Malware sample: invitation.exe

MFT section:

```
1/23/2020    10:11:19 PM    0    C    MFT    FILE    File Create                SI
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:20 PM    0    M    MFT    FILE    File Modified              SI
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:20 PM    0    B    MFT    FILE    MFT Entry                  SI
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    A    MFT    FILE    File Last Access           SI
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    C    MFT    FILE    File Create                FN1
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    M    MFT    FILE    File Modified              FN1
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    B    MFT    FILE    MFT Entry                  FN1
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    A    MFT    FILE    File Last Access           FN1
        :\Windows\System32\invitation.exe          INVITA~1.EXE    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    C    MFT    FILE    File Create                FN2
        :\Windows\System32\invitation.exe          invitation.exe    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    M    MFT    FILE    File Modified              FN2
        :\Windows\System32\invitation.exe          invitation.exe    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    B    MFT    FILE    MFT Entry                  FN2
        :\Windows\System32\invitation.exe          invitation.exe    41689    ALLOCATED

1/23/2020    10:11:19 PM    0    A    MFT    FILE    File Last Access           FN2
        :\Windows\System32\invitation.exe          invitation.exe    41689    ALLOCATED


1/23/2020    9:48:45 PM     0    C    MFT    FILE    File Create                SI
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966    ALLOCATED

1/23/2020    9:48:45 PM     0    M    MFT    FILE    File Modified              SI
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966    ALLOCATED
```

```
1/23/2020      9:48:45 PM     0        B        MFT      FILE     MFT Entry                        SI
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        A        MFT      FILE     File Last Access                 SI
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        C        MFT      FILE     File Create                      FN1
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        M        MFT      FILE     File Modified                    FN1
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        B        MFT      FILE     MFT Entry                        FN1
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        A        MFT      FILE     File Last Access                 FN1
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        INVITA~1.LNK    17966   ALLOCATED

1/23/2020      9:48:45 PM     0        C        MFT      FILE     File Create                      FN2
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        invitation.pdf.ace.lnk     17966   ALLOCATED

1/23/2020      9:48:45 PM     0        M        MFT      FILE     File Modified                    FN2
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        invitation.pdf.ace.lnk     17966   ALLOCATED

1/23/2020      9:48:45 PM     0        B        MFT      FILE     MFT Entry                        FN2
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        invitation.pdf.ace.lnk     17966   ALLOCATED

1/23/2020      9:48:45 PM     0        A        MFT      FILE     File Last Access                 FN2
        :\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\invitation.pdf.ace.lnk
        invitation.pdf.ace.lnk     17966   ALLOCATED

1/23/2020      9:48:44 PM     0        C        MFT      FILE     File Create                      SI
        :\Users\IEUser\Downloads\invitation.pdf.ace               INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM     0        M        MFT      FILE     File Modified                    SI
        :\Users\IEUser\Downloads\invitation.pdf.ace               INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM     0        B        MFT      FILE     MFT Entry                        SI
        :\Users\IEUser\Downloads\invitation.pdf.ace               INVITA~1.ACE    28628   ALLOCATED
```

```
1/23/2020      9:48:45 PM      0          A          MFT        FILE       File Last Access                      SI
               :\Users\IEUser\Downloads\invitation.pdf.ace                 INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM      0          C          MFT        FILE       File Create                           FN1
               :\Users\IEUser\Downloads\invitation.pdf.ace                 INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM      0          M          MFT        FILE       File Modified                         FN1
               :\Users\IEUser\Downloads\invitation.pdf.ace                 INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM      0          B          MFT        FILE       MFT Entry                             FN1
               :\Users\IEUser\Downloads\invitation.pdf.ace                 INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM      0          A          MFT        FILE       File Last Access                      FN1
               :\Users\IEUser\Downloads\invitation.pdf.ace                 INVITA~1.ACE    28628   ALLOCATED

1/23/2020      9:48:45 PM      0          C          MFT        FILE       File Create                           FN2
               :\Users\IEUser\Downloads\invitation.pdf.ace                 invitation.pdf.ace      28628
               ALLOCATED

1/23/2020      9:48:45 PM      0          M          MFT        FILE       File Modified                         FN2
               :\Users\IEUser\Downloads\invitation.pdf.ace                 invitation.pdf.ace      28628
               ALLOCATED

1/23/2020      9:48:45 PM      0          B          MFT        FILE       MFT Entry                             FN2
               :\Users\IEUser\Downloads\invitation.pdf.ace                 invitation.pdf.ace      28628
               ALLOCATED

1/23/2020      9:48:45 PM      0          A          MFT        FILE       File Last Access                      FN2
               :\Users\IEUser\Downloads\invitation.pdf.ace                 invitation.pdf.ace      28628
               ALLOCATED

1/23/2020      9:49:50 PM      0          C          MFT        FILE       File Create                           SI
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          B          MFT        FILE       MFT Entry                             SI
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          A          MFT        FILE       File Last Access                      SI
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          C          MFT        FILE       File Create                           FN1
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          M          MFT        FILE       File Modified                         FN1
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          B          MFT        FILE       MFT Entry                             FN1
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED

1/23/2020      9:49:50 PM      0          A          MFT        FILE       File Last Access                      FN1
               :\Program Files\WinRAR\UNACEV2.DLL              UNACEV2.DLL    31918   ALLOCATED
```

- This represents the activity of the filesystem of the Win 7 VM, so every event of our exploit related files being added to the system.
- 1/23/2020 10:11:19 PM is the timestamp for the creation of the exe of our exploit. Whereas 1/23/2020 9:48:45 PM is the timestamp for the creation of the ace file of our exploit. Therefore, we see that the activity of the stages of our exploit are captured in the MFT.

