The Evolution of Ransomware

How the threat has expanded beyond data encryption to include leak-driven extortion, supply chain attacks, and a highly organized criminal ecosystem.

///AXUR

Executive Summary

By now, ransomware needs no introduction. It has made countless headlines, kept law enforcement busy, and even worried policymakers and national security analysts who fear a ransomware attack could cripple critical infrastructure such as energy and water systems.

Within most organizations, cybersecurity teams share similar concerns.

Ransomware has the potential to bring down entire environments, including systems essential to operations, leaving the company at the mercy of criminals and threatening business continuity.

Yet every organization is ultimately responsible for shaping its own defense and prevention strategy. What works for one may not work for another, given the diversity of software stacks, processes, and risk profiles.

This makes it difficult to translate concern into an actionable plan.

That is why we created this comprehensive guide to ransomware, offering up-to-date insights into how these criminal operations work and historical context on digital extortion campaigns that shaped today's threat landscape.

From profiles of major ransomware groups to practical recommendations for prevention and recovery, we have gathered what we consider most critical so each organization can build its strategy based on its risk management priorities, available resources, and exposure level.

It is important to understand from the outset that ransomware is not a static threat. Criminals are constantly innovating, both in the technical stages of the attack and in their extortion tactics.

Defense strategies must evolve accordingly, as yesterday's best protections are not always enough to prevent or mitigate today's attacks. Ransomware is no longer just another cyber threat. In recent years, it has absorbed nearly every form of cybercrime that does not revolve around direct fraud or financial scams. Extortion attempts increasingly happen without encryption at all, using data exposure and reputational or legal risk to pressure companies into paying.

Protecting an organization against ransomware is not difficult only because ransomware is complex. It is difficult because so many IT infrastructure weaknesses ultimately converge in ransomware attacks.

Ransomware by the Numbers

Ransoms paid by companies to ransomware gangs totaled **$813 million in** 2024 and **$1.25 billion** in 2023.
(Chainalysis, 2025)

The average ransom demand in a ransomware attack is **$1.3 million.**
(Coalition)

6% of extortion attacks threaten victims with data leaks and no longer use encryption.
(Sophos, 2025)

25% of companies pay the demanded ransom.
(Veeam, Q4 2024)

When looking only at attacks that rely solely on data leaks, **41% of victims pay the extortion.**
(Veeam, Q4 2024)

What's New

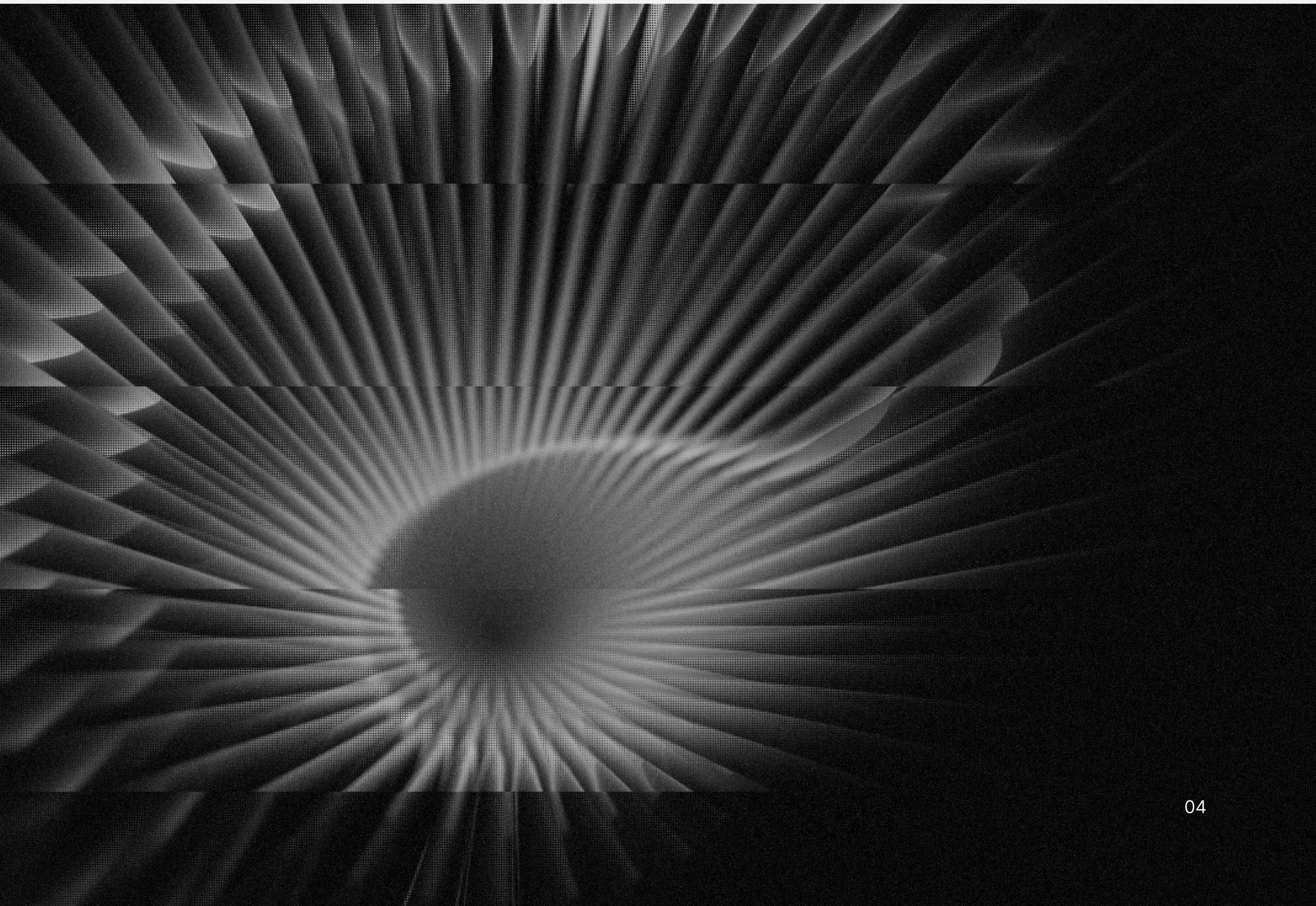
This is a revised and updated version of a document we first published in 2022. If you read the original edition, the main updates are in the chapters about ransomware groups and prevention measures.

While ransomware has become a well-established cyber threat over the past 15 years, the gangs behind these attacks are far from stable. Law enforcement actions, operational failures, and internal conflicts often lead many of them to shut down, or at least claim to shut down to evade authorities or former criminal partners. As a result, the names and key players in the ransomware landscape are no longer the same.

Prevention priorities have also shifted. Ransomware groups increasingly rely on legal and reputational pressure tied to the exposure of stolen data.

A prevention and recovery strategy focused only on backups and restoring compromised systems will not stop criminals from exerting pressure on the company.

We believe the chapters covering these topics deserve a fresh read. Some sections are entirely new (such as the one on supply chain attacks), while others have been rewritten or expanded with updated data.



Evolution of Ransomware

How We Got Here

Straight to the Point: Ransomware is not an isolated threat. The criminal ecosystem that powers ransomware fraud relies on several "services," such as payment collection, money laundering, and concealing digital traces. Here, we explain how ransomware evolved from a scam that simply locked a computer screen and demanded payment via SMS into advanced malware capable of crippling an organization's digital infrastructure and demanding multimillion-dollar ransoms in cryptocurrency.

The "first" Ransomware

After so many mentions in the news, ransomware needs no introduction. While some companies have paid millions of dollars to criminals to resume operations, others could not even consider this option and were forced to declare bankruptcy or shut down entirely. But how did this threat grow so powerful in just a decade? The first malicious code that can be considered "ransomware" appeared in 1989.

