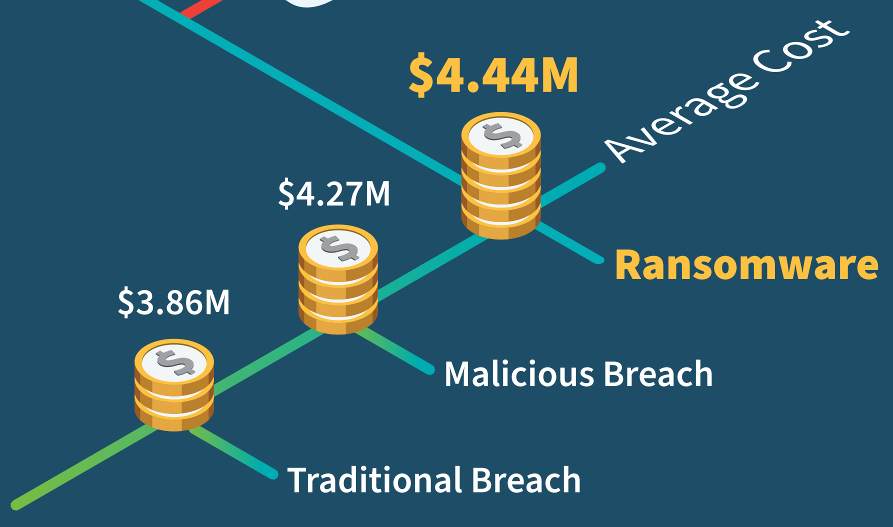
How to Boost Resilience Against Ransomware Attacks

Organizations will fall victim to a ransomware attack **every 2 seconds** by 2031, up from **every 11 seconds** in 2021.

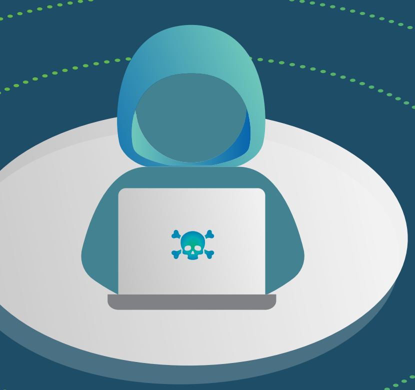
Ransomware: A Severe Threat

Threat actors are taking full advantage of today's uncertain times by launching a wave of new cyberattacks, leveraging tactics such as phishing, ransomware, and credential stuffing. Ransomware attacks alone — in which hackers take over an organization's computer systems and demand ransom payments to return them — have seen a dramatic uptick amid the new era of work from anywhere.



The Ransomware Blast Radius

Ransomware is stealing headlines. And there is a reason to all the hype. Any organization, large or small, is the target for a ransomware attack.



Albuquerque Public School District
Cancels classes due to an attack that locked district staff out of the information database they use to record student attendance, determine who is permitted to pick students up from school, and store student emergency contacts.

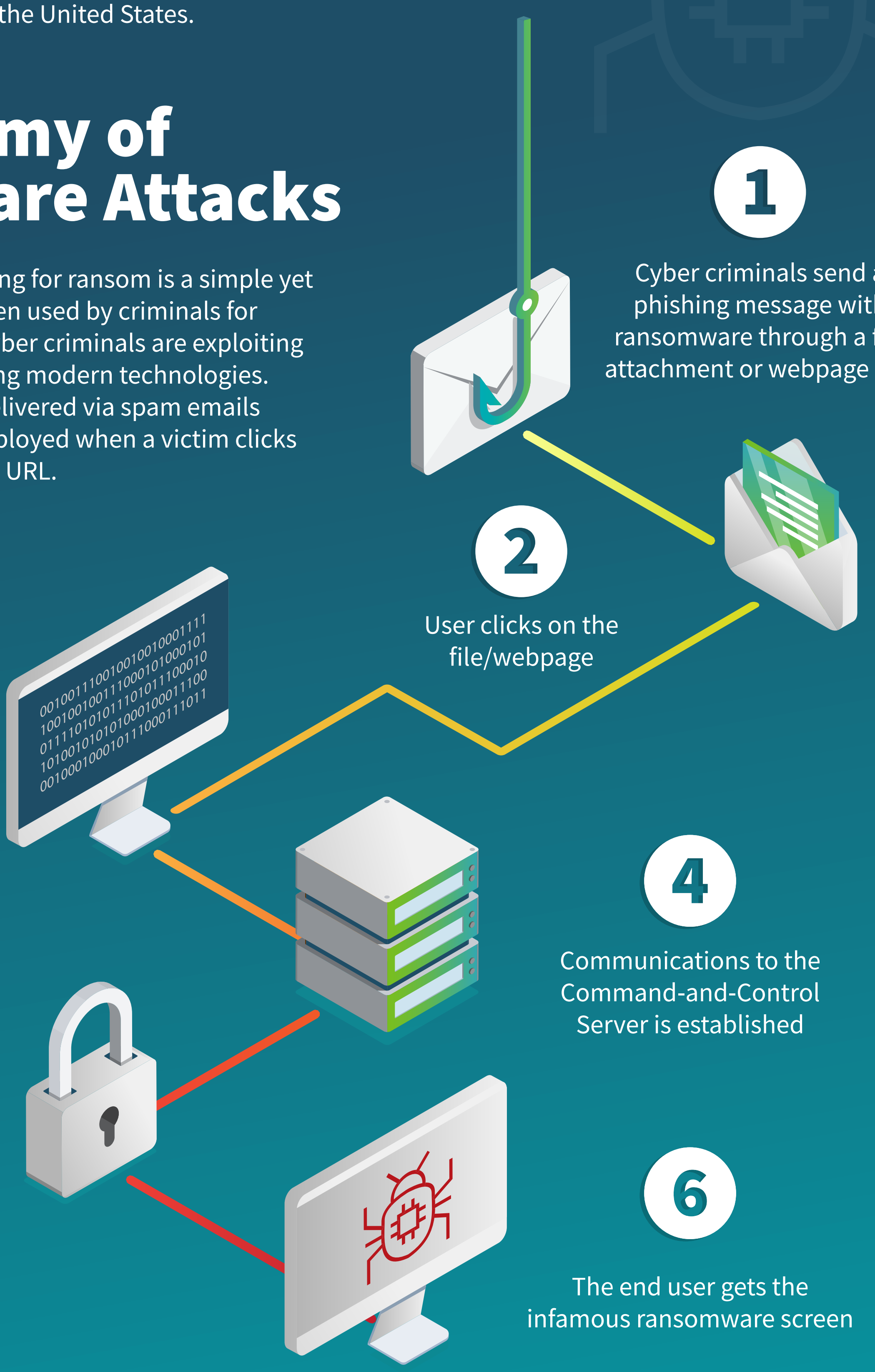
Kronos
Triggers an outage of the company's cloud service for several weeks.

