Opti Data

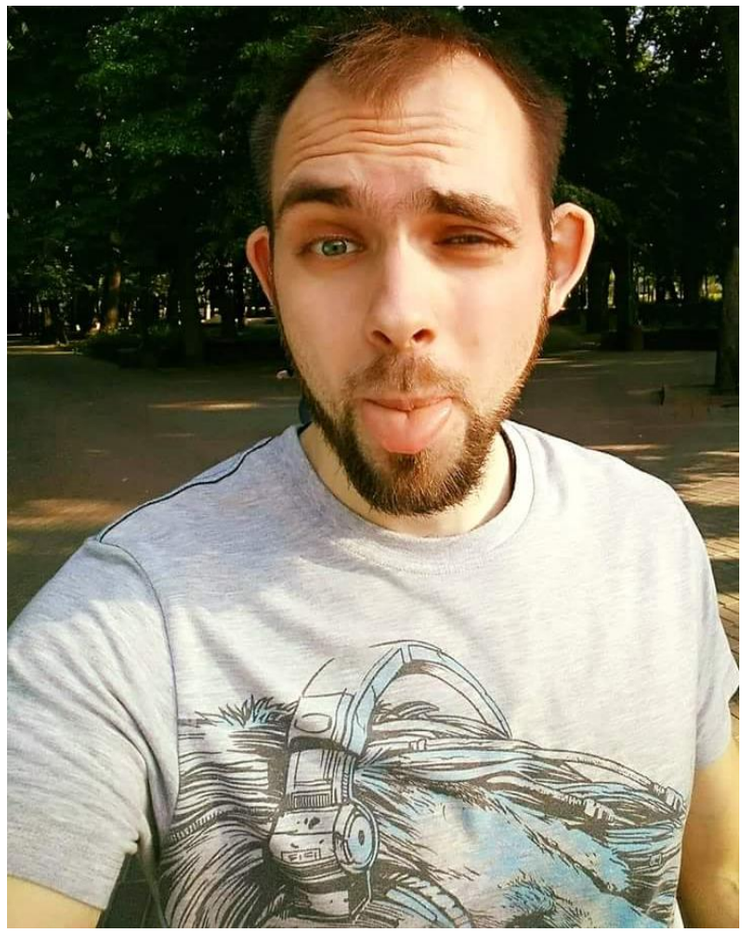
Enforce your security

Боротьба із “шкідниками” Історії з практики

Львів 2018

Владислав Радецький
vr@optidata.com.ua

#whoami



Працюю у компанії OptiData
Аналізую віруси
Пишу статті
Проводжу навчання з різних аспектів ІБ
Допомагаю з проектуванням, впровадженням та супроводом засобів захисту

Прийшов до вас щоб поділитися досвідом

vr@optidata.com.ua
radetskiy.wordpress.com

Opti Data
Enforce your security

Що таке OptiData ?

Ми – це команда спеціалістів з практичним досвідом інтеграції та супроводу рішень з ІБ.

Працюємо лише з тим, в чому розбираємось.

Більшість здійснених нами проектів захищені NDA.

Проектуємо. Навчаємо. Розгортаємо. Захищаємо.

Opti Data
Enforce your security

Важливо !