Created by biologist Dr. Joseph Popp, the malware was distributed on floppy disks that supposedly contained information about AIDS, which had drawn the medical community's attention after it was first cataloged in 1981. Once installed, this ransomware locked the system and **demanded a ransom of $189.**

In addition to demanding payment to restore access (the same type of "ransom note" **modern ransomware** uses), the malware encrypted file and folder names, making the computer unusable — a concept reminiscent of today's more advanced techniques that leverage asymmetric encryption.

This primitive code is sometimes called the "AIDS Trojan" because of the labels on the floppy disks used to spread it, but it is also known as "PC Cyborg," the name of the company supposedly designated to receive the ransom payments.

Authorities had little trouble identifying the creator of the digital plague. However, Joseph Popp suffered from mental health issues and was declared unfit to stand trial.

Modern Cybercrime, Cryptocurrencies, and OPSEC

Although the similarities are striking, it is not entirely accurate to look for explanations of modern ransomware by analyzing such old malicious programs. This threat, as it exists today, is the result of circumstances that **go beyond technical and software capabilities.** In fact, the **legal obligations and liabilities** faced by ransomware victims have emerged as one of the criminals' most powerful leverage points during their "negotiations."

For anyone tasked with defending a network, understanding the conditions that enable a successful attack and **monitoring criminal activity to anticipate moves and prepare a response** can be key to disrupting the attacker's ability to execute the fraud.

The first step is to examine what the intruder is after and the tools and resources available to them. Unfortunately, today's cybercrime infrastructure, the foundation that makes ransomware possible, was built over decades of online fraud.

In other words, ransomware is a threat shaped by at least 15 years of refinement in digital crime. One of the professional criminal's priorities is OPSEC (operational security), aimed at reducing the risk of arrest and the loss of illicit gains. The easier it is to receive illegal funds or commit "traditional" crimes such as money laundering and identity fraud, the bolder digital crime tends to become.

The transformation of ransomware into a personalized threat, where criminals know exactly who they are attacking and how much they can demand, was accelerated by the emergence of a payment method capable of moving millions: cryptocurrencies.

The connection between ransomware and cryptocurrencies runs deep. In 2017, U.S. authorities dismantled the cryptocurrency exchange BTC-e, accusing it of assisting criminals. In 2025, an investigator who goes by "GangExposed" claimed that a blockchain event was merely a front to launder fraud proceeds. Although no official action has been taken to confirm this claim, cryptocurrencies and blockchain often appear in these schemes, including through anonymity and laundering services known as "tumblers."

Despite this close relationship today, ransomware existed before cryptocurrencies. In the former Soviet bloc, early system "lockers" often demanded payment through premium SMS services: victims simply sent a text message to the provided number to receive an unlock code. The ransom amount appeared on the phone bill. In other cases, payment was made through a platform called E-Gold, which was shut down by the U.S. Department of Justice in 2007. At that time, ransom demands rarely exceeded $300, and SMS-based unlock codes typically cost around $10.

In the rest of Europe and in the Americas, where stricter telecommunications regulations prevented ransom collection via SMS, **ransomware often appeared disguised as fake antivirus software.** The pretense of selling software allowed criminals to collect ransom payments by credit card. The cost of these "programs" was typically around $50.

It was these fake antivirus tools that, in the second half of the 2000s, introduced warning messages about supposed "problems" on the computer, including tricks like changing the desktop wallpaper — something ransomware still uses today.

When negotiating with victimized companies, it is not unusual for ransomware gangs to still treat their targets as "clients" or "patients," echoing the era when criminals sold fake "security" programs. To strengthen their legal arguments, criminals even enabled "legal" support for those involved in negotiations to increase pressure on the victim.

Some iconic ransom viruses, such as CryptoLocker and CryptoWall, used the same visual language (shields and padlocks) that appeared in fake security software.

Of course, not everyone wanted or was able to process credit card payments, especially after payment processors began facing scrutiny due to excessive chargebacks. A "second tier" of screen lockers emerged, charging victims through prepaid cards and gift vouchers.

One well-known malware from this group was Reveton. Already considered a form of ransomware, it did not use encryption. **Instead, it ran an extortion scam** claiming the victim had committed a crime and needed to pay a fine. To make it more convincing, it displayed custom screens branded with the name and insignia of local law enforcement agencies.

Wallpaper used by LockBit ransomware.

Payments were handled through specialized services that simplified international transfers, such as Ukash, Paysafe, and MoneyPak. Ransom amounts were around $200.

But one notorious name in this space was Liberty Reserve, founded in 2001 and shut down in 2013 after an FBI operation uncovered extensive criminal use.

According to the U.S. Department of Justice, Liberty Reserve was used in a money-laundering scheme involving transactions totaling $250 million. The service's founder pled guilty and was sentenced to 20 years in prison in 2016.

The fall of Liberty Reserve in 2013 coincided with the maturation of the cryptocurrency market. The exchange Mt. Gox was still at its peak at the time, offering features and functions that would lay the groundwork for future competitors.

CryptoLocker: The Malware That Defined an Extortion Category

It was also in 2013 that security experts detected CryptoLocker. Distributed mainly through other existing malicious code (such as the Gameover ZeuS botnet) and spam delivery platforms, it is believed to have earned around $27 million in bitcoin.

The characteristics and operation of CryptoLocker would place it on par with modern ransomware. It used asymmetric encryption and command-and-control servers, and was categorized as “crypto-ransomware” to distinguish it from other types of digital extortion. However, CryptoLocker’s success helped **solidify this model of fraud, which we now know simply as “ransomware.”**

Unlike what happened with similar malware from the same era, CryptoLocker’s encryption was never broken. A decryption tool was only possible after a law enforcement operation allowed authorities to obtain the keys used in the scheme.

On the other hand, three aspects set CryptoLocker apart from today’s ransomware: the ransom amount, its distribution method, and the absence of “double extortion.” All these elements are interconnected. While some ransomware victims today face demands of hundreds of thousands or even millions of dollars, CryptoLocker asked for about $500.

The multimillion-dollar demands of contemporary ransomware stem from its targeted distribution and the use of double extortion. Modern operators closely manage each intrusion, deeply penetrating a company’s network and reducing the chances of recovery through backups. Double extortion involves stealing data before encryption, so victims can be threatened with public leaks.

None of this applied to CryptoLocker. The malware was distributed en masse through botnets and “exploit kits” that took advantage of browser and plugin vulnerabilities.

In other words, users were often infected simply by visiting a malicious site. These visits depended on search engines, fraudulent ads, and the compromise of vulnerable legitimate sites. It was an opportunistic, non-targeted distribution strategy.

Perhaps the last notorious ransomware to spread this way was WannaCry, in 2017. Designed to automatically exploit a Windows vulnerability, WannaCry attacked any reachable system. As a result, backup systems were more likely to remain intact, making recovery easier.

WannaCry’s ransom demands were still just a few hundred dollars (typically between $300 and $600). Almost in parallel, another less-publicized ransomware, Locky, began demanding four-figure sums.

Since 2017, important changes have taken place in the world of ransomware crime:

2017

The bitcoin exchange BTC-e is dismantled by the U.S. Department of Justice. Accused of laundering about $4 billion, the exchange was considered one of the favorites among ransomware operators. Because the main suspect could not be extradited to the United States due to a legal dispute involving Greece, Russia, and France, the case remains unresolved.

2018

The ransomware Ryuk emerges, focusing attacks on companies and organizations. Individual systems belonging to consumers and independent professionals become a lower priority. Estimates suggest that up to 81% of all ransomware attacks in 2018 targeted businesses. With higher-value victims, ransom demands skyrocketed: in 2019, Ryuk reportedly attempted to extort $12.5 million from a single victim.

2019

Services known as mixers or cryptocurrency tumblers expand, allowing criminals to obscure illicit gains by blending funds from multiple sources. According to a BitFury report, the share of bitcoins moving from darknet markets — just 1% at the start of 2019 — rose steadily throughout the year and reached 20% in the first quarter of 2020.

