SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Jak, kde a proč vzniká malware ?

Ondřej Novotný

AVG Technologies CZ, s.r.o.

Obsah

- Od slávy ke zločinu
- Proč ?
- Kdo jsou „ONI“ ?
- Jak ?
- Otázky

Od slávy ke zločinu

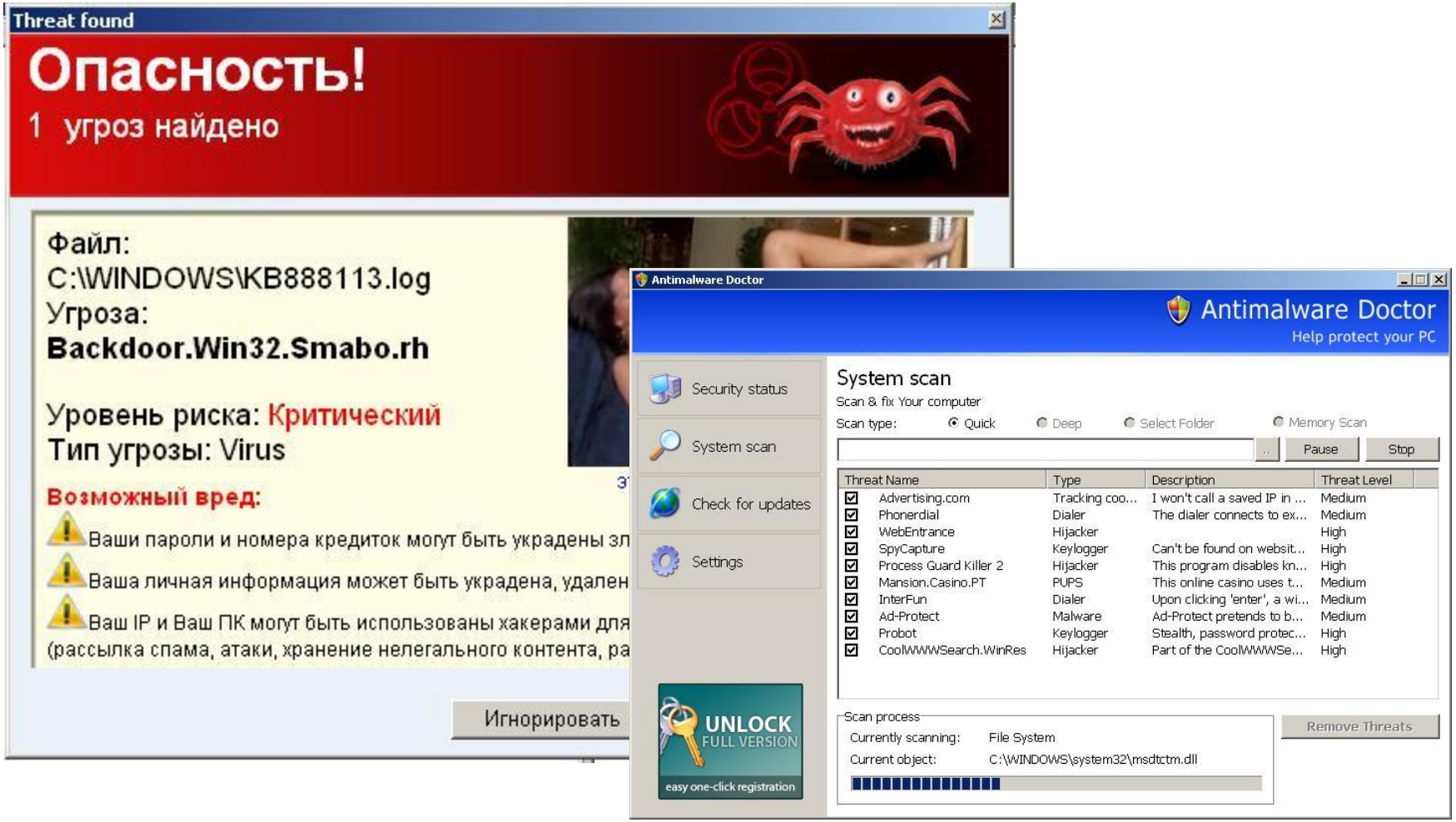
- Halloween.1376

Virus napsany specialne pro inzenyra ZAKA ze SPS
****
Nepodlehejte panice, mate nakazeno jen par souboru...
(c) 1993 II.A 1988
Tak a ted si vyzkousime treba: RESET
Kdyby kazdy nespokojeny student
napsal virus, tak v nasich skolach by
ani jiny software nekoloval a McAfee by se divil...

