GoldenSpy: Chapter Two – The Uninstaller

Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

On June 25, 2020 Trustwave SpiderLabs published research showing that the Intelligent Tax software, published by Aisino Corporation and required by a Chinese bank, actually contained a hidden backdoor that surrendered complete command and control of the victim's network. This story received international news coverage and was widely discussed in security circles. To review the original blog post click here.

On June 28, 2020, our Threat Fusion team identified a new file being downloaded by the Aisino Intelligent Tax product. But this time it had nothing to do with remote command and control of the victim. Rather, this new sample's sole mission is to delete GoldenSpy and

remove any trace it existed. Including the deletion of registry entries, all files and folders (including the GoldenSpy log file), and finally, the uninstaller deletes itself with the following command: *cmd.exe /c del /q C:\Users\admin\AppData\Local\Temp\AWX.exe*. Note the "/c" which will terminate the Windows Command-line interface after the operation is completed and "/d" which will delete without asking permission or giving any notification.

Gone without a trace, or even knowing it was there.

In our testing, this GoldenSpy uninstaller will automatically download and execute, and effectively, will negate the direct threat of GoldenSpy in your environment, however, as the deployment of this uninstaller is delivered directly from the supposedly legitimate tax software, this has to leave users of Intelligent Tax concerned about what else could be downloaded and executed in a similar manner.

While the SpiderLabs team is gratified to see GoldenSpy research and analysis result in such a rapid course reversal in the Golden Tax threat campaign, we are not so optimistic as to believe that this new development signifies a slow-down in threat actor activity. This threat is a clear and present danger, driven by incredibly smart and innovative adversaries. We will allow for the briefest of pats on the back and then return to hunting for the next threat.

Organizations must continuously be vigilant, always threat hunting, because our adversaries will continue to find new ways to trick, manipulate, and socially engineer their way into environments. The value of the GoldenSpy case-study is not the IOCs we provided, it's the lesson that malware can be cleverly hidden in any software, regardless of its source or supposed legitimacy.

Full Analysis of the GoldenSpy Uninstaller below:

GoldenSpy Uninstaller

Description:

Trustwave SpiderLabs investigated the main tax software executable again for the execution flow because we observed the software execution is derived from the command given to upgrade or install new software on the infected machines.

Once installed, the main tax module will send a POST request for any software upgrades that are needed. Initially, it would download the SVMinstaller module to implant the GoldenSpy malware, but as of June 28, we have identified a new flow that downloads and executes a customized GoldenSpy uninstaller called "AWX.exe". Currently, Aisino Intelligent Tax Software is deploying the GoldenSpy Uninstaller, instead of GoldenSpy itself. This does raise the question as to what it might deploy next.

The GoldenSpy Uninstaller, called "AWX.exe" is silently pushed to infected machines from 223.112.21.2:8090 and it cleans up all the traces of GoldenSpy's existence. The following flow begins the process:

- The command "PROTOCOL_00" will request any software upgrades
- Receives command to install "AWX.exe"
- The command "PROTOCOL_99" downloads and executes "AWX.exe"
  http://223.112.21[.2:8090]/download/AWX.exe

Analysis:

MD5: 735AC19B261DC66D5850BEA21F3D54FE

SHA256:
7F5ED71F18937ECC6DB9520CA9A9D16E3C113609C7A9A99A29BA74687F1349D2

SHA1: 4755B68996B53AD3F734127FE46723B60681856E

PDB path : D:\日常工作\客户端软件\VCProject\dgs\Release\del.pdb

Translated : D:\day-to-day work\Client software\VCProject\dgs\Release\del.pdb

Created TImeStamp : 28 June 2020 04:15PM GMT

Upon installation, AWX.exe takes the following actions:

1. Identify the executables "svm.exe" and "svmm.exe"
2. Stop the "GoldenSpy" services
3. Kills both "svm.exe" and "svmm.exe" processes.
4. Log the Processes the svm error logs

- C:\Program Files (x86)\svm\log\{yearmonthdate}-svm.log
- C:\Program Files (x86)\svm\log\{yearmonthdate}-svmm.log

The contents of the log entries are shown below:

- [yeardatemonth time] [ERROR][SVM](5056): 1063
- [yeardatemonth time] [ERROR][SVMM](3880): 1063

1. Uninstall the autostart services and delete all files and folders containing any reference to GoldenSpy. To include:

- C:\Program Files (x86)\svm\svm.exe
- C:\Program Files (x86)\svm\svmm.exe
- C:\Program Files (x86)\svm

*Note, this deletion operation also deletes the log file it just generated.

