

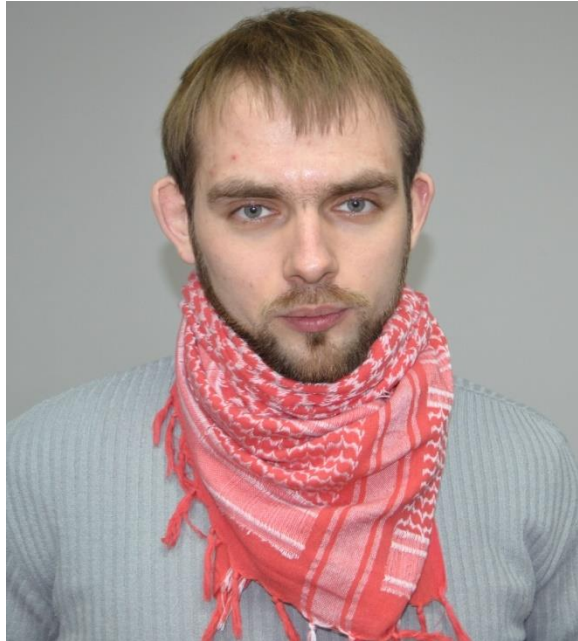


# Сучасні цільові атаки

Владислав Радецький

Technical Lead, СЕН

# 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





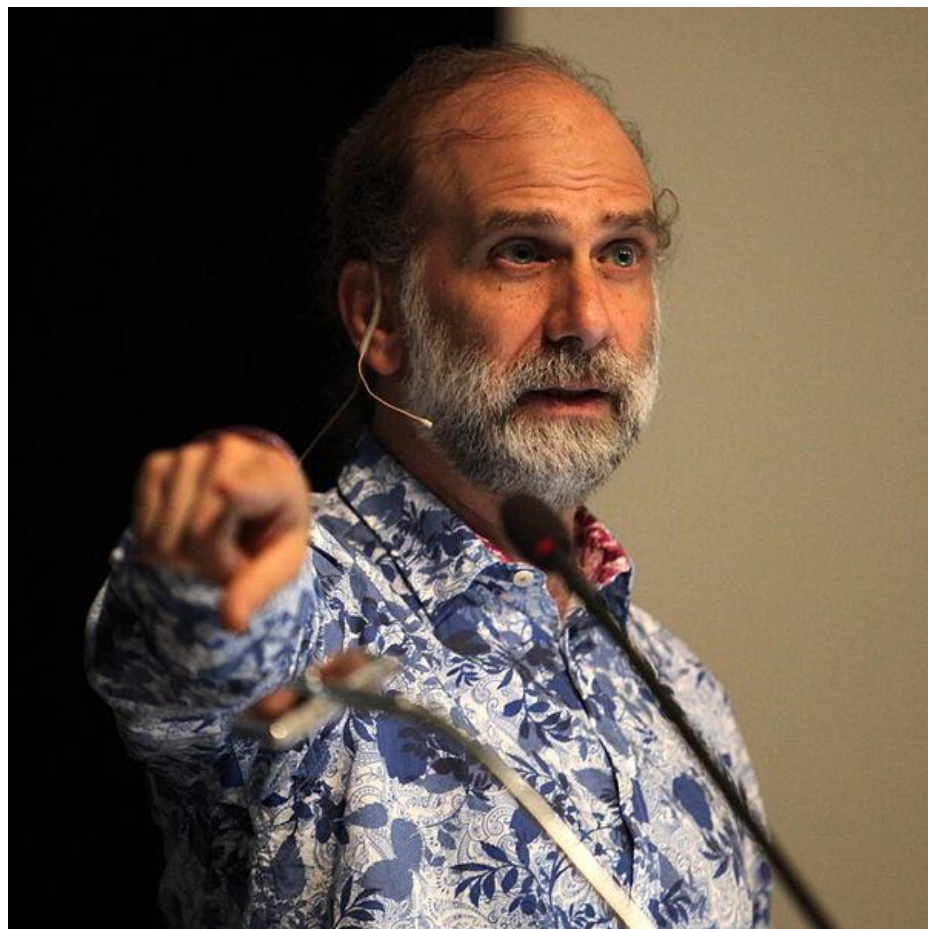
# Цільові атаки

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?**



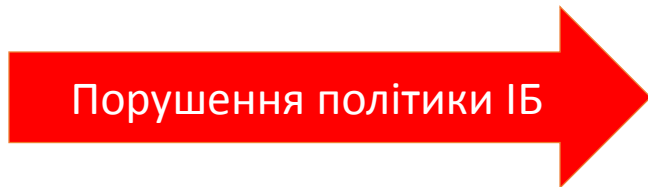


# Приклад з кіно

Флешка містила **reverse shell**, який дозволив віддалене керування скомпрометованою системою