Nesedte porad u pocitace a zkuste jednou delat neco rozumneho!
****
!! Poslouchejte HELLOWEEN - nejlepsi metalovou skupinu !!

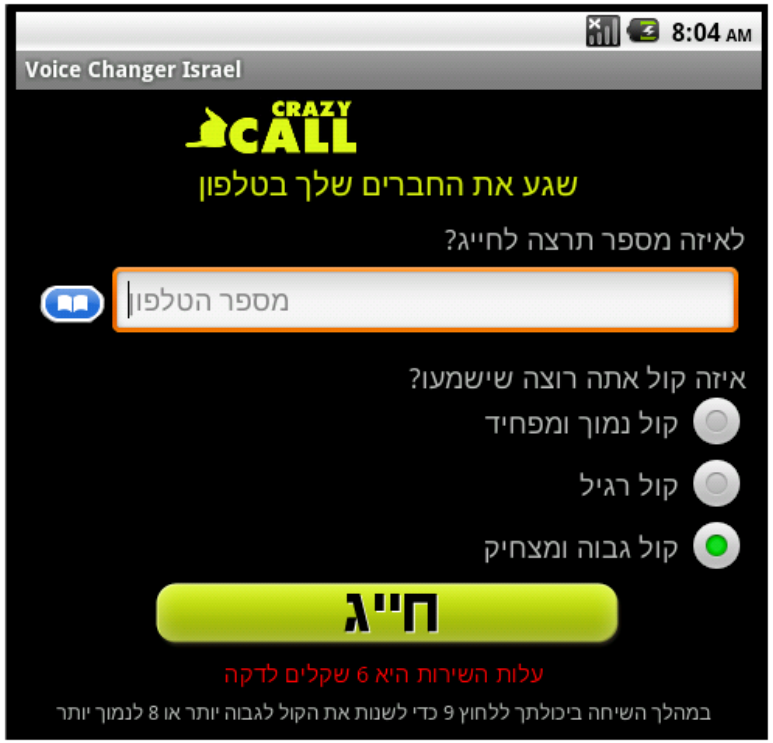
Od slávy ke zločinu

- Ransomware, falešné AV produkty



Od slávy ke zločinu

- Malware pro mobilní zařízení



012 - izraelský mobilní operátor
40 - předčíslí volané země
900720674 - prémiové číslo

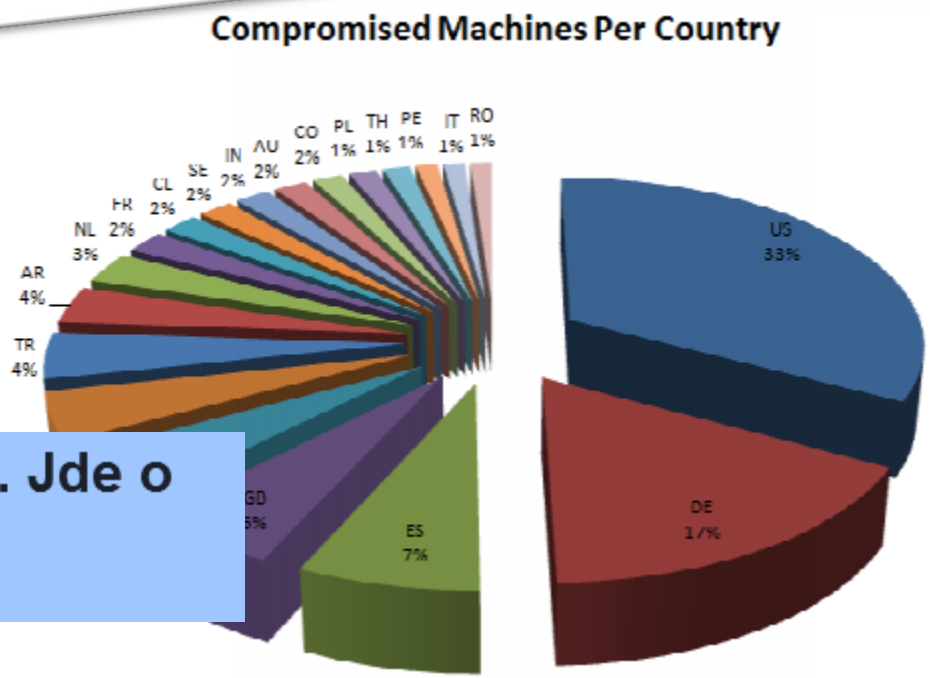
```
localObject = new Intent("android.intent.action.CALL", Uri.parse("tel:012409007206674%2C" + str + (String)localObject));
Toast.maketext(this, 2131034123,1).show();
startActivity((Intent)localObject);
return;
```

