

Přínos forezní laboratoře při řešení rozsáhlého bezpečnostního incidentu

Karel Nykles

Vážený zákazníku

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.

Dovolujeme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve výši #9941494110998527 8446.57 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 14.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #3C2749066380959C umožňuje Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 8446.57 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_3C2749066380959C.zip"

S pozdravem,

Vedoucí odboru vymahání pohledávek

Alena Malinovská

+420 603 707 347

Rozbor použitých zranitelností

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.

Dovolujeme Vás upozornit, že k 25.04.2014
dlužné částky na osobní účet ve výši
#9941494110998527 8446.57 Kč.

Nabízíme vám dobrovolně uhradit
pohledávku v plné výši do 14.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy
#3C2749066380959C umožňuje Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků
a jiných soudních nákladů.

Formální oslovení.

Připomenutí „dluhu.“

Nabídka vyrovnání.

Smířčí varianta.

Rozbor použitých zranitelností

V případě prodlení uhrady pohledávky 8446.57 Kč
v souladu s platnými právními předpisy,
jsme oprávněni zahájit **právní sankci** na základe pohledávky.

Hrozba.

Kopie smlouvy a platební údaje jsou připojeny
k tomuto dopisu jako soubor
"**smlouva_3C2749066380959C.zip**"

Návnada.

S pozdravem,
Vedoucí odboru vymahání pohledávek
Alena Malinovská
+420 603 707 347

Iluze legitimacy.

Indikátory podvodu

využívali produktu z naší banky.

Dovolujeme Vás upozornit
dlužné částky na osobní účet ve **vysí**
Nabízíme vám dobrovolně uhradit
pohledávku v plné výši do 14.05.2014.

Překlepy, stylistika.

#9941494110998527
8446.57 Kč.
#3C2749066380959C

Čísla.

Název

Typ

Obsah souboru



smlouva_14.02.2013-signed_A21...

Aplikace

Zajímavosti

využívali produktu z naší banky.

Dovolujeme Vás upozornit
dlužné částky na osobní účet ve **vysí**
Nabízíme vám dobrovolně uhradit
pohledávku v plné výši do 14.05.2014.

8446.57 Kč.



smlouva_3
C27490663
80959C.zip



smlouva_1
4.02.2013-s
igned_A21
79423018...

Český formát data.
Špatná čeština?

Anglický oddělovač desetinných
míst, správné označení koruny.

Ikona! Program na
tvorbu ikony znal „č“.
Není vidět přípona

Uživatel

Rozbalení ZIP archivu.

Obsažen soubor smlouva.

Otevření souboru.

Zobrazení smlouvy.

Smlouva se mě netýká, asi nějaký omyl.

Zavření souboru.

Návrat k původní činnosti.

Malware

Spuštěn **EXE** soubor.

Vybalen RTF dokument obsahující smlovu.

Zobrazena smlouva ve Wordpadu.

Vytvořen soubor **ATE.EXE** v **%USERPROFILE%**.

