RANSOMWARE PREVENTION IS POSSIBLE

prevent-first strategy. With the most expensive and feared malware threats-double, triple, quadruple extortion strategies-occurring, shielding your organization from ransomware requires a proper defense posture, reduced exposure, and stopping threat actors at the start.

Effective ransomware protection starts with a Zero Trust mindset and a

RANSOMWARE IS A SERIOUS THREAT TO ORGANIZATIONS AND PROVED TO BE A GROWING MENACE IN 2021:

THE IMPACT OF RANSOMWARE

MILLION WAS THE AVERAGE COST OF A RANSOMWARE BREACH IN 20211

DAYS **WAS THE AVERAGE DOWNTIME FOR**

ORGANIZATIONS²

OUT OF 16 CRITICAL *INFRASTRUCTURE*

SECTORS WERE **TARGETED** IN 2021³

32% OF THE TIME C-LEVEL

EMPLOYEES LEFT AFTER A SUCCESSFUL **RANSOMWARE** ATTACK⁴

80% **OF ORGANIZATIONS** WERE HIT BY A SECOND, REPEAT ATTACK⁵

First known

RANSOMWARE EVOLUTION TIMELINE

1989

Traditional ransomware attack: encrypt data → extort for money → decryption key provided if ransom paid

ransomware attack

· NotPetya caused about \$10 billion in damages worldwide⁷

caused global security crisis

WannaCry and Not-Petya

WannaCry attack included 150 countries⁶

triple-extortion attack

was mainly fueled by triple extortion⁹

First known

double-extortion attack

935% increase in the number of

companies that have had their data

2017

First known

Ransomware's 93% surge

2019

exposed on a data leak site during the study period⁸

2020

2021

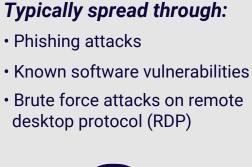
First known quadrupleextortion attack • These types of attacks are not

as frequent The average payment surged 171%, to more than \$312K¹⁰

TRENDING RANSOMWARE

According to BlackBerry® threat research, the top ransomware

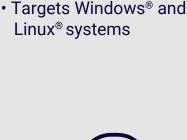
threats faced by organizations over the past year are:



REVIL

- **AVADDON** First appeared in 2020

Uses double and triple extortion



DARKSIDE

Uses double-extortion tactics

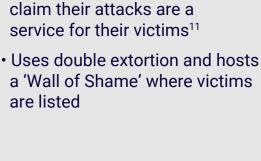


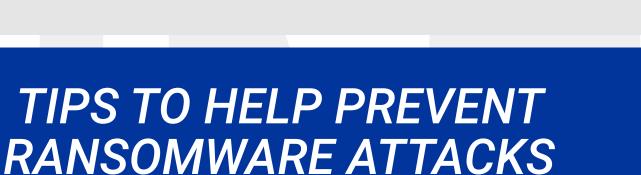
CONTI

Targets organizations in

- RAGNAR LOCKER
- Operated by threat actors who
- HIVE Notable for using the relatively new Go programming language

Employs double extortion





Exploiting known vulnerabilities is a key component of many ransomware campaigns. Keeping devices updated deprives threat actors of a major

advantage.

Adopt strong password

policies and multi-factor

authentication (MFA)

Keep software updated

Track and manage Implement a system to track vulnerabilities across environments, devices, and services because most enterprise environments are constantly changing.

Reduce the attack surface

Compromised and shared credentials are a massive vulnerability.

Protect data

and backup policies.

Create strong data recovery

(including testing of data backups)

Follow the principle of least privilege

access. Remove unnecessary devices

and software from the environment.

Where possible, reduce network

connections and access.12

Follow good

security practices

Train employees, use MFA,

and implement strong passwords.

BE RANSOMWARE PREPARED.

next level should consider managed extended detection and response (XDR) platforms and artificial intelligence (AI). The Cylance® Endpoint Security offers organizations Al-empowered protection and a Zero Trust framework that can protect any device, anywhere, from ransomware. For more information on preventing and remediating ransomware,

see our helpful guide →

Organizations looking for solutions that take ransomware protection to the

About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 215M vehicles. Based in Waterloo, Ontario, the company leverages Al and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management,

encryption, and embedded systems. BlackBerry's vision is clear--to secure a connected future you can trust.

*** BlackBerry Cybersecurity

For more information, visit **BlackBerry.com** and follow **@BlackBerry**. ©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks

are the property of their respective owners. This document may not be modified, reproduced, transmitted, or copied, in part or in whole, without the express written permission of BlackBerry Limited.

2 https://www.forbes.com/sites/hillennevins/2021/07/26/how-to-survive-a-cybersecurity-attack/ $3\ https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-secto\underline{rs-2021}$ 4 https://www.techrepublic.com/article/the-many-ways-a-ransomware-attack-can-hurt-your-organization 5 https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/ 6 https://dataprot.net/statistics/ransomware-statistics/

1 https://www.itpro.com/security/ransomware/359364/cost-of-ransomware-doubles-in-a-year

7 https://dataprot.net/statistics/ransomware-statistics/ 8 https://www.rhisac.org/ransomware/ransomware-double-and-triple-extortion/

9 https://cybernews.com/news/ransomware-surged-93-in-last-6-months-fueled-by-triple-extortion/ 10 https://threatpost.com/ransomware-payments-quadruple-extortion/168622/ 11 https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-what-you-need-to-know/ 12 https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege

05082022