# GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software

trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/


Directly preceding GoldenSpy, another malware family was used to covertly access the networks of companies doing business in China. This is the story of GoldenHelper.


Table of Contents

## Story Highlights

- **Trustwave SpiderLabs has discovered malware embedded in Chinese tax software. This campaign was active in 2018-2019, prior to the GoldenSpy campaign and is hidden in the Golden Tax Invoicing Software (Baiwang Edition), required by Chinese banks for payment of VAT taxes.**
- **The new malware is entirely different from GoldenSpy, although the delivery modus operandi is highly similar. We named this family GoldenHelper, based on its association with the Chinese National Golden Tax project and one of the primary Command and Control domains: help.tax-helper.ltd.**
- **Although called "Baiwang Edition", GoldenHelper was digitally signed by NouNou Technologies, a subsidiary of Aisino Corporation, the same company responsible for the Intelligent Tax Software with embedded GoldenSpy malware.**

- **GoldenHelper malware utilizes sophisticated techniques to hide its delivery, presence, and activity. Some of the interesting techniques GoldenHelper uses include randomization of name whilst in transit, randomization of file system location, timestomping, IP-based DGA (Domain Generation Algorithm), UAC bypass and privilege escalation.**
- **Our current telemetry shows that GoldenHelper is designed to drop a final payload, called taxver.exe. Trustwave SpiderLabs has not yet been able to obtain a copy of this file and is requesting assistance from our readers to contact us at goldenspy@trustwave.com if they have information on this file or a sample for us to analyze.**
- **Reference the original story of GoldenSpy malware here.**

## Golden Tax Project

During major fiscal reforms in 1994, China began a value-add tax (VAT) system requiring businesses to pay tax on the difference of their revenue represented on invoices and their expenses. During this same timeframe the "Golden Tax Project" (GTP) was launched to centralize VAT tax invoicing and fight against tax fraud using sophisticated software and spearheaded by the former Premier of the State Council, Comrade Zhu Rongji. This objective was clear after listening to reports from Ministry of Electronics, the Aerospace Industry Corporation, Ministry of Finance, and the State Administration of Taxation.

While this is one of many "Golden" PRC projects, it is in its third phase and known as Golden Tax III which began in 2016. Now fully implemented since 2017, online issuance of VAT invoices and uploads can occur to a centralized back-end database linking all e-invoicing. At this time, there are only two official providers of the invoicing systems, Aisino and Baiwang.

## The Golden Gateway

On June 25, 2020, the Trustwave SpiderLabs team issued an Emerging Threat Report about the GoldenSpy backdoor malware. In the full report we concluded that while we were not aware of any ongoing attack, the backdoor had several characteristics that could lead to a major compromise. As reported, the GoldenSpy malware is installed as part of the mandated Tax Software produced by Aisino. To recap, the suspicious characteristics of GoldenSpy are:

- Covert download; two hours after the Intelligent Tax software is installed.
- Two autostart services created to monitor and restart itself.
- Uninstalling the tax software does not uninstall the GoldenSpy binaries.
- Beaconing traffic to a domain that is not related to the tax software.
- Running with system level privileges and allowing for remote code execution.

Since the Trustwave SpiderLabs report went public, our team has discovered the Aisino tax software downloading and running an uninstaller, removing all evidence of the GoldenSpy malware. Again, the team released the information to the public via the Trustwave SpiderLabs blog: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/

Several characteristics make this suspicious as well:

- June 28 – Uninstaller spotted in the wild pushed from 223.112.21.2:8090
- June 29 – Uninstaller is obfuscated with Base64 encoding
- July 1 – New uninstaller pushed with further obfuscation to escape Yara Rule released by Trustwave SpiderLabs

Since our GoldenSpy publications, many people from the security community have reached out and shared their GoldenSpy related threat intelligence. As this intelligence collaboration continued, the Trustwave SpiderLabs team became aware of another Golden Tax invoice software containing malicious code. The software is linked to Aisino, as was GoldenSpy, and has the following suspicious characteristics:

