MITIGA

Developing Ransomware Readiness

Preparing Your Enterprise for Today's Most Dangerous CyberThreat

The Growing Ransomware Threat

Today's enterprises are confronting confronting cyber risks of remarkable size and scope. High-profile events have increased awareness of the problem. These include an attack on workforce management software company Kronos that may have delayed the paychecks of as many as 40 million workers in tens of thousands of organizations around the globe[1], and the Lapsus$ ransomware gang's takedown of Portugal's largest TV and media conglomerate over a New Year's holiday weekend[2]. Still, criminals continue to expand their capabilities, disseminate malware more efficiently and demand ever-larger payments. Over the past couple of years, we've witnessed a sea change in ransomware operators' sophistication and the severity of the threat.

As a result, organizations are looking to meaningfully reduce the risk that ransomware poses to their operations, reputations, and futures. They must invest in boosting resilience by proactively preparing incident responders to scope, assess, and contain attacks rapidly with solutions built for modern cloud environments.

In essence, three trends are driving the need for a shift in approach:

1. The rise of so-called double-extortion attacks, in which ransomware operators both encrypt and exfiltrate data, enabling them to demand payment even if victims have usable, reliable backups on hand.

2. The increasing professionalization of cybercriminal networks, with groups of ransomware operators selling access to a victim's environment via an as-a-service model.

3. The growing complexity of ransomware attack sequences, which today can involve multiple threat actors and incorporate additional components, such as simultaneous distributed denial-of-service (DDoS) attacks, to further increase the pressure on victims.

1 "Christmas pay for police, nurses at risk after Kronos hit by ransomware," The Stack, December 2021.
2 "Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel," The Record, January 2022.

Ransomware Attacks by the Numbers

The expanding ransomware threat further ups the ante by making response speed absolutely critical: **victims of today's double-extortion attacks often have 48 hours or less to respond** before data is released. And modern ransomware operators are capable of moving laterally across an environment to find, exfiltrate, and encrypt data faster than ever before.

An Explosion in the Number of Attacks

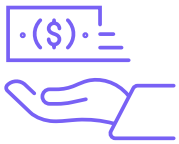
There were **304.7 million ransomware attacks in the first half of 2021 alone**, a 151% increase from the entirety of the previous year.

*- **SonicWall,** Mid-Year Update: 2021 SonicWall Cyber Threat Report*

Don't Expect an "Average" Ransom Payment

The highest confirmed ransom payment is $40 million USD by CNA Financial in May 2021

*- **Bloomberg,** CNA Financial Paid $40 Million in Ransom After March Cyberattack*



Greater Damage, Higher Costs, More Sophistication

- **$139,739 was the average payment made by a ransomware victim in Q3 of 2021.**
- **83.3% of ransomware attacks over the past year included data exfiltration** or the threat of data exfiltration.
- **83% of ransomware attacks involved lateral movement across the victim's environment.**

*- **Coveware,** Ransomware Research, "Ransomware attackers downshift to 'Mid-game' hunting in Q3 2021."*

The Payment May Be the Least Expensive Part of the Attack

$4.62 million was the average total cost of a ransomware-related breach in 2021. This includes the estimated costs of escalation, notification, lost business, and response. It does not include the cost of the ransom.

***IBM Security,** Cost of Data Breach Report 2021.*

The Evolution of the Modern Ransomware Scourge

As a category of cybercriminal attack, ransomware had humble origins. The first-known ransomware attack took place back in 1989, when criminals mailed floppy disks containing a file-encrypting trojan to victims. Once installed, the malicious software displayed a message saying that they need to mail payment to an address in Panama to regain access to their files.[3]