2020

The double extortion strategy grows nearly 500%, and ransom payments begin shifting to the cryptocurrency Monero. Ransomware also becomes a vehicle for data leaks, with the threat of exposing stolen corporate information adding a second layer of extortion. Meanwhile, mixers come under increased regulatory scrutiny, and cryptocurrency exchanges are forced to adopt stricter KYC (know your customer) processes. This pushes some notorious ransomware groups (such as REvil) to demand payments in Monero, which is harder to trace, or to charge up to 20% more from victims who can pay only in bitcoin. The result: in 2020, about $692 million in cryptocurrency transactions were linked to ransomware.

2023

Ransomware groups begin targeting suppliers and leaning more heavily on data leaks. The success of the double extortion approach led some groups to experiment with attacks involving data theft without encryption. Attacks focused on software or IT service providers, through vulnerabilities or leaked credentials, caused incidents affecting hundreds of companies simultaneously, without directly breaching their corporate networks.

Despite the evolution in ransom demands (with higher sums and more anonymous payment mechanisms), ransomware still relied heavily on other types of malware, almost "piggybacking" on previous infections. But when this model proved insufficient, cybercriminal operators moved to a more specialized structure, segmenting their activities to scale attacks.

Once ransomware groups began hunting specific, high-value targets, they could justify ever-higher ransom demands, sometimes reaching millions of dollars per victim.

This strategy culminated in attacks on companies operating in critical sectors. The DarkSide group hit Colonial Pipeline in 2021 and demanded $4.4 million, marking a historic moment for cyberattacks.

This and similar incidents demonstrated that ransomware could disrupt operations in infrastructure, healthcare, and energy, establishing it as the most significant modern digital threat.

TOTAL STOLEN BY RANSOMWARE 2020-2024:

US$ 4.8 billion

AVERAGE COST OF A RANSOMWARE ATTACK IN 2024:

US$ 5.13 billion

The Criminal Organizations Behind Ransomware

How Criminals Became Specialized Like an Assembly Line

Straight to the Point — The gangs behind ransomware attacks face multiple challenges when trying to scale their operations without compromising the effectiveness of their schemes. Understanding the day-to-day mechanics of this criminal activity is the first step for security teams — especially in monitoring and threat intelligence — to develop preventive measures or even anticipate future moves.

By analyzing groups such as BlackCat, Clop, and DragonForce, we can better understand how these criminals specialize, the internal disputes they face, and the fragile trust relationships that form under greed and the drive to increase the volume of attacks.

Clop and Scattered Spider: Extortion Through IT Services

The gangs behind ransomware are far from stable. For many reasons — such as internal disputes, reorganizations, "bad debts," and law enforcement actions — it is common for these groups to dissolve, sometimes even publicly announcing the end of their activities. However, the individuals involved and the tools they use typically remain in the ransomware scene, whether by selling the malicious code or forming new alliances and crews.

Clop is one of these groups. Formed as a successor to ransomware known as CryptoMix and active since 2019, Clop stands out for a series of attacks and extortion schemes that deviate significantly from traditional ransomware tactics.

One of Clop's defining traits is large-scale attacks carried out through IT services or widely used software. Since late 2020, Clop has conducted four mass attacks on data transfer software, stealing information from thousands of companies. One estimate suggested that a single large-scale action by Clop, targeting MOVEit Transfer, generated more than $75 million for the gang.

Clop has also distinguished itself by carrying out ransomware attacks without relying on file encryption, depending solely on the pressure created by the threat of leaking stolen corporate data.

In a more traditional ransomware scenario, a company under attack would be primarily concerned with its own data, system recovery, and business continuity. In a fraud centered on data leaks, the biggest concerns are legal and market consequences, such as losing customers and exposing sensitive projects.

Data backups do not necessarily improve the company's response capability. In fact, an unprotected backup can become a vulnerability, since criminals only need access to one copy of the files, regardless of where it is stored. This also differs from traditional ransomware, where the malware would have to compromise all backups to be effective.

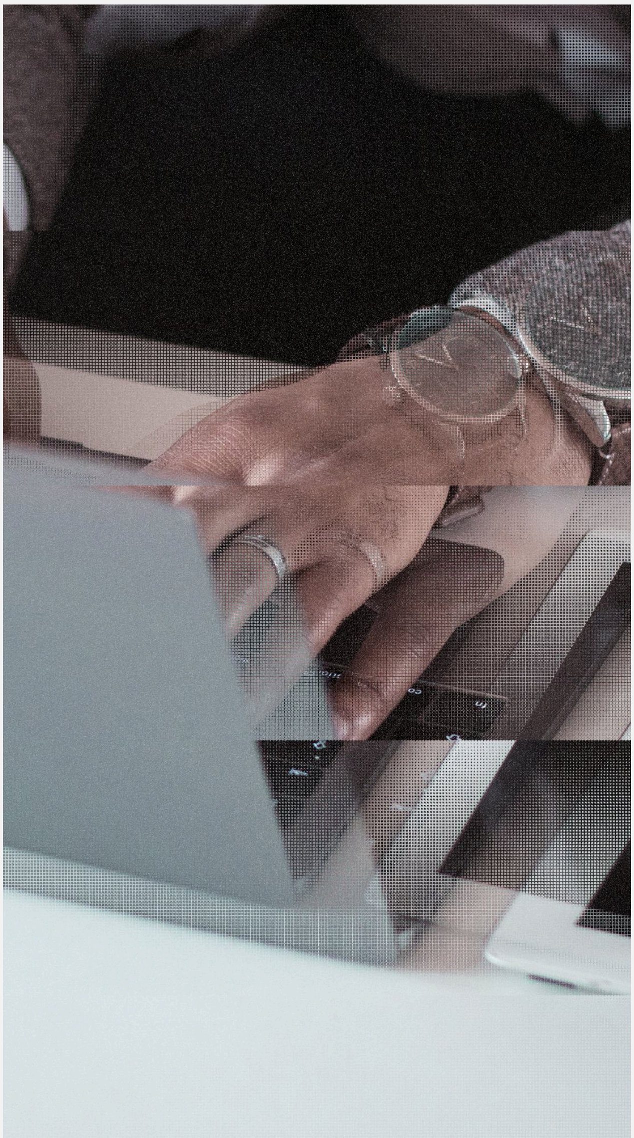
By skipping file encryption, Clop can scale its mass attacks more easily and carry them out faster. In addition, there is no need for access to corporate systems with write permissions; read access is enough to copy files and start the extortion attempt.

Of course, omitting the data encryption stage generally makes extortion less effective than double extortion (which combines encryption with the threat of leaks). Still, Clop has shown that encrypting files is not essential for a successful criminal operation. Estimates suggest Clop has collected about $500 million in ransom payments since its creation.

Scattered Spider, known by several names within the cybersecurity community and linked to a collective called "The Com," is better known for its social engineering tactics. The group is believed to have many accomplices in Western countries, as these social engineering attacks often involve phone-based manipulation.

The social engineering targets of Scattered Spider are almost always service providers working in help desk or similar support roles. In general, the group is notorious for exploiting weaknesses in authentication systems and processes through tactics such as phishing, SIM swapping, and other social engineering methods.

Like Clop, individuals associated with this gang have also carried out extortion attacks without using traditional ransomware to encrypt data. Both in the way they gain access to corporate networks and in how they conduct extortion, Scattered Spider has introduced new concerns for companies.



Dragonforce

Although there are some indications that the DragonForce gang originally organized in 2023 as a hacktivist group supporting Palestine, the group's recent actions show an undeniable financial motivation.

DragonForce grew by forming alliances under a ransomware-as-a-service (RaaS) model, gaining notoriety for its ability to attract affiliates dissatisfied with other criminal operations.
RaaS mimics the "software as a service" model, allowing ransomware creators to distance themselves from day-to-day operations and direct attacks on victims.

The RaaS model is not new. Even before DragonForce existed, the group Conti refined this approach with a highly segmented operation, leaving "affiliates" responsible for carrying out attacks. However, Conti shut down in 2022 after a series of leaks exposed its internal communications, revealing conflicts and mistrust.

