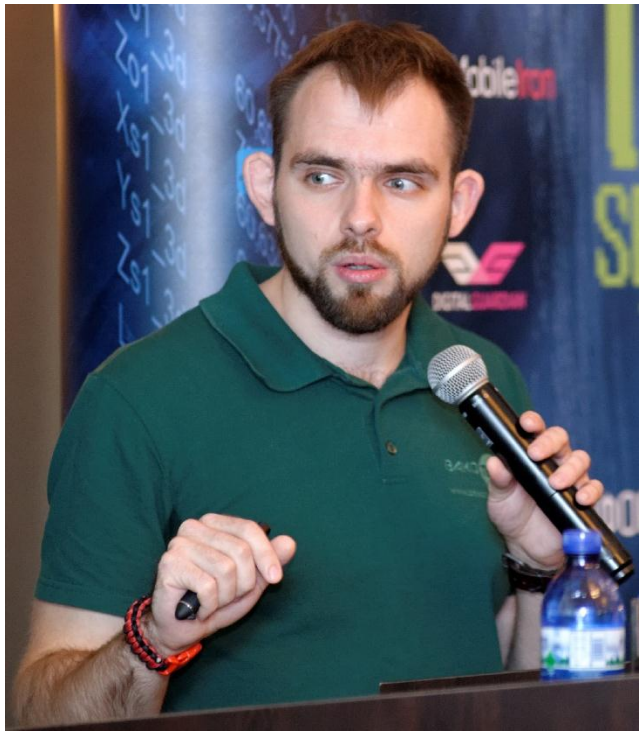
Щось на тему кібербезпеки ;)

Владислав Радецький
vr@bakotech.com

Кілька слів про мене



В IT галузі офіційно з 2007 року.

Починав як адмін / “anykey`щик”.

4 роки працював в IT-аутсорсингу.

З 2011 працюю в компанії БАКОТЕК®

Прийшов сюди щоб поділитися із вами досвідом і знаннями.

https://radetskiy.wordpress.com

http://ua.linkedin.com/pub/vladislav-radetskiy/47/405/809

Владислав Радецький

Technical Lead

vr@bakotech.com

Регламент

- У нас мало часу (як завше)
- Я не є Wiki/Google, є речі які я мало знаю або тупо не знаю))
- Бесіда стосовно ІБ
- Я хочу почути **ваші запитання – що цікавить саме вас?**
- Я буду відповідати не з позиції певного вендора…

  а з позиції технічного спеціаліста

В чому я трохи розбираюся

- Антивіруси та їх недоліки **o_0**
- DLP – за і проти? (*конфіденційно, але вам – можна*)
- Сучасні семпли та їх особливості (*ransomware та інші модні штуки*)
- Фішинг, соц. інженерія та інші прикольні слова)) **o_0**
- “Пісочниці”, що з ними варто робити а що ні?
- 5 смертних гріхів при спілкуванні з тех. підтримкою (*крик душі!!!*)
- Як і чим атакувати/ломали ГОСи? (хто пропустив минулий Бубен)

Правила безпечного використання IT

Владислав Радецький
vr@bakotech.com

Про що я буду розповідати

- Людський фактор, вразливості людей
- OSINT, соціальна інженерія

Теми, які часто ігнорують / Не беруть до уваги

- Особливості роботи електронних пристроїв
- Детальний аналіз атак на українські організації
- Рекомендації
  - Паролі
  - Пошук інформації
  - Email
  - Документи, програми, чужі системи, соц. мережі
- Висновки

Трохи прикладів типової людської необережності

Людський фактор

2012 – Фото принца Вільяма розкрили паролі авіабази ВПС Англії

Людський фактор

2014 – Чемпіонат світу з футболу, центр безпеки, пароль Wi-Fi

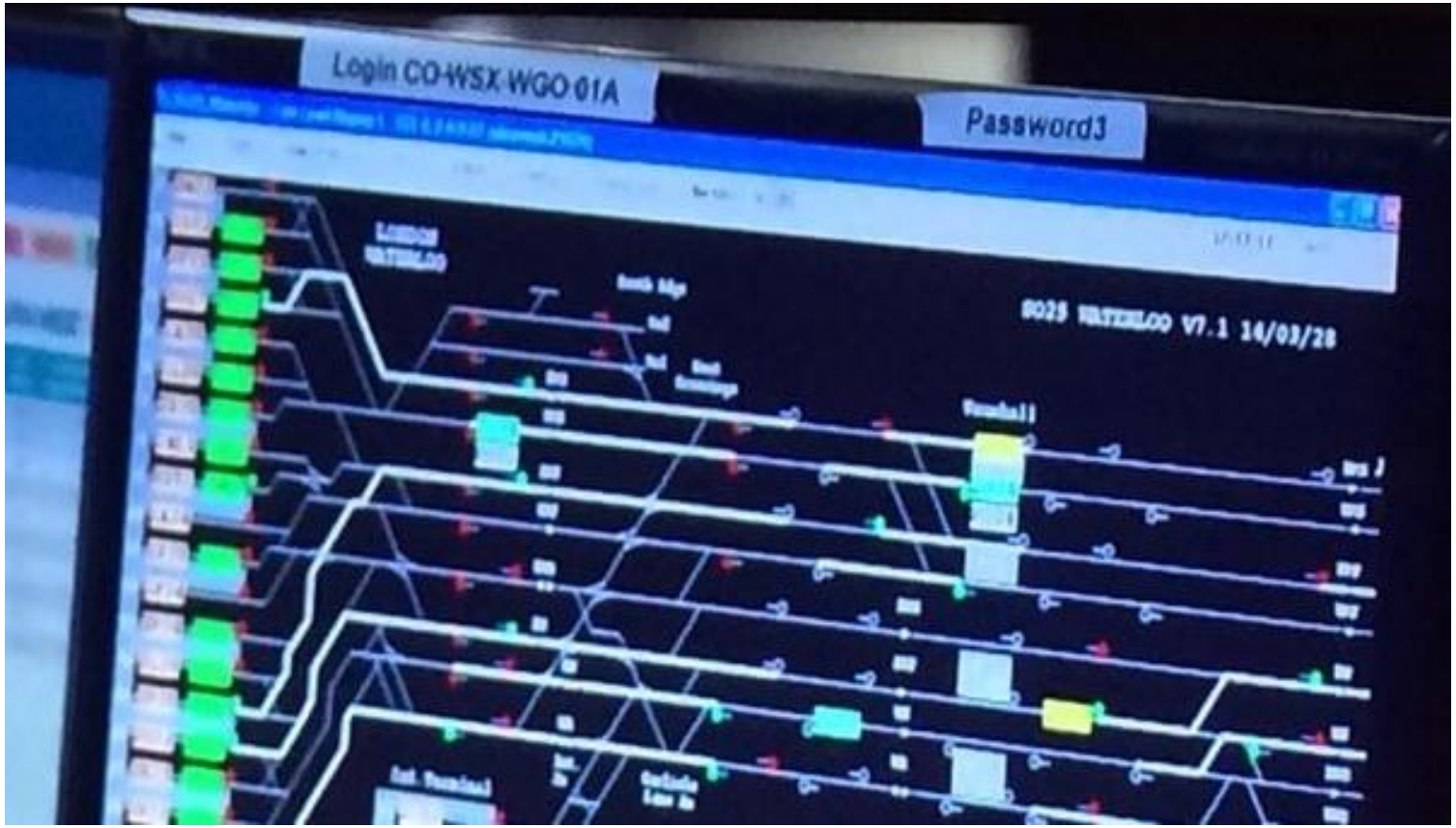
b5a2112014

Людський фактор

2015 – Канал TV5Monde “засвітив” свої паролі під час інтерв'ю

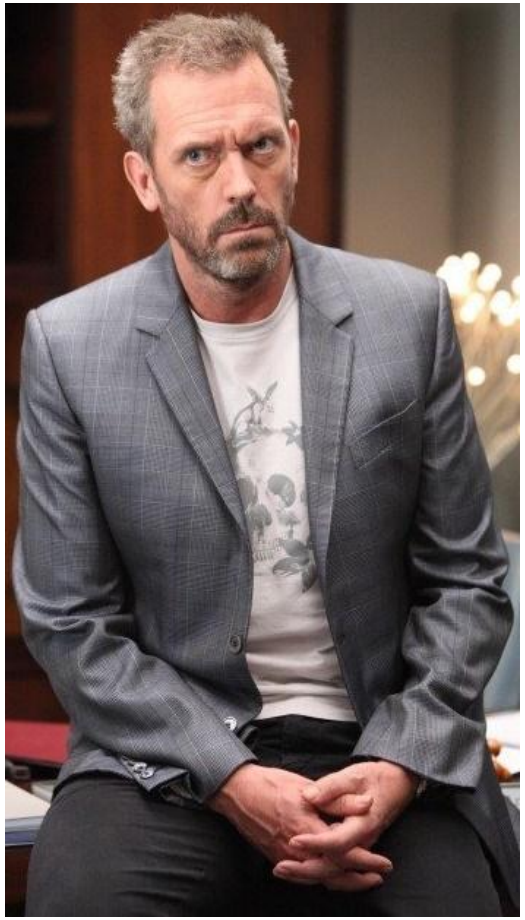
Людський фактор

2015 – В сюжеті BBC “засвітили” паролі залізничної системи Ватерлоо



Людський фактор

- “Everybody lies“
- Неуважність
- Необережність
- Цікавість/інтерес
- Відсутність культури
- Відсутність розуміння

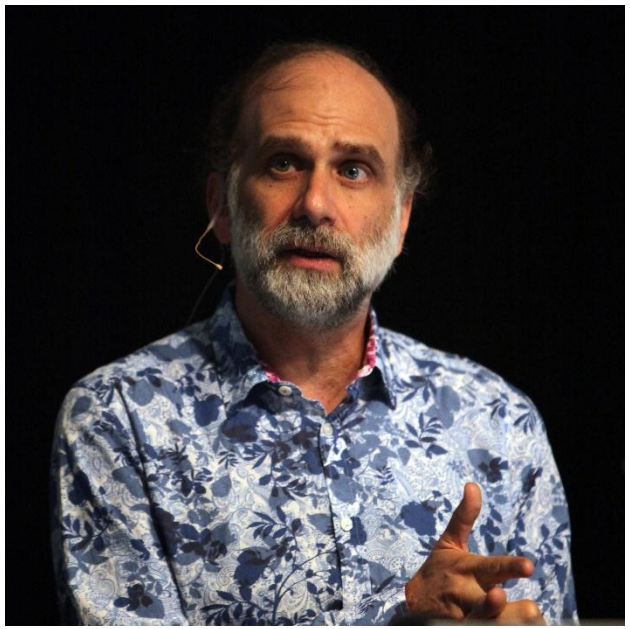


Людський фактор

“Вразливості” людей

- Бажання подобатися
- Ввічливість
- Бажання бути потрібними
- Пристрасті / Комплекси / Захоплення (fb)
- “На слабо”

Людський фактор



Брюс Шнайдер

Only amateurs attack machines; professionals target people.

Bruce Schneier - The State of Incident Response (Black Hat 2014)

Людський фактор

Джерела (Google / Youtube вам в поміч)

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)

Переклад доповіді:

noonesshadow.wordpress.com/2010/09/

OSINT, соціальна інженерія

OSINT – використання інформації з відкритих джерел
(*отримуємо інформацію не порушуючи закон*)

Soc. Eng. – акт маніпуляції для досягнення певних цілей, які можуть не бути в інтересах жертви.
(Цукерберг, Мітнік, Мавроді… ~~Кисельов~~ ворожі ЗМІ)

OSINT, соціальна інженерія

Важливо пам'ятати що інформація буває:

- Достовірна (є принаймні 1-2 підтвердження)
- Недостовірна (підтвердження не існує)

> Перевірка фактів, висновки

> Керуючись неперевіреною інформацією ви ризикуєте

OSINT, соціальна інженерія

Джерела OSINT _ безкоштовні ! публічні !

