SPCSS

Státní pokladna
Centrum sdílených služeb

Poskytovatel garantovaných služeb NDC včetně kybernetické bezpečnosti ve státní správě

Aktivní obrana proti kybernetickým útokům v resortu Ministerstva financí

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x1
Intro

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x2
Adversary

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x2

Adversary

Rozdíl mezi západní a východním přístupem

- **Východní přístup**
  - 36 stratagems
  - Sun-Tzu - umění války
- **Západní přístup**
  - Odsuzuje používaní klamu (deception)
  - Nenapadá nic a nikoho zezadu (otázka charakteru)
  - Clausewitz - Válka

Stage 0x2

Adversary

MoneyTaker

- Aktivní od jara 2016
- Útoky na banky v Rusku a USA a na jejich transakční systém
- Používá phishing, meterpreter payload a powershell skript

Stage 0x2

Adversary

Buhtrap

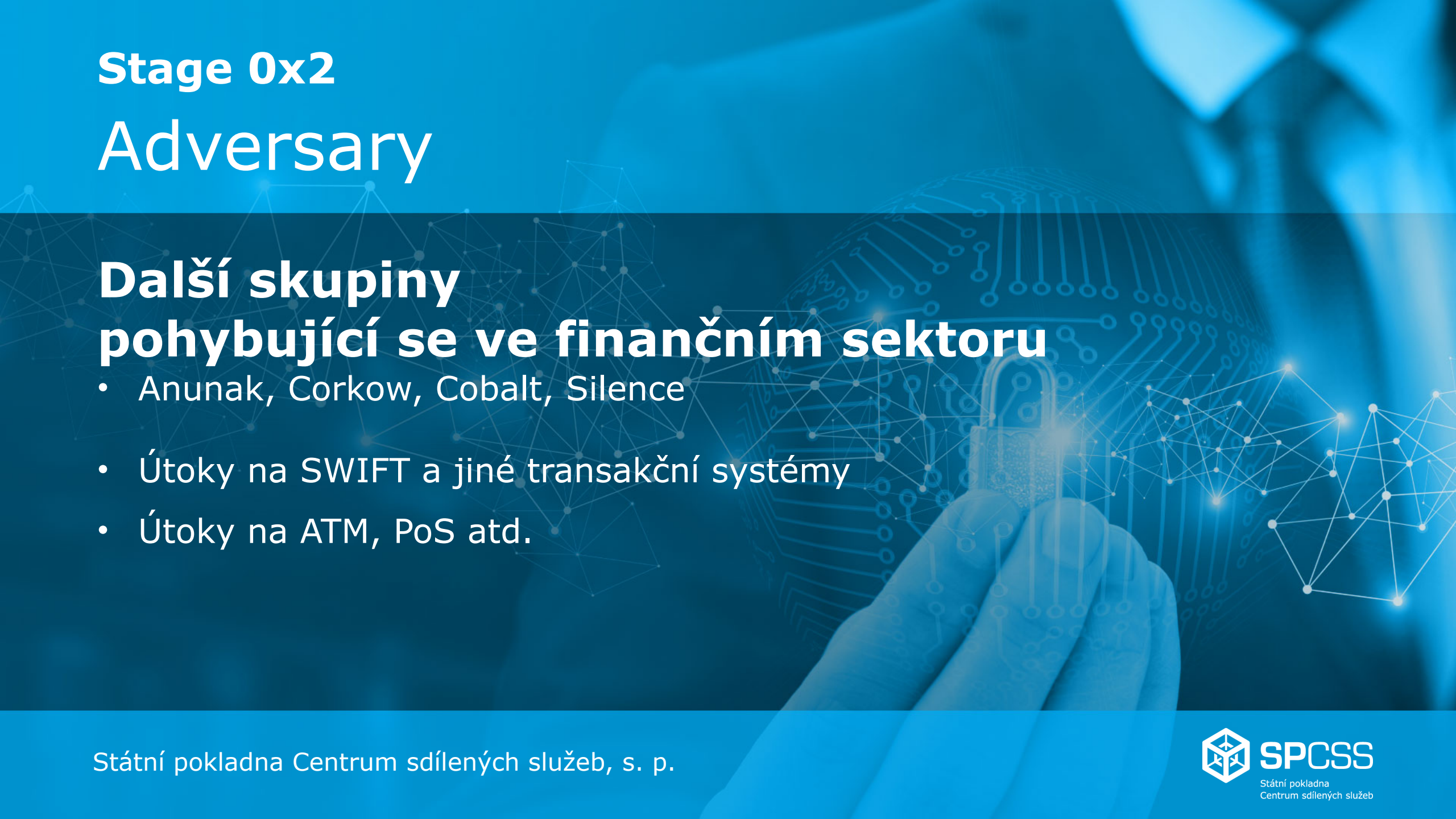
- Od 02/2016 do 08/2016 ukradeno 25 milionů dolarů
- Největší suma ukradená bance: 8.5 milionu dolarů
- Používá červa, který infikuje celou infrastrukturu bankovní instituce
- Používá phishing s přiloženým RTF souborem

