Сучасні цільові атаки

Владислав Радецький

Technical Lead, CEH

whoami

З 2011 працюю в групі компаній БАКОТЕК®.

Координую технічну підтримку проектів ІБ.

Проводжу тренінги, пишу статті, часто колупаю віруси.

Спеціалізація – захист даних та безпека кінцевих точок.

У січні 2015 почав приймати участь у розслідуванні атак.

https://radetskiy.wordpress.com

https://ua.linkedin.com/in/vladislav-radetskiy-80940547

“Звичайні” кібератаки

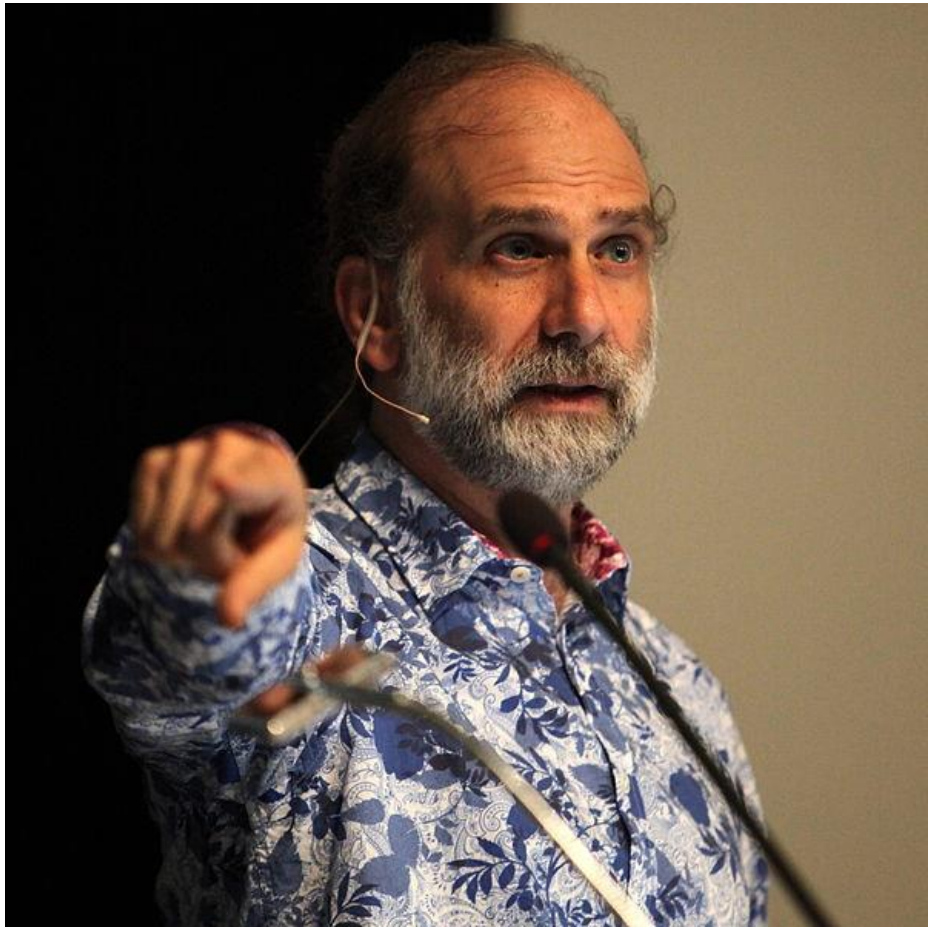
Їх результат жертва відчуває одразу

Цільові атаки

У 90% залишаються непоміченими *

Результати можуть проявитися через кілька тижнів (місяців).

Ключовий елемент – людський фактор



Only amateurs attack machines; professionals target people.

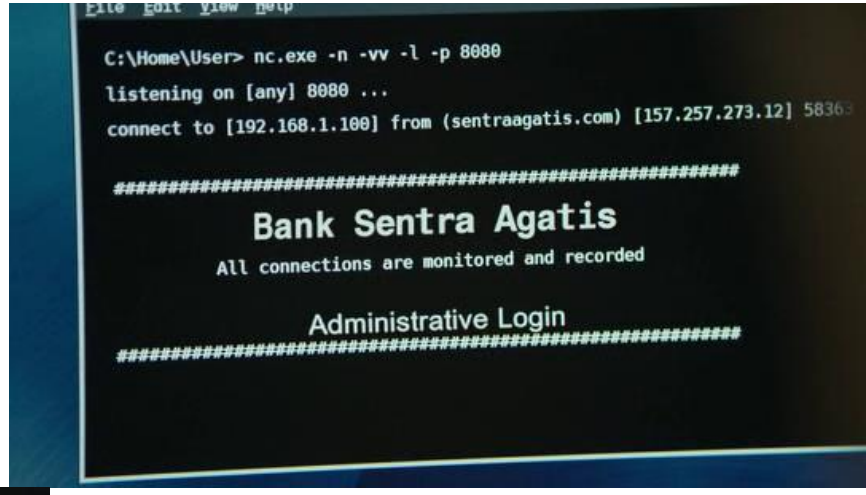
Bruce Schneier

Приклад з кіно

Прохання роздрукувати зіпсований документ. Хіба справжній джентльмен відмовить леді ?

Приклад з кіно

Флешка містила reverse shell, який дозволив віддалене керування скомпрометованою системою



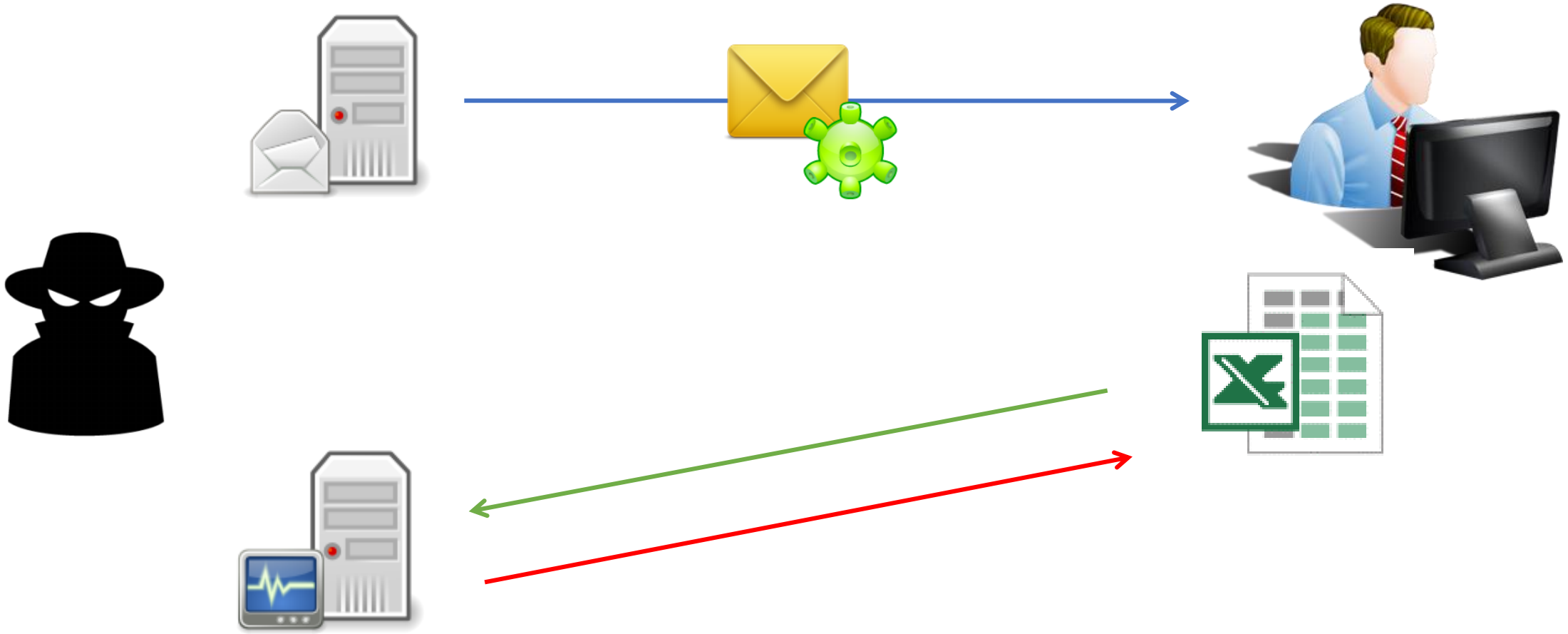
Порушення політики ІБ

Наслідки

Словничок

- Соціальна інженерія – маніпуляція людською свідомістю
- Фішинг – розсилка “фейкових” листів
- Dropper – приманка яку повинен запустити користувач
- Payload – основна частина шкідливого коду
- C&C – сервер контролю та керування

Типова схема атак через email



* Цільові атаки не обмежуються каналом пошти!

