Peter Stančík

MODERNÝ MALWARE

AKTUÁLNY VÝVOJ Z POHĽADU ESET

Agenda

- Zmeny v motivácii a spôsobe šírenia
- Pár príkladov zo sveta
- Doma a u susedov

- Čo s tým?

Kde bolo, tam…

Vývoj malvéru

Spočiatku:

- dokázať niečo „výnimočné“
- veľmi dobre kategorizovateľné
  - *- vírusy*
  - *- červy*
  - *- rootkity*
  - *- časované bomby*
  - *- trójske kone*
  - *- zadné vrátka*
  - ...

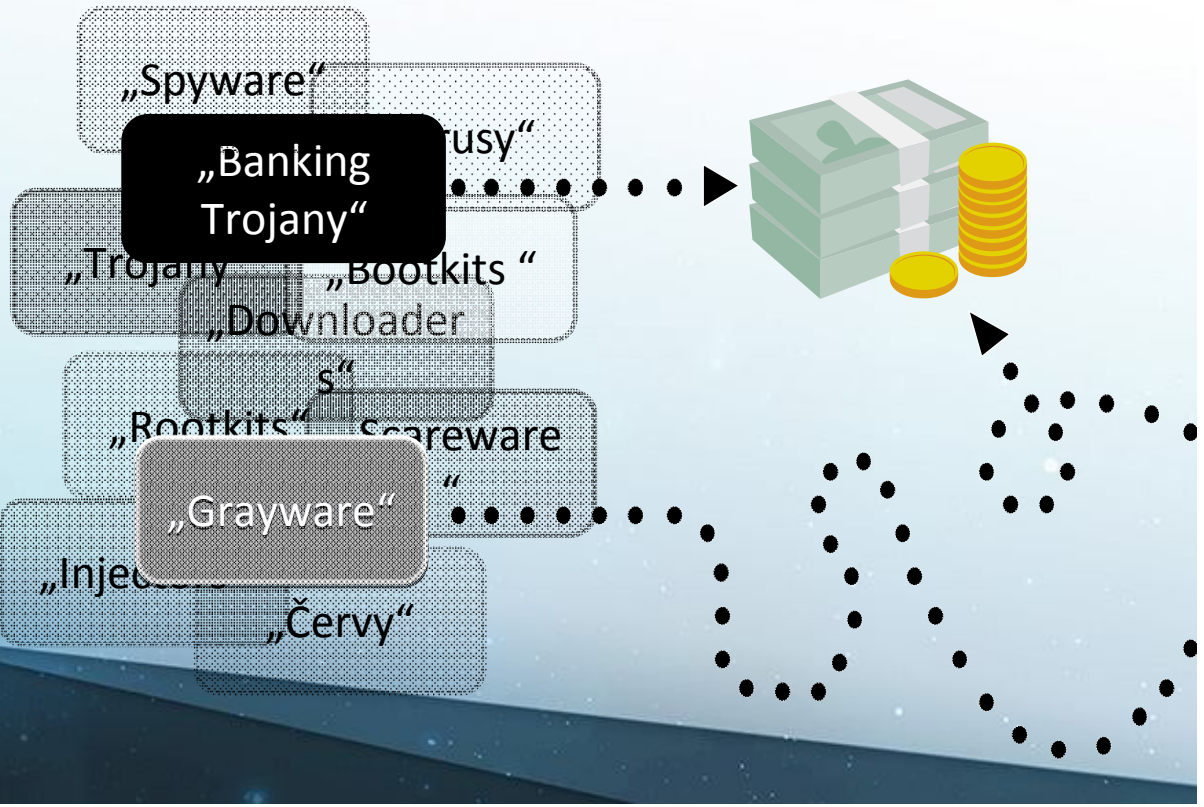
Postupné rozširovanie arzenálu:

- adware
- spyware
- stealware
...

Vývoj malvéru

Súčasnosť:

- splývanie typov / kategórii
- cielený / na mieru vytvorený malvér (špionáž, mocenské / politické záujmy)
- vytváranie a obchodovanie so sieťami infikovaných zariadení (s tzv. botnetmi)
- organizovaný zločin s veľmi rozvinutou infraštruktúrou (vrátane podpory pre „klientov“)
- moc / informácie / $$$



Total Cybercrime Market

IN U.S. DOLLARS

Source: *Group-IB*

Vektory šírenia malvéru

Spočiatku:

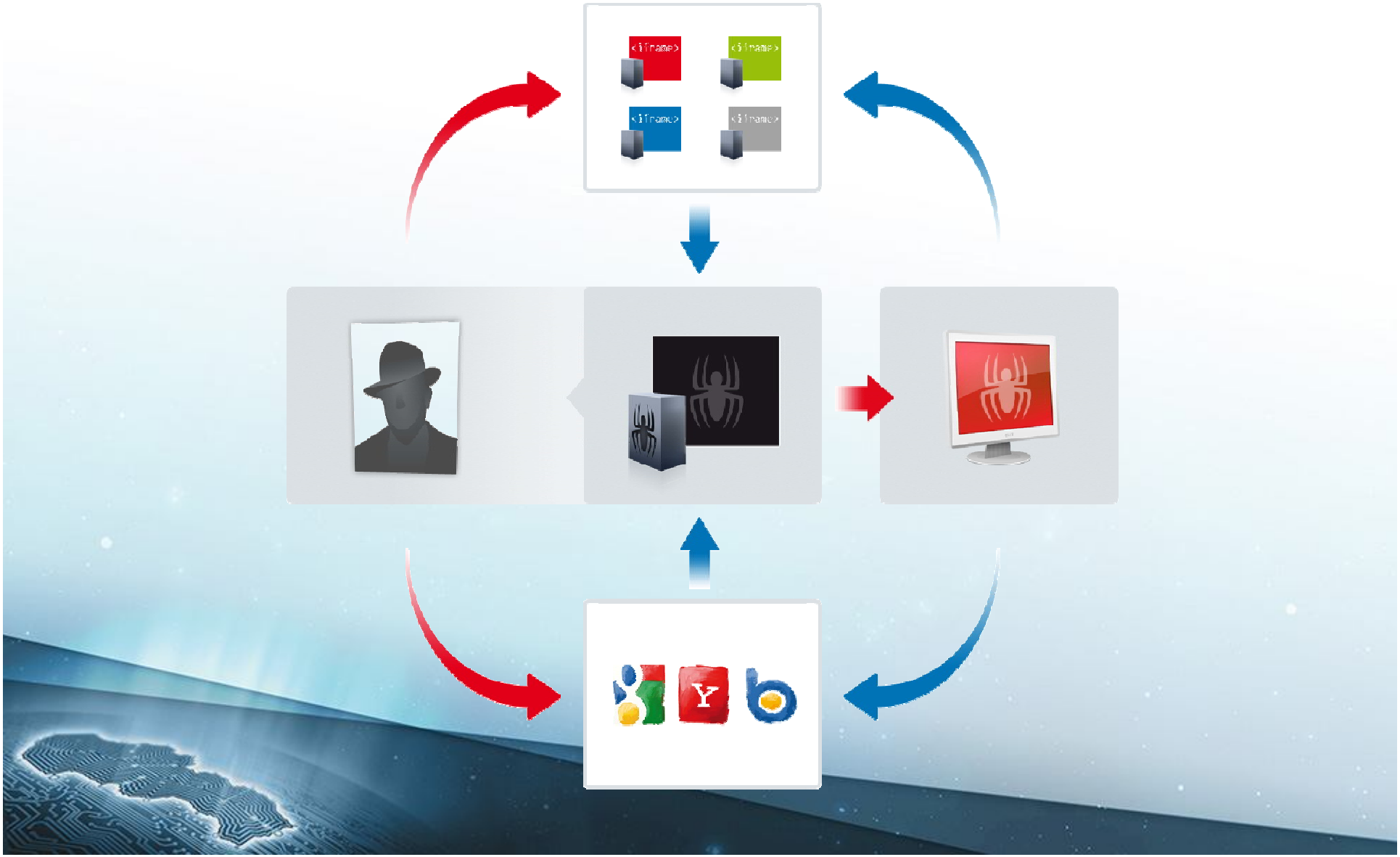
- prenosné média
- zdieľané disky
- e-maily

Súčasnosť:

- šírenie malvéru e-mailami do úzadia
- taktiež prenosnými médiami (odstránenie fukncie „autorun“ u OS od MS)

- tzv. drive-by download – buď nevedomky z infikovanej stránky, alebo
- „dobrovoľné“ stiahnutie / spustenie neopatrným používateľom

Drive-by download



Vektory šírenia malvéru

Spočiatku:

- prenosné média
- zdieľané disky
- e-maily

Súčasnosť:

- šírenie malvéru e-mailami do úzadia
- taktiež prenosnými médiami (odstránenie fukncie „autorun“ u OS od MS)

- tzv. drive-by download – buď nevedomky z infikovanej stránky, alebo
- „dobrovoľné“ stiahnutie / spustenie neopatrným používateľom
- silne podporované sociálnym inžinierstvom
  - prostredníctvom SPAMu
  - SEO
  - ...

Blackhat SEO

Vektory šírenia malvéru

Spočiatku:

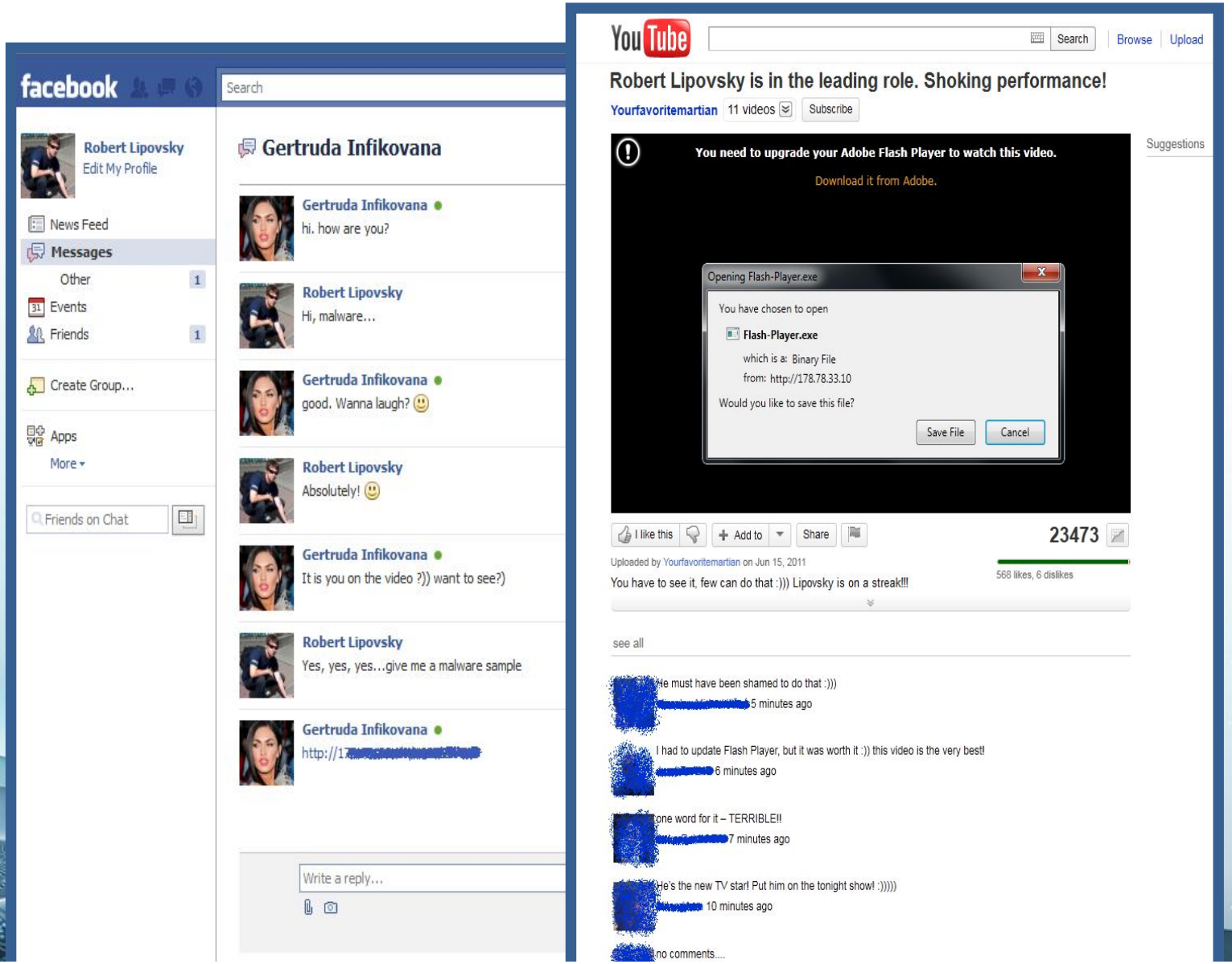
- prenosné média
- zdieľané disky
- e-maily