Netstat Section:

```
Active Connections


 Proto  Local Address          Foreign Address        State

 TCP    0.0.0.0:135            0.0.0.0:0              LISTENING

 RpcSs

[svchost.exe]

 TCP    0.0.0.0:445            0.0.0.0:0              LISTENING

Can not obtain ownership information

 TCP    0.0.0.0:554            0.0.0.0:0              LISTENING

[wmpnetwk.exe]

 TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING

Can not obtain ownership information

 TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING

Can not obtain ownership information

 TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING

[pythonw.exe]

 TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING

Can not obtain ownership information

 TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING

[wininit.exe]

 TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING

 eventlog
```

```
[svchost.exe]
 TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
 Schedule
[svchost.exe]
 TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
[lsass.exe]
 TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
[services.exe]
 TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
 PolicyAgent
[svchost.exe]
 TCP    192.168.56.103:139     0.0.0.0:0              LISTENING
Can not obtain ownership information
 TCP    192.168.56.103:2869    192.168.56.1:63298     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63302     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63303     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63310     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63314     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63316     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63318     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63326     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63328     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63335     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63339     TIME_WAIT
 TCP    192.168.56.103:2869    192.168.56.1:63347     TIME_WAIT
 TCP    192.168.56.103:49158   192.168.56.102:443     ESTABLISHED
[invitation.exe]
 TCP    192.168.56.103:49161   192.168.56.102:443     ESTABLISHED
[cmd.exe]
```

```
 TCP    [::]:135               [::]:0                 LISTENING
 RpcSs
[svchost.exe]
 TCP    [::]:445               [::]:0                 LISTENING
Can not obtain ownership information
 TCP    [::]:554               [::]:0                 LISTENING
[wmpnetwk.exe]
 TCP    [::]:2869              [::]:0                 LISTENING
Can not obtain ownership information
 TCP    [::]:5357              [::]:0                 LISTENING
Can not obtain ownership information
 TCP    [::]:10243             [::]:0                 LISTENING
Can not obtain ownership information
 TCP    [::]:49152             [::]:0                 LISTENING
[wininit.exe]
 TCP    [::]:49153             [::]:0                 LISTENING
 eventlog
[svchost.exe]
 TCP    [::]:49154             [::]:0                 LISTENING
 Schedule
[svchost.exe]
 TCP    [::]:49155             [::]:0                 LISTENING
[lsass.exe]
 TCP    [::]:49156             [::]:0                 LISTENING
[services.exe]
 TCP    [::]:49157             [::]:0                 LISTENING
 PolicyAgent
[svchost.exe]
 UDP    0.0.0.0:500            *:*
 IKEEXT
[svchost.exe]
 UDP    0.0.0.0:3702           *:*
 FDResPub
[svchost.exe]
 UDP    0.0.0.0:3702           *:*
 FDResPub
[svchost.exe]
 UDP    0.0.0.0:4500           *:*
 IKEEXT
[svchost.exe]
 UDP    0.0.0.0:5004           *:*
[wmpnetwk.exe]
 UDP    0.0.0.0:5005           *:*
[wmpnetwk.exe]
 UDP    0.0.0.0:5355           *:*
 Dnscache
[svchost.exe]
 UDP    0.0.0.0:55228          *:*
 FDResPub
[svchost.exe]
 UDP    127.0.0.1:1900         *:*
 SSDPSRV
[svchost.exe]
 UDP    127.0.0.1:58748        *:*
 SSDPSRV
[svchost.exe]
 UDP    192.168.56.103:137     *:*
Can not obtain ownership information
```

```
 UDP    192.168.56.103:138     *:*
Can not obtain ownership information
 UDP    192.168.56.103:1900    *:*
 SSDPSRV
[svchost.exe]
 UDP    192.168.56.103:58747   *:*
 SSDPSRV
[svchost.exe]
 UDP    [::]:500               *:*
 IKEEXT
[svchost.exe]
 UDP    [::]:3702              *:*
 FDResPub
[svchost.exe]
 UDP    [::]:3702              *:*
 FDResPub
[svchost.exe]
 UDP    [::]:4500              *:*
 IKEEXT
[svchost.exe]
 UDP    [::]:5004              *:*
[wmpnetwk.exe]
 UDP    [::]:5005              *:*
[wmpnetwk.exe]
 UDP    [::]:5355              *:*
 Dnscache
[svchost.exe]
 UDP    [::]:55229             *:*
 FDResPub
[svchost.exe]
 UDP    [::1]:1900             *:*
 SSDPSRV
[svchost.exe]
 UDP    [::1]:58746            *:*
 SSDPSRV
[svchost.exe]
 UDP    [fe80::b18b:a288:3a8f:396c%15]:1900  *:*
 SSDPSRV
[svchost.exe]
 UDP    [fe80::b18b:a288:3a8f:396c%15]:58745  *:*
 SSDPSRV
[svchost.exe]
```

