CYBEROPS

TO PERSPEKTIVER

- Hackerens perspektiv
- Analytikerens perspektiv

HVA ER EN HACKER



01 Motivasjon

02 Ressurser

03 Teknisk evne

NIVÅ 1

AMATØREN



01 Motivasjon

02 Ressurser

03 Teknisk evne

NIVÅ 1

AMATØREN



Motivasjon

- Nysgjerrighet
- Ideologi
- Selvhevdelse

NIVÅ 1

AMATØREN



Ressurser

- Få personlige ressurser
- Gratistjenester
- Forumer
- Youtube
- Github

NIVÅ 1

AMATØREN



Teknisk evne

- Varierende
- Kan være dyktig, men ofte større mangler
- Jobber ofte isolert, avhengig av egen kompetanse

NIVÅ 2

CYBERKRIMINELL



01 Motivasjon

02 Ressurser

03 Teknisk evne

NIVÅ 2

CYBERKRIMINELL



Motivasjon

- Økonomisk gevinst
- Bestillingsoppdrag

NIVÅ 2

CYBERKRIMINELL



Ressurser

- Tilgang til mer kostbart utstyr
- Flere som jobber sammen

NIVÅ 2

CYBERKRIMINELL



Teknisk evne

- Varierende
- Kan være flere i samme gruppe, utfyller svakheter
- Kan hente kompetanse fra statlige aktører

NIVÅ 3

ADVANCED PERSISTENT THREAT



- Høyt kapabel aktør
- Ofte styrt eller sponset av en stat

NIVÅ 3

ADVANCED PERSISTENT THREAT



Motivasjon

- Politisk styrt
- Langsiktige mål
- Spionasje, påvirkningsoperasjoner

NIVÅ 3

ADVANCED PERSISTENT THREAT



Ressurser

- Statlige midler (evig)
- Fra noen få, til hundre, til tusenvis av ansatte

NIVÅ 3

ADVANCED PERSISTENT THREAT



Teknisk evne

- Spesialiserte roller
- Ofte rekruttert fra tekniske universiteter

SÅ LA OSS HACKE NOE

CYBER KILL CHAIN

- Modell utviklet av Lockheed Martin.
- Viser stegene en aktør ofte tar før de oppnår målene sine
- “Kill” refererer til at man kan knerte et pågående angrep med utgangspunkt i hvert trinn i kjeden. Jo tidligere, jo bedre.
- Hvor langt i kjeden kom vi i vårt “angrep”?



Å SPORE AKTØREN

På endepunkt

- Deteksjonssystemer
- Logger
- Konfigurasjoner
- Skadevare

På midtpunkt

- Nettverkstrafikk
- Konfigurasjon
- Programvare
- Porter
- Tjenestetilbyder

HVORDAN BLI TATT

- Trafikk rett fra hjemmeruter
- Metadata-analyse
- Beslag og forensics av PC
- Jail

JA3 / JA4

- Bruker ukryptert informasjon fra TLS Client Hello
- Gir informasjon om programvare, tls-versjon, protokollbruk
- Hashes og struktureres slik at samme maskin kan spores basert på innholdet UA (User-Agent)
- La oss titte litt

DNS-OPPSLAG

- Domain Name System (DNS)
- Oversetter domenenavn til IP
  - Browser spør DNS-server om IP’en som matcher et domenenavn
  - DNS-server svarer med hvilken riktig IP
  - Browser kobler seg til IP
- Går ukryptert, så kan plukkes opp og brukes i analyse

VPN OG VPS

- Brukes ofte av aktør for å gjemme seg og skjule hva de gjør
- Gjør attribusjon vanskelig

VIRTUAL PRIVATE NETWORK

VPN

- Skjuler fra hvem og til hvor trafikk går
- Aktør → VPN-server → Mål
- Målet vil se at trafikken kommer fra VPN-serveren, ikke fra aktør
- En som følger med på aktør sin PC, vil se at trafikken går til VPN-server, ikke mål.
- VPN-tilbyder ser alt.