Soubor zapsán do

HKCU\Software\Microsoft\Windows\CurrentVersion\run
ATE.EXE běží

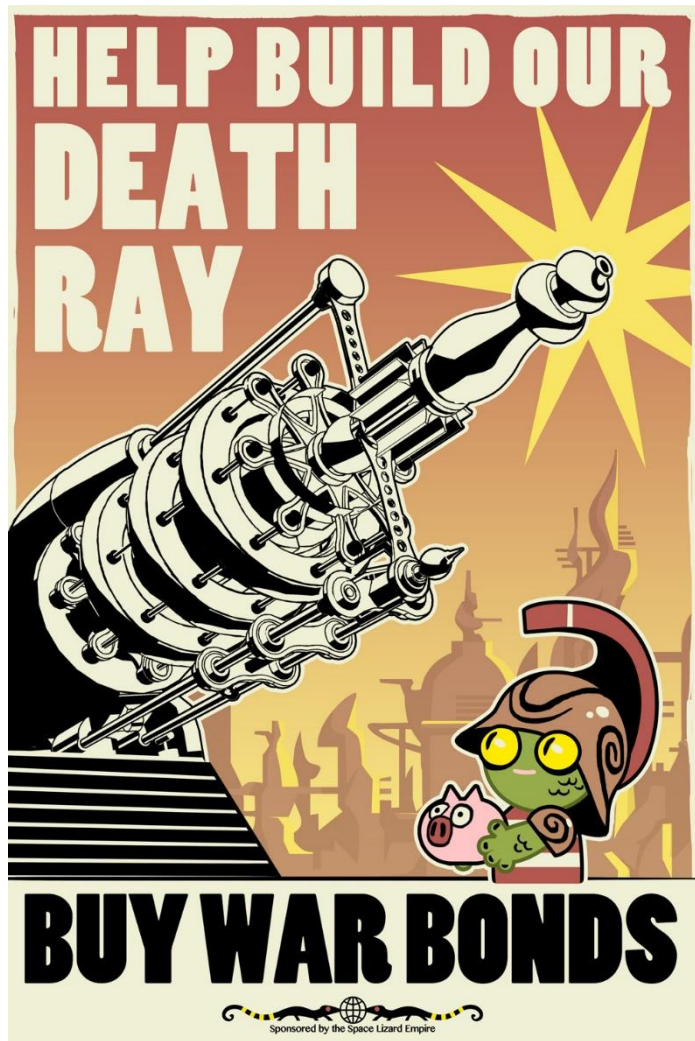
DNS dotaz na „validní doménu“

Timeout

DNS dotaz na **picapicanet.com** (IP @ **OVH.NET**)

Reakce AV řešení

Lovec virů, deathray.vbs



Autostart procesu z %USERPROFILE%?

Běží proces?

- > #Ukonči proces.
- > #Přesuň binárku do jiné lokace.
- > #Smaž referenci z AUTOSTART.
- > Zapiš informace do těla mailu.
- > Zazipuj logy #a binárku.
- > Odešli #binárku a logy mailem.

© <http://www.gabo.ca/product/death-ray-12in-x-18in-silk-screen-poster/>

Popis situace

Jednoho krásného nedělního večera...

...v nejmenované instituci na západ od Prahy.

Uživatelé začnou dostávat e-maily informující o dluhu.

Support zaměstnán plánovanou výměnou HW.

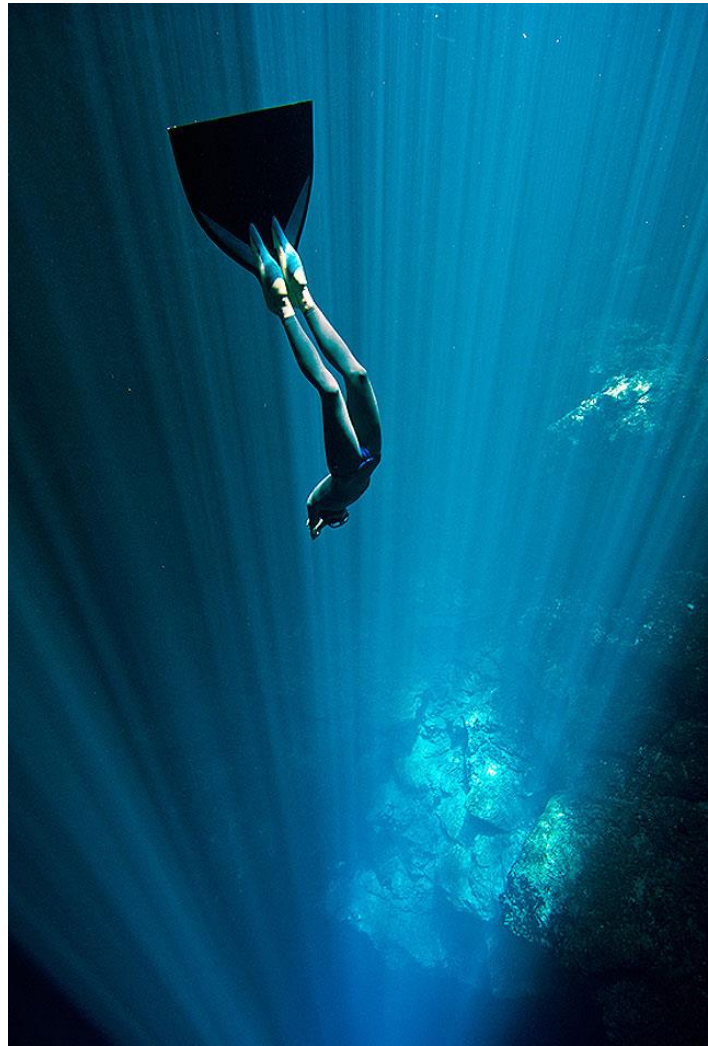
Antivirové řešení nic nedetekuje, z počátku mlčí i VirusTotal!?

Polovina bezpečáků na konferenci.

Uživatelé malware vesele spouštějí...

...a zatím nikdo nic netuší.

Tak se do toho ponoříme...



© <http://resources.news.com.au/files/2013/03/01/1226588/495108-christina-saenz-de-santamaria.jpg>

Odhalení incidentu

Jak detekujeme, že došlo k incidentu?

