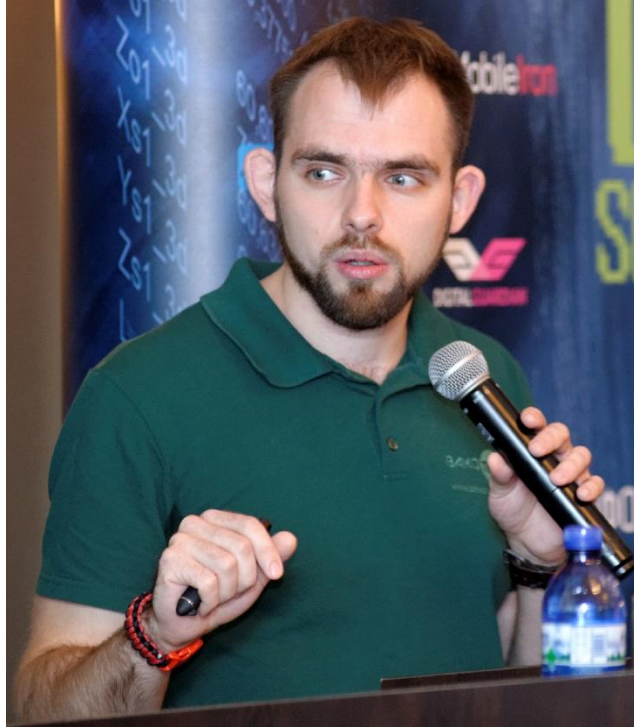


Правила безпечного використання ІТ

Владислав Радецький

vr@bakotech.com

Кілька слів про мене



Владислав Радецький
Technical Lead
vr@bakotech.com

В ІТ галузі офіційно з 2007 року.
Починав як адмін / “анукеу`щик”.
4 роки працював в ІТ-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>

Про що я буду розповідати

- Людський фактор, вразливості людей
- OSINT, соціальна інженерія
- Особливості роботи електронних пристроїв
- Детальний аналіз атак на українські організації
- Рекомендації
 - Паролі
 - Пошук інформації
 - Email
 - Документи, програми, чужі системи, соц. мережі
- Висновки