JBS USA
Pays an $11 million ransom in Bitcoin to prevent further disruption.

Colonial Pipeline Attack
Disrupts gasoline and jet fuel deliveries up and down the East Coast of the United States.

The Anatomy of Ransomware Attacks

Holding someone or something for ransom is a simple yet effective strategy that has been used by criminals for thousands of years. Today, cyber criminals are exploiting these ancient techniques using modern technologies. Ransomware is commonly delivered via spam emails whereby the crimeware is deployed when a victim clicks on a malicious attachment or URL.



1 Cyber criminals send a phishing message with ransomware through a file attachment or webpage link

2 User clicks on the file/webpage

3 Ransomware is uploaded and starts executing

4 Communications to the Command-and-Control Server is established

5 The files get encrypted

6 The end user gets the infamous ransomware screen

But that's not all — recent years have seen threat actors move from just infesting systems with ransomware to multi-faceted extortion where they also publicly name (and shame) victims, steal data, then threaten to release it to the public or sell it.

3 Basic Steps to Increase your Cyber Resilience

1 **Implement cybersecurity awareness training**

2 **Regularly update anti-virus and anti-malware software**

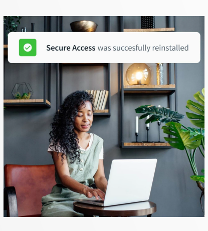
3 **Back up data to a non-connected environment and verify integrity of backups**

Absolute Ransomware Response

Ransomware attacks often put endpoints in a state where they're either open to reinfection or making it almost impossible to be re-imaged/recovered because the necessary tools are no longer functioning. Ultimately, this creates increased challenges for IT and security teams that by the time they are tasked to recover their employees' endpoints have already exhausted their resources. **Absolute Ransomware Response** enables organizations to assess their ransomware preparedness for endpoints, monitors their endpoint cyber hygiene across the entire device fleet and allows for an expedited endpoint recovery.

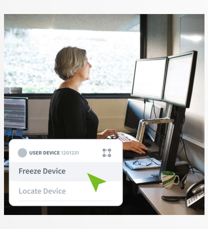
Check Strategic Ransomware Readiness

Evaluate your existing security posture across your Absolute registered endpoints and identify key security controls (e.g., anti-virus/anti-malware) as well as device management tools that are required to minimize ransomware exposure and assure expedited recovery efforts. Gain an understanding of which Absolute registered endpoints might have sensitive files so that you can ensure appropriate backup of those files, leveraging your existing tools.



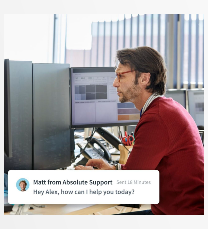
Expedite Recovery Tasks

We equip you with the capabilities to communicate with end users even when their devices are compromised, and to freeze endpoints to preserve evidence for litigation purposes while limiting further spread of infection. Ensure that endpoint security and device management tools that might have been rendered inoperable are functioning, even under distress, and execute workflow and task automation commands to expedite device recovery, leveraging a library of custom scripts.



Establish a Cyber Hygiene Baseline Across Endpoints

Jointly, we establish policies that allow for monitoring and self-healing of essential device management tools and mission-critical security controls that are needed to detect, restore, and prevent ransomware. In addition, we train your personnel on how to monitor application health and apply these baseline policies to new devices as they are enrolled.


Matt from Absolute Support
Hey Alex, how can I help you today?

Provide Remote Assistance in your Endpoint Recovery Efforts

We provide remote help in your endpoint recovery efforts for up to two incidents per year, following a pre-defined playbook and leveraging the existing Absolute product capabilities. Rely on our proven expertise to reduce the demands on your hard-pressed IT admin and security teams.

Gain an advantage for ransomware preparedness and recovery across your device fleet today

Setup a Demo

ABSOLUTE®

absolute.com

Sources: Cybersecurity Ventures, November 2020, IBM's Cost of a Data Breach Report 2020

ABT-Ransomware-Infographic-041822