[4 - Windows Forensics] GFOSS - Panoptis

Σύστημα WIN-H1MKJG48TV9 (Winserver) 10.10.10.100/24 DG 10.10.10.1 windows 2016 server
Στις 21/5/2019 09:45 έγινε join στο Domain panlab.local

Στο σύστημα έγινε ύποπτο log in στις 22/5/2019 3:02:40 μμ

Ακολούθησαν αποτυχημένες προσπάθειες σύνδεσης από αγνώστους υπολογιστές
Error 22/5/2019 3:38:36 μμ NETLOGON The session setup from computer 'DESKTOP-DQPLH9R' failed because the security database does not contain a trust account 'DESKTOP-DQPLH9R$' referenced by the specified computer.
Error 22/5/2019 3:41:43 μμ NETLOGON The session setup from computer 'DESKTOP-T10HVG9' failed because the security database does not contain a trust account 'DESKTOP-T10HVG9$' referenced by the specified computer.
Error 22/5/2019 3:41:43 μμ NETLOGON The session setup from the computer DESKTOP-DQPLH9R failed to authenticate. The following error occurred: Access is denied.
Error 22/5/2019 3:45:45 μμ NETLOGON The session setup from the computer DESKTOP-T10HVG9 failed to authenticate. The following error occurred: Access is denied.

Εγκαταστάθηκε το NXlog
Information 22/5/2019 3:47:31 μμ Service Control Manager A service was installed in the system. Service Name: nxlog Service File Name: "C:\Program Files (x86)\nxlog\nxlog.exe" -c "C:\Program Files (x86)\nxlog\conf\nxlog.conf"
Error 22/5/2019 3:47:58 μμ NETLOGON The session setup from computer 'DESKTOP-MNUQPDC' failed because the security database does not contain a trust account 'DESKTOP-MNUQPDC$' referenced by the specified computer.
Και έγιναν πολλές αλλαγές από τον χρήστη με αναγνωριστικό S-1-5-21-2600119791-1922435340-3741790263-500 (Administrator) Modifying Application: C:\Windows\System32\dllhost.exe το αρχείο φαίνεται να είναι κανονικό. 22/5/2019 4:14:12 μμ.

Εκτέλεση ύποπτου script 22/5/2019 4:15:32 μμ. Execute a Remote Command Powershell Path:
C:\Windows\TEMP\SDIAG_78575e65-cc55-4f86-b7d2-f46258717b98\UtilityFunctions.ps1

Έγινε εκτέλεση διαγνωστικών στην κάρτα δικτύου 22/5/2019 4:16:06 μμ Details about network adapter diagnosis:

Στις 22/5/2019 4:27:33 μμ. Ζητήθηκε πρόσβαση στο drobox Name resolution for the name bolt.dropbox.com

Στις 22/5/2019 4:30:53 μμ A service was installed in the system. Service Name: Mozilla Maintenance Service. Service File Name: "C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"

Στις 22/5/2019 4:31 μμ. Πρόσβαση στο https://www.mozilla.org/en-US/privacy/firefox/
Στις 22/5/2019 4:31:01 μμ. Φαίνεται πιθανό zip bomb

Στις 22/5/2019 4:32 μμ. Φαίνεται ότι έγινε login στο drobox και κατέβηκαν αρχεία εγκατάστασης – παραμετροποίησης του NXlog

Στις 22/5/2019 4:35 μμ. Φαίνεται ότι κατέβηκε το notepad++ και έγινε εγκατάσταση

Στις 22/5/2019 5:03:11 μμ The process C:\Windows\System32\RuntimeBroker.exe (WIN-H1MKJG48TV9) has initiated the restart of computer WIN-H1MKJG48TV9 on behalf of user PANLAB\Administrator for the following reason: Other (Unplanned)

Το σύστημα έχει πρόσβαση map drive στο \\10.10.10.102\sambashare

Αναβάθμιση Defender στις 6/6/2019 7:20:51 μμ Windows Defender   2010   None
Windows Defender used Dynamic Signature Service to retrieve additional signatures to help protect your machine.
Current Signature Version: 1.295.160.0

Ανακάλυψη ύποπτου αρχείου   6/6/2019 7:33:40 μμ Windows Defender   2050   None
Windows Defender has uploaded a suspicious file for further analysis.
Filename: C:\Windows\Temp\winlive.exe Sha256:

Warning   6/6/2019 7:33:45 μμ   Windows Defender   1116   None
Windows Defender has detected malware or other potentially unwanted software.
For more information please see the following:
http://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Bearfoos.A!ml&threatid=2147731250&enterprise=0

Name: Trojan:Win32/Bearfoos.A!ml
ID: 2147731250
Severity: Severe
Category: Trojan
Path: file:_C:\Windows\Temp\winlive.exe
Detection Origin: Local machine
Detection Type: FastPath
Detection Source: System
User: NT AUTHORITY\SYSTEM
Process Name: Unknown

```
Signature Version: AV: 1.295.160.0, AS: 1.295.160.0, NIS: 119.0.0.0
Engine Version: AM: 1.1.16000.6, NIS: 2.1.14600.4
```

Remote powershel

```
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
Warning    6/6/2019 19:35:58    PowerShell (Microsoft-Windows-PowerShell)    4104
Execute a Remote Command
```

```
Warning    6/6/2019 8:06:04 μμ  Windows Defender    1116    None
Windows Defender has detected malware or other potentially unwanted software.
For more information please see the following:
http://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Bearfoos.A!ml&threatid
=2147731250&enterprise=0
        Name: Trojan:Win32/Bearfoos.A!ml
        ID: 2147731250
        Severity: Severe
        Category: Trojan
   Path: file:_\\10.10.10.11\c$\users\jd\appdata\roaming\Microsoft\windows\start
menu\programs\startup\winlive.exe
        Detection Origin: Network share
        Detection Type: FastPath
        Detection Source: Real-Time Protection
        User: PANLAB\Administrator
        Process Name: C:\Windows\SysWOW64\cmd.exe
        Signature Version: AV: 1.295.160.0, AS: 1.295.160.0, NIS: 119.0.0.0
        Engine Version: AM: 1.1.16000.6, NIS: 2.1.14600.4
```

Επιβεβαιώνει πως το 10.10.10.11 χρήστης jd έχει μολυνθεί.
Είναι πολύ πιθανό το 10.10.10.102 να έχει επίσης μολυσμένα αρχεία.

Το σύστημα είναι ακόμα μολυσμένο