Ransomware: An ever-evolving and expanding threat

130.4% increase in organizations that have encountered ransomware over the last year

Millions of dollars spent on investigation and recovery

$40M highest public ransom paid

Business impact to organizations across industries

Ransomware risks

- Steal or Forge
- OS Credential
- Brute Force (T1110)
- Phishing for Gather Victim
- Gather Victim Host Information (T1598)
- Network Information (T1589)
- Kerberos Tickets Dumping (T1003) (T1555)
- Password Stores

Goals beyond ransom

- Prevent attackers from escalating their privileges
- Prevent an attacker from getting in
- Protect your critical data from access and destruction
- To learn more about strengthening your organization’s security against ransomware threats, and how to ease the recovery process if an attack occurs, visit: https://aka.ms/ransomware

Common tools, techniques, and procedures used by ransomware gangs

The underground economy of ransomware

Operators typically charge a monthly fee to affiliates in the ransomware economy and have set percentages and have set percentages for profit-sharing. There are often significant financial advantages to be taken at higher price levels, driving up ransom prices.

For example: DarkSide ransomware operators take a 25% cut for ransoms above $5,000,000. However, they only take a 10% cut for ransoms below $500,000.

$500,000 x 90% = $450,000

$5,000,000 x 25% = $1,250,000

$450,000 < $1,250,000

$5,500,000 - $500,000 = $5,000,000

Microsoft offers extensive guidance on how to protect your organization against ransomware with specific recommendations on how to:

- Prevent attackers from getting in
- Prevent an attacker from escalating their privileges
- Protect your critical data from access and destruction

Source: Microsoft Threat Analytics Report on Ransomware

© Microsoft Corporation. All rights reserved. This material is provided for informational purposes only.