

# Ransomware: A realidade

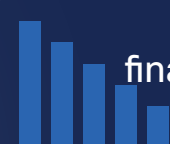
Já está aqui, é sofisticada e sorrateira.



Perda de dados confidenciais e proprietários



Interrupção



Perdas financeiras



Danos à reputação

**Malware de alto custo.**



**Reconheça a ameaça crescente**



**NÚMERO 3** na lista "Hot Topics for 2015" do FBI<sup>1</sup>

Mais de 2400 queixas ao FBI, somando extorsões no valor de

**US\$ 24 milhões**<sup>2</sup>

Fracasso da campanha de

**US\$ 60 milhões**

do kit de exploração Angler<sup>3</sup>

2015

Em processo de fortalecimento



2016

O "ano do resgate"

Extorsões no valor de

**US\$ 209 milhões**

nos primeiros três meses<sup>4</sup>

Expectativa de lucro de

**US\$ 1 bilhão** em 2016<sup>5</sup>

**Aumento de seis vezes**

do foco em usuários corporativos<sup>6</sup>



## Conheça os vetores de ataque

Os kits de exploração são ferramentas utilizadas pelos invasores para disseminar o malware. São difundidos frequentemente por:

**Email:** mensagens de phishing e spam, com links ou anexos mal-intencionados

**Servidores da Web:** pontos de entrada para acesso à rede

**Aplicativos da Web:** arquivos criptografados distribuídos por mídias sociais e mensagens instantâneas

**Malvertising:** downloads "drive-by" de um site infectado



Usa com frequência a Web e o e-mail

Obtém o controle dos sistemas atingidos

Os arquivos ficam inacessíveis

Proprietário/empresa paga o resgate (bitcoins) para liberar o sistema

**Impeça ataques com uma abordagem arquitetônica:**



Proteção para camada DNS, endpoints, e-mails, Web e rede



Proteção de dispositivos dentro e fora da rede



Detecção e contenção rápidas do deslocamento do malware

**Detecte e detenha o ransomware**

Cisco Talos detém um ataque de ransomware de **US\$ 60 milhões** ao ano<sup>7</sup>



Um dos mais difundidos e mais avançados kits de exploração, conhecido como Angler, foi utilizado em campanhas direcionadas de malvertising



Foi interrompida a exploração de **90.000 vítimas** por dia em cerca de **150 servidores proxy**, o que resultaria em **US\$ 30 milhões** ao ano

**Saiba mais hoje mesmo**

Acesse **cisco.com/go/ransomware** para obter a abordagem de segurança eficaz, automatizada, aberta e simples da Cisco.



<sup>1</sup>U.S. Department of Justice, Federal Bureau of Investigation, 2015 Internet Crime Report (Relatório de 2015 sobre crimes da Internet), [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" ("Ransomware: A ferramenta mais recente de extorsão digital"), abril de 2016 <https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool>  
<sup>3</sup>Talos, Threat Spotlight: Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60m Annually from Ransomware Alone (Threat Spotlight: A Cisco Talos detém acesso de grande kit de exploração internacional que gera US\$ 60 milhões ao ano apenas com ransomware, outubro de 2015, <http://www.talosintelligence.com/angler-exposed/>)  
<sup>4</sup>CNN Money, "Cyber-Extortion Losses Skyrocket, Says FBI" ("Prejuízos por extorsão digital aumentam, de acordo com o FBI"), David Fitzpatrick e Drew Griffin, abril de 2016, <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>  
<sup>5</sup>Id.  
<sup>6</sup>Security Week, "History and Statistics of Ransomware" ("Histórico e estatísticas do Ransomware"), Kevin Townsend, junho de 2016, <http://www.securityweek.com/history-and-statistics-ransomware>  
<sup>7</sup>Talos, Threat Spotlight: Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60m Annually from Ransomware Alone (Threat Spotlight: A Cisco Talos detém acesso de grande kit de exploração internacional que gera US\$ 60 milhões ao ano apenas com ransomware, outubro de 2015, <http://www.talosintelligence.com/angler-exposed/>)