

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

Threat found

Опасность!
1 угроз найдено

Файл:
C:\WINDOWS\KB888113.log
Угроза:
Backdoor.Win32.Smabo.rh

Уровень риска: **Критический**
Тип угрозы: Virus

Возможный вред:

- Ваши пароли и номера кредиток могут быть украдены
- Ваша личная информация может быть украдена, удалена
- Ваш IP и Ваш ПК могут быть использованы хакерами для (рассылка спама, атаки, хранение нелегального контента, ра...

Игнорировать

Antimalware Doctor

Help protect your PC

Security status
System scan
Check for updates
Settings

System scan
Scan & fix Your computer
Scan type: Quick Deep Select Folder Memory Scan

Threat Name	Type	Description	Threat Level
☒ Advertising.com	Tracking coo...	I won't call a saved IP in ...	Medium
☒ Phonerdial	Dialer	The dialer connects to ex...	Medium
☒ WebEntrance	Hijacker		High
☒ SpyCapture	Keylogger	Can't be found on websit...	High
☒ Process Guard Killer 2	Hijacker	This program disables kn...	High
☒ Mansion.Casino.PT	PUPS	This online casino uses t...	Medium
☒ InterFun	Dialer	Upon clicking 'enter', a wi...	Medium
☒ Ad-Protect	Malware	Ad-Protect pretends to b...	Medium
☒ Probot	Keylogger	Stealth, password protec...	High
☒ CoolWWWSearch.WinRes	Hijacker	Part of the CoolWWWSe...	High

Scan process:
Currently scanning: File System
Current object: C:\WINDOWS\system32\ymsdtctm.dll

