Malwarebytes cyberprotection

RANSOMWARE EMERGENCY KIT

If you are dealing with a ransomware attack right now, go straight to the **10 step ransomware recovery plan** section on page 8 and call us at **1-800-520-2796, ext. 3.**

Ransomware is a clear and present danger to organizations of all sizes. This emergency kit tells you what you need to know to understand the threat, how to harden your business against it, and what to do if your organizations is attacked.

Contents

Understanding the threat

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

Ransomware is a type of malicious software that encrypts computer files, making them unusable, and demands a cryptocurrency payment to decrypt them. The only way to decrypt files locked by ransomware is with a decryption key held by the attackers.

It has become increasingly common for ransomware gangs to steal an organization's data as well, to gain more leverage during ransom negotiations.

Modern ransomware is used in so-called "big game" attacks that target an organization's entire computer network. All types of organizations have been attacked, including organizations of all sizes, hospitals, law enforcement agencies, governments, charities, and critical infrastructure.

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 would think about a natural disaster.

287 days

The average time it takes a business to fully recover[1]

$312k

The average ransom payment in 2020[2]

11 sec

Experts predict a ransomware attack will now occur ever 11 seconds[3]

[1]Ransomware Taskforce, *Combatting Ransomware,* 2021, https://securityandtechnology.org/ransomwaretaskforce/report/

[2]Ransomware Taskforce, *Combatting Ransomware,* 2021, https://securityandtechnology.org/ransomwaretaskforce/report/

[3]Cybercrime Magazine, *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) by 2021,* 2019, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Anatomy of a ransomware attack

Ransomware is typically deployed as the last act in a sophisticated infiltration of your network 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 unathorized access to one of your computers, often throught phishing, finding or guessing a remote password, or by exploiting a software vulnerability. This can occur months in advance.

Given that most breaches are caused by email phishing, brute force attacks on RDP, or security gaps, proper prevention should be a priority.

Infiltration

Malicious malware moves laterally across networks.

You can't prevent all breaches, so scan and remediate endpoints often as advised in the National Institute of Standards and Technology (NIST) Zero Trust Architecture (ZTA) guidelines.

Attack

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

Preventing 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.

To recover rapidly you will need comprehensive backups and a plan of action. Backups are a prime target for attackers. Follow the 3-2-1 rule so they're there when you need them.

Recovery

Whether the attack is successful or not, attackers may still be on your network and may have left malware. Your willingness to pay a ransom will have been noted.

After restoring critical operations, you must discover what happened, expel the attackers from your network—remove all traces of their breach—and harden your network against a repeat attack.

Should you 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.

If you are thinking of paying the ransom you should consider the following carefully:

1. **Decryption often fails.**
   Ransomware gangs' decryption tools are poor quality and often 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.[1]

2. **You are trusting criminals to keep their word.**
   Stolen data that's held for ransom is not reliably deleted or properly secured. In multiple cases it has been leaked before a ransom is even discussed, or after the ransom has been paid.[2]

3. **The cost of recovery can dwarf the ransom.**
   Even if you pay, you will need an extensive clean-up operation, and upgraded protection to prevent future attacks. Despite receiving a decryption key for free, HSE in Ireland estimates the cost of its recovery and additional protection at $600 million.[3]

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

FBI | 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.

[1]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/
[2]Coveware, *Q3 2020 Ransomware marketplace report,* 2020, https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[3]BankInfoSecurity.com, *Irish Ransomware Attack Recovery Cost Estimate: $600 Million,* 2021 https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
[4]Cybereason, *Ransomware: The true cost to business,* 2021 https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

Ransomware prevention checklist

	Breach	Infiltration	Attack	Restoration	Recovery
Create an inventory of assets including hardware, software, and data	✓	✓			
Audit your network for unknown computers and services	✓	✓			
Disable Internet-facing systems, services, and ports you don't need	✓	✓			
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 your network structure and data flows		✓			✓
Use network segmentation to subdivide your computer networks		✓			
Use least-privilege access for all systems and services	✓	✓			
Use allowlisting to ensure that only authorized software can run		✓	✓		
Restrict the use of legitimate tools commonly used by attackers[4]		✓			
Harden domain controllers according to the latest best practice[5]		✓			
Monitor your network and endpoints using IDS, EDR, and SIEM		✓	✓		✓
Make continuous, comprehensive backups following the 3-2-1 rule				✓	
Have a process for restoring computers from clean system images				✓	
Practice restoring systems from backups, so you know they work				✓	
Create an incident response plan that aligns with regulations[6]			✓	✓	
Create a critical asset list so you know what you need to restore first				✓	

Endpoint protection checklist

Endpoint security solutions are a key part of a defense-in-depth strategy because they play a part in stopping breaches and infiltration as well as ransomware attacks themselves. Endpoint protection software, or the endpoint protection capabilities included in an endpoint detection and response (EDR) solution, should offer the following components to ensure the solution defends against ransomware:

- ✓ Protection against spyware, malicious emails, and malicious websites
- ✓ Real-time detection for zero-day, file-less, and obfuscated malware
- ✓ Application hardening to prevent exploits
- ✓ Exploit mitigation and payload analysis to block remotely activated malicious code
- ✓ Payload analysis that identifies families of known and relevant malware strains
- ✓ Ransomware mitigation to detect and block ransomware execution
- ✓ A rollback feature that can restore endpoints to a known good state

Useful resources

The Cybersecurity and Infrastructure Agency (CISA) maintains a detailed Ransomware Guide **(https://www.cisa.gov/publication/ransomware-guide),** and a Ransomware Readiness Assessment tool **(https://github.com/cisagov/cset/releases/tag/v10.3.0.0).**

The National Institute of Standards and Technology (NIST) has published a comprehensive Cybersecurity Framework **(https://www.nist.gov/cyberframework)** to help organizations better manage and reduce cybersecurity risk.

CISA's Ransomware Guide **(https://www.cisa.gov/publication/ransomware-guide)** contains a very useful Ransomware Response Checklist.

---

[4]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/

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

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

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 to contain 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, your legal team, insurance providers, 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 pre-serve evidence from the attack.
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 prepared for the next one.