digital hands®

The Billion-Dollar Extortion Scheme:

How to Reduce the Impact, Spread, and Severity of Ransomware with Managed Detection and Response (MDR).

Part 1 of a 7 part series

Table of Contents

Ransomware attacks have made headlines for so many years, they should feel like old news by now. Instead, ransomware actors have continued to shatter records, as well as evolve their tactics to make this threat even more damaging for victims across all sectors.

Some data shows that the extent of the impact is mind-boggling: as many as 83% of organizations were targeted by ransomware in the past 12 months, and 78% of those paid the ransom. Since data exfiltration is now a part of most ransomware attacks and double- and triple-extortion schemes are prevalent, more victims are forced to pay in hopes to avoid a data leak or reputational damage.

Why every CISO and SOC should care about ransomware

Surveys and incident data analysis show that finance, healthcare/pharmaceutical, manufacturing, technology/IT services, and government are the top sectors targeted by ransomware actors. However, no sector can breathe easy, especially since ransomware is the most prevalent and one of the costliest types of attacks across all sectors.

For organizations, the implications range from operational downtime to data loss (even with backups). And the stakes are getting higher:

- ✓ Almost three-fourths of small and medium-sized organizations say a ransomware attack "would be a death blow."
- ✓ Reported recovery costs from ransomware grew by 50% in 2024, to an average of $2.73 million excluding the ransom.
- ✓ Ransom costs grew fivefold in the same period, to an average of $2 million.
- ✓ 87% of ransomware attacks cause business disruption, even when ransom is paid.
- ✓ Reputational damage can be costly as well — 75% of consumers say they would switch to another brand after a ransomware attack.

The motivations behind these attacks are clear: cybercriminals go where the money is. In 2023, for instance, organizations spent an estimated record of $1.1 billion on ransomware payouts. And 2024 was on track to surpass that number.

[1] Check Point, July 2024

But it's not just the financial gains that drive the proliferation of these attacks. The booming ransomware-as-as-service market is abundant with inexpensive ransomware kits and various other plug-and-play services. This low barrier to entry incentivizes new waves of cybercriminals to get started without much sophistication.

The high degree of success is also a key driver. For example, threat actors can easily set up a testing environment in the common types of collaborations suites that organizations use. Since many organizations simply use these apps' off-the-shelf defenses, the attackers can test their capabilities efficiently, as well as fine-tune their tactics.

With such a lucrative business, cybercriminals are not going to slow down ransomware activity any time soon.

The rise of artificial intelligence and machine learning will only make things worse. Malicious actors are taking advantage of these emerging technologies to automate attacks, conduct reconnaissance more efficiently, fine-tune techniques to avoid detection, and better target organizations. Security researchers are already proving the potential of AI-powered malicious frameworks (e.g, RansomAI and EGAN), and it's only a matter of time before these kinds of tools are seen in the wild.

[8] Sophos

How a ransomware attack may unfold

The adversaries use a variety of tactics, techniques, and procedures through several stages of the attack. **Here is a plausible scenario of the attack lifecycle:**

STEP 1

Assess organizations for weaknesses (recon)

Weaknesses could be anything from open ports or vulnerabilities in software, to legacy systems or weak access controls. For instance, attackers may scan the environment for VPNs that have recently disclosed vulnerabilities published in databases (CVEs).

STEP 2

Gain initial access

Attackers deploy malware through phishing emails, employ exploit toolkits targeting software vulnerabilities, or use compromised credentials to gain a foothold inside the targeted organization.

STEP 3

Maintain access and escalate privileges

The bad actors use tactics like executing more malware to harvest credentials or exploiting misconfigurations to escalate privileges and gain admin control. If extortion is part of the plan, they exfiltrate data before moving to the next phase.

STEP 4

Spread through the network and deploy the payload

Often, the attackers encrypt or destroy backup systems first. Before launching the ransomware across the network, they may test it on a few network systems to make sure they can evade security tools.

STEP 5

Encrypt critical files and systems across the network

Victims typically see a message that their files have been encrypted, along with a ransom demand.

How to leverage managed detection and response services to protect against ransomware

It’s only a matter of time before your organization is the target of a ransomware attack. Your job is to be prepared with the right blend of people and automation to reduce the damage. This is where MDR comes it, helping you limit the impact, spread, and severity of a ransomware attack.

Let’s say a threat actor has exploited an unpatched Remote Desktop Protocol (RDP) system while flying under the radar of security tools. MDR can detect anomalous behavior like unusual access patterns, isolate the server, and prevent ransomware from encrypting additional files. **Here's what the MDR workflow may look like, using a combination of automated tools and human experts:**

1. Detection and response

The MDR vendor uses a combination of detection technologies and human analysts to identify abnormal file encryption activity and suspicious network traffic that may indicate threats that the customer’s security stack did not detect or respond to automatically. The MDR provider’s platform brings together correlated indicators of compromise and consolidates telemetry from multiple sources including servers, workstations, user accounts, and network traffic while leveraging tools like SOAR to enrich the alert. Since EDR tools alone are not 100% effective, the MDR platform has visibility across multiple layers of the environment, with enough telemetry and cross-correlations to respond beyond a single endpoint or technology layer.

2. Automation

Once the threat is detected at any of the layers, the MDR platform uses intelligent, automated rule sets to immediately isolate infected systems and disconnect any paths to lateral movement. Due to the cross-correlated telemetry at the different layers, these automated actions take place as quickly as within seconds to stop lateral movement — typically far ahead of the response generated by the customer’s EDR tool. The automations are based on the customer’s needs. For instance, some may not want to automatically shut down or disconnect the device of a high-profile role like the CEO, requiring an exception to the auto-isolation rule.

3. Human investigation

SOC analysts confirm the scope of the attack and determine if data exfiltration occurred. Devices that were exempt from automated quarantine, such as the CEO’s endpoint, are prioritized for analyst review. Investigators also analyze incident data to determine if a rollback is needed for the auto-isolated devices. In the event of false positives, endpoints are removed from quarantine.

4. Action

Affected systems are restored from secure backups. Depending on the MDR solution, MDR security analysts may also conduct root cause analysis to ensure the threat is completely eradicated. The MDR experts guide the customer on how to prioritize vulnerability patching and remediation.

Benefits of MDR beyond ransomware defense

Digital Hands' Real-World MDR offers much more than defense against the threat of ransomware.

Your MDR partner can augment your in-house SOC or security team, enabling them to:

- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Increase response time with automated containment and expert-led investigations, reducing the window of opportunity for the adversary.

Buyer's Guide

Not sure where to start?

Get your MDR Buyer's Guide to understand key evaluation criteria and the 8 must-ask questions before you buy.

Download Now