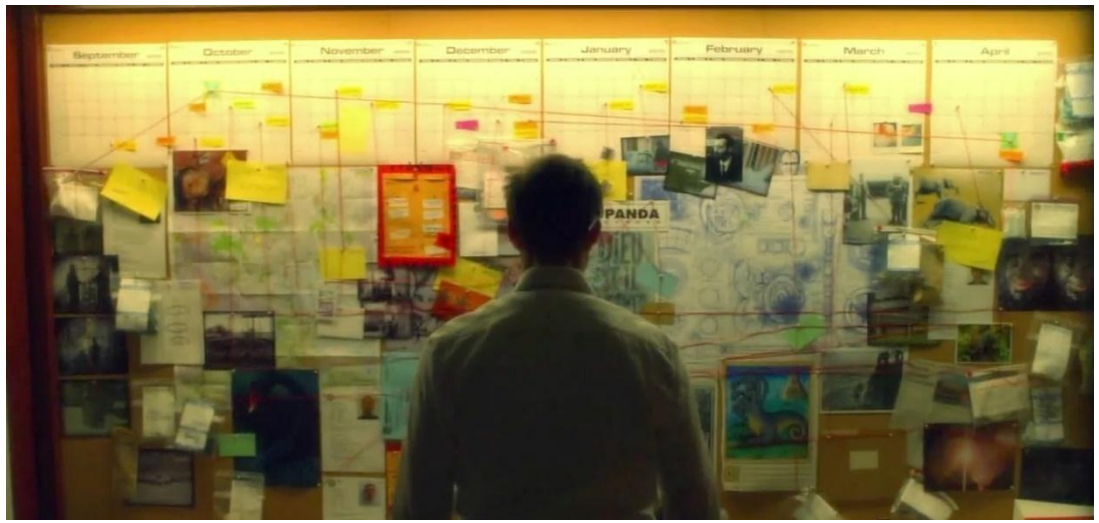
OSINT, соціальна інженерія

Інструменти OSINT

- Google dorks
- FOCA (використання метаданих)
- Maltego (побудова зав'язків)

...

* Перелік не повний, але цих більш ніж достатньо



OSINT, соціальна інженерія

Класичні підстави соц. інженерії

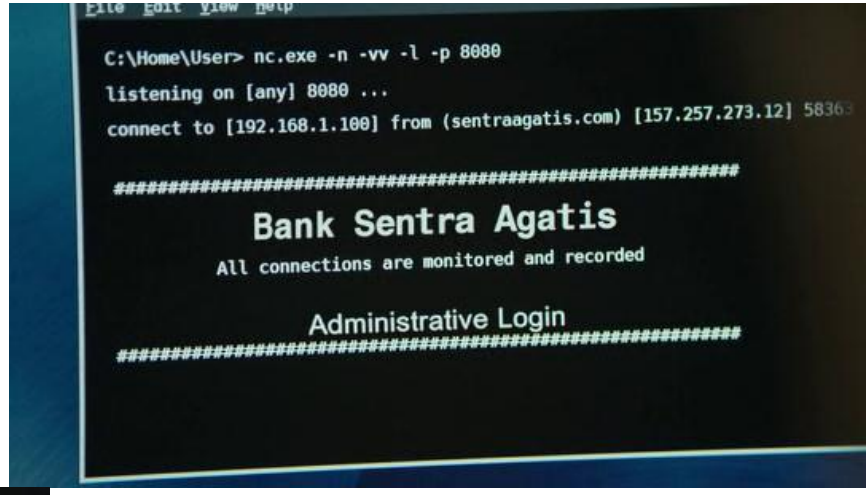
- Help Desk / Tech Support (***нагадайте ваш пароль?***)
- Співбесіда (***обидва варіанти***)
- Новий співробітник (***я тут вперше, де тут каса?***)
- Ображений/роздратований VIP замовник (***дайте мені негайно!***)
- Помилкова доставка документів (**а тут таких нема? а хто є?**)

OSINT, соціальна інженерія

Прохання роздрукувати зіпсований документ. Хіба справжній джентльмен відмовить леді ?

OSINT, соціальна інженерія

Флешка містила reverse shell, який дозволив віддалене керування скомпрометованою системою



Порушення політики ІБ

Наслідки

OSINT, соціальна інженерія

Джерела (Google / Youtube вам в поміч)

Володимир Стиран “**Прелюдия к атаке**”

securegalaxy.blogspot.com

slideshare.net/sapran/osint

Steven Rambam “**Privacy is Dead - Get Over It**”

noonesshadow.wordpress.com/2010/09/

Особливості роботи ПК/гаджетів

Навіть коли система “висне” – в фоні іде купа звернень

- Від обману до шифрування як правило **3-4 кліки**
- Шифрувальщику треба від **30 секунд** до **15 хвилин**
- Ціна помилки стартує від **$ 500**
- Більшість жертв не встигають опам'ятатися

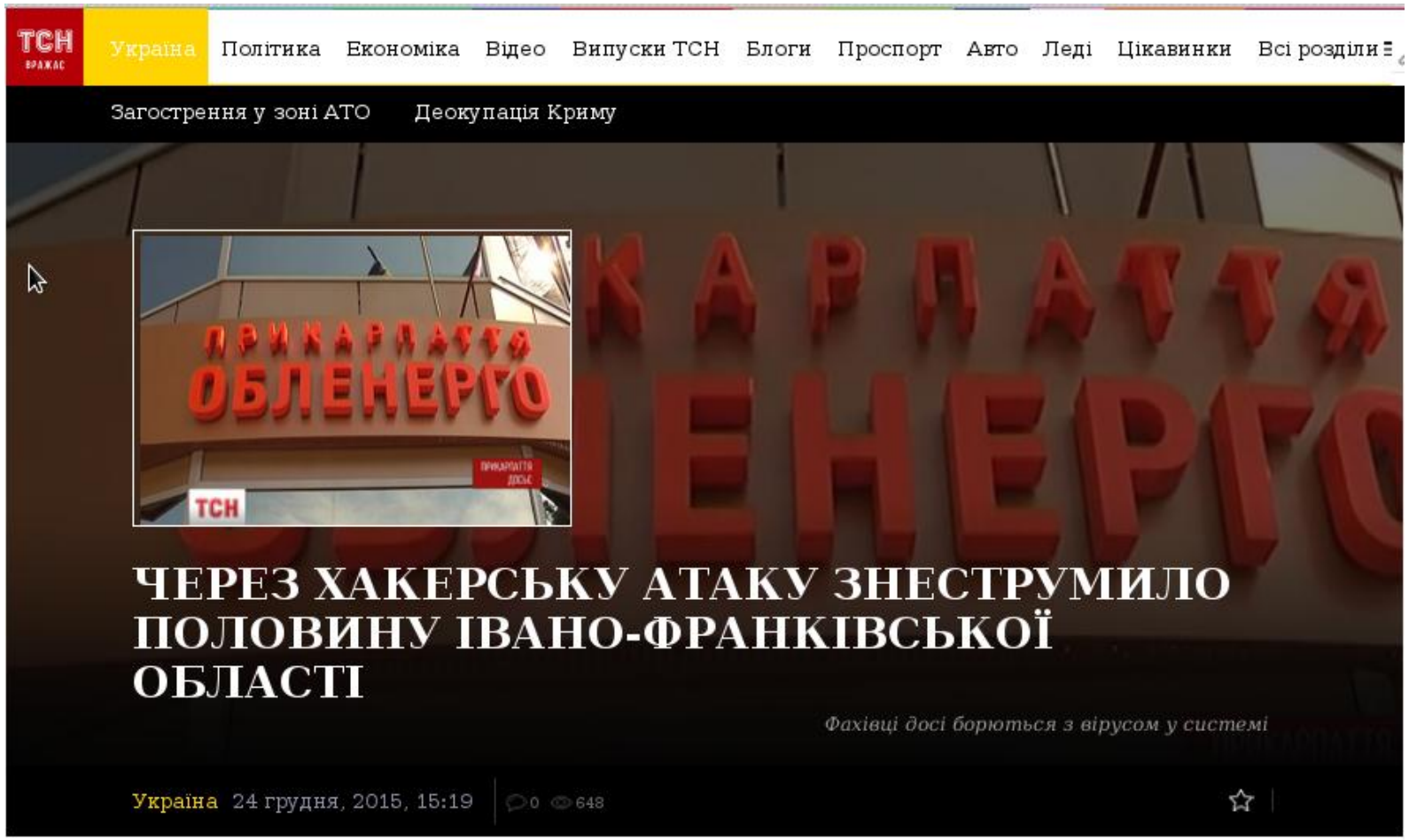
Сучасні цільові атаки
- як це було

Термінологія

Фішинг – спосіб атаки, що базується на розсилках спеціально складених, підроблених **електронних листів**, що змушують жертву запустити приєднання або перейти за посиланням.

Соц. інженерія – акт психологічної маніпуляції/обману жертви для досягнення певних цілей в інтересах зловмисників.

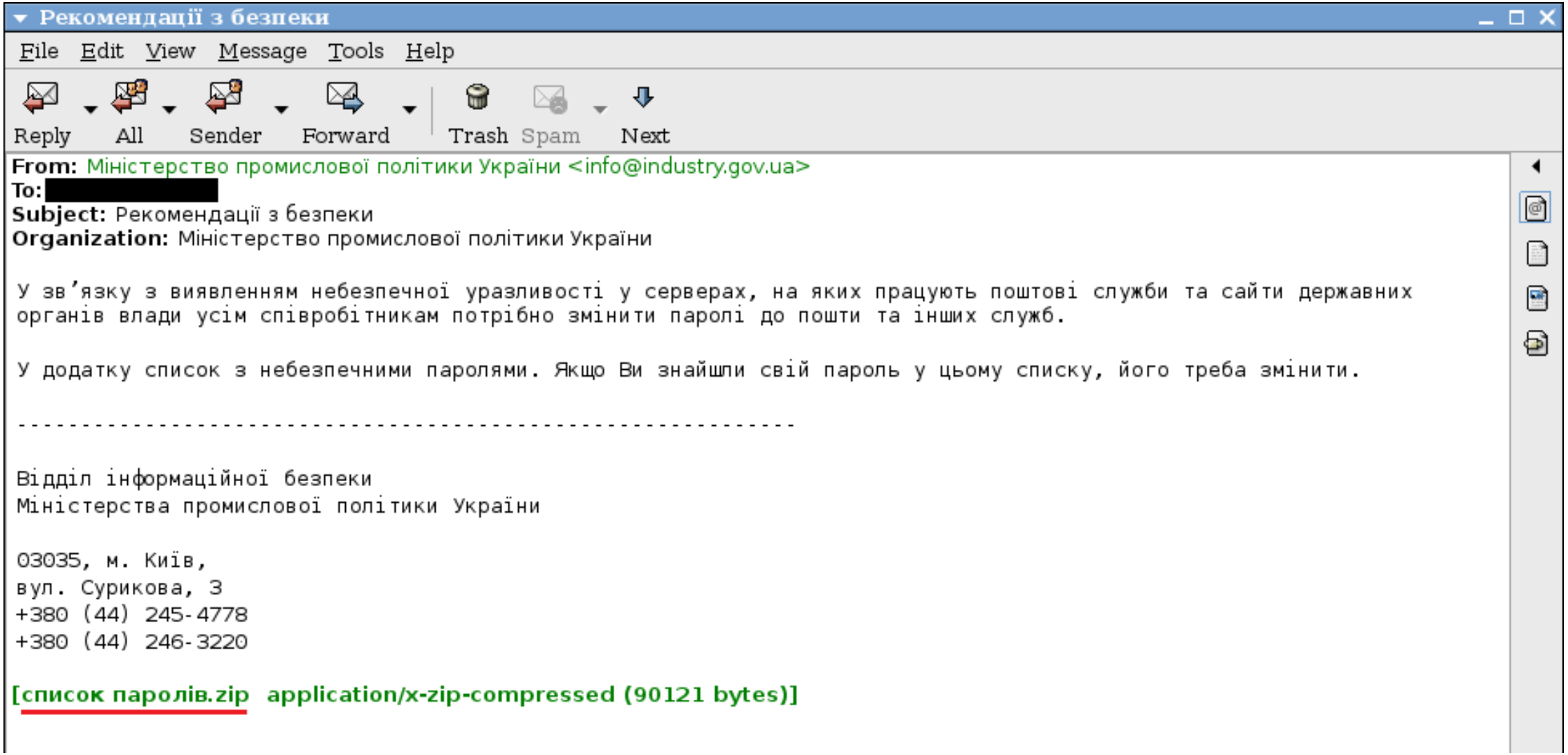
Резонанс у ЗМІ



Кілька годин фахівці відновлювали світло.

