CESNET
FLAB

Ransomware PČR

zaplaťte a bude vám odpuštěno

Aleš Padrta

Karel Nykles

Obsah

- Ransomware
  - Definice pojmu
- Ransomware PČR
  - Jak vypadá
  - Psychologické aspekty
  - Analýza vnitřního fungování
  - Výskyt na ZČU
  - Odstranění z PC

Ransomware

- Ransomware = ransom + software
  - Ransom = výkupné
  - Podmnožina malware
- Princip
  - Omezení uživatele
    - Funkčnost PC
    - Přístup k datům
    - ...
  - Obnova po splnění požadavků
- Bezpečnostní incident – kompromitace počítače

Ransomware PČR

- Simulace „pokuty“ od policie
  - Několik národních variant
    - Police ČR
    - New Scottland Yard
    - Gendarmerie Nationale
    - ...
  - Verze s Europolem a Interpolem
  - Uzamčení počítače
  - Odblokování po zaplacení „pokuty“
- První masivní výskyt ransomware
  - Organizátory prý už zatkli
  - Může být stále aktivní

ČESKÁ REPUBLIKA POLICIE
ÚSTAV POČÍTAČOVÉ TRESTNÉ ČINNOSTI

Chcete-li odblokovat Váš počítač a vyhnout se trestnímu stíhání, musíte provést platbu ve výši 2000 Kč.

Všechny operace prováděné na tomto počítači se zaznamenávají.
Pokud používáte webovou kameru, video a fotografie se ukládají pro účely identifikace.

Videozáznam: **ON**

Můžete být snadno identifikován pomocí IP adresy Vašeho počítače a s ní spojeného doménového jména.

Vaše IP adresa: [redacted]
Doménové jméno: [redacted]
Místo: [redacted]

Váš počítač byl uzamčen!

Provoz Vašeho počítače je pozastaven z důvodu podezření z neoprávněné činnosti.

Níže jsou uvedené možné narušení, které jste provedl:

Článek 274 - Autorské právo
Pokuta nebo trest odnětí svobody na dobu až 4 let
(Použití nebo sdílení souborů chráněných autorskými právy - filmy, software)

Článek 183 - Pornografická produkce
Pokuta nebo trest odnětí svobody až na 2 roky
(Použití nebo sdílení pornografických souborů)

Článek 184 - Zneužití dítěte (do 18 let) k výrobě pornografie
Trest odnětí svobody až na 15 let
(Použití nebo sdílení pornografických souborů)

Článek 104 - Propagace terorismu
Trest odnětí svobody až na 25 let
(Navštěvovali jste webové stránky teroristických organizací)

Článek 297 - Nesprávné použití počítače, které vede ke vzniku vážné škody
Pokuta nebo trest odnětí svobody až na 2 roky
(Váš počítač je infikován virem, který následně infikoval další počítače)

Článek 108 – Hazardní hry
Pokuta nebo trest odnětí svobody až na 2 roky
(Hráli jste hazardní hry, které jsou zákonem zakázané ve Vaší zemi)

V souvislosti s rozhodnutím Vlády ze dne 22. srpna, všechny tyto trestné činy mohou vést k podmíněnému trestu po zaplacení pokuty.

Výše pokuty je 2000 Kč. Platba musí být provedena do 48 hodin po objevení narušení. Pokud udělená pokuta nebude zaplacena, automaticky bude zahájeno trestné stíhání.

Po zaplacení pokuty Váš počítač bude odblokován.

Ukash

Ukash je k dostání online, e-peněženkách, trafikách a bankomatech po celém světě.

Vyměňte peníze za Ukash kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód: [ ]

1 2 3 4 5 6 7 8 9 0

Předložit

Kde lze koupit Ukash

e-va electronic value
Alles prepaid!

paysafecard

Paysafecard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech.

Vyměňte peníze za Paysafecard kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód: [ ]

1 2 3 4 5 6 7 8 9 0

Předložit

Kde lze koupit Paysafecard

Tipsport
OMV
žabka
Eni
Shell

Vezměte prosím na vědomí, že pokuta musí být zaplacena do 48 hodin. Pokud se Vám nepodaří provést platbu ve stanovené lhůtě, odblokování Vašeho počítače nebude možné.

V tomto případě proti Vám automaticky bude zahájeno trestní řízení.