- This netstat output shows the established connection of the backdoor to the pupy shell.
- The connection can be seen in two entries in the netstat dump:

  ```
  TCP    192.168.56.103:49158   192.168.56.102:443     ESTABLISHED
  ```

```
 [invitation.exe]
```

The above entry is the establishment of the first session to the pupy shell on startup.

```
  TCP    192.168.56.103:49161   192.168.56.102:443     ESTABLISHED
 [cmd.exe]
```

The above entry is the execution of the getsystem privilege escalation in the pupy shell to get a privileged session in the win 7 VM.

Autoruns section:

```
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet"	""	""	""	"1/30/2020 5:51 PM"	""
+ "rundll32"	"Windows host process (Rundll32)"	"(Verified) Microsoft Windows"	"c:\windows\system32\rundll32.exe"	"7/13/2009 3:41 PM"	""
```

```
"HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon"        ""        ""
        ""        "10/14/2012 9:44 PM"   ""

+ "Local Group Policy"    ""        ""        "c:\wallpaper\autologon.bat"    "10/14/2012 9:27 PM"   ""

"HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell"    ""        ""        ""
        "7/13/2009 8:37 PM"    ""

+ "cmd.exe"      "Windows Command Processor"        "(Verified) Microsoft Windows"  "c:\windows\
system32\cmd.exe"      "11/20/2010 1:00 AM"  ""

"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"    ""        ""        ""        "12/27/2019
6:26 PM"        ""

+ "VBoxTray"     "VirtualBox Guest Additions Tray Application"    "(Verified) Oracle Corporation"  "c:\
windows\system32\vboxtray.exe"        "12/10/2019 7:04 AM"  ""

"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"    ""        ""        ""
        "12/27/2019 4:33 PM"   ""

+ "agent.pyw"    ""        ""        "c:\programdata\microsoft\windows\start menu\programs\startup\
agent.pyw"      "12/27/2019 4:33 PM"   ""

"HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components"        ""        ""        ""
        "10/13/2012 12:09 PM" ""

+ "Browser Customizations"      "IEAK branding" "(Verified) Microsoft Corporation"        "c:\windows\
system32\iedkcs32.dll"  "3/8/2011 4:47 AM"      ""

+ "n/a"  "Microsoft .NET IE SECURITY REGISTRATION"      "(Verified) Microsoft Corporation"        "c:\
windows\system32\mscories.dll"        "9/28/2010 7:53 PM"    ""

+ "Themes Setup"        "Microsoft(C) Register Server"    "(Verified) Microsoft Windows"  "c:\windows\
system32\regsvr32.exe"        "7/13/2009 3:58 PM"    ""

+ "Windows Desktop Update"    "Microsoft(C) Register Server"    "(Verified) Microsoft Windows"  "c:\
windows\system32\regsvr32.exe"        "7/13/2009 3:58 PM"    ""

"HKLM\SOFTWARE\Classes\Protocols\Filter"      ""        ""        ""        "10/13/2012 12:07 PM" ""

+ "application/octet-stream"      "Microsoft .NET Runtime Execution Engine"       "(Verified) Microsoft
Corporation"     "c:\windows\system32\mscoree.dll"     "3/4/2010 7:06 PM"      ""

+ "application/x-complus"        "Microsoft .NET Runtime Execution Engine"       "(Verified) Microsoft
Corporation"     "c:\windows\system32\mscoree.dll"     "3/4/2010 7:06 PM"      ""

+ "application/x-msdownload"   "Microsoft .NET Runtime Execution Engine"       "(Verified) Microsoft
Corporation"     "c:\windows\system32\mscoree.dll"     "3/4/2010 7:06 PM"      ""

"HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers"       ""        ""        ""        "1/23/2020
1:49 PM"        ""
```

```
+ "WinRAR"      "WinRAR shell extension"       "(Not verified) Alexander Roshal"        "c:\program
files\winrar\rarext.dll"   "9/30/2018 10:01 AM"   ""

"HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers"          ""        ""        ""
        "1/23/2020 1:49 PM"    ""

+ "WinRAR"      "WinRAR shell extension"       "(Not Verified) Alexander Roshal"        "c:\program
files\winrar\rarext.dll"   "9/30/2018 10:01 AM"   ""

"HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers"     ""        ""        ""        "1/23/2020
1:49 PM"        ""

+ "WinRAR"      "WinRAR shell extension"       "(Not Verified) Alexander Roshal"        "c:\program
files\winrar\rarext.dll"   "9/30/2018 10:01 AM"   ""

"Task Scheduler"        ""        ""        ""        ""        ""

+ "\elevator"     ""        ""        "c:/windows/system32/invitation.exe"   "3/30/2019 3:56 AM"    ""