One aspect that stands out with DragonForce is the ability for affiliates to create their own sites to publicize attacks and manage ransom negotiations. This helps obscure the affiliate's connection to DragonForce, allowing each to build its own "brand" while using DragonForce's infrastructure.

The group calls this structure a "cartel", as it gives affiliates more autonomy.
By mid-2025, there were indications that individuals linked to Scattered Spider were deploying DragonForce ransomware in their targets, signaling a new alliance in the cybercrime world.

Such moves show how fluid relationships in cybercrime can be, often adapting to the convenience of each situation, even as criminals seek to organize under groups with a relatively strong and reputable brand.

Although DragonForce is a relatively new name, the group's structure, as well as its tactics and tools (such as Mimikatz and Cobalt Strike), have been used by other actors before.

Ransomware as a Service: A Pillar of the Ransomware Ecosystem

With RaaS, a ransomware operation has multiple “affiliates” who carry out the intrusions. However, the negotiations to collect the ransom remain under the control of the gang’s core members.

When a criminal operation reaches this level of scale and needs to manage people and its own technological infrastructure — with the added challenge that trust is scarce in the criminal world — it is not unusual for lapses, infiltrations, and mistakes to expose details of what is happening.
This type of intelligence helps build countermeasures and issue timely alerts about potential ransomware activity in monitored environments.

Some examples of insights that monitoring criminal activity can provide:

1. Tactics, Techniques, and Procedures (TTPs): How ransomware reaches the target network; what types of credentials may be in use (VPN, databases, domain controllers, cloud providers); which recent vulnerabilities require extra caution; and other operational details.

2. Indicators of Compromise (IoCs): Files, IP addresses, and system behaviors that can signal the presence of ransomware before it is activated.

3. Targets (alvos): Companies and sectors that criminals may be aiming at. Statements from groups like LAPSUS (not strictly a ransomware gang, though its attacks are similar) have named specific companies under threat, some of which were intercepted by Axur on deep and dark web channels.

4. Leaks and Credentials: To maximize returns, criminals often advertise stolen data for sale, sometimes providing sample files. Especially when credentials are exposed, this data can signal a breach or foreshadow a future compromise.

5. Corporate Data: Beyond credentials, monitoring can reveal unauthorized exposure of corporate information such as financial and accounting records, personal data of employees and customers, and partner-related projects. This exposure points to legal and reputational risks and can also help trace the source of a breach by analyzing where the leaked data originated.

Why Ransomware Has Employees and Suppliers

A successful ransomware attack depends on a complex chain of events and tools.

A leak of internal conversations from the Conti ransomware gang, which occurred in February 2022, turned out to be one of the most solid and revealing sources about the daily operations of ransomware groups. The chats were reportedly published by a Ukrainian security researcher as retaliation after the group expressed support for Russia during its military conflict with Ukraine.

The conversations confirmed much of what had long been suspected about how ransomware operations work, but also revealed that gang leaders pay actual salaries to their “employees” (in Conti’s case, at least 100 people) and maintain something resembling an HR department to recruit new members and replace underperformers.

Even so, distrust is constant in this environment. A well-known case was the **BlackCat** gang, which shut down in May 2024 and left affiliates claiming unpaid commissions.

The risk of scams and betrayals keeps tensions high in the cybercrime world.

The affiliate and “crime-as-a-service” model started to take shape back in the 2000s, when criminals sold access to malicious code and exploit kits (EKs), ready-made tools for exploiting browser vulnerabilities, sold by subscription or commission and tracked with performance metrics and success rates.

These EKs and spam networks (which also sold bulk email delivery as a service to other criminals) laid the foundation for the first ransomware infections, as well as the distribution of password and credit card stealers, cryptocurrency miners, and other types of fraud.

The fake antivirus scam, fraud disguised as software sales, also used a commission-based affiliate system, a legitimate practice borrowed from the business world.

In fact, “blaming affiliates” for any questionable tactics was a way for criminals to shield themselves at a time when they needed to avoid retaliation from banks and credit card companies.

With cryptocurrencies, that pretext is no longer useful. But the affiliate model still helps create clear incentives and sustain the specialization of each phase in the criminal operation.

The Specialties of Cybercrime

The ransomware-as-a-service model, which applies this method to ransomware, was already being outlined in 2012. That year, malware known as Winlocker or Gimemo introduced an affiliate program with a control panel that tracked paid ransoms and calculated the commission percentage each affiliate would receive.

The ransomware affiliate was solely responsible for infecting computers. There were therefore two main roles: the ransomware author, who created the software and maintained the basic control infrastructure to track statistics, and the distributor, who handled delivering the malware to victims.

Today, the landscape is far more complex. Both the author's and the distributor's responsibilities have been broken down into smaller tasks, each carried out by individuals dedicated to a specific role.

Job roles of ransomware employees and affiliates

Programmers (Coders): Responsible for developing the software needed for the operation. They create the ransomware itself, implement encryption algorithms in the code, and integrate necessary tools.

Testers: The "quality control" of ransomware depends mainly on its ability to evade antivirus tools. Testing involves analyzing the malware with security solutions and making adjustments to bypass protections.

Network Administrators: Responsible for the infrastructure, including command-and-control servers and distribution systems. Many ransomware strains use dynamic configuration files, allowing them to switch to new infrastructure if the previous one is taken down. To support this capability, the infrastructure must be rebuilt periodically.

Vulnerability Hunters: Perform reverse engineering on software and systems to find security flaws that can be exploited in attacks.

Hackers: Use the infrastructure, programs, and vulnerabilities prepared by the rest of the team to carry out attacks against planned targets. They are responsible for lateral movement within organizations, using password-stealing and network scanning tools (such as Nmap and Mimikatz) so that the ransomware deployment can reach as many systems as possible, including across different operating systems.

Negotiators and "Lawyers": Individuals responsible for communicating with ransomware victims to obtain payment. "Lawyers" may assist during negotiations by emphasizing the legal risks associated with the stolen data and increasing pressure on the victim.

Cryptocurrency Specialists: Develop money-laundering mechanisms to move ransom payments from victims into the traditional banking system.

Even with this wide range of roles and specializations, ransomware operations still rely on other external suppliers.

As in any business, scaling up has its pros and cons. In ransomware, while scaling has increased illicit profits through greater sophistication and specialization, it also creates a constant demand for new targets.

Some groups are more structured and specialized than others, but all criminals have access to the same underground ecosystem where they can acquire information or hire services.

Just as a ransomware developer can hire a spam specialist, another criminal might purchase ready-made malware to spread through social networks or social engineering, participating in the crime without deep technical knowledge.

To make this possible, criminals have created relatively open marketplaces, allowing newcomers to join and support the ecosystem, regardless of their specific skills.

For those with specialized monitoring of these forums and networks, they become a valuable data source. Through them, it is possible to anticipate or detect attacks before they happen, for example, by spotting leaked credentials early.

Because the criminal who steals a credential is not always the one who later uses it, intercepting these exchanges can be decisive in stopping an attack before it occurs.

Preventing a ransomware attack through intelligence and monitoring activities has significant potential for effectiveness in this environment.

Data leak–based extortion makes recovery and restoration measures (such as backups) insufficient to relieve the pressure to pay ransom, since the company may still face the risk of a data breach. Leaks cause damage to brand and reputation.

There have been documented cases in which attackers used the victim's customer or employee database to contact individuals directly, warning them that their personal information could be exposed if the company refused to pay.