- Does not require a user’s permission to install and escalate to SYSTEM level privilege (UAC bypass)
- Randomly generated filenames (Obfuscation)
- Randomly generated "Creation" and "Last write" timestamp (Timestomping)
- Attempts to download an executable using fake filenames with .gif, .jpg, .zip (Obfuscation)
- Hardcoded logic to control download location, what to download and where to place it based on results of DNS resolution (DNS Control)

Although this malware is functionally very different from GoldenSpy, the delivery modus operandi is highly similar. We will refer to these new samples as GoldenHelper, based on its relation to the Golden Tax project and its tax-helper domain C2 infrastructure. The installation process flow for this software is shown below:

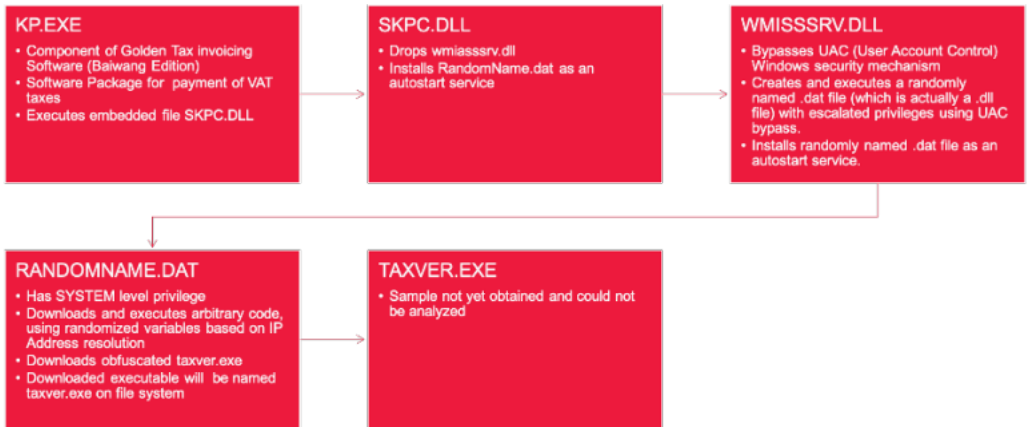


Figure 1: GoldenHelper execution process flow

This malware utilizes three different .dll files:

1. DLL – to interface with the Golden tax software
2. DLL – to bypass Windows security and escalate privileges
3. {random_name}.DAT – to download and execute arbitrary code with SYSTEM level privilege

The final payload, taxver.exe, is downloaded and executed, and could be located in several locations in the file system. To date, Trustwave SpiderLabs has been unable to procure a sample of taxver.exe. We are actively requesting community assistance in this endeavor. If you have information on taxver.exe, or can provide a sample, please reach out to us at: goldenspy@trustwave.com

Detailed malware analysis will be provided later in this report.

The Golden Tax Project is a national program in China, impacting every business operating in China. We are currently aware of only two organizations authorized to produce Golden Tax software, Aisino and Baiwang. This is now the second Golden Tax software package that Trustwave SpiderLabs has found to contain a hidden backdoor capable of remotely executing arbitrary code with SYSTEM level privileges.

During our investigation, we have been informed that the Golden Tax software may be deployed in your environment as a stand-alone system provided by the bank. Several individuals report receiving an actual Windows 7 computer (Home edition) with this Golden Tax software (and GoldenHelper) preinstalled and ready to use. This deployment mechanism is an interesting physical manifestation of a trojan horse.

It is important to remember that as a security community protecting critical data and infrastructure, we must remain vigilant and weigh all options and risks individually. Trustwave SpiderLabs understands that the VAT tax invoice software is a government requirement and recommends that any system hosting third-party applications with a potential for adding a gateway into your environment, be isolated and heavily monitored with strict processes and procedures in their usage.