Далі будуть зразки того, що проходило через мої руки.

Спроби атак на критичні об'єкти

- 23 грудня 2015 енергетика/макроси (**BlackEnergy**)

Спроби атак на критичні об'єкти

- 23 грудня 2015 енергетика/макроси (**BlackEnergy**)
- 19 січня 2016 енергетика/макроси (**RAT, Sandworm**)
- 1 лютого 2016 широкий спектр/.exe (**ZBot/ZeuS**)
- 4 лютого 2016 широкий спектр/макроси (**Dridex**)
- 3 березня 2016 енергетика / RTF + RCE (**ransomware**)

Спроби атак на критичні об'єкти

- 23 грудня 2015 енергетика/макроси (**BlackEnergy**)
- 19 січня 2016 енергетика/макроси (**RAT, Sandworm**)
- 1 лютого 2016 широкий спектр/.exe (**ZBot/ZeuS**)
- 4 лютого 2016 широкий спектр/макроси (**Dridex**)
- 3 березня 2016 енергетика / RTF + RCE (**ransomware**)

Sandworm, BlackEnergy (BE)

From: Міністерство промислової політики України <info@industry.gov.ua>
To: [redacted]
Subject: Рекомендації з безпеки
Organization: Міністерство промислової політики України

У зв'язку з виявленням небезпечної уразливості у серверах, на яких працюють поштові служби та сайти державних органів влади усім співробітникам потрібно змінити паролі до пошти та інших служб.

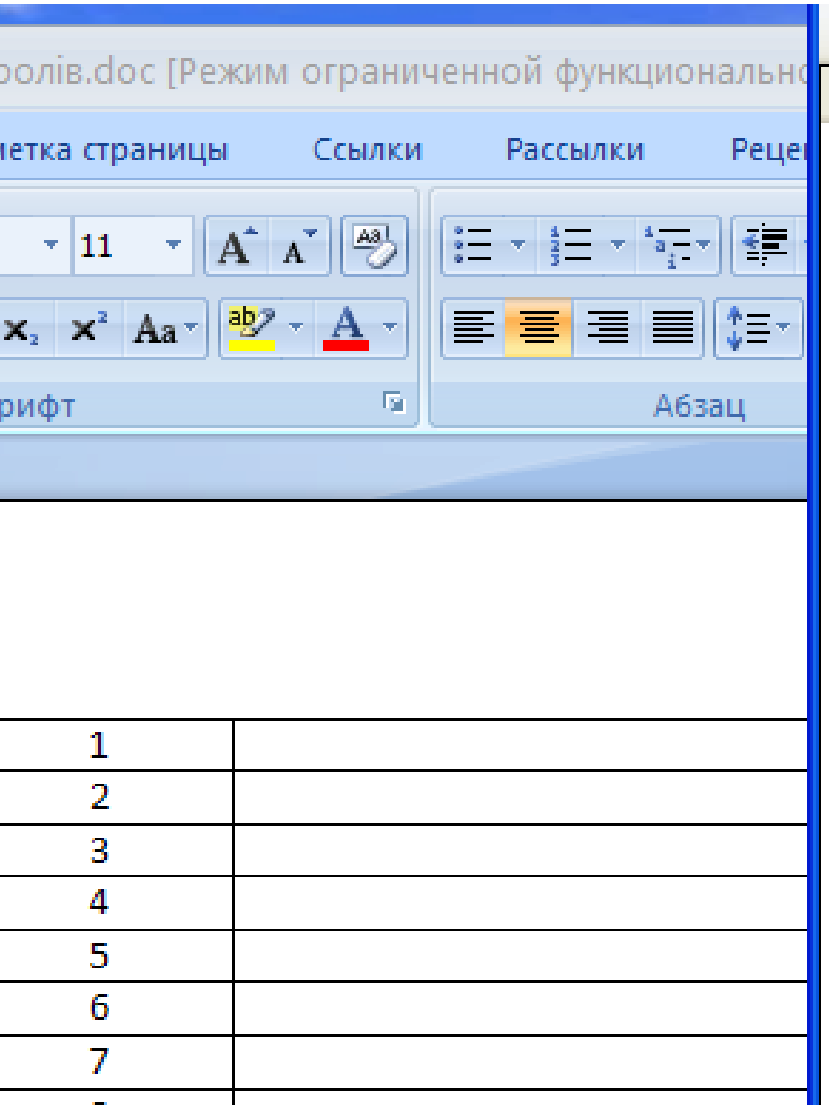
У додатку список з небезпечними паролями. Якщо Ви знайшли свій пароль у цьому списку, його треба змінити.

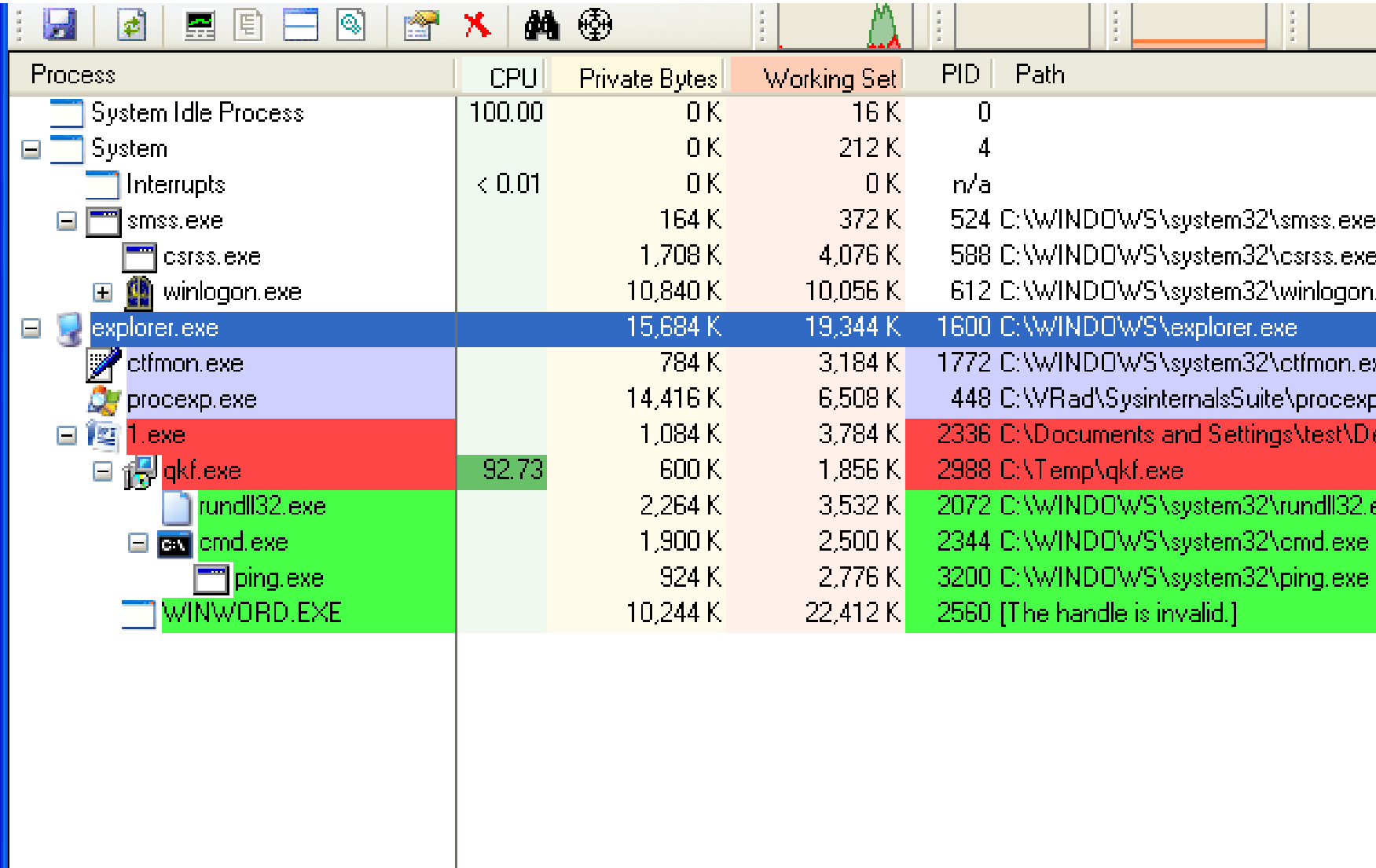
Відділ інформаційної безпеки
Міністерства промислової політики України