Теми, які часто ігнорують /
Не беруть до уваги

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

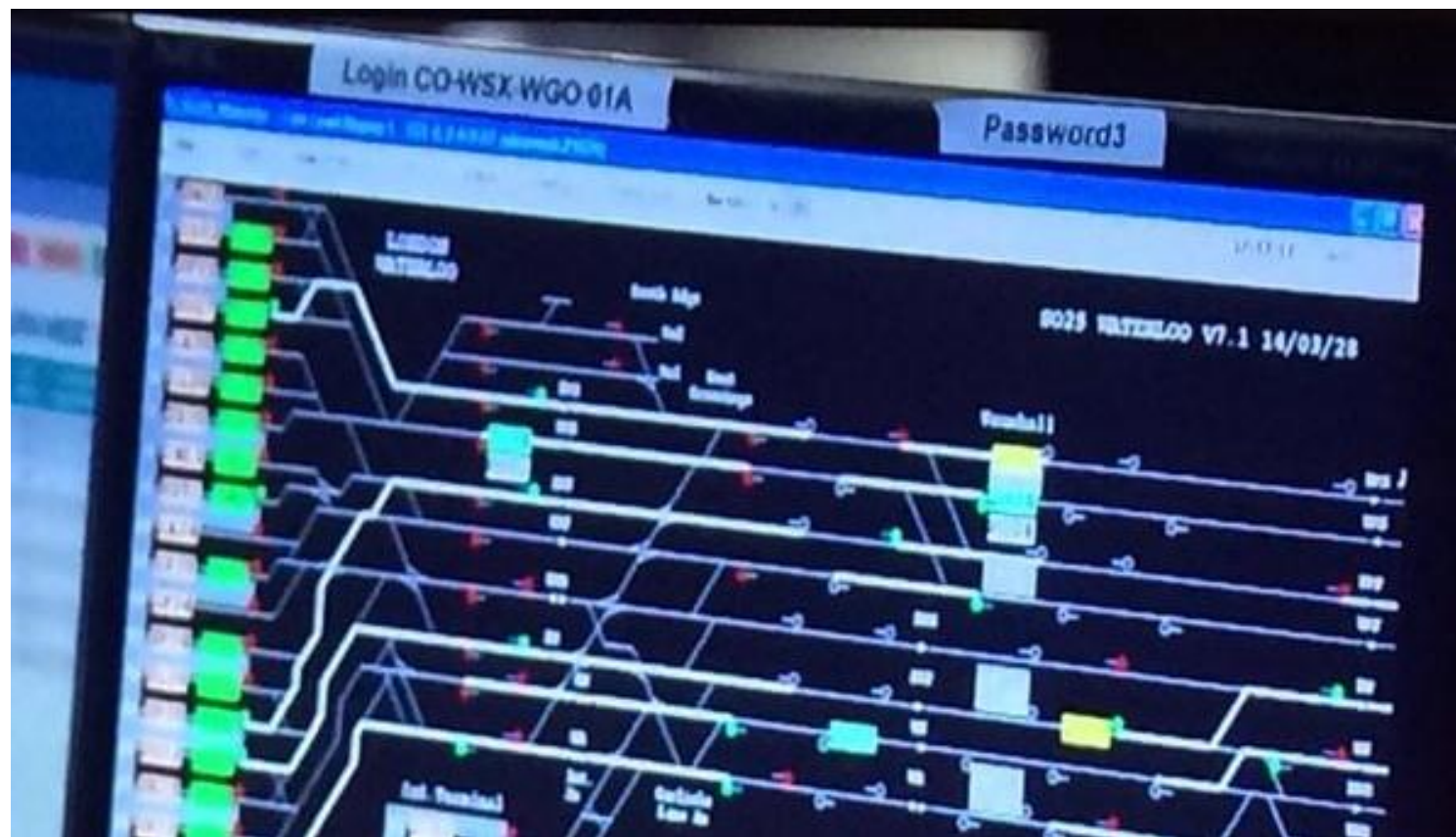
Людський фактор

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



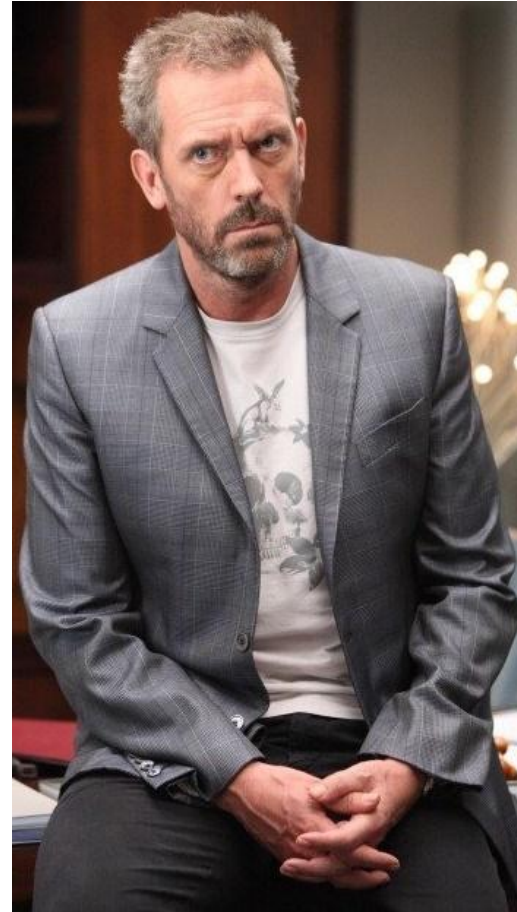
Людський фактор

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



Людський фактор

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



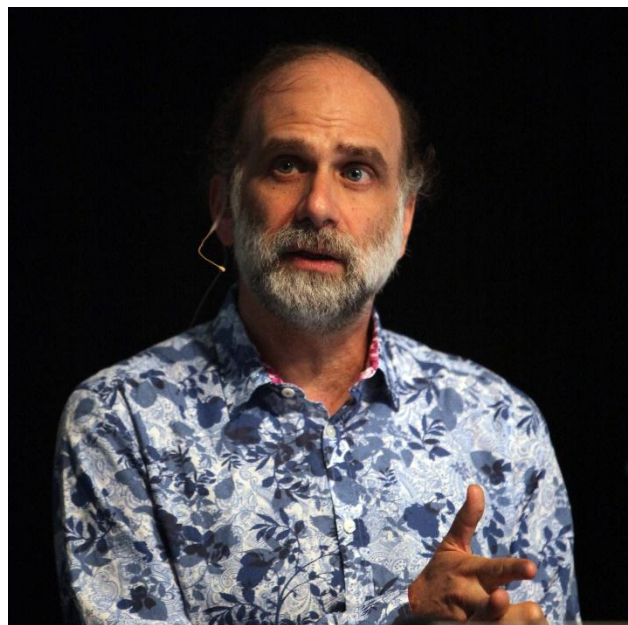
Людський фактор

“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?**)

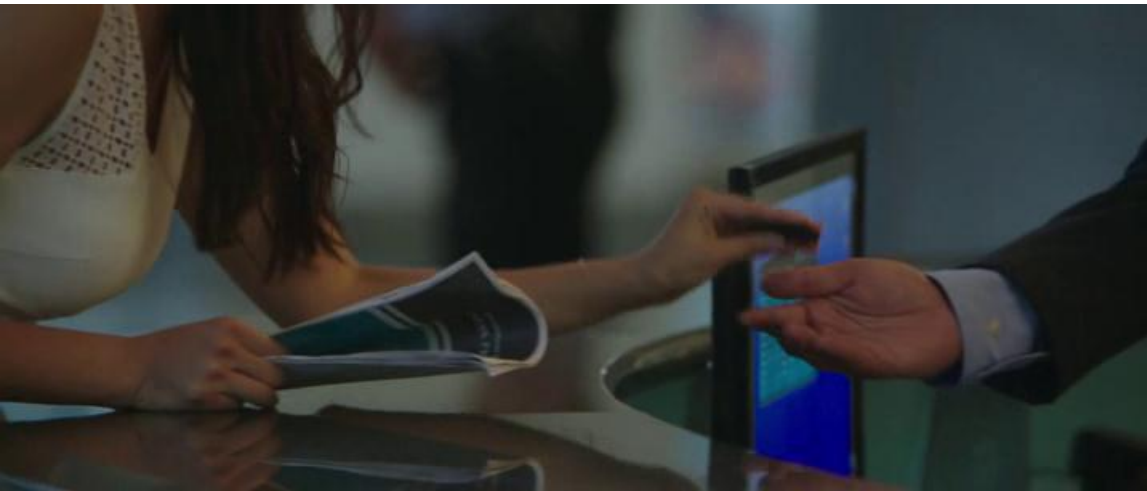
OSINT, соціальна інженерія

Прохання роздрукувати зіпсований документ. **Хіба справжній джентльмен відмовить леді?**



OSINT, соціальна інженерія

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



```
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
#####
```

Порушення політики ІБ



Наслідки

OSINT, соціальна інженерія

Джерела (Google / Youtube вам в поміч)