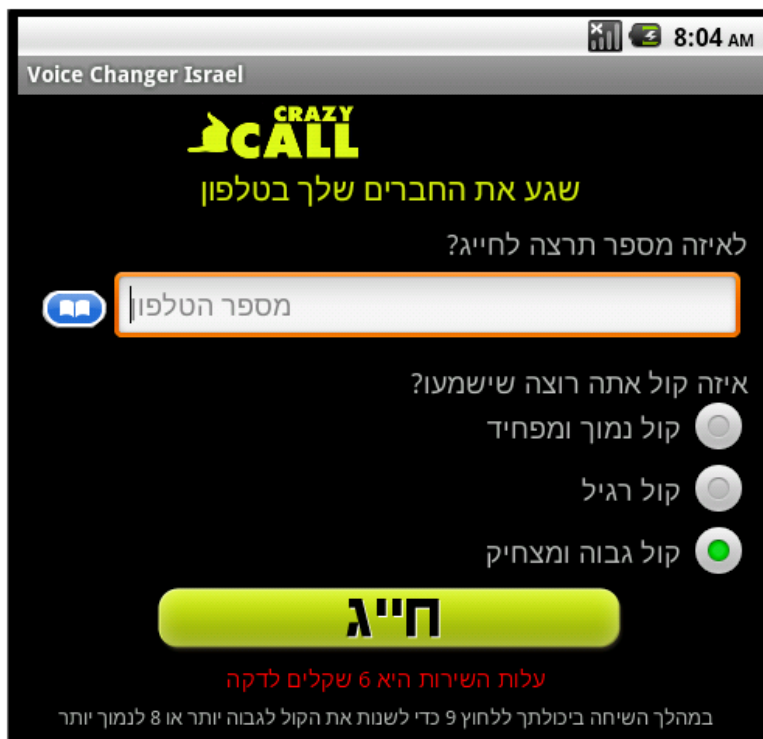
Remove Threats

UNLOCK FULL VERSION
easy one-click registration

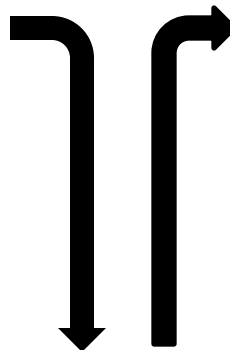


Od slávy ke zločinu

■ Malware pro mobilní zařízení



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



```
localObject = new Intent("android.intent.action.CALL", Uri.parse("tel:01240900720674%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

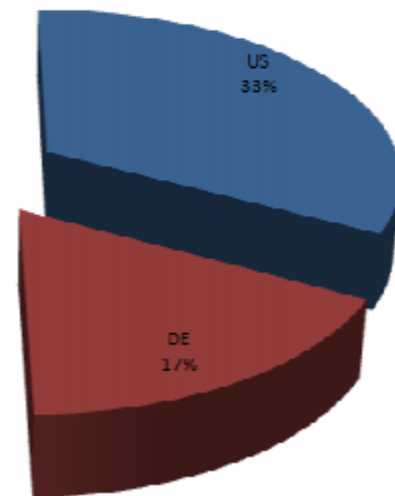
