Microsoft Security

Protect your organization from ransomware

What is ransomware?

Ransomware is a type of cyber threat in which attackers exploit a victim's data or critical infrastructure and demand monetary ransom. In recent years, ransomware attacks have become more common and increasingly sophisticated—exploding into a full-blown underground economy. Cybercriminals are economically motivated to continue ransomware attacks, as many victims, desperate to get their data back, simply pay the ransom. What's more, the ransomware economy has given rise to more malicious actors offering tools and expertise.

Impacts include:

- Business disruption
- Reputational damage
- Financial loss
- Loss of data

Microsoft security researchers have tracked a 130.4% increase in organizations that have encountered ransomware over the last year.

The underground ransomware economy

Criminals have realized how lucrative ransomware is and have created an entire underground economy to sell their expertise as ransomware-as-a-service. Operators typically charge a monthly fee to affiliates (or customers) and have a profit-sharing model that drives up ransomware prices.

For example:

DarkSide ransomware operators take a 25% cut of the ransom for amounts below $500,000 but only take a 10% cut for ransoms above $5,000,000.

Access broker
Compromises networks to establish initial access, then sells that access.

RaaS operator
Designs and maintains ransomware tools such as malware, messaging, and payment processing.

Ransomware affiliate
Distributes and runs the ransomware payload, and purchases services from the access broker and/or operator.

The evolution of ransomware

Ransomware evolves quickly, and is constantly growing more sophisticated. Today, ransomware falls into two major categories:

	Commodity ransomware	Human-operated ransomware
Actor	Out-of-the-box malware deployed by individuals or unsophisticated cyber criminals.	Sophisticated, hands-on-keyboard attacks executed by highly-skilled cyber criminals.
Strategy	Rudimentary attacks aimed at a large volume of victims, hoping for quick and easy ROI.	Personally curated and executed attacks on carefully chosen individual targets for very high payouts.
Target	Anyone, from individuals to small businesses, but less often enterprises.	Large organizations or government agencies with the means to pay significant ransoms.
Method	Automated malware, often readily available for purchase, executed very quickly to lock endpoints and/or data.	Targeted methods used to exfiltrate sensitive information or prevent access to critical infrastructure—often executed over weeks or months.

The phases of a ransomware attack

When developing a mitigation strategy, take into account every stage of ransomware attacks.

1 Initial compromise

The attacker compromises and establishes initial access to the environment.

Common methods include: Phishing; pirated software; brute force; exploitation of vulnerabilities; credential theft.

Mitigations
- ✓ Maintain software updates and proactively address vulnerabilities
- ✓ Enforce multi-factor authentication and increase password security
- ✓ Enforce Zero Trust user and device validation
- ✓ Train employees to recognize phishing
- ✓ Utilize threat intelligence to prevent known threats and actors

2 Escalation

The attacker strengthens their foothold by escalating their privileges and moving laterally across the environment.

Common methods include: Exploiting known vulnerabilities; deploying malware; persistence.

Mitigations
- ✓ Enforce session security for administration portals
- ✓ Limit account access to sensitive data with privileged access managment
- ✓ Continuously monitor resources for abnormal activity
- ✓ Adopt best-in-classs tools to detect known threats
- ✓ Implement automation to isolate any compromised resources

Note: The pre-ransom phase above could take as long as weeks or months, and often can be difficult to detect. However, once the attacker reaches the exploitation phase, the attack could happen in a matter of hours.

3 Exfiltration

The attacker exfiltrates target data or restricts access to critical systems in preparation for ransom.

Common methods include: Local deployment of malware to endpoints; defense evasion; encryption of business critical files.

Mitigations
- ✓ Ensure regular and thorough data backups
- ✓ Move data to the cloud and take advantage of the greater versioning capabilities it offers
- ✓ Review user permissions to sensitive data
- ✓ Reduce broad read/write permissions for business-critical data
- ✓ Designate protected folders with controlled folder access

4 Ransom

The attacker makes contact, demands their ransom, and either acts upon their threats or withdraws.

Common methods include: Making contact via messaging software to make their demands—typically in cryptocurrency, making payments impossible to track and trace.

Mitigations
- ✓ Maintain a disaster backup and recovery plan and protect backups.
- ✓ Even if the ransom if paid, there is no guarantee data will be returned or unencrypted. On average, organizations that paid the ransom got back only 65% of their data, with 29% getting no more than half their data.[3]
- ✓ Ensure a holistic clean up and complete removal of persistence—otherwise, the attackers can and often will strike again

Best practices

Build a security culture
Assume breach and adopt zero trust. Build resiliency with regular training and strong processes that empower people to make the right decisions.

Prepare a recovery plan
Remediate damage and remove persistence with solutions that work holistically. Deploy data backup capabilities that let you resume operations as quickly as possible.

Stop ransomware in its tracks
Invest in ransomware prevention with comprehensive solutions that work together and with your environment to block ransomware before it harms your business.

How Microsoft disrupts ransomware

Ransomware is more than isolated incidents at specific organizations—it's an entire industry. We need to fight it on every front: in each organization, in ransomware infrastructure, in courtrooms, and in research.

Holistic prevention
Automation and machine-learning analyzes signals that look and smell like ransomware across endpoints, clouds, and resources.

Detection and response
Unified SIEM + XDR—Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel—provides integrated threat protection across devices, identities, apps, email, data and cloud workloads.

Disruption of the ransomware economy
The Digital Crimes Unit (DCU) is a team of technical, legal, and business experts that works directly with law enforcement to disrupt cybercrime.

Research and threat intelligence
Microsoft's team of security experts, is constantly studying new ransomware tactics and developing threat intelligence that is incorporated into Microsoft's security solutions.

Ready to learn more?

Microsoft 365 Defender
Secure your end-user environments, including identities, endpoints, cloud apps, and email and documents.

Learn more >>
Free trial >>

Microsoft Defender for Cloud
Protect your multi-cloud and hybrid cloud workloads including servers, storage, databases, containers, and more.

Learn more >>
Free trial >>

Microsoft Sentinel
Get intelligent security analytics across your entire enterprise, including all your security solutions, with cloud-native SIEM.

Learn more >>
Free trial >>

[1] The 2020 Microsoft Digital Defense Report
[2] The 2020 State of Security Operations, Forrester, April 2020
[3] The Forrester Wave™: Security Analytics Platform Providers, Q4 2020
[4] The Forrester New Wave™: Extended Detection and Response (XDR), Q4 2021, Allie Mellen, October 13, 2021