



# RANSOMWARE

## EXPLAINED

### RANSOMWARE EXPLAINED HOW IT WORKS — PLUS TIPS FOR PREVENTION & RECOVERY

Ransomware attacks — a type of malware (a.k.a. malicious software) — are proliferating around the globe at a blistering pace. In Q1 2017, a new specimen emerged every 4.2 seconds!\* What makes ransomware a go-to mechanism for cyber attackers? The answer is in the name itself.

## HOW IT WORKS

Unlike other hacks, the point of ransomware isn't to steal or destroy valuable data; it's to hold it hostage.

YOU WIN !!!  
100 500 millions!!!  
OK

Ransomware enters computer systems via email attachments, pop-up ads, outdated business applications and even corrupted USB sticks.



From: Jane Thompson, CEO  
To: All Employees  
Subject: Important — Please Open Attachment: weird\_zip\_file.ZIP

Hello valued business associates,  
Attached and in the link below is a very important business update. Everyone oopen this now.

<http://www.supersuspiciouslink.org/please-click-here>

-Jane, The Boss

**Beware imposter emails!**  
Would your CEO really send a message like this?

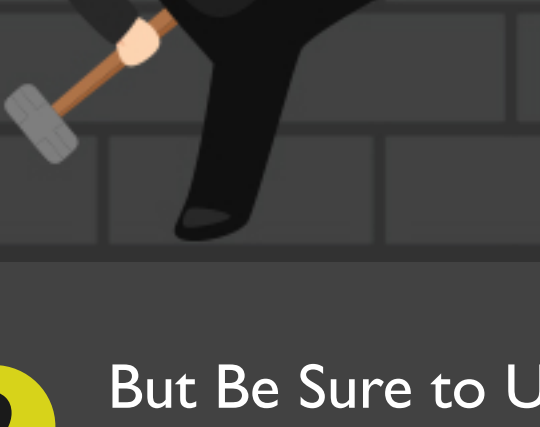
Even if one computer is initially infected, ransomware can easily spread network-wide via a LAN or by gaining access to username and passwords.

Once the malware activates, the hostage situation begins: Data is encrypted and the user is instructed to pay a ransom to regain control.



## RANSOMWARE PREVENTION

**1** Install Anti-Virus/  
Anti-Malware Software



**2** But Be Sure to Update & Patch Software/Operating Systems

**3** Invest In Enterprise Threat Detection Systems and Mail Server Filtering

**4** Educate Employees on Network Security



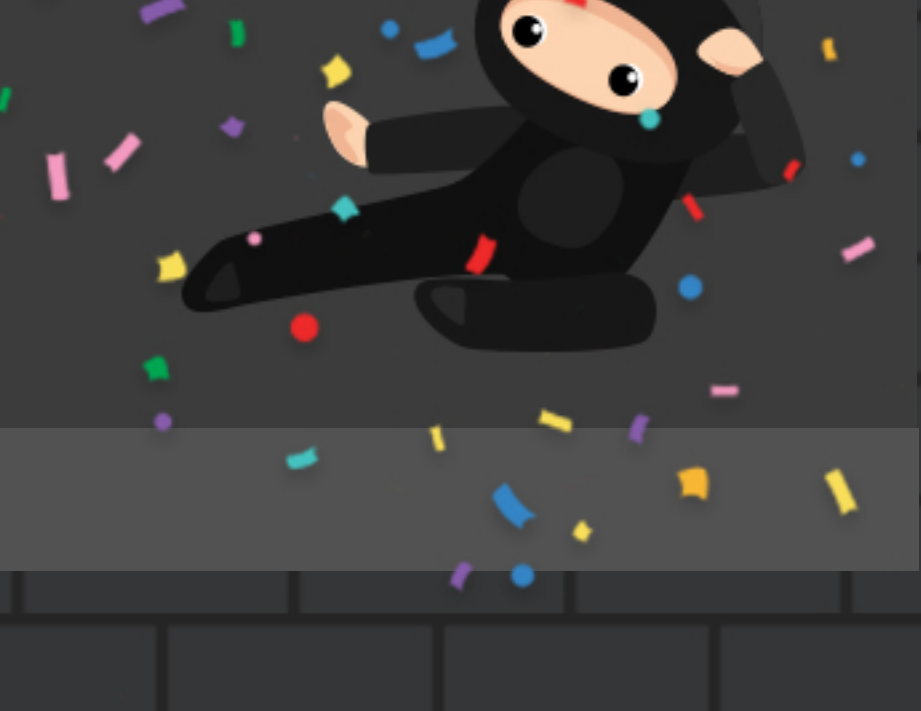
## WHAT TO DO IF YOUR DATA IS HELD HOSTAGE?

Remember: Preventative measures are never 100% effective.