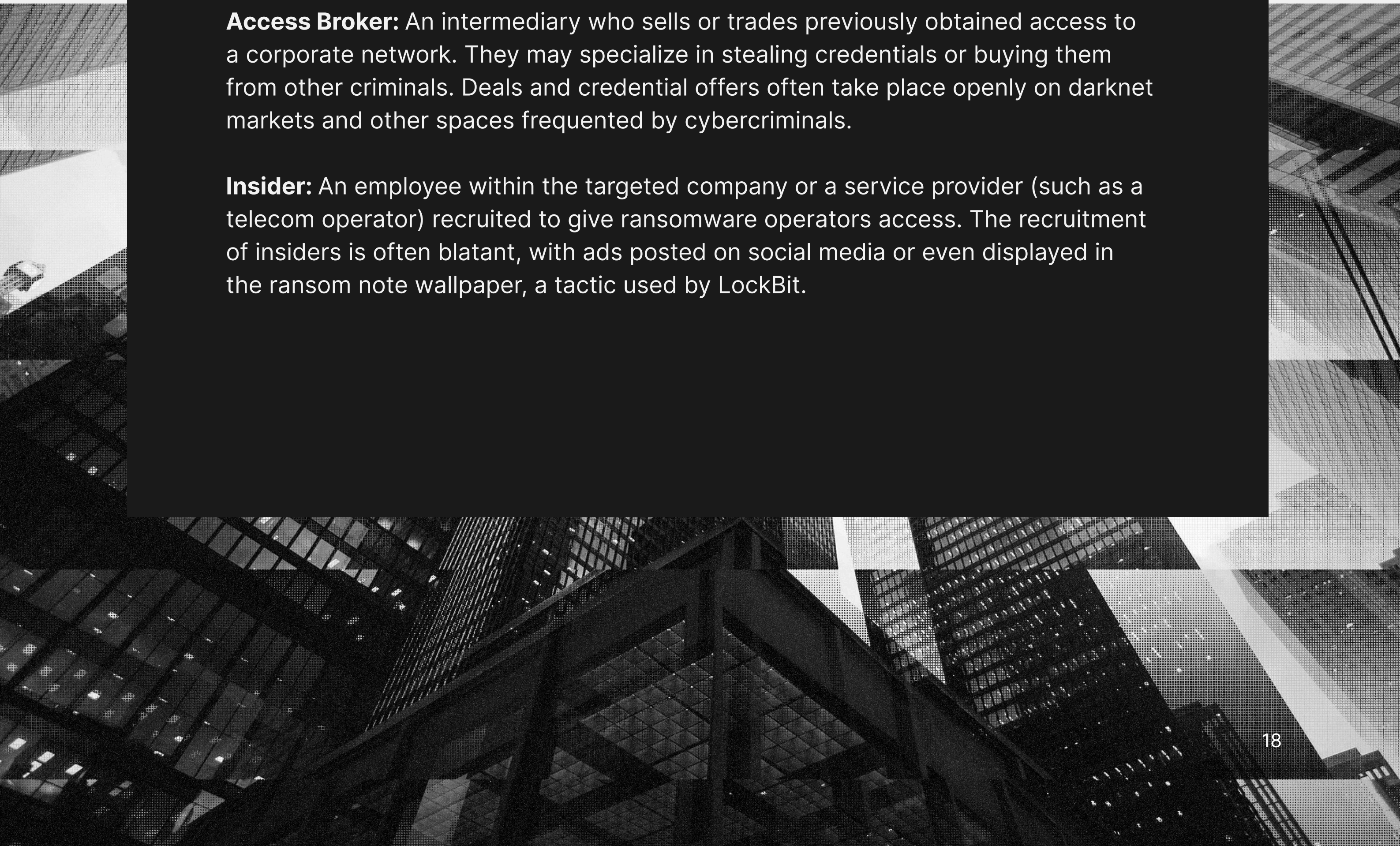
This is the core tactic of modern ransomware: even if an organization has done its homework with backups and a solid recovery plan, there is virtually no way to prevent the harm caused by data exposure. To make matters worse, there is no guarantee that criminals will actually delete the stolen data.

Ransomware Suppliers

Spammer: A criminal specialized in building or acquiring infrastructure to send malicious emails. These emails can be sent in mass campaigns or crafted to target a specific organization. The success metric for this supplier is the ability to deliver emails to inboxes, bypassing anti-spam defenses.

Access Broker: An intermediary who sells or trades previously obtained access to a corporate network. They may specialize in stealing credentials or buying them from other criminals. Deals and credential offers often take place openly on darknet markets and other spaces frequented by cybercriminals.

Insider: An employee within the targeted company or a service provider (such as a telecom operator) recruited to give ransomware operators access. The recruitment of insiders is often blatant, with ads posted on social media or even displayed in the ransom note wallpaper, a tactic used by LockBit.



Prevention

Applying What We Know About the Adversary

Straight to the Point — By understanding the cybercrime ecosystem and its weak points, it is possible to act decisively and comprehensively in collecting and processing data exposed by criminals, mapping the company's risk, and closing the entry points that would be used in attacks. Because ransomware depends on external access, these measures should not rely solely on the internal security team and must consider a broader external cybersecurity strategy.

Ransomware Hardening

Quick Guide

Assess your defenses against ransomware attack vectors:

Stolen Credentials

- Use a credential monitoring service
- Implement phishing-resistant multi-factor authentication (MFA)
- Deploy an identity management system
- Train and raise user awareness on proper credential use
- Adopt a *zero trust* architecture

Malware

- Use an EDR/XDR solution
- Connect your security tools to threat intelligence platforms
- Implement IDS solutions or restrict the use of unauthorized applications

Social Engineering

- Include employee awareness and training in your security policy
- Add browser protections such as sandboxing or restrictions on external access

Vulnerabilities

- Use an External Attack Surface Management (EASM) solution to detect internet-exposed systems and vulnerabilities
- Apply patches and updates to fix known vulnerabilities
- Avoid exposing remote access systems (RDP) to the internet
- Keep security features enabled
- Protect corporate network resources with Kerberos authentication and security features in domain controllers

Suppliers and Third Parties

- Monitor the security practices of suppliers and third parties to ensure they align with the company’s overall standards
- Create isolation mechanisms with least-privilege access and strict controls for cloud resources

How the Threat of Data Leaks Changed the Weight of Prevention

A solid recovery strategy was once enough to mitigate the impact of ransomware, but the rise of double extortion, ransom demands combined with the threat of data leaks, changed this reality. Even after restoring systems, the risk of data exposure makes it difficult to avoid other damages from the attack, such as harm to brand reputation and potential legal consequences under data privacy and breach notification laws.

With the threat of double extortion firmly established, some groups began exploring a new approach based exclusively on data leaks. These attacks remove the need for attackers to obtain write access to data, greatly expanding the possibilities for carrying out extortion campaigns.

Some experts now prefer using the term “data extortion” to describe all forms of this crime, moving away from the traditional concept of ransomware.

Clop, which we mentioned earlier, Hunters International, and criminals linked to The Com (Scattered Spider) are among the actors that have found success with this type of threat.

According to Sophos’ State of Ransomware 2025 report, the number of extortion attacks without encryption — relying solely on the threat of data leaks — doubled in a single year. In the study, these attacks account for 6% of all extortion incidents and 13% of incidents in companies with fewer than 250 employees.

Whether part of double extortion or as standalone data extortion, stealing data and threatening to expose corporate information has reshaped defense priorities against ransomware.

In this context, measures that can prevent or interrupt an ongoing attack add significant value to a defense strategy.

By cutting off an attacker’s access to the corporate network before data theft occurs, a company protects its trade secrets and reputation — and avoids facing a decision about paying a multimillion-dollar ransom.

Preventing any cyberattack requires a solid level of information security maturity, including timely patching, strong security policies, and well-defined processes. However, these basic steps are not always enough. Ensuring there are no gaps or misconfigurations is a constant challenge.

Ransomware campaigns are often tailored to each organization, with human operators supported by criminal gangs intent on bypassing traditional defenses like antivirus software. Meanwhile, internal security resources may be limited, worsened by the ongoing talent shortage in the cybersecurity industry.

For this reason, it is essential to rely on specialized teams that can mitigate specific risks — many of which are visible externally due to the challenges ransomware operators create for themselves when organizing large-scale, sophisticated criminal operations.

Credential Leaks: The Warning Sign of Ransomware

According to the 2025 edition of Verizon's Data Breach Investigations Report (DBIR), 22% of intrusions begin with stolen credentials. This includes extortion attacks, whether carried out through traditional ransomware or threats to leak corporate information.