Súčasnosť:

- šírenie malvéru e-mailami do úzadia
- taktiež prenosnými médiami (odstránenie fukncie „autorun“ u OS od MS)

- tzv. drive-by download – buď nevedomky z infikovanej stránky, alebo
- „dobrovoľné“ stiahnutie / spustenie neopatrným používateľom
- silne podporované sociálnym inžinierstvom
  - prostredníctvom SPAMu
  - SEO
  - cez sociálne siete
  - ...

Malware na sociálnych sieťach



Súčasní „reprezentanti“

Banking Trojany

Gaming Trojany

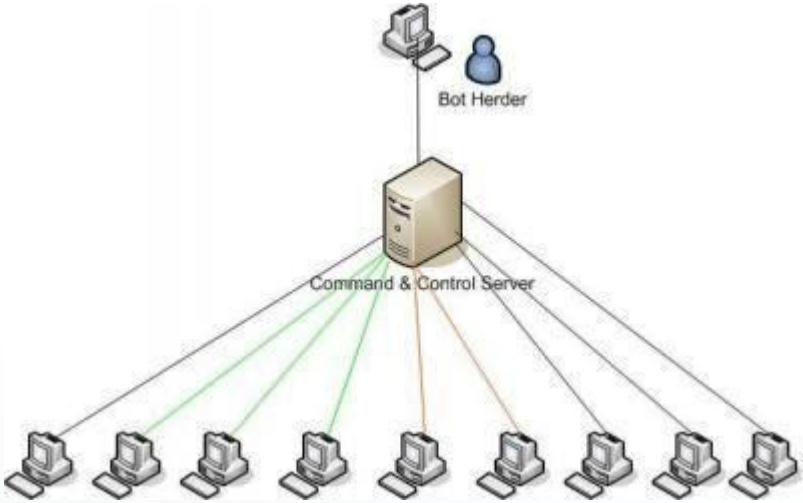
Botnety

Scareware / Ransomware

Mobilné (Android) hrozby

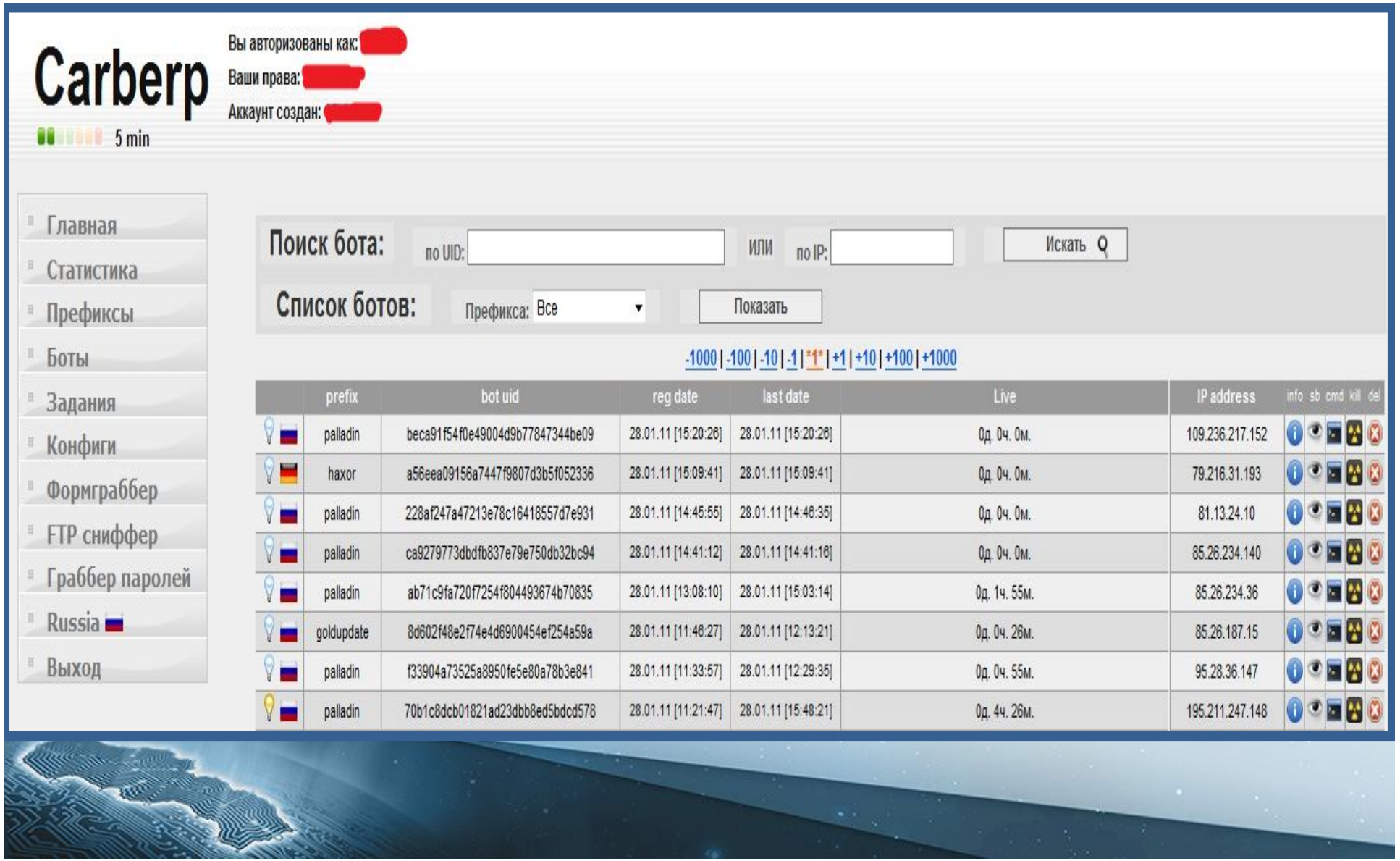
Priemyselná špionáž

Botnet



- sieť robotov – infikovaných počítačov
- takáto armáda je schopná prijímať a vykonávať príkazy od útočníka
- typ „činnosti“ záleží na „schopnostiach“ botov
- rozosielanie SPAMu, DDOS útoky, zber informácií...