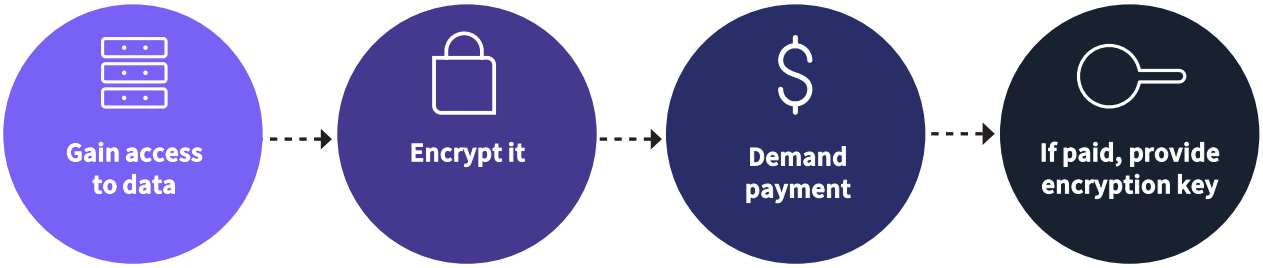
Although this early attempt at software-driven extortion was laughably unsophisticated (security researchers developed and released a free decryption tool to combat the trojan within days), since then ransomware has evolved into one of the most prolific and dangerous cyber threats faced by the modern world.

For ransomware to pose the far-reaching menace to enterprise networks and organizational computing ecosystems that it does today, criminals needed to:

- Find a way to collect anonymous digital payments (the advent of Bitcoin and other cryptocurrencies served this purpose)
- Develop strong encryption algorithms
- Cultivate strategies for disseminating malware across victim environments rapidly and widely

By May 2017, when the WannaCry ransomware attack wrought havoc for more than 230,000 victims around the world, cybercriminals had figured out how to achieve these aims on a massive scale.[4] In the process of doing so, they developed the classic ransomware attack sequence.

In the classic ransomware attack sequence, cybercriminals need to take only four basic steps:

