ThreatMatrix/
Modelling for DC/Server-Operators

A simple Threatmodelling – matrix incase of DFIR or risk-analysis

Actor	E	D	C	B	A
Botnet-Infection [1]					
Direct Attack / APT [2]					
James Bond					
Malicious Insider					
Ransomware					
Skiddos					
Bad Luck					
By-catch [3]					

Version 0.17 2020-11-03

Explanations:

[1]

- Cryptotrojan
- Mal/Spam – Bots
- DDoS-Bots

[2]

- StateActors
- Competitors
- HighProfile - Hacking

[3]

- an attack from within the datacenter (other amchine hacked first) or
- somethign that was not initially directed towards you, but ended on one of your systems by mistake or chance

Scores:

- A – highly likely
- B – most likely
- C – possible
- D – not likely
- E - impossible

ThreatMatrix/
Modelling for DC/Server-Operators

Detectionpossibilities by Actors

Actor	Automation	Noisyness	Artefacts	Documented	IOCs
Botnet-Infection [1]	high	high	many	yes	many
Direct Attack / APT [2]	med/low	med/low	luck	sometimes	some
James Bond	low	low	luck	no	no
Malicious Insider	low	low/med	some	no	no
Ransomware	high	med	some	yes	many
Skiddos	low	high	some	sometimes	some
Bad Luck	?	?	?	?	?
By-catch [3]	?	?	?	?	?

Version 0.17 2020-11-03