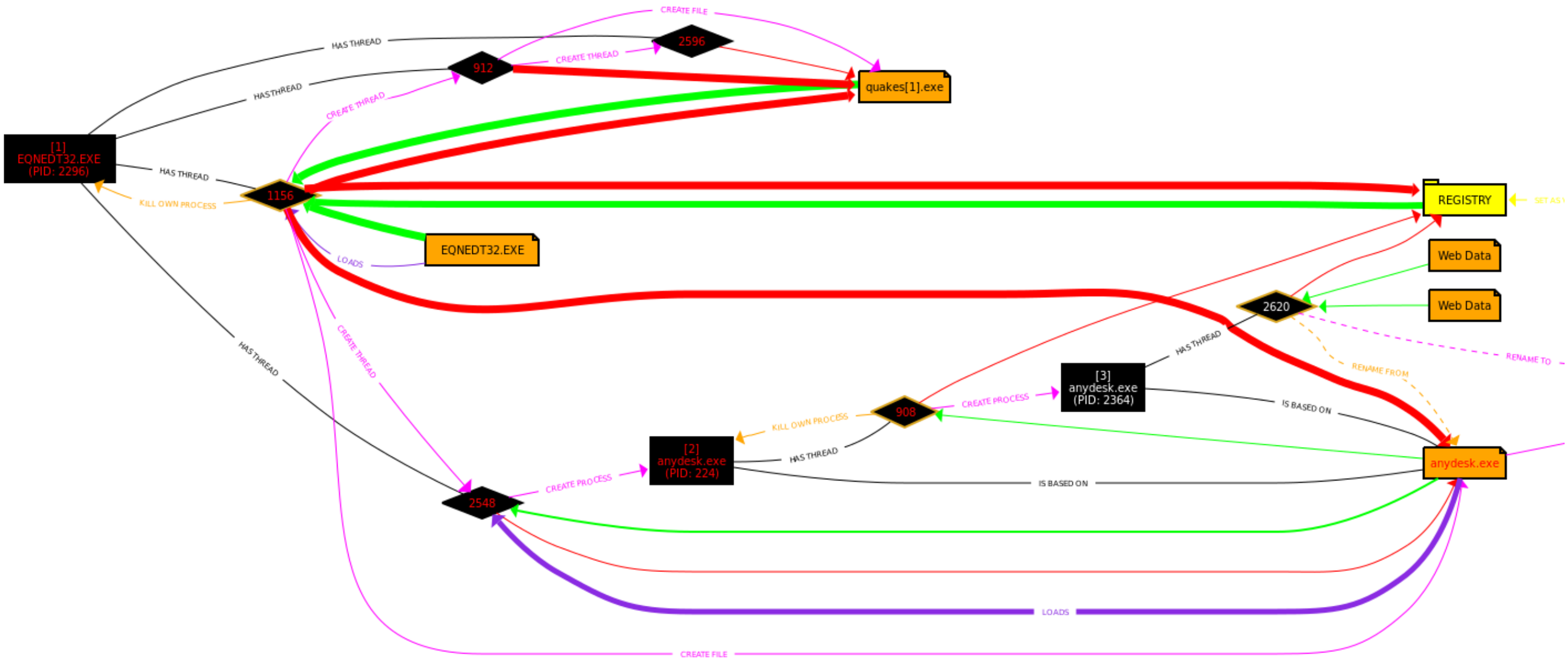
Усе про що я говоритиму – моя особиста точка зору

Усе, що ви сьогодні почуєте може не співпадати
із офіційною позицією компанії

Усі події та персонажі є вигаданими,
а будь-які співпадіння є випадковими

Opti
Data
Enforce your
security

Чого сьогодні не буде



#IOC та звіти шукайте тут:
radetskiy.wordpress.com

Opti Data
Enforce your security

Чого сьогодні не буде

http.request

No.	Time	Destination	Host	Info	User-Agent
8	12:49:13	140.128.99.228	servicelearning.thu.edu.tw	GET /quakes.exe HTTP/1.1	Mozilla/4.0 (compatible; MSIE 7
-	12:49:48	91.235.116.153	nextlevlcourier.com	POST /locky/quakes/anel/five/fre.php HTTP/1.0	Mozilla/4.08 (Charon; Inferno)
-	12:49:49	91.235.116.153	nextlevlcourier.com	POST /locky/quakes/anel/five/fre.php HTTP/1.0	Mozilla/4.08 (Charon; Inferno)
-	12:49:49	91.235.116.153	nextlevlcourier.com	POST /locky/quakes/anel/five/fre.php HTTP/1.0	Mozilla/4.08 (Charon; Inferno)
-	12:50:49	91.235.116.153	nextlevlcourier.com	POST /locky/quakes/anel/five/fre.php HTTP/1.0	Mozilla/4.08 (Charon; Inferno)

Process Tree - C:\ddd\911.PML

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Command	Owner	Image Path
DllHost.exe (1336)	C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}	APM11\operator	C:\Windows\system32\DllHost.exe
EQNEDT32.EXE (2296)	"C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	APM11\operator	C:\Program Files (x86)\Common Files\Microsoft
anydesk.exe (224)	"C:\Users\operator\AppData\Roaming\anydesk.exe"	APM11\operator	C:\Users\operator\AppData\Roaming\anydesk
anydesk.exe (2364)	"C:\Users\operator\AppData\Roaming\anydesk.exe"	APM11\operator	C:\Users\operator\AppData\Roaming\anydesk