1. Delete the registry entries

1. Self-Delete “GoldenSpy Uninstaller” AWX.exe

cmd.exe /c del /q C:\Users\admin\AppData\Local\Temp\AWX.exe

Second Sample Identified – BWXT.EXE

In the early morning hours of June 29, a second version of this GoldenSpy Uninstaller was identified to be downloaded by the Intelligent Tax software, only a few hours after the original was identified. The new sample was compiled on 29 June 2020 at 10:38PM GMT. Behaviorally, it was identical to AWX.EXE, however, this version obfuscated its variables with Base64 encoding. SpiderLabs cannot verify the reason for this change, but we hypothesize that it may have been to evade antivirus, as several AV engines began to alert on AWX.EXE.

Strings within the AWX.EXE include:

Project path:
D:\日常工作\客户端软件\VCProject\dgs\Release\BWXT.pdb
Translated Project Path:
D:\day-to-day work\Client software\VCProject\dgs\Release\BWXT.pdb

Observation:

During our analysis, we found that the GoldenSpy threat actors followed our removal recommendations step by step with their uninstaller. The table below shows our recommendations, compared to their installer.

Trustwave Recommendations	GoldenSpy Uninstaller
Freeze both svm.exe and svmm.exe processes	Stops the “GoldenSpy” services
Kill SVM processes	Looks “svm.exe” and “svmm.exe” and kills both processes
Go to SVM directory and permanently delete related files	Uninstall the service and delete the files and folder
Remove all registry artifacts related to SVM service	Remove all registry artifacts related to SVM service

N/A	Self-delete "AWX.exe"

Indicators of Compromise:

AWX.exe

MD5	735AC19B261DC66D5850BEA21F3D54FE
SHA256	7F5ED71F18937ECC6DB9520CA9A9D16E3C113609C7A9A99A29BA74687F1
SHA1	4755B68996B53AD3F734127FE46723B60681856E
Network	http://223.112.21[.2:8090]/download/AWX.exe

BWXT.exe

MD5	F2A7363CF43B5900BB872B0D4C627A48
SHA256	7D48F65FF9E904AC98E0F41B94F04723CE907FC221EFFFBBF83545CA167F
SHA1	3DFF337E2B3E1D3DC995A4B6965AE09C1BF5B137
Network	http://223.112.21[.2:8090]/download/BWXT.exe

GoldenSpy Uninstaller YARA Rule:

```
rule Goldenspy_Uninstaller
{
meta:
  author = "SpiderLabs"
  malware_family = "GoldenSpy"
 filetype =  "exe_dll"

strings:
```

```
    $str1 = "taskkill /IM svm.exe /IM svmm.exe /F" ascii    //Kill the running process
    $str2 = "\\svm.exe -stopProtect" ascii                  //Stop the service
    $str3 = "\\svmm.exe -u" ascii                           //Uninstall the malware
    $str4 = "\\VCProject\\dgs\\Release\\" ascii             //Project path
    $str5 = "dGFza2tpbGwgL0lNIHN2bS5leGUgL0lNIHN2bW0uZXhlIC9GIA" ascii
    $str6 = "c3ZtLmV4ZSAtc3RvcFByb3RlY3Q" ascii
    $str7 = "XHN2bW0uZXhlIC11" ascii
    $str8 = "Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\svm" ascii
    $str9 =
"U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWx
ascii


condition:

    (uint16(0) == 0x5A4D) and 4 of ($str*)

}
```

Special Thanks to SpiderLabs Threat Hunter Reegun Richard Jayapaul for his analysis of this new GoldenSpy threat actor activity.