03035, м. Київ,
вул. Сурикова, 3
+380 (44) 245-4778
+380 (44) 246-3220

[список паролів.zip application/x-zip-compressed (90121 bytes)]

Sandworm, BlackEnergy (BE)





Розсилка 19-го січня

Wed 1/20/2016 8:20 AM

[redacted]

УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025

To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

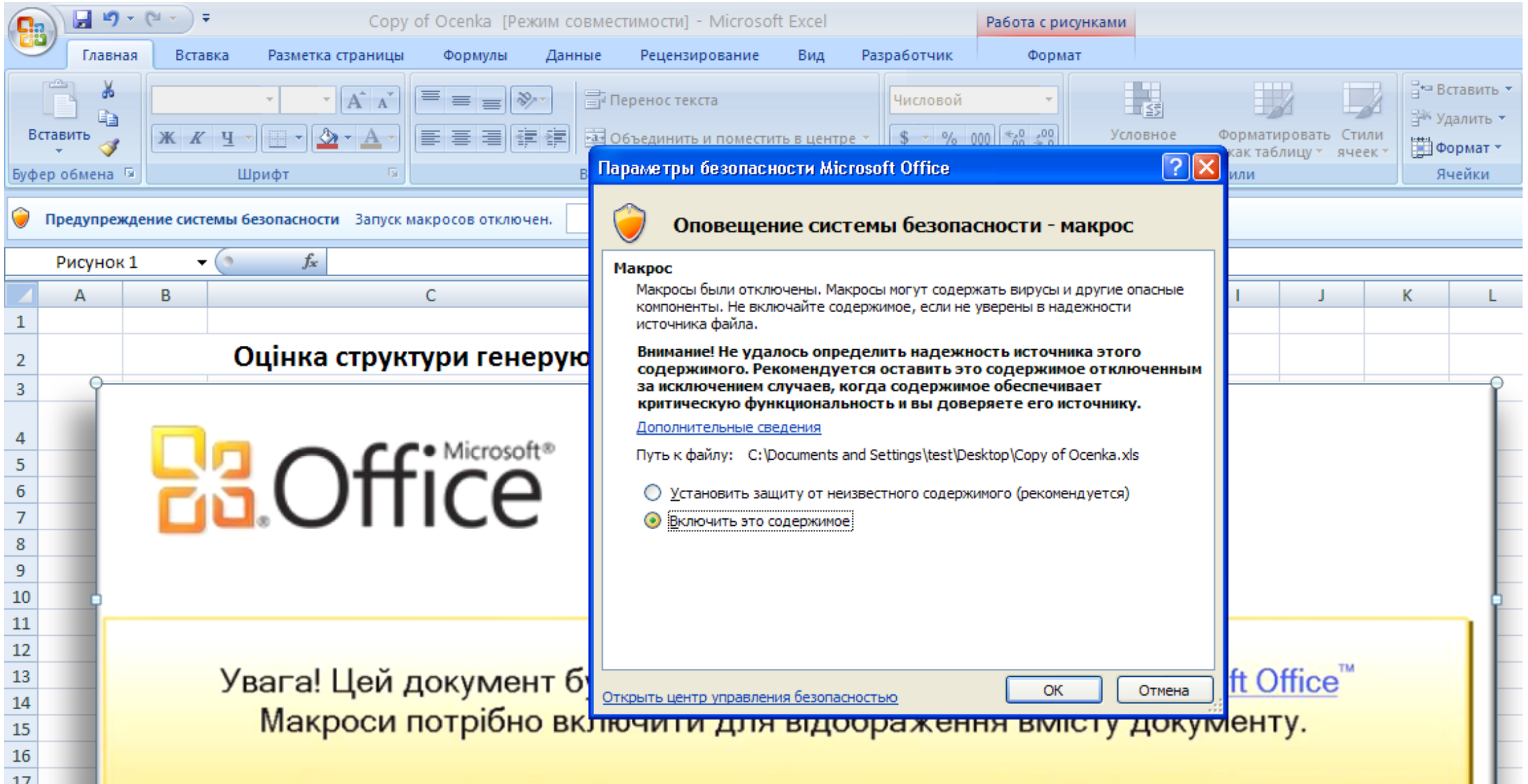
Message Ocenka.xls (816 KB)

Відповідно до положень Закону України «Про засади функціонування ринку електричної енергії України» та «Порядку підготовки Системним оператором плану розвитку Об'єднаної енергетичної системи України на наступні десять років», затвердженого наказом Міністерства енергетики та вугільної промисловості України від 29.09.2014 № 680, системним оператором було розроблено та розміщено на офіційному сайті компанії проект «Плану розвитку ОЕС України на 2016 – 2025 роки».

Проект Плану розвитку знаходиться в додатку до листа.

На виконання пункту 5 положення Порядку підготовки 20 січня 2016 року о 14-00 в адміністративному приміщенні ПС 750 кВ «Київська» (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б) будуть проводитись громадські обговорення та консультації щодо проекту Плану розвитку.

Розсилка 19-го січня



Розсилка 19-го січня

explorer.exe	17,600 K	19,844 K	1600	C:\WINDOWS\explorer.exe
VBoxTray.exe	1,516 K	4,260 K	1684	C:\WINDOWS\system32\VBoxTray.exe
jusched.exe	2,136 K	4,412 K	1764	C:\Program Files\Common Files\Java\Java Update\jusched.exe
ctfmon.exe	784 K	3,160 K	1772	C:\WINDOWS\system32\ctfmon.exe
Autoruns.exe	22,780 K	27,640 K	3768	C:\VRad\SysinternalsSuite\Autoruns.exe
procexp.exe	15,260 K	8,096 K	3772	C:\VRad\SysinternalsSuite\procexp.exe
Procmon.exe	5,912 K	9,280 K	4064	C:\VRad\SysinternalsSuite\Procmon.exe
Tcpview.exe	1,980 K	5,928 K	804	C:\VRad\SysinternalsSuite\Tcpview.exe
EXCEL.EXE	20,056 K	37,772 K	2012	C:\Program Files\Microsoft Office2007\Office12\EXCEL.EXE
test_vb.exe	1,136 K	4,280 K	268	C:\Temp\test_vb.exe

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
test_vb.exe	3480	TCP	10.0.2.15	1420	193.239.152.131	80	ESTABLISH

Розсилка 1-го лютого

Пн 01.02.2016 14:52

ДП "Изюминка" <sales@aerocredo.ru>

документы по оформлению

To [redacted]

This message was sent with High importance.

Message | сканы.zip (770 KB)

ПАСПОРТ.exe

Добрий день. відправляю вам документи для оформлення довіреностей.
З повагою Фролова Тетяна
ДП "Изюминка"
044-783-22-56


