

# Ransomware Threats are Real

Take control with Veritas Backup Exec™

This year, we've seen a rise in attacks on businesses, government organizations, and public services—large and small, across the globe. They've caused gas shortages, disrupted healthcare systems, closed grocery stores, shut down schools, and halted manufacturing.



of companies experienced a cyberattack



of attack victims reported losing customer data



65%

of organizations reported revenue loss



53%

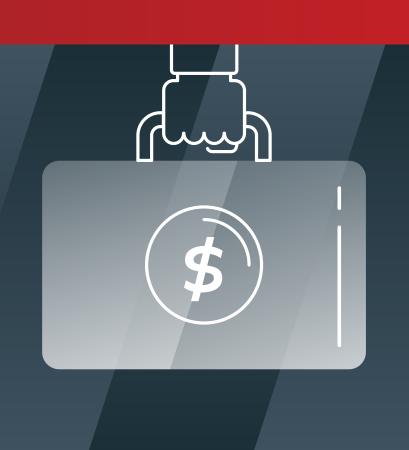
of organizations experienced brand & reputation damage



25%

of organizations had to shut their business down

# The Hackers Are Motivated



Victims typically paid up to \$50,000 in remediation costs, whether or not they paid the ransom.

The average ransom demand jumped 43% in 2021, with the median payment jumping 58% to

\$78,398

#### **Criminal Collective**

### **REvil**

Averaged US\$2.5 million in payouts per breach

## Conti

Often demands million-dollar payouts

# Maze

Made average ransom demands of US\$420,000

# **DarkSide**

Receives millions in ransoms

Estimated to have stolen upwards of a billion dollars

# Responsible For...

- JBS (US\$11 million)
- Kaseya that affected thousands of small businesses and locked down tens of thousands of systems (demanded US\$70 million for a universal decryption key)
- ExaGrid attack (US\$2.6 million)
- Attack on Irish health system
- Attacks on 400+ organizations worldwide, including 290 U.S. companies
- Attack on City of Pensacola, FL Attack on Southwire
- Attack on Colonial Pipeline (US\$4.4 million)

# Lazarus Group

- Cyber-heists of banks (for example, US\$81 million from the Central Bank)
- of Bangladesh)
- WannaCry that affected more than 200,000 computers across 150 countries

# Take Control of Your Data

Taking a proactive approach to prevention through layered security solutions is smart, but only one thing can guarantee protection if attackers get in—having a reliable backup system. With Veritas Backup Exec, all your critical data (virtual, physical, and cloud workloads) can be backed up, locked down against ransomware, and recovered quickly and easily.



#### Air Gap **Backups**

Create an offline backup copy of your data to keep it out of reach.



#### Multiple Copies

Store copies of backup images in different locations to reduce the attacker's ability to gain access.



#### **Restrict Backup Credentials**

To minimize phishing, limit and continually monitor backup credentials.



#### **Shrink Your RPO**

Running backups more often to shrink your RPO can reduce potential data loss to hours or even minutes.



#### Secure Your **Backup Copies**

Secure your disk-based backups from encryption, deletion, or modification from outside sources.

# Get resilient against ransomware with Veritas Backup Exec



https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html https://searchsecurity.techtarget.com/feature/The-biggest-ransomware-attacks-this-year https://threatpost.com/ransomware-victims-dont-pay-up/166989/ https://www.theregister.com/2021/07/07/revil\_tactics\_and\_multimillion\_dollar/ https://www.theguardian.com/business/2021/jun/10/worlds-biggest-meat-producer-jbs-pays-11m-cybercrime-ransom

https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline

https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers https://www.bbc.com/news/world-europe-57197688

https://www.forbes.com/sites/daveywinder/2021/07/05/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit/?sh=6b71897257c0

https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/ https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response// https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk and the sum of the shttps://www.technologyreview.com/2020/01/24/276082/lazarus-group-dragonex-chainalysis https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/, https://en.wikipedia.org/wiki/WannaCry\_ransomware\_attack

https://www.zdnet.com/article/fbi-identifies-16-conti-ransomware-attacks-striking-us-healthcare-first-responders/https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/

https://www.csoonline.com/article/3276584/what-does-a-ransomware-attack-cost-beware-the-hidden-expenses.html





Contact your Connection Account Team for more information. **Enterprise Solutions Business Solutions Public Sector Solutions** 

1.800.800.0014

1.800.369.1047 www.connection.com/Veritas

1.800.800.0019