Bitdefender Global Leader In Cybersecurity

Ransomware Revealed: How to Determine If You're a Target

English

Table of Contents

Introduction 3
Evolution of Ransomware 4
A Ransomware Attack, Step-By-Step 5
Top 5 Common Misconceptions 6
How Great *Is* Your Risk? 7
What It Takes to Stop Ransomware 8
Stop Ransomware with Bitdefender MDR 9

Introduction

Every company is at risk of ransomware. Regardless of the company's size, industry, or sector, ransomware continues to be a major threat — and that isn't going to change anytime soon.

Ransomware has become a booming business, complete with its own ecosystem of suppliers, specializations, and affiliate programs. And, as businesses go, ransomware is a lucrative one with a low barrier to entry. Ransomware-as-a-service kits attract non-technical criminals to the ranks of nation states and highly-skilled attackers who leverage ransomware for extortion.

The effort required to bring down ransomware rings illustrates the complexity of these criminal operations. The arrest of a Ukrainian national charged with deploying ransomware to attack businesses and government entities in the U.S. was the result of coordination between the U.S. Attorney's Office, FBI, Europol, and Eurojust. Similarly, detecting and stopping a ransomware attack requires a coordinated effort — one that is risk-informed.

This ebook will show you how to evaluate your organization's risk in the face of rising ransomware threats through insights from Bitdefender's threat research team. By the end, you'll be better positioned to understand your risk profile and the necessary next steps to protect your assets, including the benefits of adopting a Managed Detection & Response (MDR) solution.

Evolution of Ransomware

Like other cyber threats, ransomware has evolved considerably over the past 10-15 years. Early ransomware attacks were often opportunistic and utilized worm-like behavior, focusing on the most direct route to monetization. Today's attacks are highly sophisticated and complex, involving multiple parties with various expertise. However, with the availability of ransomware-as-a-service kits on the dark web, there's no need for advanced technical skills. The low barrier of entry means that practically anyone can get in the ransomware business.

Getting in the business generally means participating in ransomware-as-a-service, a profit-sharing model in which ransomware operators work with affiliates. The ransomware operators develop the malware and run the infrastructure. The affiliates, resembling self-employed contractors, compromise the victims' networks. After a successful breach and deployment, the ransomware operators negotiate and collect the ransom and distribute their shares to the affiliates.

The ransomware-as-a-service model benefits attackers:

- Ransomware groups can run at scale, attacking multiple organizations simultaneously.
- Threat actors are motivated to find new ways to maximize the potential yield.

In the last few years, the power has shifted from those who control the ransomware code to those who control access to the networks. So, while ransomware operators lead negotiations and get all the media credit for successful attacks, the largest share of the profit goes to the affiliates, who often receive up to 80 or 90% of payment. Meanwhile, ransomware operators reinvest some of their profits to advance their tactics and tools for the next attack.

Disrupting Business

One way to bring down ransomware criminals is to disrupt their cash flow. Bitdefender, in coordination with Europol, the Romanian Police and law enforcement authorities in several countries, released a decryption tool for GandCrab, one of the world's most prolific ransomware. Together, the two versions of the tool helped close to 10,000 victims retrieve their encrypted files, saving them USD 5 million in ransomware payment.

A Ransomware Attack, Step-By-Step

Modern ransomware attacks focus on maximizing damage and pressure. Attackers move low and slow, spending weeks or months preparing to execute an attack. During this time, the attacker may scan the target's network for vulnerabilities, identify privileged users, purchase user credentials on the dark web, and gather publicly available information about the target's infrastructure.

Depending on what was uncovered during reconnaissance, the attacker accesses the network one of three ways:

- A misconfiguration
- Legitimate identity and access credentials
- Exploiting a vulnerability in the environment