Od slávy ke zločinu

- Botnety, krádeže bankovních účtů, loginů
- Cílené útoky

Zappos hacknuto, data 24 milionů zákazníků v rukou hackerů

Sony Hacked Again; 25 Million at Risk

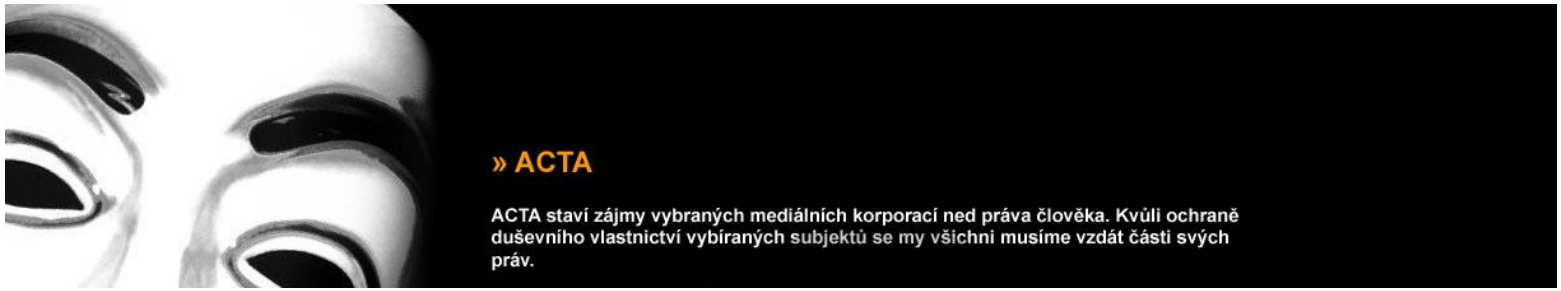


Malware Duqu napadá továrny. Jde o výnosný business

25. 10. 2011 6:25 Pavel Čepský

Proč ?