VIRTUAL PRIVATE SERVER

VPS

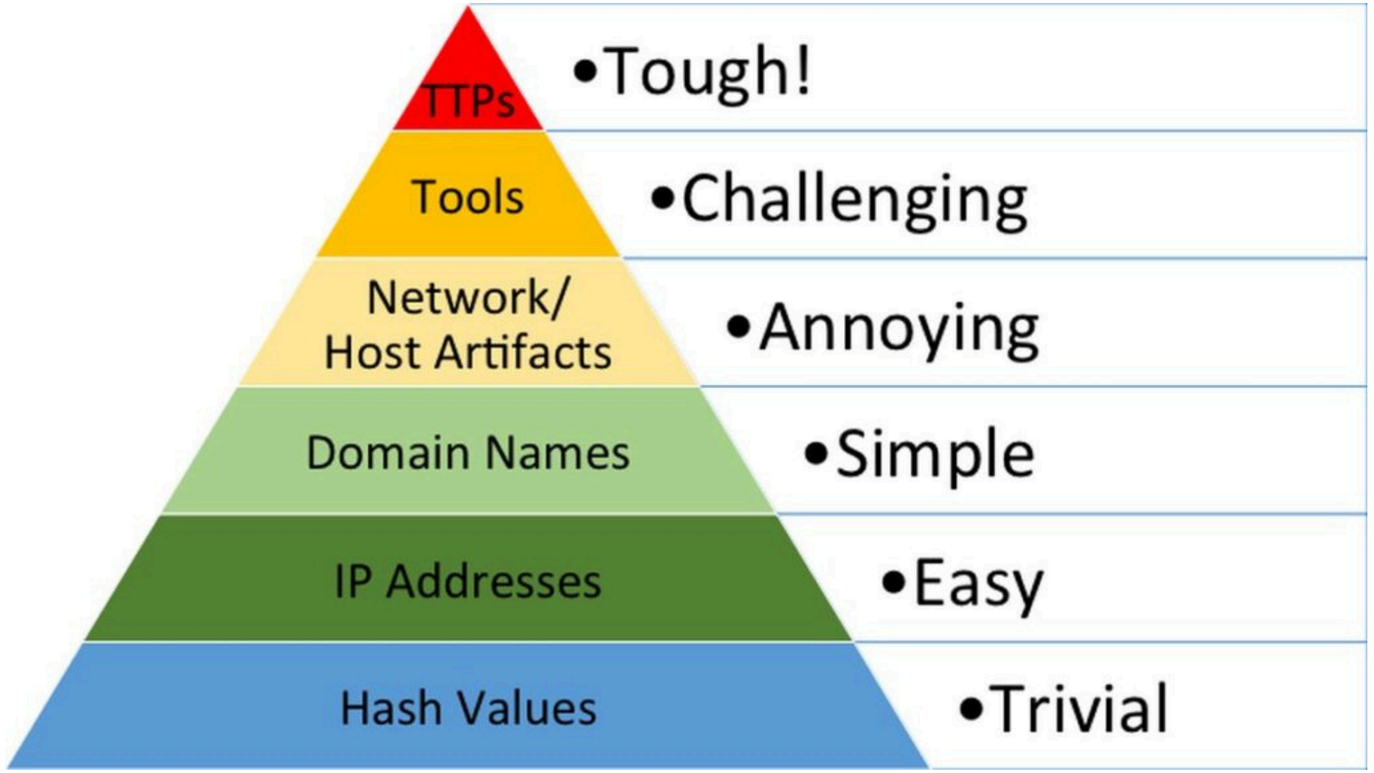
- Server du kan leie
- Kun en virtualisert del av en fysisk server, delt med mange andre
- Gjør at aktør kan lage en kjede med servere som kommuniserer med hverandre over VPN
- Vanskelig å spore

TACTICS

TECHNIQUES

PROCEDURES

- TTP
- Den samlede tekniske profilen til aktør
- Veldig vanskelig for aktør å endre på
- Brukes for å spore dem



CYBER THREAT INTELLIGENCE

CTI

- Kunsten å forstå, følge og attribuere aktør
- Strategisk
- Taktisk
- Teknisk

Hvem driver med dette?

NORSKE STATLIGE AKTØRER

EOS-TJENESTENE

- NSM
- PST
- Etterretningstjenesten

- Samarbeider i Felles cyberkoordineringssenter (FCKS)

NSM

NASJONAL SIKKERHETSMYNDIGHET

- Myndighet for nasjonale sikkerhetshendelser
- Ansvar for håndteringen av større dataangrep mot kritisk infrastruktur
- Eier VDI, Varslingssystem for Digital Infrastruktur

PST

POLITIETS SIKKERHETSTJENESTE

- Ansvar for intern, nasjonal sikkerhet
- Forebygger lovbrudd som kan true landets sikkerhet

E

ETTERRETNINGSTJENESTEN

- Ansvar for etterretningsoppdrag i utlandet
- Følger med på utenlandske trusselaktører
- APT’er er ofte styrt av andre lands etterretningstjenester
- Har tilgang til TI, (Tilrettelagt innhenting), som fanger opp all nettverkstrafikk inn og ut av landet

KOMMERSIELLE AKTØRER

CTI

- Crowdstrike
- Fireeye
- Mandiant