Jsme mezi zasaženými.

Uživatelé si stěžují.

Máme vlastní nástroj, který anomálii zachytí.

AV software nás časem informuje.

IDS ...

Informuje nás cizí CSIRT.

Něco se děje...

Situace

Pondělí ráno:

Deathray hlásí podezřelé *exe* u více uživatelů.

Znalejší uživatelé oznamují phishing na HelpDesk.

Nevíme, kolik PC/uživatelů je kompromitováno.

Mezi kompromitovanými je i několik „überuserů“.

Nevíme, co malware dělá.

Situace je nepřehledná...zavoláme WIRT.

WIRT – první kroky

Pondělí kolem poledne:

Rozdělení sil, mezi školení a incident.

Získat co nejvíc dat, co nejrychleji to jde.

Odjistit deathray – odkomentovat likvidační kód.

Informovat ostatní uživatele

Získat vzorky malware.

Koordinovat kroky supportu, správců a uživatelů.

Spolupracovat s dalšími CSIRT týmy

Problém bobtná, co na to CESNET-CERTS?

Akce:

Sdílet informaci o útoku.

Získat globální pohled na situaci.

Získat další informace od ostatních CSIRT týmů.

Připravit se na monitoring a koordinaci postupů.

Sbírat a sdílet veškeré dostupné informace.

Aktivovat forenzní laboratoř FLAB, zaslat data.

FLAB je v pohotovosti

Úkoly pro forenzní laboratoř

Rozsah útoku, byl cílený?

Definovat indikátory pro nalezení kompromitovaných:

počítačů, účtů, služeb, dat.

Zajištění

Najít způsob, jak zabránit malware ve spuštění.

Odstranění

Zjistit, jak vyčistit kompromitované:

počítače, účty, služby, data.

Sepsat zprávu, formulovat doporučení pro příště.

Vstupy:

Vzorky neznámého kódu.

Útok zasáhl téměř celou republiku

Detekce na VirusTotal 3 z 5, AV řešení jsou slepá.

Potřebujete **odpovědi** a to **rychle**.

Udržovat kontakt s a informovat nadřazený CSIRT

Vzorek mailu:

Vážený zákazníku,

Jsme velmi rádi, že jste vyuzívali produktu z naší banky.
Dovolujeme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve výši
#9941494110998527 8446.57 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do
14.05.2014.

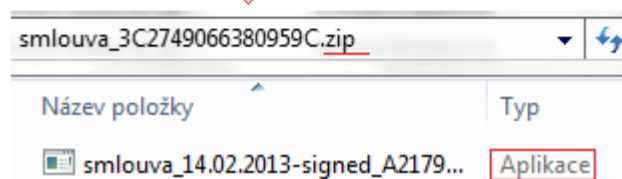
Dobrovolné uhrazení pohledávky a dodržení smlouvy #3C2749066380959C umožňuje Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 8446.57 Kč v souladu s platnými právními předpisy,
jsme oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor
"smlouva_3C2749066380959C.zip"

S pozdravem,
Vedoucí odboru vymahání pohledávek
Alena Malinovská
+420 603 707 347



Náhled přílohy ve Windows

Dynamická Analýza

Jak se malware chová

Příprava VM

ProcessMonitor

Wireshark

CaptureBat

Procdot - Christian Wojner, CERT.at

Spuštění ve VM

Monitoring sítě – Wireshark, CaptureBat

Monitoring registrů – Procmon, RegShot

Monitoring filesystému – CaptureBat, Procmon

Analýza dat

Regshot - Compare

CaptureBat – zaznamená smazané soubory

Wireshark – Co máme v pcapu

ProcDot – to nejlepší nakonec!