Прикарпаттяобленерго назвало **причину вимкнення електроенергії**, що мало місце напередодні, 23 грудня. Причиною стала хакерська атака, повідомляє ТСН.

З чого почався ВЕ **у 2014-му році**



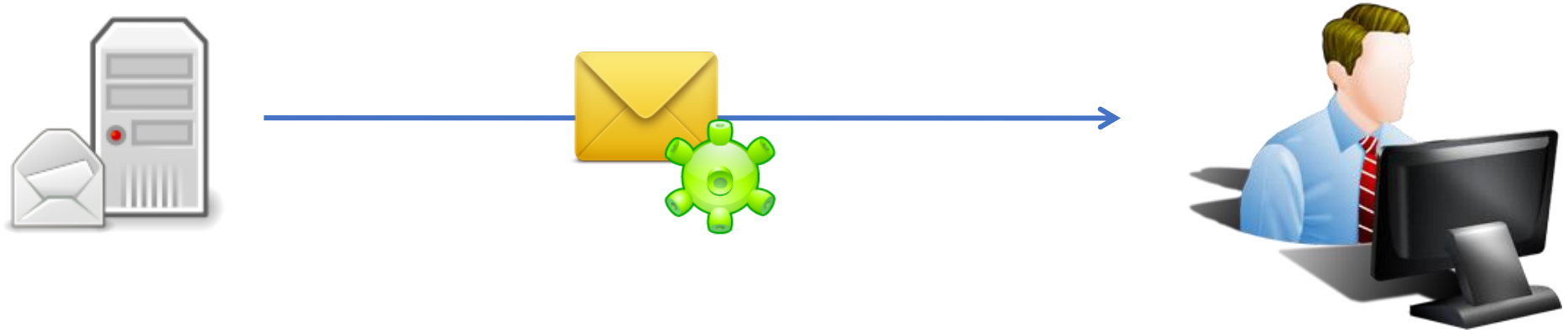
Спроби атак на критичні об'єкти

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

Спроби атак на критичні об'єкти

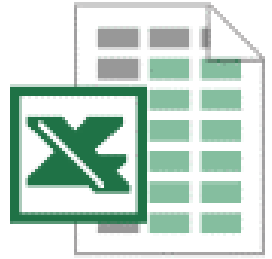
- 23 грудня 2015 енергетика/макроси (**BlackEnergy**)
- 19 січня 2016 енергетика/макроси (**RAT, Sandworm**)
- 1 лютого 2016 широкий спектр/.exe (**ZBot/ZeuS**)
- 4 лютого 2016 широкий спектр/макроси (**Dridex**)
- 3 березня 2016 енергетика / RTF + RCE (**ransomware**)

Типова схема атаки



Зловмисники запускають розсилку фішингових листів із приєднаннями. Текст листів підштовхує жертву запустити/відкрити приєднання.

Типова схема атаки

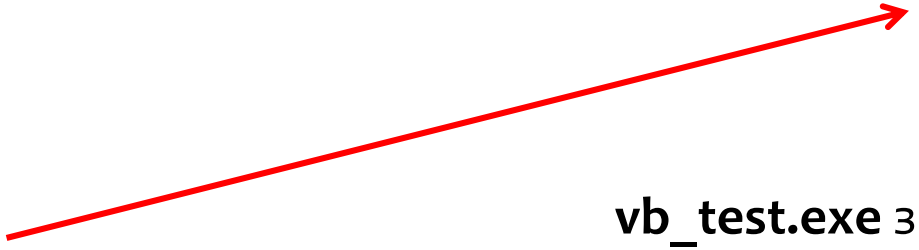


Якщо жертва відкрила приєднання
та активувала макрос, він
видобуває із себе dropper
І зберігає його у **%temp%\vb_test.exe**

Типова схема атаки

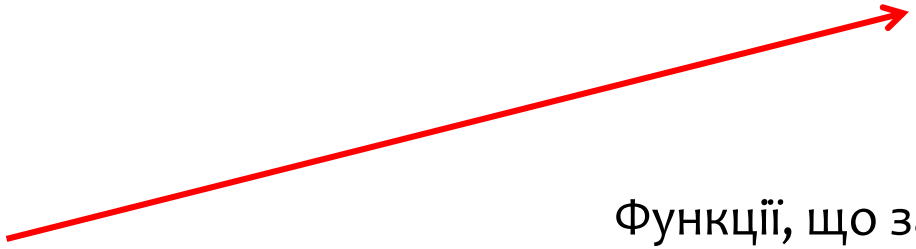
vb_test.exe перевіряє параметри системи, змінює налаштування проксі та активує комунікацію із C&C сервером

Типова схема атаки



vb_test.exe завантажує з C&C сервера модуль віддаленого керування (RAT), і зберігає його у ***\AppData*\iesecurity.exe**

Типова схема атаки



Функції, що забезпечує RAT:
- кейлогер
- знімки екрану
- завантаження/вигрузка файлів
- запуск процесів та ін.

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.

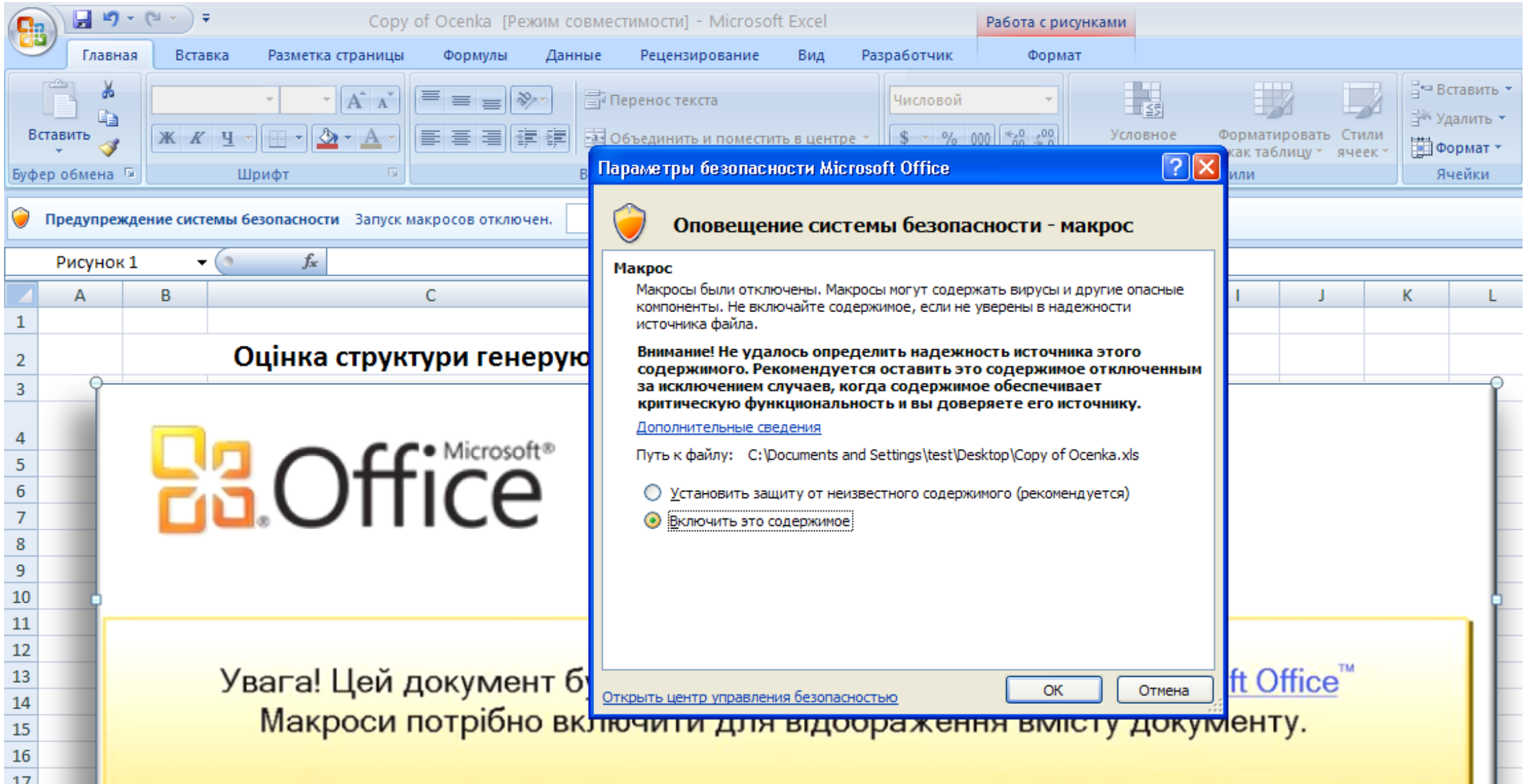
Message | Ocenka.xls (816 KB)

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».

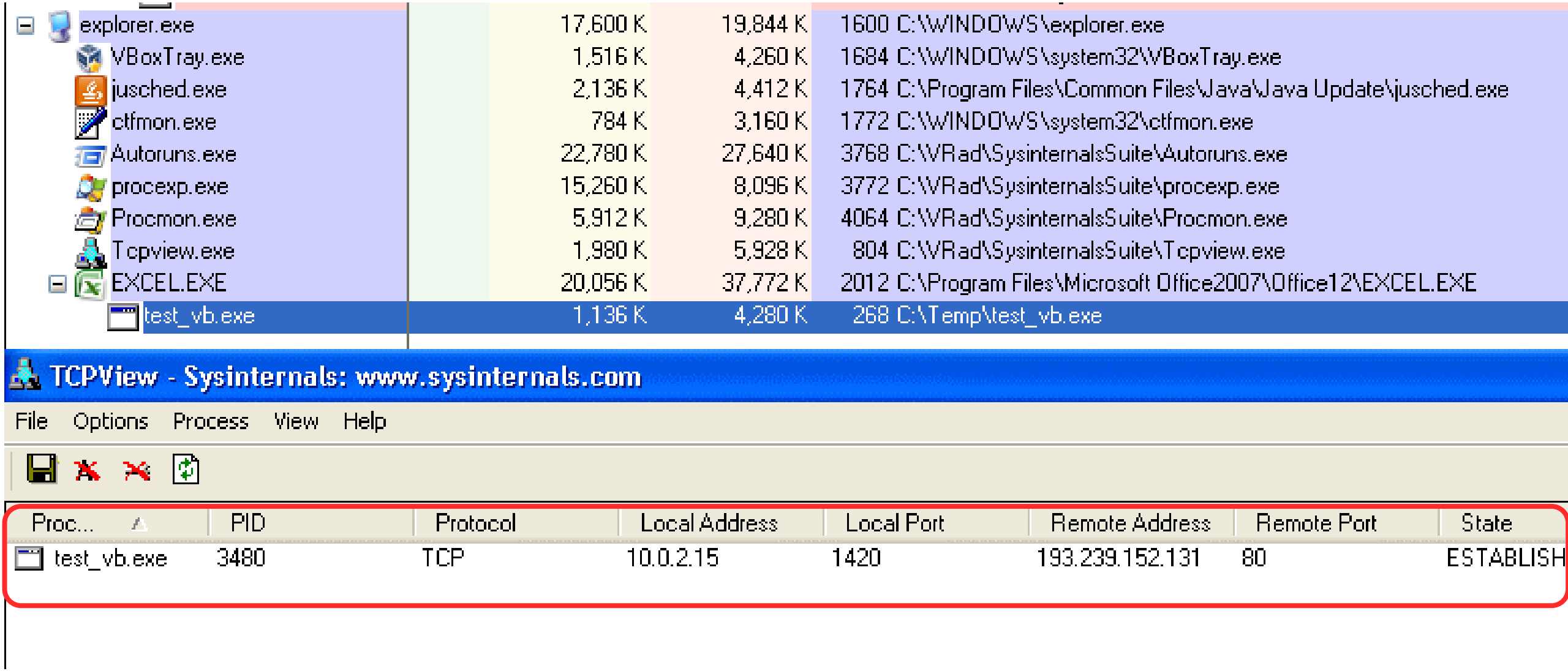
Проект Плану розвитку знаходиться в додатку до листа.

