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:









loss





Loss of data



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

RaaS operator

Commodity

Criminals have realized how lucrative ransomware is and For example:

Strategy

Target

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.

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.



tools such as malware, messaging, and payment processing.

Rudimentary attacks aimed

at a large volume of victims,

Anyone, from individuals

to small businesses, but

less often enterprises.

hoping for quick and easy ROI.

Designs and maintains ransomware



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

of ransomware Ransomware evolves

The evolution

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

ransomware Out-of-the-box malware

deployed by individuals or **Actor** unsophisticated cyber criminals.



ransomware Sophisticated, hands-on-keyboard

attacks executed by highly-skilled

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

significant ransoms.

cyber criminals.

Targeted methods used to exfiltrate sensitive information or prevent access

to critical infrastructure—often

agencies with the means to pay

Large organizations or government

Method

executed very quickly to lock endpoints and/or data.

Automated malware, often

readily available for purchase,

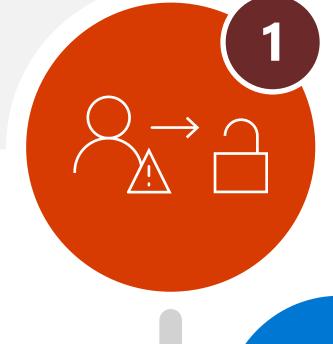


executed over weeks or months.

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

The phases of a ransomware attack

Initial compromise



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 Zero Trust user and device validation



Mitigations

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

✓ Enforce multi-factor authentication and increase password security

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

Escalation

privileges and moving laterally across the environment. Common methods include: Exploiting known vulnerabilities; deploying malware; persistence.

The attacker strengthens their foothold by escalating their

✓ 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



101010

010101

101010

✓ Implement automation to isolate any compromised resources

✓ Enforce session security for administration portals

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



capabilities it offers

to critical systems in preparation for ransom. Common methods include: Local deployment of malware to endpoints; defense evasion; encryption of business critical files.

✓ Reduce broad read/write permissions for business-critical data ✓ Designate protected folders with controlled folder accesss

✓ Ensure regular and thorough data backups

✓ Review user permissions to sensitive data

✓ Move data to the cloud and take advantage of the greater versioning

and either acts upon their threats or withdraws.

Mitigations

The attacker makes contact, demands their ransom,

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

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

✓ Maintain a disaster backup and recovery plan and protect backups. ✓ Even if the ransom if paid, there is no guarantee data will be returned

> 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

> > Prepare a recovery plan

operations as quickly as possible.

Remediate damage and remove persistence

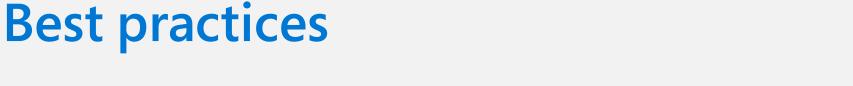
with solutions that work holistically. Deploy

data backup capabilities that let you resume

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

Mitigations

Ransom





clouds, and resources.

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.

Holistic prevention Automation and machine learning analyzes signals

Microsoft 365 Defender

Secure your end-user

Learn more

environments, including

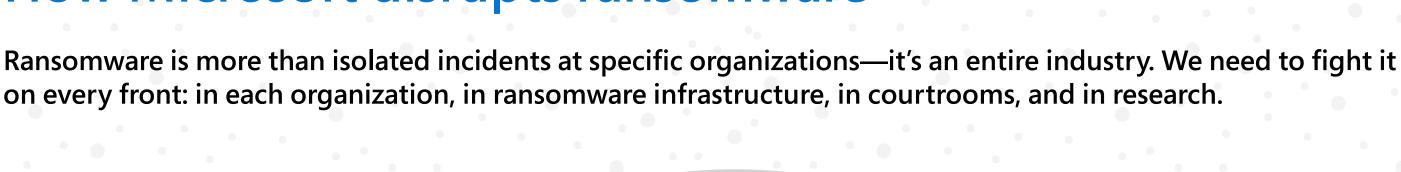
identities, endpoints, cloud

apps, and email and documents.

¹ The 2020 Microsoft Digital Defense Report



that look and smell like ransomware across endpoints,



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.

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.

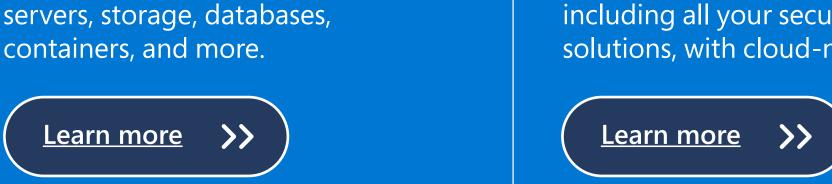
Disruption of the ransomware economy The Digital Crimes Unit (DCU) is a team of technical, legal, and business experts that works directly with law enforcement to disrupt cybercrime.

Research and threat intelligence

Microsoft's team of security experts, is constantly

Ready to learn more?

Microsoft Sentinel



Free trial Free trial >>

² The 2020 State of Security Operations, Forrester, April 2020

Learn more

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.

Microsoft Defender for Cloud

Protect your multi-cloud and

hybrid cloud workloads including

studying new ransomware tactics and developing threat intelligence that is incorporated into Microsoft's security solutions.

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

>>

Free trial