Role forenzní analýzy v činnosti CSIRT týmů

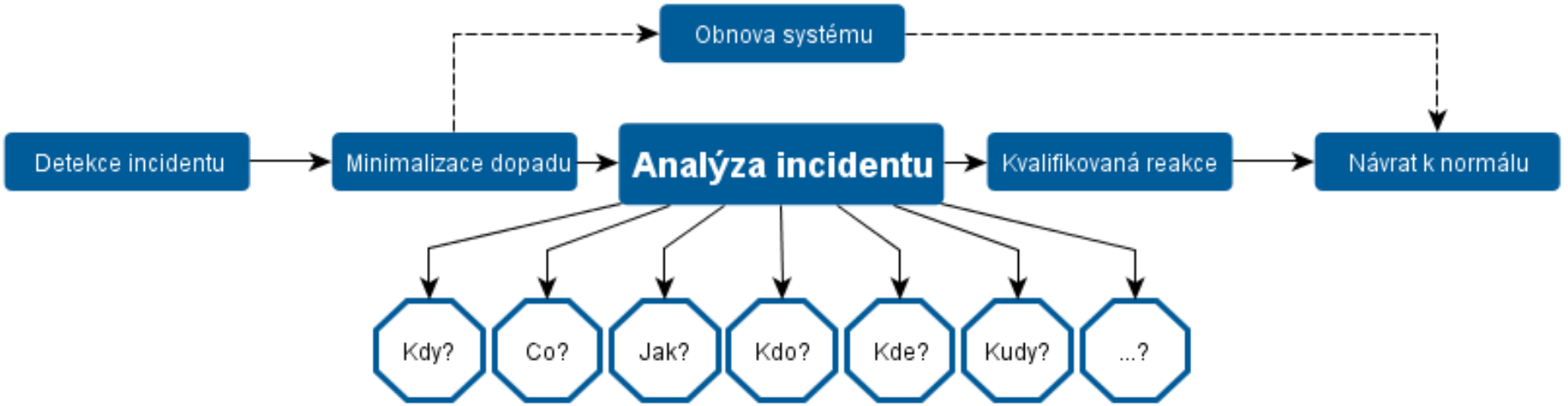
Aleš Padrta

CESNET-CERTS

- CESNET, z. s. p. o.
  - Provoz národní e-infrastruktury pro vědu, výzkum a vzdělávání
- CESNET-CERTS
  - CSIRT pro síť CESNET2
- FLAB
  - Forenzní laboratoř CESNET
  - Podpůrné pracoviště CESNET-CERTS
  - Analýza bezpečnostních incidentů
  - Penetrační a zátěžové testy