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 3-го березня

Чт 03.03.2016 8:48

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

Документы

To [redacted]

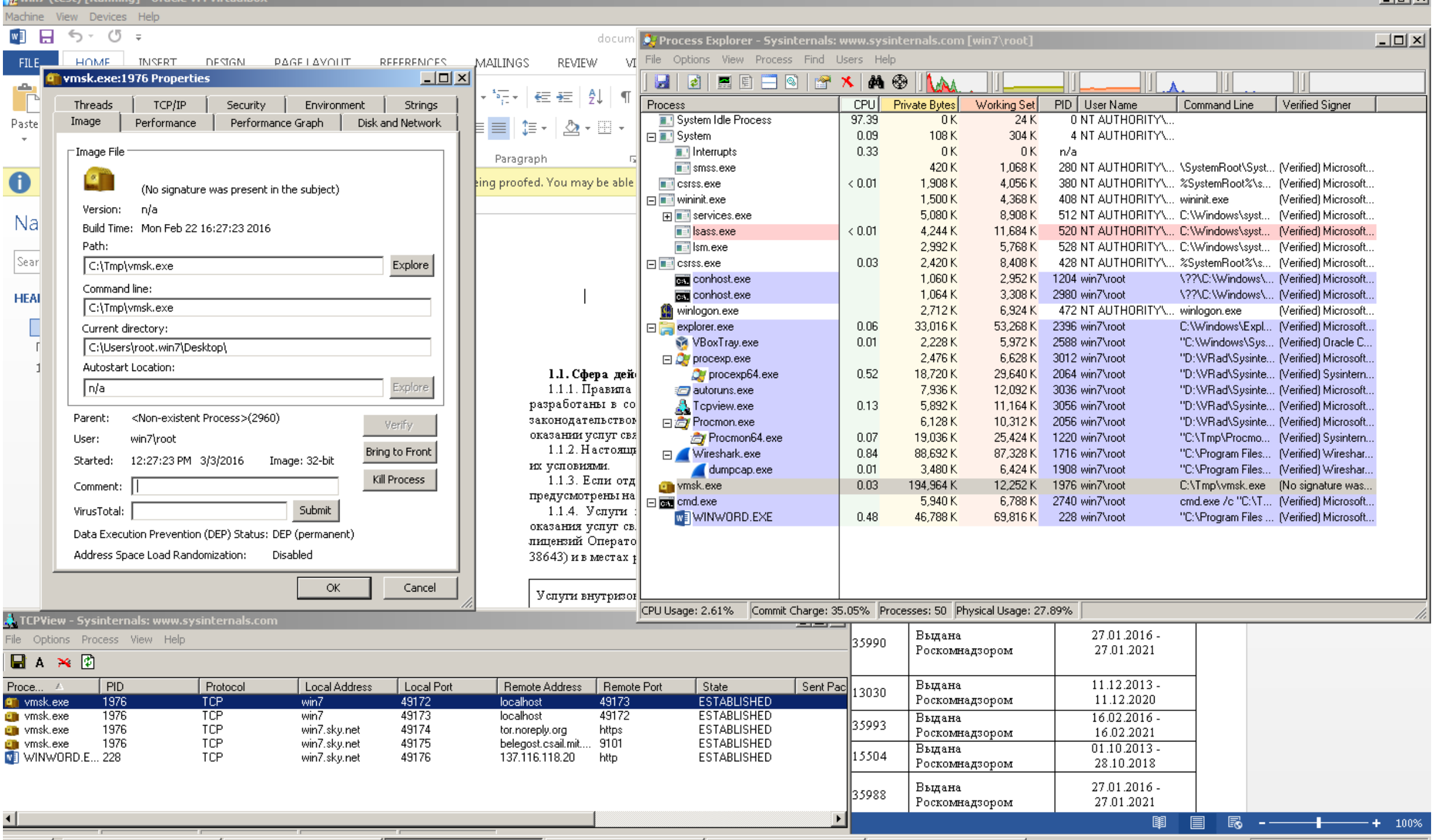
You forwarded this message on 03.03.2016 10:12.

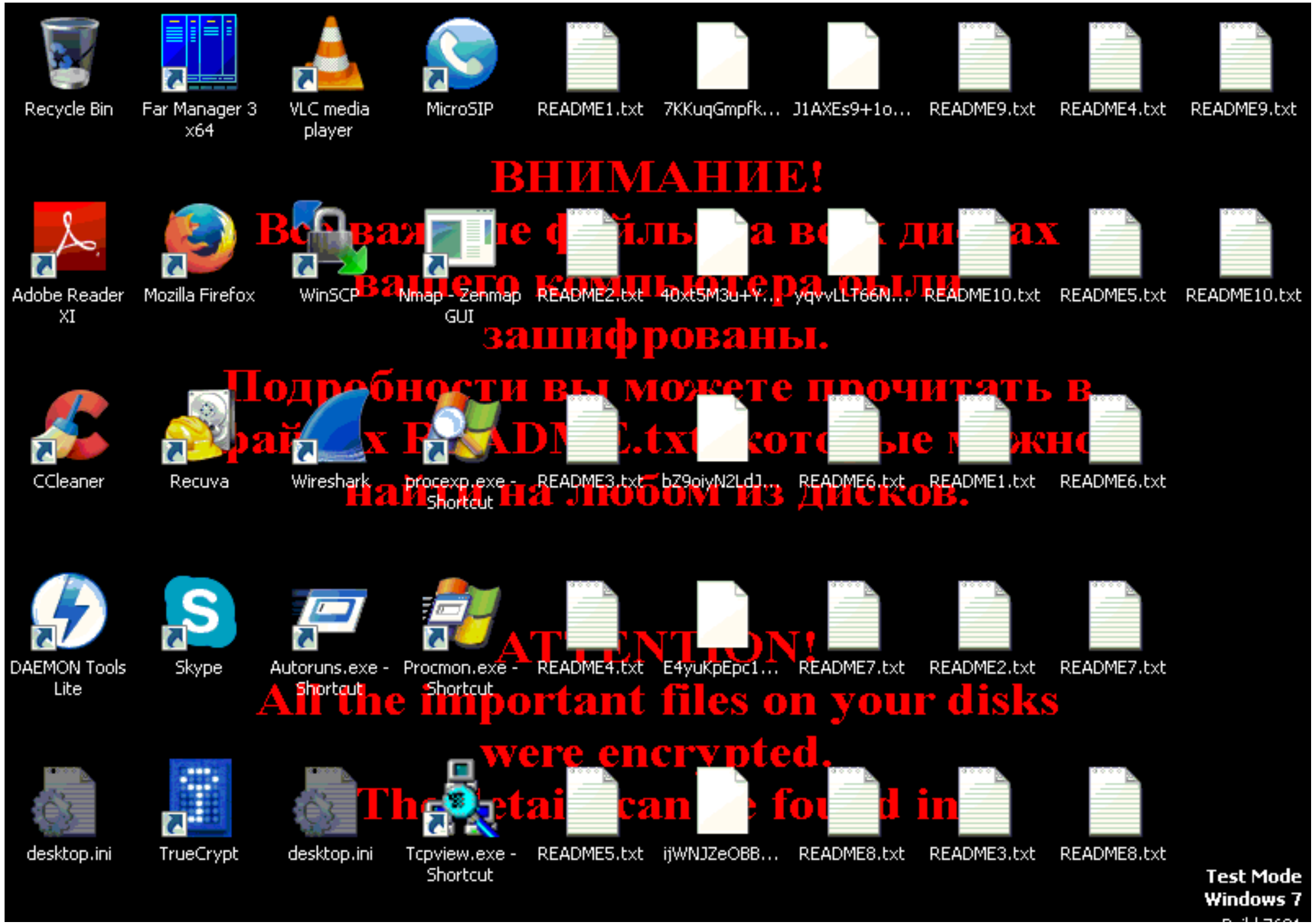
Message schet[redacted].doc (1 MB)

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

Чт 14.07.2016 19:08

Анастасія Котэнко <liam.seeger@t-online.de>

info Пропонуємо ознайомитись з належними документами

To

You forwarded this message on 14.07.2016 15:08.

Message | Позов_примірник_info.doc (40 KB)

Шановний пане/пані!

Фінансовий підрозділ Діамантбанк звертається до Вас з приводу того, що на Ваше ім'я 12.09.2015 року, за допомогою нашої послуги онлайн банкінгу, було укладено договір на терміновий кредит на суму 121 433,00 гривень.

На даний момент належну суму за кредитом не погашено. Станом на дату надсилання цього листа року Ваш борг з урахуванням пені (0,7% за кожну добу прострочення оплати) становить 51 000,59 грн.

У зв'язку з цим, на підставі кредитної угоди, керівництвом відділення було прийнято рішення про складання судового позову на Ваше ім'я.

Пропонуємо ознайомитись з відповідними документами.

Чт 14.07.2016 22:02

Онисим Миргородский <arsoy.nej@t-online.de>

office, Угоду_про_кредитування - ВТБ Банк

To

You forwarded this message on 14.07.2016 17:03.

Message | Угоду_про_видачу безготівкового_кредиту_office.doc (40 KB)

Високошановний добродію!

Юридичний підрозділ нагадує вам, що, відповідно до наявних документів, 11.12.2015 року на Ваш ідентифікаційний код було укладено кредитний договір на суму 210 000,00 гривень.

Вважаємо за свій обов'язок сповістити Вас про те, що Вашу заборгованість на сьогоднішній день досі не погашено, натомість сума продовжує зростати за рахунок процентів та штрафних санкцій, що становить 0,9% за кожен банківський день прострочення.

Оскільки Ви, всупереч умовам договору, і досі не внесли належну суму позики, ми змушені призупинити дію договору та звернутись до суду для примусового стягнення суми кредиту та штрафних санкцій.

Пропонуємо Вам ознайомитись з відповідною документацією.

P.S. Запевняємо Вас, що, якщо протягом 20 банківських днів Ви внесете на рахунок банку вказану суму заборгованості, ми й надалі співпрацюватимемо на попередніх умовах.

Правило 30 секунд

- Коли вам надходить email, не спішіть відкривати приєднання чи переходити за посиланням!!!