Stage 0x2

Adversary

Další skupiny pohybující se ve finančním sektoru

- Anunak, Corkow, Cobalt, Silence
- Útoky na SWIFT a jiné transakční systémy
- Útoky na ATM, PoS atd.



Stage 0x2

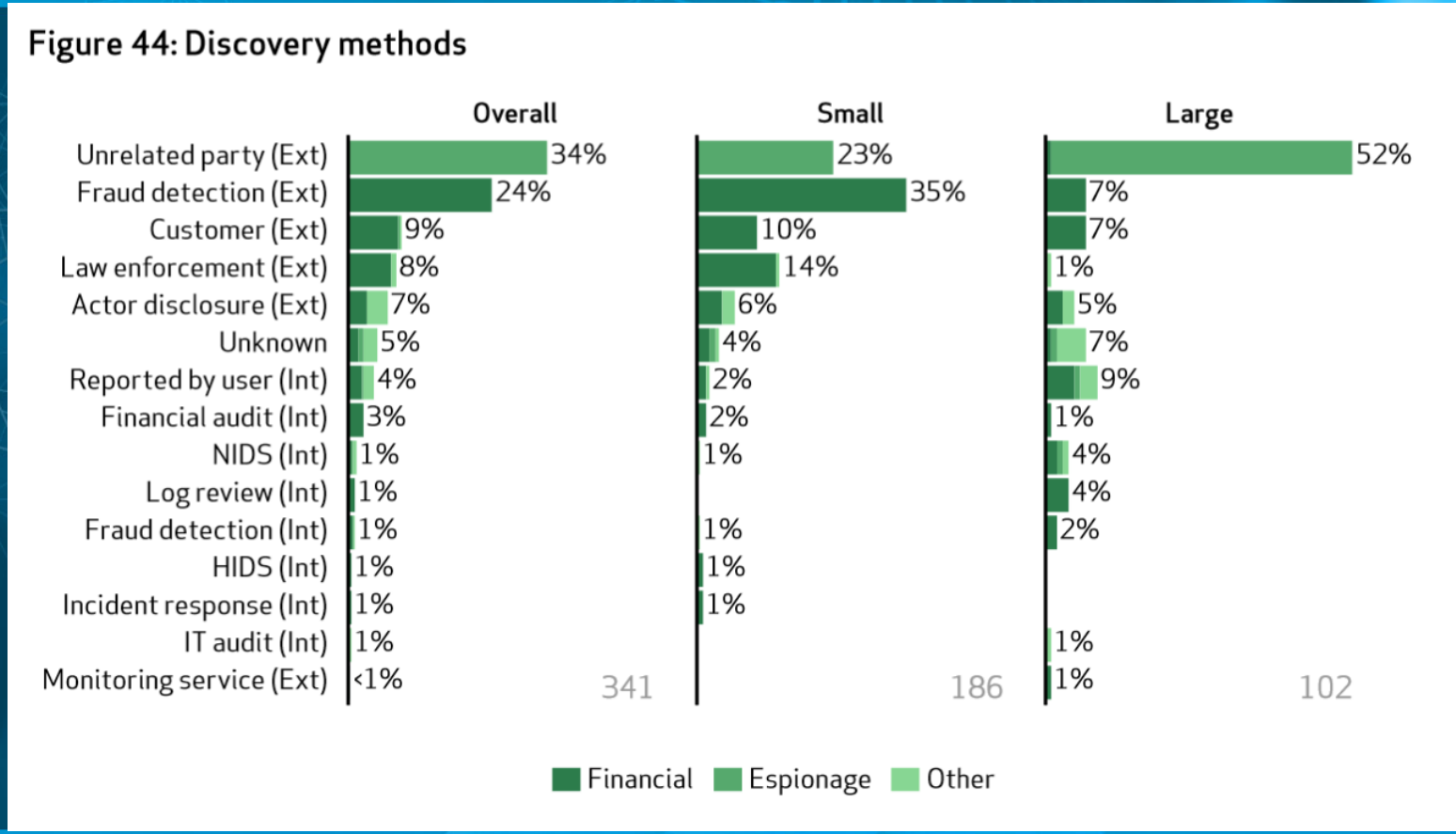
Adversary

- **Reaktivní obrana**
  - AV, IDS, FW . . .