Володимир Стиран “Прелюдія 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



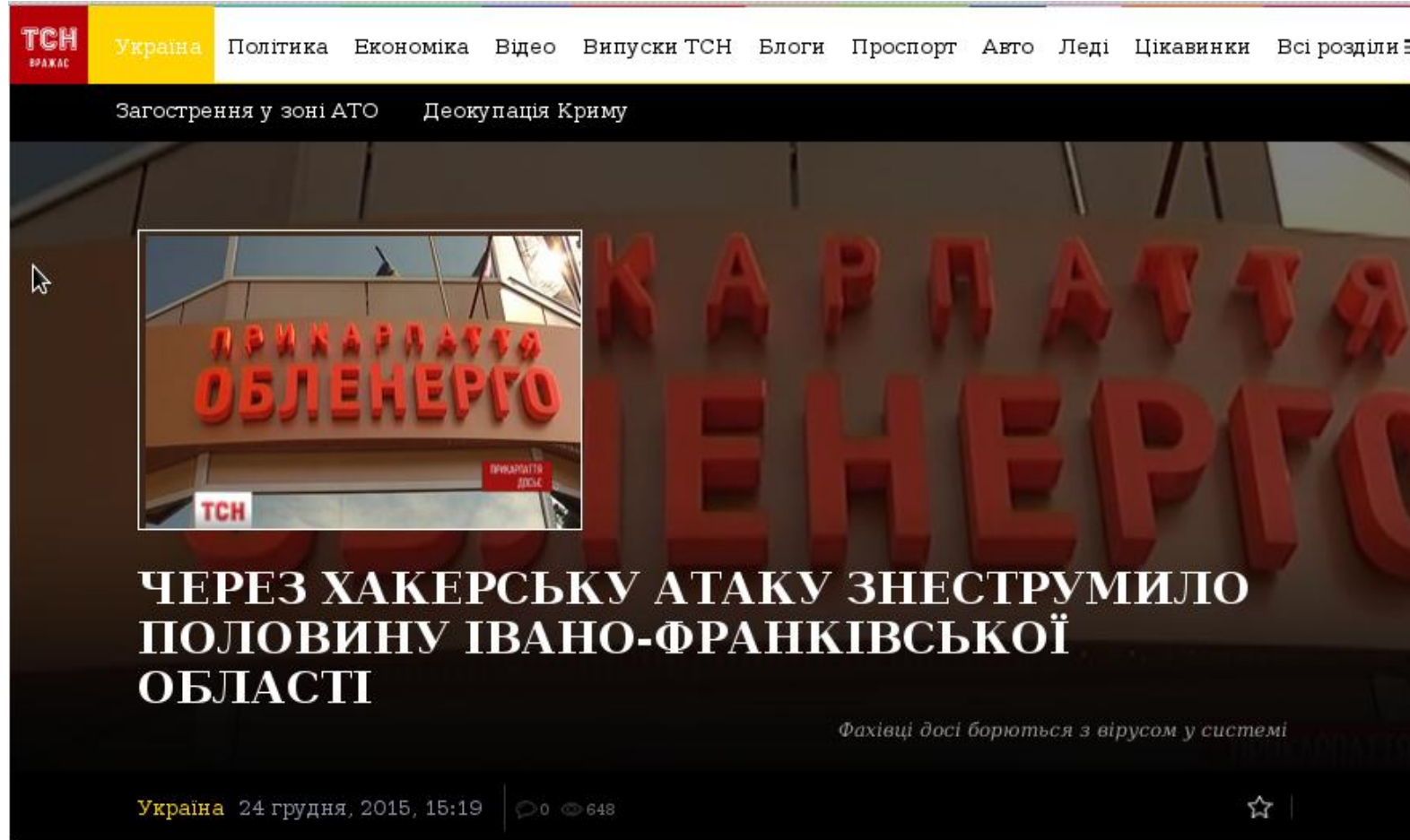
Сучасні цільові атаки
- як це було

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



ЧЕРЕЗ ХАКЕРСЬКУ АТАКУ ЗНЕСТРУМИЛО ПОЛОВИНУ ІВАНО-ФРАНКІВСЬКОЇ ОБЛАСТІ

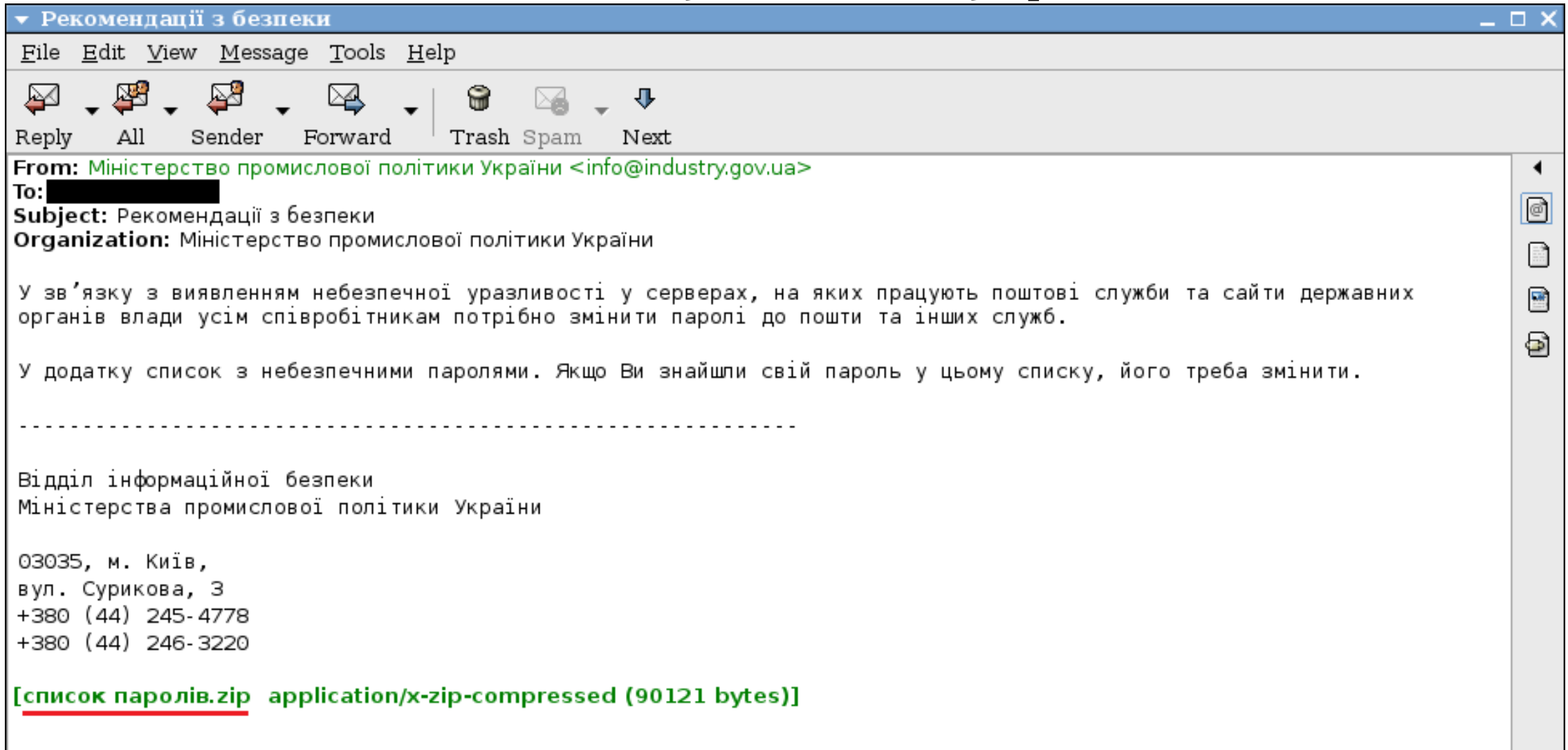
Фахівці досі борються з вірусом у системі