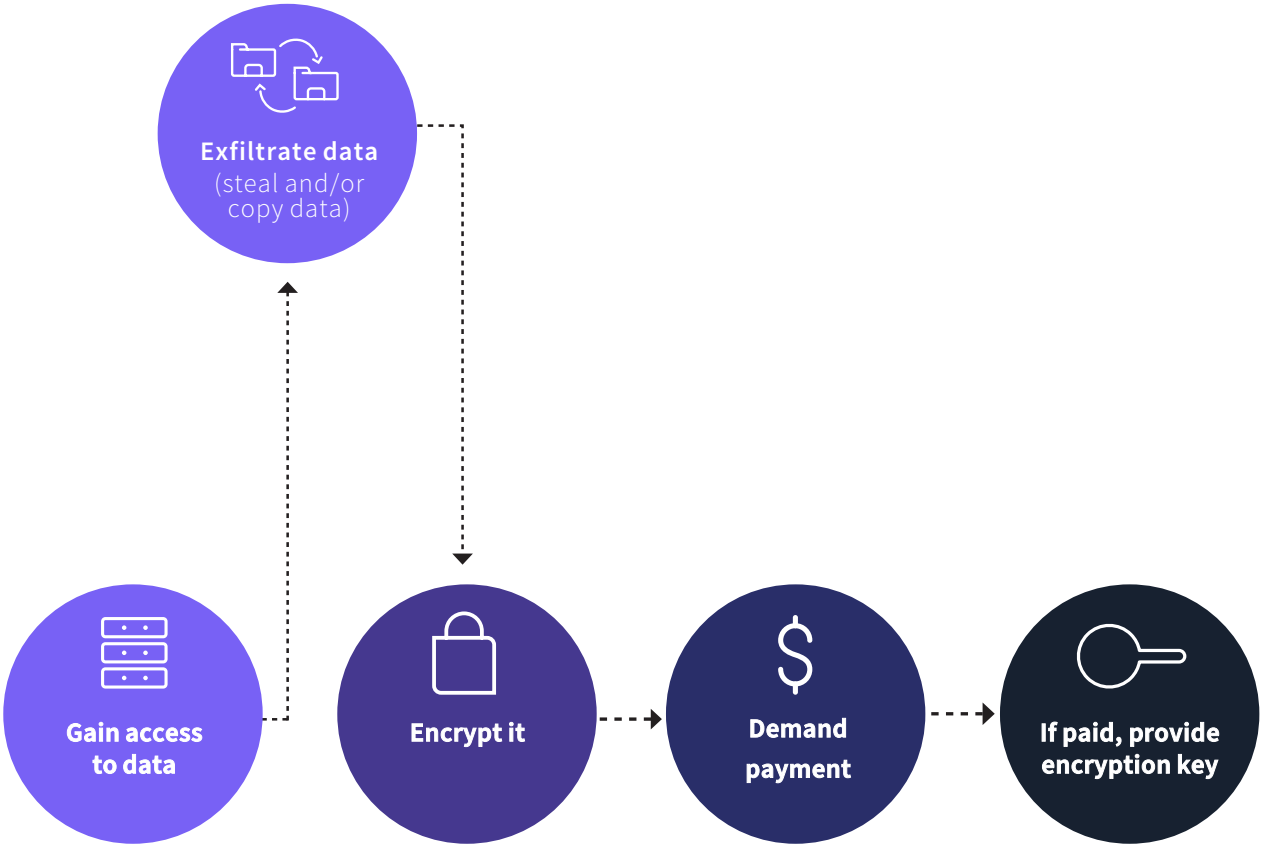


3 "30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world," Danny Palmer, ZDNet, December 2019.
4 "WannaCry ransomware crisis, one year on: Are we ready for the next global cyberattack?" Danny Palmer, ZDNet, May 2018.

The Rise of Double Extortion

The modern ransomware attack sequences that have become popular today are more complex. They often involve longer attacker dwell times, which gives ransomware operators the chance to find and exfiltrate sensitive data as well as the ability to wait for the most opportune moment to launch the attack. It's also common for today's ransomware operators to encrypt and/or compromise backups, and to perform ongoing defense evasion and maintain persistence in the victim environment.

In particular, the last two years have seen a dramatic rise in the number of double extortion ransomware attacks. At a minimum, these attacks involve an additional step beyond the classic ransomware attack sequence:



New Response Strategies are Required

In today's world, where ransomware operators commonly exfiltrate data, maintaining reliable backups is no longer an adequate defensive strategy. The modern ransomware **attack landscape is far more complex** than that of the past. This means that incident investigation demands **greater forensic capabilities.** Victims must be able to investigate the full scope of the incident before beginning negotiations with the criminals.

If you can't answer these questions with confidence, you're not ready to make a decision about whether or not to pay the ransom. And today's ransomware attacks often give victims **no more than 48 to 72 hours** before publishing sensitive information to a leak site.

Questions to answer before beginning negotiations with the attackers:

- How long have the attackers maintained access to your environment?
- Will the attackers continue to have persistent access even after a ransom is paid?
- Have the criminals exfiltrated sensitive data? (It's not uncommon for ransomware operators to claim that they have data when they actually don't, or to pretend to have more data than they do).
- If so, how much data do they have, what data do they have, and how sensitive is it?

How Modern Ransomware Attacks Have Evolved

IR Phase	Classic Ransomware Attack	Modern Ransomware Attack
Prepare	• Backups	• Backups • Forensic Data
Identify/Investigate	• What part of the network was encrypted?	• What part of the network was encrypted? • What part of the network was accessed by the attacker? • What data was exfiltrated?
Contain	• Stop Encryption	• Stop encryption • Notify on data breach
Eradicate	• Remove malware	• Remove malware • Block attacker‘s access to the network
Recover	• Use backups or key provided by attacker	• Use backups or key provided by attacker
Lessons Learned	• Review controls • Backups • Exercise	• Some additional forensic data and investigation capabilities • Review controls • Backups • Exercise

Responding to Modern Ransomware Attacks: Five Steps to Take

01

Identify

Understand what data has been encrypted, and also understand the attack sequence, which resources the attackers were able to access, which data was exfiltrated, and how. If an attacker encrypted the environment, stole sensitive data, and published some of it as a proof-of-concept, it's critical to know whether the attackers have all the data or just some of it. It's impossible to gather that knowledge without doing a thorough investigation.

