ThreatDown™
Powered by Malwarebytes

2024 Ransomware Emergency Kit

The ransomware cheat sheet and what to do when attacked

Contents

Understanding the threat

- **Ransomware targets entire organizations**
- **Attacks aim to stop organizations from functioning**
- **Organizations of all sizes are at risk**

Modern ransomware attacks operate on a different scale to the viruses and malware of old. When planning how to prepare and respond, organizations should think about the potential impact on their business in the same way as they think about natural disasters.

In a ransomware attack, criminal hackers break into a computer network and try to compromise the organization that owns it. They may steal company secrets and threaten to leak them, or encrypt the organization's files so it cannot function. Many ransomware gangs do both.

Attackers can spend days or even weeks inside a victim's network and demand huge cryptocurrency payments in return for decryption keys, or for destroying stolen data instead of leaking it.

The average ransomware payment in Q4 2023 was $570,000,[1] and the highest confirmed demand in 2023 was $80 million.[2] Ransom negotiations can take weeks to conclude, and the average cost of an attack, excluding the ransom, is $4.7 million.[3]

The target in a modern ransomware attack is an entire organization. All types of organizations have been attacked, including businesses of all sizes, hospitals, law enforcement agencies, governments, charities, and critical infrastructure.

287 DAYS
The average time it takes a business to fully recover.[4]

$4.7M
The average cost of a ransomware attack.

$80M
The largest confirmed ransomware demand in 2023.

[1] Coveware, New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying, https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying
[2] Malwarebytes, Royal Mail schools LockBit in leaked negotiation, https://www.threatdown.com/blog/royal-mail-schools-lockbit-in-leaked-negotiation
[3] IBM, Cost of a data breach 2023, https://www.ibm.com/uk-en/reports/data-breach
[4] Ransomware Taskforce, Combatting Ransomware, 2021, https://securityandtechnology.org/ransomwaretaskforce/report/

Anatomy of a ransomware attack

Ransomware is typically deployed as the last act in a sophisticated infiltration of networks by criminal hackers. Every ransomware attack is different, but they often follow a predictable pattern, which can be broken down into five phases.

Breach

Attackers gain unauthorized access to a computers with malware; by phishing, guessing or finding a remote password; or through a software vulnerability. This can occur months before the attack phase.

The best way to stop a ransomware attack is to prevent the initial breach. This requires web protection, effective vulnerability and patch management, hardening of remote desktops, and users who can identify and report phishing attempts.

Infiltration

Attackers quietly explore networsk and prepare their attack. They may steal data, and may try to disable security software and backups.

Since preventing every breach isn't possible, structure and monitor networks to identify suspicious activity quickly and stop intruders before the attack phase.

Attack

Attackers run ransomware throughout the network, often at night or the weekend. Critical business operations stop. Ransom notes explain how to negotiate with attackers.

Stopping attacks requires multiple layers of security defense, anomaly detection for unknown "zero-day" threats, and ransomware prevention technology.

Response

Attackers demand a ransom, which could be millions of dollars. They will issue deadlines and may threaten to leak sensitive data.

Restore critical operations while talking to customers, suppliers, insurance, press, lawyers, law enforcement, and others. Offline backups and a plan will be critical.

Recovery

Whether the attack is successful or not, attackers may still be the network, and lingering malware or artifacts could cause reinfection. Any willingness to pay a ransom will have been noted.

After restoring critical operations, focus on discovering what happened, expelling the attackers, and denying them access. Finally, harden the network against a repeat attack.

To pay or not to pay the ransom?

Most experts and government agencies do not recommend paying a ransom. Ransom payments incentivize further attacks and fund the continued development of ransomware, making everyone less secure. Before paying the ransom, consider the following carefully:

1. **Decryption often fails.**
   Ransomware gangs' decryption tools are poor quality and may lead to partially corrupted data. In May 2021, Colonial Pipeline paid a $4.4 million ransom. The decryption app it received was so slow it rebuilt systems from backups instead.[5]

2. **You are trusting criminals to keep their word.**
   When global law enforcement agencies disrupted the notorious LockBit ransomware gang in February 2024, they discovered the criminals had not deleted all the data belonging to victims who had paid a ransom.[6]

3. **The cost of recovery can dwarf the ransom.**
   After paying the ransom, extensive clean-up, and upgraded protection to prevent future attacks will be needed.

4. **Paying leads to repeat attacks.**
   Attackers will note any willingness to pay, and that you were not prepared to withstand an attack. As many as 80% of ransom payers suffer a second attack.[7]

FBI

WARNING

The FBI does not support paying a ransom in response to a ransomware attack.
Paying a ransom doesn't guarantee you or your organization will get any data back.