Україна 24 грудня, 2015, 15:19 | 648

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



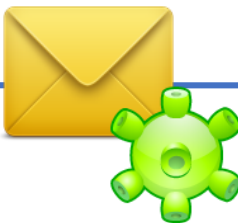
Спроби атак на критичні об'єкти

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

Спроби атак на критичні об'єкти

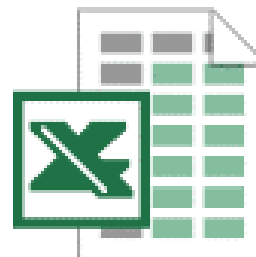
- 23 грудня 2015 енергетика/макроси (**BlackEnergy**)
- 19 січня 2016 енергетика/макроси (**RAT, Sandworm**)
- 1 лютого 2016 широкий спектр/.exe (**ZBot/ZeuS**)
- 4 лютого 2016 широкий спектр/макроси (**Dridex**)
- 3 березня 2016 енергетика / RTF + RCE (**ransomware**)

Типова схема атаки



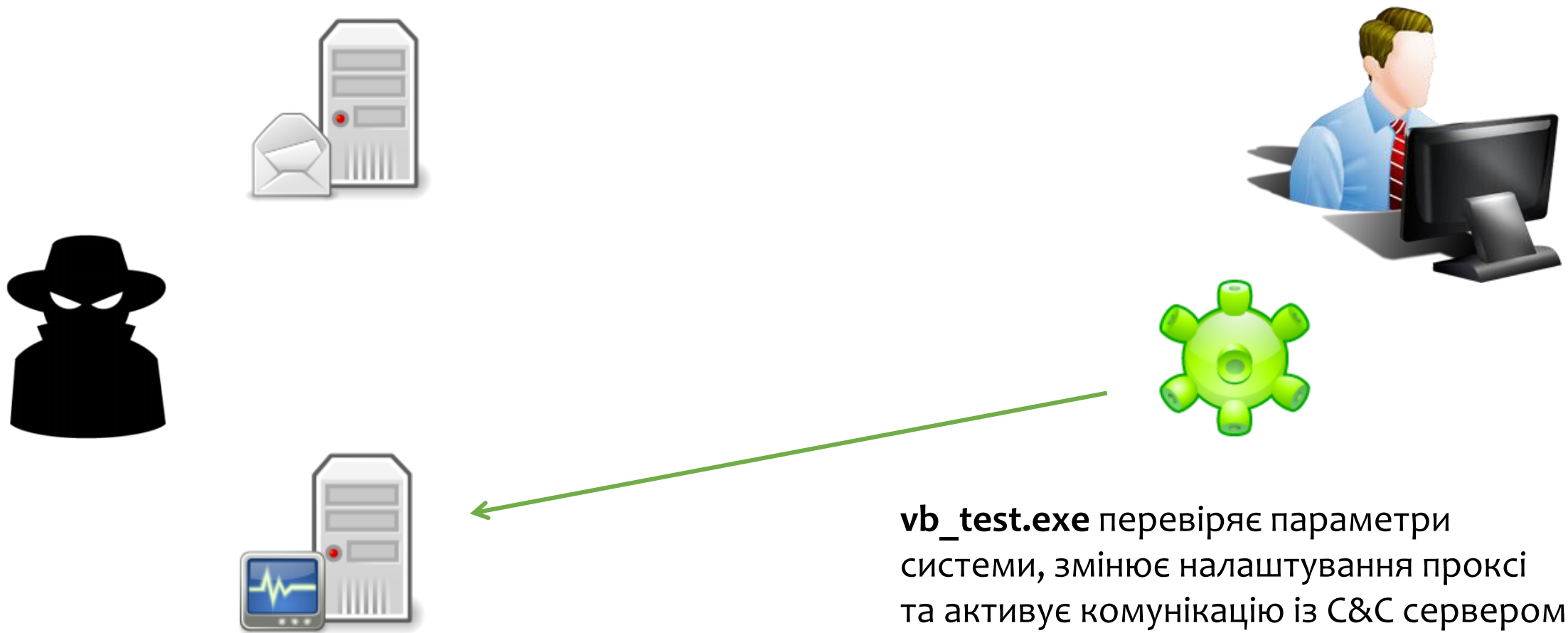
Зловмисники запускають розсилку фішингових листів із приєднаннями. Текст листів підштовхує жертву запустити/відкрити приєднання.