02

Contain

Stop the spread of malware or ongoing encryption if possible; contain the attacker's access and stop ongoing exfiltration as quickly as you can.

03

Eradicate

Remove the existing assets and access that the ransomware operators possess. The attackers may try to maintain ongoing access to the victim organization's network throughout the negotiation process. Do the criminals know about conversations that are taking place internally? It's essential to close doors quickly and thoroughly. Otherwise, the attackers might have a tunnel into systems that will enable them to keep stealing data or conducting other malicious activities.

04

Recover

Either by restoring from backups or by paying the ransom and decrypting data. On rare occasions, it may be possible to decrypt without the attackers' help, but this isn't common.

05

Lessons Learned

Reduce the risk that an organization will be re-victimized. Based on their investigation in the aftermath of an attack, incident responders may review security controls and backups or conduct additional exercises to prevent future attacks. Having access to historic forensic data immensely improves IR teams' ability to investigate during the attack as well as recover and increase resiliency afterwards.

When a ransomware attack occurs in the cloud, it can be challenging to gather forensic data retroactively in dynamic environments. Many cloud providers only store log data for inadequately short periods of time. Some logs aren't available at all.

This can be especially problematic in recently built cloud environments. During the early days of the COVID-19 pandemic, many organizations adopted new Software-as-a-Service (SaaS) solutions or set up cloud-hosted infrastructures on the fly. Very few organizations have the forensic data collection capabilities in place to conduct a thorough investigation of a ransomware attack. Fewer still store the data for enough time to be able to uncover attackers' initial access and activities. In addition, most organizations have not yet defined which logs are needed for analysis. Teams need to be able to review access to and compromise of the digital assets critical to accomplishing the organization's mission. Almost none can access, analyze, and investigate forensic data at the speed that today's threats demand.

If you're relying on traditional incident response processes, it can take days to get the right data feeds and access to all the logs you need to start an investigation. This is time you don't have when you're facing an immediate ransom demand.

Data sources required for ransomware investigations in the cloud

- Identity and Access Management (IAM) logs showing account activities, including failed login attempts and password changes
- Security tool telemetries
- System and cloud resource activity logs
- Mail flow logs
- Traffic throughput logs (can indicate data exfiltration)
- Configuration change records
- Machine images

Enabling Rapid Recovery from Cloud-based Ransomware Attacks

To ensure faster recovery and accelerate your return to business as usual, your enterprise needs to be able to start incident response immediately and conduct a thorough forensic investigation in hours, not days.

Capabilitiies you need include:

- Collecting and store all the data you need to investigate and respond to cloud ransomware incidents
- Assessing the scope of a ransomware attack rapidly to enable security and leadership teams to manage the associated risks appropriately
- Conducting technical analyses quickly and accurately of whether, how, and if the data in the cloud could have been encrypted, stolen, or deleted
- Preparing technical and executive stakeholders for the challenges they'll face in a ransomware attack by conducting readiness drills and functional exercises on a cross-organizational level

Having searchable, analyzable data at hand is the key to conducting forensic investigations at scale and speed in the cloud. Each organization must capture, store, and prepare the right cloud forensic data so that incident responders and ransomware experts can quickly identify Indicators of Compromise (IoCs) to enable them to assemble the incident's timeline, determine its scope, and make informed business decisions quickly.

How much data do you need?

In 2022, it took an average of 277 days for a "cloud-mature organization" to detect and contain a data breach.

*- **IBM:** Cost of a Data Breach Report 2022*

Do your log retention capabilities exceed this bare minimum?

Protect Your Enterprise from the Full Impact of a Ransomware Attack

The impacts of modern ransomware attacks are significant, and the potential financial and business losses go well beyond the ransom itself.