100%

Psychologické aspekty

- Moc autority
  - Policejní „akce“
  - Obvinění z „neoprávněné činnosti“
  - Hrozba trestním stíháním
- Pocit identifikovatelnosti
  - Kamera
  - IP adresa
  - Lokalizační údaje
- Časový nátlak
  - Zaplaťte pokutu do 48 hodin

Psychologické aspekty

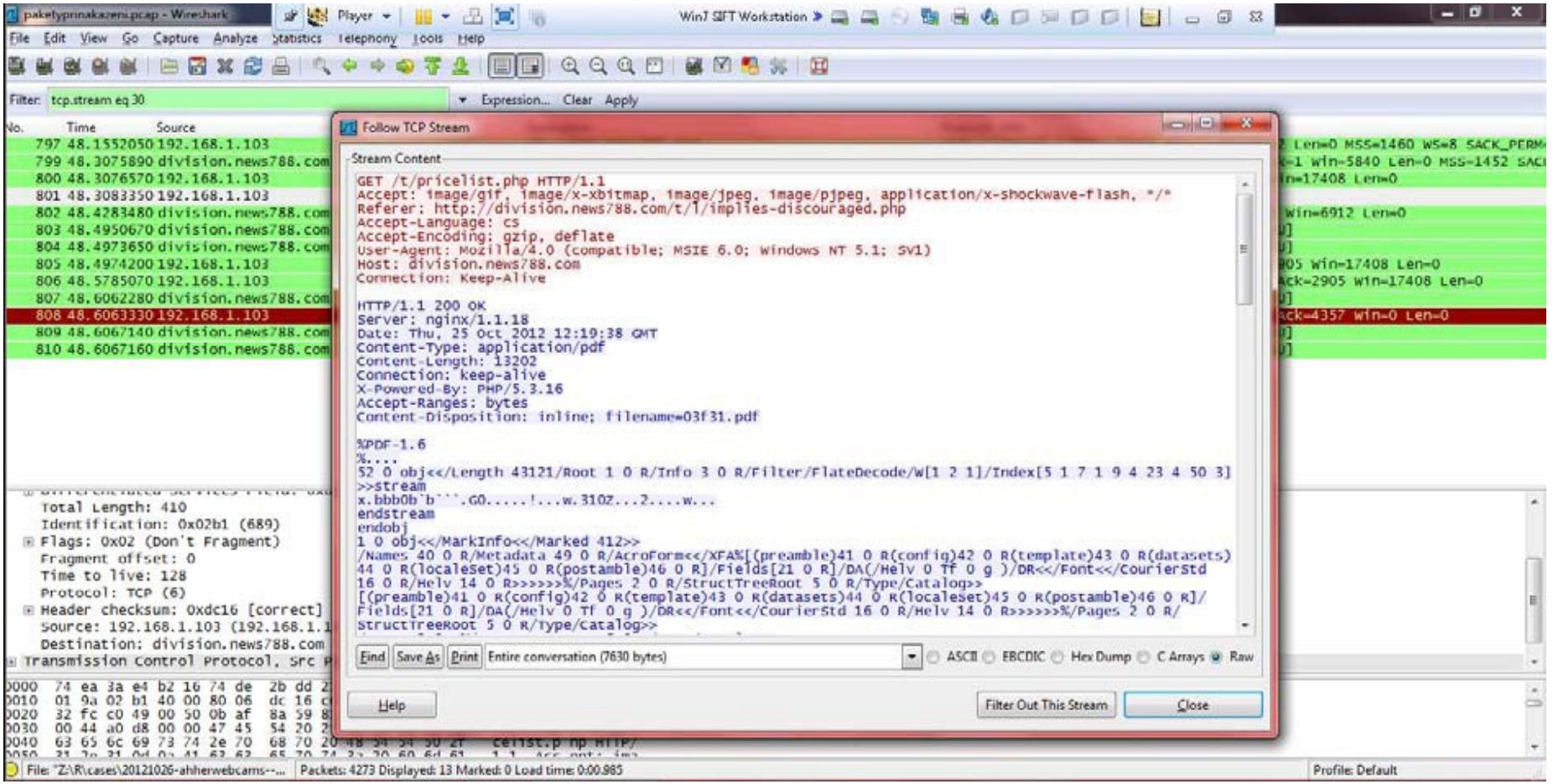
- Omezená možnost výběru
  - Počítač nepoužitelný
  - Neumím sám opravit
  - Zaplatit nebo dát „do servisu“?
- Proč radši zaplatit?
  - Do háje! Ví co dělám!
  - Nákaza na „nestandardních stránkách“
    - Snaha utajit tuto činnost (manželka, zaměstnavatel)
  - Třeba je to opravdu od PČR
    - Nechci k soudu, do vězení, ...
  - 2000,- Kč je „rozumná“ částka