Типова схема атаки



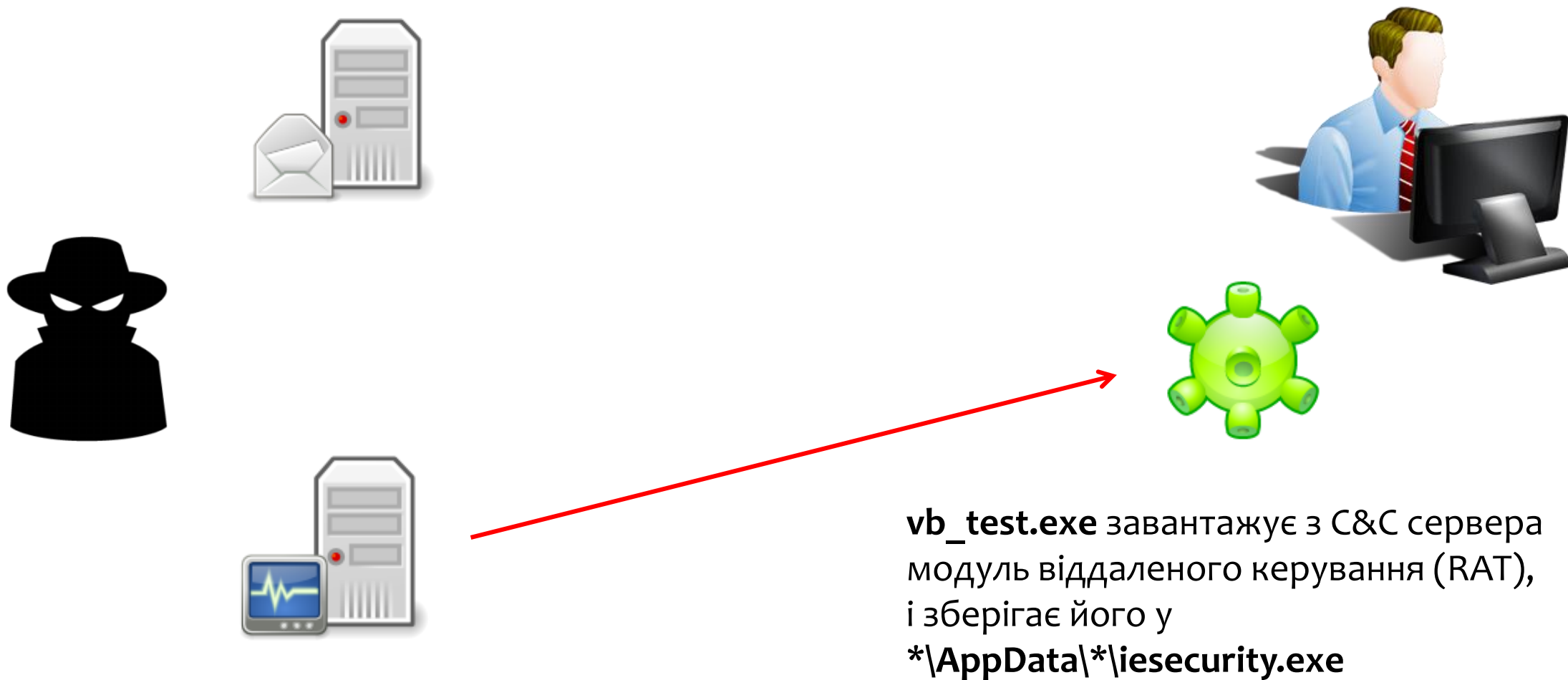
Якщо жертва відкрила приєднання та активувала макрос, він видобуває із себе dropper і зберігає його у **%temp%\vb_test.exe**

Типова схема атаки



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

Типова схема атаки



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

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

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

Предупреждение системы безопасности Запуск макросов отключен.

Рисунок 1

Оцінка структури генерую

Microsoft Office

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

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

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

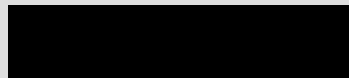


Пн 01.02.2016 14:52

ДП "Изюминка" <sales@aerocredo.ru>

документы по оформлению

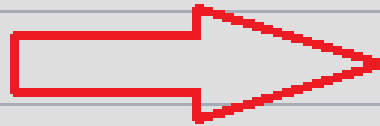
To



This message was sent with High importance.

Message

сканы.zip (770 KB)



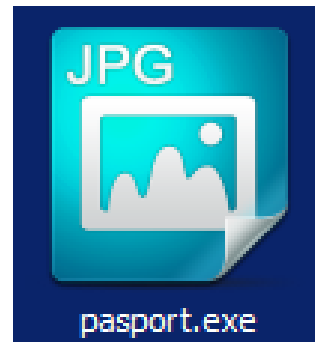
ПАСПОРТ.exe

Добрий день. відправляю вам документи для оформлення довіреностей.

З повагою Фролова Тетяна

ДП "Изюминка"

044-783-22-56



scan.jpg

Розсилка 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...
lsm.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...

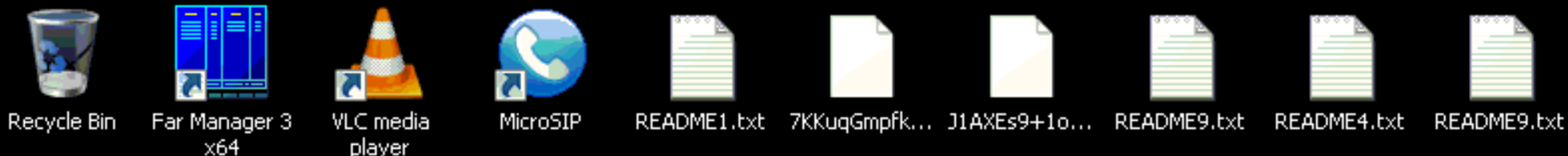
CPU Usage: 2.61% Commit Charge: 35.05% Processes: 50 Physical Usage: 27.89%

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

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 кожен день 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