## GoldenHelper Campaign Timeline

Trustwave SpiderLabs does not believe that the GoldenHelper campaign is currently active because the command and control domains utilized by the dropper mechanisms described in this report expired in January 2020. However, we have not yet been able to obtain a sample of taxver.exe, the final payload of the attack, and cannot confirm if it uses the same network infrastructure. So, the threat contained within the final payload of this attack may still be active.

The timeline below shows the currently confirmed dates relevant to the GoldenHelper campaign. The dates include domain registration and expiration and malware sample compilation. It is important to note that we have not recovered every sample likely to be involved with this campaign (first recovered skpc.dll was version 2.1.0.11), however, our analysis makes it clear that GoldenHelper was active from January 2018 until July 2019. This leads directly into the launch of the GoldenSpy campaign in April 2020 (only to be prematurely shut down in June 2020, due to Trustwave SpiderLabs public exposure of the incident details).

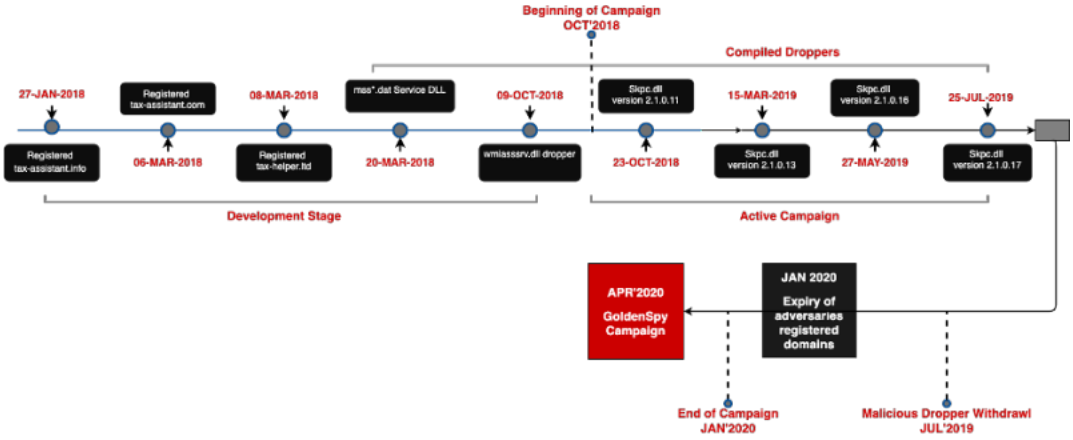


Figure 2: GoldenHelper campaign timeline

We cannot definitively know why the GoldenHelper campaign was abruptly abandoned in July 2019. The incremental malware development cycle continued for the known samples from early 2018 to July 2019 and the domains associated with the it expired and were released in January 2020. It is important to note that the final version of Skpc.exe (2.1.0.17) was released July 25, 2019 and it contained no malicious artifacts. Hence, anyone installing the Baiwang edition of the Golden Tax Invoicing Software after July 2019 would not be impacted by this campaign. While this taxver.exe deployment mechanism appears to no longer be active, it is important to understand that taxver.exe may still be an active and operational threat on countless victim networks. We cannot know its purpose until we obtain and analyze a sample.

We can hypothesize on the reasoning for the end of GoldenHelper in July 2019. The pictures below show the VirusTotal detection rates for the various samples during the first quarter of 2019. All saw a significant jump in detection ratios during that time frame. Wmiasssrv.dll was detected by 1/71 antivirus engines in January of 2019, compared to 29/71 by March of 2019. Similarly, RandomName.dat was identified as malicious by 3/71 AV engines in January 2019, and 26/71 in March 2019. We believe that the increasing antivirus engine detection capability contributed to the decision to abandon the GoldenHelper campaign in January 2020.

