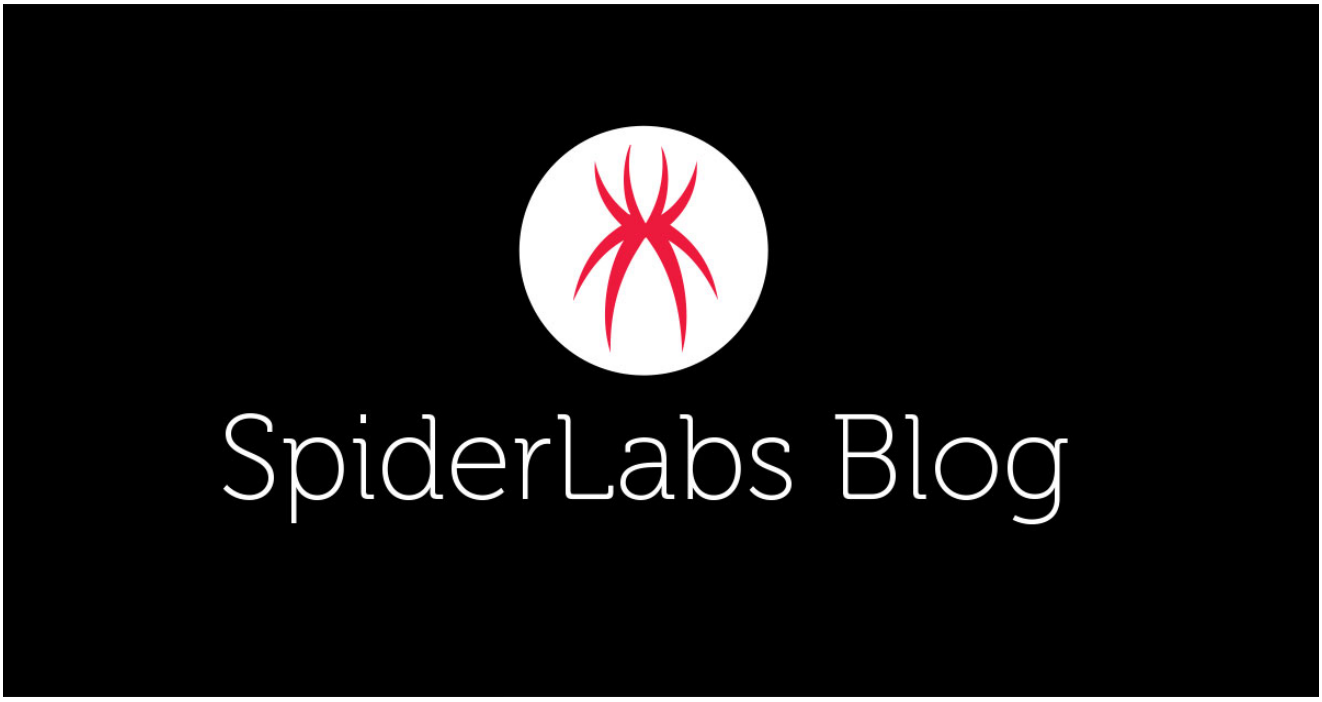
GoldenSpy Chapter 3: New and Improved Uninstaller

trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-3-new-and-improved-uninstaller/



Background:

- On June 25th, Trustwave SpiderLabs published our research on a backdoor, dubbed GoldenSpy, that was hidden in required Chinese tax software. See the details here.
- On June 30th, we published an analysis of a new binary that the tax software is deployed and executed to delete and remove all traces that GoldenSpy existed. We also provided a YARA rule to proactively identify the uninstaller. See the details here.
- This blog shows our analysis of a new binary, now being distributed by Intelligent Tax software, that is identical in operations to the original GoldenSpy Uninstallers, but specifically designed to evade detection by the YARA rule provided in our blog.