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

anydesk.exe — File not found: C:\Users\operator\AppData\Roaming/Microsoft/Skype.exe.exe

Roaming/Microsoft/Skype.exe.exe

#IOC та звіти шукайте тут:
radetskiy.wordpress.com

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

12-15 травень

WannaCry

+C2, Mimikatz, SMB, +service, -MBR, -MFT, -signed, $300 - $600

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

17-18 травень

xData

HOW_CAN_I_DECRYPT_MY_FILES.txt — Блокнот

Файл Правка Формат Вид Справка

```
Your IMPORTANT FILES WERE ENCRYPTED on this computer: documents, databases, photos, videos, etc.

Encryption was produsedusing unique public key for this computer.
To decrypt files, you need to obtain private key and special tool.

To retrieve the private key and tool find your pc key file with '.key.~xdata~' extension.
Depending on your operation system version and personal settings, you can find it in:
'C:/',
'C:/ProgramData',
'C:/Documents and Settings/All Users/Application Data',
'Your Desktop'
folders (eg. 'C:/PC-TTT54M#45CD.key.~xdata~').

Then send it to one of following email addresses:

begins@colocasia.org
bilbo@colocasia.org
frodo@colocasia.org
trevor@thwonderfulday.com
bob@thwonderfulday.com
bil@thwonderfulday.com

Your ID: APM11#A60E545F1A6FDF8578BA6FA7CCB93E91

Do not worry if you did not find key file, anyway contact for support.
```

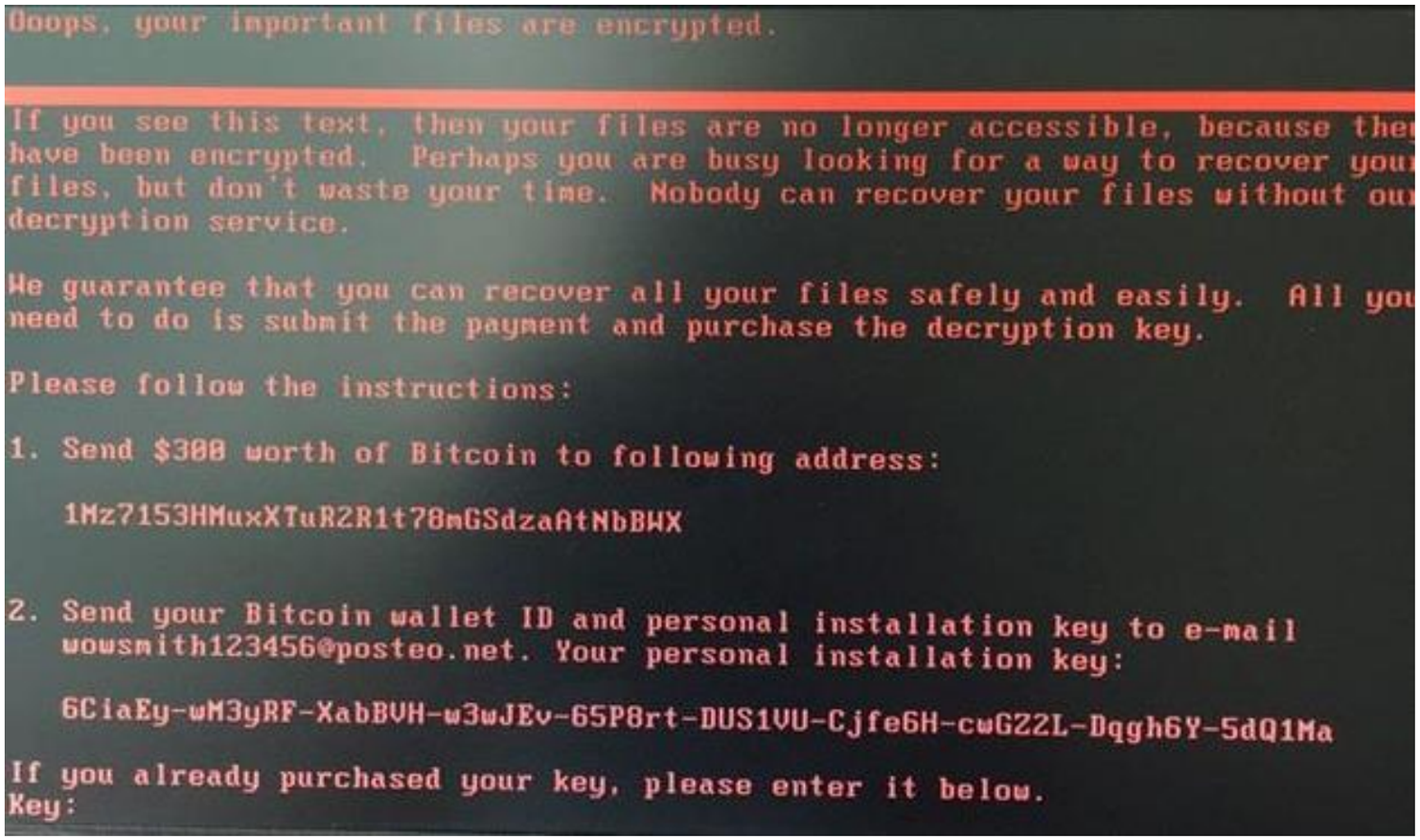
-C2, Mimikatz, SMB, -MBR, -MFT, -signed, $100 - $600