Process monitor

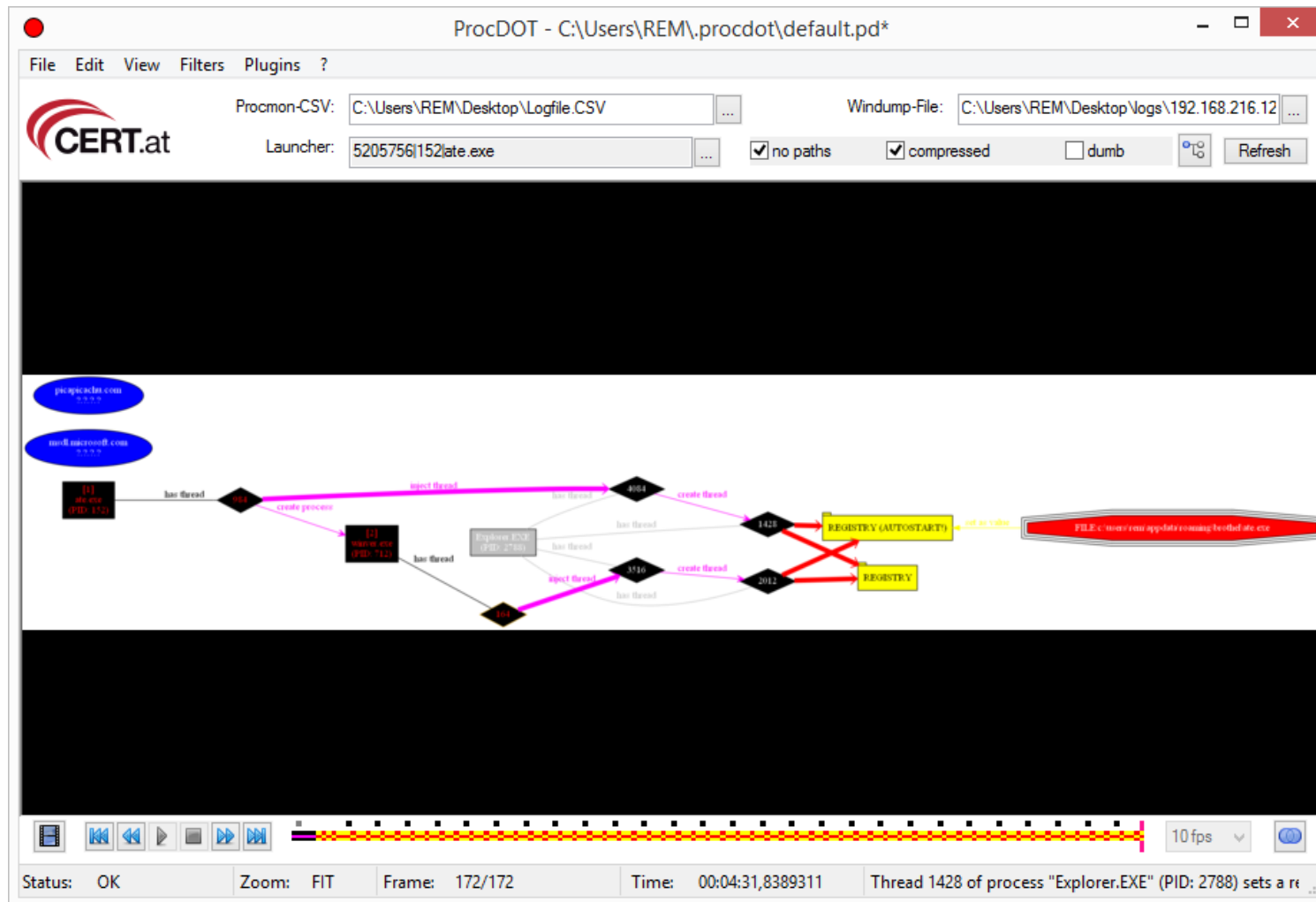
Process Monitor - C:\Program Files\Process Monitor\procmon_event_data.pml

Time ...	Process Name	PID	Operation	Path	Result	Detail	TID
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows\explorer.exe	NAME INVALID	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows	IS DIRECTORY	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	FileSystemControl	C:\Windows	NOT REPARSE P...	Control: FSCTL_G...	4796
4:44:2...	svchost.exe	1112	CloseFile	C:\Windows	SUCCESS		4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	CloseFile	C:\Windows	SUCCESS		4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	DeviceIoControl	C:\Windows	INVALID PARAME...	Control: IOCTL_M...	4796
4:44:2...	svchost.exe	1112	CloseFile	C:\Windows	SUCCESS		4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	FileSystemControl	C:\Windows	NOT REPARSE P...	Control: FSCTL_G...	4796
4:44:2...	svchost.exe	1112	CloseFile	C:\Windows	SUCCESS		4796
4:44:2...	svchost.exe	1112	RegOpenKey	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	RegOpenKey	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows\explorer.exe	SUCCESS	Desired Access: R...	4796
4:44:2...	svchost.exe	1112	QueryNetwork...	C:\Windows\explorer.exe	SUCCESS	CreationTime: 11/1...	4796
4:44:2...	svchost.exe	1112	CloseFile	C:\Windows\explorer.exe	SUCCESS		4796
4:44:2...	svchost.exe	1112	RegQueryValue	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	SUCCESS	Type: REG_QWO...	4796
4:44:2...	svchost.exe	1112	RegCloseKey	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	SUCCESS		4796
4:44:2...	svchost.exe	1112	RegQueryValue	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	NAME NOT FOUND	Length: 144	4796
4:44:2...	svchost.exe	1112	RegCloseKey	\REGISTRY\A\{AB4CC77E-3254-86C4-C354-7695F7523AB...	SUCCESS		4796
4:44:2...	svchost.exe	1112	CreateFile	C:\Windows\WinSxS\FileMaps\\$\$cdf-ms	SUCCESS	Desired Access: G...	4796
4:44:2...	svchost.exe	1112	ReadFile	C:\Windows\WinSxS\FileMaps\\$\$cdf-ms	SUCCESS	Offset: 0, Length: 8...	4796
4:44:2...	svchost.exe	1112	ReadFile	C:\Windows\WinSxS\FileMaps\\$\$cdf-ms	SUCCESS	Offset: 336, Length...	4796
4:44:2...	svchost.exe	1112	ReadFile	C:\Windows\WinSxS\FileMaps\\$\$cdf-ms	SUCCESS	Offset: 84, Length...	4796

