse and use the keyboard as if they were in front of the computer.

A summary on these two groups can be seen below:

Characteristics	Guacamaya	Conti
Fundamental Behavior	Hacktivist	Organized Crime
Origin	Allegedly, Central America	Allegedly, Russia
Techniques Used	Exploiting equipment vulnerabilities: update or configuration failures in operating systems or specific applications.	Phishing via attached malicious files or documents, exploiting known vulnerabilities, attacking equipment via access to the remote desktop protocol, cracking passwords.
Focus Area	Military intelligence, government entities, national security, mining and extractive companies.	Government entities or key companies that affect the citizenry and a country's dynamics.
Organization	Group organized and centralized around a common cause – supposedly, social wellbeing and national interests.	Decentralized group of operation on a global scale, with goals both economic and linked to extortion.
Objective	Greater transparency in government and extractive/mining company information.	Uncertainty, instability, chaos, and economic gain.
Philosophy	Hacking as a means of resistance.	Hacking as a means of creating political instability and turning a profit.
Desired Result	Exfiltration of sensitive data.	Contain, exfiltrate, and encode data to secure payment.

Table 1. Description of Guacamaya and Conti

Conclusions

Ransomware is a form of organized crime that results from the digital transformation of crime over the last 10 to 15 years, when it began with the issue of *botnets* (see definitions, at start). The ability to control a computer without the victim knowing it is one of the most relevant expressions and motivations experienced by attackers in carrying out criminal actions based on possible anonymity or the lack of traceability that this can create. (Kardile, 2017).

Current aspects of digital crime include: i) maximum anonymity with minimum evidence, ii) maximum legal ambiguity with the minimum available technological knowledge, and iii) maximum effectiveness of their actions with minimum effort, thus establishing an economy of cybercrime that enables development of sufficiently sophisticated technical, social, and intelligence capabilities to increase the level of uncertainty in people, organizations, and countries, and thus motivate lucrative illegal actions that can pass under the radar of official authorities (Interpol, 2020).

Before a person or organization becomes a ransomware victim, they should consider their action strategies to clearly and holistically establish the most appropriate response to limit the adverse effects of this condition as far as possible, for which it is necessary to apply best practices and maintain a permanent exercise of practices and simulations that create “procedural and practical memory” to act in a coordinated manner and that limits the adversary’s agenda: to generate confusion, instability, and uncertainty in the victim.

Appendix

List of Internet Resources Available to Fight Ransomware

Given the accelerated evolution of ransomware at the international level, a set of certain resources available via Internet is detailed below; these can serve to provide support and guidance for decisionmakers' consultation and review, to act in a coordinated and focused manner amidst the tensions that this type of event generates.

- Allianz Global Corporate & Specialty (AGCS) (2021). Ransomware trends: Risks and Resilience - https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

- Cybereason (2022). Ransomware. The True Cost to Business 2022. A Global Study on Ransomware Business Impact - https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

- Institute for Security and Technology (2022). Blueprint for Ransomware. Defense. An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises - https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf

- ThreatPost (2021). 2021: The Evolution of Ransomware - https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf

- NIST (2020). Data Integrity: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11 - https://www.nist.gov/news-events/news/2020/09/data-integrity-recovering-ransomware-and-other-destructive-events-nist

Relevant Statistics on Global Ransomware

Multiple reports at the international level demonstrate the challenges and implications of extortion with data, thus indicating the need to move forward and specify strategies that allow for it to be identified and treated in the most appropriate way to limit the damage that its occurrence may cause. In this sense, Gartner[19], in discussing emerging risks in 2022 (Cohn, 2022), first establishes the appearance of new ransomware models as the most important trend to have on the corporate radar, given that its permanent evolution and attackers' ability to transform their extortion practices warn of new alternatives and adaptations on this theme.

On the other hand, the website *Cybersecurity Ventures* (2021), in its most recent report on extortion with data, presents a statistic that establishes the fact that, by 2031, a ransomware attack will materialize in a business, consumer, or device every two seconds, thus implying an acceleration compared to the every 11 seconds calculated in 2021. This data represents a permanent alert and vigilance exercise that, correlated with that established by Gartner, requires differential and specific treatment, given this threat's high probability of success.

19 An information technology research and consulting company based in Stamford, Connecticut, United States.

Other recent reports (Coverware, 2022) indicate marked attack vectors used by cybercriminals, such as phishing, software vulnerabilities (some known or unpatched, such as the one associated with WannaCry[20]), and the use of the *Remote Desktop Protocol* (RDP), which configures a basic strategy to specify the kind of unauthorized access required to plant malicious code and proceed with its execution. It is important to note that an attacker requires a victim's action to initiate the process; therefore, to the extent that a victim becomes more resistant to deception, an adversary must spend more time to achieve their goal.

When an organization has been a victim of ransomware, its direct effects are distributed over at least five themes (SpyCloud, 2022):

- Exposure of proprietary or sensitive data;
- Damage to reputation;
- High effort in the recovery and restoration of operations;
- Loss of customers or their satisfaction due to operational failures; and/or
- Disruption of services and/or critical infrastructure.