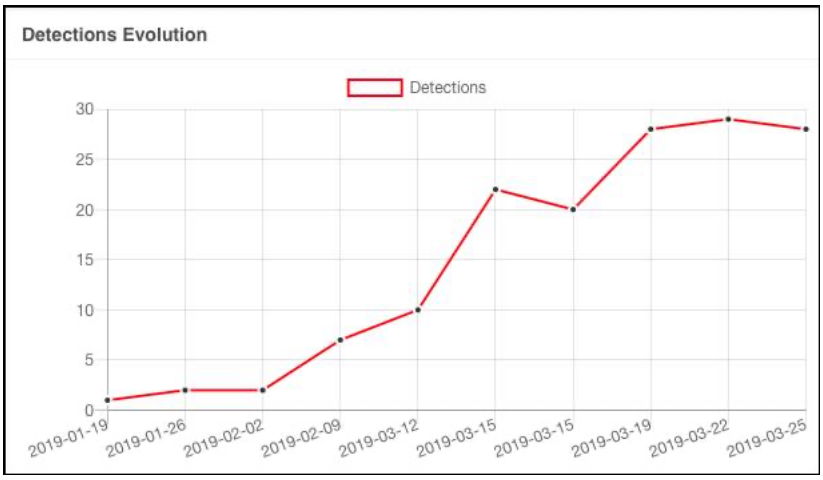


Figure 3: Wmiasssrv.dll – Detection increases on March 2019

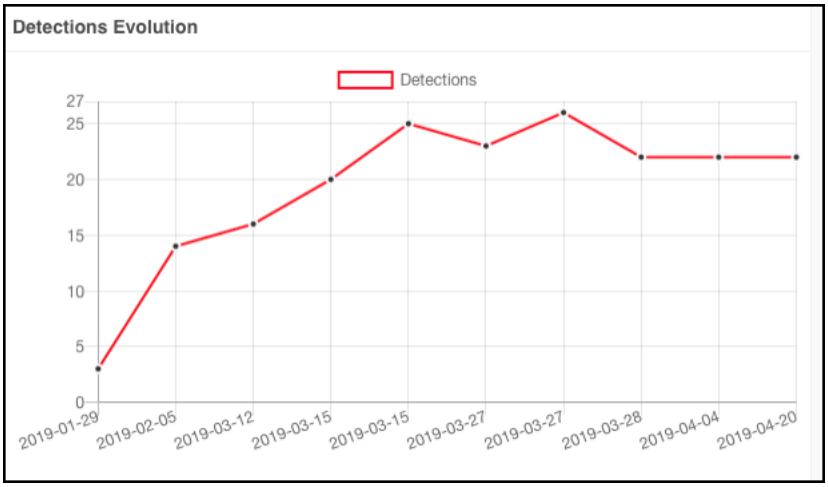


Figure 4: RandomName.dat detection increases on March 2019

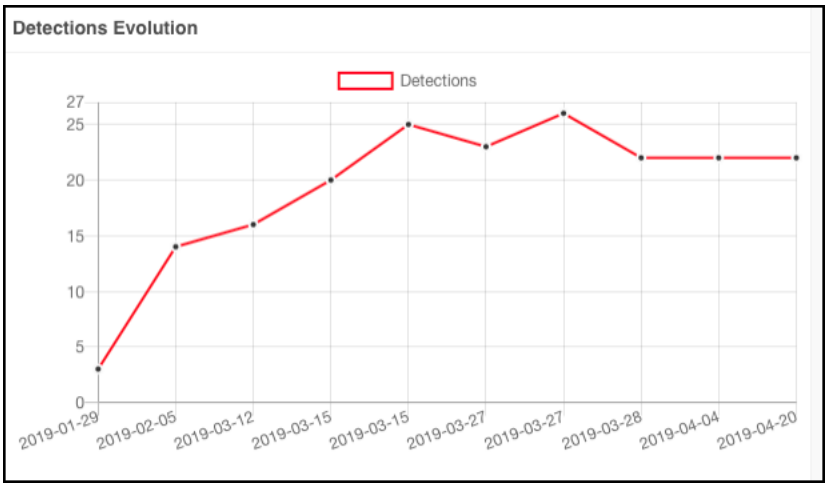


Figure 5: Skpc.dll 2.1.0.13 – Detection increases on April 2019

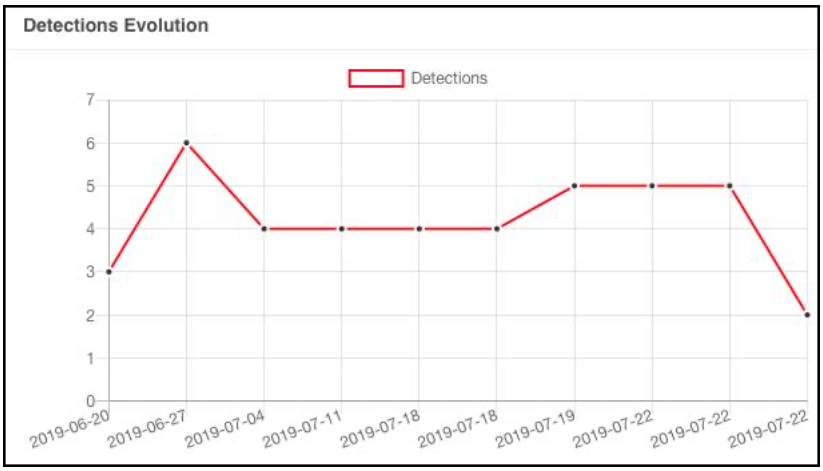


Figure 6: Skpc.dll 2.1.0.16 – Detection increases on June 2019

The GoldenHelper deployment mechanism may no longer be active, but we cannot say if the overall threat presented by taxver.exe is still operational, or not. The GoldenHelper campaign was directly followed by GoldenSpy, and while Trustwave SpiderLabs was able to quickly identify and expose the current iteration of GoldenSpy, leading the adversaries to draw down the campaign, we have no doubt that this threat will continue to evolve to a new methodology targeting businesses with operations in China.

## What is taxver.exe?

The GoldenHelper campaign is designed to covertly download and execute a final payload with SYSTEM level privileges called taxver.exe. We currently do not have a sample of this file and cannot state its purpose. However, there are a few key characteristics that are important for hunters to consider:

1. exe cannot be directly identified by searching network traffic, based on the algorithm the dropper utilizes, it will appear to be one of several names while in transit:
    - jpg
    - gif
    - dat
    - rar
    - zip