Analýza vnitřního fungování

- Rozbor
  - Forenzní laboratoř (R.Bodó, K.Nykles, A.Padrta)
- Otázky
  - Jak se malware dostane do systému?
  - Jaké změny tam provede?
  - Jaká data sbírá a odesílá?
  - S jakými C&C komunikuje?
- Podklady k analýze
  - Obrazy disků napadených stanic
  - Obraz paměti
  - Odchycená síťová komunikace

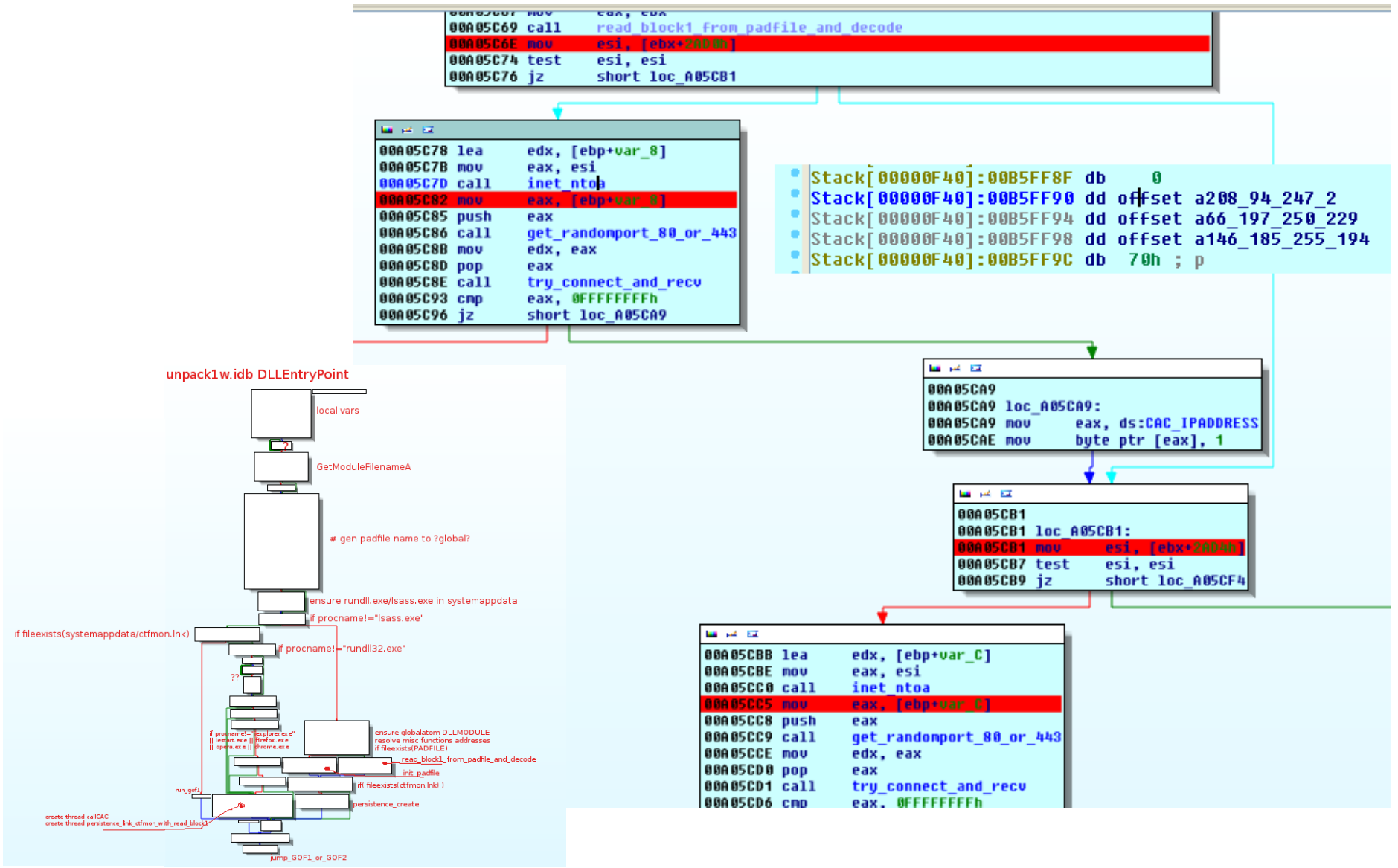
Analýza vnitřního fungování

- Pozorování vnějších projevů
- Analýza komunikace



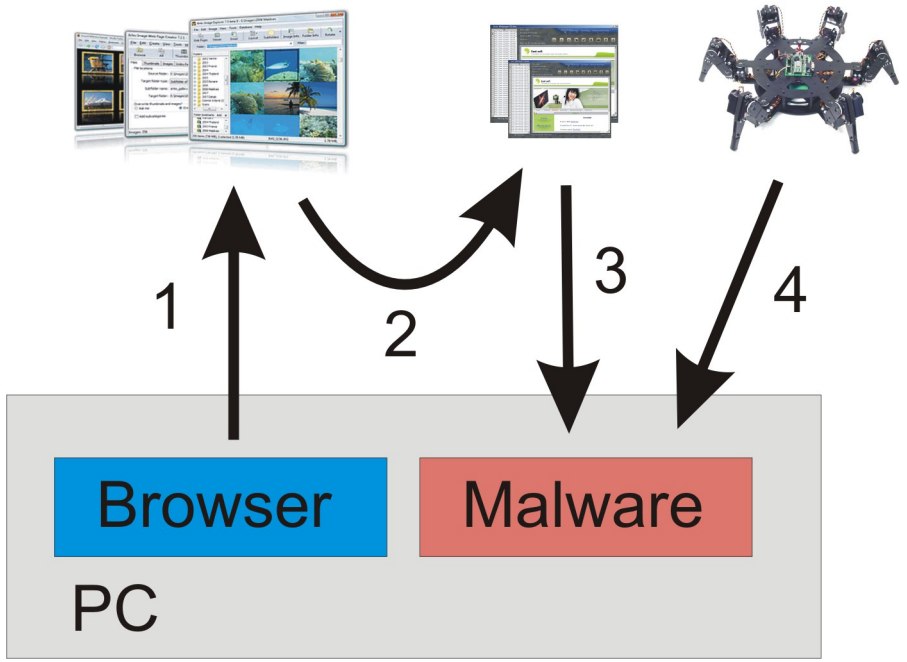
Analýza vnitřního fungování

- Reverzní analýza malware



Analýza vnitřního fungování

- Fáze I. – nakažení
  - Stránky s návnadou (přesměrování)
  - Stránky s exploitem (ovládnutí)
  - Stažení „botnet-klienta“



Analýza vnitřního fungování

- Fáze II. – zahnízdění
  - Zápis do „po spuštění“ / registrů Run a RunOnce
    - Kontrola po 500ms
  - Skrývání správce úloh
    - Kontrola po 500ms
  - Komunikace s C&C
    - Maskováno v procesu prohlížeče
    - Code injection
    - Navenek se jeví jako činnost prohlížeče
  - Ostatní procesy nekomunikují
    - Využívají padfile (odkládací soubor)

