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



encountered ransomware over the last year.

Microsoft security researchers have tracked a 130.4% increase in organizations that have

For example: Criminals have realized how lucrative ransomware is and

The underground ransomware economy

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. Access broker **RaaS** operator

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.



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



tools such as malware, messaging, and payment processing.

Designs and maintains ransomware



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

Ransomware affiliate

Ransomware evolves

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



ransomware Out-of-the-box malware

Commodity

unsophisticated cyber criminals.



ransomware

of ransomware

The evolution

Method



Strategy

Target

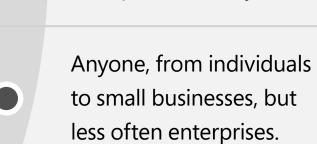
deployed by individuals or

Rudimentary attacks aimed at a large volume of victims, hoping

for quick and easy ROI.

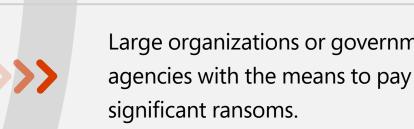


Sophisticated, hands-on-keyboard attacks executed by highly-skilled cyber criminals.



Automated malware, often

readily available for purchase,



attacks on carefully chosen individual targets for very high payouts. Large organizations or government

Personally curated and executed



executed very quickly to lock endpoints and/or data.



to critical infrastructure—often executed over weeks or months.

Targeted methods used to exfiltrate

sensitive information or prevent access

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

The phases of a ransomware attack

Initial compromise The attacker compromises and establishes initial access

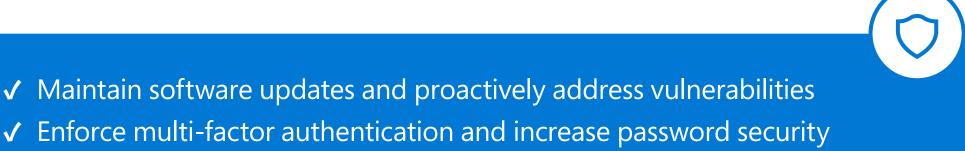


Common methods include: Phishing; pirated software; brute force; exploitation

to the environment.

of vulnerabilities; credential theft.

✓ Enforce multi-factor authentication and increase password security ✓ Enforce Zero Trust user and device validation



Mitigations

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

Escalation

Common methods include: Exploiting known vulnerabilities;

deploying malware; persistence.

✓ Enforce session security for administration portals

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

✓ Continuously monitor resources for abnormal activity

✓ Implement automation to isolate any compromised resources

The attacker strengthens their foothold by escalating their

privileges and moving laterally across the environment.



101010

01010

101010

Ransom

Mitigations

Mitigations

- - **Exfiltration** The attacker exfiltrates target data or restricts access to

✓ Limit account access to sensitive data with privileged access management

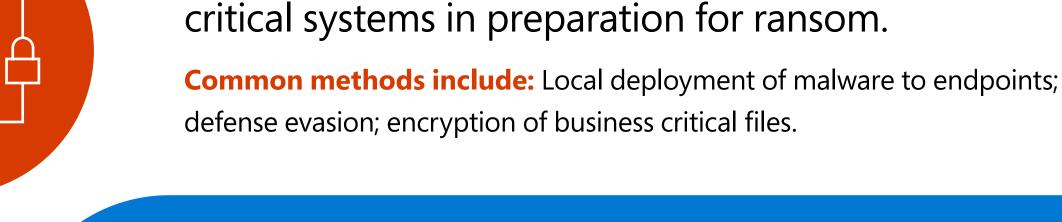
capabilities it offers Mitigations ✓ Review user permissions to sensitive data ✓ Reduce broad read/write permissions for business-critical data

Note: The pre-ransom phase above could take as long

However, once the attacker reaches the exploitation

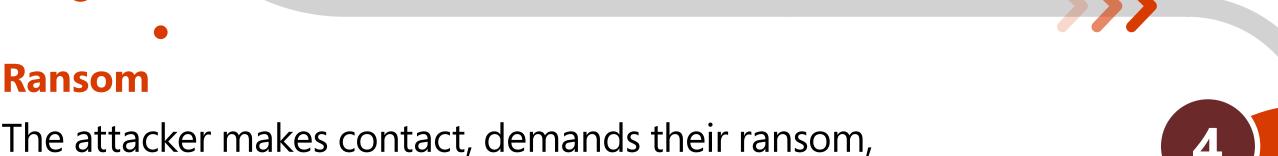
phase, the attack could happen in a matter of hours.

