2019 RANSOMWARE by the Numbers

What you don't know might hurt you

Most Notorious Ransomware

2013 CryptoLocker

2014 CryptoWall

2015 TeslaCrypt

2016 Locky

2017 WannaCry/ Petya

2018 SamSam

2019 LockerGoga

Petya – the first ransomware-as-a-service

Top Ransomware
Infiltration Tactics

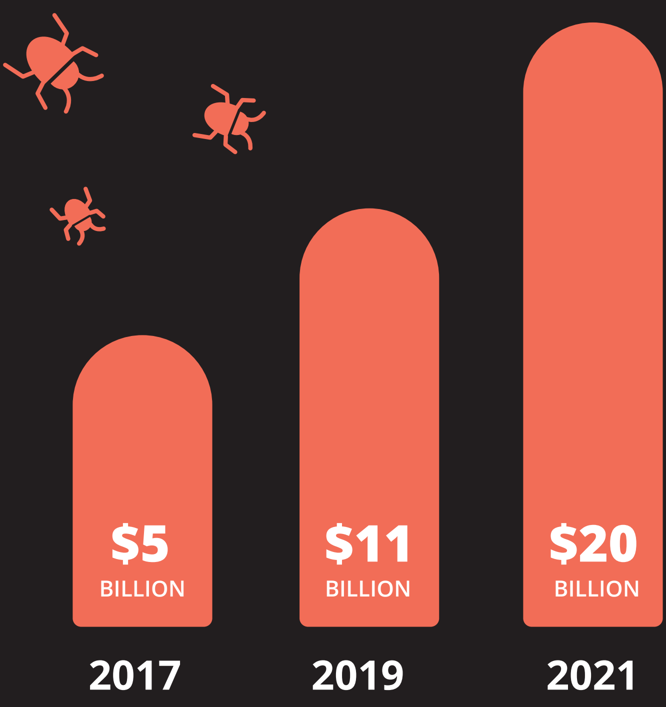
- Phishing emails, attachments & links
- Malicious or unsecure websites
- Online ads
- Free downloads and other clickbait
- Unencrypted communications

10 MOST
Targeted Industries

- Healthcare
- Manufacturing
- Financial services
- Professional services
- Educational
- Government
- Hospitality
- Retail
- Transportation

5X Predicted growth of ransomware attacks on hospitals by 2021

Global Ransomware
Damage Predictions



69 DAYS

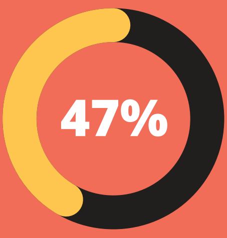
Average time to contain a data breach once identified

COST
OF RANSOMWARE

$300 MILLION	FedEx earnings loss due to the NotPetya ransomware attack
$5 MILLION	Amount City of Atlanta, Georgia, spent rebuilding its computer network
$50 THOUSAND	The amount businesses willing to pay to decrypt their data

of consumers said they won't do business with companies they don't trust to protect their data.

of cyberattacks committed against small businesses - and the percentage is expected to continue rising.



percent of firms that get their data back after paying a ransom

BEST PRACTICES
for Avoiding Ransomware

- Ensure your network and all your software is up-to-date
- Deploy threat detection tools such as anti-virus or endpoint security software.
- Backup and encrypt your data, such as with an external cloud backup provider.
- Be vigilant and educate/train your staff about how ransomware spreads to help mitigate user error as the point of entry.

MSPs Can Be Liable for a Client's Ransomware Attack!

If a company's IT services are out sourced to a third-party partner such as an MSP, the managed solution provider can be liable for any data breach or loss cause by attacks such as ransomware unless they can prove that they made commercially reasonable measures to prevent the data breach/loss.

Secure Ransomware Protection from Dropsuite

Get fully recoverable copies of your business data to guard against ransomware.

The ONLY way to guarantee data from ransomware attacks is with an automated, ongoing, cloud-based backup solution that maintains complete copies of your **Microsoft Office 365** files such as: Exchange Online (email, attachments, contacts, calendars and tasks) -- plus your SharePoint, OneDrive, Groups and Teams.

Dropsuite also offers cloud backup solutions for:

- G Suite Gmail
- Websites and databases
- IMAP/POP email
- Hosted Exchange
- Open-Xchange

Contact Dropsuite for an email backup and archiving product demo and free trial.

dropsuite.com
sales@dropsuite.com

Sources:

"A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time," Digital Guardian
"Atlanta was not prepared to respond to a ransomware attack," StateScoop
"Beazley 2018 Breach Briefing," Beazley
"Cyber attack, hurricane weigh on FedEx quarterly profit," Reuters
"Cybercrime Damages $6 Trillion By 2021," Cybersecurity Ventures
"IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses," IBM Security and Ponemon Institute
"Internet Security Threat Report, Government, Vol. 22," Symantec
Interview with attorney, Kathy Winger; Dropsuite "Declination of Backup Coverage" addendum
"MSSPs, Be Warned: You Can Be Liable for a Client's Data Breach," Channel Futures
"New Survey Finds Deep Consumer Anxiety over Data Privacy and Security," Cision PR Newswire
"Ransomware: What Businesses Need to Know," Dropsuite

Dropsuite

© 2019 Dropsuite Limited. All Rights Reserved.
2019.05.06.V1