Lecture 5 - attack evolution

dinsdag 29 november 2022 10:37

least popular part of a targeted attack : lateral movement

living off the land attack : use legitimately available tools for malicious purposes

alternative : install malware

Powershell

WMI (Windows Management Instrumentation)

\+ no need for specific malware
\+ difficult to detect

\- speed

\- cost

general purpose malware is very difficult to create for ICS networks

hence, living off the land is more common

fixing high-severity vulnerabilities is not better than fixing some(more) random vulnerabilities ; an attacker only needs a few of their choice

zero-day exploits are similar to attack weapons nowadays

zero-days have a lifetime of 19 days - 30 months

updates are not applied quickly
you cannot fix something if you do not know what to fix

Nowadays, vulnerabilities are traded on a market

triple extortion → 1. no money ⇒ system and data lost
2. no money ⇒ leak all data
new! 3. no money from customer of victim ⇒ leak all data

drop in ransomware in 2022: geopolitics,
volatile cryptocurrency prices
double jeopardy : paying sanctioned entity can lead to a fine

log4shell : remote code execution (RCE) in commonly used logging library

IoT malware

software supply chain attacks

learn list of advantages!

cryptojacking → mining coins using victim's hardware

Mitre att&ck Enterprise matrix

APT 28

APT 29