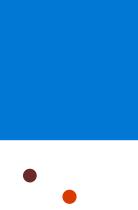
as weeks or months, and often can be difficult to detect.



✓ Ensure regular and thorough data backups ✓ Move data to the cloud and take advantage of the greater versioning

✓ Designate protected folders with controlled folder access





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

✓ Ensure a holistic clean up and complete removal of persistence otherwise, the attackers can and often will strike again

and either acts upon their threats or withdraws.

Best practices

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

only 65% of their data, with 29% getting no more than half their data.3

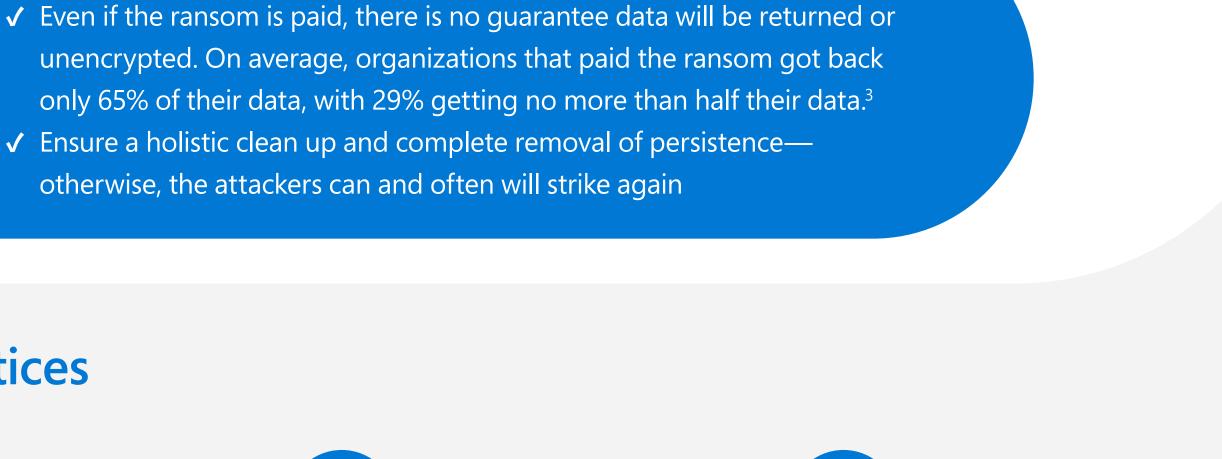
Prepare a recovery plan

operations as quickly as possible.

Remediate damage and remove persistence

with solutions that work holistically. Deploy

data backup capabilities that let you resume



Stop ransomware in its tracks

and with your environment to block

Invest in ransomware prevention with

comprehensive solutions that work together

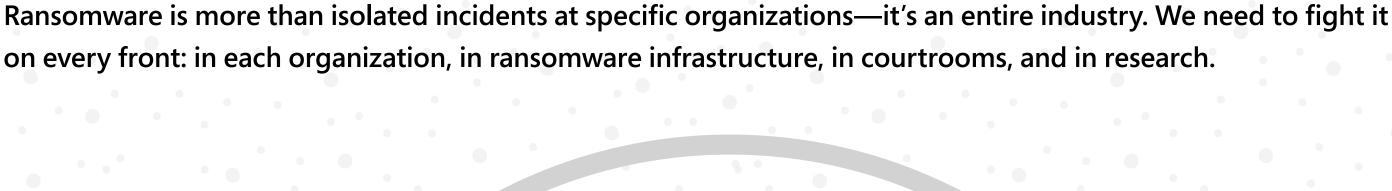
ransomware before it harms your business.

Build a security culture Assume breach and adopt zero trust. Build resiliency with regular training and

strong processes that empower people

How Microsoft disrupts ransomware

to make the right decisions.







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.



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

enforcement to disrupt cybercrime.

Holistic prevention

Automation and machine learning analyzes signals



Learn more about how to protect your organization from ransomware at <u>aka.ms/ransomware</u>.

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. © Microsoft Corporation. All rights reserved. This material is provided for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED.