Microsoft Security

Ransomware: An ever-evolving and expanding threat

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

»

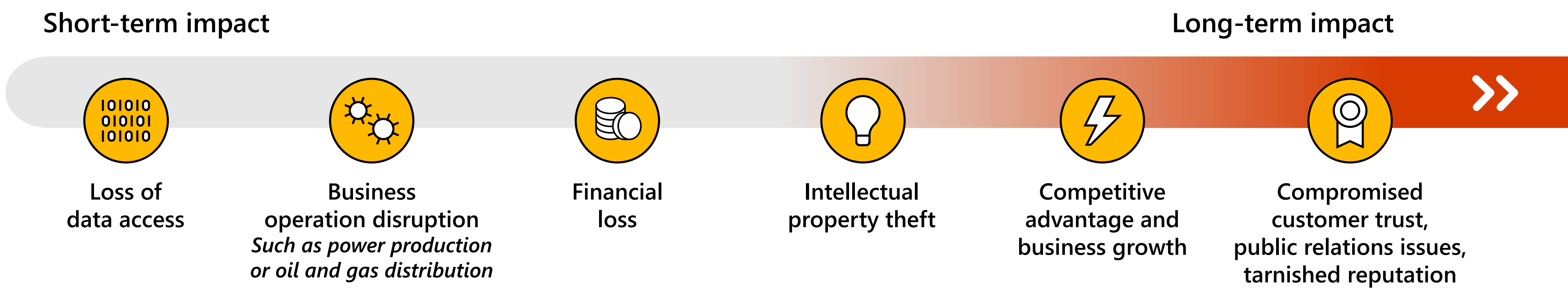
Millions of dollars
spent on investigation and recovery

»

$40M
highest public ransom paid[1]

Business impact to organizations across industries

Ransomware risks

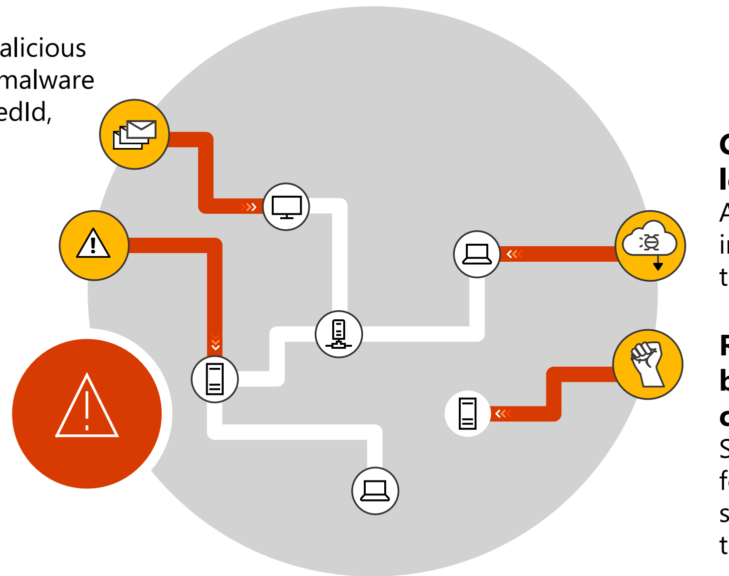


- Loss of data access
- Business operation disruption *Such as power production or oil and gas distribution*
- Financial loss
- Intellectual property theft
- Competitive advantage and business growth
- Compromised customer trust, public relations issues, tarnished reputation

Ransomware attacks have humans in the driver's seat

These "hands-on-keyboard" attacks target an organization rather than a single device and leverage human attackers' knowledge of common system and security misconfigurations to infiltrate the organization, navigate the enterprise network, and adapt to the environment and its weaknesses as they go.

Human-operated ransomware known entry points:



Email
Using phishing lures and malicious documents that download malware like Trickbot, Bazaloader, IcedId, and Qakbot

Vulnerabilities
Using exploits in known vulnerabilities, for instance, web server vulnerabilities

Cracked copies of legitimate software
A user pirates and installs software for their device

Remote access brute forcing and credential exposure
Scanning for and brute forcing devices, such as servers, that are exposed to the internet

The ransomware ecosystem

Money is to be made beyond just the ransom payments. Players in the ransomware economy profit on the various services that they offer such as:

- Access as a service
- Ransomware as a service (RaaS)
- Decryption and payment services
- Extortion services

Common tools, techniques, and procedures used by ransomware gangs[2]

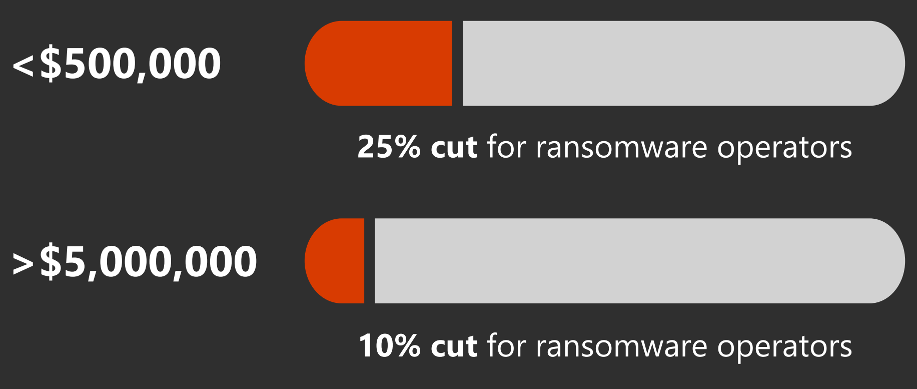
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
• Gather Victim Host Information (T1589) • Gather Victim Network Information (T1590) • Phishing for Information (T1598)	• Acquire Infrastructure (T1583) • Compromise Infrastructure (T1584) • Obtain Capabilities (T1588) • Develop Capabilities (T1587) • Stage Capabilities (T1608)	• Phishing (T1566) • Exploit Public-Facing Application (T1190) • Valid Accounts (T1078)	• Command and Scripting Interpreter (T1059) • User Execution (T1204) • Windows Management Instrumentation (T1047)	• Boot or Logon Autostart Execution (T1547) • Create or Modify System Process (T1543) • Scheduled Task/Job (T1053)	• Access Token Manipulation (T1134) • Domain Policy Modification (T1484) • Event Triggered Execution (T1546) • Process Injection (T1055)	• Deobfuscate/Decode Files or Information (T1140) • Impair Defenses (T1562) • Masquerading (T1036) • Signed Binary Proxy Execution (T1218)