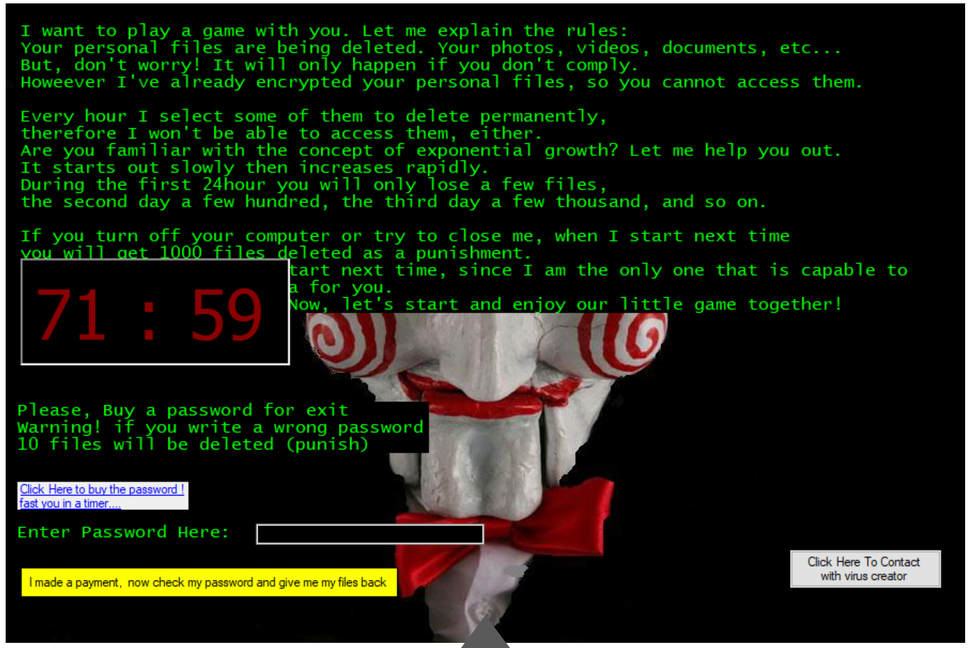
Once inside the network, the attacker spends the time to become acquainted with their surroundings — mapping the infrastructure, exfiltrating sensitive data, understanding the security controls and how to circumvent them. They look for anything that can be used to make the biggest possible impact and increase pressure on the target. This includes tracking down the company's cyber insurance policy and calculating a ransom demand the victim is likely to pay.

Insights from Bitdefender Research Team: In most ransomware cases, 99% of what happens inside the network during an attack is manual work. Because the commands are not automated or templated, the activity bypasses detection mechanisms.

Now, the attacker starts the encryption mechanism and notifies the target of the ransom.

If the target doesn't comply with the attacker's demands or the attacker simply wants to shame the company, they'll commit double extortion and publicize the attack via extortion blogs and forums, or even start auctioning some of the target's data or giving it away for free.

If the victim still doesn't pay up, the attacker may commit triple extortion — calling or emailing journalists or the victims' customers.



> **"The company you're doing business with has been compromised. They have been infected by ransomware and didn't notify you, so we are."**

Top 5 Common Misconceptions

"It won't happen to us."

Truth: No company or organization is safe from a ransomware attack. Ransomware is not limited to the private sector or any single industry. If you have important data, you're a potential target. You could be a target for six months before the initial security breach or simply a lucky shot.

"We'll negotiate our way out of it."

Truth: Ransomware operators are criminals who are expert negotiators. Any attempts at negotiations are likely to drive attackers to further means of extortion, such as notifying journalists, customers, etc., of the attack.

"It's pointless to involve law enforcement."

Truth: Companies simply do not have the wherewithal to deal with ransomware alone. The more companies that reach out to law enforcement, the more effective they can be in stopping ransomware operations. Law enforcement will work faster if they know the problem is bigger and can better prioritize higher risk operations. And, unlike your vendors, law enforcement can access an attacker's technology to take it offline.

"We'll just pay the ransom. Isn't that what cyber insurance is for?"

Truth: Paying the ransom isn't a guarantee you'll get your data back. The decryption key may not work, or your data may be corrupt. Furthermore, the attacker has a copy of your data and can sell or leak it on the dark web, regardless of whether you pay. It's also worth noting that in some jurisdictions it is actually illegal to pay a ransom.

"But we have backups."

Truth: Backups do not solve the problem of ransomware any more than paying the ransom. The risk to your reputation remains, as well as the risk of a data breach. The attacker knows your environment, can break in again the same way if the original issue was not fixed and knows other ways to break in.

How Great *Is* Your Risk?