While credential theft is a major risk, there are ways to address this challenge.

Because modern ransomware relies on a full cybercrime ecosystem, there are many opportunities to detect suspicious activity through continuous monitoring of that underground environment. Such intelligence can indicate whether an organization is at risk or, in the worst case, already targeted by criminals. With this privileged view of criminal activity, a company can act proactively to close vulnerabilities or access channels that may have been compromised.

Beyond leaked passwords from breached databases, CTI (Cyber Threat Intelligence) teams and the Axur Research Team (ART) also monitor leaks coming from malware designed to steal credentials (credential stealers). Although these malware families are not strictly part of ransomware operations, the credentials they gather are packaged and sold in the cybercrime underground, fueling a wide range of malicious activity.

Stolen credentials can be sold to access brokers or directly to ransomware gangs, which may look for attractive victims or specific system credentials (such as cloud infrastructures, dashboards, or databases) they already know can provide a strong foothold into a company's network.

Axur's monitoring has identified more than 17 billion stolen credentials, and about 700,000 new credentials are detected each month, posing risks to thousands of individuals and the companies they work for.

This work helps break the chain of events that could lead to a ransomware attack. By being alerted to stolen passwords or vulnerable access points, an organization can respond proactively: canceling the compromised credential stops malicious activity from escalating.

In both the Colonial Pipeline attack in 2021 and the Change Healthcare attack in 2024, initial access was gained through a stolen credential. From what is known, the series of attacks that affected companies using the Snowflake storage system in 2024 also resulted from stolen credentials.

An early warning about the compromised credentials involved could have changed the outcome of these incidents.

A credential stealer can be distributed via email (using social engineering and phishing), but it is also very common for these malware to spread through social media. Their ability to steal login sessions stored in browsers — often bypassing multi-factor authentication (MFA) — makes them valuable for hijacking accounts of content creators, even those who use all the security features offered by major internet service providers.

An employee can put the company at risk even if the credential stealer is installed on their personal computer after clicking a link on social media. All stolen passwords, including those seemingly unrelated to corporate systems, can be used in credential stuffing attacks, where criminals attempt to access a target using credentials originally obtained for other platforms.

In other words, a password stolen for one service can be tested and validated against a corporate system, a far more valuable target for ransomware gangs. Through access brokers, intermediaries who trade access points, the stolen credential can end up in the hands of operators most capable of launching a ransomware attack.

Credentials can also be exposed through unauthorized access to databases, whether belonging to the company or a third-party supplier. Implementing tracking tokens can help identify leaks early and stop attacks by canceling credentials or cutting off supplier access that may have been compromised.

This type of monitoring can be integrated into the company's security operations.

With mechanisms to detect security policy violations and other compliance breaches, including employees reusing passwords or suppliers with weak practices, the organization improves its ransomware protection while raising overall security maturity across its entire operational chain.

External Attack Surface Monitoring

Even before obtaining credentials or corporate data, criminals can scan systems the company has exposed to the internet, such as web servers, email, VPNs, and API endpoints. By discovering a vulnerability, misconfiguration, or exposed data in these systems, an attacker may find an entry point to start compromising the target.

In today's complex corporate digital environments, it is common for dashboards, web services, cloud storage, and many other tools to be adopted ad hoc. In other words, set up to address a specific or temporary need without clear integration into broader processes and systems. Often these resources lack proper documentation, and their existence is not always communicated to IT, creating what is known as shadow IT.

For this reason, it is not enough for a company to focus only on its internal attack surface and the assets managed by the IT department.

In most cases, the attacker is outside the organization, and their first point of contact with the company's environment is through this external attack surface — including resources that are not officially managed by the IT team.

The bottom line is that an attacker may end up knowing this external surface better than the company itself, especially if there has been no coordinated effort to monitor, map, and protect it. You cannot apply a security patch to a system the IT team does not even know exists.

External Attack Surface Management (EASM) solutions help companies gain a clearer view of their infrastructure from the outside, just as an attacker would. EASM supports vulnerability management, detects misconfigurations, and identifies software and equipment that are improperly exposed to the internet.

Monitoring, mapping, and ensuring the compliance of all these external systems is essential to prevent attackers from finding "shortcuts" into the corporate environment.

The Risk of Third-Party Attacks and Supply Chain Security

Instead of targeting their victims directly, some ransomware groups have begun looking for common points of failure among company suppliers. Attacks on these third parties are often referred to as supply chain attacks, as they reach companies through the other organizations they depend on.

Because many companies allow direct or indirect connections from these third parties into their IT infrastructure, the risk involved in such campaigns is not very different from a direct attack on the company itself.

For the attacker, discovering a vulnerability or weakness in a supplier can enable access to dozens or even hundreds of companies in a single move. In this way, one cyberattack can turn into dozens of separate extortion attempts, each applied to an individual victim.

Types of Third-Party Attacks

There is no formal categorization of different supplier attacks, but many of these incidents can be grouped based on the type of third party exploited.

Attacks on Outsourced Infrastructure

These attacks take advantage of characteristics, weaknesses, or common points of failure in a digital service used by multiple companies.

The most emblematic example is the Snowflake cloud storage service. Although the attackers did not exploit any vulnerability in the platform itself, the lack of multi-factor authentication (MFA) in many customer accounts created an opening for a massive data theft, impacting 165 organizations without breaching any of their internal infrastructures.

In other cases, criminals have tried to exploit weaknesses in outsourced identity providers and other types of IT services.

This strategy has also been used by attackers outside the ransomware sphere. One of the most concerning cases was reported in 2023, when Chinese hackers obtained a cryptographic key from Microsoft's cloud infrastructure to attack the company's U.S. government customers. The incident prompted an investigation by the newly formed Cyber Safety Review Board.

Attacks on Support Services

Cybercriminals have used social engineering to deceive call centers or outsourced help desks in order to gain access to corporate infrastructure. Because these teams often have permissions to reset user passwords, they can become a weak point in the authentication process.

An attacker may impersonate a company employee and request a password reset or even the deactivation of additional authentication factors.

There have also been reports of physical threats against the outsourced employees providing these services. If there is no mechanism to track and record such incidents, the contracting company may only become aware of the attempted attack after the breach has already occurred.

Attacks on Software

Attacks that exploit software vulnerabilities are not new. However, the type of vulnerability targeted and the attacker's objective create a very specific scenario that must be understood within the broader context of supply chain threats.

The key factor to consider is the purpose behind exploiting the flaw — specifically, whether it will be used for data extortion. Software that supports critical corporate network functions, such as data transfer services and remote administration tools, are prime targets for these campaigns.

It is not always necessary for the vulnerability to exist in the software itself. Attackers may also target the company behind the software, tampering with its code to reach end users. The SolarWinds case in 2020 is the most well-known example of this type of attack, though it did not involve ransomware.

That does not mean ransomware operators will avoid this tactic. In 2017, the M.E. Doc accounting software was compromised to distribute malware known as NotPetya. NotPetya is now considered a wiper because it lacked any genuine mechanism for decrypting and recovering files.

Even so, the consequences for victims were very similar to those of ransomware attacks at the time, and it is unlikely that ransomware operators are not actively searching for software that could serve as an entry point into corporate networks.

The most recent and notable extortion campaigns exploiting software vulnerabilities were carried out by the Clop group, which abused flaws in services such as GoAnywhere and MOVEit Transfer, threatening hundreds of organizations with the stolen data.

⚠

With external cybersecurity tools, companies can gain visibility into issues in their connections with third parties. For example, credential monitoring can be extended to include external partners that hold access credentials to corporate systems.

At the same time, tracking threat intelligence insights keeps security teams informed about the latest tactics used by ransomware groups and which software is being exploited in active campaigns, enabling a swift and effective response to prevent or minimize the impact of attacks.

Cybersecurity Intelligence

Tracking the movements of ransomware gangs makes it possible to map the vulnerabilities and techniques they use. In practice, this allows organizations to prioritize the most effective actions to protect themselves.