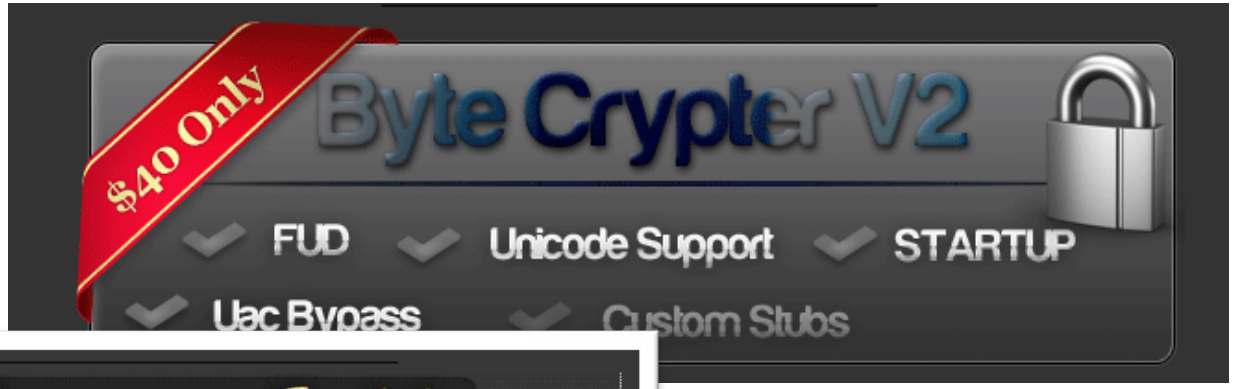
- Hacktivism



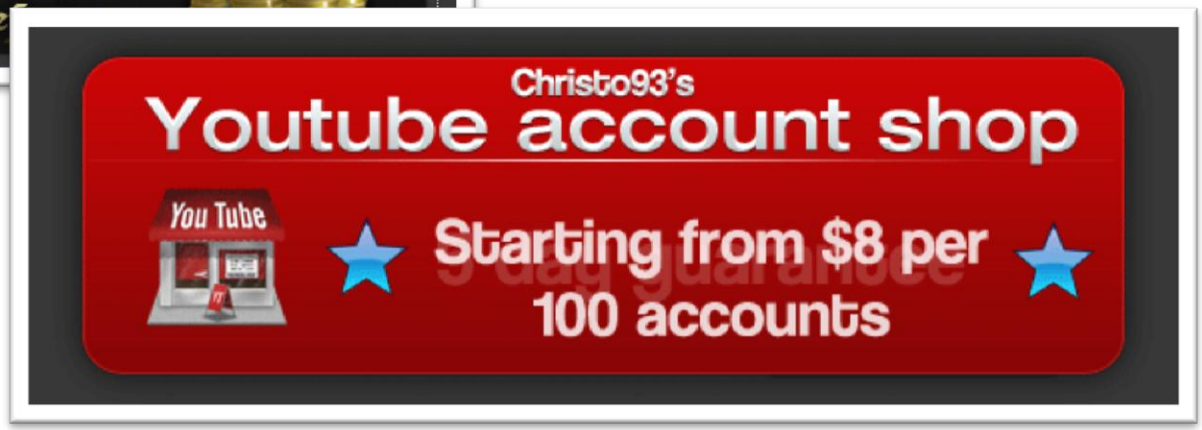
- Zisk

Proč ?

- Zisk


$40 Only
Byte Crypter V2
FUD
Unicode Support
STARTUP
Uac Bypass
Custom Stubs


iCrypt Gold
100% fud
No Dependencies
4 Years and Still Running


Christo93's
Youtube account shop
You Tube
Starting from $8 per
100 accounts

Proč ?

- Zisk

Kdo ?

VS

Koobface botnet master
Nikolaevich Korotchenko - http://ddanchev.blogspot.com

Kdo ?

- Script kiddies
  - Minimum vlastního kódu
  - Recyklace hotových řešení
  - VB6, .NET
  - Cena: řádově desítky USD
- Profesionálové
  - Robustní a sofistikovaný malware
  - Znalost kernelu OS, MBR, rootkit technik
  - Botnety s C&C
  - Cena: řádově stovky až tisíce USD

Kdo ?

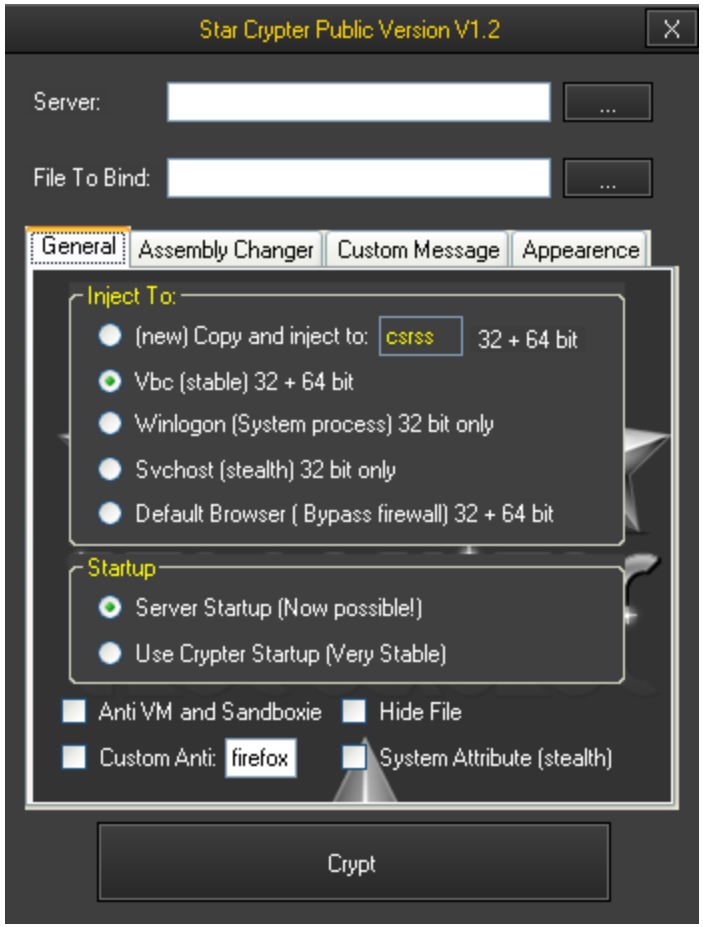
- A co AV společnosti ?
  - Strach jako marketingový nástroj
  - Konkurence
  - Převod a legalizace získaných prostředků
  - Globální, decentralizovaná distribuce malware

Jak ? H4ck3r$ - |-|4(|{3®$

- Chci psát malware, ale nevím jak...

Jak ?

- Nástroje



ScanWatch

ScanWatch

ScanWatch is a brand new service offering you...