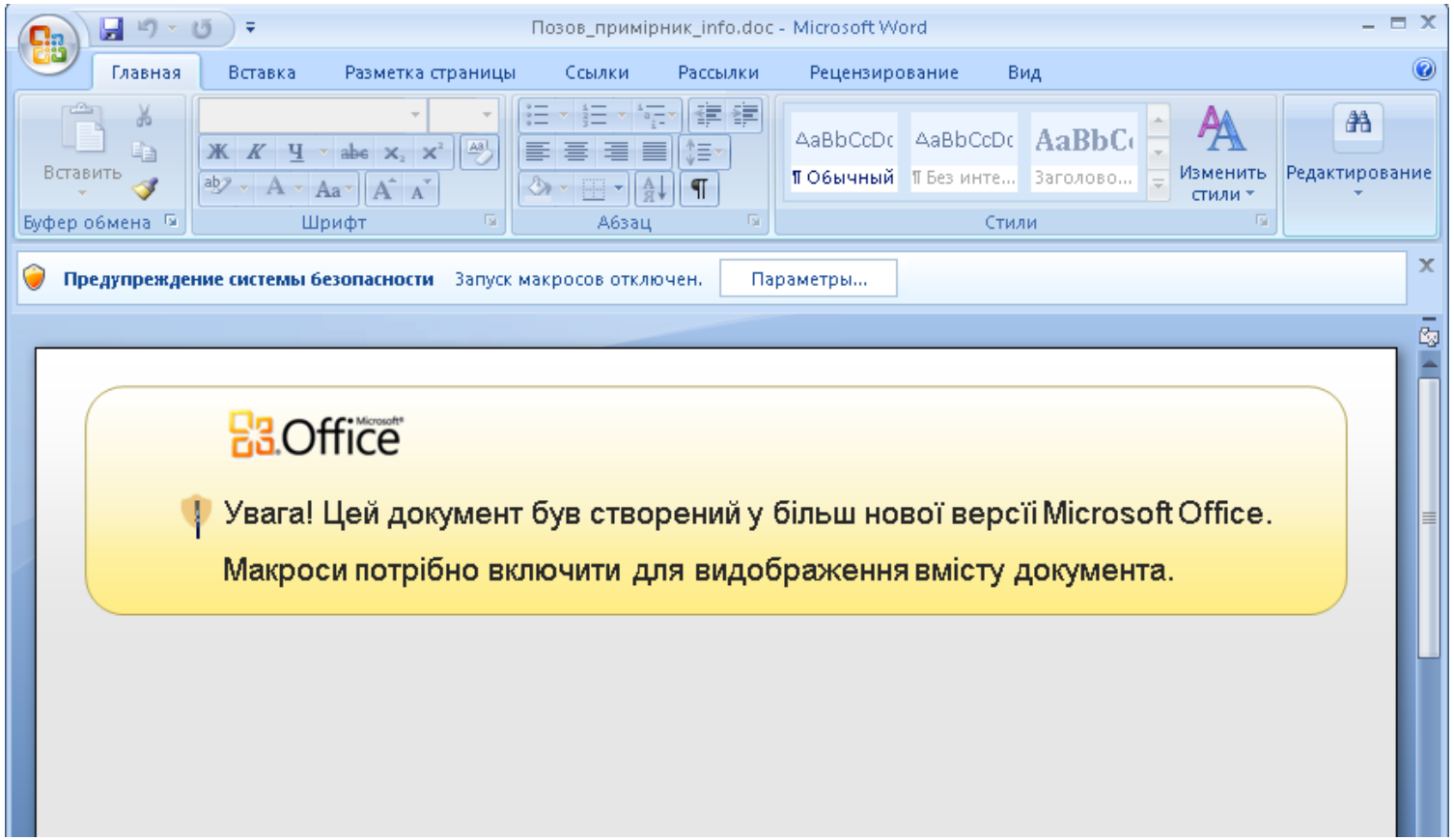
Витратьте 30 секунд щоб уважно перевірити лист:

- Чи співпадає адреса в полі “від” тій компанії про яку йдеться в самому листі?
- Чи співпадає поштова скринька із ПІБ людини яка начебто написала листа?
- Чи немає в тексті орфографічних/граматичних помилок? Відмінки? Слова переплутані?
- Чи є внизу листа корпоративний підпис?

Якщо щось викликає підозру – не нехтуйте можливістю звернутися за телефоном у підписі

і перепитати людину що саме вона вам надіслала? Як правило 90% фішингу виявляються при уважній перевірці змісту листа.

НЕ АКТИВУЙТЕ МАКРОСИ!



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

Сигнатури тупо НЕ встигають

Паролі

Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	[illegible]	123qwe
password1	[illegible]	1q2w3e4r5t
000000	[illegible]	123456789
zaq12wsx	654321	111111
tinkle	gfhjkm	zxcvbnm
qwerty123	777777	1234qwer
monkey	112233	qwer1234
target123	121212	asdfgh
dragon	987654321	marina
1q2w3e4r	159753	q1w2e3r4t5

2014

2013

Rank	Password	Change from 2012
1	123456	*Up 1*
2	password	*Down 1*
3	12345678	*Unchanged*
4	qwerty	*Up 1*
5	abc123	*Down 1*
6	123456789	*New*
7	111111	*Up 2*
8	1234567	*Up 5*
9	iloveyou	*Up 2*
10	adobe123	*New*
11	123123	*Up 5*
12	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
14	[illegible]	[illegible]
15	photoshop	*New*
16	1234	*New*
17	monkey	*Down 11*
18	shadow	*Unchanged*
19	sunshine	*Down 5*
20	12345	*New*

Паролі

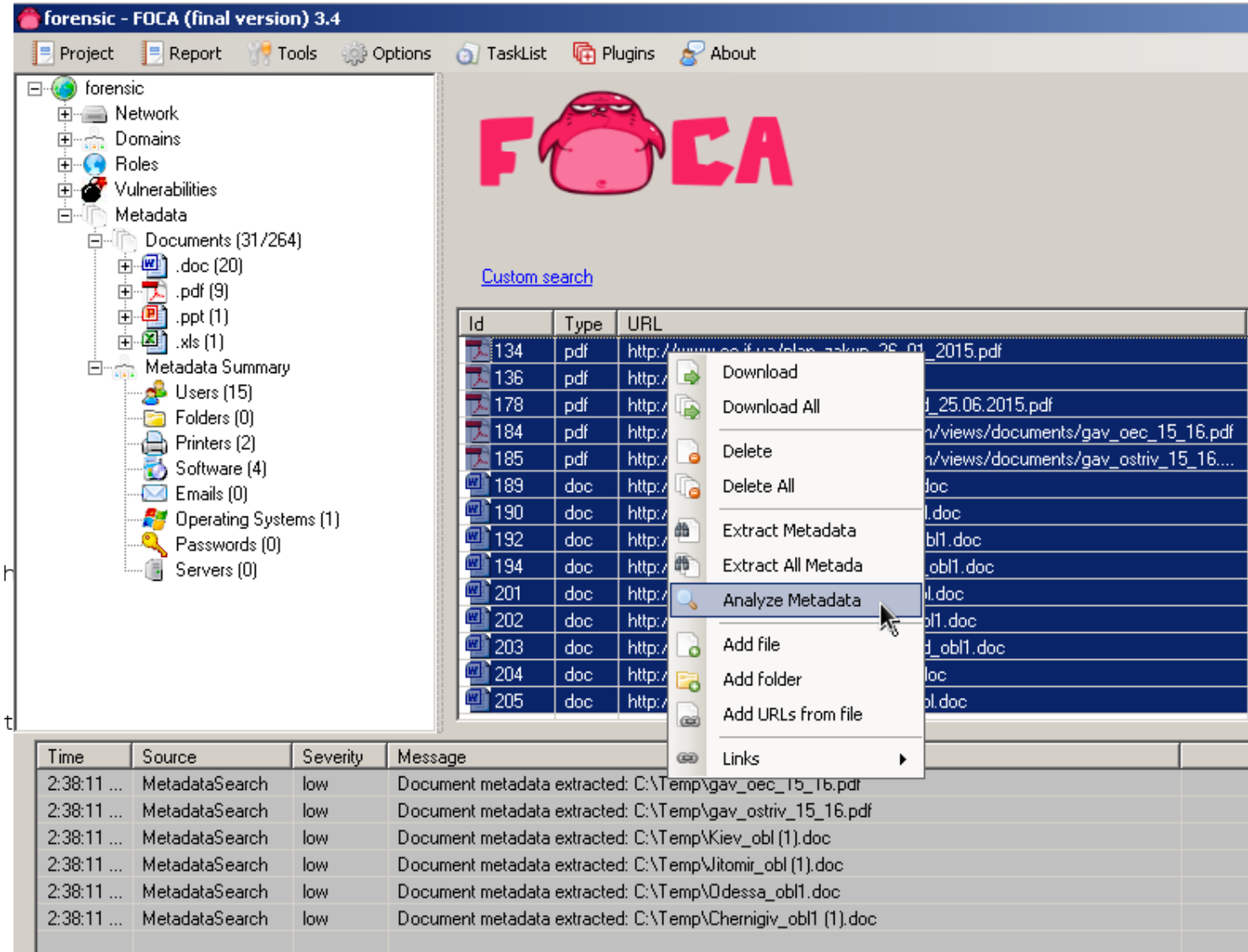
- Паролі потрібно пам'ятати, а не зберігати у бравзерах і т.д.
- Розділіть пароль ні три категорії:
  - Робота (максимум)
  - Особисте (не слабше)
  - Сміття (розсилки, форуми на 1 раз і т. ін)
- Пароль **не повинен** включати інформацію яку ви про себе уже розповіли/запостили!
- Пароль, а радше **парольна фраза** мусить складатися із двох різних половинок
- Пароль мусить бути довжиною **від 10-12** символів
- Варто і потрібно застосовувати методи ускладнення перебору – укр. розкладку і цифри
- Приклади: _k0@L@#p@RK3r_

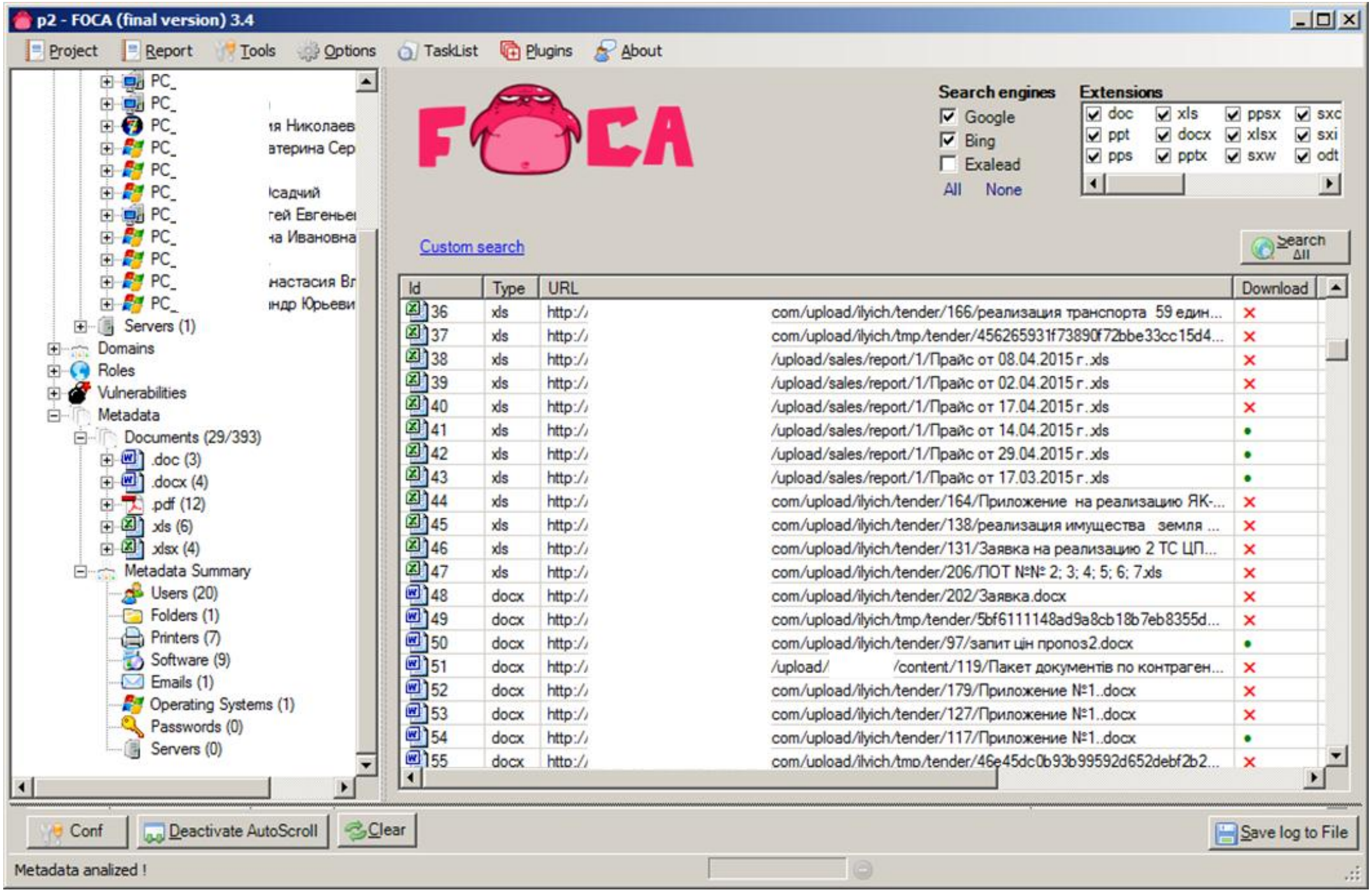
  %Ь»Ь)НТ!І0зк0ь»е (мамонт!сопромат)

