2018 Cybersecurity Trends

- According to the 2018 Verizon Data Breach Investigation Report, over 75% of breaches are motivated by financial gain. Corporate espionage has decreased over time, but attacks as the result of a grudge against a company are increasing. Stealing money has always been the top motivation for attacking a company,[1] but destruction of systems and data is increasing in relevance.[2]
- The largest percentage of attacks overall (~48%) use hacking to steal account credentials to gain access to corporate systems and data. Using malware is the second highest method but social engineering (i.e., phishing) is becoming more common overall. Phishing is the most common attack method in the financial services industry. [1]
- Organized crime rings are by far the most common threat actor in 2018 (50%), but 28% of breaches involve internal actors in some way.[1]
- Personal information and payment card information are the top two types of data that are stolen in the financial industry.[1]
- 68% of data breaches took months or longer to discover.[1]
- According to the Cisco 2018 Annual Cybersecurity Report, attacks are becoming automated very quickly. Malware is becoming adaptive so that it can self-propagate much more easily.[2] This means that a few attackers can have a much larger impact now than in the past and existing antivirus applications are not equipped to deal with new malware variants.[3] Also, the sheer amount of malware has increased substantially year over year from 2017 – over 102% higher in 2018.[4]
- Attackers are using encryption to evade detection and launching attack campaigns from legitimate internet services like Google and Dropbox which makes identification almost impossible.[2] Therefore, attackers can get in easier and stay longer before being detected. Attacks that use encryption to hide their true motives increased 275% year-to-date in 2018 over 2017.[4]
- Internet of Things (IoT) devices that are on corporate networks but are unknown to the organization are opening security gaps that are exploited by adversaries.[2] Our desire for easy access and convenience is causing a lot of the problems that we're trying to fix.
- 53% of attacks result in damages of $500,000 or more. 30% of attacks cost between $1M and $5M.[2]
- Cryptojacking/cryptomining is supplanting ransomware as the most lucrative attack. This attack uses computer resources to mine bitcoin rather than destroying data or holding the computer ransom. Cryptomining malware is difficult to detect and can remain hidden and active for a very long period of time,[5] although sometimes the malware persistently requests admin access until it's granted.[4]

---

[1] 2018 Verizon Data Breach Investigation Report
[2] Cisco 2018 Annual Cybersecurity Report
[3] Ponemon State of Endpoint Security Risk Report
[4] 2018 Sonicwall Cyber Threat Report
[5] Malwarebytes blog on February 2, 2018: https://blog.malwarebytes.com/cybercrime/2018/02/ransomwares-difficult-second-album/