Every organization is at risk of ransomware, but some are at greater risk than others. Some companies make for easier targets due to a lack of standards and best practices. Others are at greater risk because they operate legacy technology. To gauge your risk, assess the following:

Visibility

How well do you know your environment? To protect your assets, you need to know what assets you have, where they are stored, and who has access to them, including supply chain/ third party access. Insights from Bitdefender Research Team: This information is crucial for making the risk decision of whether to pay a ransom.

Backups

Do your critical systems have backups? Always keep an offline backup of your critical systems and data.

Patch Management

Do you have mature patch management processes? Patch management processes should be standardized and automated, ensuring patches are deployed in a timely manner. Keep hardware and software up to date with the latest versions and avoid legacy OEM hardware and software that are no longer supported. These systems are at greater risk of being targeted by ransomware because they are often unpatched and unmanaged. In addition to being an easy target for attackers, successful exploitation of one of these systems can bring operations to a standstill.

Vulnerability Management

Do you have a formal vulnerability management program and secure software development processes? It only takes one vulnerability, one set of default credentials, or one exposed RDP connection to become a target. Vulnerability management should take a risk-based approach to prioritizing remediation of vulnerable critical assets. Run penetration tests regularly and integrate security into every step of software development lifecycle.

Identity and Access Management

Are you adhering to IAM best practices? Compromised credentials can lead attackers to a treasure trove of data. Identity and access management should follow best practices such as the principle of least privilege to reduce the scope of access, enforced password rotation, and formalized policies and processes for revoking access when employees change roles or leave the company.

What It Takes to Stop Ransomware

While a solid foundation of cybersecurity processes and controls can help reduce the risk of a ransomware attack, they can't eliminate it. To stop ransomware, organizations also need:

1 Good Cyber Hygiene

Organizations must impart good cyber hygiene to their users, giving them the necessary skills and habits to maintain the safety and security of their data and systems. Regular and consistent employee education and awareness training help enforce a security-centric mindset and practices that help prevent security breaches. While being a necessary, cost-effective start, good cyber hygiene is just that: a start. Organizations also need...

2 24x7 Security Monitoring

Attackers actively avoid detection. They use legitimate credentials to access the network late at night or on the weekend when no one is looking. A 24x7 security monitoring capability that includes anomaly detection can help detect attacker activity disguised as legitimate user activity at all hours of the day and night.

3 Endpoint Detection and Response (EDR)

EDR combines continuous monitoring of endpoints with detection capabilities and automated response actions to stop active threats in real-time. Your EDR provider should have a robust library of signatures for known ransomware and have the resources to write signatures for new ransomware.

4 Threat Hunting

Attackers are continually advancing and improving their tools and techniques, rendering existing detection methods ineffective. When an attacker bypasses detection, threat hunting provides a comprehensive approach to reducing system compromise and attacker dwell time. Ideally, organizations conduct periodic, targeted threat hunting as well as proactive, risk-based threat hunting triggered by expert analysis of the global threat landscape.

5 Threat Intelligence

To proactively stop ransomware, organizations must also look beyond their own environment. They need threat intelligence that includes current cyber threats, geopolitical activity, and vertical-specific data trends, which they can then apply to their own environment. For example, understanding if and how the company's brand appears on the dark web can shed light on who and how the organization may be targeted.

Stop Ransomware with Bitdefender MDR

Few organizations today have the resources to build a fully functioning security operations center (SOC), complete with 24x7 monitoring and threat hunting capabilities, but every company needs protection against ransomware. That's where Bitdefender MDR comes in.