  Е1т1_Я»иге1р_3к3вл1м№Veresen` (тіні_забутих_предків#Veresen`)

Документи, 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]
```

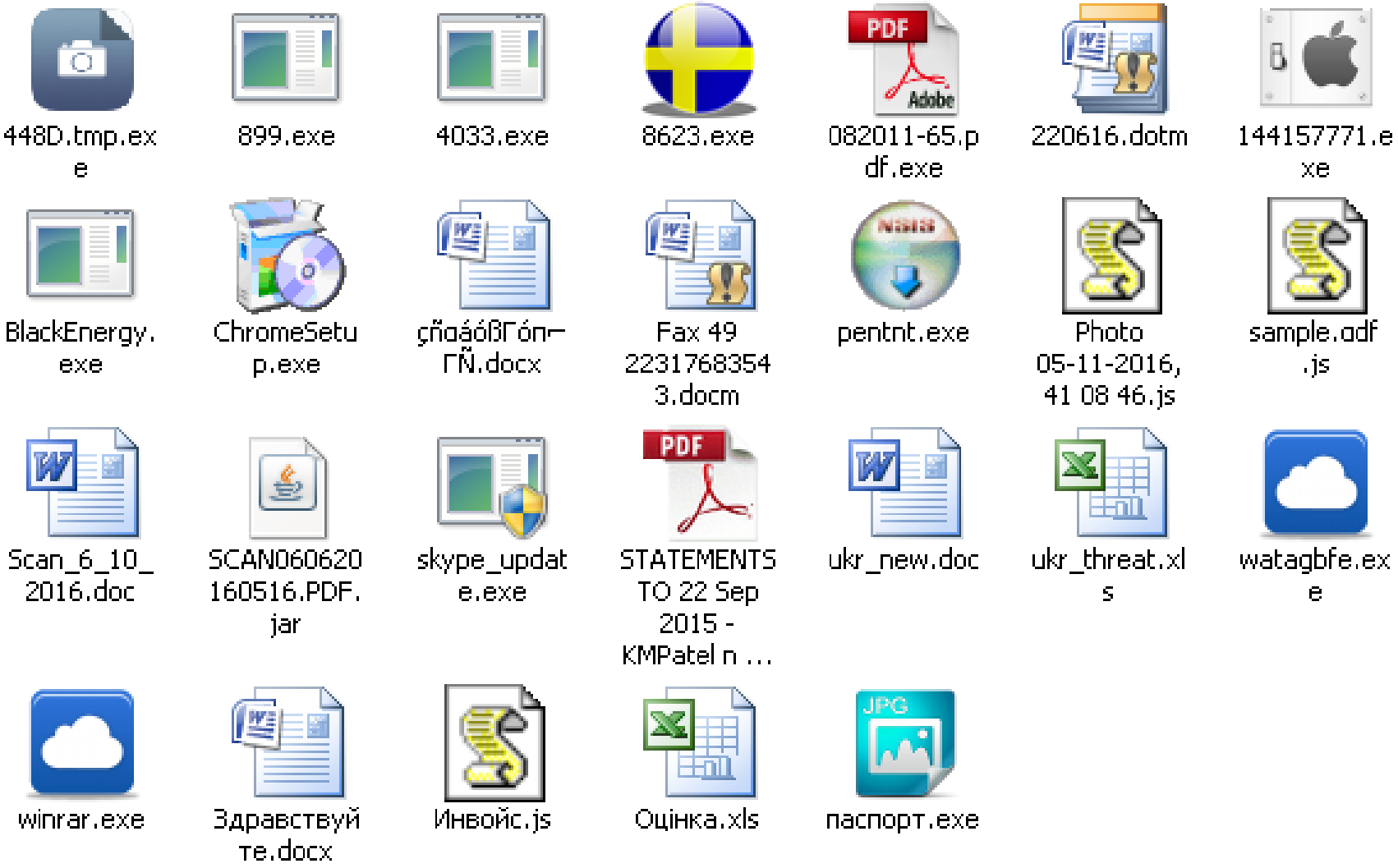
Документи, метаінформація…

- Документи MS Office та інших форматів можуть містити **метаінформацію**

- Не говорячи про зміст документу можна отримати:
  - ім'я автора
  - ім'я системи (!) перевірка запуску
  - електрону адресу
  - мережеві принтери
  - тип ПЗ та ОС (!) експлойти

- **Видаляйте метаінформацію** перед тим як публікувати/пересилати !!!

Програми

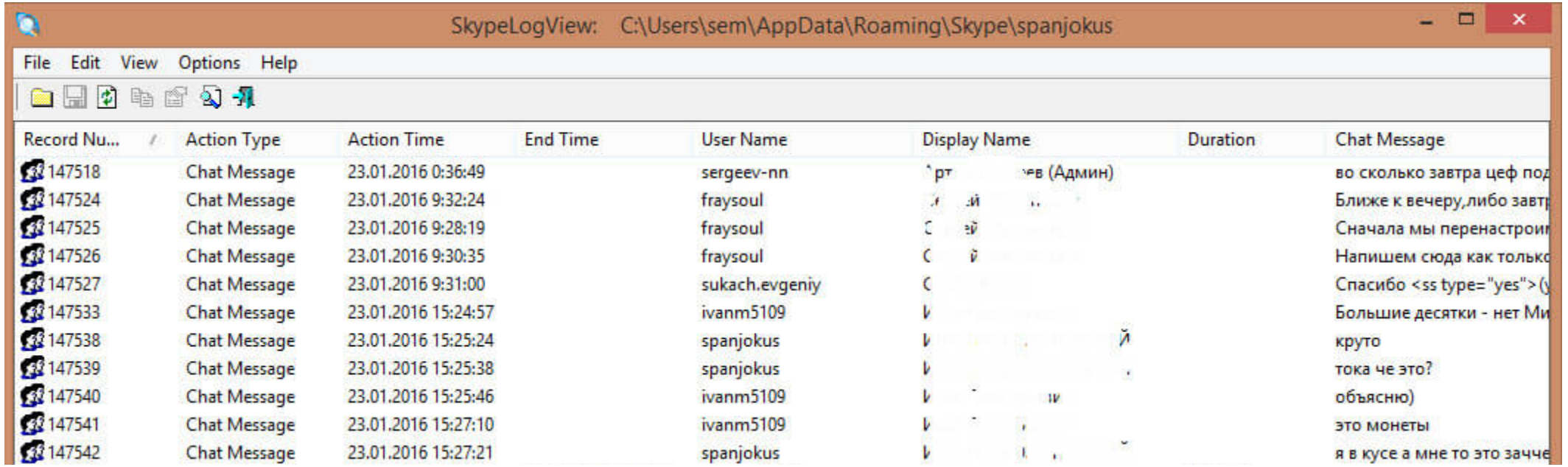

448D.tmp.exe
899.exe
4033.exe
8623.exe
082011-65.pdf.exe
220616.dotm
144157771.exe
BlackEnergy.exe
ChromeSetup.exe
çñöáóßГón–ГÑ.docx
Fax 49 2231768354 3.docm
pentnt.exe
Photo 05-11-2016, 41 08 46.js
sample.adf.js
Scan_6_10_2016.doc
SCAN060620160516.PDF.jar
skype_update.exe
STATEMENTS TO 22 Sep 2015 - KMPatel n ...
ukr_new.doc
ukr_threat.xls
watagbfe.exe
winrar.exe
Здравствуйте.docx
Инвойс.js
Оцінка.xls
паспорт.exe

Програми

- Дистрибутиви брати **тільки** з офіційних джерел!
- **http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/**
- Для платного/зламаного ПЗ можна пошукати альтернативу
- Не користуватися файлозвалищами!
- Своєчасно оновлювати ОС та ПЗ, особилво бравзери
- По можливості, якщо не критично відмовитись від:
  - Adobe Flash -> HTML5
  - Java RE
  - Adobe Acrobat (Reader) -> PDF Exchange Viewer

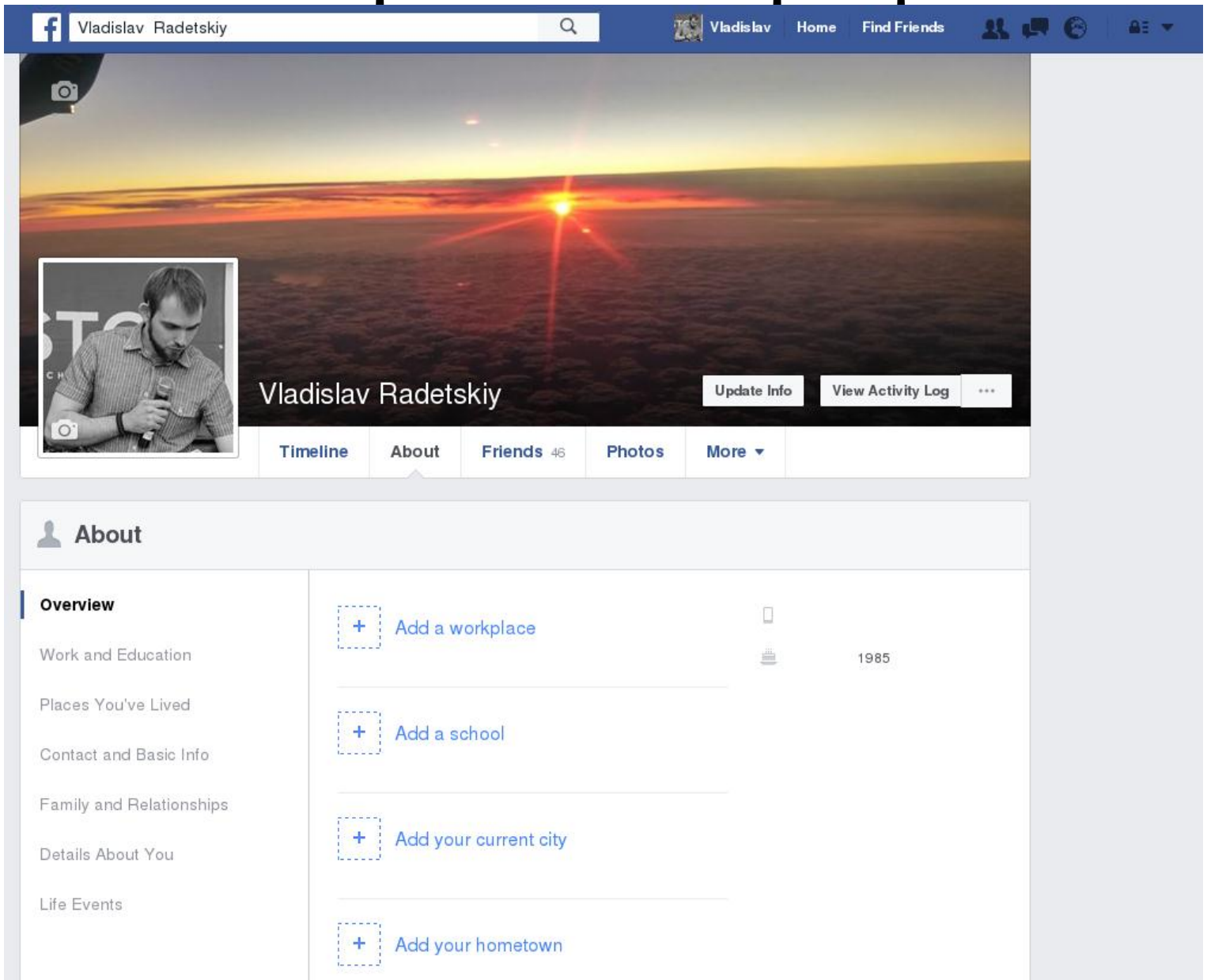
Чужі системи

- Чужа система = чорна діра
- Там можуть бути кейлоггери, трояни та інше ШПЗ
- Не залишайте своїх паролів на чужих системах
- Простий приклад зі Skype



Record Nu...	Action Type	Action Time	End Time	User Name	Display Name	Duration	Chat Message
147518	Chat Message	23.01.2016 0:36:49		sergeev-nn	[illegible] (Админ)		во сколько завтра цеф под
147524	Chat Message	23.01.2016 9:32:24		fraysoul	[illegible]		Ближе к вечеру,либо завтр
147525	Chat Message	23.01.2016 9:28:19		fraysoul	[illegible]		Сначала мы перенастроим
147526	Chat Message	23.01.2016 9:30:35		fraysoul	[illegible]		Напишем сюда как только
147527	Chat Message	23.01.2016 9:31:00		sukach.evgeniy	[illegible]		Спасибо <ss type="yes">(
147533	Chat Message	23.01.2016 15:24:57		ivanm5109	[illegible]		Большие десятки - нет Ми
147538	Chat Message	23.01.2016 15:25:24		spanjokus	[illegible]		круто
147539	Chat Message	23.01.2016 15:25:38		spanjokus	[illegible]		тока че это?
147540	Chat Message	23.01.2016 15:25:46		ivanm5109	[illegible]		объясню)