+ "\ievms"        ""        ""        "c:\ievms.bat"   "12/27/2019 11:25 AM"""

"HKLM\System\CurrentControlSet\Services"     ""        ""        ""        "1/30/2020 5:38 PM"    ""

+ "clr_optimization_v2.0.50727_32"      "Microsoft .NET Framework NGEN v2.0.50727_X86:
Microsoft .NET Framework NGEN"        "(Verified) Microsoft Corporation"        "c:\windows\
microsoft.net\framework\v2.0.50727\mscorsvw.exe"     "6/3/2009 9:25 PM"      ""

+ "FontCache3.0.0.0"     "Windows Presentation Foundation Font Cache 3.0.0.0: Optimizes performance
of Windows Presentation Foundation (WPF) applications by caching commonly used font data. WPF
applications will start this service if it is not already running. It can be disabled, though doing so will
degrade the performance of WPF applications." "(Verified) Microsoft Corporation"        "c:\windows\
microsoft.net\framework\v3.0\wpf\presentationfontcache.exe" "5/22/2009 5:22 PM"    ""

+ "idsvc"          "Windows CardSpace: Securely enables the creation, management, and disclosure of
digital identities."        "(Verified) Microsoft Corporation"        "c:\windows\microsoft.net\framework\
v3.0\windows communication foundation\infocard.exe" "9/28/2010 10:44 PM"   ""

+ "VBoxService" "VirtualBox Guest Additions Service: Manages VM runtime information, time
synchronization, remote sysprep execution and miscellaneous utilities for guest operating systems."
        "(Verified) Oracle Corporation"  "c:\windows\system32\vboxservice.exe"        "12/10/2019
7:04 AM"        ""

"HKLM\System\CurrentControlSet\Services"     ""        ""        ""        "1/30/2020 5:38 PM"    ""

+ "Synth3dVsc"  "Synth3dVsc: "  ""        "File not found: System32\drivers\synth3dvsc.sys"        ""
        ""

+ "tsusbhub"     "tsusbhub: "     ""        "File not found: system32\drivers\tsusbhub.sys"          ""
        ""
```

```
+ "VBoxGuest"   "VirtualBox Guest Driver: VirtualBox Guest Driver"        "(Verified) Oracle Corporation"
        "c:\windows\system32\drivers\vboxguest.sys"   "12/10/2019 7:04 AM"   ""

+ "VBoxMouse" "VirtualBox Guest Mouse Service: VirtualBox Mouse Filter"        "(Verified) Oracle
Corporation"    "c:\windows\system32\drivers\vboxmouse.sys" "12/10/2019 7:04 AM"   ""

+ "VBoxSF"      "VirtualBox Shared Folders: VirtualBox Shared Folders Minirdr"   "(Verified) Oracle
Corporation"    "c:\windows\system32\drivers\vboxsf.sys"        "12/10/2019 7:04 AM"   ""

+ "VBoxVideo"   "VBoxVideo: VirtualBox Video Driver"    "(Verified) Oracle Corporation"   "c:\windows\
system32\drivers\vboxvideo.sys"          "12/10/2019 7:04 AM"   ""

+ "VGPU"        "VGPU: "         ""        "File not found: System32\drivers\rdvgkmd.sys" ""        ""

"HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)"    ""        ""        ""
        "10/11/2012 10:11 PM" ""

+ "C:\Program Files\Internet Explorer\iexplore.exe"      "Internet Explorer"      "(Verified) Microsoft
Corporation"    "c:\program files\internet explorer\iexplore.exe"          "8/23/2012 10:49 PM"   ""

"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions"     ""        ""
        ""        "10/14/2012 9:15 PM"   ""

+ "{4CFB60C1-FAA6-47f1-89AA-0B18730C9FD3}"          "IEAK branding" "(Verified) Microsoft
Corporation"    "c:\windows\system32\iedkcs32.dll"     "3/8/2011 4:47 AM"      ""

+ "{7B849a69-220F-451E-B3FE-2CB811AF94AE}"          "IEAK branding" "(Verified) Microsoft
Corporation"    "c:\windows\system32\iedkcs32.dll"     "3/8/2011 4:47 AM"      ""

+ "{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}"          "IEAK branding" "(Verified) Microsoft
Corporation"    "c:\windows\system32\iedkcs32.dll"     "3/8/2011 4:47 AM"      ""

+ "{CF7639F3-ABA2-41DB-97F2-81E2C5DBFC5D}"          "IEAK branding" "(Verified) Microsoft
Corporation"    "c:\windows\system32\iedkcs32.dll"     "3/8/2011 4:47 AM"      ""

"HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order"     ""        ""        ""
        "12/27/2019 6:27 PM"   ""

+ "VBoxSF"      "VirtualBox Shared Folders"      "(Verified) Oracle Corporation"  "c:\windows\system32\
vboxmrxnp.dll"  "12/10/2019 7:04 AM"   ""
```

2. Autoruns shows the auto-loading programs on boot, and this showcases that our backdoor has persistence since it boots on start.