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

27 червень

PetyaA



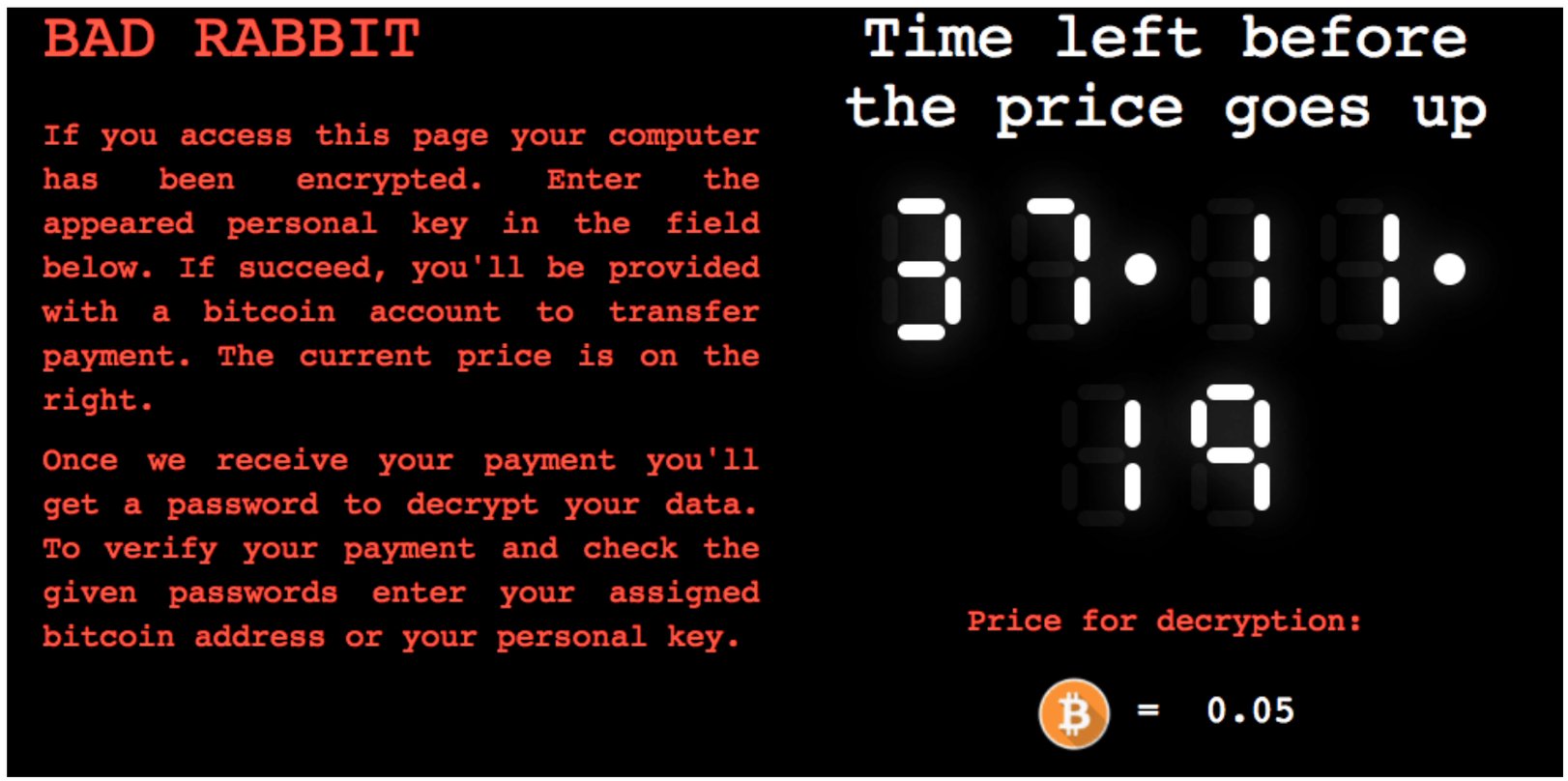
-C2, Mimikatz, SMB, +service, +MBR, +MFT, +signed, $300