- **Proaktivní obrana**
  - Threat hunting, Vulnerability Scaning . . .
- **Aktivní obrana**
  - Decoys, tokens, emulators, deception, counterdeception . . .

Stage 0x2

Adversary

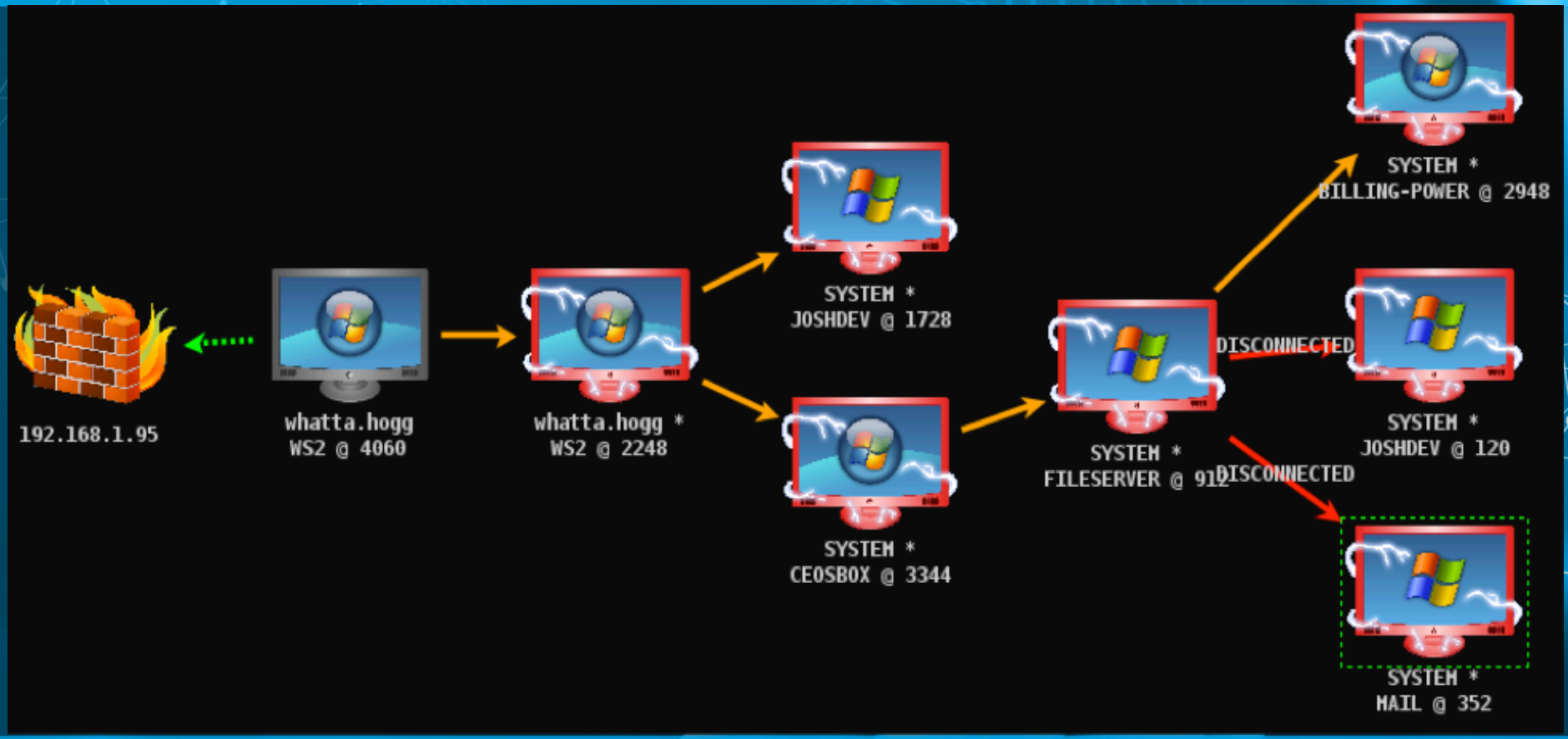
Verizon Data Breach Investigations Report 2013