**IF ATTACKED, SHOULD YOUR COMPANY PAY?**

**NO!**  
Paying the ransom might get you off the hook quickly, but will make you a repeat target for attack.

Pay Ransom:



Don't Pay Ransom:



## THERE'S A BETTER WAY

Beat the attackers to the punch by investing in Cloud Backups and Disaster Recovery as a Service.

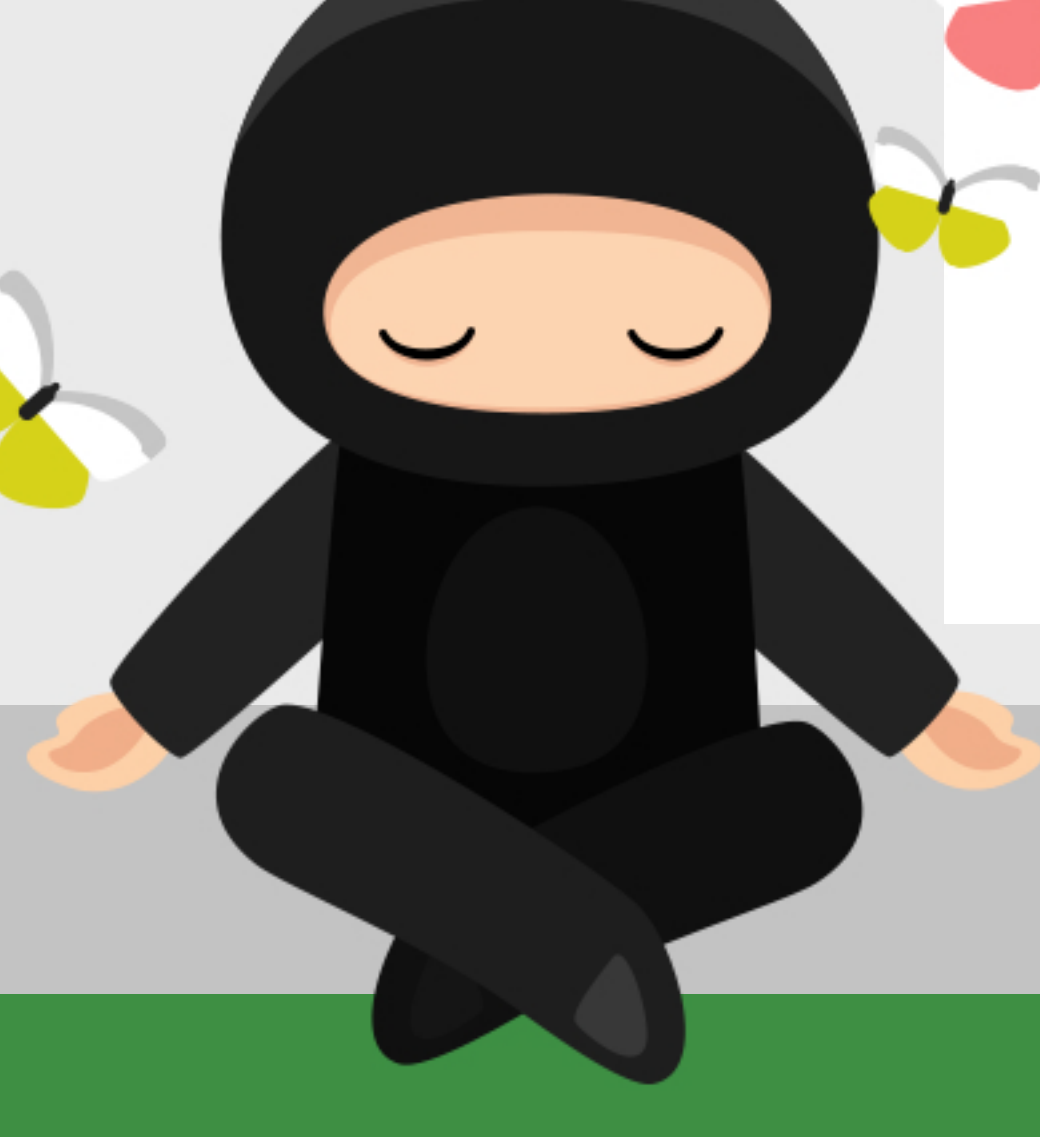
### BACKUPS

Daily Offsite Backups = You'll Always Have Clean, Recent Copies of Your Data



### DISASTER RECOVERY

Disaster Recovery Solutions are crucial in the event Ransomware compromises your entire system. Here, you'll be able to operate your business as usual via a redundant network and infrastructure. Sorry, Malware Ninjas.



LEARN MORE ABOUT SECURITY AND BUSINESS CONTINUITY SOLUTIONS AT:

[WWW.SINGLEHOP.COM](http://WWW.SINGLEHOP.COM)

\*Source: "Malware Trends 2017." G Data Security Blog. <https://www.gdatasoftware.com/blog>

**SINGLEHOP**