```
File Edit View Help
C:\Home\User> nc.exe -n -vv -l -p 8080
listening on [any] 8080 ...
connect to [192.168.1.100] from (sentraagatis.com) [157.257.273.12] 58363
#####
Bank Sentra Agatis
All connections are monitored and recorded
Administrative Login
#####
```

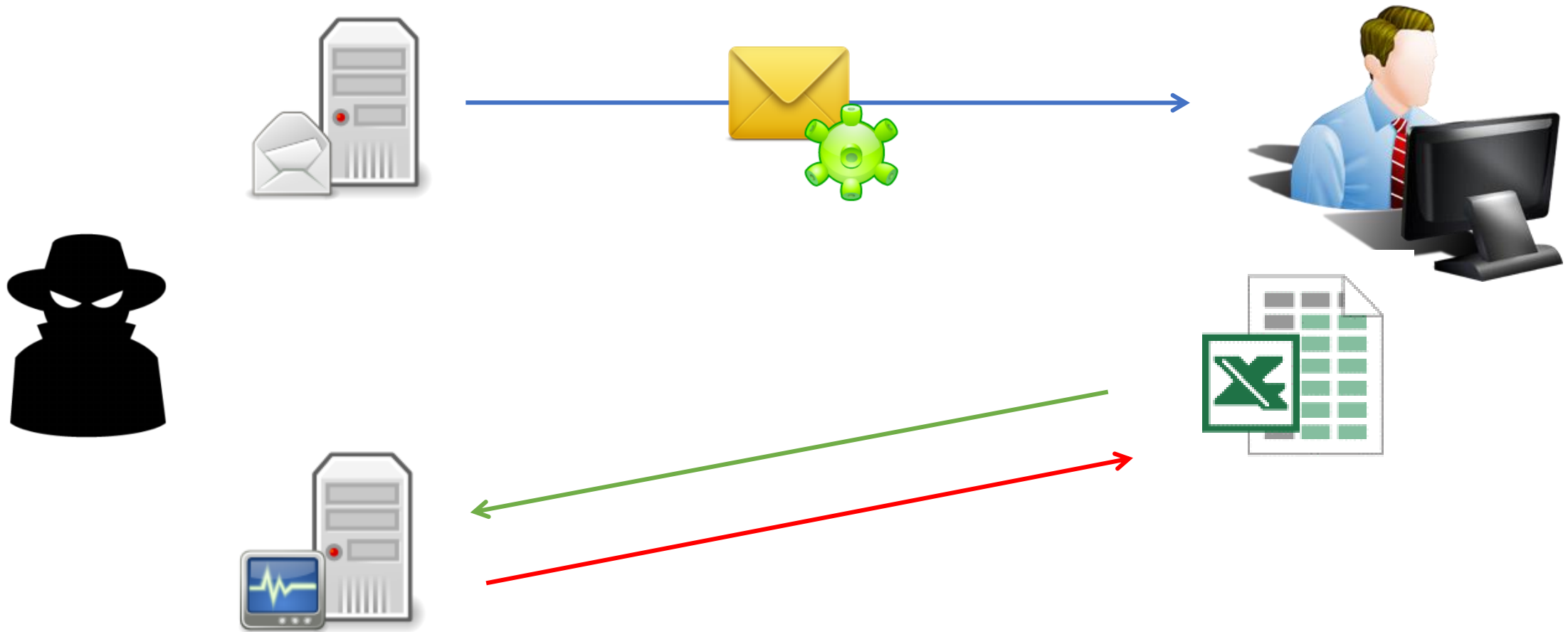


# СЛОВНИЧОК

- 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)