Stage 0x2

Adversary

Pwned

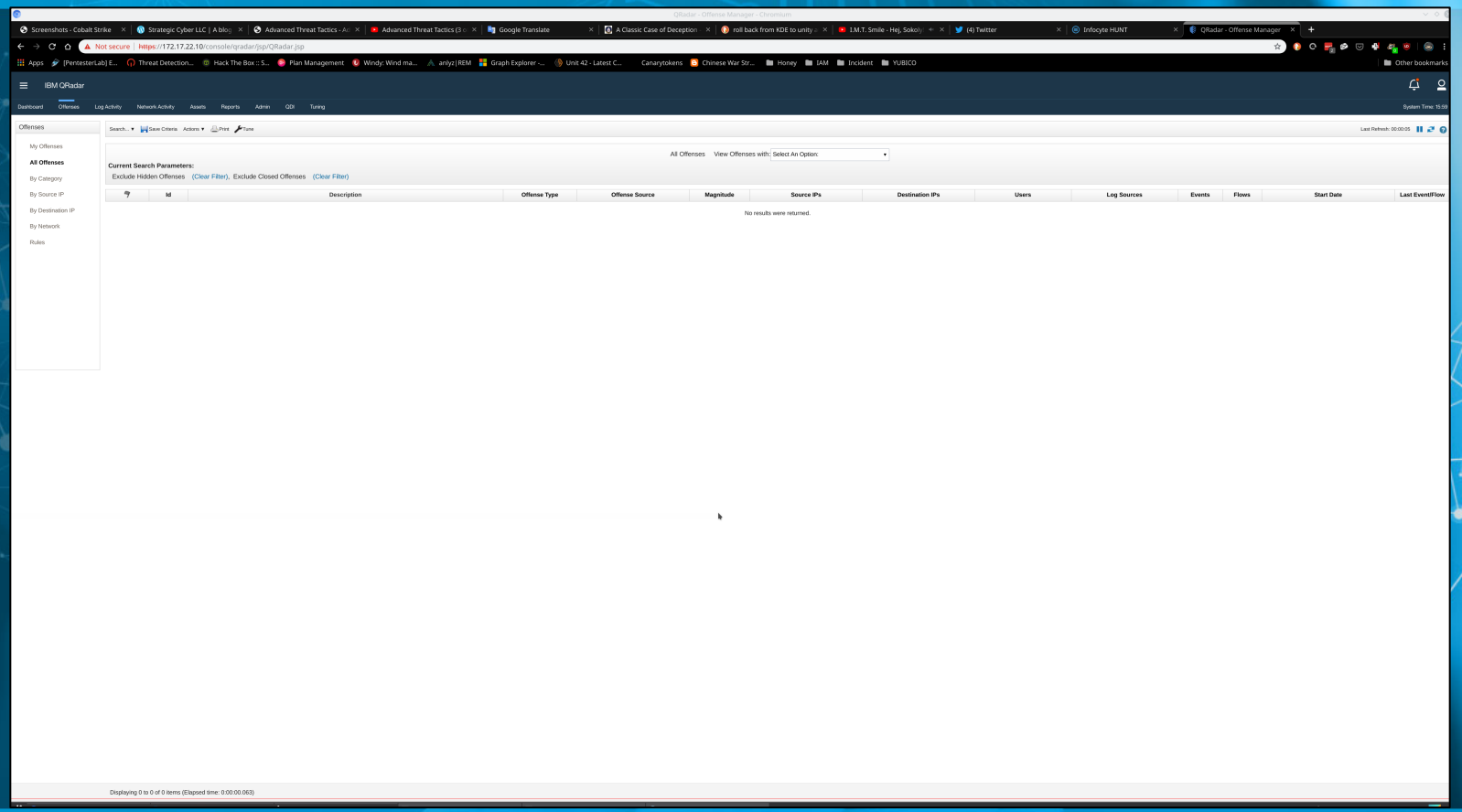


Stage 0x2

Adversary

Tradiční Obrana:

Bez reakce!