[5] Forbes, Here's Yet Another Reason Ransomware Victims Shouldn't Pay The Ransom, 2021, https://www.forbes.com/sites/leemathews/2021/05/29/heres-yet-another-reason-ransomware-victims-shouldnt-pay-the-ransom/

[6] National Crime Agency, International investigation disrupts the world's most harmful cyber crime group, https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

[7] Cybereason, Ransomware: The true cost to business, 2021, https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

Ransomware prevention checklist

What to do:	Breach	Infiltration	Attack	Restoration	Recovery
Create an inventory of assets including hardware, software and data	✓	✓			
Audit the network for unknown computers and services	✓	✓			
Disable Internet-facing systems, services, and ports not needed	✓	✓			
Perform regular vulnerability scans	✓	✓			
Patch systems regularly, prioritizing the most vulnerable and critical	✓	✓			
Ensure systems are properly configured, and security features are enabled	✓	✓			
Harden remote access with MFA, password rate limits, and password lockouts	✓				
Deploy endpoint security software to all endpoints and servers	✓	✓	✓		
Provide staff with cybersecurity awareness training	✓	✓			
Implement a process for reporting and responding to suspicious activity	✓	✓	✓		
Document the network structure and data flows		✓			✓
Use network segmentation to subdivide computer networks		✓			
Use least-privilege access for all systems and services	✓	✓			
Use allow listing to ensure that only authorized software can run		✓	✓		
Restrict the use of legitimate tools commonly used by attackers[8]		✓			
Harden domain controllers according to the latest best practice[9]		✓			
Monitor the network and endpoints using IDS, EDR and SIEM		✓	✓		✓
Make regular, comprehensive backups, keeping at least one copy offline				✓	
Have a process for restoring computers from clean system images				✓	
Practice restoring systems from backups				✓	
Create an incident response plan[10] that aligns with regulations			✓	✓	
Create a critical asset of list of what needs to be restored first				✓	

[8] This is known as "living off the land." The Living Off The Land Binaries and Scrip (LOLBAS) project maintains a list of legitimate software used by attackers at https://lolbas-project.github.io/

[9] Domain controllers are a prime target for attackers. Microsoft maintains a guide to securing domain controllers against attack at https://docs.microsoft.com/ven-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack

[10] You can find a response plan template at https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md

Useful resources

CISA Ransomware Guide

The Cybersecurity and Infrastructure Security Agency (CISA) maintains a detailed Ransomware Guide.

Learn more

Among other things, it contains a very useful Ransomware Response Checklist. CISA also maintains a Ransomware Readiness Assessment tool.

Learn more

The anatomy of a Medusa ransomware attack: ThreatDown MDR team investigates

In early April 2024, a prominent service chain in the United States fell victim to a Medusa ransomware attack. This case study dissects the attack's framework, key indicators of compromise (IOCs), and steps the ThreatDown MDR team took to mitigate the infection.

Learn more

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has published a comprehensive Cybersecurity Framework to help organizations better manage and reduce cybersecurity risk.

Learn more

Understanding ransomware reinfection: An MDR case study

Victims of ransomware are vulnerable to repeat attacks unless they discover how they were compromised and remove the backdoors, accounts, and tools their attackers used. This article details a real-life episode where MDR mitigated a resilient ransomware reinfection by the Royal ransomware gang.

Learn more

10-step ransomware recovery plan

If you are dealing with a ransomware incident you may be working under extreme pressure. Ransomware may still be encrypting files, attackers may have issued ultimatums, and your organization will be desperate to get up and running again. **Ask for help, prioritize your actions, communicate clearly, and take care of each other.** We recommend you take the following actions, in order:

1. **Contain the attack.**
   Isolate infected systems or networks to limit the impact of the attack. Your priority should be containing the attack but if you can do so while also preserving evidence by leaving affected systems turned on, do so.

2. **Establish the scope of the attack.**
   Understand what systems and what kind of data are affected, and prioritize critical systems for recovery.

3. **Communicate with stakeholders.**
   Stakeholders may include senior management, PR, the legal team, cyber-insurance providers, security vendors and law enforcement.

4. **Seek assistance.**
   Consider seeking expert assistance from local and national law enforcement, vendors or other third parties familiar with ransomware recovery.

5. **Preserve evidence.**
   With the help of law enforcement and third parties, try to preserve evidence from the attack if you can.

6. **Identify the ransomware being used.**
   This will help you discover if a decryptor is available, and it will inform the specifics of containment and clean up.

7. **Contain the breach.**
   Try to identify systems and accounts used in the initial breach, and any precursor malware or persistence mechanisms left by the attackers.

8. **Rebuild systems.**
   Use known good system images and backups to restore critical systems. Take care to segregate clean systems from affected systems.

9. **Reset, patch, upgrade.**
   Reset passwords, patch and upgrade software, and instigate any additional security checks necessary to prevent a recurrence of the attack.

10. **Document lessons learned.**
    Ransomware is constantly evolving. Use what you have learned from this attack to better prepare for the next one.

Too much for your team? ThreatDown MDR can help.

Talk to an expert >

ThreatDown™
Powered by Malwarebytes

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054 USA
+1-800-520-2796