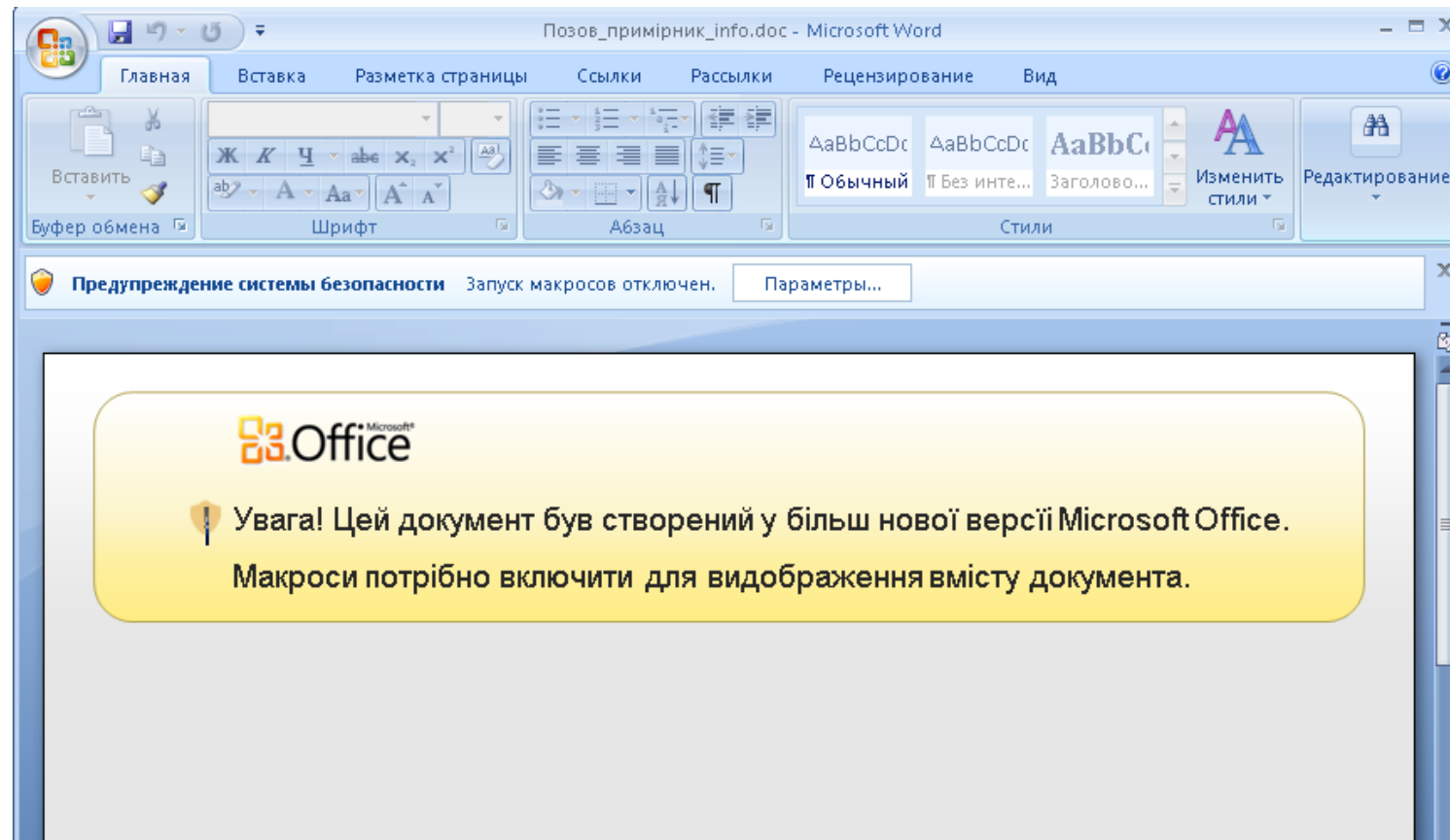
- Коли вам надходить email, не спішіть відкривати приєднання чи переходити за посиланням!!!

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



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

Сигнатури тупо НЕ встигають



Паролі

Gmail

123456
password
123456789
qwerty
12345678
111111
abc123
123123
1234567
1234567890
iloveyou
password1
000000
zaq12wsx
tinkle
qwerty123
monkey
target123
dragon
1q2w3e4r

Yandex

123456
123456789
111111
qwerty
1234567890
1234567
7777777
123321
000000
123123
1234567
123456789
123456789
123456789
654321
gfhjkm
777777
112233
121212
987654321
159753

Mail.ru

qwerty
123456
qwertyuiop
qwe123
qweqwe
klaster
1qaz2wsx
1q2w3e4r
qazwsx
1q2w3e
123qwe
1q2w3e4r5t
123456789
111111
zxcvbnm
1234qwer
qwer1234
asdfgh
marina
q1w2e3r4t5

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	123456789	New
13	1234567890	New
14	letmein	Down 7
15	photoshop	New
16	1234	New
17	monkey	Down 11
18	shadow	Unchanged
19	sunshine	Down 5
20	12345	New

2014

2013

Паролі

- Паролі потрібно пам'ятати, а не зберігати у браузері і т.д.
- Розділіть пароль на 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/запустили!
- 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!Юзк0ь»е (мамонт!сопромат)
E1т1_Я»иге1р_3к3вл1м№Veresen` (тіні_забутих_предків#Veresen`)

- + 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

- | | | | |
|---|--|--|---|
| <input checked="" type="checkbox"/> doc | <input checked="" type="checkbox"/> xls | <input checked="" type="checkbox"/> ppsx | <input checked="" type="checkbox"/> sxc |
| <input checked="" type="checkbox"/> ppt | <input checked="" type="checkbox"/> docx | <input checked="" type="checkbox"/> xlsx | <input checked="" type="checkbox"/> sxi |
| <input checked="" type="checkbox"/> pps | <input checked="" type="checkbox"/> pptx | <input checked="" type="checkbox"/> sxw | <input checked="" type="checkbox"/> 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

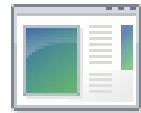
Документи, метаінформація...

- Документи MS Office та інших форматів можуть містити **метаінформацію**
- Не говорячи про зміст документу можна отримати:
 - ім'я автора
 - ім'я системи (!) перевірка запуску
 - електронну адресу
 - мережеві принтери
 - тип ПЗ та ОС (!) експлойти
- **Видаляйте метаінформацію** перед тим як публікувати/пересилати !!!