- Prioritize patching vulnerabilities currently being exploited by ransomware groups
- Strengthen the security of channels and services (such as a specific cloud provider) that are involved in recent attacks
- Enhance existing security systems (such as antivirus and firewalls) with relevant Indicators of Compromise (IoCs), including malicious IP addresses and files
- Stay informed about risks specific to your industry
- Take action to deter the recruitment of insiders who could collaborate with criminals
- Adopt password management systems (vaults) and phishing-resistant multi-factor authentication (MFA) to secure credentials and access channels. These measures can prevent credential exposure or reduce the usefulness of a stolen credential.

How Monitoring Leaks Breaks the Ransomware Chain at Its First Link

1. Ransomware operators acquire credentials and access to corporate systems from other criminals specialized in initial breaches or in stealing logins and passwords (these criminals are sometimes called access brokers).

2. Monitoring the flow of these transactions and offers makes it possible to identify who else may be at risk and how attackers could gain access to the corporate network.

3. When a leaked credential is detected, the organization can block it.

4. The ransomware operator will not be able to gain initial access to the organization.

5. Without this initial access, the attack becomes much harder to carry out and cannot progress.

Recovery and Response

How to React to a Ransomware Attack

Straight to the Point — Because companies often rely heavily on their technology infrastructure, a ransomware attack can disrupt the entire business. Halting operations requires a proactive stance that conveys resilience to investors, customers, and other stakeholders. This demands preparation, clear communication channels, and a solid checklist to guide teams through the most critical moments. For this guide, we reference the checklist provided by the United States Cybersecurity and Infrastructure Security Agency (CISA).

A visão executiva da resposta ao ransomware

In a double extortion scheme (file encryption combined with the threat of data leaks), which is the standard in today's prominent ransomware attacks, an organization faces two main challenges:

1. Restoring IT infrastructure to resume operations and minimize losses caused by encrypted systems.
2. Protecting the company's brand and reputation with customers, employees, and other stakeholders.

While brand protection is not a direct responsibility of the technical recovery team, it is important to define clear communication channels for the teams handling this aspect.

The IT team can also take practical steps to show concern for customers, such as securing credentials that may have been stolen. For instance, the organization can invalidate old passwords and require users to reset them at their next login, without alarming customers through a forced immediate password change.

It is also important to note that the organization may have legal obligations regarding data breaches. In the United States, data breach notification and privacy laws in many states require companies to inform affected individuals in certain cases.

Similar rules apply in the European Union under the General Data Protection Regulation (GDPR).

If the attack did not encrypt data, the extortion usually relies mainly on legal and reputational pressure. Criminals may even threaten to inform customers and partners whose information was stolen during the incident.

For these scenarios, it is advisable to prepare a robust communication strategy to inform customers and partners about the situation and prevent criminals from controlling the narrative around the breach.

Communication will be more effective if the company has security controls or processes in place to accurately determine what information was compromised and what actions should be taken by all affected parties.

Preparation Is Essential

Responding to a ransomware incident can be made easier through a series of proactive measures.

Train the IT team for the initial incident response.

It is not uncommon for network administrators and IT analysts to react to routine issues by rebooting or shutting down systems. This can destroy evidence that would later help clarify the incident. Because administrators and analysts are often the first to encounter symptoms of an intrusion, a well-prepared initial response can greatly simplify subsequent steps.

Test backups and plan for recovery.

Backups are at the center of ransomware concerns. However, simply performing backups is not enough — files must be protected and preferably kept offline.

Consider the specific risks of cloud backups.

For cloud backups, factors such as restoration time (limited by network speed and other constraints) and the potential vulnerability of connected systems must be evaluated. Using multiple cloud solutions and immutable storage can help prevent attackers from compromising all backups. Because cloud backups can be accessed remotely, they should be encrypted to prevent attackers from using them for data-leak extortion.

Establish Emergency Communication Channels

The company's usual communication channels may be unreliable or even unavailable during a ransomware incident. Be prepared to set up a war room and establish contact with security consultants, stakeholders, and leadership through channels that do not depend directly on the corporate infrastructure.

Build Data Control and Privacy Processes

In many countries, existing laws require companies to protect personal data and provide notifications to individuals affected by a breach. Determining whether an attacker accessed personal information can be critical to avoid extortion attempts based on data exposure threats.

Develop a Disaster Recovery and Business Continuity Plan (BCP) and Conduct a Business Impact Analysis (BIA)

Disaster recovery and business continuity plans (BCPs) map risks and interdependencies across business processes, making it easier to prioritize which systems should be restored first.

Without this, a system considered critical during an ad hoc incident assessment might be restored but remain unusable due to a dependency on another system not included in the recovery sequence.

A Business Impact Analysis (BIA) evaluates the impact of service disruptions to define the organization's operational requirements and associated resources. This helps set recovery milestones and estimate realistic restoration timelines.

The less prepared an organization is when facing a ransomware incident, the more work will be required from the response team, prolonging system downtime and increasing losses.

Additionally, the faster the response and restoration of normal operations, the lower the reputational damage is likely to be, especially if it becomes clear that no ransom was paid.

Checklist: Responding Effectively to a Ransomware Incident

A solid reference for building a ransomware response strategy is the Ransomware Guide published by CISA (Cybersecurity and Infrastructure Security Agency), the government agency responsible for cybersecurity and critical infrastructure protection.

The checklist includes 19 key actions organized into three major response phases. Below are the 19 items with adapted commentary:

Phase 1: Detection and Analysis

1. Identify impacted systems and isolate them immediately

- If multiple subnets may have been impacted, disconnect them all at the switch. It may not be feasible to disconnect individually during the incident.
- If it is not possible to disconnect the network as a whole, disconnect individual systems by unplugging cables or removing them from Wi-Fi.
- Systems can also be disconnected or isolated by segmenting them into VLANs. In some environments or services (such as public cloud), this may be the most viable option.
- If the intrusion began with a third party or partner, revoke all credentials or access channels associated with them.
- The attackers may try to monitor the company's internal communications. Prefer alternative communication methods (such as phone calls) and proceed in a coordinated way to prevent lateral movement by the criminals or escalation of the attack.

2. Only shut systems down if it is not possible to disconnect them from the network.

- Shutting systems down should be done only as a last resort, because it destroys volatile evidence (such as system memory) and makes forensic analysis more difficult.

3. Sort and prioritize the systems that need to be restored and recovered.

- Identify and prioritize them by mapping the nature of the data stored on each one and the role it plays (security, healthcare, revenue generation).

Stage 1: Detection and Analysis

4. Start a Threat Hunting effort to understand how the attack happened.

- Look for new accounts created in the user directory or accounts whose authentication properties have been altered.
- Check logins on remote access systems and VPNs.
- Search endpoints for tools that could have compromised backups and credentials (such as Mimikatz) or exfiltrated data (tools like Rclone and cloud storage clients not normally used by the organization).
- Review activity logs for outbound data transfers over any port.

Intermediate Stage: Communication, Documentation, and Management

Although this stage is not explicitly described in CISA's guide, this is the moment to compile all the information gathered during the initial phase. It is also when communication with managers and stakeholders begins, **a process that should continue throughout the incident response to protect the organization's brand.**

5. Meet with your team to develop and document an initial understanding of what happened based on the analysis so far.

6. Using the organization's contact information for authorities and service providers, coordinate with internal and external teams and stakeholders, knowing what each can contribute to help mitigate, respond to, and recover from the incident.
    - Share the information you have so that assistance is relevant. Keep managers and executives updated with regular progress reports on the situation.

Stage 2: Containment and Eradication

7. Preserve a system image and a memory dump from a sample of affected devices (such as workstations and servers). Collect relevant logs, copies of precursor malware files, and any other observable data that can be considered an Indicator of Compromise (IoC) (e.g., command-and-control server IP addresses, suspicious registry entries, other artifacts).
   - Pay close attention to preserving highly volatile information such as logs and system memory data to prevent loss or alteration.