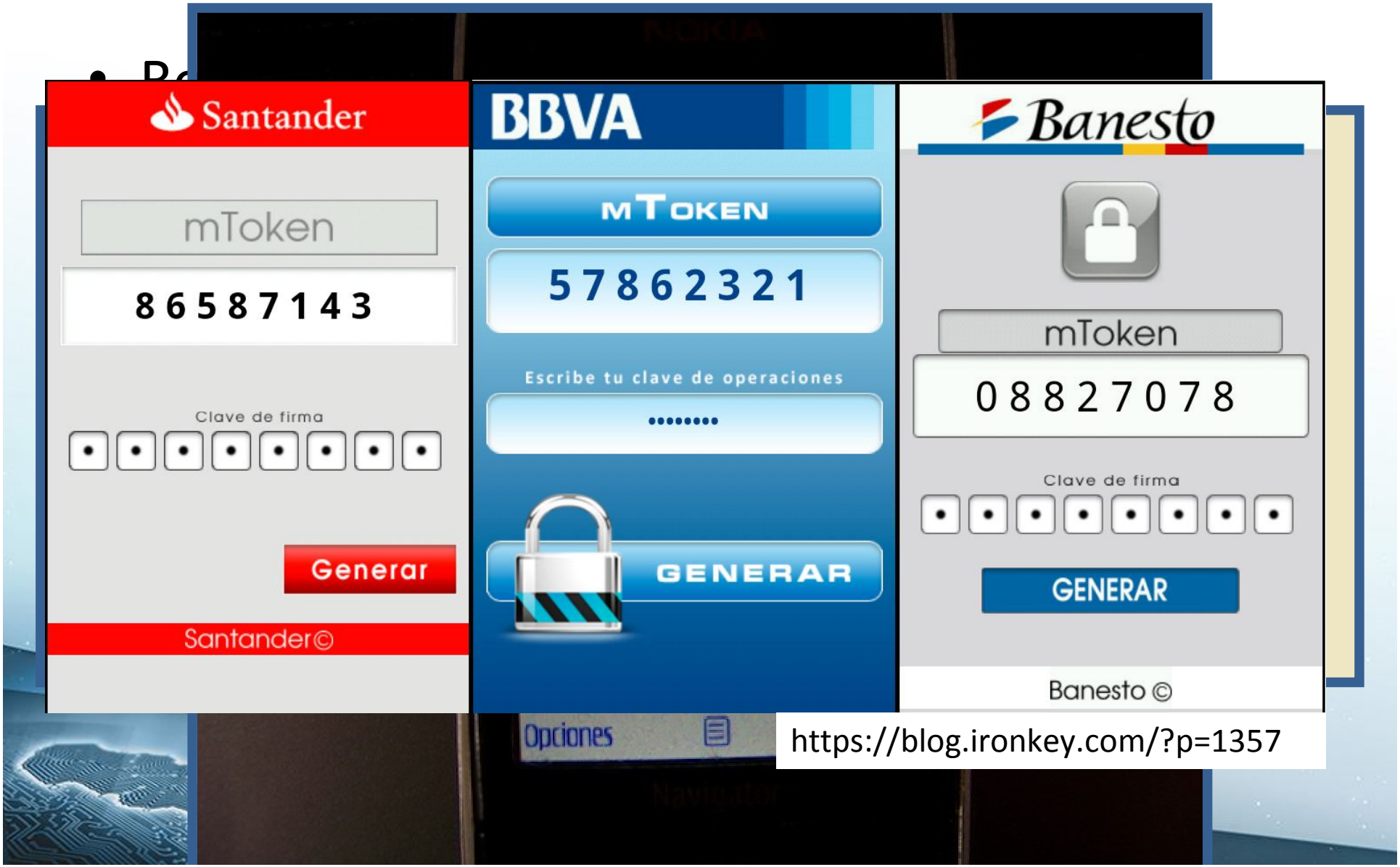
Carberp


Carberp
Вы авторизованы как:
Ваши права:
Аккаунт создан:
5 min
Главная
Статистика
Префиксы
Боты
Задания
Конфиги
Формграббер
FTP сниффер
Граббер паролей
Russia
Выход
Поиск бота:
по UID:
ИЛИ
по IP:
Искать
Список ботов:
Префикса: Все
Показать
-1000 | -100 | -10 | -1 | *1* | +1 | +10 | +100 | +1000
prefix
bot uid
reg date
last date
Live
IP address
info sb cmd kill del
palladin beca91f54f0e49004d9b7847344be09 28.01.11 [15:20:26] 28.01.11 [15:20:26] 0д. 0ч. 0м. 109.236.217.152
haxor a56eea09156a7447f9807d3b5f052336 28.01.11 [15:09:41] 28.01.11 [15:09:41] 0д. 0ч. 0м. 79.216.31.193
palladin 228af247a47213e78c16418557d7e931 28.01.11 [14:45:55] 28.01.11 [14:46:35] 0д. 0ч. 0м. 81.13.24.10
palladin ca9279773dbdfb837e79e750db32bc94 28.01.11 [14:41:12] 28.01.11 [14:41:16] 0д. 0ч. 0м. 85.26.234.140