Analýza vnitřního fungování

- Fáze III. – vydírání
  - Stažení aplikace (do padfile)
    - Napsána v Borland's Delphi
  - Spuštění aplikace
    - Nastavena jako „vždy navrchu“ (StayOnTop)
  - Uživatel
    - Nevidí jiné aplikace „pod ransom dialogem“
    - Nemůže si vyvolat správce úloh
    - Vidí svou IP adresu, geolokační údaje
    - Má-li webkameru, vidí svůj obrázek
    - Je vyzván k zaplacení ...

Button1

[redacted] Label4

ČESKÁ REPUBLIKA POLICIE
ÚSTAV POČÍTAČOVÉ TRESTNÉ ČINNOSTI

Image15 Löschen

Combobox1 100

Timer1,3,4

Chcete-li odblokovat Váš počítač a vyhnout se trestnímu stíhání, musíte provést platbu ve výši 2000 Kč.

Všechny operace prováděné na tomto počítači se zaznamenávají.
Pokud používáte webovou kameru, video a fotografie se ukládají pro účely identifikace.

Videozáznam: **ON**

Panel1

Můžete být snadno identifikován pomocí IP adresy Vašeho počítače a s ní spojeného doménového jména.

Vaše IP adresa: [redacted]
Doménové jméno:
Místo: Label1-3

Váš počítač byl uzamčen!

Provoz Vašeho počítače je pozastaven z důvodu podezření z neoprávněné činnosti.

