Ransomware: The Reality

It's here, it's sophisticated—and it's shifty!

Loss of sensitive, proprietary data

Financial losses

Disruption

Harm to reputation

Malware with a hefty price tag.

Recognize the accelerating threat

2015

NUMBER 3 on the FBI's "Hot Topics for 2015" list[1]

Gaining momentum

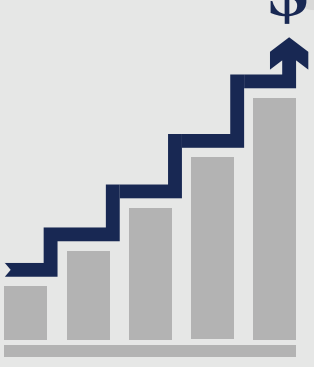
$24 million extorted in more than 2400 complaints to the FBI[2]

$60 million campaign of Angler Exploit Kit thwarted[3]

2016

The "year of the ransom"

$209 million extorted in first 3 months[4]



$1 BILLION in profit expected in 2016[5]

6-fold increase in corporate user targets[6]

Know the Attack Vectors

Exploit kits are tools used by attackers to distribute malware. They are often delivered through:

- **Email:** phishing messages and spam with malicious links or attachments
- **Web servers:** entry points for access into the network
- **Web-based apps:** encrypted files spread through social media and instant messaging
- **Malvertising:** drive-by downloads from an infected site

Infection Vector	Command and Control	Encryption of Files	Request of Ransom
Frequently uses the web and email	Takes control of targeted systems	Files become inaccessible	Owner/company pay the ransom (bitcoins) to free the system

Prevent attacks with an architectural approach:

- Protection across DNS layer, endpoints, email, web, and network
- Secure devices on and off the network
- Be prepared to detect and contain movement of malware quickly

Detect and Disrupt Ransomware

Cisco Talos disrupts a **$60 million** annual ransomware attack[7]

One of the largest and most advanced exploit kits, known as Angler, was used in targeted malvertising campaigns

Exploitation of **90,000 victims** a day for **$30 million** annually through nearly **150 proxy servers** was stopped

Learn More Today

Go to **cisco.com/go/ransomware** for Cisco's simple, open, automated, and effective approach to security.

CISCO

[1]U.S. Department of Justice, Federal Bureau of Investigation, 2015 Internet Crime Report, https://pdf.ic3.gov/2015_IC3Report.pdf
[2]The Federal Bureau of Investigation, "Ransomware: Latest Cyber Extortion Tool," April 2016 https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool
[3]Talos, Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60m Annually from Ransomware Alone, October 2015, http://www.talosintelligence.com/angler-exposed/
[4]CNN Money, "Cyber-Extortion Losses Skyrocket, Says FBI," David Fitzpatrick and Drew Griffin, April 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5]Ibid.
[6]Security Week, "History and Statistics of Ransomware," Kevin Townsend, June 2016, http://www.securityweek.com/history-and-statistics-ransomware
[7]Cisco Talos, Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60m Annually from Ransomware Alone, October 2015, http://www.talosintelligence.com/angler-exposed/