147541	Chat Message	23.01.2016 15:27:10		ivanm5109	[illegible]		это монеты
147542	Chat Message	23.01.2016 15:27:21		spanjokus	[illegible]		я в кусе а мне то это зачче

Соц. Мережі – закривайте профіль!



Intro

технічна скромняга, одна штука

Photos

Friends

Vladislav Radetskiy updated his cover photo.
October 29 at 9:13pm

Share

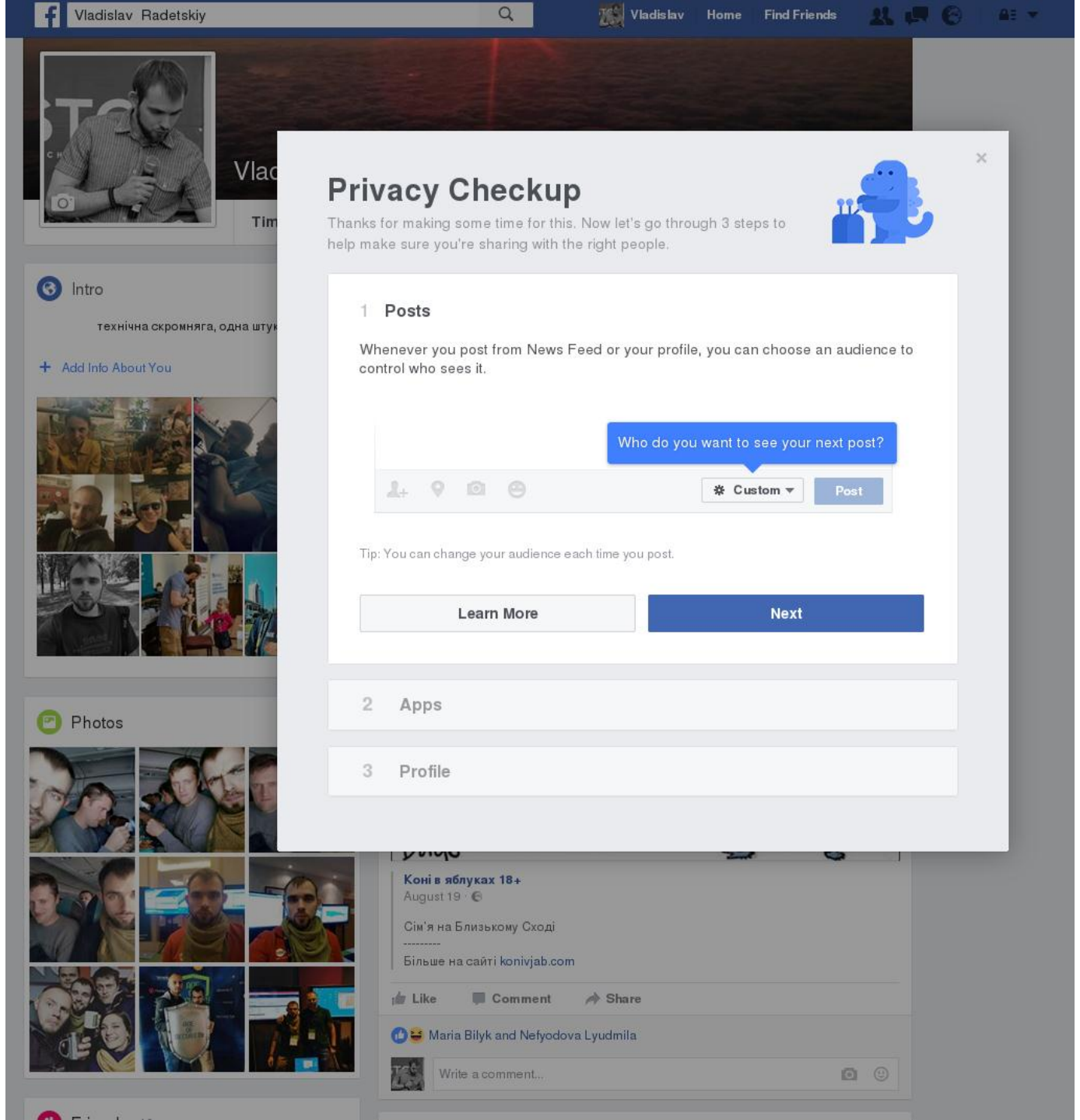
6

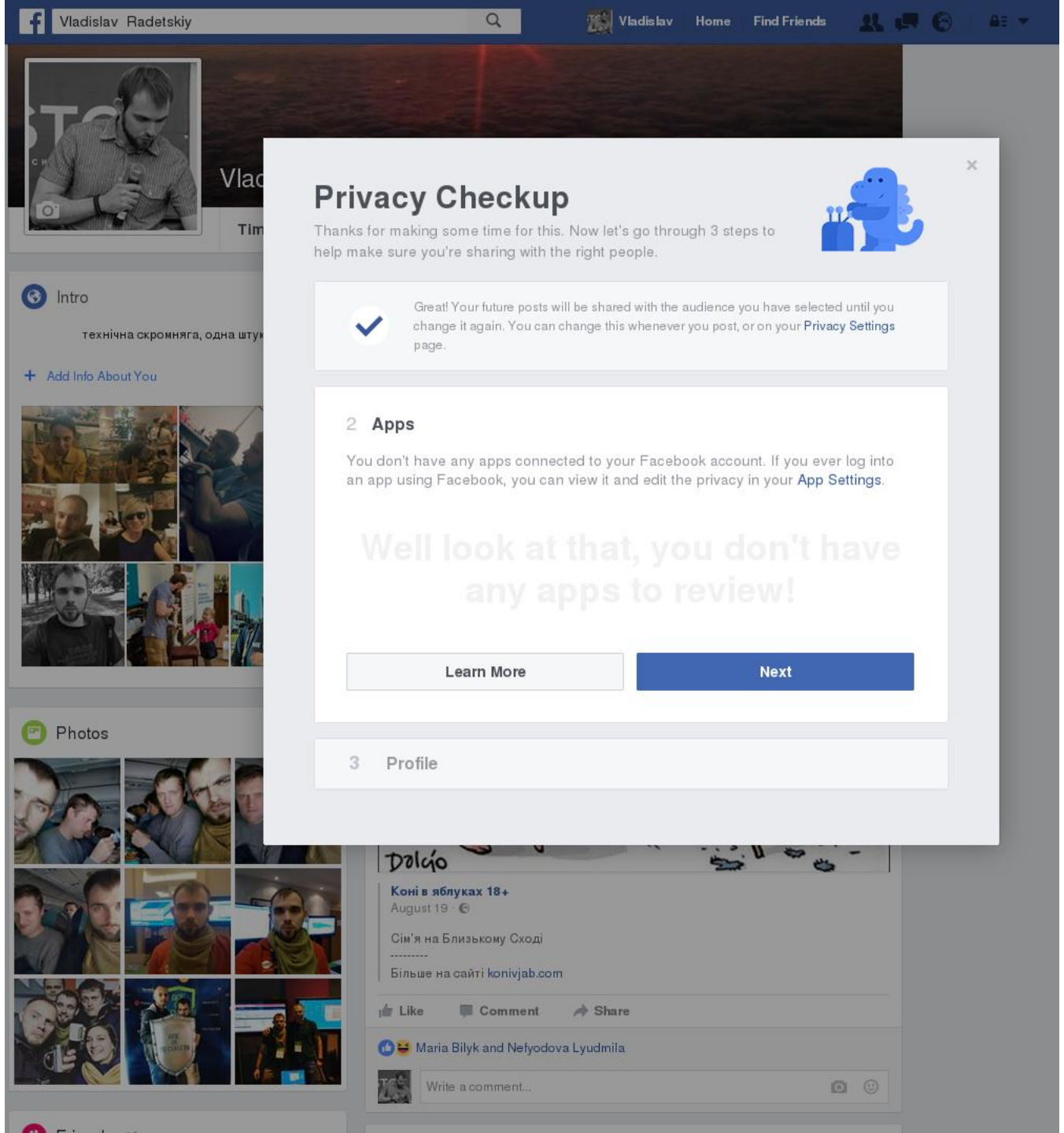
Vladislav Radetskiy
September 23

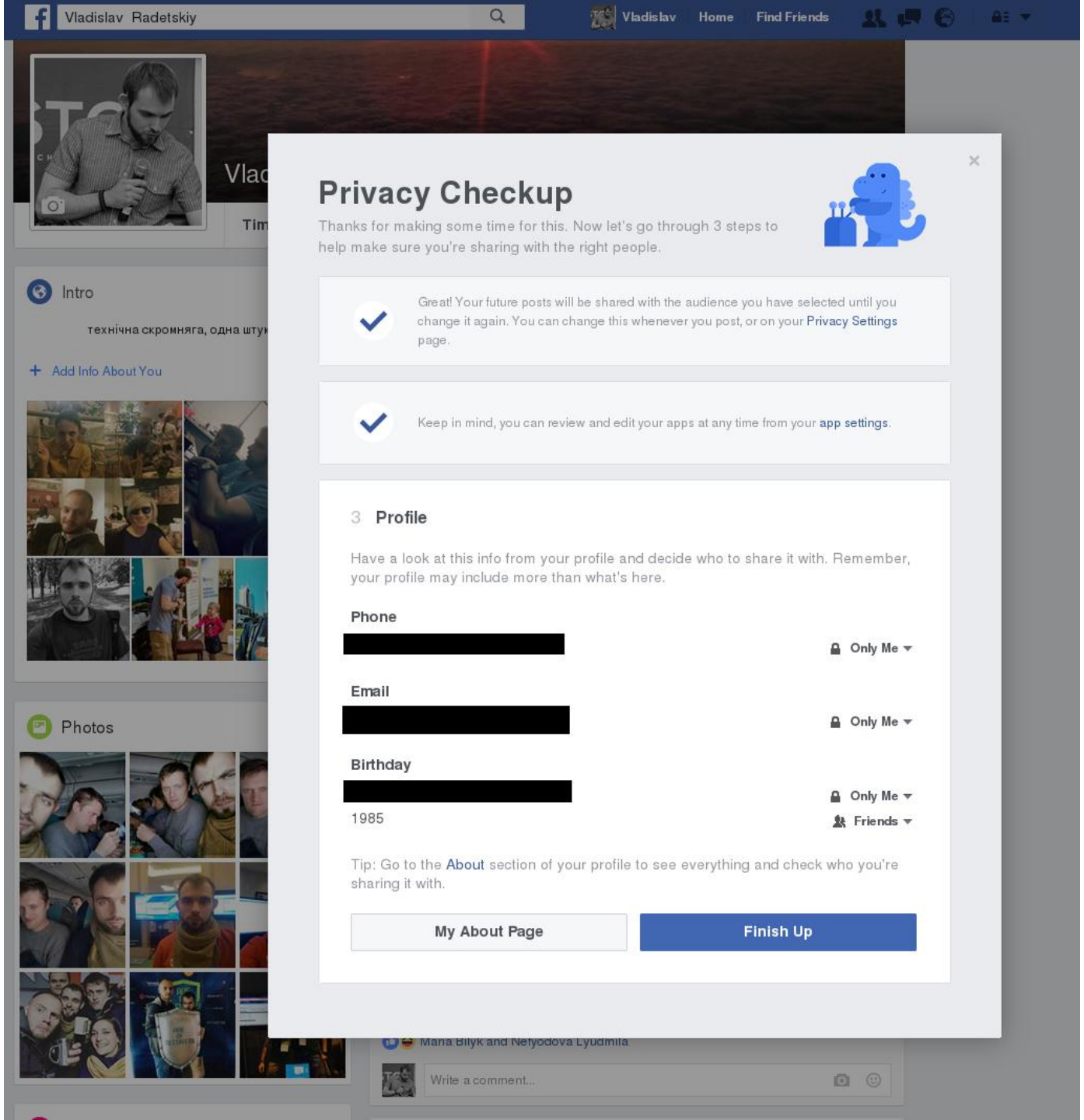
Готуємось...
See Translation

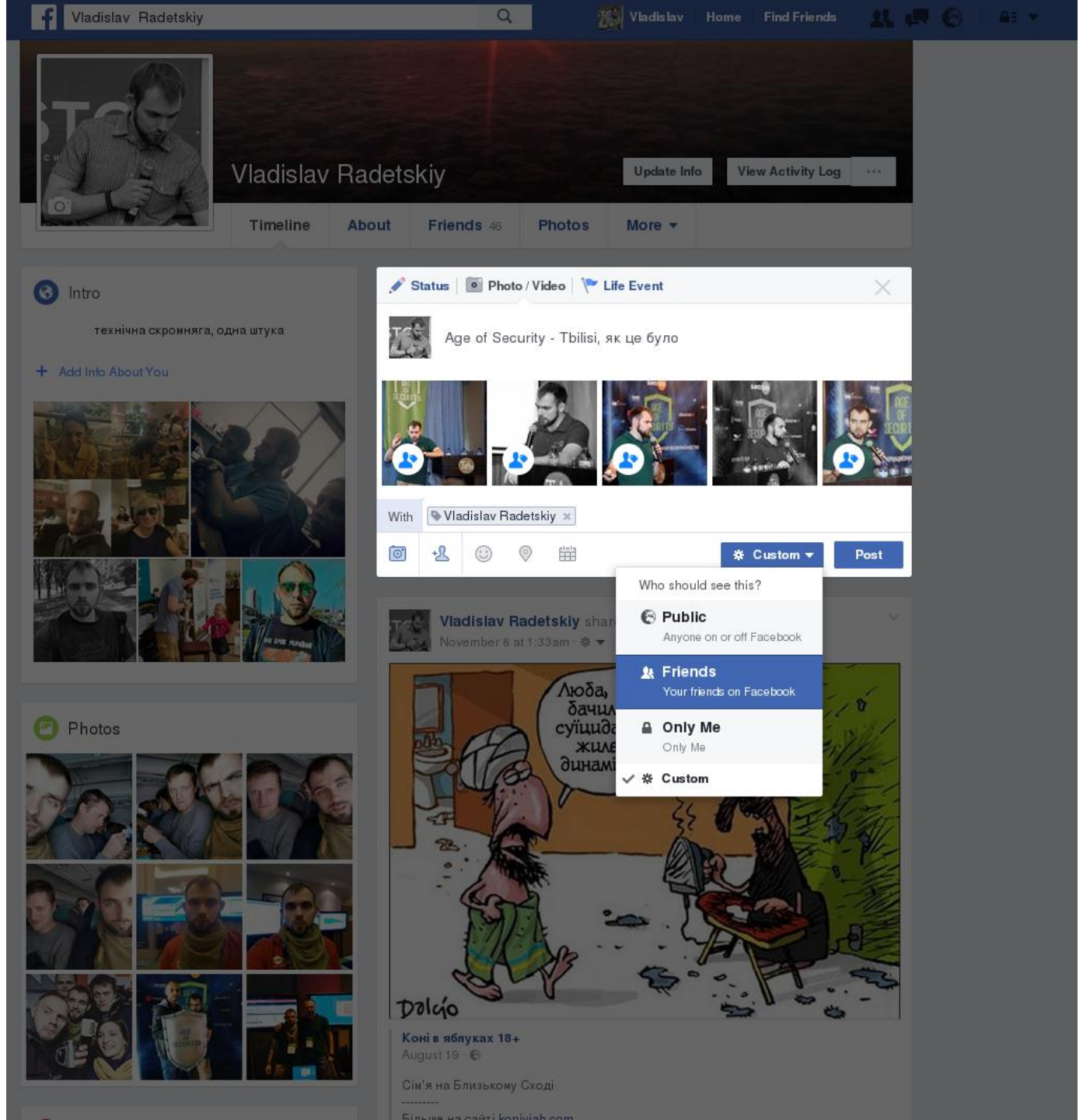
OCT 28 **Age of Security Forum 2016**
Oct 28 - Nov 4
58 people interested · 93 people going
★ Interested

Share


Vladislav Radetskiy
Vladislav
Home
Find Friends
Intro
технічна скромняга, одна штук
Add Info About You
Photos
Коні в яблуках 18+
August 19
Сім'я на Близькому Сході
Більше на сайті konivjab.com
Like
Comment
Share
Maria Bilyk and Nefyodova Lyudmila
Write a comment...
Privacy Checkup
Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.
1 Posts
Whenever you post from News Feed or your profile, you can choose an audience to control who sees it.
Who do you want to see your next post?
Custom
Post
Tip: You can change your audience each time you post.
Learn More
Next
2 Apps
3 Profile


Vladislav Radetskiy
Vladislav
Home
Find Friends
Intro
технічна скромняга, одна штук
Add Info About You
Photos
Privacy Checkup
Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.
Great! Your future posts will be shared with the audience you have selected until you change it again. You can change this whenever you post, or on your Privacy Settings page.
2 Apps
You don't have any apps connected to your Facebook account. If you ever log into an app using Facebook, you can view it and edit the privacy in your App Settings.
Well look at that, you don't have any apps to review!
Learn More
Next
3 Profile
Коні в яблуках 18+
August 19
Сім'я на Близькому Сході
Більше на сайті konivjab.com
Like
Comment
Share
Maria Bilyk and Nefyodova Lyudmila
Write a comment...


Vladislav Radetskiy
Vladislav
Home
Find Friends
Intro
технічна скромняга, одна штук
Add Info About You
Photos
Privacy Checkup
Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.
Great! Your future posts will be shared with the audience you have selected until you change it again. You can change this whenever you post, or on your Privacy Settings page.
Keep in mind, you can review and edit your apps at any time from your app settings.
3 Profile