Showing 49,790 of 125,924 events (39%) Backed by C:\Program Files\Process Monitor\procmon_event_data.pml

Monitorovací nástroj od SysInternals

Procdot



Grafická vizualizace dat z ProcMonu a WireSharku, Christian Wojner, CERT.at

The diagram illustrates the execution flow of a malware sample, showing the relationship between processes, threads, and registry operations.

Processes and Threads:

- [1] ate.exe (PID: 152)** (Black box) has a thread **984** (Black diamond).
- 984** creates process **[2] winver.exe (PID: 712)** (Black box).
- 984** injects a thread into process **4084** (Black diamond).
- Explorer.EXE (PID: 2788)** (Grey box) has threads **164** (Black diamond) and **3516** (Black diamond).
- 164** injects a thread into process **3516**.

Registry Operations:

- Threads **1428** (Black diamond) and **2012** (Black diamond) create threads (indicated by pink arrows labeled "create thread").
- Thread **1428** interacts with **REGISTRY (AUTOSTART!)** (Yellow box) and **REGISTRY** (Yellow box).
- Thread **2012** interacts with **REGISTRY (AUTOSTART!)** and **REGISTRY**.
- The file path **FILE:c:\users\rem\appdata\roaming\brothel\ate.exe** (Red box) is set as a value in **REGISTRY (AUTOSTART!)** (indicated by a yellow arrow labeled "set as value").

První výsledky analýzy

DNS jméno C2C

Picapicachu.com -> IP @ OVH.net

Picapicanet.com - fallback

Detekce, blokace

IP lze sledovat přes *PassiveDNS*

Persistence

Registrový klíč, HKCU

Hlídací vlákna – injektované do procesu

Původní proces lze zabít!

Sdílet zjištěné informace dál!

