CISCO

Inside Ransomware

Ransomware has evolved to become the most profitable malware type in history.

Ransomware is Big Business

Ransomware is expected to gross cyberthieves **$1 billion** in 2016.[i]

Globally, **40% of businesses** experienced a ransomware incident during the past year.[ii]

Over **50% of U.S. companies** experienced a ransomware incident during the past year.

60% of ransomware attacks in **the enterprise** demanded **$1,000 or more.**[iii]

50% of US ransomware victims pay the ransom.

Globally, more than **40% of ransomware victims pay the ransom**[iv]

Under Attack

In the News:

Orange County Transportation Authority[v]

- Ransomware attack encrypted files on **88 servers**
- Ransom demand: **$8,500**
- OCTA chose **NOT** to pay. Time to restore data: **2.5 days**
- Total cost: **$600,000**

"One of the biggest security concerns for retailers right now is ransomware… Threats are increasingly sophisticated so multilayered protection is also necessary to help defeat advanced malware."

– Perry Stockwell, Systems Administrato, SCHEELS

How Ransomware Works

Infection Vector

User clicks malicious link to a compromised site or malvertising OR user clicks links in phishing emails or a malicious attachment. Most common attack vectors:

- Email - Worldwide, **46%** of all ransomware attacks originate from email[vi]
- Vulnerabilities in popular software - Flash accounts for **80%** of successful exploit attempts[vii]

Initial payload exploits a system

- Drops an effective ransomware variant
- Exploit kit or ransomware file is downloaded on the endpoint

C2 Comms & Assymetric Key Exchange

- A callback is made to the malicious ransomware infrastructure
- 2015 averaged **1000** new ransomware code variants **daily**[viii]

Encryption of File

- Time to total system encryption varies from **16 minutes to 18 seconds**[ix]
- Data on endpoint is crypted when reansomware retrieves the private encryption keys, encrypting as many files as possible

Request of Ransom

- After encryption is complete, code displays ransom message
- Victim pays ransom, remediates, or both

"While Ransomware is a growing and evolving threat, there are ways to thwart these attacks. Having great tools in your arsenal is the best way to combat this ever-evolving problem. Umbrella provides the leverage and visibility to block traffic to these malicious sites, along with providing the investigation tools to research an existing problem."

– Freud Alexandre, Enterprise Architect & Security Manager, City of New Orleans

A Multi-Layered Defense Strategy

Prevent:

- Back up all of your critical data
- Protect users on any device, anywhere, anytime
- Consistent and comprehensive patch management

Detect and Contain:

- Continuously monitor your networks
- Identify malware exploit kits and prevent malware code form executing
- Block malicious command and control traffic, malicious files and malicious URLs in email

Reduce Risk of Infection:

- Develop a proactive security plan that leverages a multi-layer defense
- Use predictive intelligence to understand where attacks are staged on the internet
- Continuously improve network hygiene and evaluate your security posture

"The primary protection against Ransomware is user training. When this fails, you need to have systems such as Umbrella and Firepower to build layers of protection when your users inevitably click on that attachment or link."

– Tyler Warren, Security Consultant, Prologis

For more information about protecting your business against the threat of ransomware, visit:
cisco.com/go/ransomware

[i] David Fitzpatrick and Drew Griffin, "Ransomware is expected to gross cyberthieves $1 billion in 2016 says FBI," CNN Money, April 15, 2016 (http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/)
[ii] "40 Percent of Enterprises Hit by Ransomware in the Last Year," Secuirty Magazine, August 4, 2016 (http://www.securitymagazine.com/articles/87332-percent-of-enterprises-hit-by-ransomware-in-the-last-year)
[iii] Ibid.
[iv] Ibid.
[v] Nick Gerda, "Transportation Authority Kept Secret Cyber Attack That Cost $600,000," VoiceOC, August 2, 2016 (https://voiceofoc.org/2016/08/transportation-authority-kept-secret-cyber-attack-that-cost-600000/)
[vi] "40 Percent of Enterprises Hit by Ransomware in the Last Year," Secuirty Magazine, August 4, 2016 (http://www.securitymagazine.com/articles/87332-percent-of-enterprises-hit-by-ransomware-in-the-last-year)
[vii] Cisco, "Cisco 2016 Midyear Cybersecurity Report," 2016
[viii] Rick Correa, "How Fast Does Ransomware Encrypt Files? Faster than You Think," Barkley, 2016 (https://blog.barkly.com/how-fast-does-ransomware-encrypt-files)
[ix] Ibid.

ZIFF DAVIS