THE RISING THREAT OF RANSOMWARE

Ransomware Q&A

What Is Ransomware?

Ransomware is a type of malicious software — i.e., malware — that blocks access to a device or data until a ransom is paid.

What Does Ransomware Do?

When a device is infected with ransomware, some type of encryption is applied, effectively locking you out of your files or your device. If you are infected, you will receive a ransom message from the attacker asking for payment which, allegedly, will grant you access to the digital key needed to unlock your files and/or system.

How Much Are Ransoms?

Some ransom demands are relatively low, in the range of a few hundred dollars. However, cybercriminals are getting more aggressive. Attacks that target healthcare institutions and larger organizations can carry very high ransom demands. For example, a South Korean web hosting firm admitted to paying a $1M ransom to its attackers in June 2017.

How Are Ransoms Collected?

Attackers generally require ransoms to be paid in Bitcoin or another "untraceable" electronic format. These "cryptocurrencies" are fully digital. They are created and held electronically, have no physical form, and are not controlled by any banking entity.

Ransomware by the Numbers

80+%

The portion of malicious email messages that contained ransomware or banking Trojans in 2017

Source:
Proofpoint's 2018 Human Factor report

350%

The global increase in ransomware volume during 2017

Source:
NTT Security 2018 Global Threat Intelligence Report

$11.5 BILLION » The estimated total of global ransomware damages by 2019

Source:
Cybersecurity Ventures

FACT: There are several well-known ransomware variants (including WannaCry, Locky, and Cerber). Many ransomware variants are continuously modified to bypass antivirus software, demand different ransom amounts, take advantage of different infrastructure vulnerabilities, etc.

184 MILLION

The number of ransomware attacks globally in 2017

$544

The average ransom demand by attackers worldwide in H1 2017

Source:
Statista

327 The number ransomware families newly identified in 2017 (up from 29 in 2015)

HEALTHCARE ORGANIZATIONS THE RATE OF RANSOMWARE ATTACKS ON HEALTHCARE ORGANIZATIONS IS EXPECTED TO QUADRUPLE BY 2020.

Source:
2017 Healthcare Cybersecurity Report, Cybersecurity Ventures

Ransomware Prevention and Protection

To Pay or Not to Pay?

Security experts generally advise against paying a ransom. Paying only encourages these types of attacks.

However, if an organization has not backed up files to a secure location, paying the ransom might be regarded as the only option for recovering data. Though some services claim they can recover files without the decryption key, it can be next to impossible to reverse an infection.

Will Paying a Ransom Restore My Files?

Sometimes. But there have been known instances in which the attackers never delivered the decryption key following payment, as well as ransomware with critical programming flaws that rendered data unrecoverable, even with the key. In other cases, an organization has paid the ransom only to be hit with a second, larger payment request.

Bottom Line: DON'T COUNT ON 'HONOR AMONG THIEVES.' »

DON'T BECOME A RANSOMWARE VICTIM!

Know how to prevent an infection and be prepared to recover your data if you do get hit.

AVOID unknown links, ads, and websites

DON'T download unverified attachments or apps

KEEP software up to date and patch known vulnerabilities

BACK UP data and files to a secure location daily or even hourly (if possible)

We deliver security awareness and training about a range of cybersecurity threats, including ransomware. Our assessment and education tools change behaviors and reduce risk in the workplace and beyond.

wombat™ security
a division of proofpoint.

40 24th St, Pittsburgh, PA 15222
www.wombatsecurity.com
+1 (412) 621 1484 | +44 (20) 3807 3472