Have a look at this info from your profile and decide who to share it with. Remember, your profile may include more than what's here.
Phone
[redacted]
Only Me
Email
[redacted]
Only Me
Birthday
[redacted]
1985
Only Me
Friends
Tip: Go to the About section of your profile to see everything and check who you're sharing it with.
My About Page
Finish Up
Maria Bilyk and Nelyodova Lyudmila
Write a comment...


Vladislav Radetskiy
Vladislav
Home
Find Friends
Vladislav Radetskiy
Update Info
View Activity Log
Timeline
About
Friends 46
Photos
More
Intro
технічна скромняга, одна штука
Add Info About You
Photos
Status
Photo / Video
Life Event
Age of Security - Tbilisi, як це було
With
Vladislav Radetskiy
Custom
Post
Who should see this?
Public
Anyone on or off Facebook
Friends
Your friends on Facebook
Only Me
Only Me
Custom
Vladislav Radetskiy
November 6 at 1:33am
Коні в яблуках 18+
August 19
Сім'я на Близькому Сході

Vladislav Radetskiy

Vladislav | Home 3 | Find Friends

Vladislav Radetskiy

Update Info | View Activity Log | ...

Timeline | About | Friends 46 | Photos | More

Intro

технічна скромняга, одна штука

+ Add Info About You

Photos

Status | Photo / Video | Life Event

What's on your mind?

Friends | Post

Vladislav Radetskiy added 5 new photos.
4 mins

Age of Security - Tbilisi, як це було

Like | Comment | Share

Write a comment...

Vladislav Radetskiy shared Коні в яблуках 18+'s photo.
November 6 at 1:33am

Vladislav Radetskiy

Vladislav | Home 3 | Find Friends

This is what your Timeline looks like to: Public **View as Specific Person**

Vladislav Radetskiy

Message ...

Timeline | About | Friends | Photos | More

DO YOU KNOW VLADISLAV?

If you know Vladislav, send him a message.

Intro

технічна скромняга, одна штука

Photos · Nothing to show

Friends

English (US) · Українська · Русский · Español · Português (Brasil) +

Privacy · Terms · Advertising · Ad Choices · Cookies · More

Facebook © 2016

Vladislav Radetskiy updated his cover photo.
October 29 at 9:13pm

Share

6

Vladislav Radetskiy
September 23

Готуємось...

See Translation

Висновки

1) Будьте обережними та уважними при роботі з IT
2) Пам'ятайте те, за що вас можна зачепити
3) Не сидіть під обліковим записом admin/root, не вимикайте UAC (!)

3) Вчасно оновлюйте софт

4) Не забувайте про VirusTotal!

6) Система без Java, Flash та Adobe Reader? + 77 до карми

7) Не залишайте власних слідів на чужих системах (*паролі, облікові записи..*)

8) Не пускайте аби-кого за свої системи (“*подивитись пошту*” *тощо*)

Дякую Вам за увагу!