Process	CPU	Private Bytes	Working Set	PID	Path
System Idle Process	100.00	0 K	16 K	0	
System		0 K	212 K	4	
Interrupts	< 0.01	0 K	0 K	n/a	
smss.exe		164 K	372 K	524	C:\WINDOWS\system32\smss.exe
csrss.exe		1,708 K	4,076 K	588	C:\WINDOWS\system32\csrss.exe
winlogon.exe		10,840 K	10,056 K	612	C:\WINDOWS\system32\winlogon.exe
explorer.exe		15,684 K	19,344 K	1600	C:\WINDOWS\system32\explorer.exe
ctfmon.exe		784 K	3,184 K	1772	C:\WINDOWS\system32\ctfmon.exe
procexp.exe		14,416 K	6,508 K	448	C:\Program Files\Microsoft Sysinternals Suite\procexp.exe
1.exe		1,084 K	3,784 K	2336	C:\Documents and Settings\test\Documents\1.exe
qkf.exe	92.73	600 K	1,856 K	2988	C:\Temp\qkf.exe
rundll32.exe		2,264 K	3,532 K	2072	C:\WINDOWS\system32\rundll32.exe
cmd.exe		1,900 K	2,500 K	2344	C:\WINDOWS\system32\cmd.exe
ping.exe		924 K	2,776 K	3200	C:\WINDOWS\system32\ping.exe
WINWORD.EXE		10,244 K	22,412 K	2560	[The handle is invalid.]

# Розсилка 19-го січня

Wed 1/20/2016 8:20 AM

[УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025](#)

To

 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

The image shows a screenshot of Microsoft Excel in compatibility mode. The title bar reads "Copy of Ocenka [Режим совместимости] - Microsoft Excel". The ribbon is set to "Работа с рисунками" (Work with Pictures). A security warning dialog box titled "Параметры безопасности Microsoft Office" (Microsoft Office Security Settings) is displayed in the foreground. The dialog box has a yellow background and a shield icon. The main text reads: "Оповещение системы безопасности - макрос" (Security system notification - macro). Below this, it states: "Макросы были отключены. Макросы могут содержать вирусы и другие опасные компоненты. Не включайте содержимое, если не уверены в надежности источника файла." (Macros were disabled. Macros may contain viruses and other dangerous components. Do not include content unless you are sure of the reliability of the source file). A warning message follows: "Внимание! Не удалось определить надежность источника этого содержимого. Рекомендуется оставить это содержимое отключенным за исключением случаев, когда содержимое обеспечивает критическую функциональность и вы доверяете его источнику." (Attention! Failed to determine the reliability of the source of this content. It is recommended to leave this content disabled except in cases where the content provides critical functionality and you trust the source). There is a link for "Дополнительные сведения" (Additional information). The file path is shown as "C:\Documents and Settings\test\Desktop\Copy of Ocenka.xls". Two radio buttons are present: "Установить защиту от неизвестного содержимого (рекомендуется)" (Set protection for unknown content (recommended)) and "Включить это содержимое" (Include this content), with the latter being selected. At the bottom, there are "Открыть центр управления безопасностью" (Open Security Center), "OK", and "Отмена" (Cancel) buttons. In the background, a yellow warning banner is visible with the text: "Увага! Цей документ б... Макроси потрібно включити для відображення вмісту документу." (Attention! This document b... Macros need to be included for content display in the document).

Copy of Ocenka [Режим совместимости] - Microsoft Excel

Работа с рисунками

Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид Разработчик Формат

Вставить Вставка Удалить Формат Ячейки

Буфер обмена Шрифт

Перенос текста Объединить и поместить в центре Числовой

Условное Форматировать как таблицу Стили ячеек

Предупреждение системы безопасности Запуск макросов отключен.