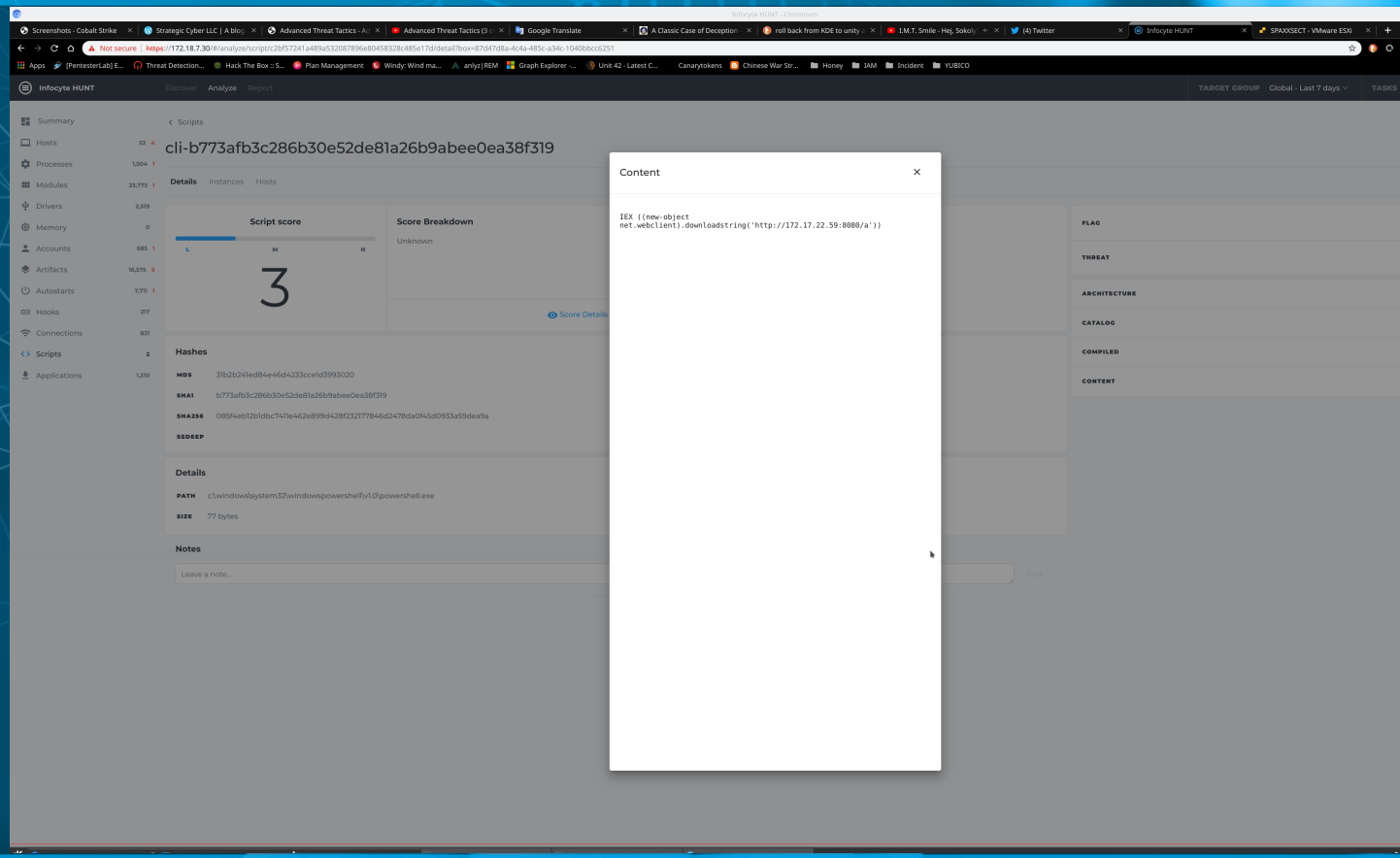


Stage 0x2

Adversary

Proaktivní obrana (memory dump)

- Odhalila spuštěný script, označen jako bezpečný
- Bez akce



SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x03
Defender

Státní pokladna Centrum sdílených služeb, s. p.