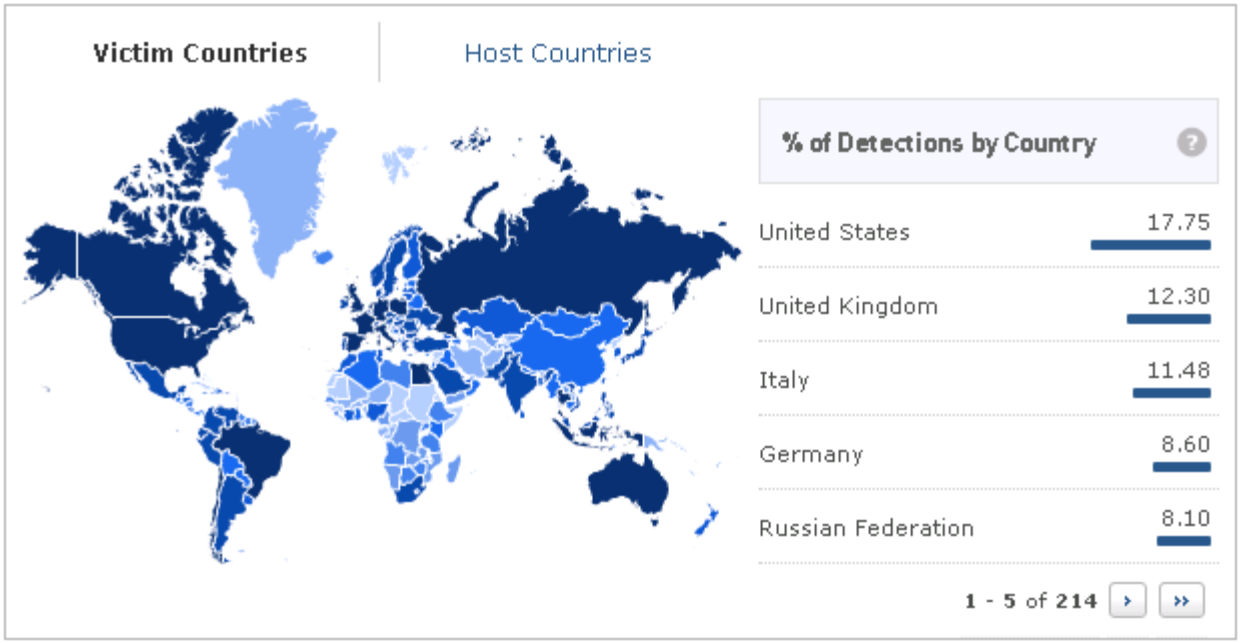
Online Crypting

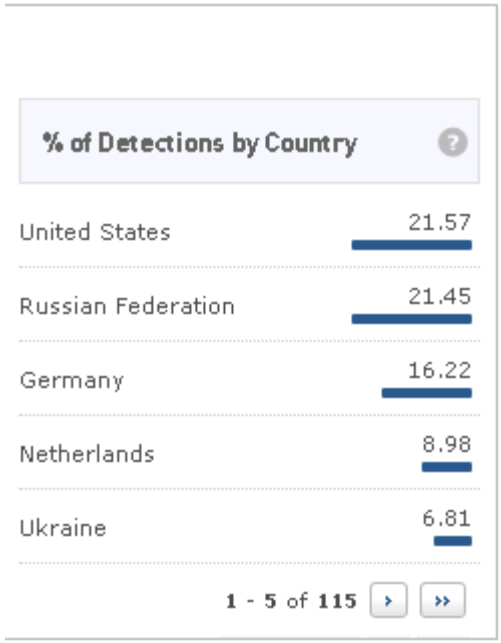
CRYPT A FILE

Crypting using 3rd Party Crypters!

Jak ?

- **Exploit Kits (Blackhole, Phoenix)**





Jak ?

- Zakoupení zdrojového kódu
- Zakoupení botnetu

```
EnderecoAtual := 0;
  EnderecoMax := high(DNS);

  ChromeFile := GetAppDataDir + '\' + 'SQLite3.dll';

  if RootKITBuffer <> '' then
  begin
    MyHideProcess;
    Write2Reg(HKEY_CURRENT_USER, 'SOFTWARE\Microsoft\', 'PIDprocess', inttostr(GetCurrentProcessID));
    MainMutexRootKIT := CreateMutex(nil, False, pchar(MutexRootKIT));
    StartThread(@StartRootKIT);
  end;

  StartThread(@StartMailSend);
  StartThread(@VerificarConexao);

  // aqui eu jõ deixo algumas senhas prontas...
```

Kde ?

- Neanglicky mluvící země
  - Brazílie
  - Čína
  - Země ruské federace
- Anglicky mluvící země

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Ondřej Novotný
AVG Technologies CZ, s.r.o.
ondrej.novotny@avg.com