Ransomware: la realtà

È qui, è sofisticato ed è subdolo.

Perdita di dati proprietari e sensibili

Perdite finanziarie

Turbative

Danni alla reputazione

Malware che costa caro.

Riconosci la minaccia sempre maggiore

2015

NUMERO 3 nell'elenco "Hot Topics for 2015" dell'FBI[1]

Un argomento di attualità

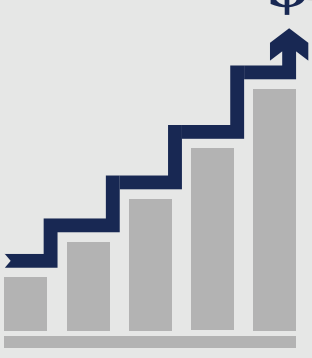
24 milioni di dollari estorti, come emerge da oltre 2400 denunce all'FBI[2]

60 milioni Contrasto alla campagna da di dollari di Angler exploit kit[3]

2016

"L'anno del riscatto"

209 milioni di dollari estorti nei primi 3 mesi[4]



1 MILIARDO DI DOLLARI di profitti previsti nel 2016[5]

Aumento di 6 volte degli utenti aziendali bersagliati[6]

Conosci i vettori di attacco

Gli exploit kit sono strumenti utilizzati dagli hacker per diffondere il malware. Spesso vengono diffusi attraverso:

- **E-mail:** messaggi di phishing e spam con link o allegati dannosi
- **Server Web:** punti di accesso per entrare nella rete
- **Applicazioni basate su Web:** file crittografati diffusi attraverso i social media e l'instant messaging
- **Malvertising:** download drive-by da un sito infetto

Vettore di infezione — Utilizza spesso il Web e le e-mail

Comando e controllo — Prende il controllo dei sistemi colpiti

Crittografia dei file — I file diventano inaccessibili

Richiesta di riscatto — Il proprietario/l'azienda paga il riscatto (bitcoin) per liberare il sistema

Previeni gli attacchi con un approccio architetturale:

- Protezione a livello di DNS, endpoint, e-mail, Web e rete
- Metti in sicurezza i dispositivi in rete e fuori dalla rete
- Preparati a rilevare e contenere velocemente lo spostamento del malware

Rileva e blocca il ransomware

Cisco Talos blocca gli attacchi ransomware per un valore di **60 milioni** di dollari l'anno

Uno dei maggiori e più avanzati exploit kit, noto come Angler, è stato utilizzato in campagne mirate di malvertising

È stato interrotto lo sfruttamento di **90.000 vittime** al giorno per **30 milioni** di dollari l'anno attraverso circa **150 server proxy**

Ulteriori informazioni

Accedi a **cisco.com/go/ransomware** per informazioni sull'approccio semplice, aperto, efficace e automatizzato di Cisco alla sicurezza.

[1]US Dipartimento di giustizia, Federal Bureau of Investigation, 2015 Internet Crime Report, https://pdf.ic3.gov/2015_IC3Report.pdf
[2]Federal Bureau of Investigation, "Ransomware: Latest Cyber Extortion Tool," aprile 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, ottobre 2015, http://www.talosintelligence.com/angler-exposed/
[4]CNN Money, "Cyber-Extortion Losses Skyrocket, Says FBI," David Fitzpatrick e Drew Griffin, aprile 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5]Ibid.
[6]Security Week, "History and Statistics of Ransomware," Kevin Townsend, giugno 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, ottobre 2015, http://www.talosintelligence.com/angler-exposed/