1. When copied to the victim file system, it will be called taxver.exe, however, based on the randomization algorithm, it may be located in any of the following paths:
    - "%WINDIR%\system32\taxver.exe
    - "%WINDIR%"\debug\wia\taxver.exe
    - "%WINDIR%"\debug\taxver.exe
    - "%WINDIR%"\taxver.exe
    - "%ALLUSERPROFILE%"\taxver.exe
    - "%COMMONPROGRAMFILES%"\taxver.exe

1. While we do not have a sample of taxver.exe and cannot confirm that it is malicious, it is important to note that legitimate software does not:
    - Utilize UAC bypass to evade Windows security controls and escalate privilege
    - Randomize file system location
    - Hide its name and true nature in network traffic
    - Lack version negotiation protocols
    - A legitimate updater tends to have its main control protocol purposely designed rather than overriding DNS records

## Indicators of Compromise: Files

As stated, we believe the GoldenHelper campaign was active from January 2018 to July 2019. During that time, the adversary created several variations of their malware. The versions listed below are all of the samples that Trustwave SpiderLabs could recover from this campaign, although the list is likely not complete. Behaviorally, there are no substantive changes amongst the different versions, except for the last one, Skpc.dll Version 2.1.0.17, which contains no malicious artifacts. We suspect that at the point when this version was released, the GoldenHelper campaign was being rolled back due to increasing antivirus detection rates.