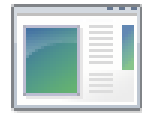
Програми



448D.tmp.exe



899.exe



4033.exe



8623.exe



082011-65.pdf.exe



220616.dotm



144157771.exe



BlackEnergy.exe



ChromeSetup.exe



σῆμαόβΓόν-ΓΝ.docx



Fax 49
2231768354
3.docm



pentnt.exe



Photo
05-11-2016,
41 08 46.js



sample.pdf.js



Scan_6_10_2016.doc



SCAN060620
160516.PDF.jar



skype_update.exe



STATEMENTS
TO 22 Sep
2015 -
KMPatel n ...



ukr_new.doc



ukr_threat.xls



watagbfe.exe



winnrar.exe



Здравствуй
те.docx



Инвойс.js



Оцінка.xls



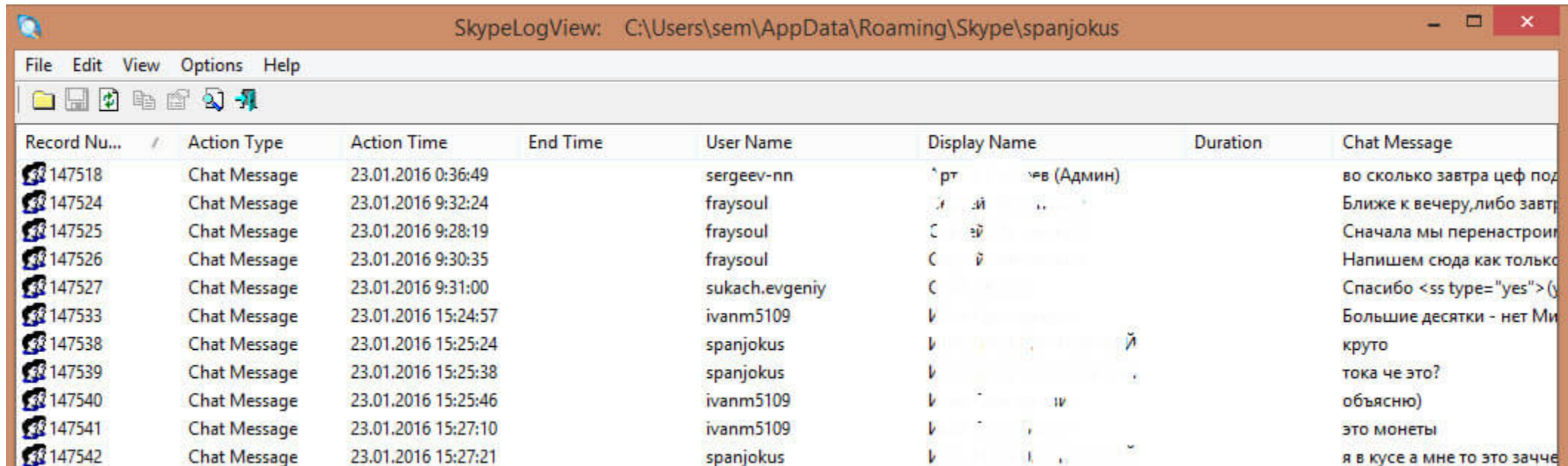
паспорт.exe

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/зламаною ПЗ можна пошукати альтернативу
- Не користуватися файлозвалищами!
- Своєчасно оновлювати ОС та ПЗ, особливо браузер
- 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



The screenshot shows a window titled "SkypeLogView: C:\Users\sem\AppData\Roaming\Skype\spanjokus". The window contains a table with the following columns: Record Nu..., Action Type, Action Time, End Time, User Name, Display Name, Duration, and Chat Message. The table lists several chat messages from January 23, 2016.

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	рт		во сколько завтра цеф под
147524	Chat Message	23.01.2016 9:32:24		fraysoul	й ай		Ближе к вечеру, либо завтра
147525	Chat Message	23.01.2016 9:28:19		fraysoul	С ай		Сначала мы перенастроим
147526	Chat Message	23.01.2016 9:30:35		fraysoul	С й		Напишем сюда как только
147527	Chat Message	23.01.2016 9:31:00		sukach.evgeniy	С		Спасибо <ss type="yes">(y
147533	Chat Message	23.01.2016 15:24:57		ivanm5109	В		Большие десятки - нет Ми
147538	Chat Message	23.01.2016 15:25:24		spanjokus	В		круто
147539	Chat Message	23.01.2016 15:25:38		spanjokus	В		тока че это?
147540	Chat Message	23.01.2016 15:25:46		ivanm5109	В		объясню)
147541	Chat Message	23.01.2016 15:27:10		ivanm5109	В		это монеты
147542	Chat Message	23.01.2016 15:27:21		spanjokus	В		я в курсе а мне то это зачче

Соц. Мережі – закривайте профіль!

The image shows a screenshot of a Facebook profile page for Vladislav Radetskiy. The profile picture is a man with a beard, and the cover photo is a sunset over a body of water. The 'About' section is visible, showing a list of categories on the left and options to add information on the right. The options are: 'Add a workplace' (with a mobile phone icon and the year 1985), 'Add a school', 'Add your current city', and 'Add your hometown'.

Profile Header: Vladislav Radetskiy | Home | Find Friends

Cover Photo: Sunset over water

Profile Picture: Vladislav Radetskiy

Navigation: Timeline | About | Friends 46 | Photos | More

About Section:

- Overview**
- Work and Education
- Places You've Lived
- Contact and Basic Info
- Family and Relationships
- Details About You
- Life Events

Information Options:

- + Add a workplace (1985)
- + Add a school
- + Add your current city
- + Add your hometown

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

Vladislav Radetskiy Timeline Recent



Intro

технічна скромняга, одна штука



Photos



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

Готуюсь...