Рисунок 1

Оцінка структури генерую

Microsoft Office

Увага! Цей документ б...  
Макроси потрібно включити для відображення вмісту документу.

ft Office™

Параметры безопасности Microsoft Office

Оповещение системы безопасности - макрос

Макрос

Макросы были отключены. Макросы могут содержать вирусы и другие опасные компоненты. Не включайте содержимое, если не уверены в надежности источника файла.

**Внимание! Не удалось определить надежность источника этого содержимого. Рекомендуется оставить это содержимое отключенным за исключением случаев, когда содержимое обеспечивает критическую функциональность и вы доверяете его источнику.**

[Дополнительные сведения](#)

Путь к файлу: C:\Documents and Settings\test\Desktop\Copy of Ocenka.xls

Установить защиту от неизвестного содержимого (рекомендуется)

Включить это содержимое

[Открыть центр управления безопасностью](#) OK Отмена



# 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](http://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

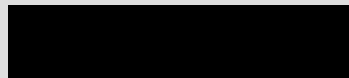


Пн 01.02.2016 14:52

ДП "Изюминка" <sales@aerocredo.ru>

документы по оформлению

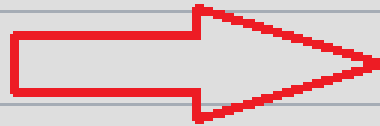
To



This message was sent with High importance.

Message

сканы.zip (770 KB)



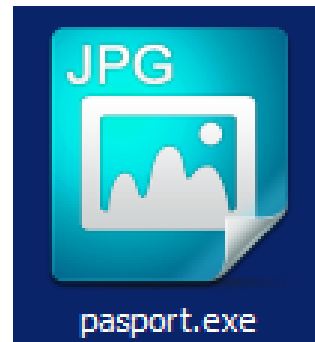
**ПАСПОРТ.exe**

Добрий день. відправляю вам документи для оформлення довіреностей.

З повагою Фролова Тетяна

ДП "Изюминка"

044-783-22-56



scan.jpg

# Розсилка 1-го лютого

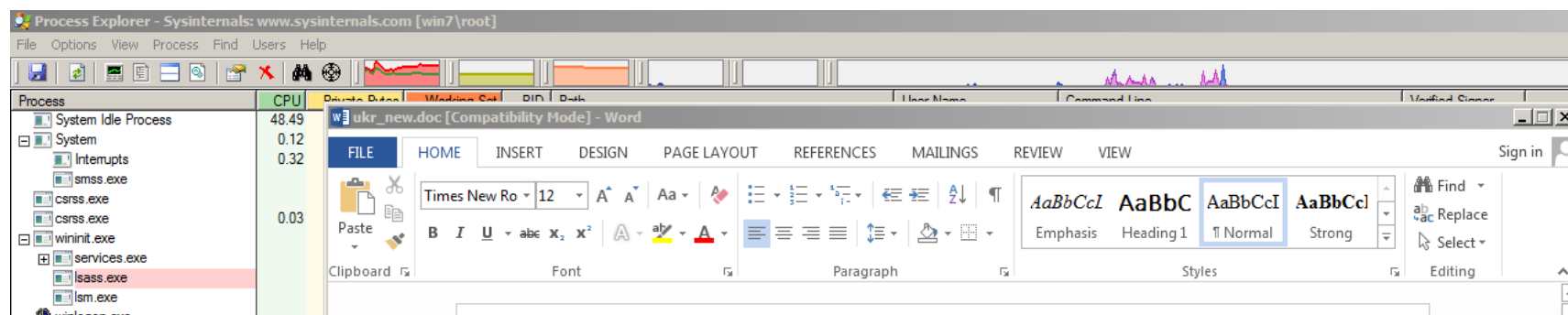


# Розсилка 1-го лютого

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\smss
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\servi
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\SysintemalsSuite
procexp64.exe	1.16	23,124 K	33,512 K	1212	win7\root "D:\VRad\SysintemalsSuite
Tcpview.exe	0.04	6,876 K	12,032 K	688	win7\root "D:\VRad\SysintemalsSuite
Procmon.exe		6,184 K	9,236 K	3420	win7\root "D:\VRad\SysintemalsSuite
Procmon64.exe	6.36	20,896 K	47,080 K	3456	win7\root "C:\Users\ROOT~1\WIN\A
passport.exe	0.04	3,208 K	10,460 K	3596	win7\root "C:\Users\root.win7\Desktop
winrar.exe	4.11	5,836 K	10,044 K	3624	win7\root "C:\Users\root.win7\Desktop