CSIRT a informace

- CSIRT
  - Základní služba = reakce na incident

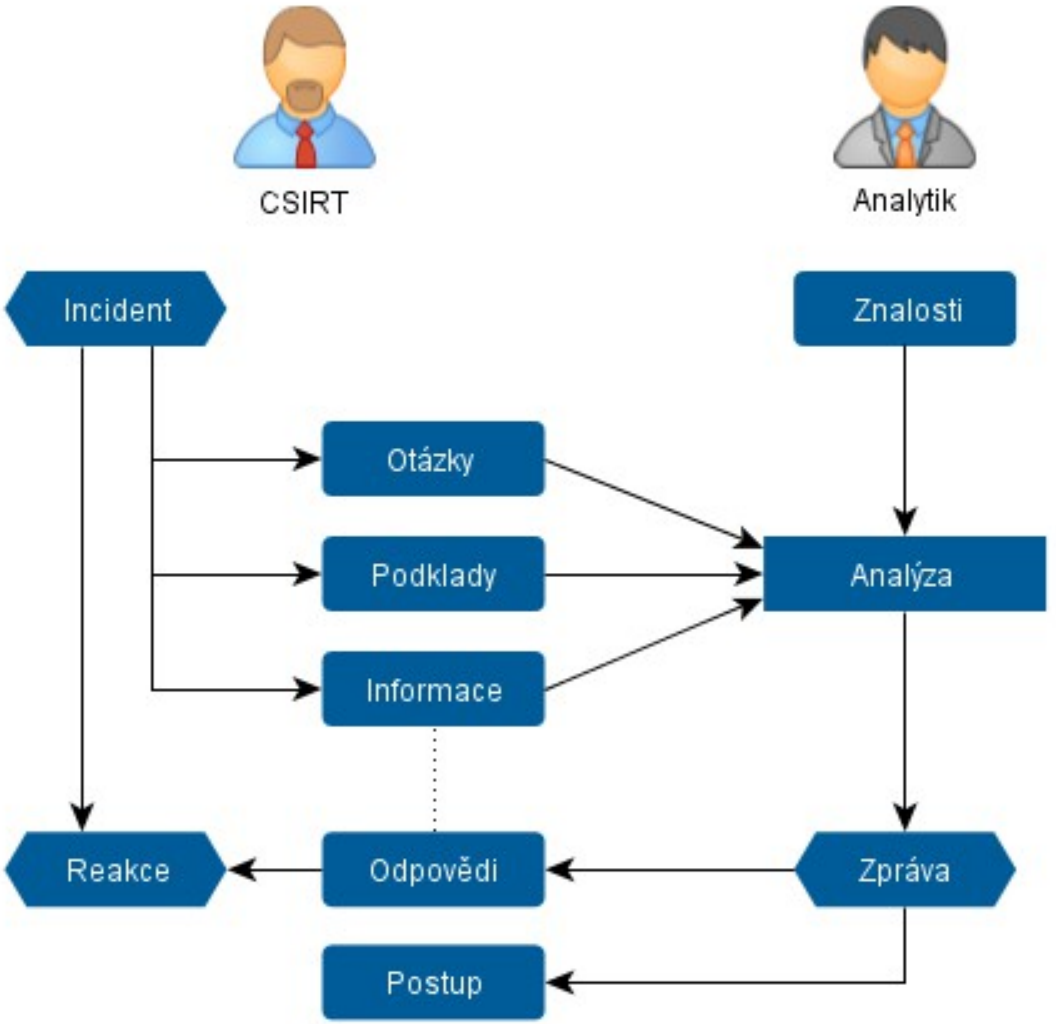


- Potřeba získat informace
  - Podklady pro rozhodování ⇨ přesné a důvěryhodné
  - Detailní (forenzní) analýza

Schéma spolupráce

- CSIRT
  - Incident (problém)
  - Potřeba informací
    - Otázky
  - Umí poskytnout
    - Podklady
    - Informace
- Forenzní analytik
  - Znalosti
  - Analýza

