

Ransomware: de realiteit

Aanwezig, geraffineerd – en bijna ongrijpbaar!



Verlies van gevoelige eigendomsinformatie



Disruptie



Financiële verliezen



Schade aan reputatie

Malware met een flink prijskaartje.



Herken de groeiende bedreiging



NUMMER 3 op de lijst 'Hot Topics for 2015' van de FBI¹

\$ 24 miljoen afgeperst in meer dan 2400 klachten bij de FBI²

\$ 60 miljoen gered door campagne met Angler-exploitkit te dwarsbomen³

2015

Toenemende impact



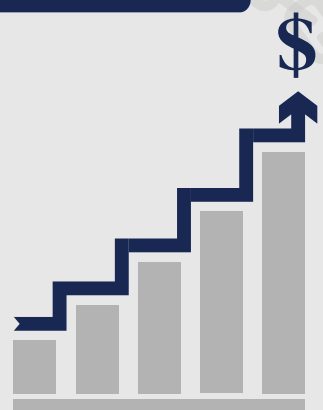
2016

Het 'jaar van het losgeld'

\$ 209 miljoen afgeperst in de eerste 3 maanden⁴

\$ 1 MILJARD winst verwacht in 2016⁵

zesvoudige toename onder zakelijke gebruikers⁶



Ken de aanvalsvectoren

Exploitkits zijn tools die aanvallers gebruiken om malware te verspreiden. Ze worden vaak geleverd via:

E-mail: phishingberichten en spam met kwaadaardige koppelingen of bijlagen

Webservers: toegangspunten voor toegang tot het netwerk

Webgebaseerde apps: versleutelde bestanden verspreiden zich via sociale media en instant messaging

Malvertising: verborgen downloads vanaf een geïnfecteerde site



Voorkom aanvallen met een op architectuur gebaseerde benadering:

Bescherm de DNS-laag, endpoints, e-mail, het web en het netwerk

Beveilig apparaten op en buiten het netwerk

Wees voorbereid om bewegingen van malware snel te detecteren en in te perken

Detecteer en verstoort ransomware

Cisco Talos verstoort een ransomwareaanval van **\$ 60 miljoen** op jaarbasis



Een van de grootste en meest geavanceerde exploitkits, Angler, werd gebruikt in gerichte malvertisingcampagnes



Er werd einde gemaakt aan exploitatie van **90.000 slachtoffers** per dag (**\$ 30 miljoen** op jaarbasis) via bijna **150 proxyservers**

Kom vandaag nog meer te weten

Ga naar cisco.com/go/ransomware voor informatie over Cisco's eenvoudige, open, geautomatiseerde en effectieve aanpak van beveiliging.



¹Amerikaanse ministerie van Justitie, Federal Bureau of Investigation, 2015 Internet Crime Report, https://pdf.ic3.gov/2015_IC3Report.pdf
²Federal Bureau of Investigation, 'Ransomware: Latest Cyber Extortion Tool', april 2016 <https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool>
³Talos, 'Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60M Annually from Ransomware Alone', oktober 2015, <http://www.talosintelligence.com/angler-exposed/>
⁴CNN Money, 'Cyber-Extortion Losses Skyrocket, Says FBI', David Fitzpatrick en Drew Griffin, april 2016, <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>
⁵ibid.
⁶Security Week, 'History and Statistics of Ransomware', Kevin Townsend, juni 2016, <http://www.securityweek.com/history-and-statistics-ransomware>
⁷Talos, 'Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60M Annually from Ransomware Alone', oktober 2015, <http://www.talosintelligence.com/angler-exposed/>