EMAIL
THE WEAKEST LINK

THERE ARE APPROXIMATELY
269 BILLION
EMAILS SENT EVERY DAY¹

91% OF ALL CYBER CRIMES BEGIN WITH AN EMAIL²

ATTACKER MOTIVATIONS
FOR SPEAR PHISHING AND RANSOMWARE

BUSINESS DISRUPTION

FINANCIAL

REPUTATIONAL DAMAGE

RANSOMWARE INFECTION VIA EMAIL

RECON → SOCIAL ENGINEERING → SPEAR PHISHING

INFECTION → CONTACT CNC → MISSION ACCOMPLISHED

MISSION ACCOMPLISHED

The attacker targets a healthcare administrator — learning about him through social media.

An email is crafted to appear like it's from the healthcare administrator's manager, recommending a critical software update.

The healthcare administrator, assuming the email is real, clicks on a link embedded in the email to install the software update.

Ransomware is downloaded from the attacker's server and infects the healthcare administrator's machine.

Activated malicious code triggers a callback to a command-and-control server.

The healthcare administrator's data is encrypted and a ransom is demanded.

FireEye Email Security:
Better Protection against Email-Borne Attacks

Industry-leading detection of, and protection from, targeted threats such as ransomware to safeguard business assets

Real-time, automated protection from spear-phishing and other socially engineered attacks to minimize impostor calls-to-action

Flexible deployment models to support on-premises, cloud and hybrid email environments

Always up-to-date protection; no upgrades needed

Comprehensive, contextual threat intelligence to provide your security team the information it needs to respond to threats

Protection from hard-to-detect multi-stage, multi-flow attacks

Learn More at www.FireEye.com/email

PROTECT YOUR PEOPLE, DATA AND ASSETS WITH FIREEYE EMAIL SECURITY

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.