

Cyber wars

Trends and recent attacks

The more technology evolves, the more sophisticated the cyber attacks on corporations, government agencies, hospitals, and national interests. Here's what we've learned about trends in cyber warfare, and a list of recent serious attacks.

Trends in cyber attacks



Ransomware

Digital version of extortion: Malware that prevents computer or network use until ransom is paid, usually in bitcoin.



Bots and botnets

Bot: Malware that takes control of an infected computer.

Botnet: Network of infected machines. They want personal information, credit card numbers, bank credentials, and ransom.



Attacks on third parties

Infiltrations as entry points to larger companies and entities.



Nation-state threats

Cyber attacks against states and societies. Goals: Political destabilization, cyber espionage, monetary gain.



Attacks on the Internet of Things (IoT)

Connected homes, offices, hospitals, and governments susceptible to mounting threats. Industries targeted include energy, utilities, healthcare, and finance.



Hacktivism

"Hacking for a cause" to promote political or social agenda. Well-known hacktivists: WikiLeaks, Anonymous, Xbox Underground, and RedHack.

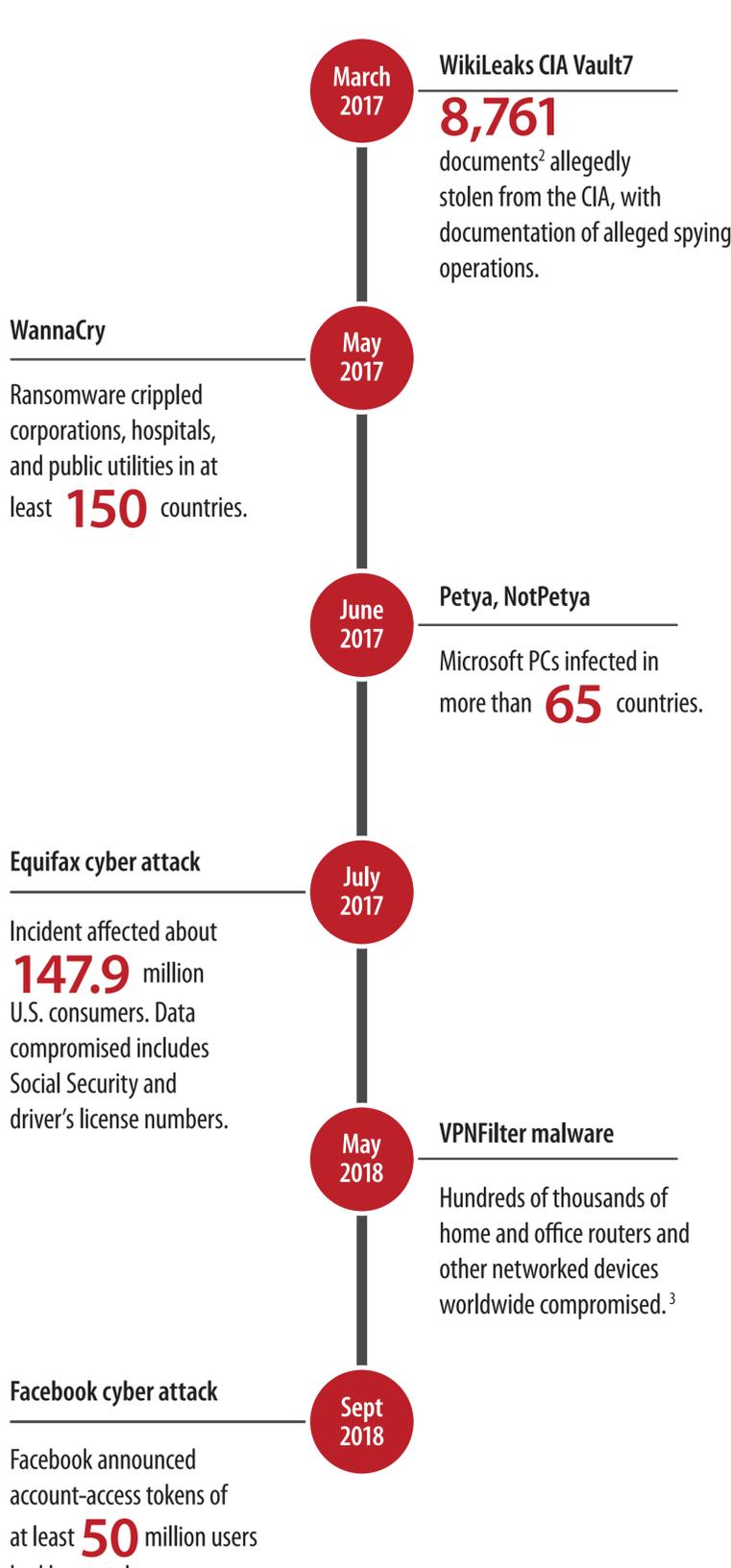
Data records across industries lost or stolen since 2013¹

14,644,949,623

Frequency of data records lost or stolen¹



2017–2018 large cyber attacks



Data sources:

1. Breach Level Index, <http://www.breachlevelindex.com/>, Gemalto, as of Oct. 1, 2018.
2. "The biggest cybersecurity disasters of 2017 so far," Wired.com, July 1, 2017.
3. FBI, Internet Crime Complaint Center (IC3), May 25, 2018.