palladin ab71c9fa720f7254f804493674b70835 28.01.11 [13:08:10] 28.01.11 [15:03:14] 0д. 1ч. 55м. 85.26.234.36
goldupdate 8d602f48e2f74e4d6900454ef254a59a 28.01.11 [11:46:27] 28.01.11 [12:13:21] 0д. 0ч. 26м. 85.26.187.15
palladin f33904a73525a8950fe5e80a78b3e841 28.01.11 [11:33:57] 28.01.11 [12:29:35] 0д. 0ч. 55м. 95.28.36.147
palladin 70b1c8dcb01821ad23dbb8ed5bdcd578 28.01.11 [11:21:47] 28.01.11 [15:48:21] 0д. 4ч. 26м. 195.211.247.148

Carberp


F:
Information.txt
screen.jpeg
Вход в систему
iBank2
internet-banking
iBank2.ru
интернет-банкинг
Тип хранилища:
Ключ на диске
Путь:
F:\keys.dat
Обзор...
Ключ:
Ключ_бухгалтер
Пароль:
****
Язык:
русский
Прокси
Список служб: Подключение к банковскому серверу
Войти
Помощь
© 1999-2007 Bifit (bifit.com)

Banking Trojany



https://blog.ironkey.com/?p=1357

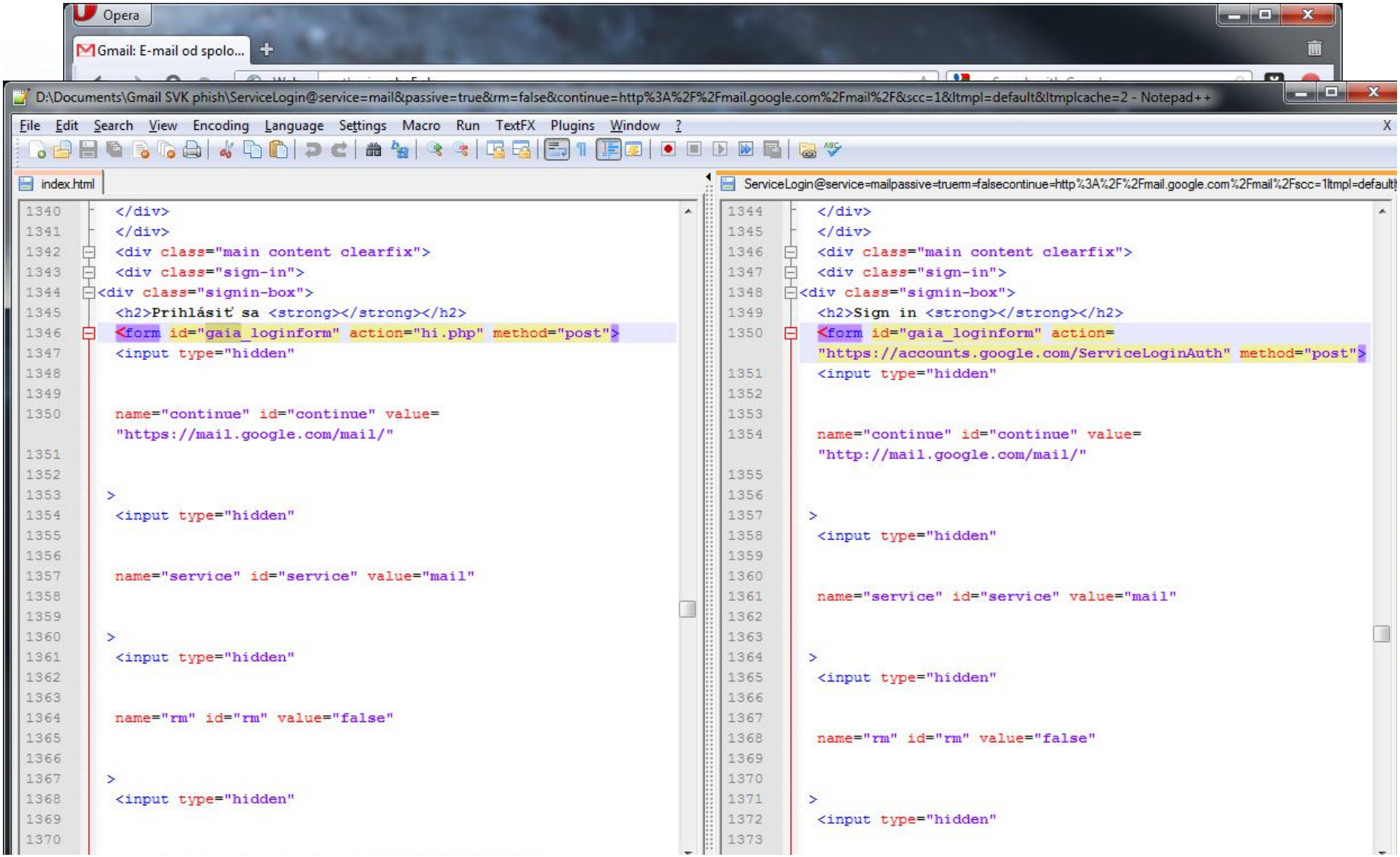
Banking Trojan made in Slovakia?

