Threat Landscape Resources

Summary information on the scope of cyber threats:

FBI Director Christopher Wray's speech at the International Conference on Cyber Security in New York. https://www.fbi.gov/news/stories/international-conference-on-cyber-security-2018

The Global Impact of Cybercrime - https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime-summary.pdf

Threats:

Threat actors vary by motivation. The availability of tools via hacking forums on the dark web allows less sophisticated actors to utilize more sophisticated tools.

Russian Threats:

Executive Summary on Grizzly Steppe: https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary

US indictment of FSB Officers and criminal hackers for hack of Yahoo!: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

Tracking of Ukrainian Field Artillery Units: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Iranian Threats:

Massive hacking indictment from March 2018: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

Denial of service attacks against US financial sector: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Chinese Threats:

Economic espionage by Chinese military officers: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Current Topics of Interest:

Weak passwords and reuse of passwords continues to be exploited by all threat actors. Companies and individuals should implement two factor authentication.

Password guidance: https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

Consider the use of a password manager.

Remote access credentials continue to be a hot commodity for adversaries. These may be issued to users to work from home, work while traveling, connect from satellite offices, and connect with business

partners. Outsourced IT and security firms also use them to provide off-site support, maintenance, and response. Weak or re-used passwords in these environments are particularly dangerous.

Ransomware – Prevention and Response: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Business Email Compromise: https://www.ic3.gov/media/2017/170504.aspx

Valuable Resources

FBI - https://www.ic3.gov/default.aspx; https://www.fbi.gov/investigate/cyber

DHS - https://www.us-cert.gov/home-and-business

NSA Information Assurance - https://www.iad.gov/iad/index.cfm