

# Ransomware: The Reality

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



Loss of sensitive, proprietary data



Disruption



Financial losses



Harm to reputation

Malware with a hefty price tag.



Recognize the accelerating threat



**NUMBER 3** on the FBI's "Hot Topics for 2015" list<sup>1</sup>

**\$24 million** extorted in more than 2400 complaints to the FBI<sup>2</sup>

**\$60 million** campaign of Angler Exploit Kit thwarted<sup>3</sup>

2015

Gaining momentum



2016

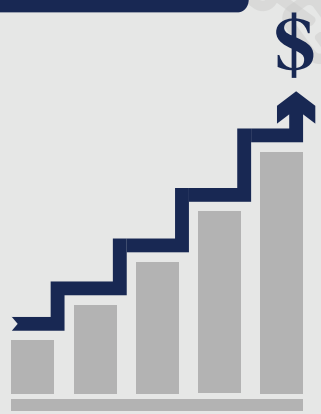
The "year of the ransom"

**\$209 million** extorted in first 3 months<sup>4</sup>



**\$1 BILLION** in profit expected in 2016<sup>5</sup>

**6-fold increase** in corporate user targets<sup>6</sup>



## Know the Attack Vectors

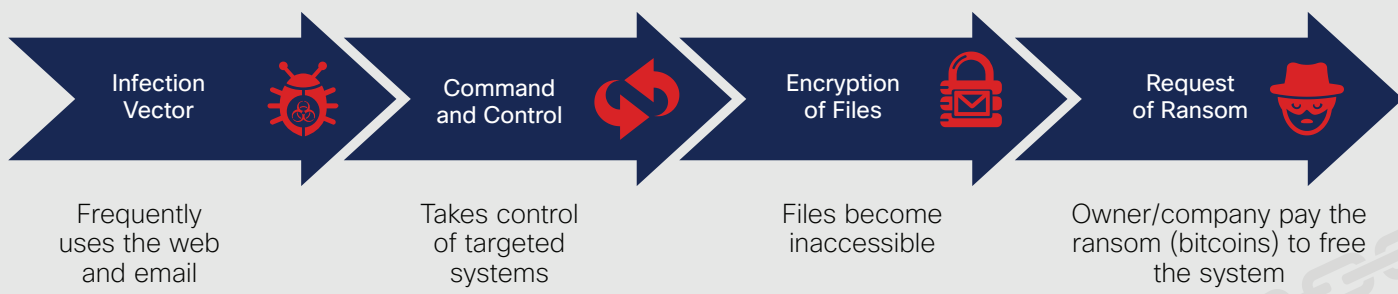
Exploit kits are tools used by attackers to distribute malware. They are often delivered through:

**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



**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<sup>7</sup>

- 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](http://cisco.com/go/ransomware) for Cisco's simple, open, automated, and effective approach to security.



<sup>1</sup>U.S. Department of Justice, Federal Bureau of Investigation, 2015 Internet Crime Report, [https://pdf.ic3.gov/2015\\_IC3Report.pdf](https://pdf.ic3.gov/2015_IC3Report.pdf)  
<sup>2</sup>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>  
<sup>3</sup>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/>  
<sup>4</sup>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/>  
<sup>5</sup>Ibid.  
<sup>6</sup>Security Week, "History and Statistics of Ransomware," Kevin Townsend, June 2016, <http://www.securityweek.com/history-and-statistics-ransomware>  
<sup>7</sup>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/>