See Translation



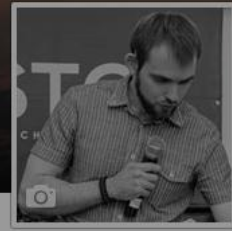
OCT 28 Age of Security Forum 2016

Oct 28 - Nov 4

58 people interested · 93 people going

★ Interested

Share

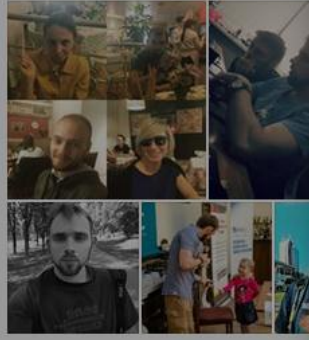


Vlad

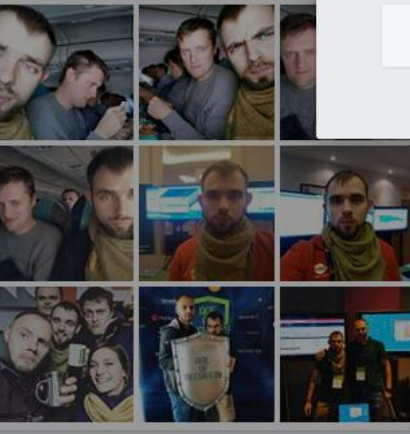
Intro

технічна скромняга, одна шту...

+ Add Info About You



Photos



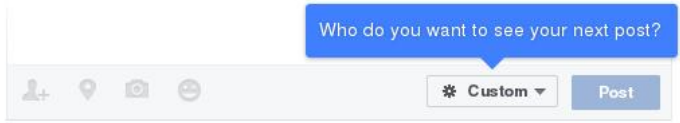
Privacy Checkup



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.

1 Posts

Whenever you post from News Feed or your profile, you can choose an audience to control who sees it.



Tip: You can change your audience each time you post.

[Learn More](#) [Next](#)

2 Apps

3 Profile

Кони в яблуках 18+
August 19 · 🌐

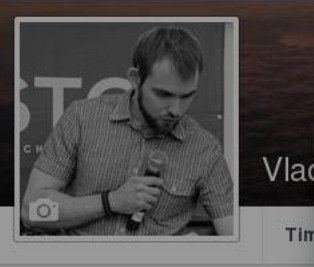
Сім'я на Близькому Сході

Більше на сайті konivjab.com

Like Comment Share

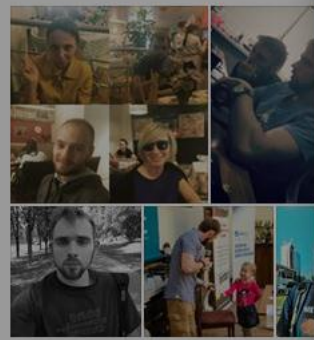
Maria Bilyk and Nefyodova Lyudmila

Write a comment...

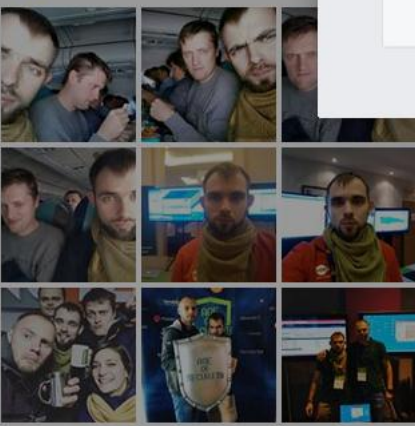


Vlad

Intro
технічна скромняга, одна шту
+ 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

Dolció
 Коні в яблуках 18+
 August 19 · €

Сім'я на Близькому Сході

 Більше на сайті konivjab.com

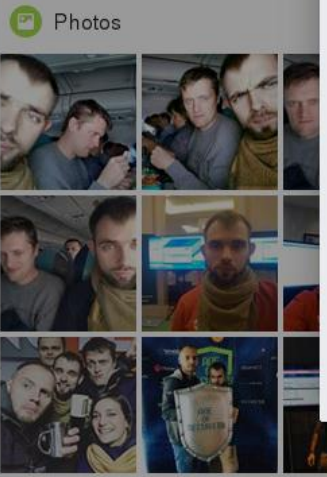
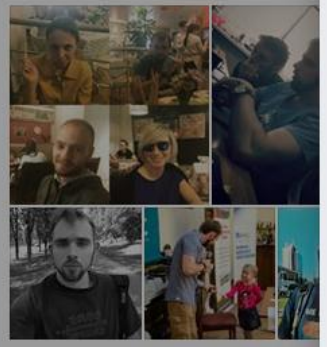
Like Comment Share

Maria Bilyk and Nefyodova Lyudmila

Write a comment...



Intro
технічна скромняга, одна штука
[+ Add Info About You](#)



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 Blyk and Netyodova Lyudmila

Write a comment...



Vladislav Radetskiy

Update Info

View Activity Log

Timeline

About

Friends 46

Photos

More

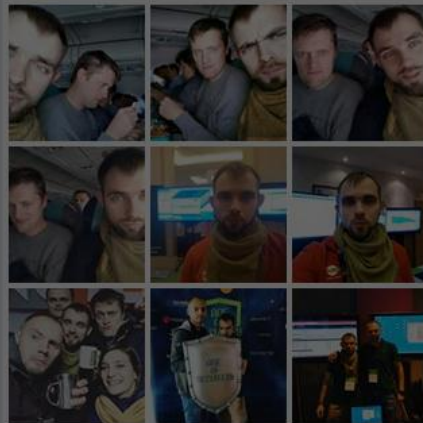
Intro

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 shared November 6 at 1:33am



Кони в яблуках 18+ August 19

Сін'я на Близькому Сході

Більше на сайті koniviah.com



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 ·

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 · עִבְרִית · Português (Brasil)

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 ІТ
- 2) Пам'ятайте те, за що вас можна зачепити
- 3) Не сидіть під обліковим записом admin/root, **не вимикайте УАС (!)**
- 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!