Zsarolóvírusok: Valóság, nem mese

Köztünk vannak, kifinomultak – és rafináltak!

Bizalmas, egyedi adatok elvesztése

Anyagi veszteség

Leállás

Hírnévvesztés

Malware tetszetős árcédulával.

Ismerje fel az erősödő fenyegetést

2015

3. az FBI **„2015 legfelkapottabb témái”** listáján[1]

Gyorsuló lendület

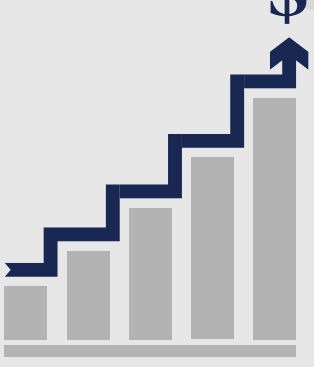
24 millió $ kizsarolása az FBI-hoz forduló több mint 2400 panaszostól[2]

Az Angler Exploit Kit **60 millió dollár bevételt** hozó kampányának meghiúsítása[3]

2016

„A zsarolás éve”

209 millió $
kizsarolása az első 3 hónapban[4]



Várhatóan
1 MILLIÁRD $
profit 2016-ban[5]

6x több vállalati célpont[6]

Ismerje meg a támadási felületeket

Az exploit kitek a támadók által a malware terjesztésére használt eszközök. Leginkább az alábbiakon keresztül terjednek:

E-mail:
adathalász üzenetek és kártékony linkeket vagy mellékleteket tartalmazó levélszemét

Webszerverek:
belépési pontok a hálózathoz való hozzáféréshez

Web-alapú alkalmazások:
a titkosított fájlok közösségi oldalakon és azonnali üzenet-küldésen keresztül terjednek

Malvertising (hirdetésekbe rejtett vírusok):
nem szándékos letöltések fertőzött oldalakról

Támadási felület	Vezérlés és irányítás	Fájlok titkosítása	Váltságdíj követelése
Gyakran az internetet és az e-mailt használja	Átveszi az irányítást a megtámadott rendszerek felett	A fájlok elérhetetlenné válnak	A tulajdonos/vállalat váltság-díjat fizet (bitcoinban) a rendszer felszabadításáért

Előzze meg a támadásokat architekturális megközelítéssel:

- DNS-rétegre, végpontokra, e-mailre, webre és hálózatra kiterjedő védelem
- Tegye biztonságossá a hálózaton lévő és attól távoli eszközeit
- Legyen felkészülve a malware észlelésére és mozgásának gyors behatárolására

Észlelje és ártalmatlanítsa a zsarolóvírusokat

A Cisco Talos évente **60 millió dollárnyi** kárt okozó zsarolóvírus-támadást ártalmatlanít.[7]

Az egyik legnagyobb és legfejlettebb, Angler néven ismert exploit kitet célzott malvertising kampányokban használták fel

Közel **150 proxy szerveren** keresztül elért, napi **90 000 áldozat** kifosztásának és éves szinten **30 millió $** váltságdíj kifizetésének vetettek véget

Bővebb információ

A **cisco.com/go/ransomware** oldalon megismerheti a Cisco egyszerű, nyílt, automatizált és hatékony biztonsági megközelítését.

CISCO

[1] Amerikai Igazságügyi Minisztérium, FBI, 2015 Internet Crime Report, https://pdf.ic3.gov/2015_IC3Report.pdf
[2] FBI, „Ransomware: Latest Cyber Extortion Tool,” 2016. április, 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, 2015. október, http://www.talosintelligence.com/angler-exposed/
[4] CNN Money, „Cyber-Extortion Losses Skyrocket, Says FBI,” David Fitzpatrick and Drew Griffin, 2016. április, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5] Ibid.
[6] Security Week, „History and Statistics of Ransomware,” Kevin Townsend, 2016. június, 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, 2015. október, http://www.talosintelligence.com/angler-exposed/