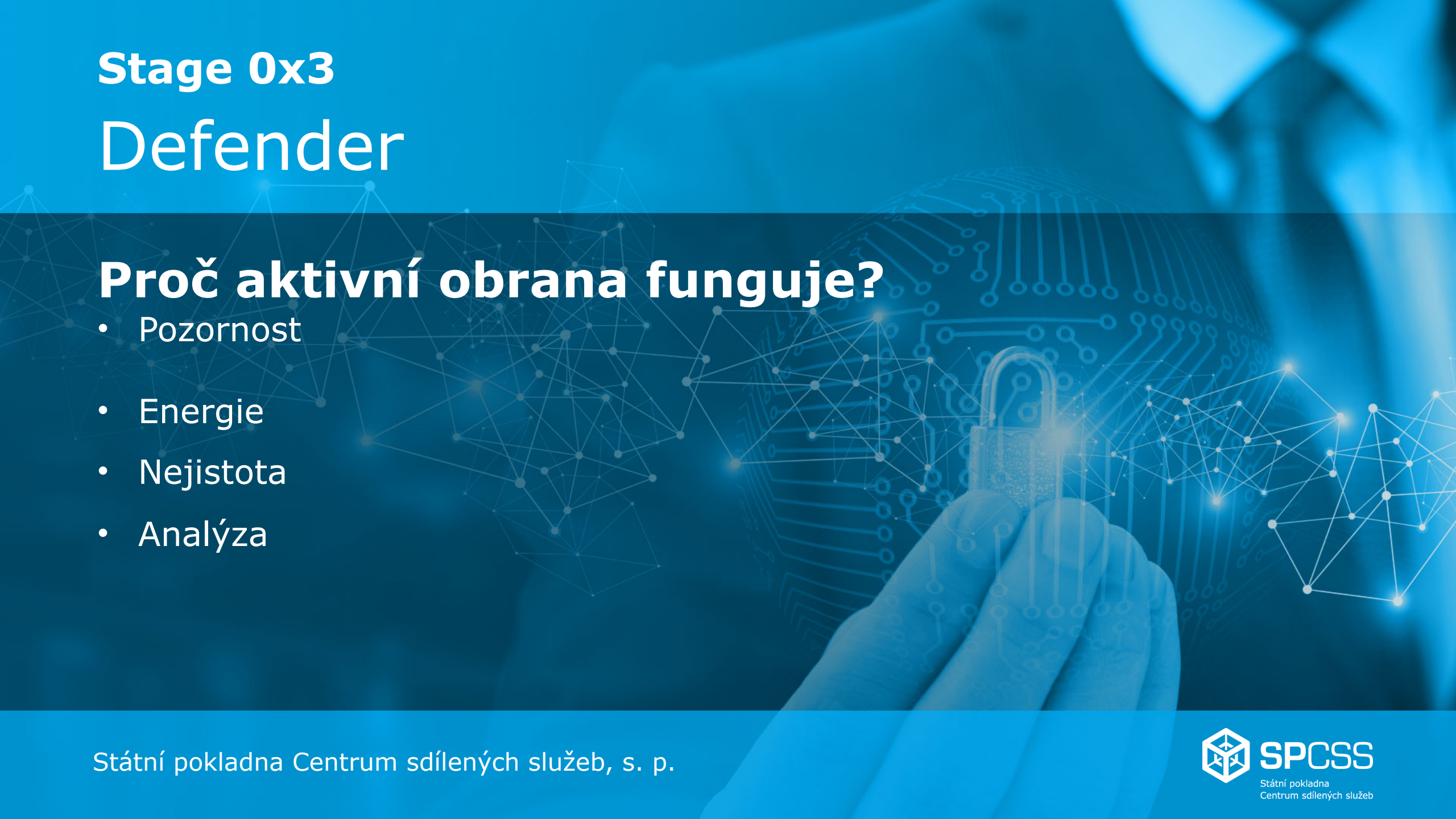
SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x3

Defender

Proč aktivní obrana funguje?

- Pozornost
- Energie
- Nejistota
- Analýza



Stage 0x3

Defender

Co je aktivní obrana?

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x3

Defender

Metody aktivní obrany

- Deception
- Counterdeception
- Counter-Deception

Stage 0x3

Defender

Nejdostupnější prvky aktivní obrany

- Decoys
- Tokens
- Emulators

Státní pokladna Centrum sdílených služeb, s. p.