    ⇨ Odpovědi + Postup

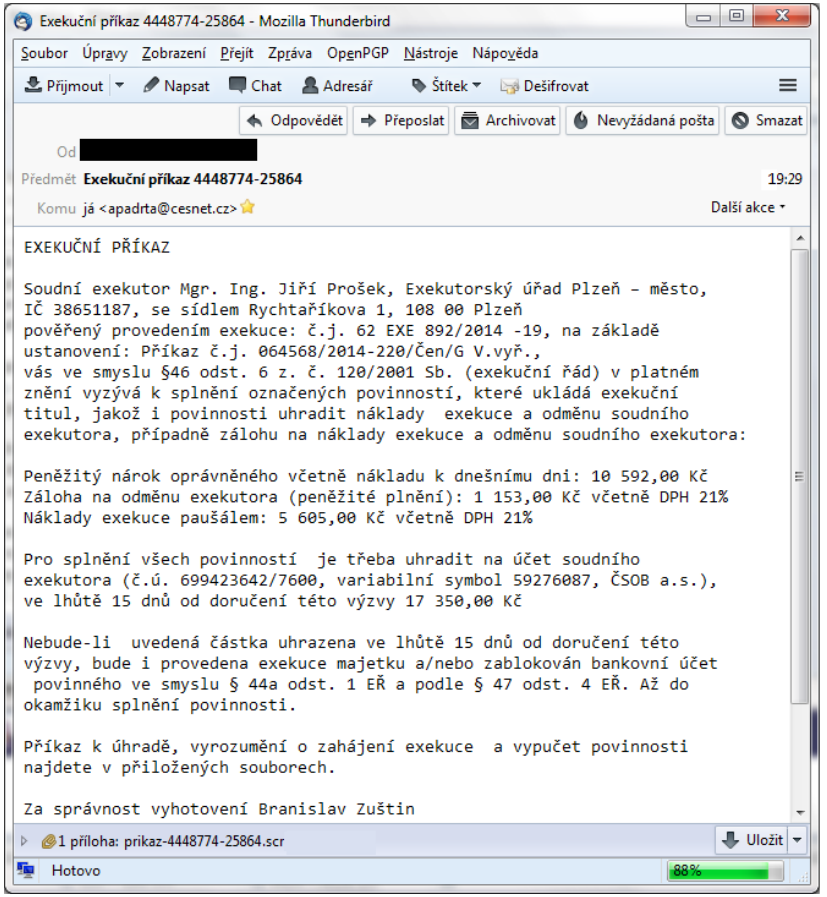


Spolupráce CSIRT – FLAB

Případová studie

Popis situace

- Organizace Cypherfix, a. s.
  - 25 000 uživatelů
  - Vlastní CSIRT tým
- Neděle večer
  - Podvodný e-mail
  - Doručen do 3000+ schránek
  - Různé přílohy <random>.scr
  - Sociální inženýrství
    - Nutí k otevření přílohy



Popis situace

- Pondělí ráno
  - Uživatelé přicházejí do práce
    - Čtou si elektronickou poštu
    - Někteří hlásí podezřelý e-mail …
    - … ale někteří otevírají přílohu
  - Uživatelská podpora kontaktuje CSIRT
  - CSIRT začíná řešit mimořádnou událost
    - Příloha je závadná, téměř na 100% malware
    - Antivirové řešení přílohu nepovažuje za problém
  - Nad Cyberfixem se stahují mračna ...

Reakce na incident

- Plánované kroky – standardní postup
  - Minimalizovat problém
    - Zabránit dalšímu doručování
    - Zabránit dalším kompromitacím
  - Identifikovat „systémy“ k nápravě
    - Najít kompromitované stanice
    - Najít uživatele těchto stanic
  - Podniknout nápravu
    - Vyčistit kompromitované stanice
    - Napravit aktivity kompromitovaných účtů
    - Změna hesel kompromitovaných účtů

Problémy CSIRT

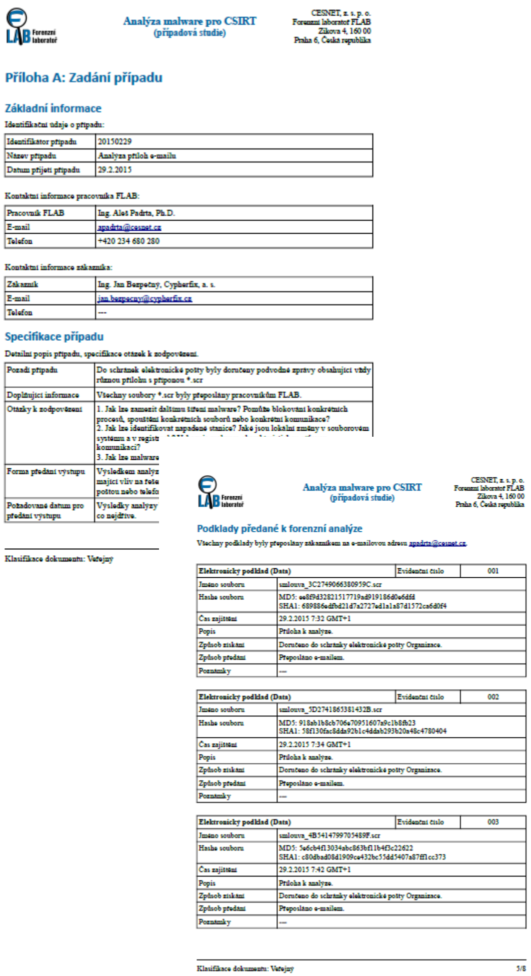
1. **Zabránit dalšímu doručování**
   - Zadáno správci mailového serveru ⇨ Filtrování spustitelných příloh
2. **Zabránit dalším kompromitacím**
   - Jak? AV nepozná, každá příloha jiná … chybí informace
3. **Najít kompromitované stanice**
   - Jak? Jaké jsou příznaky … chybí informace
4. **Vyčistit kompromitované stanice**
   - Jak? Jaké změny se provedou … chybí informace
5. **Najít uživatele kompromitovaných stanic**
   - Logy + seznam stanic ⇨ CSIRT zvládne sám
6. **Napravit aktivity kompromitovaných účtů**
   - Auditní záznamy, změna hesel ⇨ CSIRT vytvoří postup + předá uživ. podpoře

