HOW DOES RANSOMWARE WORK?

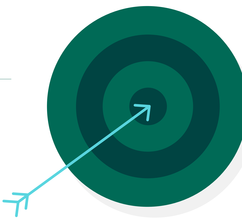
From 2021 to 2022, ransomware incidents rose by 13%. It's also estimated that, on average, a business suffered an attack every 11 seconds.[1] While these malicious actors rarely choose a single specific target — preferring instead to cast a wider net for an entry point — they usually follow a series of stages for infiltration, data gathering, and deployment.

Ever wondered how a ransomware attack progresses? Here's a general pattern:

STAGE 1:

Targets are chosen

Potential victims are identified based on their industry, infrastructure, and role in sensitive data handling. The threat actor begins to consider the best infiltration techniques.



STAGE 2:

An infection vector is chosen

Attackers select a method for infection, whether it's phishing, malicious site reroutes, or a Remote Desktop Protocol (RDP) with stolen credentials.

STAGE 3:

The virus gains entry

Someone mistakenly downloads the ransomware file or hands over their login information. Your system is now compromised.

88% of cybersecurity incidents result from human error.[2]

STAGE 4:

Infiltration spreads

Once the ransomware is in your network, it moves laterally to infiltrate as much data as it can, often lying dormant for weeks or months.

STAGE 5:

The attack launches

The threat actor triggers the ransomware assault, grabbing files and replacing them with newly encrypted substitutes you can't access.

STAGE 6:

The demand is made

By now, you'll see either a ransom note on screen or within text file directories.

Companies paid $468.8 million in ransomware demands during 2022.[3]

STAGE 7:

You deal with the fallout

Restoring backups or using a data recovery service or decryption tool is far better than paying. But returning to baseline can still take businesses out.

31% of U.S. companies end up closing down after an attack.[4]

FORTRA

Although ransomware can be devastating, you can secure your organization, as well as trace the scale of any attack in progress. By protecting your organization with Fortra's Alert Logic Managed Detection and Response (MDR), you'll have unrivaled security for any environment, comprehensive coverage to protect against known and unknown threats, and pre- and post-breach ransomware protection.

Request a demo.

alertlogic.com/request-demo

1. IBM: Cost of a Data Breach Report 2022
2. cisomag.com
3. blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/
4. atlasvpn.com/blog/31-of-us-companies-close-down-after-falling-victim-to-ransomware