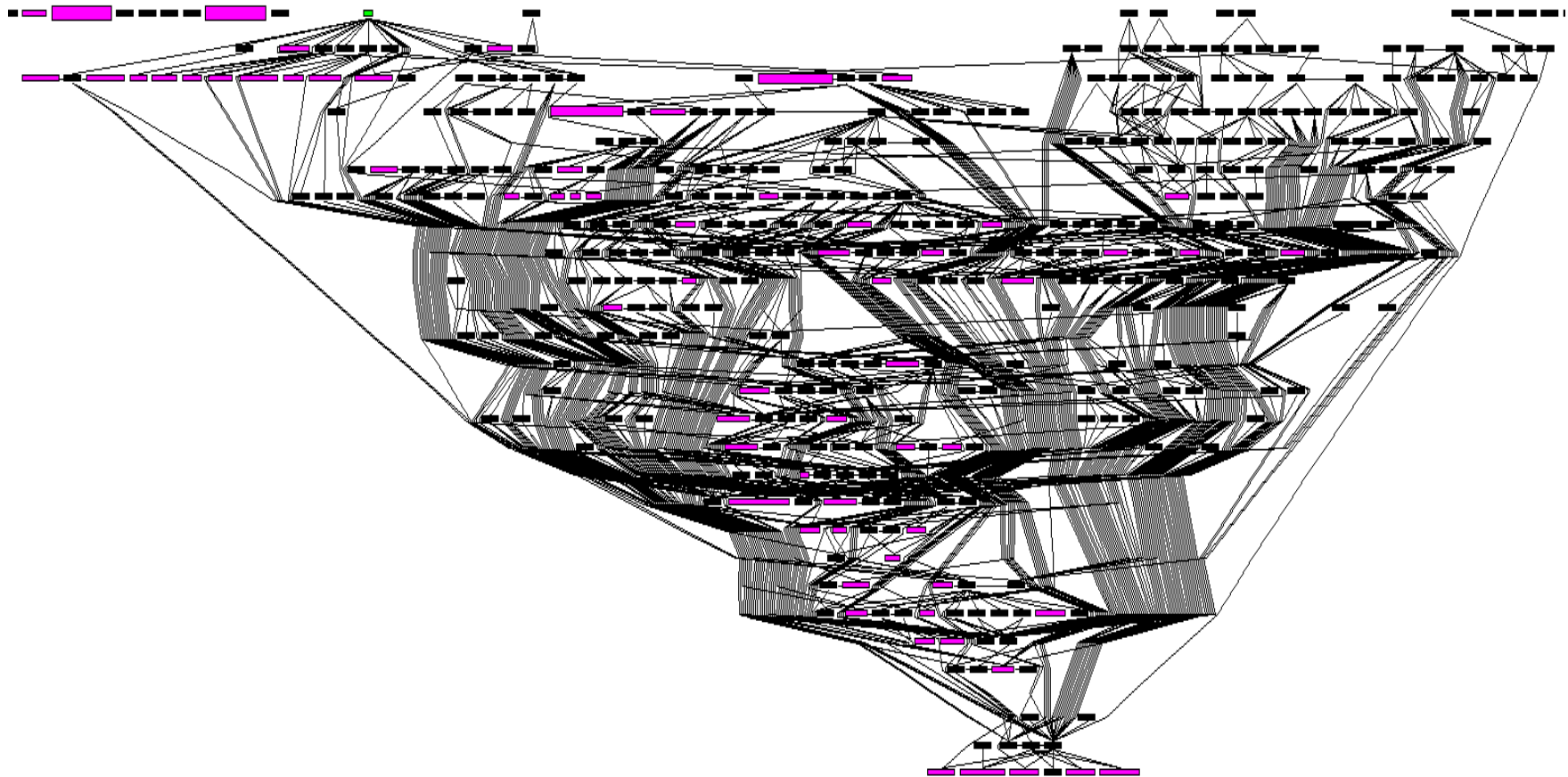
Závadná IP a doména – monitoring, kontakt abuse

Registrový klíč – shodný pro různé instalace!



©<http://38ccda.medialib.glogster.com/media/2db6ccd809d557ab0f5b27a6ae243400134ec7ae1364e5744c5d5814be1d002/pikachu-cat.jpg>

Reverzní analýza_



Distribuce detekčních pravidel

- Soubory a složky
- Registrové klíče
- Závadné IP/domény

Monitoring provozu na závadné adresy

- Informování napadených sítí/uživatelů

Technická podpora

- Pro organizace bez odpovídajícího technického zázemí.

Aplikace detekčních pravidel do managementu stanic

Detekování složek a souborů, klíčů v registrech.

Logy z Deathray

Kontrola komunikace se závadnými IP.

Blokace PC mimo management (Except for DNS server! :-)

Přesun do karanténí sítě.

Sdílený sešit se seznamem napadených strojů a jejich stavem

Jednotlivé stroje pak řešit v tiketovacím systému.

Definovat postup pro support

Jednoduchý, rychlý, efektivní.

Instrukce:

Malware vzdáleně zlikvidovat (viditelné části)

Smazat persistenci a binárky

Informovat uživatele

Dohodnout a připravit na reinstalaci.

Přeinstalovat počítač

Vygenerovat nový profil.

Změnit uživatelská hesla.

Vyškolit uživatele!

Druhá vlna phishingu

T+7 dní:

Malware v druhé vlně je složitější

Zpráva je téměř stejná, podle stejné šablony.

V AV je jednoduché pravidlo na blokaci malware

Brání rozbalení exe ze zazipované přílohy

Deathray je stále aktivní

Likviduje persistenci malware

Co na to uživatelé?

Co na to AV skener?

Reakce AV skeneru, týden po

Proč AV nefunguje?

Proč *náš* AV nedetekuje tento malware?

Detekční signatury jsou závislé na dodavateli AV.

Poměr velikosti výrobce AV ku rozsahu útoku = pravděpodobnost úspěchu.

Cílenému útoku se nelze ubránit

Po týdnu jsme získali extra definice pro minulou vlnu.

Jak si s AV poradit?

Být připraven

Nezávislý primitivní nástroj.

Použít všech možností AV řešení – blokace rozbalení přílohy.

Okamžitě po detekci kontaktujte dodavatele/výrobce AV se vzorky.

Sledujte, co se děje okolo, hledejte novinky a anomálie

Twitter, SANS, stížnosti uživatelů.

