Ransomware: die Realität

Eine aktuelle, komplexe und raffinierte Bedrohung

Verlust vertraulicher, unternehmenseigener Daten

Finanzielle Verluste

Störungen

Reputationsverlust

Malware, die hohe Kosten verursacht

Erkennen Sie die wachsende Bedrohung.

2015

PLATZ 3 auf der Liste der wichtigsten **“Themen des Jahres 2015”** des FBI[1]

Zunehmende Angriffe

24 Millionen USD
erpresst – mehr als 2.400 Meldungen beim FBI[2]

60-Millionen-USD-
Kampagne des Angler-Exploit-Kits vereitelt[3]

2016

Das „Jahr der Ransomware“

209 Millionen USD
in den ersten drei Monaten erpresst[4]

1 MILLIARDE USD
Gewinn für 2016 erwartet[5]

6-fache Zunahme
der Angriffe auf Unternehmensbenutzer[6]

Informieren Sie sich über die Angriffsvektoren.

Exploit-Kits sind Tools, über die Angreifer Malware verbreiten. Oft werden sie über folgende Wege übertragen:

- **E-Mails:** Phishing-und Spam-Mails mit schädlichen Links oder Anhängen
- **Webserver:** Eingangspunkte für den Netzwerkzugriff
- **Webbasierte Anwendungen:** Verbreitung verschlüsselter Dateien über Social-Media und Instant-Messaging
- **Malvertising:** Drive-by-Downloads von einer infizierten Website

Infektionsvektor	Command-and-Control	Dateiverschlüsselung	Lösegeldforderung
Oft per Web oder E-Mail	Übernahme der Kontrolle über die Zielsysteme	Dateizugriff nicht mehr möglich	Eigentümer/Unternehmen zahlt das Lösegeld (Bitcoins) zur „Befreiung“ des Systems

Verhindern von Angriffen mit einem architekturbasierten Ansatz:

- Schutz für DNS-Layer, Endpunkte, E-Mail, Web und Netzwerk
- Absicherung von Geräten innerhalb und außerhalb des Netzwerks
- Voraussetzungen zum schnellen Erkennen und Aufhalten der Verbreitung von Malware

Erkennen und Aufhalten von Ransomware

Cisco Talos hält Ransomware-Angriff im Umfang von **60 Millionen USD** pro Jahr auf.[7]

„Angler“, eines der größten und raffiniertesten Exploit-Kits, wurde in gezielten Malvertising-Kampagnen eingesetzt.

Die Ausbeutung von **90.000 Opfern** pro Tag über knapp **150 Proxyserver** für ein Lösegeld von **30 Millionen USD** im Jahr wurde gestoppt.

Mehr Informationen

Unter **cisco.com/go/ransomware** finden Sie Informationen über den unkomplizierten, offenen, automatisierten und effektiven Sicherheitsansatz von Cisco.

CISCO

[1]U.S. Department of Justice, Federal Bureau of Investigation, 2015 Internet Crime Report, https://pdf.ic3.gov/2015_IC3Report.pdf
[2]The Federal Bureau of Investigation, „Ransomware: Latest Cyber Extortion Tool“, April 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, Oktober 2015, http://www.talosintelligence.com/angler-exposed/
[4]CNN Money, „Cyber-Extortion Losses Skyrocket, Says FBI“, David Fitzpatrick und Drew Griffin, April 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5]Ebd.
[6]Security Week, „History and Statistics of Ransomware“, Kevin Townsend, Juni 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, Oktober 2015, http://www.talosintelligence.com/angler-exposed/