Níže jsou uvedené možné narušení, které jste provedl:

Článek 274 - Autorské právo
Pokuta nebo trest odnětí svobody na dobu až 4 let
(Použití nebo sdílení souborů chráněných autorskými právy - filmy, software)

Článek 183 - Pornografická produkce
Pokuta nebo trest odnětí svobody až na 2 roky
(Použití nebo sdílení pornografických souborů)

Článek 184 - Zneužití dítěte (do 18 let) k výrobě pornografie
Trest odnětí svobody až na 15 let
(Použití nebo sdílení pornografických souborů)

Článek 104 - Propagace terorismu
Trest odnětí svobody až na 25 let
(Navštěvovali jste webové stránky teroristických organizací)

Článek 297 - Nesprávné použití počítače, které vede ke vzniku vážné škody
Pokuta nebo trest odnětí svobody až na 2 roky
(Váš počítač je infikován virem, který následně infikoval další počítače)

Článek 108 – Hazardní hry
Pokuta nebo trest odnětí svobody až na 2 roky
(Hráli jste hazardní hry, které jsou zákonem zakázané ve Vaší zemi)

V souvislosti s rozhodnutím Vlády ze dne 22. srpna, všechny tyto trestné činy mohou vést k podmíněnému trestu po zaplacení pokuty.

Výše pokuty je 2000 Kč. Platba musí být provedena do 48 hodin po objevení narušení. Pokud udělená pokuta nebude zaplacena, automaticky bude zahájeno trestné stíhání.

Po zaplacení pokuty Váš počítač bude odblokován.

Ukash

Ukash je k dostání online, e-peněženkách, trafikách a bankomatech po celém světě.

Vyměňte peníze za Ukash kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód: Edit1

1 2 3 4 5 6 7 8 9 0

Image3 Předložit

Kde lze koupit Ukash

eva electronic value
Alles prepaid!

paysafecard

Paysafecard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech.

Vyměňte peníze za Paysafecard kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód: Edit2

1 2 3 4 5 6 7 8 9 0

Image2 Předložit

Kde lze koupit Paysafecard

Tipsport
OMV
žabka
Eni
Shell

Vezměte prosím na vědomí, že pokuta musí být zaplacena do 48 hodin. Pokud se Vám nepodaří provést platbu ve stanovené lhůtě, odblokování Vašeho počítače nebude možné.

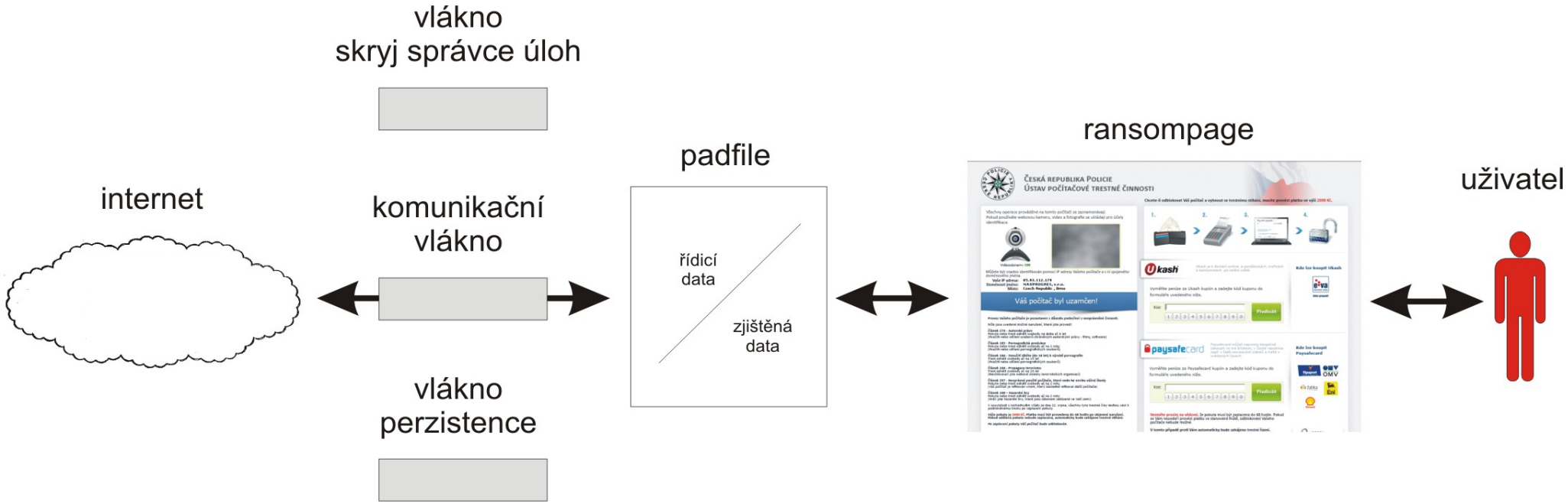
V tomto případě proti Vám automaticky bude zahájeno trestní řízení.