scan.jpg

Розсилка 1-го лютого


passport.jpg

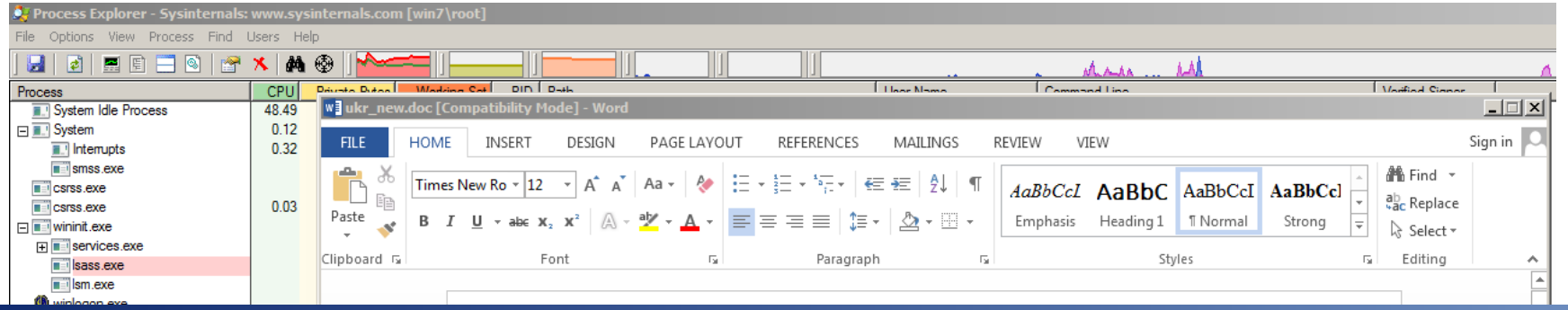

scan.jpg

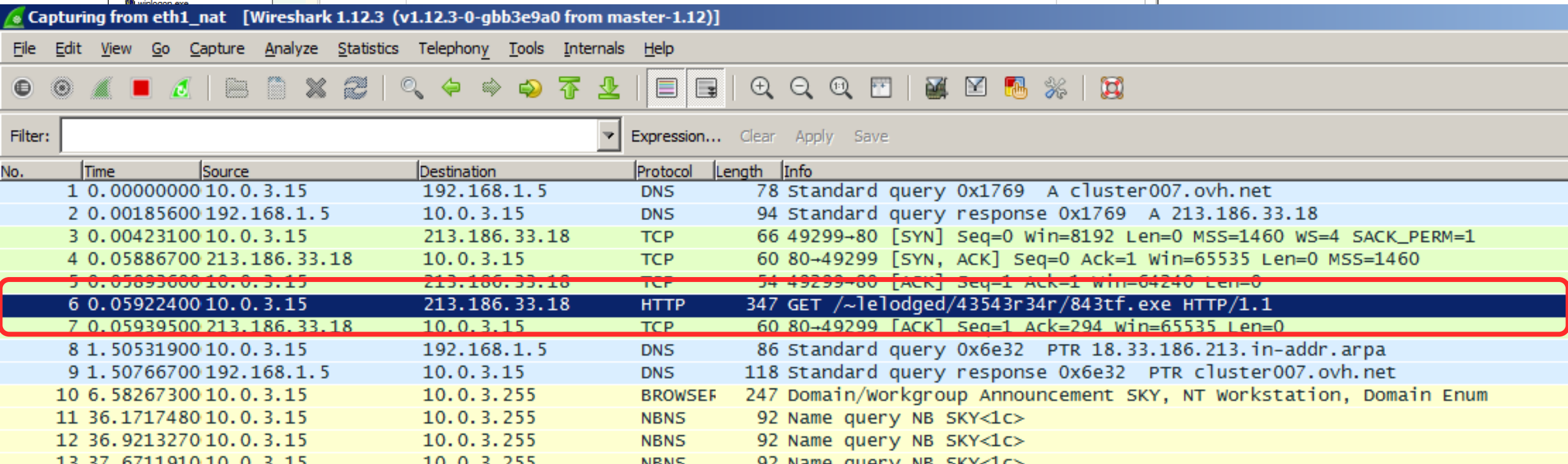

winrar.exe

Розсилка 1-го лютого

System Idle Process	27.10	0 K	24 K	0	NT AUTHORITY\...	
System	0.92	128 K	612 K	4	NT AUTHORITY\...	
Interrupts	3.93	0 K	0 K	n/a		
smss.exe		440 K	1,092 K	280	NT AUTHORITY\...	\SystemRoot\System32\sms
csrss.exe		1,944 K	4,072 K	380	NT AUTHORITY\...	%SystemRoot%\system32\c
wininit.exe		1,488 K	4,404 K	416	NT AUTHORITY\...	wininit.exe
services.exe		4,820 K	8,716 K	512	NT AUTHORITY\...	C:\Windows\system32\serv
lsass.exe	0.01	4,104 K	11,352 K	520	NT AUTHORITY\...	C:\Windows\system32\lsass
lsm.exe		3,064 K	5,700 K	528	NT AUTHORITY\...	C:\Windows\system32\lsm.e
csrss.exe	0.01	2,096 K	5,212 K	428	NT AUTHORITY\...	%SystemRoot%\system32\c
winlogon.exe		2,808 K	6,976 K	456	NT AUTHORITY\...	winlogon.exe
explorer.exe	0.06	50,416 K	54,916 K	2456	win7\root	C:\Windows\Explorer.EXE
VBoxTray.exe		1,696 K	5,008 K	2596	win7\root	"C:\Windows\System32\VB
procexp.exe		2,512 K	6,716 K	1876	win7\root	"D:\VRad\SysinternalsSuite
procexp64.exe	1.16	23,124 K	33,512 K	1212	win7\root	"D:\VRad\SysinternalsSuite
Tcpview.exe	0.04	6,876 K	12,032 K	688	win7\root	"D:\VRad\SysinternalsSuite
Procmon.exe		6,184 K	9,236 K	3420	win7\root	"D:\VRad\SysinternalsSuite
Procmon64.exe	6.36	20,896 K	47,080 K	3456	win7\root	"C:\Users\ROOT~1.WIN\A
pasport.exe	0.04	3,208 K	10,460 K	3596	win7\root	"C:\Users\root.win7\Deskto
winrar.exe	4.11	5,836 K	10,044 K	3624	win7\root	"C:\Users\root.win7\Deskto

Розсилка 4-го лютого





Розсилка 3-го березня

Чт 03.03.2016 8:48

[redacted] <samobratov.e@[redacted]>

Документы

To [redacted]

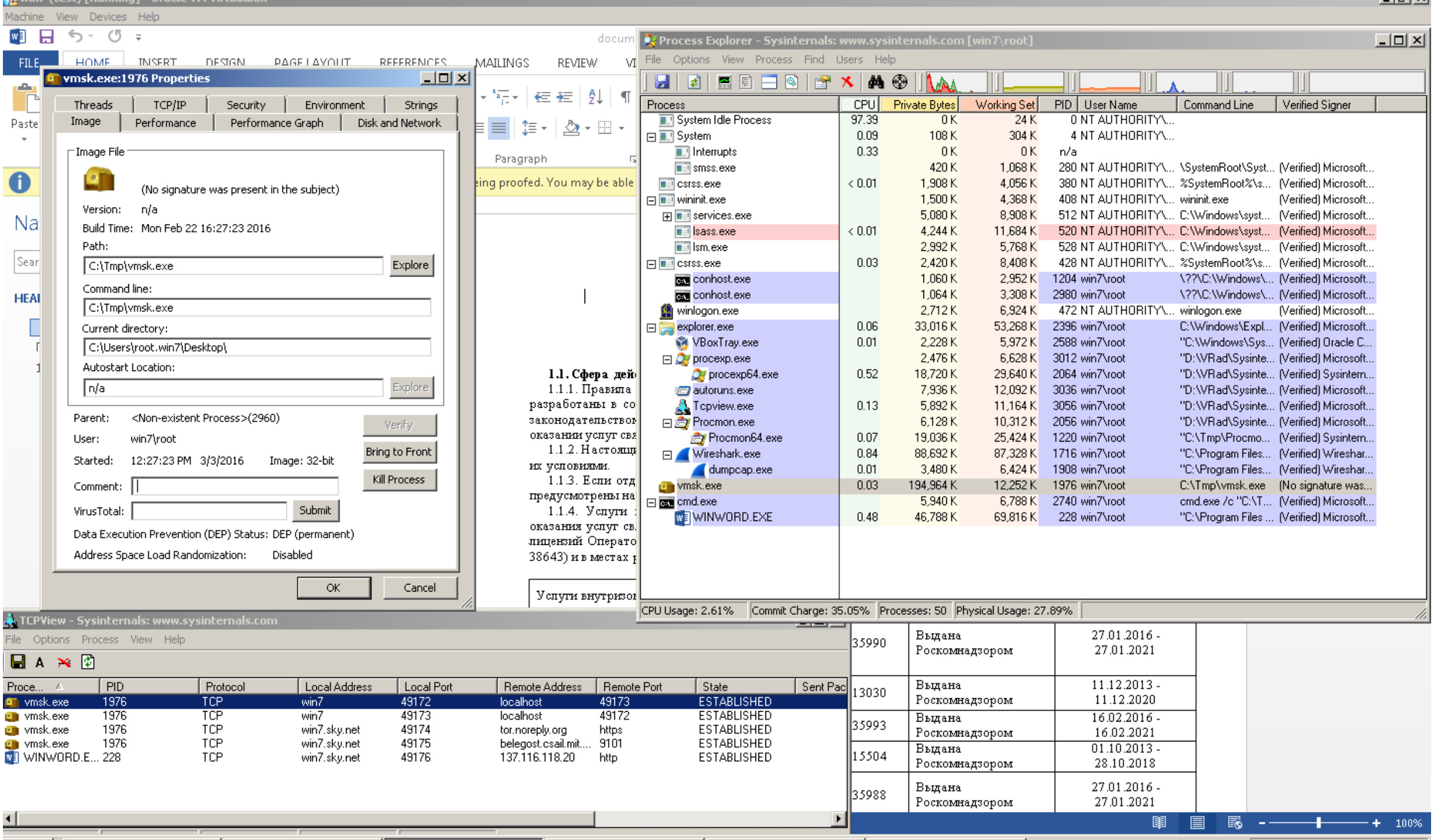
You forwarded this message on 03.03.2016 10:12.