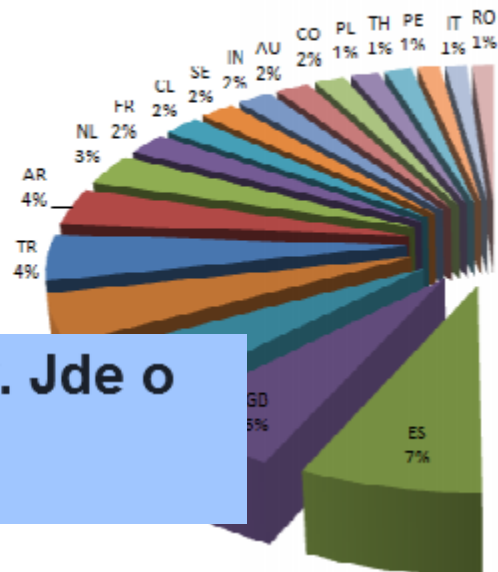
**Zappos hacknuto, data 24 milionů zákazníků
v rukou hackerů**

**Sony Hacked Again; 25 Million
at Risk**

**Malware Duqu napadá továrny. Jde o
výnosný business**

25. 10. 2011 6:25 [Pavel Čepský](#)

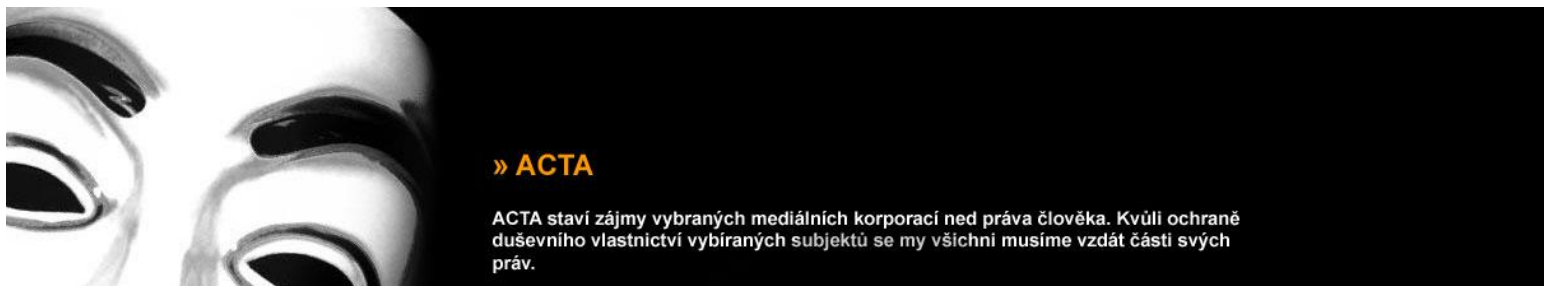
Compromised Machines Per Country





Proč ?

■ Hacktivism



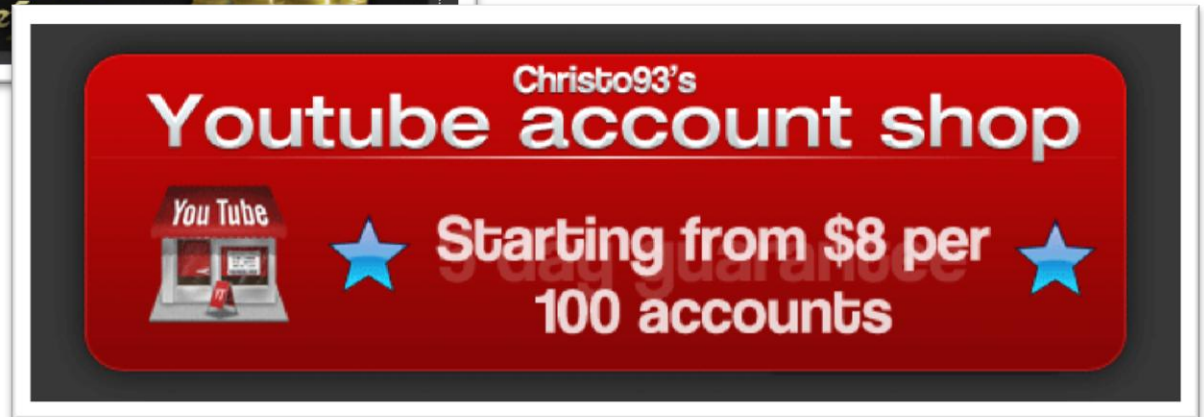
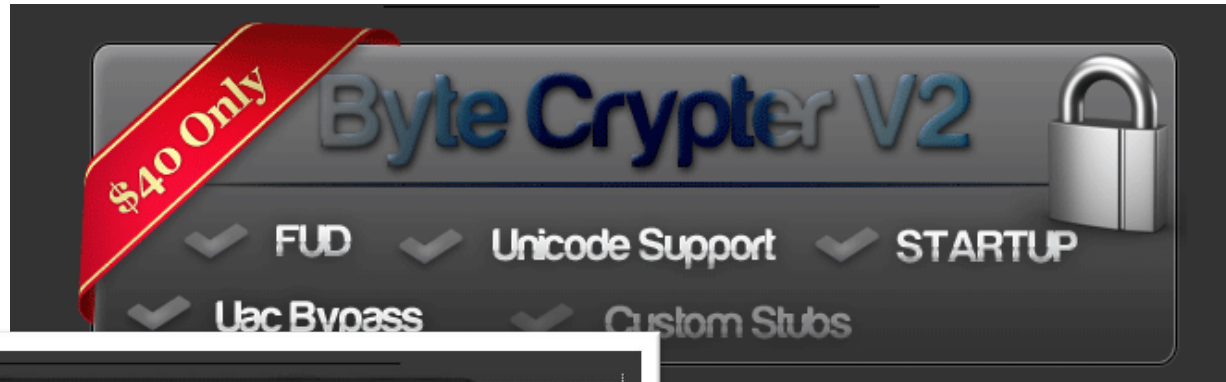
■ Zisk





Proč ?