Připravit si kanál pro informování uživatelů.

Pohled uživatele

Proč by vůbec uživatelé takovou přílohu otvírali?

Je česky.

Vypadá zmatečně, ale na druhý pohled už zase ne tolik, zmate.

Nežádá o přístupové údaje, na to jsou uživatelé již zvyklí.

Pokročilejší soubor zkonstolovali pomocí AV s výsledkem.

Nezaplacená faktura, komu se to ještě nestalo?

Zkontrolujte přílohu, nebo přijdou právníci.

Psychologie útoku

Kdo je v organizaci nejzranitelnější pro takový útok?

Netechnický management – dluh se dostal ke mně = průšvih!

Ekonomické oddělení - kdo si zase co objednal?

Koleje – řeší dluhy dnes a denně.

Zvědavci – „Asi to je virus, ale tak mám AV, tak to bude v pohodě.” Nebylo.

Přetížení zaměstnanci – “TL;DR, rovnou se podívám na přílohu.”

Dunning-Kruger pozitivní uživatelé. (Otevřeli druhou vlnu i přes poučení)

„Nikdo mi neřekl, že je to závadná příloha!”

Výsledky - FLAB

Rozsah

Několik C2C serverů, rozšířený útok.

Indikátory: registry, síťový provoz, soubory a složky

Zajištění

Karanténní síť

Manuální pravidla pro AV a FW

Informování uživatele

Odstranění nákazy

PC Dat Hesel Profilu

Reinstall / obnova / reset / znovuvytvoření

Závěrečná zpráva s doporučením

Blokování příloh, AV pravidla, rychlejší komunikace s uživateli

Výsledky - Organizace

~120 kompromitovaných pracovních stanic

Nalezeno díky zprávě FLAB a sdílení adres C2C serverů mezi CSIRTy

~20 pracovních stanic kompromitováno ve druhé vlně.

2 dva uživatelé se chytili opakovaně ☹

~120 hodin (pouze) práce na obnově prostředí

Přeinstalace OS.

Reset všech hesel.

Znovuvytvoření uživatelského profilu.

Pozitivní přínos

Máme postupy pro podobné situace.

Support má připraven kanál pro informování uživatelů.

Šablony pravidel pro blokaci malware v AV

Deathray jede naostro

Spustitelný kód v přílohách e-mailů je blokován.

Přibližně 120 uživatelů absolvovalo reálné bezpečnostní školení na téma práce s internetem, nezapomenou.

Se zprávou z FLABu

Náhled do detailů incidentu.

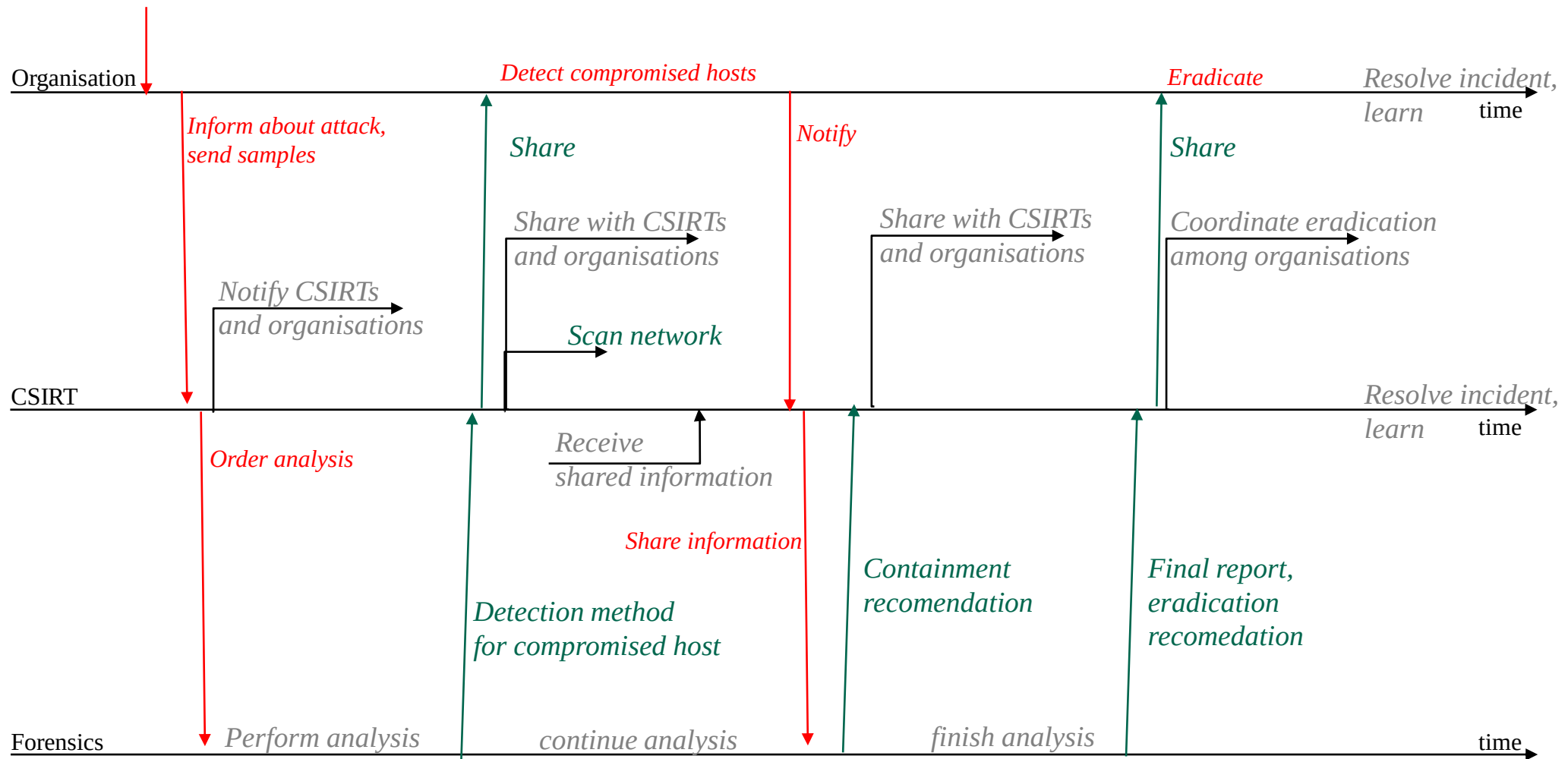
Plynulá koordinace.