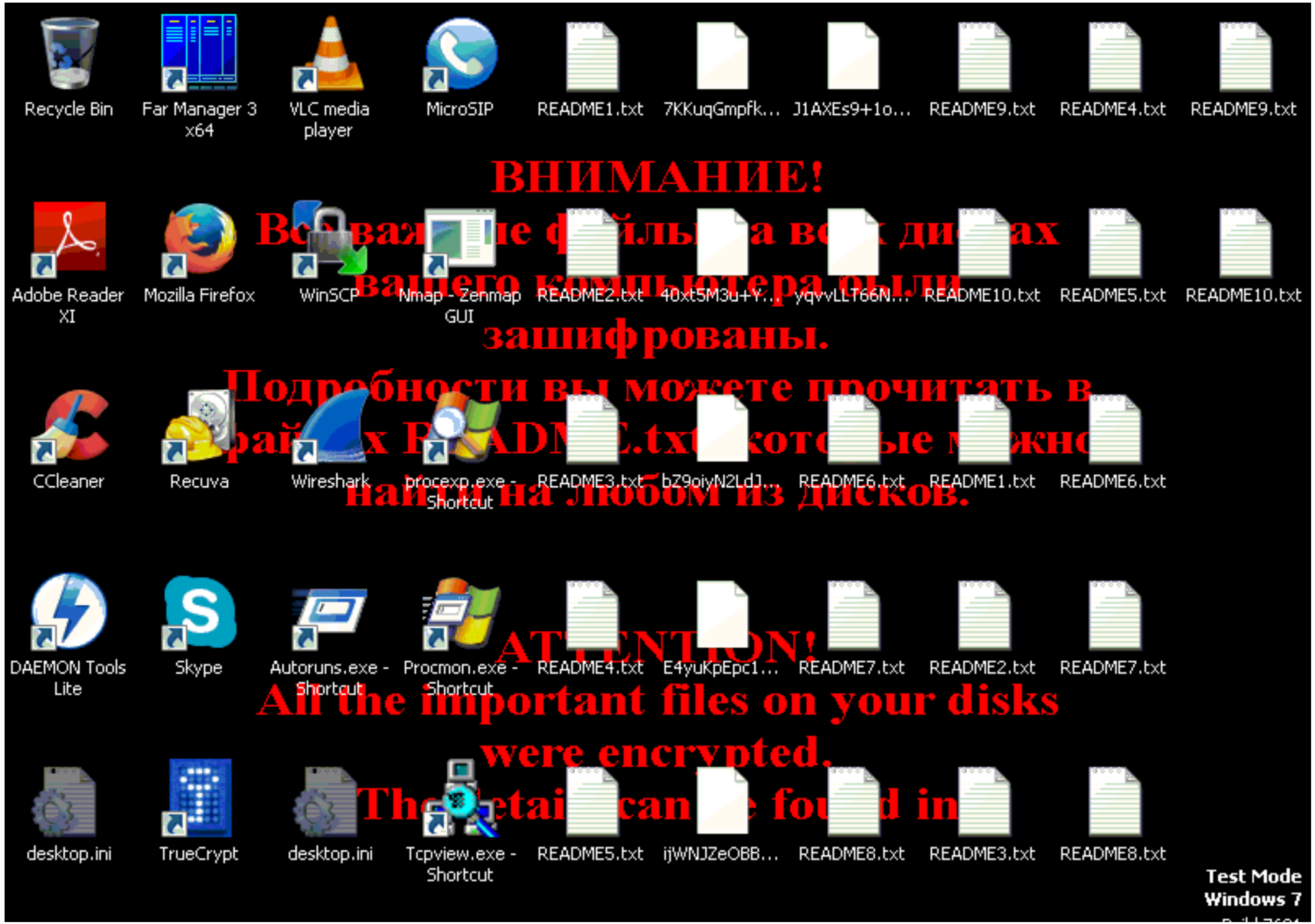
Message schet[redacted].doc (1 MB)

Здравствуйте!

В связи с изменениями в тарифных планах мы переделали платежные документы.
Новый счет во вложенных файлах.

С уважением
Егор Самобратов.
Менеджер компании[redacted]


vmsk.exe:1976 Properties
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
Disk and Network
Image File
(No signature was present in the subject)
Version: n/a
Build Time: Mon Feb 22 16:27:23 2016
Path:
C:\Tmp\vmsk.exe
Explore
Command line:
C:\Tmp\vmsk.exe
Current directory:
C:\Users\root.win7\Desktop\
Autostart Location:
n/a
Explore
Parent: <Non-existent Process>(2960)
User: win7\root
Started: 12:27:23 PM 3/3/2016 Image: 32-bit
Comment:
VirusTotal:
Submit
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: DEP (permanent)
Address Space Load Randomization: Disabled
OK
Cancel
Process Explorer - Sysinternals: www.sysinternals.com [win7\root]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID User Name Command Line Verified Signer
System Idle Process 97.39 0 K 24 K 0 NT AUTHORITY\...
System 0.09 108 K 304 K 4 NT AUTHORITY\...
Interrupts 0.33 0 K 0 K n/a
smss.exe 420 K 1,068 K 280 NT AUTHORITY\... \SystemRoot\Syst... (Verified) Microsoft...
csrss.exe < 0.01 1,908 K 4,056 K 380 NT AUTHORITY\... %SystemRoot%\s... (Verified) Microsoft...
wininit.exe 1,500 K 4,368 K 408 NT AUTHORITY\... wininit.exe (Verified) Microsoft...
services.exe 5,080 K 8,908 K 512 NT AUTHORITY\... C:\Windows\syst... (Verified) Microsoft...
lsass.exe < 0.01 4,244 K 11,684 K 520 NT AUTHORITY\... C:\Windows\syst... (Verified) Microsoft...
lsm.exe 2,992 K 5,768 K 528 NT AUTHORITY\... C:\Windows\syst... (Verified) Microsoft...
csrss.exe 0.03 2,420 K 8,408 K 428 NT AUTHORITY\... %SystemRoot%\s... (Verified) Microsoft...
conhost.exe 1,060 K 2,952 K 1204 win7\root \??\C:\Windows\... (Verified) Microsoft...
conhost.exe 1,064 K 3,308 K 2980 win7\root \??\C:\Windows\... (Verified) Microsoft...
winlogon.exe 2,712 K 6,924 K 472 NT AUTHORITY\... winlogon.exe (Verified) Microsoft...
explorer.exe 0.06 33,016 K 53,268 K 2396 win7\root C:\Windows\Expl... (Verified) Microsoft...
VBoxTray.exe 0.01 2,228 K 5,972 K 2588 win7\root "C:\Windows\Sys... (Verified) Oracle C...
procexp.exe 2,476 K 6,628 K 3012 win7\root "D:\VRad\Sysinte... (Verified) Microsoft...
procexp64.exe 0.52 18,720 K 29,640 K 2064 win7\root "D:\VRad\Sysinte... (Verified) Sysintern...
autoruns.exe 7,936 K 12,092 K 3036 win7\root "D:\VRad\Sysinte... (Verified) Microsoft...
Tcpview.exe 0.13 5,892 K 11,164 K 3056 win7\root "D:\VRad\Sysinte... (Verified) Microsoft...
Procmon.exe 6,128 K 10,312 K 2056 win7\root "D:\VRad\Sysinte... (Verified) Microsoft...
Procmon64.exe 0.07 19,036 K 25,424 K 1220 win7\root "C:\Tmp\Procmo... (Verified) Sysintern...
Wireshark.exe 0.84 88,692 K 87,328 K 1716 win7\root "C:\Program Files... (Verified) Wireshar...
dumpcap.exe 0.01 3,480 K 6,424 K 1908 win7\root "C:\Program Files... (Verified) Wireshar...
vmsk.exe 0.03 194,964 K 12,252 K 1976 win7\root C:\Tmp\vmsk.exe (No signature was...
cmd.exe 5,940 K 6,788 K 2740 win7\root cmd.exe /c "C:\T... (Verified) Microsoft...
WINWORD.EXE 0.48 46,788 K 69,816 K 228 win7\root "C:\Program Files ... (Verified) Microsoft...
CPU Usage: 2.61% Commit Charge: 35.05% Processes: 50 Physical Usage: 27.89%
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Proce... PID Protocol Local Address Local Port Remote Address Remote Port State Sent Pac
vmsk.exe 1976 TCP win7 49172 localhost 49173 ESTABLISHED
vmsk.exe 1976 TCP win7 49173 localhost 49172 ESTABLISHED
vmsk.exe 1976 TCP win7.sky.net 49174 tor.noreply.org https ESTABLISHED
vmsk.exe 1976 TCP win7.sky.net 49175 belegost.csail.mit.... 9101 ESTABLISHED
WINWORD.E... 228 TCP win7.sky.net 49176 137.116.118.20 http ESTABLISHED
35990 Выдана Роскомнадзором 27.01.2016 - 27.01.2021
13030 Выдана Роскомнадзором 11.12.2013 - 11.12.2020
35993 Выдана Роскомнадзором 16.02.2016 - 16.02.2021
15504 Выдана Роскомнадзором 01.10.2013 - 28.10.2018
35988 Выдана Роскомнадзором 27.01.2016 - 27.01.2021
100%