Zadání pro forenzní laboratoř

- CSIRT potřebuje informace
  - Sám nemá kapacitu
    - Malý počet členů
    - Plno práce s řízením incidentu
    - Nemá znalosti – nikdy malware neanalyzoval
  - Kontaktuje forenzní laboratoř
    - Telefonická konzultace
    - Popis mimořádné situace
    - Probrán plán reakce
    - Konkretizace otázek a vytvoření zadání
    - Předání několika vzorků malware

Zadání pro forenzní laboratoř

- Kontaktní údaje
  - abuse@cypherfix.cz, +420 555 ...
- Informace o případu
  - Analýza malware z přílohy e-mailu.
- Otázky
  - Jak lze zamezit dalšímu šíření malware?
  - Jak lze identifikovat napadené stanice?
  - Jak lze malware z napadených stanic odstranit?
- Přebrané důkazy
  - Předané soubory a jejich hashe



Analýza malware pro CSIRT
(případová studie)

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Příloha A: Zadání případu

Základní informace

Identifikační údaje o případu:

Identifikátor případu	20150229
Název případu	Analýza příloh e-mailu
Datum přijetí případu	29.2.2015

Kontaktní informace pracovníka FLAB:

Pracovník FLAB	Ing. Aleš Padrta, Ph.D.
E-mail	apadrta@cesnet.cz
Telefon	+420 234 680 280

Kontaktní informace zákazníka:

Zákazník	Ing. Jan Bezpečný, Cypherfix, a. s.
E-mail	jan.bezpecny@cypherfix.cz
Telefon	---

Specifikace případu

Detailní popis případu, specifikace otázek k zodpovězení.

Pozadí případu	Do schránek elektronické pošty byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr
Doplňující informace	Všechny soubory *.scr byly přeposlány pracovníkům FLAB.
Otázky k zodpovězení	1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace? 2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v regist... komunikaci? 3. Jak lze malware...
Forma předání výstupu	Výsledkem analýz... mající vliv na řeše... poštou nebo telefo...
Požadované datum pro předání výstupu	Výsledky analýzy... co nejdříve.

Klasifikace dokumentu: Veřejný

Analýza malware pro CSIRT
(případová studie)

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Podklady předané k forenzní analýze

Všechny podklady byly přeposlány zákazníkem na e-mailovou adresu apadrta@cesnet.cz.

Elektronický podklad (Data)	Evidenční číslo	001
Jméno souboru	smlouva_3C2749066380959C.scr	
Hashe souboru	MD5: ee8f9d32821517719ad919186d0e6dfd SHA1: 689886edfbd21d7a2727ed1a1a87d1572ca6d0f4	
Čas zajištění	29.2.2015 7:32 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

Elektronický podklad (Data)	Evidenční číslo	002
Jméno souboru	smlouva_5D27418653814 32B.scr	
Hashe souboru	MD5: 918ab1b8cb706e70951607a9c1b8fb23 SHA1: 58f130fac8dda92b1c4ddab293b20a48c4780404	
Čas zajištění	29.2.2015 7:34 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

Elektronický podklad (Data)	Evidenční číslo	003
Jméno souboru	smlouva_4B5414799705489F.scr	
Hashe souboru	MD5: 5e6cb4f13034abc863bf11b4f3c22622 SHA1: c80dbad08d1909ce432bc55dd5407a87ff1cc373	
Čas zajištění	29.2.2015 7:42 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