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

24 жовтень

BadRabbit



-C2, Mimikatz, SMB, +service, +MBR, +MFT, +signed, $300

Opti Data
Enforce your security

WannaCry	Petya	Bad Rabbit
WannaCry 2.0, WannaCrypt0r, WannaCrypt, WCrypt, WCRY	ExPetr, PetWrap, NotPetya,Nyetya, Petna	Bad Rabbit
12 May 2017	28 June 2017	24 October 2017
UK, RU, UKR, IN, TW	UKR, DE, TR, BG, JPN, US	UKR, RU, BG, TR
NHS UK, Telefonica Spain, FedEx, Deutsche Bahn, Nissan, Iberdrola and Gas Natural, All Indian ATMs, VTB RU Bank, University of Waterloo, RZD RU, Portugal Telecom, etc.	Maersk Group; Maerk Line, APM Terminals and Damco, Saint-Gobain, Mondelez International, Merck & Co., WP, Evraz and Rosneft, DLA Piper, Heritage Valley Health System, etc.	UKR subway, Odessa Airport, Interfax, Fontanka.ru
Telecoms, universities, energy & gas, public systems, banks, transport, public sector, automotive, media	Shipping, telecoms, energy, public systems, steel and oil, legal, pharmaceutical, media	Media, transportation
Likely financial gain	Likely destruction/disruption	Likely destruction/disruption
Likely North Korean-based actors	Likely Russian-based actors	Likely Russian-based actors
Malicious email spam campaigns	Malicious email spam campaigns, Hacking Ukraine supply chain "MeDoc" and using automatic update feature to download malware	Original server to deliver malware (after ~6hrs down), Compromised websites (drive-by download)
Requires connection with attacker's C2 prior execution	Able to execute, spread and encrypt without C2 connection	Requires connection with C2 prior execution, if this fails, use of WMI to remotely execute the malware
EternalBlue, DoublePulsar, shellcode injection	EternalRomance, EternalBlue	EternalRomance-like, but no DoublePulsar or shellcode like WannaCry (based on zzz_exploit.py by sleepya)
@WanaDecryptor@.exe, b.wnry, c.wnry, r.wnry, s.wnry, t.wnry, u.wnry, taskdl.exe, taskse.exe, taskhsvc.exe	perfc.dat	infpub.dat, cscc.dat
N/A	Yes (expired Microsoft signature)	Yes (expired Microsoft signature, invalid Symantec signature)
Port 139, 445, 3389	Port 139, 445 and disk enumeration for MFT/MBR	Only port enumeration on 139, 445 ports for write access. No disk enumeration prior writing on MFT, UPnP
Mimikatz (custom)	Mimikatz (custom)	Mimikatz (custom), Hardcoded credential list
EternalBlue, SMBv1 exploit, DoublePulsar	EternalRomance, EternalBlue, SMBv1(patched) exploit, SMB/NetBIOS (scanning), PsExec and WMIC (if SMB fails)	zzz_exploit, SMB/NetBIOS (scanning), SVCCTL (aka SCMR), WMIC (if SVCCTL fails)
No	Yes (scheduled task; NtRaiseHardError)	Yes (scheduled task)
Yes, if connection fails, over SMB (mssecsvc2.0 ServiceHandler Function)	No	Yes (Windows Client Side Caching DDriver)
Yes	Yes	Yes
No	Yes (via wevutil and fsutil)	Yes (via wevutil and fsutil)
AES-128 CBC mode, RSA-2048	AES-128 CBC mode, RSA-2048	AES-128 CBC mode, RSA-2048
Yes	Yes	Yes
N/A	Modified Petya bootloader	Custom bootloader and DiskCryptor (legitimate tool)
No	Yes (installed at the beginning of MBR)	Yes (installed at the end of MBR)
No	Yes (Salsa20)	Yes (AES-256-XTS)
Yes	Yes	Yes

