The Rise of RANSOMWARE

WHAT IS RANSOMWARE?

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto- ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

IN 2016

RANSOMWARE INCREASED BY A STAGGERING 500%, WITH EMAIL PHISHING AS THE MOST-USED DISTRIBUTION METHOD.

RANSOMWARE ALSO INFECTED

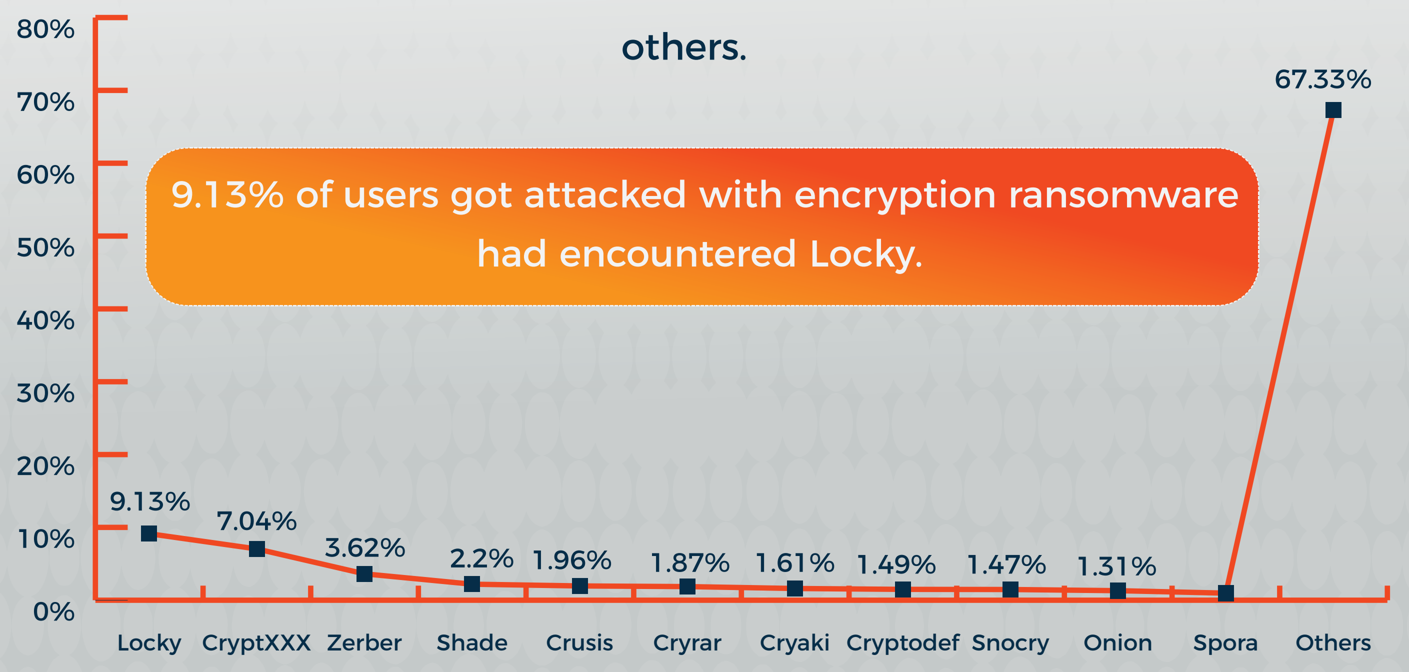
30,000-35,000

DEVICES ON AVERAGE.

THE PROFITS GENERATED THROUGH RANSOMWARE ARE EXPECTED TO HIT $1 BILLION IN 2017.

During the first 6 months of 2016, 300 new ransomware variants were developed.

In 2017, many users got attacked with some ransomware variants such as Locky, CryptXXX, Zerber, Shade, Crusis, Cryrar, Cryaki, Cryptodef, Snocry, Onion, Spora and others.



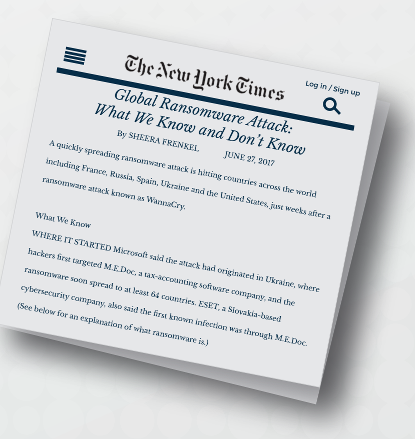
9.13% of users got attacked with encryption ransomware had encountered Locky.

DISTRIBUTION OF USERS ATTACKED WITH RANSOMWARE VARIANTS IN 2017

HOW CAN ORGANIZATIONS PREVENT RANSOMWARE ATTACKS ?

1. Predict and be informed before the attack occurs:

Proactively research what's discussed on the dark web, new exploits that will be used, and industries or companies that will be targeted.