Pokec Sniffer

- W
- F
- K TP

“Lockscreeny”, Ransomware

Gmail.sk?


Opera
Gmail: E-mail od spolo...
D:\Documents\Gmail SVK phish\ServiceLogin@service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&scc=1&ltmpl=default&ltmplcache=2 - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
index.html
ServiceLogin@service=mailpassive=truerm=falsecontinue=http%3A%2F%2Fmail.google.com%2Fmail%2Fscc=1ltmpl=default
1340
1341
1342
1343
1344
1345 <h2>Prihlásiť sa </h2>
1346 <form id="gaia_loginform" action="hi.php" method="post">
1347 <input type="hidden"
1348
1349
1350 name="continue" id="continue" value=
"https://mail.google.com/mail/"
1351
1352
1353 >
1354 <input type="hidden"
1355
1356
1357 name="service" id="service" value="mail"
1358
1359
1360 >
1361 <input type="hidden"
1362
1363
1364 name="rm" id="rm" value="false"
1365
1366
1367 >
1368 <input type="hidden"
1369
1370
1344
1345
1346
1347
1348
1349 <h2>Sign in </h2>
1350 <form id="gaia_loginform" action=
"https://accounts.google.com/ServiceLoginAuth" method="post">
1351 <input type="hidden"
1352
1353
1354 name="continue" id="continue" value=
"http://mail.google.com/mail/"
1355
1356
1357 >
1358 <input type="hidden"
1359
1360
1361 name="service" id="service" value="mail"
1362
1363
1364 >
1365 <input type="hidden"
1366
1367
1368 name="rm" id="rm" value="false"
1369
1370
1371 >
1372 <input type="hidden"
1373

ACAD/Medre

Priemyselná špionáž v Latinskej Amerike?

Prípady z poslednej doby…

- Stuxnet
- Duqu
- Flame
- Gauss
- …
- ACAD/Medre

Stuxnet y Flame, los dos virus de ciberespionaje más relevantes

Empresa de seguridad informa que ambos comparten el código fuente y que estarían vinculados

Los virus Flame y Stuxnet estarían vinculados entre sí. (AP)

Madrid (EFE). Los dos virus de ciberespionaje más relevantes hasta el momento, Stuxnet y Flame, dirigidos ambos contra computadoras

