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:





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 For example:

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.

then sells that access.

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 RaaS operator Compromises networks Designs and maintains ransomware to establish initial access,

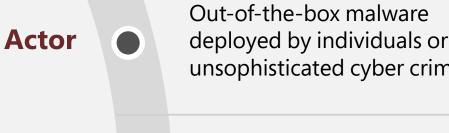
tools such as malware, messaging, and payment processing.



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. ransomware



Commodity

deployed by individuals or unsophisticated cyber criminals. Rudimentary attacks aimed

at a large volume of victims, hoping for quick and easy ROI. Anyone, from individuals to small businesses, but

Personally curated and executed attacks on carefully chosen individual targets for very high payouts.

cyber criminals.

Large organizations or government agencies with the means to pay significant ransoms.

Targeted methods used to exfiltrate

sensitive information or prevent access

Human-operated

Sophisticated, hands-on-keyboard

attacks executed by highly-skilled

ransomware

Strategy

Target

executed very quickly to lock endpoints and/or data.

Automated malware, often

readily available for purchase,

less often enterprises.



to critical infrastructure—often executed over weeks or months.

Today, ransomware falls into two major categories: **Method**

ransomware attacks.

The phases of a ransomware attack

Initial compromise

When developing a mitigration strategy, take into account every stage of



to the environment.

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

The attacker compromises and establishes initial access

✓ Maintain software updates and proactively address vulnerabilities ✓ Enforce multi-factor authentication and increase password security

Mitigations

- ✓ Train employees to recognize phishing ✓ Utilize threat intelligence to prevent known threats and actors

✓ Enforce Zero Trust user and device validation

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.

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

Escalation

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

✓ Enforce session security for administration portals ✓ Limit account acess to sensitive data with privileged access managment Mitigations ✓ Continuously monitor resources for abnormal activity

✓ Adopt best-in-classs tools to detect known threats

✓ Implement automation to isolate any compromised resources

Exfiltration The attacker exfiltrates target data or restricts access 101010 to critical systems in preparation for ransom. 010101 Common methods include: Local deployment of malware to endpoints; 101010 defense evasion; encryption of business critical files.



Mitigations

✓ Reduce broad read/write permissions for business-critical data

✓ Ensure regular and thorough data backups

✓ Review user permissions to sensitive data

capabilities it offers

or unencrypted. On average, organizations that paid the ransom got back **Mitigations**

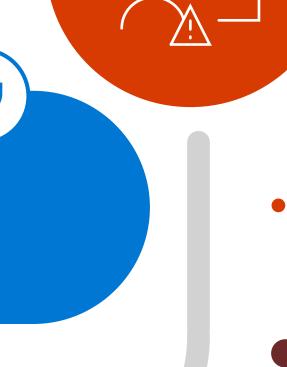
Common methods include: Making contact via messaging software to make their

demands—typically in cryptocurrency, making payments impossible to track and trace.

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

✓ Maintain a disaster backup and recovery plan and protect backups.







and strong processes that empower

people to make the right decisions.

Holistic prevention

Automation and machine learning analyzes signals

Ransom

✓ Even if the ransom if paid, there is no guarantee data will be returned

The attacker makes contact, demands their ransom,

and either acts upon their threats or withdraws.

Best practices

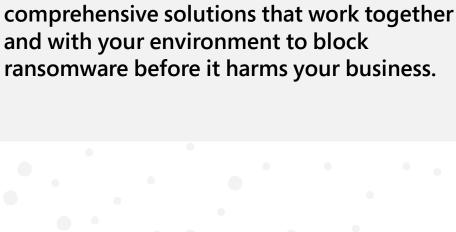
✓ Designate protected folders with controlled folder accesss

Build a security culture Prepare a recovery plan Stop ransomware in its tracks Assume breach and adopt zero trust. Invest in ransomware prevention with Remediate damage and remove persistence Build resiliency with regular training with solutions that work holistically. Deploy

data backup capabilities that let you resume

operations as quickly as possible.

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.



that look and smell like ransomware across endpoints, clouds, and resources.

How Microsoft disrupts ransomware



apps, email, data and cloud workloads.

Detection and response

Unified SIEM + XDR—Microsoft 365 Defender, Microsoft

Defender for Cloud, and Microsoft Sentinel—provides

integrated threat protection across devices, identities,

Research and threat intelligence Disruption of the ransomware economy The Digital Crimes Unit (DCU) is a team of technical, Microsoft's team of security experts, is constantly legal, and business experts that works directly with studying new ransomware tactics and developing threat intelligence that is incorporated into Microsoft's security solutions.

Ready to learn more?

environments, including

Microsoft 365 Defender

Secure your end-user

Free trial

law enforcement to disrupt cybercrime.

identities, endpoints, cloud apps, and email and documents. Learn more

>>

Microsoft Defender for Cloud Protect your multi-cloud and

hybrid cloud workloads including servers, storage, databases, containers, and more.

<u>Learn more</u>

Free trial

Microsoft Sentinel Get intelligent security analytics

across your entire enterprise,

solutions, with cloud-native SIEM.

including all your security



Sources: Microsoft Threat Analytics Report

>>