Klasifikace dokumentu: Veřejný 5/8

Zamyšlení nad analýzou

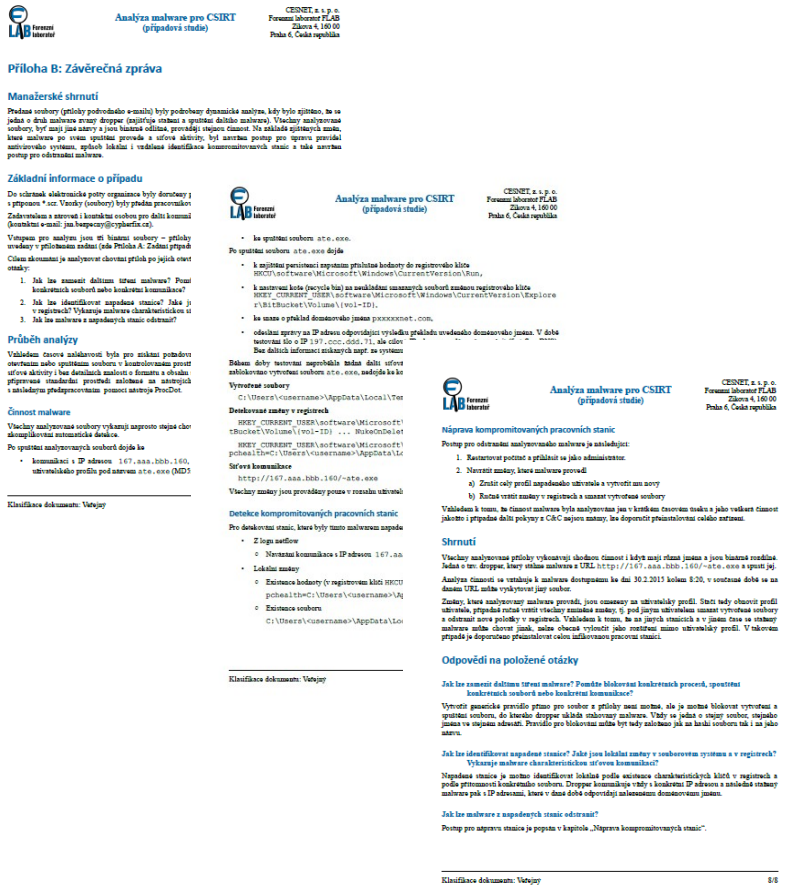
- Během konzultace – rozbor cílů
  - Zamezení dalšího šíření
    - Malware v příloze pokaždé jiný (binárně)
    - Analýza činnosti ⇨ společné aktivity
  - Identifikace napadených stanic
    - Lokálně – změny souborů a registrů
    - Vzdáleně – komunikace s C&C / dropzone
  - Způsob nápravy
    - Jaké změny jsou v systému provedeny
    - Další dopady na bezpečnost (hesla, šifrování dat, …)
  - Výsledky je potřeba rychle – součást reakce na incident

Výsledky analýzy

- Dílčí výsledky
  - +2h od prvního telefonátu
  - Způsob zamezení šíření (ruční úprava pravidel AV)
    - Příloha je dropper – vždy spouští stejný malware
  - Způsob detekce
    - Změny v souborovém systému (nové soubory)
    - Změny v registrech (zajištění persistence)
    - Komunikace s konkrétními IP adresami
- Kompletní výsledky
  - +3h od prvního telefonátu
  - Způsob odstranění: User-profile malware – návod k odstranění

Výsledky analýzy

- Závěrečná zpráva
  - Manažerské shrnutí
  - Zadání
  - Průběh analýzy
    - Použité prostředí
    - Dosažené výsledky
    - Zhodnocení
  - Shrnutí
  - Odpovědi na otázky



Analýza malware pro CSIRT (případová studie)

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Příloha B: Závěrečná zpráva

Manažerské shrnutí

Základní informace o případu

Průběh analýzy

Činnost malware

Klasifikace dokumentu: Veřejný

Analýza malware pro CSIRT (případová studie)

Detekce kompromitovaných pracovních stanic

Klasifikace dokumentu: Veřejný

Analýza malware pro CSIRT (případová studie)