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

Opti Data
Enforce your security

Зауважте:

MS17-010 в травні була 0day ?

Mimikatz це щось нове (у 2017му) ?

Opti Data
Enforce your security

Зауважте:

MS17-010 – був опублікований …

Mimikatz – був опублікований у 20..

Opti Data
Enforce your security

Зауважте:

MS17-010 – був опублікований 14 / 03 / 17

Mimikatz – був опублікований у 2011

Opti Data
Enforce your security

Що нам це дає?

- Не достатньо просто знати про вразливість
- Не достатньо розуміти як саме працює вразливість
- Не достатньо поставити виправлення і заспокоїтись

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

Що змінилося для нас?

Opti Data
Enforce your security

Україна. Кібератаки 2017го року

Сприйняття атак стало іншим

(але не у той бік…)

Opti Data
Enforce your security

Україна. Кібератаки **до 2015го**

Мені нічого втрачати

Opti Data
Enforce your security

Україна. Кібератаки **2017го року**

~~Мені нічого втрачати~~

Я не боюсь – у мене є бекапи

(Petya.A із-за лаштунків “Ню-ню..”)

Opti Data
Enforce your security

Україна. Кібератаки **2020го року**

~~Мені нічого втрачати~~

~~Я не боюсь – у мене є бекапи~~

Ніколи знову !

Opti Data
Enforce your security

Історія #1 “**Макрос**”

Opti Data
Enforce your security

Історія #1 “**Макрос**”

- Хтось відкриває документ 2013го року
- Спрацьовує макрос – пандемія (файли .doc)
- Паніка, розслідування, ~~розстріли~~
- За 5 годин усі документи на **x**00 системах інжектовано
- А якби це був #Pony або Ransom ?
- …

Opti Data
Enforce your security

Історія #2 “**Впертий ransomware**”

Opti Data
Enforce your security

Історія #2 “**Впертий ransomware**”

- Жертва отримує фішинг із приманкою
- Запускається ransomware
- “**Аааааа, ваш антивірус пропустив…**”
- Надаю людині маркери + контрзаходи

- Рекурсія, рекурсія, (сумно, боляче)
- Зашифровано систему керівника
- “То шо ви там казали, який параметр поставити?”

Opti Data
Enforce your security

Історія #3 “**Страх або як роблять новини про ІБ**”

Opti Data
Enforce your security

Історія #3 “**Страх або як роблять новини про ІБ**”

- Хтось “качає” фейковий AdobeFlash
- Зараження, виведення АРМ з ладу
- Чутки поширюються зі швидкістю світла
- В одному міністерстві вирішують вимкнути сервери
- Журналіст намагається зайти на сайт міністрества
- 503 = “Аааааа! Хакери поламали міністерство”

Opti Data
Enforce your security

Висновки #1

- Інструкції на випадок атаки
- Автономне прийняття рішень та контрзаходів
- Службові розслідування, форензика
- Мінімізація втрат
- Навчання персоналу

Opti Data
Enforce your security

Висновки #2

- Оновлення/виправлення MS Office та Windows ! ! !
- Блок створення та запуску C:\Users***.exe
- Контроль/блок WSH, PowerShell, HTA, CMD etc.
- Посилена фільтрація Web та Email
- Відмова від RTF, макросів, JRE, Flash

Opti Data
Enforce your security

Запитання ?

Дякую вам за увагу!

Владислав Радецький
vr@optidata.com.ua