Niečo zvláštne v Peru…

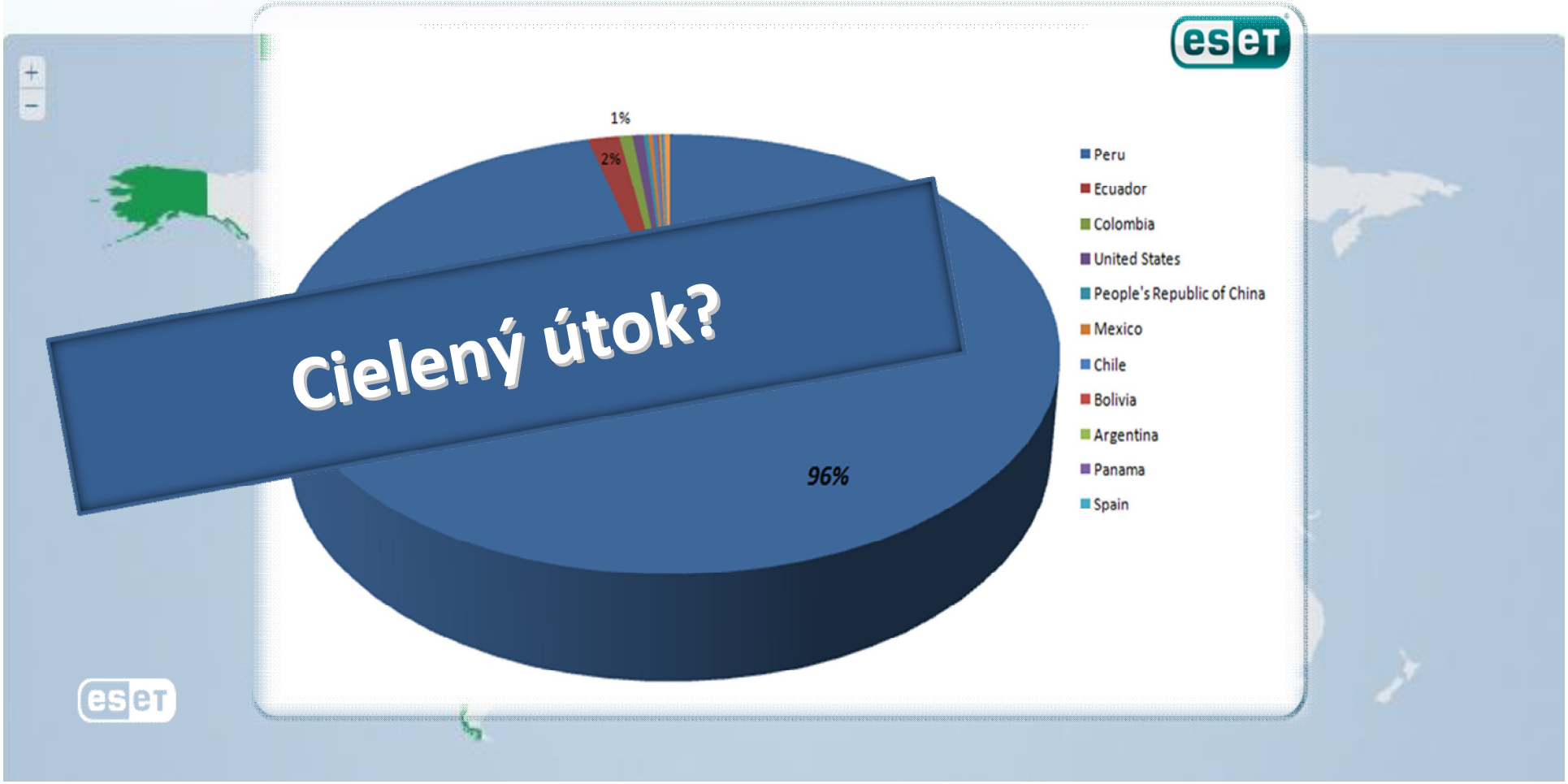
LIVEGRID

ESET Live Grid® 2012 Štatistiky pre Peru

1	INF/Autorun	9,86%
2	Win32/Dorkbot	5,88%
3	Win32/Sirefef	4,07%
4	Win32/Conficker	2,94%
5	Win32/AutoRun.Delf.EP	2,63%
6	HTML/Iframe.B	2,44%
7	Win32/Packed.Themida	2,39%
8	ACAD/Medre.A	2,29%
9	HTML/ScrInject.B	2,04%
10	Win32/Olmarik	1,93%

ACAD/Medre.A štatistiky

LIVEGRID



AutoLISPový červ

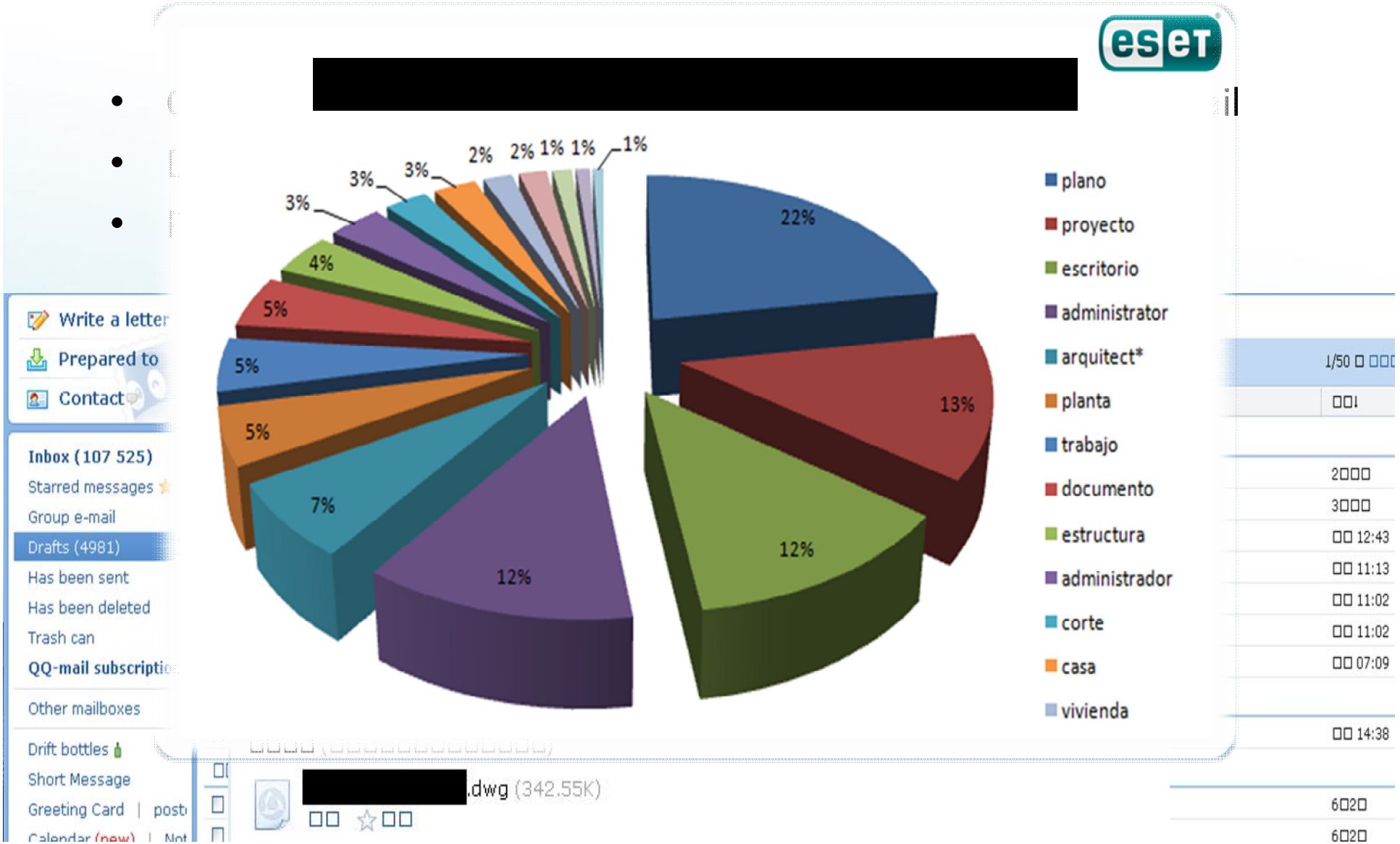
- Napísaný v AutoLISPe, postihuje projekty AutoCAD