Náprava kompromitovaných pracovních stanic

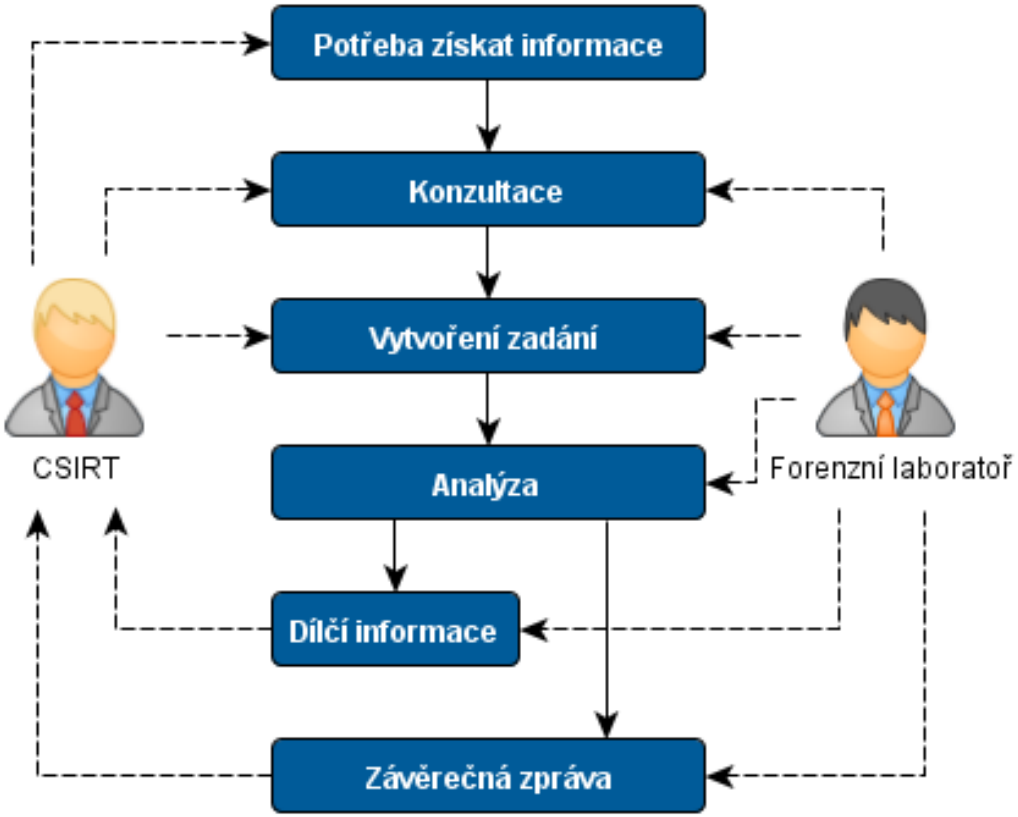
Shrnutí

Odpovědi na položené otázky

Klasifikace dokumentu: Veřejný 8/8

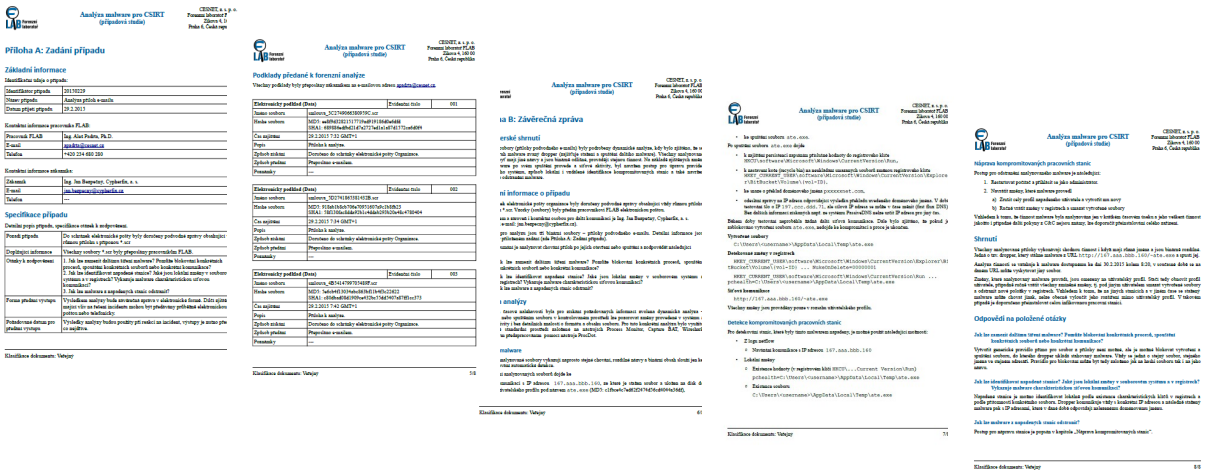
Shrnutí

- Forenzní laboratoř
  - Podpora při reakci na incident
  - Dodání informací
- CSIRT
  - Poskytne podklady
  - Zadá otázky
  - Dostane výsledky
    - Průběžně - dílčí výsledky
    - Závěrečná zpráva



URL pro případovou studii

- Odkaz z http://flab.cesnet.cz
- Přímé URL https://flab.cesnet.cz/_media/cs/sluzby/case_study-analyza_malware.pdf



Děkuji za pozornost