| File Name | >MD5 | PE Compile Time | Version | Malware Artifacts | Verdict |
|---|---|---|---|---|---|
| msxxxs999.dat (RandomName.dat) | 490d17a5b016f3abc14cc57f955b49b3 | 2018:03:20 00:26:36 | Service DLL | Yes | Malicious |
| Wmiasssrv.dll | 682a0826db8572bad205a4db12005e13 | 2018:10:09 12:26:36 | Service Dropper | Yes | Malicious |
| Wmiasssrv.dll | 26e71f1d387298162c1b19e858d001a1 | 2018:10:09 12:26:36 | Service Dropper | Yes | Malicious |
| Skpc.dll | 9e2ebdbc9ba4dca69a712e3268f3ab77 | 2018:10:23 3:30:26 | 2.1.0.11 | Yes | Malicious |
| Skpc.dll | fbb35e8f16e7d5a735f06ae03e8bfaac | 2019:03:15 08:53:30 | 2.1.0.13 | Yes | Malicious |
| Skpc.dll | 61eed90b1ae70244cd87a3abd3ec622a | 2019:03:15 08:53:30 | 2.1.0.13 | Yes | Malicious |
| Skpc.dll | d312336fd46972a544929d0dc4e07b83 | 2019:03:15 08:53:30 | 2.1.0.13 | Yes | Malicious |
| Skpc.dll | 27d448f9d2bed761e15541c55b5966f2 | 2019:05:27 01:28:44 | 2.1.0.16 | Yes | Malicious |
| Skpc.dll | bee06d785b7e51a0127a96c5854d4345 | 2019:05:27 01:28:44 | 2.1.0.16 | Yes | Malicious |
| Skpc.dll | 471c75acc284396354c89616f9030718 | 2019:07:25 09:12:33 | 2.1.0.17 | No | Clean |

## Indicators of compromise: Domains

The Randomname.dat file is not actually fully random. Its name will always begin with "ms", followed by three random characters, then "s", then a number. Put another way, the file is named like this: ms{3-random-chars}s{0-999}.dat. This report will just refer to RandomName.dat to reduce confusion. Of course, this file is not a data or configuration file, as would be expected from a .dat extension. Rather, this is an executable file, utilizing the thin veil of obfuscation by changing the extension.

RandomName.dat contacts the following 3 hard-coded domains whose response is delivered in the format of an IP address, but each octet of the IP address actually contains the hidden instructions for delivery of the final payload. Hidden within the IP address are instructions for where to download taxver.exe from, what to name it in transit, and where to save it on the victim file system. Each of the following domains will be resolved until one returns the expected IP address. While the GoldenHelper campaign was active, all of these domains were registered to Chengdu West Dimension Digital Technology Co., LTD. They were all registered around the same time and the registration for each was allowed to expire in January 2020.

| Domain | Actor registration | Deletion due to expiry |
|---|---|---|
| tax-helper.ltd | 3/8/18 | 2/5/20 |
| tax-assistant.com | 3/6/18 | 3/1/20 |
| tax-assistant.info | 1/27/18 | 2/4/20 |

## Introduction to the Players

Aisino Corporation plays a central role in both the GoldenHelper and GoldenSpy campaigns. The Trustwave SpiderLabs' GoldenSpy report clearly shows how Aisino produced the "Intelligent Tax Software", but utilized a company called Nanjing Chenkuo Network Technology to produce the GoldenSpy malware. In the case of the "Golden Tax Invoicing software (Baiwang Edition)", NouNou Technology Ltd. produced both the legitimate tax software and the hidden GoldenHelper malware. NouNou Technology is a subsidiary of Aisino, and Aisino's website states that they are owned by state company CASIC (China Aerospace Science & Industry Corporation Limited).

It is worth noting that although the Golden Tax Invoicing Software is referred to as "Baiwang Edition", we could not identify any links between Baiwang and the software development. The only link we found was that the software utilized an API connection to Baiwang cloud infrastructure for the legitimate tax transactions.