8. Consult law enforcement about the possible existence of decryption tools that may be available.
   - Axur specialists can help identify a decryption tool; however, decryption will not be possible in most cases.

9. Research trusted sources for recommendations related to the specific ransomware variant and follow the steps provided to detect and isolate impacted systems or networks.

10. Identify the credentials and systems involved in the initial intrusion. The compromised credential may be, for example, an email account.

11. Based on the intrusion data identified in the previous steps, isolate any associated systems that could be used to maintain unauthorized access. Ransomware intrusions are often accompanied by mass credential theft.
    - Protect the network and other information sources against further unauthorized access, which may require disabling VPN and remote access services, single sign-on (SSO), and other publicly accessible or cloud-based assets.

12. Additional suggested action — identifying server-side data encryption
    - Data on servers may be encrypted by ransomware installed directly on the server, but in some cases the encryption is performed from an authorized endpoint without direct server compromise.
    - Open sessions to shared folders, file ownership details, and login histories for RDP services can help determine whether server-stored data is being encrypted by ransomware running on a workstation.
    - Windows security logs, SMB service event logs, and network traffic analysis tools (such as Wireshark) can also help trace the source of unauthorized access.

Stage 2: Containment and Eradication

13. Examine existing detection and prevention systems within the organization (antivirus, endpoint response, IDS and IPS systems, etc.) and review their logs. This may reveal additional evidence about systems or malware involved in the early stages of the attack.
    - Look for evidence of dropper malware, which acts as a precursor to ransomware. As explained earlier in the cybercrime ecosystem, access to corporate networks is often purchased by ransomware operators, while access brokers specialize in initial entry using remote access or credential-stealing malware.

14. Conduct a thorough analysis to identify persistence mechanisms, both inbound and outbound..
    - Inbound: stolen or attacker-created credentials, vulnerabilities, perimeter systems infected with remote access malware.
    - Outbound: remote access tools installed on internal systems, ranging from professional offensive security frameworks like Cobalt Strike to typical remote support tools such as AnyDesk.

15. Restore systems by prioritizing critical services (such as healthcare, safety, or revenue-generating functions), preferably using preconfigured system images.
    - Ensure that appropriate patches are applied and that the proper security systems (antivirus or XDR) are in place.

16. After the environment has been fully cleaned and restored — including resetting impacted credentials and removing or eradicating malicious persistence mechanisms — perform a password reset for all affected systems and address security gaps or visibility issues. This can include applying patches, security updates, and other protective measures not previously implemented.

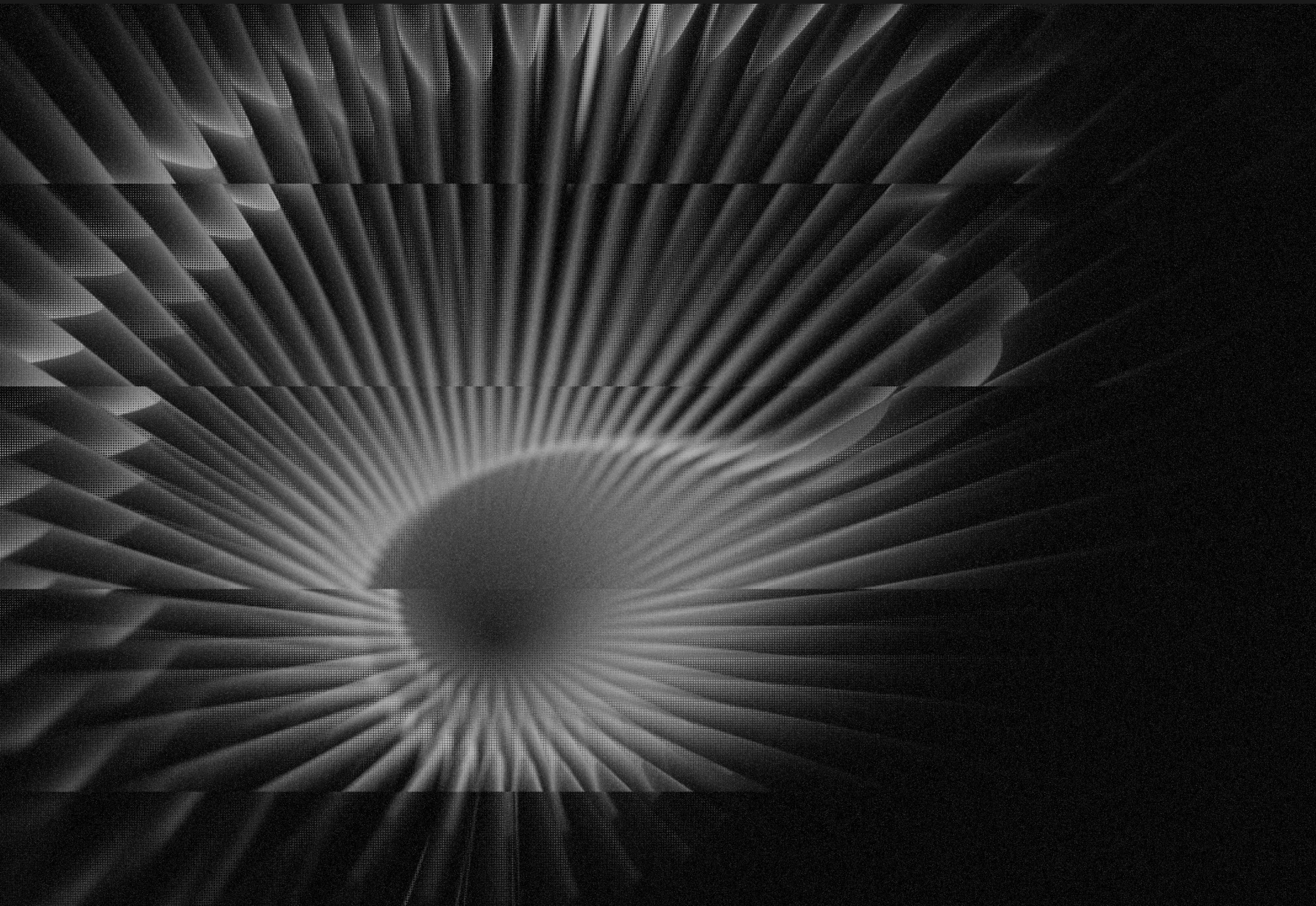
17. Based on an established decision criterion — which may include the steps above or external assistance — the organization’s IT or security authority should formally declare the end of the ransomware incident.

Stage 3: Recovery and Post-Incident Activity

18. Reconnect systems and restore data from offline, encrypted backups, prioritizing critical services.
    - Remember: paying the ransom is no guarantee that your data will be returned.

19. Document the lessons learned from the incident and the response activities to support updates and refinements to the organization’s policies, plans, and procedures, and to guide future exercises based on them.

20. Consider sharing the lessons learned and Indicators of Compromise (IoCs) with law enforcement or relevant industry organizations to help strengthen the broader community.



Leverage External Intelligence to Anticipate Attacks

Axur strengthens ransomware defense by acting where criminals start, outside the corporate perimeter.

Our platform continuously monitors leaked credentials, sensitive data, and exposure points across your organization's external attack surface and that of your suppliers, intercepting access that could be sold to ransomware operators.

With this early visibility, security teams can block compromised credentials, patch critical vulnerabilities, and drastically reduce the chances of intrusion before an attack even begins.

Beyond prevention, Axur accelerates incident response. Our intelligence on ransomware groups' tactics, techniques, and procedures feeds detection and investigation tools, making it easier to identify unauthorized access and quickly contain lateral movement.

Through automated analysis, actionable data, and intelligent dashboards, your team gains an advantage over a dynamic criminal ecosystem and can maintain business continuity and reputation, even under high-pressure scenarios.

Strengthen your ransomware defense

BOOK A DEMO

Discover all our solutions at **axur.com**

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CleanDNS Trusted Reporter

///AXUR