3. As can be seen in the above output, our backdoor has persistence among any number attempts of restarts.

Wimpmem && Volatility section:

****

invitation.exe pid: 1968

Command line : C:/Windows/System32/invitation.exe

```
Process: invitation.exe Pid: 1968 Address: 0x1d0000

Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE

Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6


0x001d0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x001d0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 1d 00   ................

0x001d0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x001d0030  00 00 00 00 00 00 00 00 1c 00 1d 00 00 00 00 00   ................


0x001d0000 0000           ADD [EAX], AL

0x001d0002 0000           ADD [EAX], AL

0x001d0004 0000           ADD [EAX], AL

0x001d0006 0000           ADD [EAX], AL

0x001d0008 0000           ADD [EAX], AL

0x001d000a 0000           ADD [EAX], AL

0x001d000c 0000           ADD [EAX], AL

0x001d000e 0000           ADD [EAX], AL

0x001d0010 0000           ADD [EAX], AL

0x001d0012 0000           ADD [EAX], AL

0x001d0014 0000           ADD [EAX], AL

0x001d0016 0000           ADD [EAX], AL

0x001d0018 0000           ADD [EAX], AL

0x001d001a 0000           ADD [EAX], AL

0x001d001c 0000           ADD [EAX], AL

0x001d001e 1d00000000       SBB EAX, 0x0

0x001d0023 0000           ADD [EAX], AL

0x001d0025 0000           ADD [EAX], AL
```

```
0x001d0027 0000           ADD [EAX], AL

0x001d0029 0000           ADD [EAX], AL

0x001d002b 0000           ADD [EAX], AL

0x001d002d 0000           ADD [EAX], AL

0x001d002f 0000           ADD [EAX], AL

0x001d0031 0000           ADD [EAX], AL

0x001d0033 0000           ADD [EAX], AL

0x001d0035 0000           ADD [EAX], AL

0x001d0037 001c00         ADD [EAX+EAX], BL

0x001d003a 1d00000000     SBB EAX, 0x0

0x001d003f 00             DB 0x0
```

```
0x85331030 invitation.exe        1968   1792     5     140     0     0 2020-01-31 01:51:31 UTC+0000

Process: 1968 invitation.exe 2020-01-31 01:51:31 UTC+0000

2020-01-23 21:48:36 UTC+0000|[IEHISTORY]| explorer.exe->Visited:
IEUser@http://192.168.56.102/invitation.pdf.ace| PID: 1624/Cache type "URL " at 0x1f87880 End:
2020-01-23 21:48:36 UTC+0000

2020-01-23 21:48:45 UTC+0000|[IEHISTORY]| explorer.exe->Visited:
IEUser@file:///C:/Users/IEUser/Downloads/invitation.pdf.ace| PID: 1624/Cache type "URL " at
0x1f87980 End: 2020-01-23 21:48:45 UTC+0000

2020-01-31 01:51:31 UTC+0000|[PROCESS]| invitation.exe| PID: 1968/PPID: 1792/POffset: 0x3e931030

2009-07-14 04:37:09 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\NLS\SORTING\
VERSIONS| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030

2019-12-28 03:28:39 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\SESSION
MANAGER| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030

2020-01-31 04:51:14 UTC+0000|[Handle (Key)]| MACHINE| invitation.exe PID: 1968/PPID:
1792/POffset: 0x3e931030

2009-07-14 04:42:25 UTC+0000|[Handle (Key)]| USER| invitation.exe PID: 1968/PPID: 1792/POffset:
0x3e931030

2009-07-14 04:37:06 UTC+0000|[Handle (Key)]| USER\CONTROL PANEL\INTERNATIONAL| invitation.exe
PID: 1968/PPID: 1792/POffset: 0x3e931030
```

```
2020-01-16 21:16:34 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\SERVICES\WINSOCK2\
PARAMETERS\PROTOCOL_CATALOG9| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030

2012-10-15 03:53:48 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\SERVICES\WINSOCK2\
PARAMETERS\NAMESPACE_CATALOG5| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030

2019-12-28 02:27:15 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\
NETWORKPROVIDER\HWORDER| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030

2019-03-30 11:56:09 UTC+0000|[PE HEADER (exe)]| invitation.exe| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x00400000

-|[PE DEBUG]| invitation.exe| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x00400000

1970-01-01 00:00:00 UTC+0000|[DLL LOADTIME (exe)]| invitation.exe| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x00400000

2010-11-20 12:05:02 UTC+0000|[PE HEADER (dll)]| | Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x77090000

-|[PE DEBUG]| | Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base:
0x77090000

1970-01-01 00:00:00 UTC+0000|[DLL LOADTIME (dll)]| | Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x77090000

2010-11-20 12:08:07 UTC+0000|[PE HEADER (dll)]| webio.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x71740000

-|[PE DEBUG]| webio.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x71740000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| webio.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71740000

2009-07-14 01:10:28 UTC+0000|[PE HEADER (dll)]| sechost.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x77230000

-|[PE DEBUG]| sechost.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x77230000

2020-01-31 01:51:38 UTC+0000|[DLL LOADTIME (dll)]| sechost.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77230000

2009-07-13 23:12:01 UTC+0000|[PE HEADER (dll)]| CRYPTBASE.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75170000

-|[PE DEBUG]| CRYPTBASE.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x75170000
```

```
2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| CRYPTBASE.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75170000

2010-11-20 12:05:54 UTC+0000|[PE HEADER (dll)]| RPCRT4.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x76b80000

-|[PE DEBUG]| RPCRT4.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x76b80000

2020-01-31 01:51:38 UTC+0000|[DLL LOADTIME (dll)]| RPCRT4.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76b80000

2010-11-20 12:05:06 UTC+0000|[PE HEADER (dll)]| OLEAUT32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76d90000

-|[PE DEBUG]| OLEAUT32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x76d90000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| OLEAUT32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76d90000

2010-11-20 12:02:48 UTC+0000|[PE HEADER (dll)]| MSWSOCK.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74c60000

-|[PE DEBUG]| MSWSOCK.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x74c60000

2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| MSWSOCK.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74c60000

2010-11-20 12:09:12 UTC+0000|[PE HEADER (dll)]| WS2_32.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x771d0000