There is a constant battle between cyber adversaries and the security community, happening every minute of every day. Offensive operations and defensive countermeasures are constantly being launched back and forth, often to the massive detriment to the victim of a successful attack. But defenders are constantly monitoring for new offensive techniques and countering with innovative defensive measures to detect, disrupt, and deter the cyber-attacks. I have tremendous respect for both sides of this battle as each new strike shows creativity, innovation, and intelligence. However, rarely in my career have I ever witnessed such a clear demonstration of the back and forth than the GoldenSpy campaign that SpiderLabs has been reporting on.

To be fair, SpiderLabs does not know if this backdoor would have been used for malicious purposes or if the uninstall operation is anything more than an attempted clean-up by the company. The secretive nature of the clean-up and the remaining risk of the tax software being able to arbitrarily execute any code it likes is undeniable, but we are not claiming confirmed malicious intent. Just stating the facts.

The back and forth went like this: they planted a secret backdoor in the tax software, we identified it and published our research. They then secretly deployed a new binary to remove any trace that the backdoor ever existed, we reported on that as well and provided a method to detect it. Within hours, they responded with a new version that evades our detection method. Now, we report the new binary and provide an updated detection method. It's a real soap opera.

This is a true example of the cat and mouse game between cyber adversaries and the security community, the Intelligent Tax software now deploys and executes a third version of the GoldenSpy uninstaller. Based on our analysis, the new version conducts identical operations to delete all traces of GoldenSpy, but this one is specifically designed to evade the YARA rule we provided in our *GoldenSpy Chapter 2 The Uninstaller* blog. Our rule was based on identifying specific encoded and plain-text variables existing in both versions of the GoldenSpy, this new version alters its use of base64 encoding so that it will not be detected by our original YARA rule. This is the only difference in the new version.

The new executable was compiled on 1 July 2020 at 15:52:46 GMT. It is called AWX.exe, as was the original. We are providing the new YARA rule below, which will identify all variants of the GoldenSpy uninstaller. (At least all that we know of now, who knows what tomorrow will bring…) We appreciate the patronage of our blog by the GoldenSpy developers. Please stay tuned for future posts.

Binary Details:

File Name : AWX.EXE

SHA256 : 10E8C9ADE8687CFB2BADB23C90E8F025C2B2E35D0934D287E19C2B14746395C2

MD5 : 573ADB1569A08472094F0CFBB6264360

CRC32 : 739DA9B2

Format : Portable executable for 80386 (PE)

Timestamp : 5EFCB14E (Wed Jul 01 15:52:46 2020)

PDB File Name : D:\日常工作\客户端软件\VCProject\dgs\Release\AWX.pdb

OS type : MS Windows

Application type: Executable 32bit

GoldenSpy Uninstaller YARA rule – Version 2

```
rule Goldenspy_Uninstaller_v2
{
meta:
    author = "SpiderLabs"
    malware_family = "GoldenSpy"
    filetype =  "exe_dll"
    version = "3.0"

    strings:
    $str1 = "taskkill /IM svm.exe /IM svmm.exe /F" ascii
    $str2 = "\\svm.exe -stopProtect" ascii
    $str3 = "\\svmm.exe -u" ascii
    $str4 = "\\VCProject\\dgs\\Release\\" ascii
    $str5 = "Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\svm" ascii
    $str6 = "\\svmm.exe -stopProtect" ascii
    $str7 = "\\svm.exe -u" ascii
    $str8 = "Software\\Microsoft\\Windows\\CurrentVersion\\App Paths\\svm.exe" ascii
    $str9 = "dGFza2tpbGwgL0lNIHN2bS5leGUgL0lNIHN2bW0uZXhlIC9GIA" ascii
    $str10 = "c3ZtLmV4ZSAtc3RvcFByb3RlY3Q" ascii
    $str11 = "XHN2bW0uZXhlIC11" ascii
    $str12 =
"U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWx
ascii
    $str13 =
"U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cQXBwIFBhdGhz
ascii
    $str14 = "XHN2bS5leGUgLXU" ascii
    $str15 = "c3ZtbS5leGUgLXN0b3BQcm90ZWN0" ascii


condition:

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

    }
```