Health Care Remains Hot Target

Phishing, spear phishing campaigns, and threats targeting the health care sector were down 78% in Q4, but increased dramatically by 211% in 2017. Cybercriminals are increasingly turning to fileless malware as their “go-to” toolbox—with PowerShell attacks surging 432% in 2017. Gold Dragon is a recent PowerShell attack that targeted organizations involved with the Pyeongchang winter games. Here is a quick look at how these attacks work.

McAfee GTI received on average 48 billion queries per day in Q4.

Threat Statistics

- Incidents: We counted 222 publicly disclosed security incidents in Q4, a decrease of 16% over Q3. Individual victims were the leading sector, comprising 28% of the total. 38% of all publicly disclosed security incidents in Q4 took place in the Americas.

- Malware: New malware samples increased in Q4 to an all-time high of 63 million, a 32% increase. The total number of malware samples grew 36% in the past four quarters to almost 690 million samples. Mac OS malware grew by 24% in Q4 over Q3. Still small compared with Windows threats, the total number of Mac OS malware samples increased by 7% in Q4. PowerShell malware grew 267%, reaching a total count of more than 47,000 samples.

- Mobile malware: Global infections of mobile devices fell by 0.2%; South America reported the highest rate, at 16%. Total mobile malware grew 46% in the past four quarters to 24 million samples.

- Ransomware: New ransomware samples increased in Q4, by 35%. The total number of ransomware samples grew 59% in the past four quarters to 14.8 million samples.

- URLs: McAfee GTI protections against risky URLs fell to 57 million per day in Q4 from 99 million per day in Q3.

- Files: McAfee GTI protections against malicious files increased to 45 million per day in Q4 from 40 million per day in Q3.

- IPs: McAfee GTI protections against risky IP addresses rose to 84 million per day in Q4 from 48 million per day in Q3.

Download: McAfee Labs Threats Report: March 2018

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 3785_0318


36% Incident: Delivery methods include malicious websites, documents, or emails.

57 million McAfee GTI protections against risky URLs per day

84 million McAfee GTI protections against malicious files per day

465 million McAfee GTI protections against risky IP addresses per day

Fileless Malware Powers Up

fileless malware

Threats Report

PowerShell malware

PowerShell

implant

Gather

Report

Permanent

Establish permanent presence on target system

Gather system data

Report to control server

Americas

Europe

Asia

Oceania

59%

27%

36%

16%

46%