-|[PE DEBUG]| WS2_32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x771d0000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| WS2_32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x771d0000

2010-11-20 12:00:25 UTC+0000|[PE HEADER (dll)]| IPHLPAPI.DLL| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x747e0000

-|[PE DEBUG]| IPHLPAPI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x747e0000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| IPHLPAPI.DLL| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x747e0000

2009-07-14 01:07:53 UTC+0000|[PE HEADER (dll)]| MSCTF.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x756c0000
```

```
-|[PE DEBUG]| MSCTF.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x756c0000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| MSCTF.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x756c0000

2010-11-20 12:00:01 UTC+0000|[PE HEADER (dll)]| CRYPT32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75400000

-|[PE DEBUG]| CRYPT32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75400000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| CRYPT32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75400000

2010-11-20 12:00:05 UTC+0000|[PE HEADER (dll)]| IMM32.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77210000

-|[PE DEBUG]| IMM32.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77210000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| IMM32.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77210000

2009-07-14 01:09:45 UTC+0000|[PE HEADER (dll)]| NSI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76840000

-|[PE DEBUG]| NSI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76840000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| NSI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76840000

2009-07-14 01:10:25 UTC+0000|[PE HEADER (dll)]| sfc.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x70a10000

-|[PE DEBUG]| sfc.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x70a10000

2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| sfc.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x70a10000

2010-11-20 11:59:06 UTC+0000|[PE HEADER (dll)]| GDI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77250000

-|[PE DEBUG]| GDI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77250000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| GDI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x77250000
```

```
2010-11-20 12:06:54 UTC+0000|[PE HEADER (dll)]| SHELL32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75860000

-|[PE DEBUG]| SHELL32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75860000

2020-01-31 01:51:38 UTC+0000|[DLL LOADTIME (dll)]| SHELL32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75860000

2010-11-20 12:02:17 UTC+0000|[PE HEADER (dll)]| MSASN1.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75290000

-|[PE DEBUG]| MSASN1.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75290000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| MSASN1.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75290000

2009-07-14 01:07:09 UTC+0000|[PE HEADER (dll)]| CRYPTSP.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74ca0000

-|[PE DEBUG]| CRYPTSP.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74ca0000

2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| CRYPTSP.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74ca0000

2010-11-20 12:09:08 UTC+0000|[PE HEADER (dll)]| WTSAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74500000

-|[PE DEBUG]| WTSAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74500000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| WTSAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74500000

2010-11-20 12:03:31 UTC+0000|[PE HEADER (dll)]| NETAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73310000

-|[PE DEBUG]| NETAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73310000

2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| NETAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73310000

2010-11-20 12:07:59 UTC+0000|[PE HEADER (dll)]| srvcli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74e40000

-|[PE DEBUG]| srvcli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74e40000
```

```
2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| srvcli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74e40000

2009-07-14 01:06:33 UTC+0000|[PE HEADER (dll)]| LPK.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76750000

-|[PE DEBUG]| LPK.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76750000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| LPK.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76750000

2010-11-20 12:06:58 UTC+0000|[PE HEADER (dll)]| SHLWAPI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76790000

-|[PE DEBUG]| SHLWAPI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76790000

2020-01-31 01:51:38 UTC+0000|[DLL LOADTIME (dll)]| SHLWAPI.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76790000

2010-11-20 12:08:30 UTC+0000|[PE HEADER (dll)]| winhttp.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71790000

-|[PE DEBUG]| winhttp.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71790000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| winhttp.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71790000

2010-11-20 12:02:56 UTC+0000|[PE HEADER (dll)]| KERNELBASE.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x753b0000

-|[PE DEBUG]| KERNELBASE.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x753b0000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| KERNELBASE.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x753b0000

2009-07-14 01:10:26 UTC+0000|[PE HEADER (dll)]| sfc_os.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x709c0000

-|[PE DEBUG]| sfc_os.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x709c0000

2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| sfc_os.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x709c0000

2009-07-14 01:11:31 UTC+0000|[PE HEADER (dll)]| WINNSI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x747d0000
```

```
-|[PE DEBUG]| WINNSI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x747d0000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| WINNSI.DLL| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x747d0000