Whatever the impact, organizations are exposed and customer trust is affected, thus creating a spiral of loss of credibility and control that will end up affecting the entity's dynamics and its digital initiatives over the medium- and long-term.

Recently in Latin America and the Caribbean, significant exfiltration[21] and extortion[22] activity has been reported for data in the region, on behalf of two particular groups called "Guacamaya" and "Conti"; although these groups have different intentions and methods, both have created instability and financial losses in many countries throughout the region. Their actions directed against government entities, national defense entities, critical infrastructures, and mining-energy sector companies reveal a markedly aggressive agenda that seeks not only to attract attention, but also to carry out lucrative extortion deals to increase both their capabilities and profits.

> By 2031, a ransomware attack will hit a business, consumer, or device every two seconds, up from an estimated every 11 seconds in 2021.

20 A vulnerability is exploited in Microsoft's implementation of the Server Message Block (SMB) protocol. Server Message Block (SMB) is a network protocol that allows for sharing of files, printers, etc., between nodes on a computer network, using the Microsoft Windows operating system. Source: https://www.avast.com/es-es/c-eternalblue

21 See the definitions section.

22 Data or information hijacking, for which a ransom is requested, generally via payment in cryptocurrencies.

Ransomware Anatomy: Exploitability Level and Key Stages

From a practical point of view, extortion with data requires understanding the level of exploitability that a target organization has in the face of this type of threat. This requires knowing and identifying (Stallings, 2019):

- **Attack Vector:** The proximity of the attacker to the vulnerable component.
- **Attack Complexity:** The level of difficulty required for an attacker to exploit a vulnerability, once the target component has been identified.
- **Required Privileges:** The access level needed by an attacker to exploit a vulnerability.
- **User Interaction:** Indicative of whether a user, other than the attacker, must participate for the attack to succeed.

In this sense, for extortion with data to be successful, it is necessary for the person to participate directly – that is, for an individual to take a specific action on their computer or device, such as clicking on a malicious link (see section definitions), to create a base point that initiates the three key stages required to materialize said threat (Figure No.1)

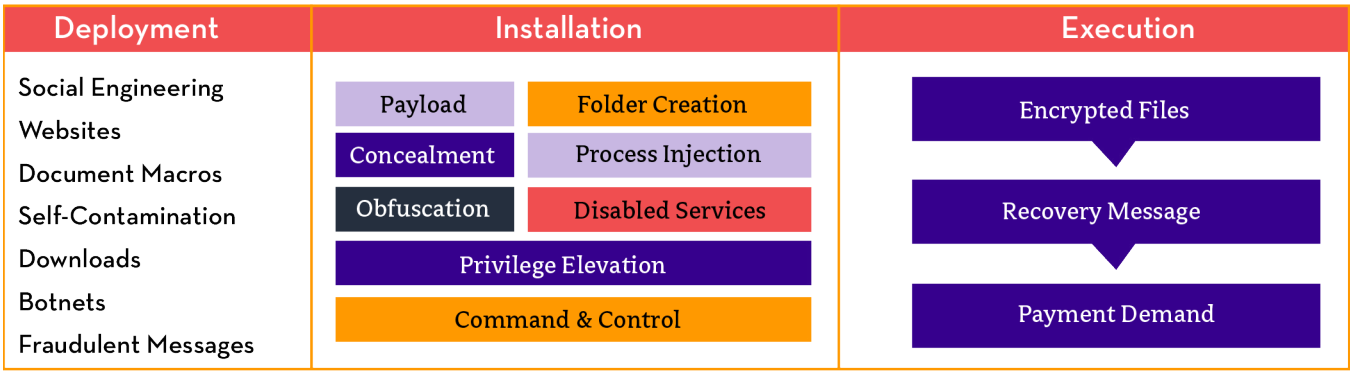


Figure 1. Anatomy of Ransomware (own creation, with ideas from Osorio et al., 2020)

The first stage is *deployment*, a process specified through the attacker's planned and designed effort and that begins with intelligence on information regarding individuals or a target community, to specify the interests and topics that are relevant to the social dynamics of the potential victims. Next, a *credible and reliable hoax* is developed to allow people to access a website, download documents, and access fraudulent messages without realizing their true nature. Finally, *distraction*, which implies taking advantage of people's inattention to carrying out an action that initiates a download or access of malicious code to mobile, laptop, or desktop equipment.

Once the malware download has been completed, ransomware installation begins. The *"payload"* is activated, which triggers a series of hidden events on the device, such as the creation of folders, concealment and obfuscation of malicious code, elevation of privileges in the target system, the injection of processes that mimic the operating system's standard process, and disabling monitoring and protection services, to finally prepare the compromised system for full command and control.

Once this stage is complete and the device has been prepared for adversary control and handling, two activities usually occur at the same time. One initiates exfiltration of any sensitive data that the adversary has managed to obtain and later, encryption[23] on the same on the device, which is developed via algorithms executed in parallel to achieve maximum efficiency in this process. Once the process is completed, an alert message is generated regarding the new condition of the machine and demand for payment is issued in exchange for recovering any information that has been compromised.