# Розсилка 4-го лютого



Capturing from eth1\_nat [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.0.3.15	192.168.1.5	DNS	78	standard query 0x1769 A cluster007.ovh.net
2	0.00185600	192.168.1.5	10.0.3.15	DNS	94	standard query response 0x1769 A 213.186.33.18
3	0.00423100	10.0.3.15	213.186.33.18	TCP	66	49299->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.05886700	213.186.33.18	10.0.3.15	TCP	60	80->49299 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
5	0.05893600	10.0.3.15	213.186.33.18	TCP	54	49299->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
6	0.05922400	10.0.3.15	213.186.33.18	HTTP	347	GET /~telodged/43543r34r/843tf.exe HTTP/1.1
7	0.05939500	213.186.33.18	10.0.3.15	TCP	60	80->49299 [ACK] Seq=1 Ack=294 win=65535 Len=0
8	1.50531900	10.0.3.15	192.168.1.5	DNS	86	standard query 0x6e32 PTR 18.33.186.213.in-addr.arpa
9	1.50766700	192.168.1.5	10.0.3.15	DNS	118	standard query response 0x6e32 PTR cluster007.ovh.net
10	6.58267300	10.0.3.15	10.0.3.255	BROWSEF	247	Domain/workgroup Announcement SKY, NT workstation, Domain Enum
11	36.1717480	10.0.3.15	10.0.3.255	NBNS	92	Name query NB SKY<1c>
12	36.9213270	10.0.3.15	10.0.3.255	NBNS	92	Name query NB SKY<1c>
13	37.6711810	10.0.3.15	10.0.3.255	NBNS	92	Name query NB SKY<1c>

# 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]

Machine View Devices Help

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VI

### 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

Command line: C:\Tmp\vmsk.exe  
Current directory: C:\Users\root.win7\Desktop\  
Autostart Location: n/a

Parent: <Non-existent Process>(2960)   
User: win7/root   
Started: 12:27:23 PM 3/3/2016 Image: 32-bit   
Comment:   
VirusTotal:    
Data Execution Prevention (DEP) Status: DEP (permanent)  
Address Space Load Randomization: Disabled

OK Cancel

Paragraph

being proofed. You may be able

**1.1. Сфера дей**  
1.1.1. Правила разработаны в со законодательств... оказания услуг св...  
1.1.2. Настоящ... их условиями.  
1.1.3. Если от... предусмотрены на...  
1.1.4. Услуги : оказания услуг св... лицензий Операто... 38643) и в местах р...  
Услуги внутризо...

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%\Sys...	(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\sys...	(Verified) Microsoft...
lsass.exe	< 0.01	4,244 K	11,684 K	520	NT AUTHORITY\...	C:\Windows\sys...	(Verified) Microsoft...
lsmd.exe		2,992 K	5,768 K	528	NT AUTHORITY\...	C:\Windows\sys...	(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...

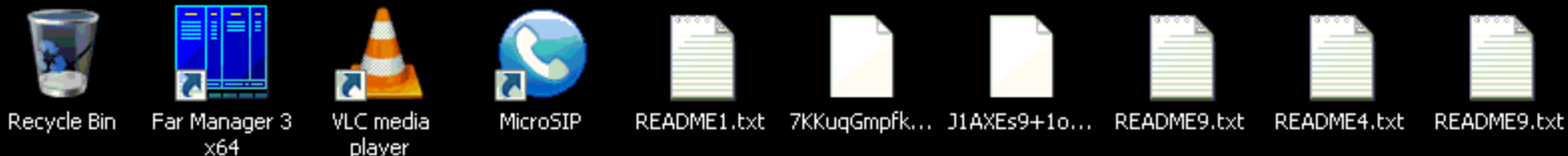
CPU Usage: 2.61% Commit Charge: 35.05% Processes: 50 Physical Usage: 27.89%

