WINNING THE WAR ON RANSOMWARE

A Crash Course on Solving One of Your Most Terrifying and Costly Security Threats

THE HISTORY OF RANSOMWARE

1989

One of the earliest examples of ransomware appears which infects computers through floppy disks.

2012

Reveton ransomware, bundled with a banking Trojan, displays a lock-screen message telling the victim that they engaged in illegal online activities and must pay a penalty.

2013

CryptLocker emerges as the first ransomware to encrypt files in addition to locking systems.

2015

Ransomware-as-a-service arrives. Trustwave researchers conclude purveyors can earn a 1,425% ROI in just 30 days.

2016

- A business was hit with ransomware every 40 seconds, and an individual every 10 seconds.
- NoMoreRansom project partnership launched between police and security experts
- Hackers behind the Maze and REvil/Sodinokibi strains first steal files to hold for ransom

2017

Nation-states emerge as suspects in using ransomware for disruption, e.g., North Korea suspected with WannaCry and Russian attack on Ukraine with NotPetya

2018

Critical infrastructure, municipalities, and healthcare targeted with SamSam, Ryuk, others

2019

GandCrab takes 40% of ransomware market by employing affiliate business model.

2020

- Gartner recognizes Microsoft 365 and other cloud email providers is not enough to prevent attacks.
- Cryptocurrency ransomware payments total $350 million

2021

Cybercriminals use REvil, Darkside, and Phoenix Locker to extract major ransoms: Kaseya ($70 million), JBS ($11 million), Colonial Pipeline ($2+ million), Brenntag ($4.4 million), and CNA Financial ($40 million).

2022-23

- Rackspace suffers significant outages and disruptions to its Hosted Exchange services.

School districts large and small suffer ransomware attacks:

- 2022: The 500,000-student Los Angeles Unified School District suffers an attack days before the start of the school year in September
- 2023: Public schools in the Mass. towns of Swansea and Nantucket are closed for a day in January and February due to attacks.

RANSOMWARE ATTACKS ON ORGANIZATIONS LAST YEAR

78% EMAIL-BASED RANSOMWARE

68% RANSOMWARE INFECTIONS

58% RANSOMWARE PAYMENTS

YOUR ESSENTIAL CHECKLIST FOR RESISTANCE, RESCUE AND RECOVERY

BEFORE

- ☑ **TURN SECURITY AWARENESS INTO REPEATABLE PROCESSES:** Users who receive training more than once a year are less likely to fall for tricks like suspicious links and attachments that can lead to ransomware.
- ☑ **TEST EVERYTHING:** Sniff out vulnerabilities and weak spots across your IT environment that need addressing before attackers use them to deliver ransomware.
- ☑ **DO THE BASICS:** Keep your systems, plug-ins and extensions up to date – and follow the principle of least privilege for your users.
- ☑ **IMPLEMENT TECHNOLOGY SAFEGUARDS:** Help stop infections in real time with anti-malware, email protection, application whitelisting and endpoint detection and response solutions.
- ☑ **BACK UP YOUR SYSTEMS:** Backups of your sensitive information can be your most valuable defense against ransomware. Double-check their integrity and keep them in an offline, secure location.

DURING & AFTER

- ☑ **GET OFFLINE:** If you're infected by ransomware, disconnect the affected systems from the internet.
- ☑ **PRACTICE R&R:** Ensure you both reimage your machines and restore your data.
- ☑ **ASSESS YOUR LEGAL OBLIGATIONS:** You may be required to report a ransomware attack to your customers like you would a data breach.
- ☑ **TRY TO AVOID PAYING:** Remember, even if you pony up the ransom demand, there is no guarantee the attackers will release the decryption keys.
- ☑ **PERFORM FORENSICS:** Discover how the attack unfolded so measures can be taken to block the same type of attack in the future.
- ☑ **IMPLEMENT A MULTI-LAYERED STRATEGY:** Ensure email is secured across multiple touchpoints, ideally with machine-learning algorithms that can anticipate attacks

Trustwave®

www.trustwave.com

Sources:
https://www.gartner.com/en/documents/3992321
https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware
https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks
https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report
https://www.zdnet.com/article/2300-local-governments-schools-healthcare-providers-impacted-by-ransomware-in-2021
https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts
https://www.zdnet.com/article/ransomware-in-2022-were-all-screwed/
https://www.techtarget.com/searchsecurity/news/252511430/10-of-the-biggest-ransomware-attacks
https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help
https://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive
https://grahamcluley.com/cryptoworms-future-ransomware
https://www.trustwave.com/en-us/resources/library/documents/best-practices-for-dealing-with-phishing-and-ransomware
https://venturebeat.com/2022/02/22/22-very-bad-stats-on-the-growth-of-phishing-ransomware