2009-07-14 01:07:02 UTC+0000|[PE HEADER (dll)]| MPR.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x74810000

-|[PE DEBUG]| MPR.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL
Base: 0x74810000

2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| MPR.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x74810000

2010-11-20 12:08:06 UTC+0000|[PE HEADER (dll)]| USER32.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x75790000

-|[PE DEBUG]| USER32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x75790000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| USER32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x75790000

2010-11-20 11:54:46 UTC+0000|[PE HEADER (dll)]| ADVAPI32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76e20000

-|[PE DEBUG]| ADVAPI32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x76e20000

2020-01-31 01:51:38 UTC+0000|[DLL LOADTIME (dll)]| ADVAPI32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76e20000

2010-11-20 12:05:03 UTC+0000|[PE HEADER (dll)]| ole32.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x76c30000

-|[PE DEBUG]| ole32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x76c30000

2020-01-31 01:51:41 UTC+0000|[DLL LOADTIME (dll)]| ole32.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76c30000

2009-07-14 01:09:52 UTC+0000|[PE HEADER (dll)]| rsaenh.dll| Process: invitation.exe/PID: 1968/PPID:
1792/Process POffset: 0x3e931030/DLL Base: 0x74a40000

-|[PE DEBUG]| rsaenh.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset:
0x3e931030/DLL Base: 0x74a40000

2020-01-31 01:51:42 UTC+0000|[DLL LOADTIME (dll)]| rsaenh.dll| Process: invitation.exe/PID:
1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74a40000
```

```
2009-07-14 01:11:50 UTC+0000|[PE HEADER (dll)]| wship6.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74c50000

-|[PE DEBUG]| wship6.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74c50000

2020-01-31 01:52:02 UTC+0000|[DLL LOADTIME (dll)]| wship6.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x74c50000

2009-07-14 01:11:54 UTC+0000|[PE HEADER (dll)]| wshtcpip.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x745c0000

-|[PE DEBUG]| wshtcpip.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x745c0000

2020-01-31 01:52:02 UTC+0000|[DLL LOADTIME (dll)]| wshtcpip.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x745c0000

2010-11-20 12:08:09 UTC+0000|[PE HEADER (dll)]| USP10.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76a80000

-|[PE DEBUG]| USP10.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76a80000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| USP10.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76a80000

2009-07-14 01:09:34 UTC+0000|[PE HEADER (dll)]| PSAPI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x772a0000

-|[PE DEBUG]| PSAPI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x772a0000

2020-01-31 01:51:47 UTC+0000|[DLL LOADTIME (dll)]| PSAPI.DLL| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x772a0000

2010-11-20 12:02:55 UTC+0000|[PE HEADER (dll)]| kernel32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x764b0000

-|[PE DEBUG]| kernel32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x764b0000

2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| kernel32.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x764b0000

2009-07-14 01:07:59 UTC+0000|[PE HEADER (dll)]| msvcrt.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76ec0000

-|[PE DEBUG]| msvcrt.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76ec0000
```

```
2020-01-31 01:51:31 UTC+0000|[DLL LOADTIME (dll)]| msvcrt.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x76ec0000

2009-07-13 23:53:51 UTC+0000|[PE HEADER (dll)]| netbios.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x744d0000

-|[PE DEBUG]| netbios.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x744d0000

2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| netbios.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x744d0000

2010-11-20 09:32:23 UTC+0000|[PE HEADER (dll)]| wkscli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x732e0000

-|[PE DEBUG]| wkscli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x732e0000

2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| wkscli.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x732e0000

2009-07-13 23:53:57 UTC+0000|[PE HEADER (dll)]| wshqos.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71b50000

-|[PE DEBUG]| wshqos.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71b50000

2020-01-31 01:52:02 UTC+0000|[DLL LOADTIME (dll)]| wshqos.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x71b50000

2010-11-20 09:32:22 UTC+0000|[PE HEADER (dll)]| netutils.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73300000

-|[PE DEBUG]| netutils.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73300000

2020-01-31 01:51:49 UTC+0000|[DLL LOADTIME (dll)]| netutils.dll| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x73300000

2020-01-31 01:51:34 UTC+0000|[THREAD]| invitation.exe| PID: 1968/TID: 1412

2020-01-31 01:51:31 UTC+0000|[THREAD]| invitation.exe| PID: 1968/TID: 1972

2020-01-31 01:52:02 UTC+0000|[THREAD]| invitation.exe| PID: 1968/TID: 1616

2020-01-31 01:51:49 UTC+0000|[THREAD]| invitation.exe| PID: 1968/TID: 1604

2020-01-31 01:51:47 UTC+0000|[THREAD]| invitation.exe| PID: 1968/TID: 1600

2020-01-23 22:38:19 UTC+0000|[USER ASSIST]| %windir%\system32\invitation.exe| Registry: \??\C:\Users\IEUser\ntuser.dat /ID: N/A/Count: 3/FocusCount: 0/TimeFocused: 0:00:00.500000

2020-01-23 22:11:20 UTC+0000|[SHIMCACHE]| \??\C:\Windows\System32\invitation.exe|
2019-02-22 06:03:06 UTC+0000|[SHIMCACHE]| \??\C:\Users\IEUser\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Startup\invitation.exe|

REG_BINARY    %windir%\system32\invitation.exe :

Count:        3

Focus Count:    0

Time Focused:   0:00:00.500000

Last updated:   2020-01-23 22:38:19 UTC+0000

Raw Data:

0x00000000  00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00   ................

0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................

0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................

0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 20 81 b6 cf   ................

0x00000040  3d d2 d5 01 00 00 00 00                            =.......
```