The literature establishes at least four (4) types of extortion that attackers can carry out, once the data is compromised (MunichRe, 2022):

- **Simple Extortion:** A payment request to return the encrypted data;
- **Double Extortion:** Theft and a threat of data publication;
- **Triple Extortion:** A threat to launch a distributed denial of service (DDoS) attack against the victim, in case of default on a payment; or
- **Quadruple Extortion:** An attack on the victim's suppliers, supply chain, and customers to exacerbate and create pressure for payment.

Since this type of illegal activity is a highly profitable business that generates an average of $1 billion a year (Chainalysis, 2022), the economic gains from this type of extortion are based on three fundamental aspects (Falco & Rosenbach, 2022, p.24):

1. Leveraging the sale of stolen data to interested third parties;
2. Threatening organizations with a cyber-attack or sensitive information leak; and
3. Ransom in which an organization is barred from accessing its data until the extortion is paid.

Whatever the type of extortion that takes place, the institution will feel the pressure and the demands that require it be accountable for any consequences created to its interest groups and, at the same time, to recognize the conditions and ability that the adversary has to achieve threat materialization and achieve its purposes: extortion and/or exfiltration.

The economic profits of ransomware are based on three fundamental aspects:
- Leveraging the sale of stolen data to interested third parties;
- Threatening organizations with a cyber-attack or sensitive information leak; and
- Ransom in which an organization is barred from accessing its data until the extortion is paid.

23 Encryption of information carried out by the adversary to prevent its owner from having access to the same.

References

Abrams, L. (2022). Conti ransomware finally shuts down data leak, negotiation sites. *Bleepingcomputer*. https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/

Baykara, M. & Sekin, B. (2018). A novel approach to ransomware: Designing a safe zone system. *2018 6th International Symposium on Digital Forensic and Security* (ISDFS), Antalya. 1-5. Doi: 10.1109/ISDFS.2018.8355317

Burgess, M. (2022). The Workaday Life of the World's Most Dangerous Ransomware Gang. *Wired*. https://www.wired.co.uk/article/conti-leaks-ransomware-work-life

Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. *Actas X Congreso Iberoamericano de Seguridad Informática 2020*. Universidad Politécnica de Madrid - Universidad del Rosario. Enero. Doi: 10.12804/si9789587844337.09

Chainalysis (2022). The 2022 crypto crime report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Cohn, L. (2022). The Cutting Edge: 2Q22 Cool New Data Points. *Gartner Business Quarterly. Second Quarter*. 5-8. https://www.gartner.com/en/insights/gartner-business-quarterly

Coverware (2022). Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

El-Kosairy, A. & Azer, M. A. (2018). Intrusion and ransomware detection system. *2018 1st International Conference on Computer Applications & Information Security* (ICCAIS), Riyadh. 1-7, Doi: 10.1109/CAIS.2018.8471688

Falco, G. & Rosenbach, E. (2022). *Confronting cyber risk. An Embedded Endurance Strategy for Cybersecurity*. New York, NY. USA: Oxford University Press.

Herrera Silva, J. A.; Barona López, L. I.; Valdivieso Caraguay, A. L. & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sens*. 11(10). 1-20. Doi: 10.3390/rs11101168

Interpol (2020). Cybercrimen: Covid-19 Impact. August. De: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Kardile, A. (2017). Crypto ransomware analysis and detection using process monitor. *Master Thesis*. University of Texas, Arlington. De: http://hdl.handle.net/10106/27184

MunichRe (2022). Global Cyber Risk and Insurance Survey 2022. *Global Report*. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

Osorio, A., Mateus, M. & Vargas, H. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*. 13(3). 131-142. doi: 10.18273/revuin.v19n3-2020013

Richard, L. (2022). "LA LUCHA POR UN TERRITORIO ES LA LUCHA DE TODAS". Forbidden Stories. https://forbiddenstories.org/es/la-lucha-por-un-territorio-es-la-lucha-de-todas/

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, 7(2), 624–632. Doi: 10.4338/ACI-2016-04-SOA-0064

SpyCloud (2022). Ransomware defense report. https://spycloud.com/resource/ransomware-defense-report-2022

Stallings, W. (2019). *Effective cybersecurity. A guide to using best practices and standards*. USA: Addisson Wesley.

Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. *ESET*. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/

Vicens, A. (2022). Hacking group focused on Central America dumps 10 terabytes of military emails, files. *CyberScoop*. https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

Grimes, R. (2022). *Ransomware Protection Playbook*. Hoboken, NJ. USA: John Wiley & Sons.

Leo, P., Isik, O. & Muhly, F. (2022). The Ransomware Dilemma. *Sloan Management Review*. https://sloanreview.mit.edu/article/the-ransomware-dilemma/

2023

White paper series
Issue 10

Challenges and Strategies:

Considerations on Ransomware Attacks in the Americas

OAS More rights for more people

aws