Analýza vnitřního fungování

- Aktivita ransompage
  - Obrázek z webkamery/bílý šum
  - IP adresa + geolokační údaje
  - Validace platebních kódů
    - Lokálně
    - Délka, typ znaků
    - Úvodní řetězec
  - VolumeID – sériové číslo disku
  - Uložení informací do padfile
    - Následně odesláno komunikačním vláknem

Analýza vnitřního fungování

- Fungování malware



- Zjišťovaná a odesílaná data
- IP adresy účastnící se napadení
- IP adresy C&C

Ransomware PČR na ZČU

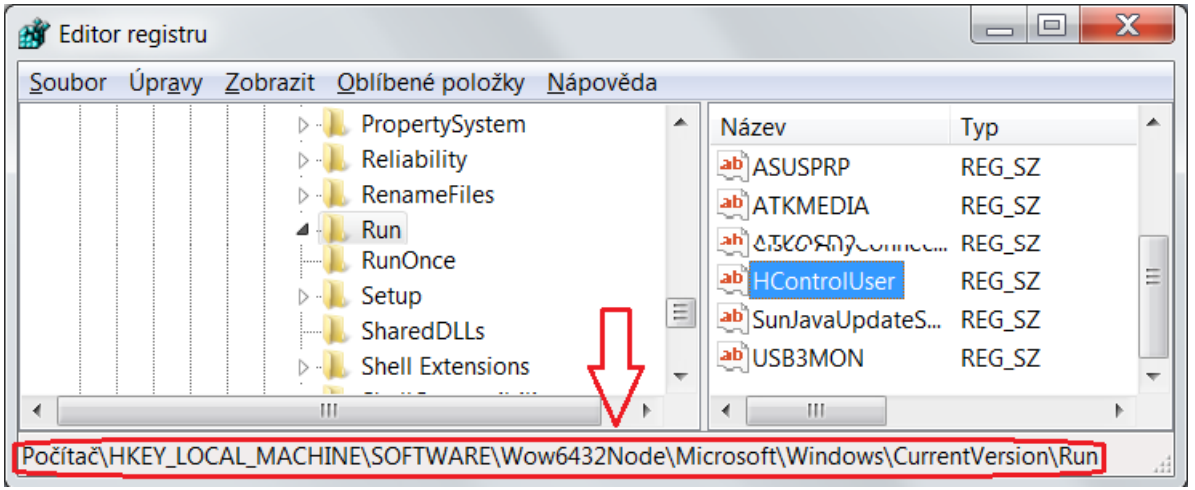
- Uživatelé sítě WEBnet
  - Také chodí na „podivné“ stránky
  - Také se nakazili
- Občas i stanice IS
  - Řešení bezpečnostního incidentu
  - Víme i jak došlo k nákaze
    - Historie prohlížeče
    - Provozní informace (NetFlow)
  - Neděláte nám radost!
- Zkušenosti s odstraňováním

Odstranění z PC

- Způsob přežití viru na PC (Persistence)
  - Spuštění viru po restartu PC
- Obranné mechanismy viru
  - Vyřazení antiviru, skrývání
  - Omezení činnosti uživatele
- Možnosti odstranění viru z PC
  - Nalezení infikovaných souborů
  - Zapnutý a vypnutý systém
- Deathray.vbs
  - Jednoduchý nástroj pro boj s viry
  - Nasazení na ZČU