- The winpmem and volatility modules that were executed captured various information about our Windows 7 vm. In this case, we had multiple modules that served different purposes of giving information about our backdoor. Pslist gives the active tasks on the system. Userassist finds programs and associates them with their run count and most recent execution. Cmdline shows our processes command-line arguments. Cmdscan shows the command history of our system. Malfind will show the hidden and injected code on our system. Sessions shows the details of the logon sessions for users. Finally, timeliner shows a timeline of different system occurrences in memory.

- These volatility modules gave a wealth of information when it came to our exploit. As can be seen above, pslist shows our invitation.exe as a running process on the system. The userassist module actually captured the dynamics of our binary when it came to execution with various run count and time associated metrics as can be seen here:

```
REG_BINARY    %windir%\system32\invitation.exe :

Count:        3 Focus Count:    0 Time Focused:   0:00:00.500000 Last updated:   2020-01-23 22:38:19
UTC+0000
```

- The cmdline showed our exploit to be the associated with the following information: invitation.exe pid: 1968 Command line : C:/Windows/System32/invitation.exe. It seemed that our exploit avoided detection by cmdscan. As for malfind, this module detects inject code ran and we can see that our exploit was picked up through the following: Process: invitation.exe Pid: 1968 Address: 0x1d0000 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6. It also showed associated binary instructions with the exploit. Sessions was also very helpful in detecting our backdoor as the initial boot sessions was caught and can be seen here: Process: 1968 invitation.exe 2020-01-31 01:51:31 UTC+0000. Finally, timeliner gave an in-depth look at the history of the actions taken by our exploit in its way through our system. We can see through various lines like: 2020-01-23 21:48:36 UTC+0000|[IEHISTORY]| explorer.exe->Visited: IEUser@http://192.168.56.102/invitation.pdf.ace| PID: 1624/Cache type "URL " at 0x1f87880 End: 2020-01-23 21:48:36 UTC+0000 and: 2020-01-31 01:51:31 UTC+0000|[PROCESS]| invitation.exe| PID: 1968/PPID: 1792/POffset: 0x3e931030, 2009-07-14 04:37:09 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2019-12-28 03:28:39 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\SESSION MANAGER| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2020-01-31 04:51:14 UTC+0000|[Handle (Key)]| MACHINE| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2009-07-14 04:42:25 UTC+0000|[Handle (Key)]| USER| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2009-07-14 04:37:06 UTC+0000|[Handle (Key)]| USER\CONTROL PANEL\INTERNATIONAL| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2020-01-16 21:16:34 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2012-10-15 03:53:48 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2019-12-28 02:27:15 UTC+0000|[Handle (Key)]| MACHINE\CONTROLSET001\CONTROL\NETWORKPROVIDER\HWORDER| invitation.exe PID: 1968/PPID: 1792/POffset: 0x3e931030, 2019-03-30 11:56:09 UTC+0000|[PE HEADER (exe)]| invitation.exe| Process: invitation.exe/PID: 1968/PPID: 1792/Process POffset: 0x3e931030/DLL Base: 0x00400000 give a history of the initial download all the way to our exploit "getting in" to the system and being registered.

- While most of the tools we utilized were external tools taken from an archive of tools, there are useful ways within Windows to analyze the system to find exploits like ours. For one, netstat, which we used, is a built-in utility that will be incredibly useful in determining exploits as weak as ours that must re-establish a consistent connection to the central command server. Another built-in utility that could be used to find registry associations for any suspicious programs is reg.exe or its gui counterpart rededit.exe. The one area that provides probably the most consistent activity information are the Windows Event Logs themselves. These could be analyzed to obtain a wealth of information for suspicious behavior by threats, and these logs are hard to consistently and stealthily remove so they could theoretically be depended upon. Last, but not least, we could utilize the powerful Sysmon tool. This method would remain across any reboot to monitor the system activity and record them in the Windows event logs that were mentioned as being useful. This monitoring during reboot would be very effective for catching somewhat noticeable exploits like ours when they execute at startup. Sysmon would also give us a nice array of activity on the system such as process creation, connections in terms of networking, and the modification of files and their details. This Sysmon information covers most of the volatility module output that we gathered in this lab, so we would have a built-in Windows method to get some of this information.