Čas na přípravu protiopatření.

Odpovědi uživatelům či zákazníkům se mají oč opřít.

Průběh spolupráce

Došlo k incidentu



Bonus – malware v akci

Kompromitovaný FB profil:

+ Nová zpráva Akce 🔍

Ahoj jsi tu??potřebovala bych pomoc 2014/05/30 10:30 dopol.

Dobrý den slečno Kozo 😊 2014/05/30 10:31 dopol.
Ptej se

Nezaplatíš mi přes kartu prosímte 50 Kč ? v hotovosti ti dám
klidně 200 potřebuju si dobit fortuna ja na karte nemam ani
korunu jinak bych si to poslala sama 2014/05/30 10:31 dopol.

No problem 😊 2014/05/30 10:31 dopol.
dávej instrukce

http://gopay.mzf.cz/gw_gpo_lts2.html tady to vyplň a dej tam
částku 50kč a platnost karty máš na přední straně a ověřovací
kód na zadní straně u podpisu 2014/05/30 10:32 dopol.

Platební brána GoPay

Joo, už tomu rozumím, tím jakože pošlu peníze rovnou tobě na
účet ano? 2014/05/30 10:33 dopol.
mi to přišlo nějaký divný 😊

ano 2014/05/30 10:33 dopol.

ok, chceš tam jen 50, nemám ti tam dát víc, ať máš nějakou
rezervu? 2014/05/30 10:34 dopol.

nene stací 50 😊 2014/05/30 10:34 dopol.

ok 2014/05/30 10:34 dopol.
hele, kde jsi vzala ten formulář?
mě se nezdá

z banky 2014/05/30 10:37 dopol.

hmm, jako fakt se mi to nezdá 2014/05/30 10:38 dopol.
a to bezesrandy
není to důvěryhodný
není to šifrovaný

jako vyplnil jsem to
odeslal
a nic
a řekl bych, že si nechám zablokovat kartu

jak to? nic??74 2014/05/30 10:38 dopol.

ne, nic 2014/05/30 10:38 dopol.
vyhodilo to dost divnou neprofesionální hlášku
rozsypaný čaj

nemusíš se bát je to bezpečný 2014/05/30 10:40 dopol.
podívám se jestli to dorazilo

Exploitovaná zranitelnost
Sociální inženýrství

Cíl útoku
Peníze
Přístupové údaje

Výsledky
Spolupráce
Rychlost reakcí
Poučení uživatelů
Spolupracující uživatel je nejlepší detektor!

*V roce 2011 založeno jako projekt CESNETu, za účelem
poskytovat forenzní kapacity pro členy sítě CESNET2.*

Otázky

?

Děkuji za pozornost!