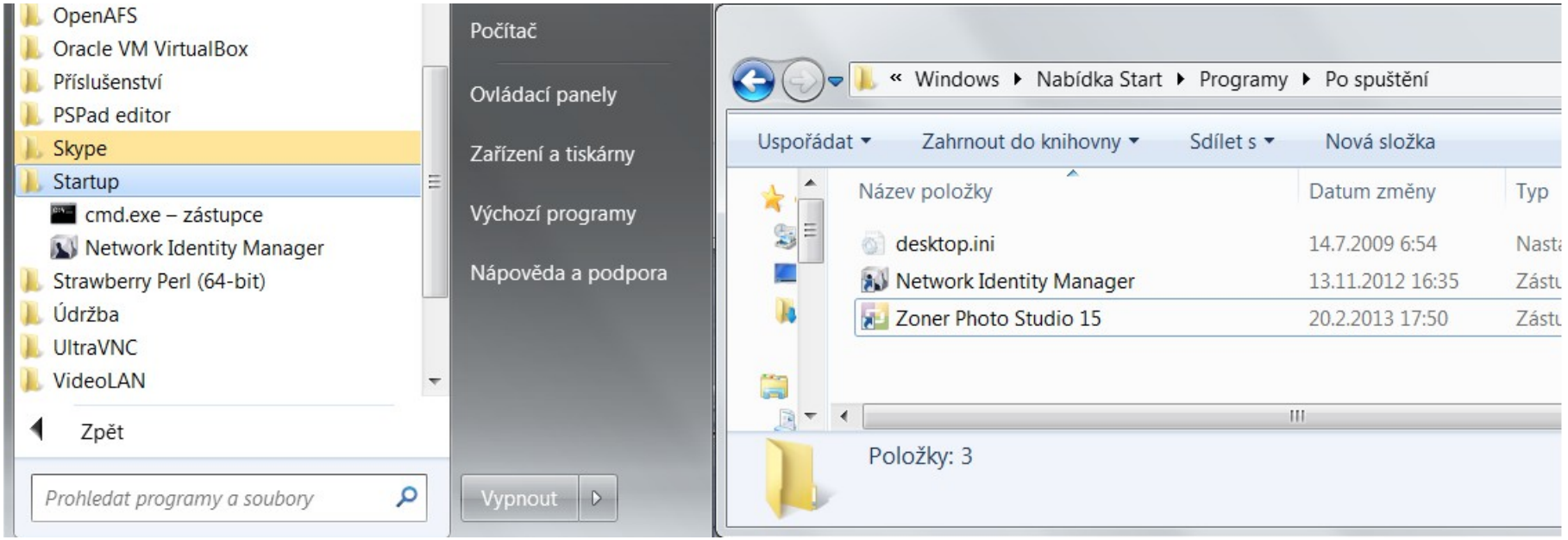
Perzistentní mechanismy

- Registrové klíče
  - Systémová část, HKLM = HKEY_LOCAL_MACHINE
    - **Virus v HKLM = PROBLÉM**
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    - HKLM\Software**Wow6432Node**\Microsoft\Windows\CurrentVersion\Run
      - 64 bitový systém!
    - HKLM\Microsoft\Windows NT\CurrentVersion\Winlogon – “shell“
  - Uživatelská část, HKCU = HKEY_CURRENT_USER
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run



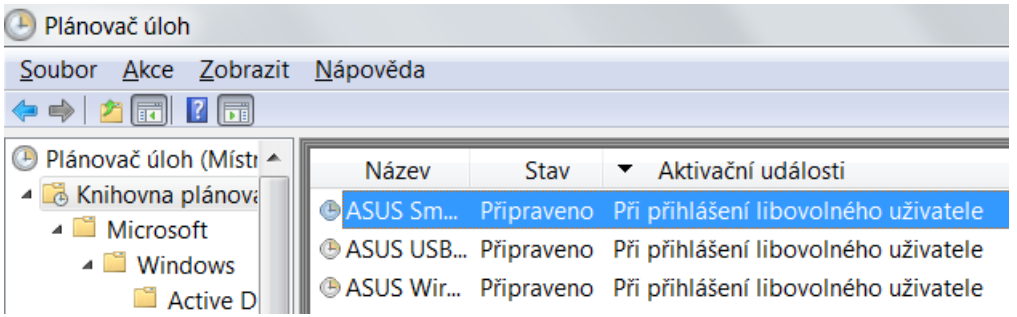
Perzistentní mechanismy

- Složka „Po spuštění“
  - %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    - Uživatelská část, každý uživatel má svou
  - %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup
    - Systémová část, společná pro všechny uživatele
  - Skryté soubory se nespouští

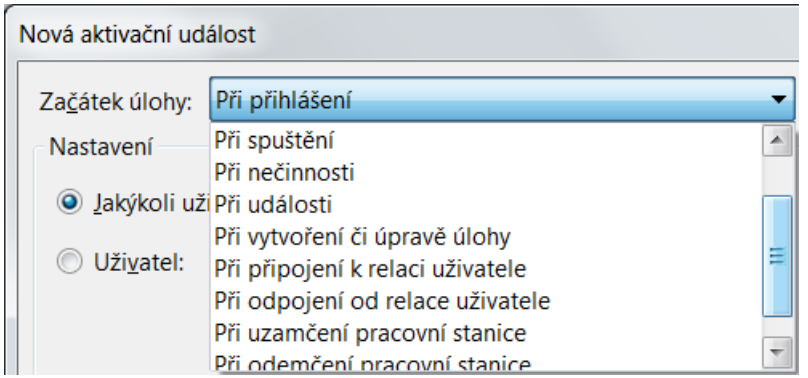


Perzistentní mechanismy

- Plánovač úloh - taskschd.msc
  - C:\Windows\System32\Tasks – xml soubory s parametry
  - Aktivace v zadaný čas, nebo na základě události
  - Není tolik „vidět“