Lost Business Revenue

66% of ransomware victims report a significant loss of revenue following the attack.

C-Level Talent Loss

32% of ransomware victims reported losing C-level talent as a direct result of the ransomware attack.

Business Closure

26% of ransomware victims were forced to shut down operations for some period of time.

Exorbitant Ransom Demands

35% of the businesses that paid a ransom shelled out between $350,000 and $1.4 million; 7% paid ransoms in excess of $1.4 million.

Employee Layoffs

29% of ransomware victims were forced to lay off employees due to financial pressures resulting from the attack.

*- **Cybereason,** Ransomware Attacks and the True Cost to Business: Report*

From Readiness to Resilience: How Modern IR Solutions Lead the Way

When it comes to real-world readiness, modern ransomware attacks demand a new and different approach. Threat actors stand ready to compromise their victims' environments at great speed, leveraging sophisticated tactics such as double extortion. Some attackers may claim to have exfiltrated sensitive data or reports but are lying about the scope of exfiltration. Accurately evaluating ransomware attacks requires thorough investigation.

In the aftermath of an attack, executives will have to decide how to respond as well as how to manage the risks related to the incident.

> **With modern ransomware attacks, investigation is essential, because it's no longer just about recovery. Instead, it's about increasing readiness and resilience to minimize risks.**
>
> *-Ariel Parnes,*
> *Co-Founder and COO, Mitiga*

Should they notify regulatory authorities? Customers and clients? The public? Would it be worthwhile to consider paying the ransom?

It's impossible to make decisions like these without sufficient information.

Advance preparation, including executive readiness drills and tabletop exercises, can help stakeholders across the enterprise keep their cool in times of crisis. This is the human element that's an essential part of resiliency.

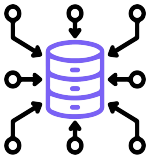
A **modern cloud incident response automation (CIRA) platform** will give internal teams (both technical and executive) as well as third-party providers continuous visibility into the status of the incident and your response. This enables rapid and accurate decision-making, even under pressure.

It's critical to provide key stakeholders with immediate answers to all key questions about the incident, so that they can make decisions based on knowledge and understanding rather than guesswork or "gut feel."

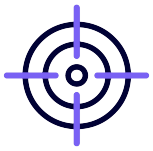
Today's ransomware threats are more prevalent and sophisticated than ever. And modern technology environments – especially cloud and SaaS environments – demand different forensic investigation capabilities and response strategies. Your team must be able to access, analyze, and investigate the right forensic data, without delay. Only with access to innovative incident response and readiness technologies can IR teams begin an investigation rapidly – within minutes of being notified about the incident.

Mitiga's IR2 Platform Delivers

This revolutionary Cloud Incident Reponse Automation (CIRA) solution provides the speed and answers required for modern ransomware reponse.



PREPARE
Proactively gathering the data to ready your enterprise for cloud and SaaS breaches



HUNT
Uncovering emerging attacks across all your cloud and SaaS environments

RESPOND
Dramatically speeding investigation of all your cloud and SaaS breaches

RECOVER
Advanceing your cloud resiliency by providing IR advisory and remediation recommendations

Protect Your Organization: Be Ready for Ransomware Attacks *Before* They Strike

Today's ransomware operators move fast. And their attacks are becoming more frequent, more costly, and more damaging. To minimize the risk to your business, you need to prepare in advance. Mitiga helps customers respond effectively even in the most complex and sophisticated attack scenarios, to help you get back to business-as-usual in record time.

Mitiga provides:

- Cloud security expertise
- 24/7 emergency service
- Cloud incident-readiness SaaS
- Rapid incident analysis
- Situational awareness

Ready to take the next step?

Contact us to learn more about how you can advance your enterprise's ransomware readiness and dramitically accelerate your response times.

Mitiga provides next-gen cloud and SaaS incident response solutions to simplify and dramatically accelerate investigation and recovery.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** + 972-3-978-6654 | **SG** +65-3138-3094