Funkcionality:

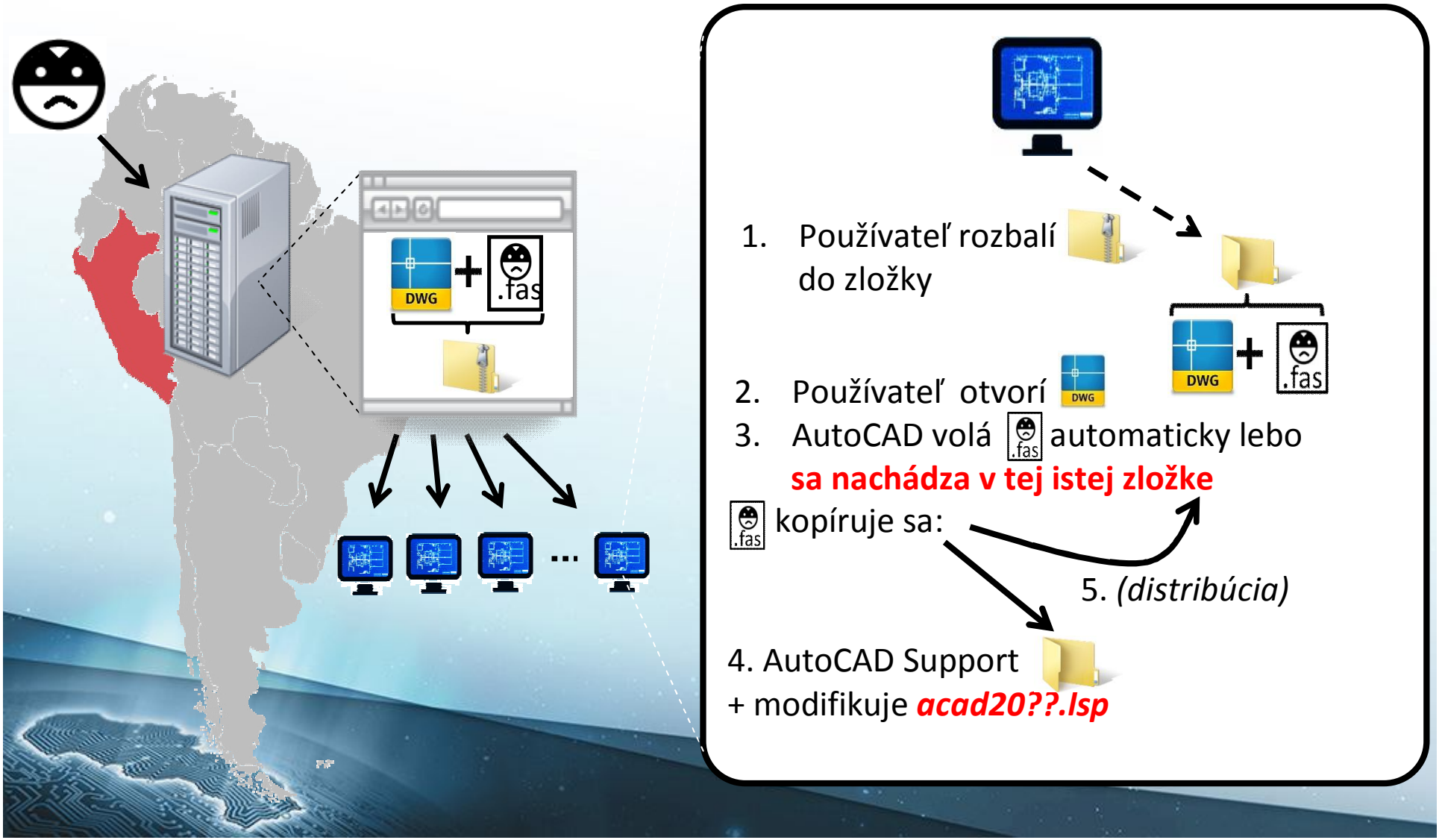
- Kopírovanie – “inštalácia” a distribúcia
- Kradnutie AutoCADových projektov z napadnutých systémov

Kradnutie dát...

- [redacted]
-
-



Infikovanie a inštalácia



Ďalšie podniknuté akcie…

Po objavení sme kontaktovali:

- AutoDesk
- Čínskeho prevádzkovateľa e-mailu
- Peruánske organizácie

Vytvorili sme Stand-alone cleaner

Zhrnutie

- Zmeny v PREČO? a AKO? vytvárania a šírenia malware
- Príklady zo sveta a od nás:
    - Bankové trojany
    - Ransomware
    - Priemyslená špionáž? – ACAD/Medre

Čo s tým?

- Bežný používateľ
- Priemysel
- Vládne zložky

http://www.eset.com/sk/firmy/services/

Ďakujem za pozornosť!

Peter Stančík

stancik@eset.sk