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
• Brute Force (T1110) • Credentials from Password Stores (T1555) • OS Credential Dumping (T1003) • Steal or Forge Kerberos Tickets (T1558)	• Account Discovery (T1087) • Domain Trust Discovery (T1462) • Permission Groups Discovery (T1069) • Remote System Discovery (T1018)	• Exploitation of Remote Services (T1210) • Remote Services (T1021) • Software Deployment Tools (T1072) • Taint Shared Content (T1080)	• Input Capture (T1056) • Data from Local System (T1039) • Data from Information Repositories (T1212) • Archive Collected Data (T1560)	• Application Layer Protocol (T1071) • Encrypted Channel (T1573) • Ingress Toll Transfer (T1105) • Non-Standard Port (T1571) • Protocol Tunneling (T1572) • Remote Access Software (T1219)	• Exfiltration over C2 Channel (T1041) • Exfiltration over Web Service (T1567) • Transfer Data to Cloud Account (T1537)	• Data Destruction (T1485) • Data Encrypted for Impact (T1486) • Inhibit System Recovery (T1490) • Service Stop (T1489)

The underground economy of ransomware

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



Goals beyond ransom

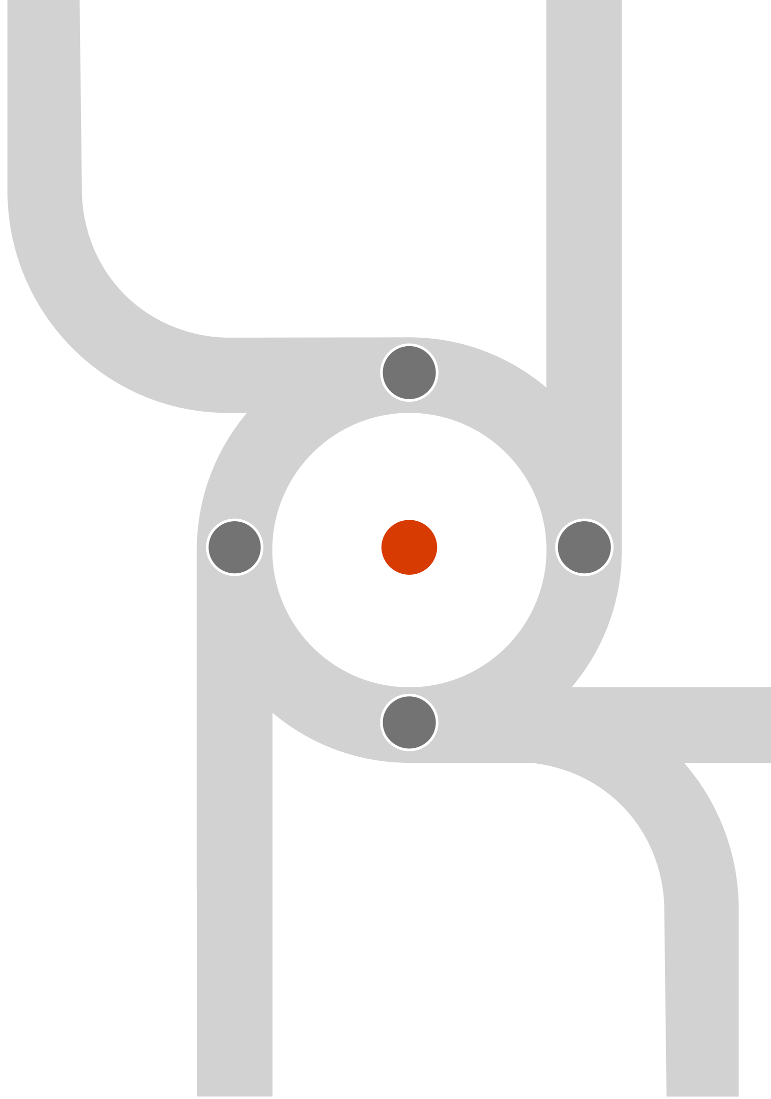
Actors often look for opportunities to **steal and extort data.** If the target hesitates to pay, the actor can threaten to cause further damage by **leaking the data.**

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

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 »



Source: Microsoft Threat Analytics Report on Ransomware

[1] Kartikay Mehrotra, William Turton. "CNA Financial Paid $40 Million in Ransom After March Cyberattack." Bloomberg, May 20, 2021.

[2] MITRE ATT&CK Matrix, https://attack.mitre.org/