Recycle Bin
Far Manager 3 x64
VLC media player
MicroSIP
README1.txt
7KKuqGmpfk...
J1AXEs9+1o...
README9.txt
README4.txt
README9.txt
ВНИМАНИЕ!
Все важные файлы на всех дисках
вашего компьютера были
зашифрованы.
Подробности вы можете прочитать в
файлах README.txt, которые можно
найти на любом из дисков.
Adobe Reader XI
Mozilla Firefox
WinSCP
Nmap - Zenmap GUI
README2.txt
40xt5M3u+Y...
yqvvLLT66N...
README10.txt
README5.txt
README10.txt
CCleaner
Recuva
Wireshark
procexp.exe - Shortcut
README3.txt
bZ9oiyN2LdJ...
README6.txt
README1.txt
README6.txt
ATTENTION!
All the important files on your disks
were encrypted.
The details can be found in
DAEMON Tools Lite
Skype
Autoruns.exe - Shortcut
Procmon.exe - Shortcut
README4.txt
E4yuKpEpc1...
README7.txt
README2.txt
README7.txt
desktop.ini
TrueCrypt
desktop.ini
Tcpview.exe - Shortcut
README5.txt
ijWNJZeOBB...
README8.txt
README3.txt
README8.txt
Test Mode
Windows 7

Одна із небезпек таких атак – сигнатурний аналіз не забезпечує достатній рівень захисту.

.XLS та .EXE – **24 години** після розсилки

virustotal

SHA256: 0bb5e98f77e69d85bf5068bcbc5b5876f8e5855d34d9201d1caffbf83460cccc

File name: Ocenka.xls

Detection ratio: 5 / 54

Analysis date: 2016-01-20 08:45:25 UTC (0 minutes ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Arcabit	HEUR.VBA.Trojan	20160120
Avast	VBA:Downloader-AAH [Trj]	20160120
CAT-QuickHeal	X97M.Dropper.RO	20160119
Qihoo-360	heur.macro.drop.c	20160120
VIPRE	Trojan-Downloader.O97M.Donoff.d (v)	20160120
ALYac	✓	20160120
AVG	✓	20160120
Ad-Aware	✓	20160120
AegisLab	✓	20160120
Agnitum	✓	20160119
AhnLab-V3	✓	20160119
Alibaba	✓	20160120
Antiy-AVL	✓	20160120
Avira	✓	20160120
Baidu-International	✓	20160119
BitDefender	✓	20160120

virustotal

SHA256: 43b69a81693488905ef655d22e395c3f8dee2486aba976d571d3b12433d10c93

File name: test_vb.exe

Detection ratio: 4 / 53

Analysis date: 2016-01-20 11:21:18 UTC (0 minutes ago)

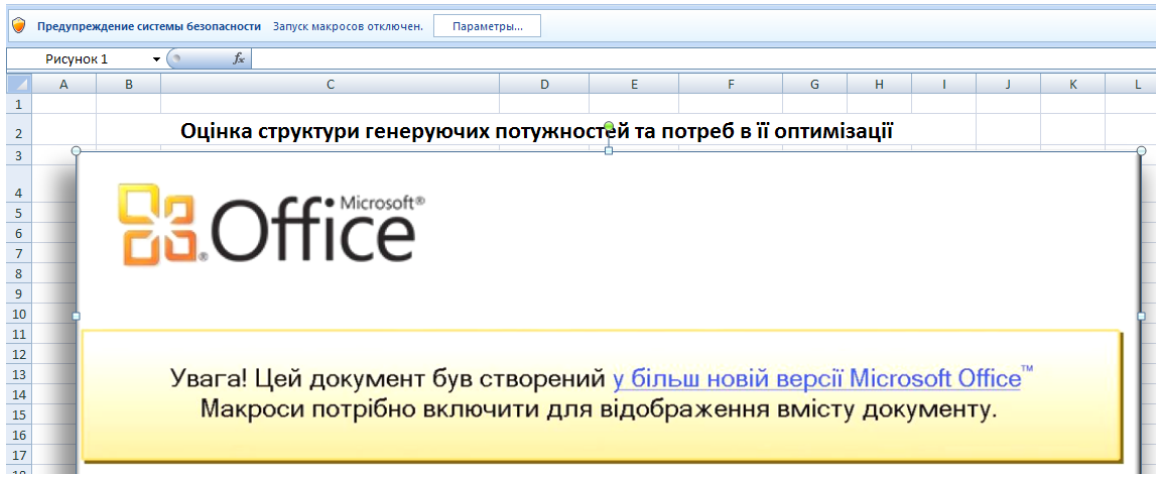
Analysis | File detail | Additional information | Comments | Votes | Behavioural information

Antivirus	Result	Update
Avira	TR/Downloader.Gen	20160120
Bkav	W32.eHeur.Downloader	20160119
McAfee-GW-Edition	BehavesLike.Win32.Multiplug.qm	20160120
Qihoo-360	HEUR/QVM10.1.Malware.Gen	20160120
ALYac	✓	20160120
AVG	✓	20160120
Ad-Aware	✓	20160120
AegisLab	✓	20160120
Agnitum	✓	20160119
AhnLab-V3	✓	20160119
Alibaba	✓	20160120
Antiy-AVL	✓	20160120
Arcabit	✓	20160120
Avast	✓	20160120

.XLS та .EXE – **24 години** після розсилки

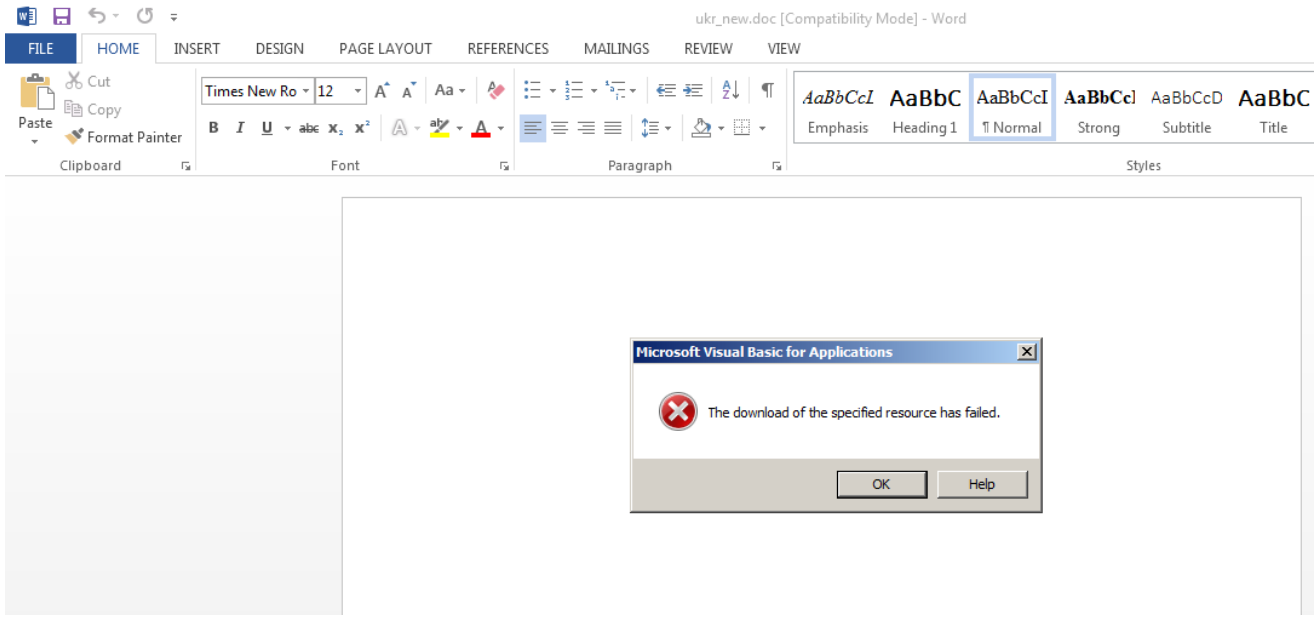
Трохи аналітики

19-го січня



Розсилка була виключно по енергетикам.
Був претекст і сам файл містив прохання.