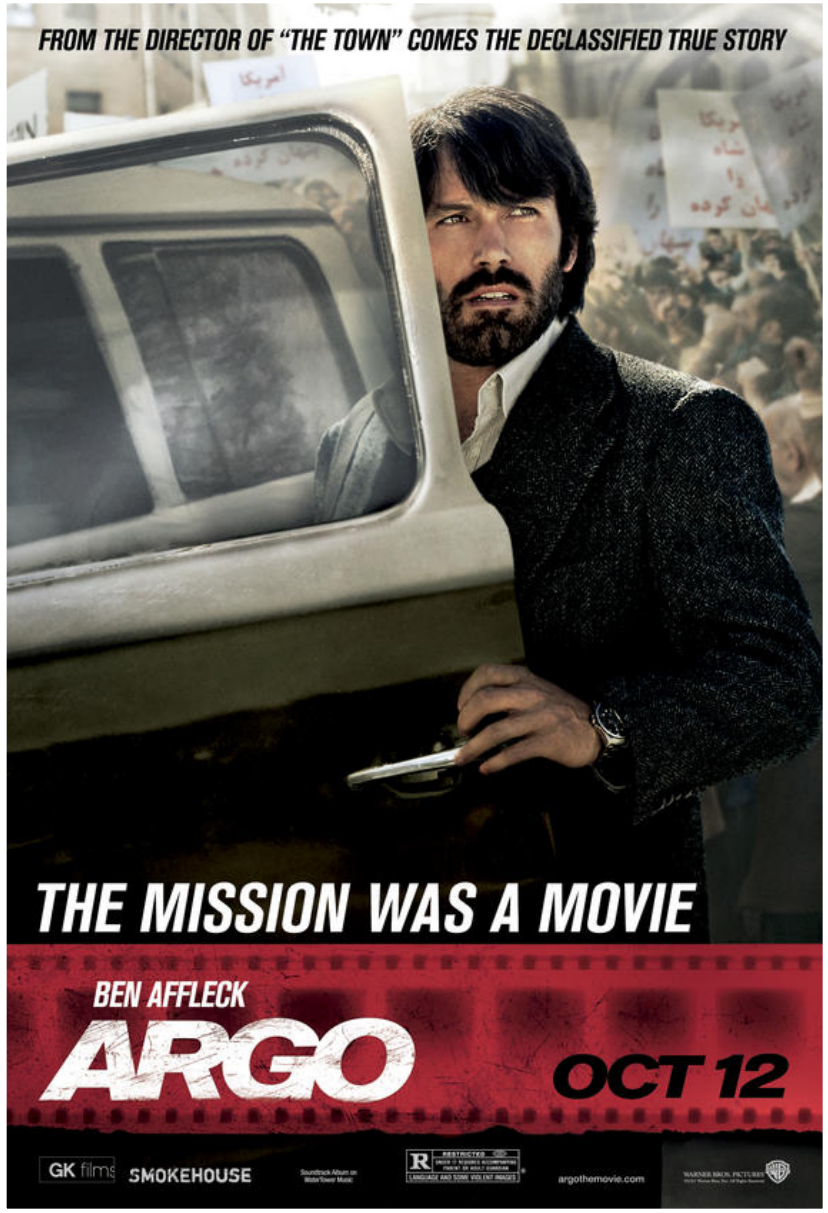
SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x3

