Atacurile de tip ransomware: în realitate

Există, sunt complexe și sunt ingenioase!

Pierderea datelor sensibile și brevetate

Pierderi financiare

Întreruperi ale activității

Distrugerea reputației

Malware cu un cost prea mare.

Recunoașteți amenințările alarmante

2015

Luați avânt

102 milioane RON sustrași în peste 2.400 de plângeri către FBI[1]

255 milioane RON Campania Angler Exploit Kit a fost sabotată[2]

2016

„Anul răscumpărărilor”

890 milioane RON
sustrase în primele 3 luni[3]

4.25 miliarde RON
profit estimat în 2016[4]

Creștere de 6 ori mai mare
în segmentul de utilizatori vizați din corporații[5]

Cunoașteți vectorii de atac

Kiturile de vulnerabilitate sunt instrumente utilizate de atacatori pentru a distribui malware. Acestea sunt de obicei trimise prin:

E-mail:
mesaje de phishing și spam cu linkuri sau atașamente cu conținut rău intenționat

Servere web:
puncte de intrare pentru accesul în rețea

Aplicații bazate pe web:
fișiere criptate, răspândite prin intermediul rețelelor de socializare și mesageriei instant

Publicitate infectată cu malware:
descărcări de tip drive-by de pe un site infectat

Vector de infectare
Utilizează frecvent internetul și e-mailul

Comandă și control
Controlează sistemele vizate

Criptare a fișierelor
Fișierele devin inaccesibile

Solicitări de răscumpărare
Deținătorul/compania plătește răscumpărarea (în bitcoin) pentru eliberarea sistemului

Prevenirea atacurilor printr-o abordare arhitecturală:

- Protecție la nivel DNS, terminale, e-mail, web și rețea
- Securizarea dispozitivelor din interiorul sau din afara rețelei
- Pregătiți-vă pentru detectarea și oprirea rapidă a malware-ului

Detectare și întrerupere Ransomware

Cisco Talos întrerupe un atac de tip ransomware de **255 milioane RON** anual[6]

Unul dintre cele mai mari și complexe kituri de vulnerabilitate, cunoscut ca Angler, a fost utilizat în campanii vizate de publicitate infectată cu malware

A fost oprită exploatarea a **90.000 de victime** pe zi, în valoare de **127 milioane RON** anual prin **aproximativ 150 de servere proxy**

Aflați mai multe astăzi

Accesați **cisco.com/go/security** pentru a afla mai multe despre abordarea Cisco simplă, deschisă, automatizată și eficientă.

CISCO

[1]FBI, „Ransomware: Latest Cyber Extortion Tool”, aprilie 2016, https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool
[2]Talos, Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60m Annually from Ransomware Alone, octombrie 2015, http://www.talosintelligence.com/angler-exposed/
[3]CNN Money, „Cyber-Extortion Losses Skyrocket, Says FBI”, David Fitzpatrick și Drew Griffin, aprilie 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[4]Ibid.
[5]Security Week, „History and Statistics of Ransomware”, Kevin Townsend, iunie 2016, http://www.securityweek.com/history-and-statistics-ransomware
[6]Cisco Talos, Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60m Annually from Ransomware Alone, octombrie 2015, http://www.talosintelligence.com/angler-exposed/