Oprogramowanie ransomware: rzeczywistość

Już tu jest, groźne i pomysłowe.

Utrata poufnych, zastrzeżonych danych

Straty finansowe

Zakłócenia działalności

Uszczerbek dla reputacji

Złośliwe oprogramowanie, które może kosztować fortunę.

Rozpoznaj rosnące zagrożenie

2015

Dynamiczny rozwój

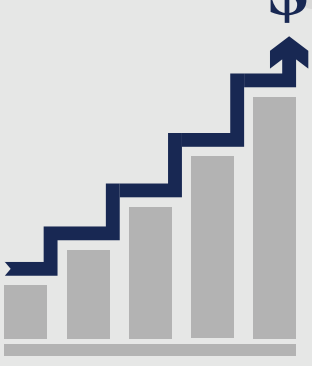
100 mln PLN Wartość wymuszeń z ponad 2400 skarg do FBI[1]

250 mln PLN Walka z kampanią pakietu wykorzystującego luki w zabezpieczeniach o nazwie Angler[2]

2016

„Rok okupu”

870 mln PLN
Wartość wymuszeń w pierwszych trzech miesiącach[3]



4 bln PLN
Prognozowane zyski w 2016 r.[4]

Sześciokrotny wzrost
częstości ataków na użytkowników korporacyjnych[5]

Poznaj wektory ataku

Przestępcy rozpowszechniają złośliwe oprogramowanie przy użyciu pakietów wykorzystujących luki w zabezpieczeniach. Są one często rozsyłane przy użyciu:

Poczty e-mail: fałszywe wiadomości i wiadomości-śmieci zawierające złośliwe łącza lub załączniki

Serwerów WWW: punkty dostępu do sieci

Aplikacji internetowych: zaszyfrowane pliki są rozsyłane poprzez media społecznościowe i komunikatory

Złośliwych reklam: pliki pobierane z zarażonej witryny

Wektor zarażenia	Przekazywanie sterowania i nadzoru	Szyfrowanie plików	Żądanie okupu
Często korzysta z sieci WWW i poczty e-mail	Przejmuje kontrolę nad zaatakowanymi systemami	Pliki stają się niedostępne	Właściciel/firma płaci okup (w bitcoinach), aby odzyskać system

Zapobieganie atakom przy użyciu metody opartej na architekturze:

- Ochrona w warstwie DNS, punktów końcowych, poczty e-mail, Internetu i sieci
- Zabezpiecz urządzenia w sieci i poza nią
- Przygotuj się na szybkie wykrywanie i eliminowanie ruchu złośliwego oprogramowania

Wykrywaj i zniszcz oprogramowanie ransomware

Cisco Talos eliminuje ataki oprogramowania ransomware o wartości **250 mln PLN** rocznie[6]

Jeden z największych i najbardziej zaawansowanych pakietów wykorzystujących luki w zabezpieczeniach, noszący nazwę Angler, został użyty w ukierunkowanych kampaniach z wykorzystaniem złośliwych reklam

Udaremniono ataki na **90 000 ofiar** dziennie o łącznej wartości **125 mln PLN** rocznie przy użyciu **prawie 150 serwerów proxy**.

Dowiedz się więcej już dzisiaj

Odwiedź stronę **cisco.com/go/security**, aby poznać prostą, otwartą, zautomatyzowaną i skuteczną metodę ochrony oferowaną przez Cisco.

CISCO

[1]Federalne Biuro Śledcze, „Ransomware: Latest Cyber Extortion Tool”, kwiecień 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, październik 2015, http://www.talosintelligence.com/angler-exposed/
[3]CNN Money, „Cyber-Extortion Losses Skyrocket, Says FBI”, David Fitzpatrick i Drew Griffin, kwiecień 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[4]Ibid.
[5]Security Week, „History and Statistics of Ransomware”, Kevin Townsend, czerwiec 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, październik 2015, http://www.talosintelligence.com/angler-exposed/