The New York Times

Log in / Sign up

Global Ransomware Attack: What We Know and Don't Know

By SHEERA FRENKEL JUNE 27, 2017

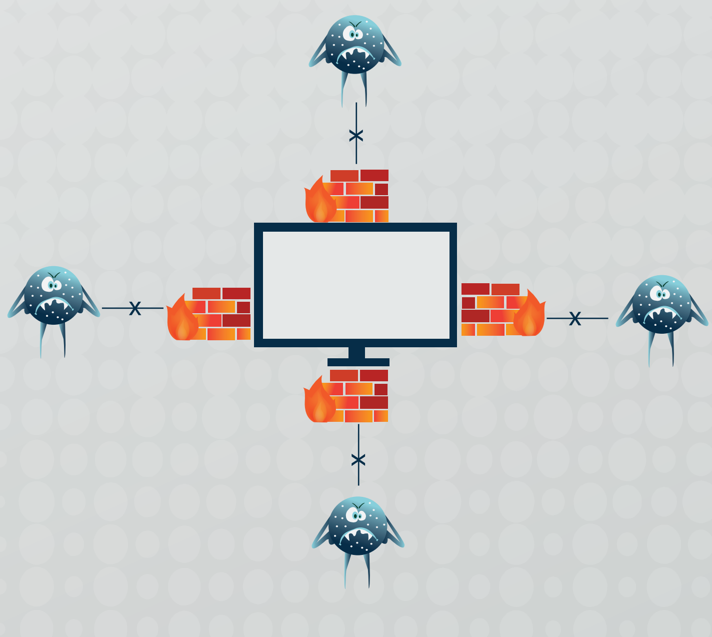
A quickly spreading ransomware attack is hitting countries across the world including France, Russia, Spain, Ukraine and the United States, just weeks after a ransomware attack known as WannaCry.

What We Know

WHERE IT STARTED Microsoft said the attack had originated in Ukraine, where hackers first targeted M.E.Doc, a tax-accounting software company, and the ransomware soon spread to at least 64 countries. ESET, a Slovakia-based cybersecurity company, also said the first known infection was through M.E.Doc. (See below for an explanation of what ransomware is.)

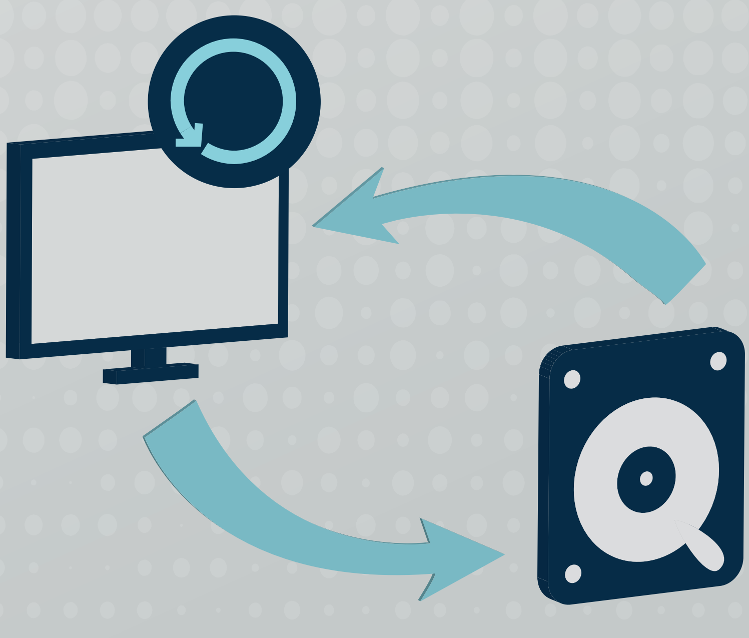
2. Protect: Identity and access management (IAM) tools are essential to protecting enterprise devices and computing assets. Network access control (NAC) ensures that only devices that have the adequate security settings and adhere to IT security policies are able to access corporate systems.

3. Detect: Technologies should be in place to detect anomalies in the infrastructure, in the event that malware has infiltrated the endpoints or network. The network must be monitored to check for indicators of compromise. Turning on AI-enabled malicious traffic detection, can also help automate detection swiftly before the attack worsens.



4. Respond: When a ransomware incident has been detected, security experts must work fast to block malicious communication channels at the firewall or IPS, and quarantine infected machines.

5. Recover: Backup is a critical part of the strategy for fast recovery. In addition, the backup system needs to prevent the replication of files that were maliciously encrypted by ransomware. This can be achieved with dynamic segmentation and inherent security features.



The ransomware steps included are from the *Ransomware: The Pervasive Business Disruptor.*

LIQUIDTECHNOLOGY
www.liquidtechnology.net

Sources:

https://www.trendmicro.com/vinfo/us/security/definition/ransomware

https://edgylabs.com/20-million-confirmed-attacks-in-24-hours-recent-ransomware/

http://www.cxotoday.com/story/how-companies-can-disrupt-ransomware-attacks/

https://www.statista.com/statistics/593093/leading-types-of-encryption-ransomware/