- Zisk





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®\$

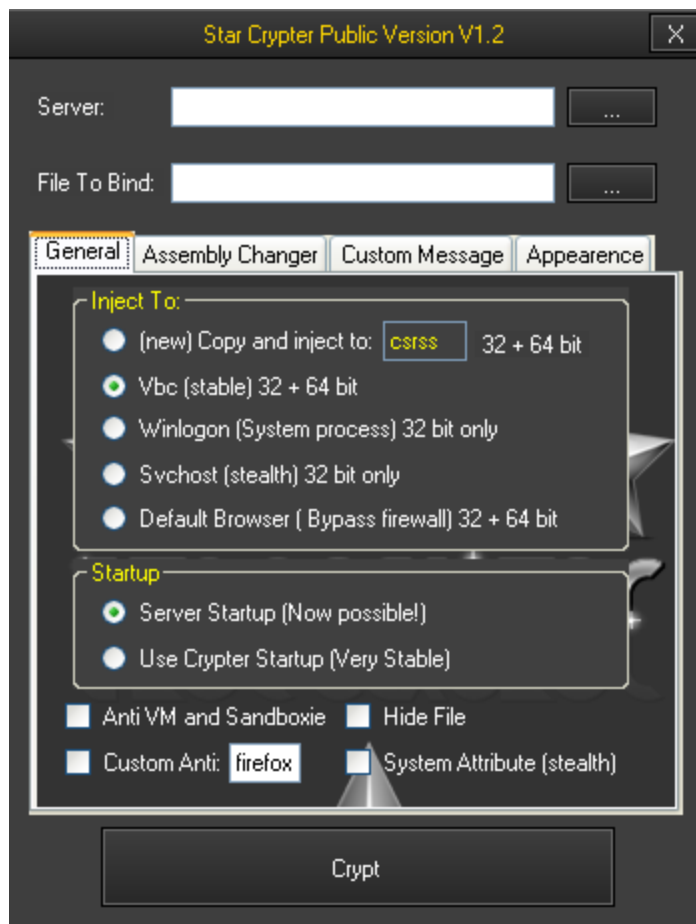
- Chci psát malware, ale nevím jak...





Jak ?

■ Nástroje



ScanWatch



ScanWatch is a brand new service offering you...

Online Crypting

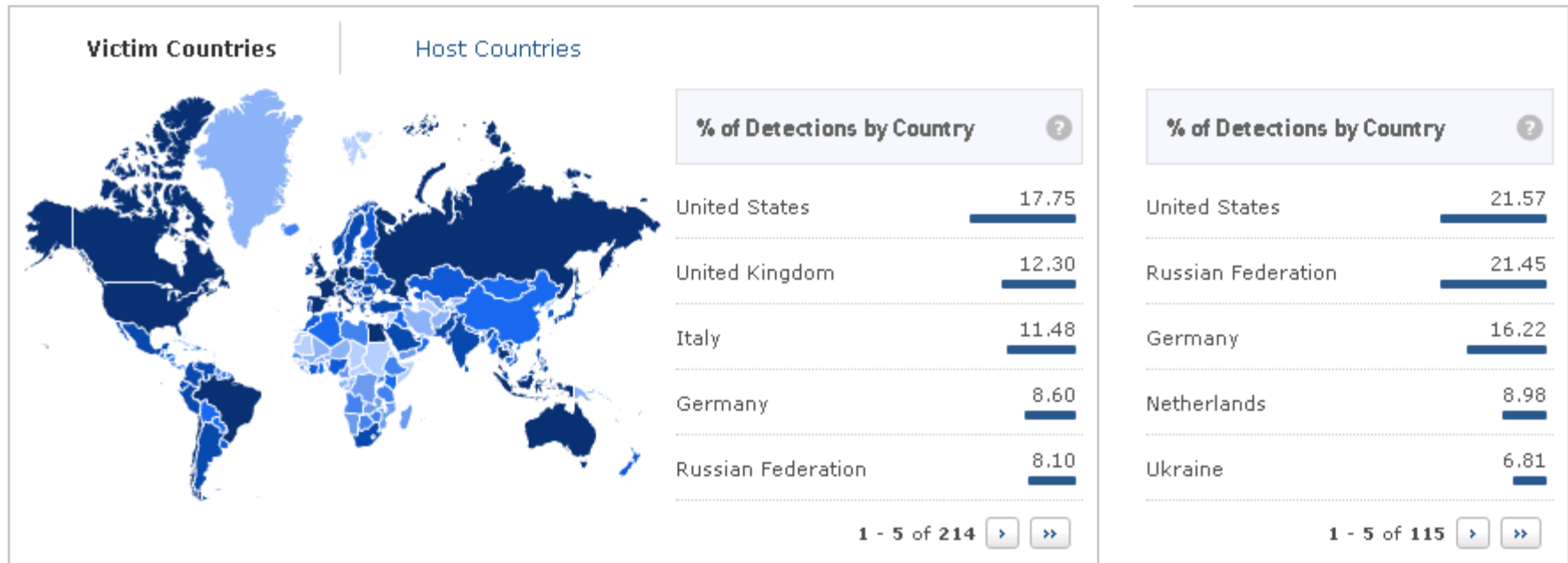


Crypting using 3rd Party Crypters!



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 j6 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