4-го лютого

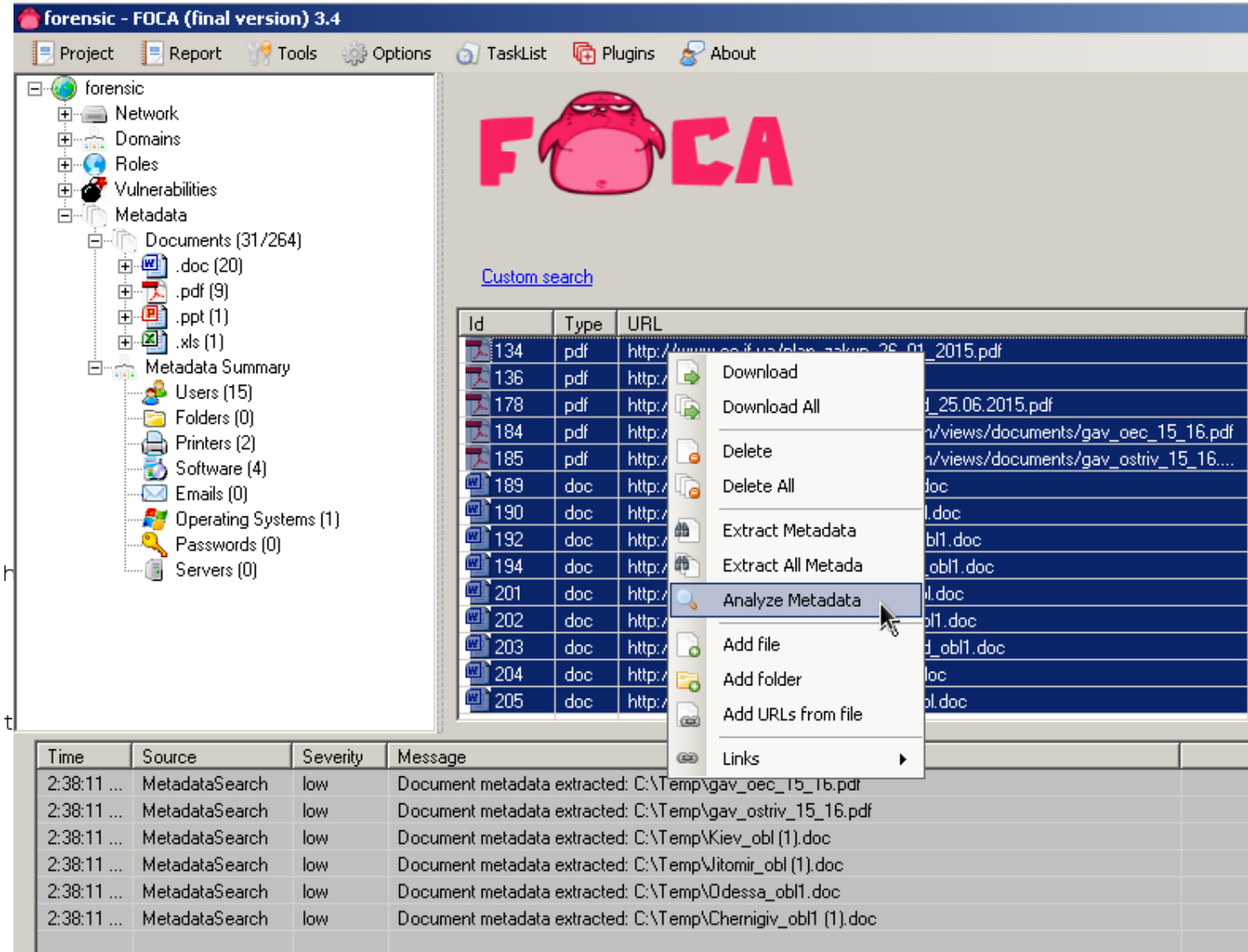


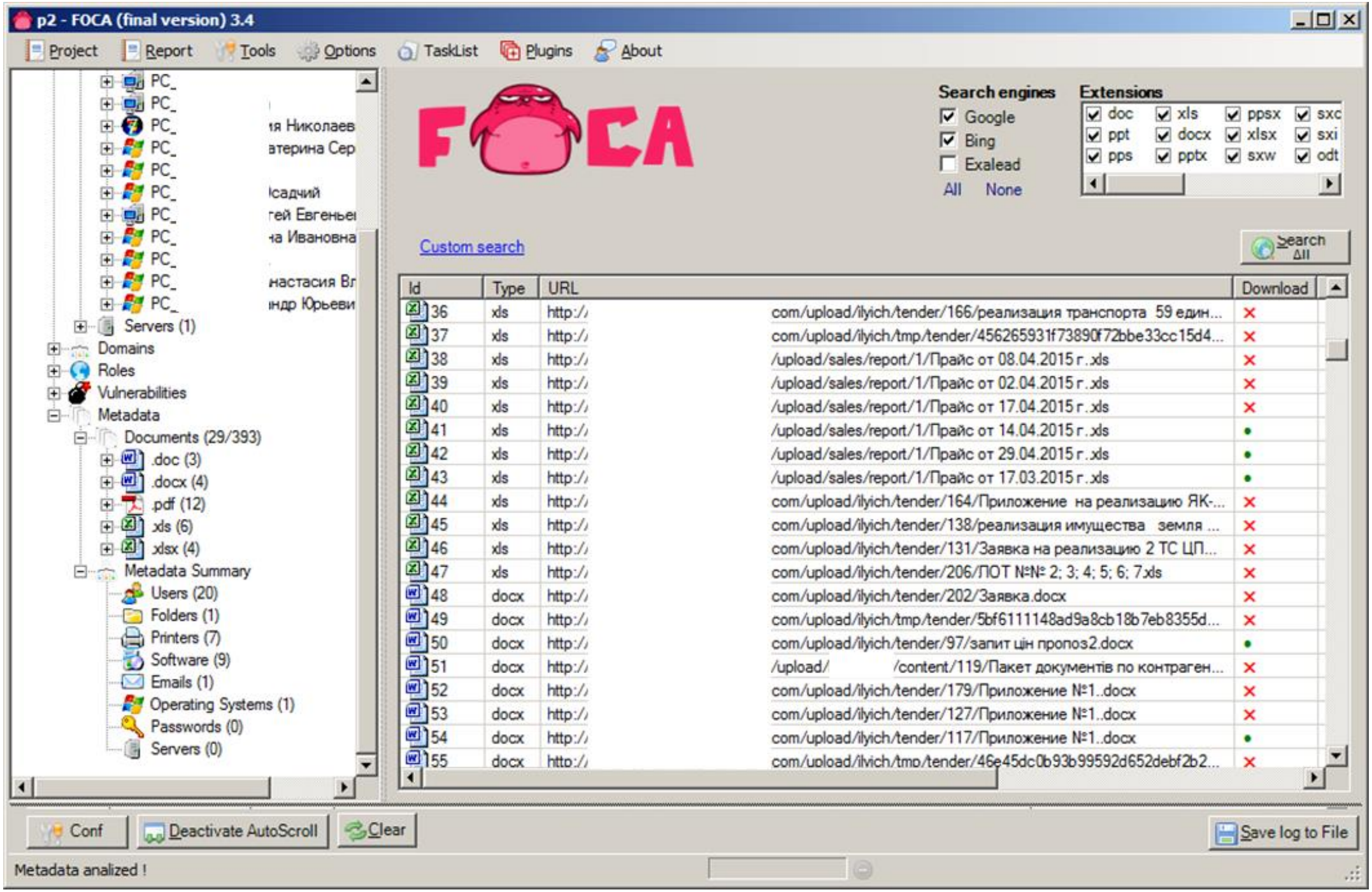
Розсилка була загальною (по держ. установам)
Файл містив макрос без прохання.