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



**ВНИМАНИЕ!**



**Все важные файлы на всех дисках  
вашего компьютера были  
зашифрованы.**



**Подробности вы можете прочитать в  
файлах README.txt которые лежат  
на любом из дисков.**



**ATTENTION!**  
**All the important files on your disks  
were encrypted.**



**The details can be found in**

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

# .XLS та .EXE – 24 ГОДИНИ після розсилки



SHA256: 0bb5e98f77e69d85bf5068bcb5b5876f8e5855d34d9201d1caffb83460cccc  
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



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



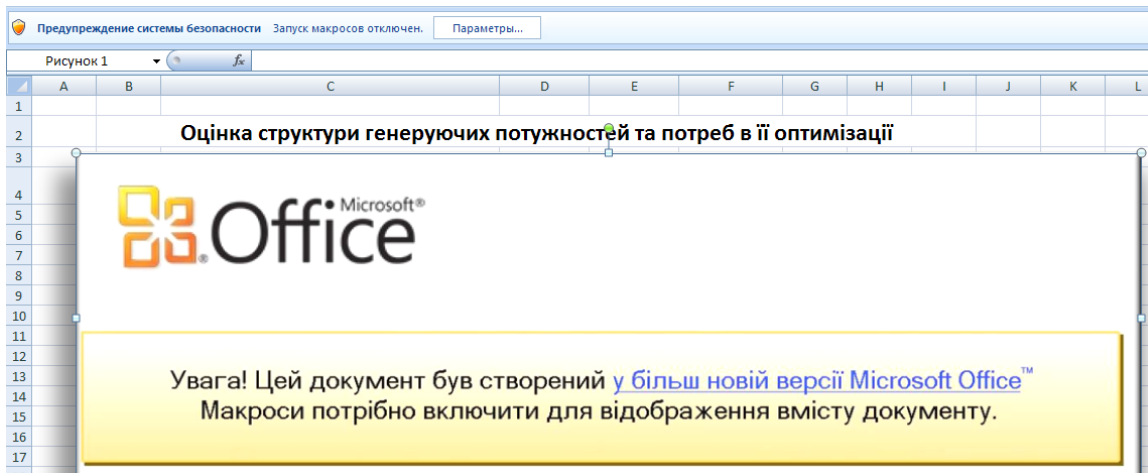
.XLS та .EXE – **24 години** після розсилки