Defender

Scénář ARGO

- Deception
- Zakryj pravdu, odkryj faleš



SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x3

Defender

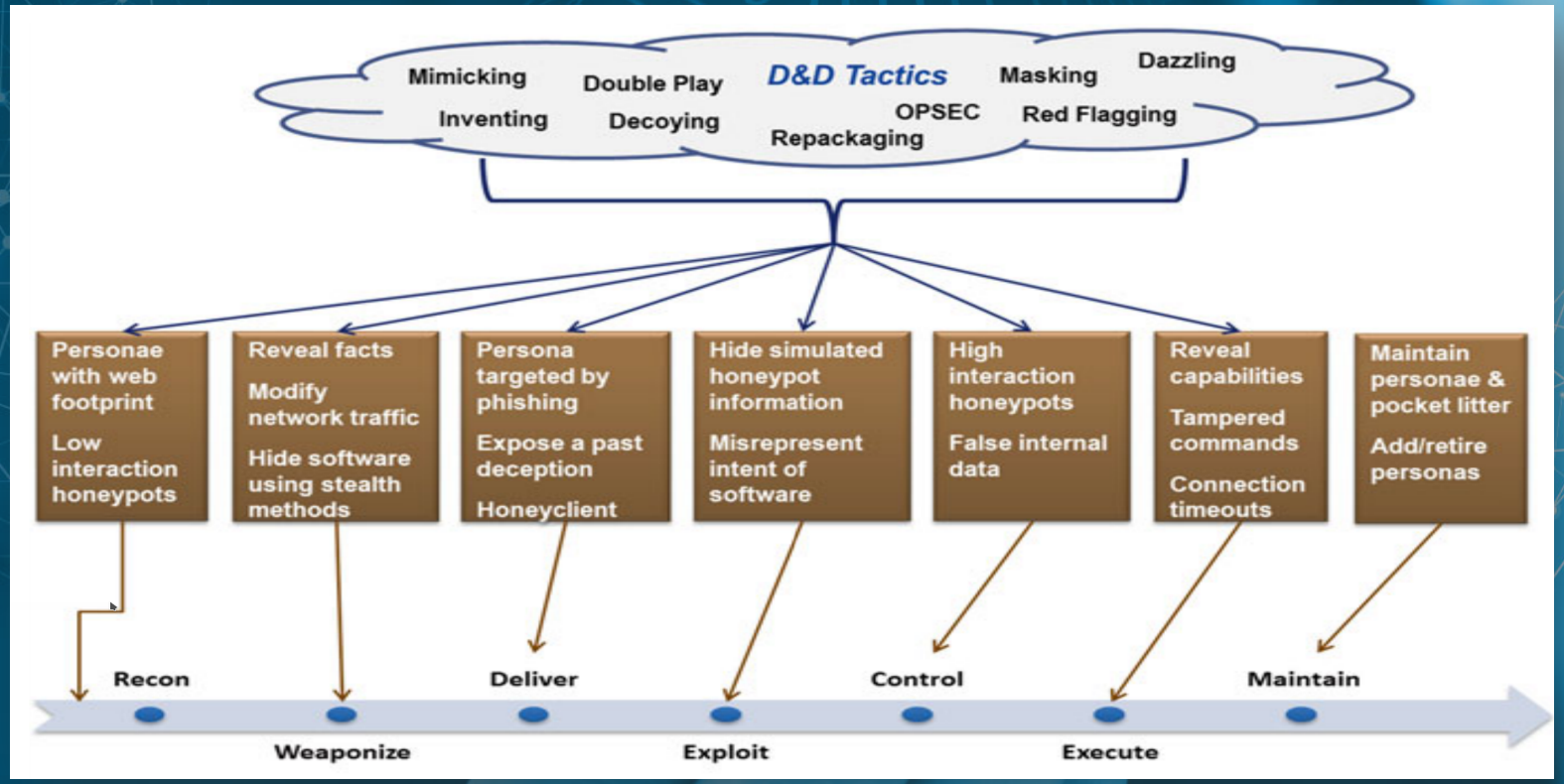
Scénář F-35 vs J-31

- Counterdeception
- Counter-Deception

Stage 0x3

Defender

Deception taktika pro cyber killchain



Stage 0x4
Framework

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Framework

Definice týmu

- Mastermind
- Realizační tým
- Méně je vždy více

Stage 0x4

Framework

Účel

- Definice strategie
- Operační a taktický cíl
- Důvod
- Kritéria

Analýza

- Útočník
- Chování útočníka
- Odhad chování

Stage 0x4

Framework

Tvorba příběhu

- Uvěřitelný
- Řetězení příběhů
- Může se stát cokoliv
- Test příběhu
- Rozsah příběhu - Argo

Bojový plán

- Zohlednit analýzu
- Nastavit prostředí
- Důraz na příběh

Stage 0x4

Framework

Plán B

- Možnost selhání
- Záložní řešení
- Zařadit do příběhu

Spuštění

- Technologie a příběh pod kontrolou

Stage 0x4

Framework

Monitoring

- Real-time monitoring
- Alerty
- Trasování
- Vyrušení, odklonění, absolutní eliminace (vyčerpání zdrojů)

Redesign

- Aktualizovat příběh
- Celý nebo jeho část

Stage 0x5

EOF

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

EOF

Coming soon – Limitovaná místa

- **17. 9. – 18. 9. 2019**
  MISP training
  s CIRCL.lu
- **19. 9. 2019**
  AIL Framework workshop s
  CIRCL.lu
- **7. 11. 2019**
  Hunting Season session
  0x00 (ver.2019.11)
- **8.11.2019**
  Hunting Season
  session 0x00 (ver.2019.11)

Děkujeme

Napište nám na CSIRT@SPCSS.CZ