Як жертви допомагають нападникам (або про незачинені двері…)

OSINT, метаінформація...

```
*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: google, googleCSE, bing, bingapi, pgp
                        linkedin, google-profiles, people123, jigsaw,
                        twitter, googleplus, all

       -s: Start in result number X (default: 0)
       -v: Verify host name via dns resolution and search for virtual h
       -f: Save the results into an HTML and XML file
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 t
       -h: use SHODAN database to query discovered hosts
            google 100 to 100, and pgp doesn't use this option)

Examples:
        theharvester -d microsoft.com -l 500 -b google
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```




p2 - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
Search engines
Google
Bing
Exalead
All
None
Extensions
doc
xls
ppsx
sxc
ppt
docx
xlsx
sxi
pps
pptx
sxw
odt
Custom search
Search All
Id
Type
URL
Download
Servers (1)
Domains
Roles
Vulnerabilities
Metadata
Documents (29/393)
.doc (3)
.docx (4)
.pdf (12)
.xls (6)
.xlsx (4)
Metadata Summary
Users (20)
Folders (1)
Printers (7)
Software (9)
Emails (1)
Operating Systems (1)
Passwords (0)
Servers (0)
Conf
Deactivate AutoScroll
Clear
Save log to File
Metadata analized !

```
VRad@GK17:~$ theharvester -d [redacted].lviv.ua -l 50 -b bing

*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __   *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |     *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Bing:
        Searching 50 results...


[+] Emails found:
------------------
@[redacted].lviv.ua
info@[redacted].lviv.ua
nfo@[redacted].lviv.ua

VRad@GK17:~$ theharvester -d [redacted].lviv.ua -l 50 -b linkedin

[-] Searching in Linkedin..
        Searching 100 results..
Users from Linkedin:
====================
Olena [redacted]
Oleksiy [redacted]
```

Рекомендації

1. Співбесіди з персоналом на тему фішингу та соц. інженерії
2. Періодичні тести на проникнення
3. Жорстка фільтрація пошти (exe, macro, js …)
4. Блок/контроль запуску скриптів та .exe із %temp%
5. Застосування механізмів т.з. “білих списків”
6. Застосування т.з. “пісочниць”
7. Обережність, обачність, зосередженість

Some useful tools

Defense side

- Virustotal
- olevba, peepdf, pdfid, pdfx
- Virtualbox + sysinternals tools + wireshark

Pentest side

- Google dorks, Foca, Maltego, theharvester
- Gophish, macroshop (github), veilevasion
- nmap, amap, masscan, msf

* повний перелік шукайте в методичках

```
VRad@GK17:~/Distrib/samples/26.05.16/oletools-0.46/oletools$ python olevba.py -a clean_table.xls
olevba 0.46 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------
OLE:-------- clean_table.xls
==============================================================================
FILE: clean_table.xls
Type: OLE
No VBA macros found.

VRad@GK17:~/Distrib/samples/26.05.16/oletools-0.46/oletools$ python olevba.py -a fax.docm
olevba 0.46 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------
OpX:MASIHB-- fax.docm
==============================================================================
FILE: fax.docm
Type: OpenXML
------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: u'VBA/ThisDocument'
------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/Module1'
------------------------------------------------------------------------------
VBA MACRO Module2.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/Module2'
------------------------------------------------------------------------------
VBA MACRO Class1.cls
in file: word/vbaProject.bin - OLE stream: u'VBA/Class1'
------------------------------------------------------------------------------
VBA MACRO Module3.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/Module3'
------------------------------------------------------------------------------
VBA MACRO UserForm1.frm
in file: word/vbaProject.bin - OLE stream: u'VBA/UserForm1'
------------------------------------------------------------------------------
```

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
Suspicious	Open	May open a file
Suspicious	Run	May run an executable file or a system command
Suspicious	CreateObject	May create an OLE object
Suspicious	Chr	May attempt to obfuscate specific strings
Suspicious	SaveToFile	May create a text file
Suspicious	Write	May write to a file (if combined with Open)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	http://www.vbforums.com/showthread.php?460464-RESOLVED-is-there-a-method-like-quot-isAlphabetic-quot	URL
IOC	http://stackoverflow.com/questions/275160/regex-for-names	URL
IOC	https://davidcel.is/posts/stop-validating-email-addresses-with-regex/	URL
IOC	http://stackoverflow	URL

Sources

- Vlad Styran slides — slideshare.net/sapran/presentations
- Steven Rambam
  - "Privacy is Dead - Get Over It" (1.08.10 _ HOPE)
  - "Privacy: A Postmortem" (14.07.12 _ HOPE)
  - "… Taking Anonymity" (19.07.14 _ HOPE)
- Paula Januszkiewicz videos — channel9.msdn.com/Events/Speakers/Paula-Januszkiewicz
- Mark Russinovich videos — channel9.msdn.com/Events/Speakers/Mark-Russinovich
- 7 кроків у напрямку безпеки — https://radetskiy.wordpress.com/2015/04/10/7_steps_ua/
- Pentesting_ практика — https://radetskiy.wordpress.com/2015/05/18/pentest2015_practice/

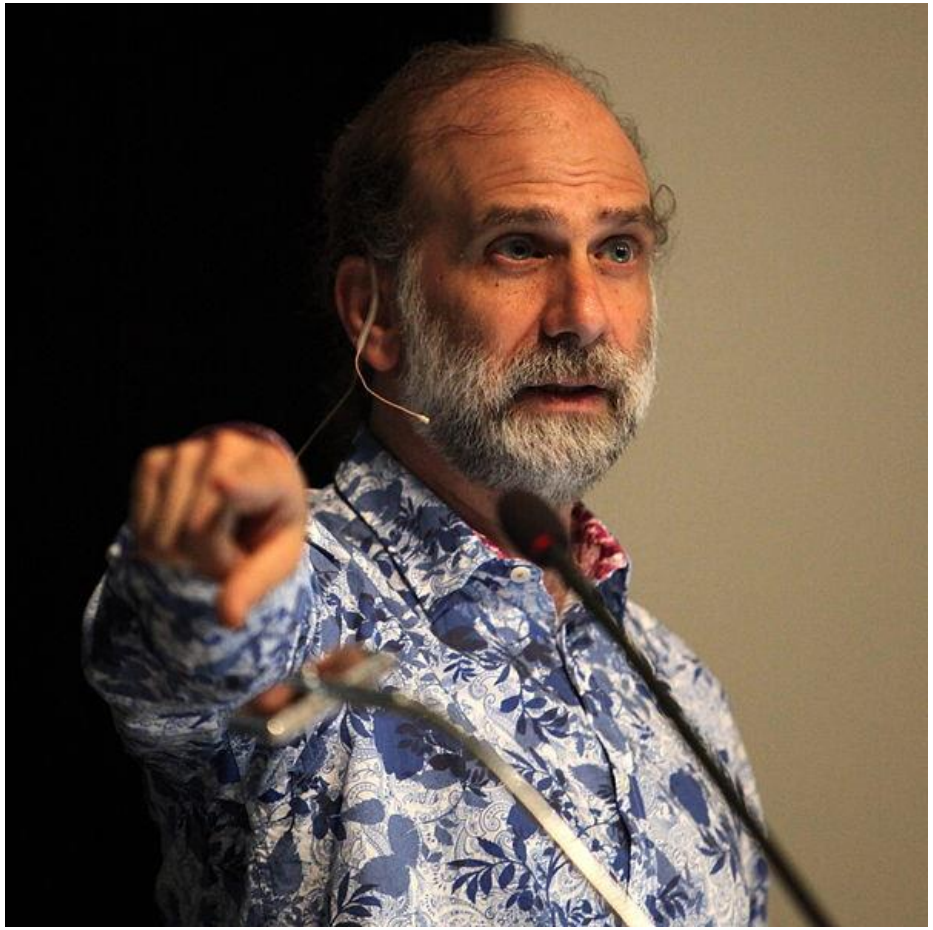
Дякую Вам за увагу!

Владислав Радецький

vr@bakotech.com

radetskiy.wordpress.com

І не забувайте про слова Брюса Шнайєра



Only amateurs attack machines; professionals target people.

Bruce Schneier