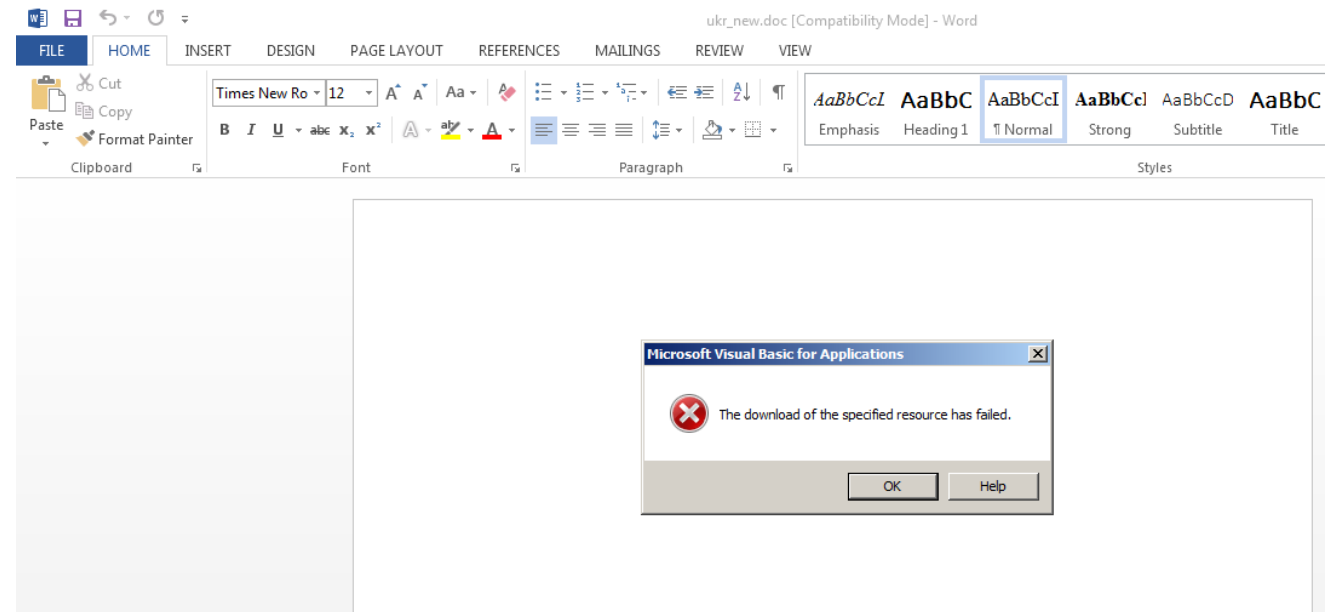
# Трохи аналітики

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...)



- + PC\_
- + PC\_
- + PC\_ ня Николаев
- + PC\_ атерина Сер
- + PC\_
- + PC\_ Исадчий
- + PC\_ гей Евгеньел
- + PC\_ на Ивановна
- + PC\_
- + PC\_ настасия Вл
- + PC\_ индр Юрьеви
- + 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)



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
36	xls	http://com/upload/ilyich/tender/166/реализация транспорта 59 един...	X
37	xls	http://com/upload/ilyich/tmp/tender/456265931f73890f72bbe33cc15d4...	X
38	xls	http://upload/sales/report/1/Прайс от 08.04.2015 г..xls	X
39	xls	http://upload/sales/report/1/Прайс от 02.04.2015 г..xls	X
40	xls	http://upload/sales/report/1/Прайс от 17.04.2015 г..xls	X
41	xls	http://upload/sales/report/1/Прайс от 14.04.2015 г..xls	.
42	xls	http://upload/sales/report/1/Прайс от 29.04.2015 г..xls	.
43	xls	http://upload/sales/report/1/Прайс от 17.03.2015 г..xls	.
44	xls	http://com/upload/ilyich/tender/164/Приложение на реализацию ЯК...	X
45	xls	http://com/upload/ilyich/tender/138/реализация имущества земля ...	X
46	xls	http://com/upload/ilyich/tender/131/Заявка на реализацию 2 ТС ЦП...	X
47	xls	http://com/upload/ilyich/tender/206/ПОТ №№ 2; 3; 4; 5; 6; 7.xls	X
48	docx	http://com/upload/ilyich/tender/202/Заявка.docx	X
49	docx	http://com/upload/ilyich/tmp/tender/5bf6111148ad9a8cb18b7eb8355d...	X
50	docx	http://com/upload/ilyich/tender/97/запит цн пропоз2.docx	.
51	docx	http://upload/ /content/119/Пакет документів по контраген...	X
52	docx	http://com/upload/ilyich/tender/179/Приложение №1..docx	X
53	docx	http://com/upload/ilyich/tender/127/Приложение №1..docx	X
54	docx	http://com/upload/ilyich/tender/117/Приложение №1..docx	.
55	docx	http://com/upload/ilyich/tmp/tender/46e45dc0b93b99592d652debf2b2...	X

Conf Deactivate AutoScroll Clear

Save log to File

Metadata analyzed !



# 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. “пісочниця”
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	<a href="http://www.vbforums.com/showthread.php?460464-RESOLVED-is-there-a-method-like-quot-isAlphabetic-quot">http://www.vbforums.com/showthread.php?460464-RESOLVED-is-there-a-method-like-quot-isAlphabetic-quot</a>	URL
IOC	<a href="http://stackoverflow.com/questions/275160/regex-for-names">http://stackoverflow.com/questions/275160/regex-for-names</a>	URL
IOC	<a href="https://davidcel.is/posts/stop-validating-email-addresses-with-regex/">https://davidcel.is/posts/stop-validating-email-addresses-with-regex/</a>	URL
IOC	<a href="http://stackoverflow.com/questions/11501">http://stackoverflow.com/questions/11501</a>	URL