  - Různé aktivační události



Perzistentní mechanismy

- Služba, driver, hook do kernelu...
  - Virus má k dispozici administrátorská, nebo systémová práva
  - Systému se nedá věřit
  - Vypnout, disk připojit do jiného PC, zálohovat data
  - Naformátovat disk a reinstalovat systém

Obranné mechanismy viru

- Obranné mechanismy viru
  - Obrana před antivirovým skenem
  - Aktivní vyřazení antiviru
    - Nový virus – AV nemá definice
    - AV je jen software, lze jej shodit
    - Odinstalace AV :-)
  - Úprava NTFS oprávnění (nelze smazat)
  - Omezení činnosti uživatele
    - Skrytí plochy
    - Blokování diagnostických nástrojů
    - Blokování spouštění nových procesů

Odstranění z PC

- Možnosti odstranění viru z PC – běžící systém
  - Na zapnutém systému hledáme „podezřelý“ proces
    - Např.: wgsdgsdgsdgs.exe, svclhost.exe...
    - Pozměněný název, spuštěný ze špatného adresáře
  - Pokud to jde, sestřelíme jej
    - Právce úloh – Win+R taskmgr.exe
    - Nástroj „kill“ – taskkill.exe /im svclhost.exe /f
  - Vyhledáme jeho výskyty v registru
    - Editor registru – regedit.exe a CTRL+F
    - Klíče zaznamenáme
  - Najdeme všechny soubory a složky podle času změny u „zlé“ binárky
    - Vlastnosti souboru svclhost.exe – vytvořeno/změněno
    - Může odhalit další součásti malware, zaznamenáme umístění
  - Vypneme PC

Odstranění z PC

- Možnosti odstranění viru z PC – Vypnutý systém
  - Kontrola persistence – hledáme podezřelé věci
    - Neznámé procesy
    - Spouštění z uživatelského profilu
  - Kontrola uživatelského profilu na podezřelé soubory
    - Binárky, dll soubory nebo jiné nezvyklé v %userprofile%
  - Podle času změny podezřelého souboru hledáme další
    - V době prvního nahrání na PC došlo k dalším akcím
  - Nalezené soubory hledáme v registrech
    - Možnost úprav v registrech vypnutého počítače
    - Odstraníme klíče s infekcí
  - Odstraníme infikované soubory, binárky a knihovny viru
  - Disk z infikovaného počítače proskenujeme v čistém počítači antivirem

Ransomware

- Obranné mechanismy
  - Nový, aktualizovaný – AV nemá definice
  - Skrytý, navenek komunikuje jako Internet Explorer
    - Dll injection
  - Blokuje činnost uživatele
    - Přes celou obrazovku
  - Hlídá persistenci
    - Každých 500ms kontroluje registr
  - Blokuje správce úloh
    - Každých 500ms zjišťuje zdali neběží

Ransomware

- Použité mechanismy persistence
  - HKCU\Microsoft\Windows\CurrentVersion\run
    - Použito většinou na Windows XP
  - %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    - Zástupce na binárku v profilu
    - Použito ve Windows 7
  - HKLM\Microsoft\Windows NT\CurrentVersion\Winlogon – “shell“
    - Klíč „shell“ normálně spouští plochu – explorer.exe
    - „Zmizí“ nabídka start, ikony na ploše
    - Aplikovalo by se pro všechny uživatele
    - Nebylo aktivní, zápis do tohoto klíče hlídá UAC

Ransomware

- Odstranění
  - Spustit PC v nouzovém režimu
    - Nejlépe pod jiným uživatelem
  - Nalézt binárky, podle času změny dohledat další soubory
    - Zaznamenat si názvy souborů
    - Odstranit soubory
  - Najít mechanismus persistence – podle názvů z minulého kroku
    - Odstranit persistenci - smazat klíče v registru a/nebo zástupce
  - Restartovat, přihlásit se ověřit zdali se virus neprojevuje
  - Aktualizovat antivir, proskenovat celý počítač
  - V případě možnosti provést z jiného počítače

Dotazy

???