Lecture 4

Tuesday, 22 November 2022 13:30

old ransomware: non-targeted "shotty in the wild", hundreds of $ of ransom

new ransomware: targeted one attack, millions of ransom

Cryptolocker 2013 vector: spear email (double extension: .pdf.exe)
downloaded from botnet

Petya 2016 overwrite master boot record (MBR)

WannaCry 2017 spreads like a worm, no human interaction used hacking tool from NSA

250000 detections in 4 days

NotPetya 2017 not ransomware; it just destroys
originally spread via backdoor in accounting software used in Ukraine

initially: shift to coin mining

then: targeted ransomware

afraid: companies with trade secrets, governments

target: local government, hospitals, ... buyers with insufficient protection; blocks company's operations

↓

also: no payment ⇒ data will be published

Maastricht University

↳ started with phishing email

↓

Office macro

↓

lateral movement

probably opportunistic

↓

investment (after one) is needed

colonial pipeline (oil) → compromised password

Equifax hack → system command execution through vulnerability in Apache Struts 2

security update not installed sufficiently quickly

direct attacks allow for opportunistic attacks

big problem: with people whose data are stored not the customer, the market does not value cybersecurity (i.e. if data is leaked, the individual customer does not suffer)

hacking team hack: embedded systems (e.g. routers) are a weak link

there are almost always other options (e.g. email server)

DDOS attacks: low cost, for hire