# Sources

- Vlad Styran slides
- Steven Rambam

[slideshare.net/sapran/presentations](https://slideshare.net/sapran/presentations)

[“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
- Mark Russinovich videos

[channel9.msdn.com/Events/Speakers/Paula-Januszkiewicz](https://channel9.msdn.com/Events/Speakers/Paula-Januszkiewicz)

[channel9.msdn.com/Events/Speakers/Mark-Russinovich](https://channel9.msdn.com/Events/Speakers/Mark-Russinovich)

- 7 кроків у напрямку безпеки
- Pentesting\_ практика

[https://radetskiy.wordpress.com/2015/04/10/7\\_steps\\_ua/](https://radetskiy.wordpress.com/2015/04/10/7_steps_ua/)

[https://radetskiy.wordpress.com/2015/05/18/pentest2015\\_practice/](https://radetskiy.wordpress.com/2015/05/18/pentest2015_practice/)

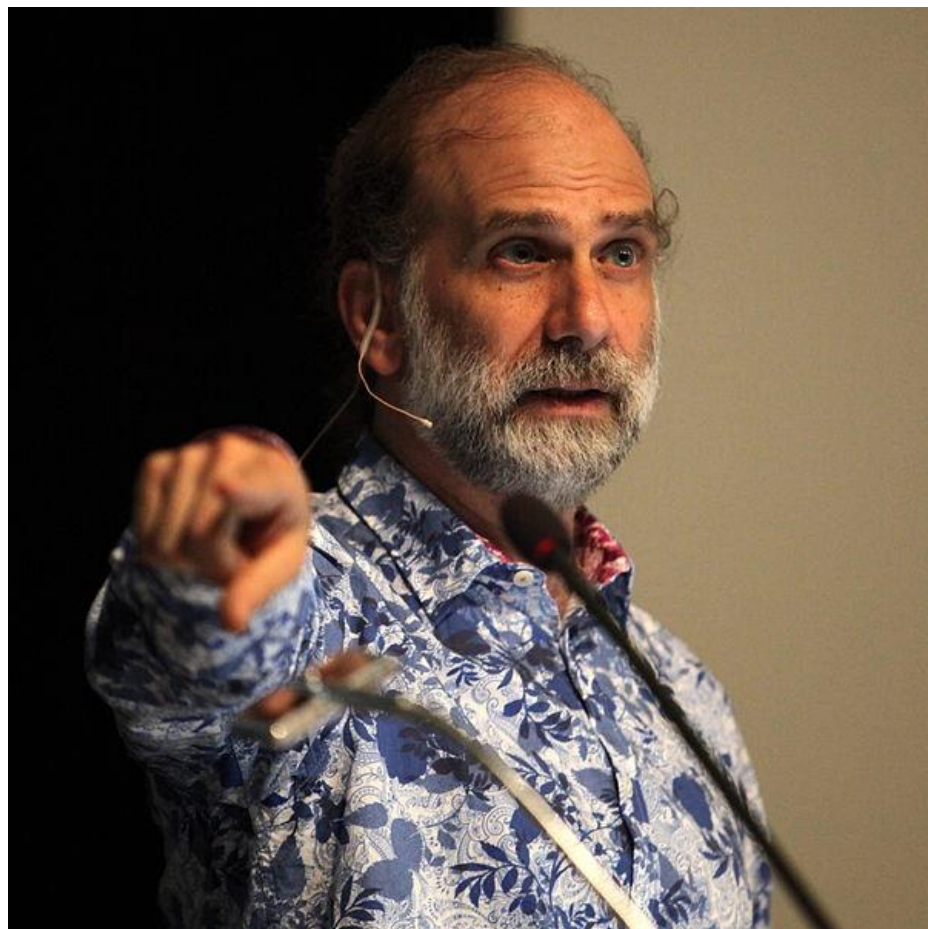
Дякую Вам за увагу!

Владислав Радецький

[vr@bakotech.com](mailto:vr@bakotech.com)

[radetskiy.wordpress.com](http://radetskiy.wordpress.com)

# І не забувайте про слова Брюса Шнайєра



*Only amateurs attack machines;  
professionals target people.*

Bruce Schneier