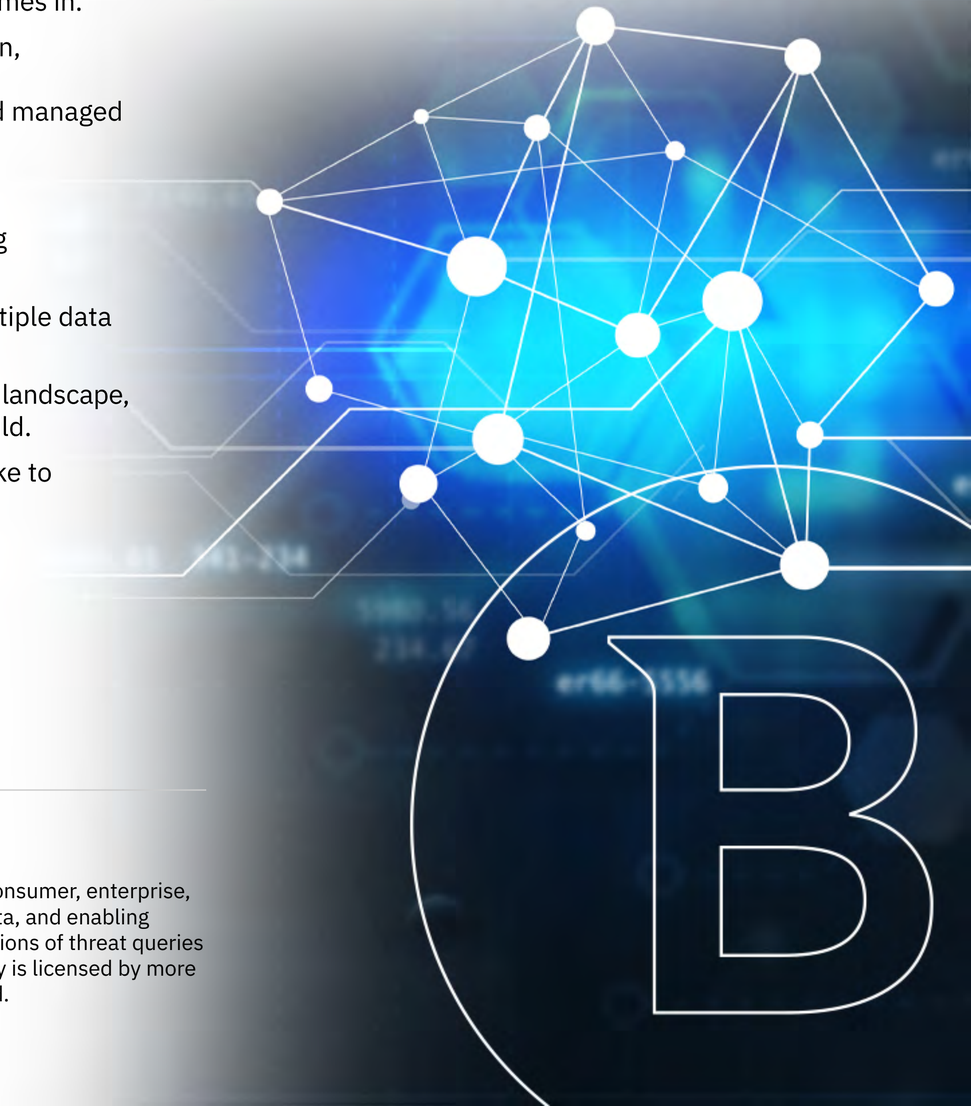
Bitdefender MDR enables organizations to stop ransomware with 24x7 security monitoring, and advanced attack prevention, detection, and response from a team of experts you can hold accountable. Besides the benefit of our endpoint technology, GravityZone® Business Security Enterprise, and its comprehensive feature set, organizations receive dedicated support and managed onboarding through the security expertise in Bitdefender's Global Security Operations Center.

Bitdefender MDR features:

- 24x7 monitoring and response to eliminate operational overhead of managing security alerts and events while providing continuous protection against ransomware.
- Threat hunting via continuously monitoring the global threat landscape to best protect your organization. We utilize multiple data sources and proactive analysis to investigate anomalies and suspicious activity that detection alone will miss.
- Bitdefender Labs, threat intelligence teams, and security researchers continuously monitor all aspects of the global threat landscape, using the knowledge gained to drive threat hunts across your systems and build signatures to stop new threats in the wild.
- Incident root cause and impact analysis for comprehensive after-action reporting. Understand the changes you can make to harden your environment.
- Dark web monitoring to discover leaked organizational information.

Learn more about Bitdefender MDR

Together, Bitdefender's industry renowned endpoint technology, industry leading research team, and expert cybersecurity practitioners, give organizations a proactive solution to reduce ransomware risk and stop a ransomware attack.



About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 180 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Bitdefender

Trusted. Always.