The diagram below shows the corporate relationships behind both GoldenHelper and GoldenSpy campaigns. For color schema reference:

- Green indicates legitimate usage by tax software
- Orange indicates Aisino Corporation and its subsidiaries
- Red indicates shadow backdoor network infrastructure
- Blue is the overall background of the Chinese Golden Tax Project

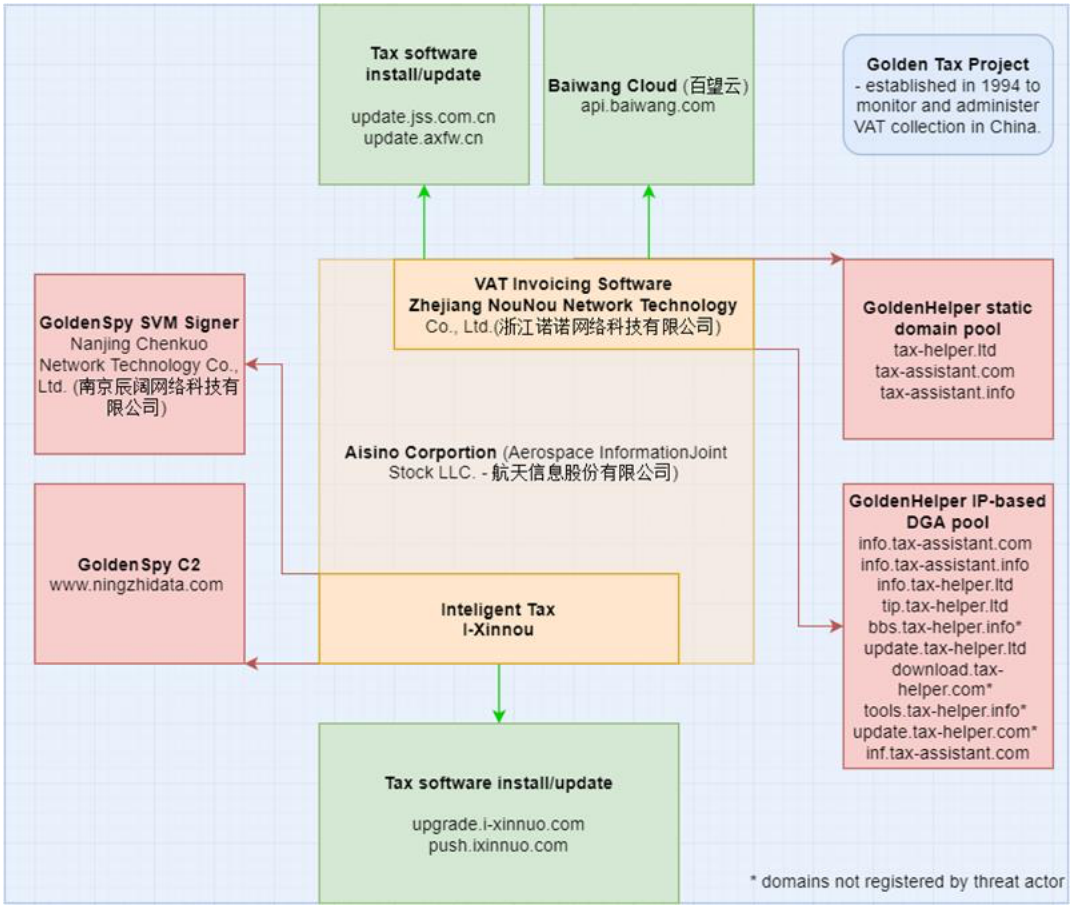


Figure 7: Skpc.dll 2.1.0.16 – Organizations and their roles ini GoldenSpy and GoldenHelper

Based on the GoldenHelper and GoldenSpy campaigns, several similar characteristics present themselves:

- A subsidiary of Aisino corporation creates Golden Tax related software.
- The tax software utilizes dedicated infrastructure and components (installer, uninstaller, updater and main tax software). Components are installed and uninstalled on user demand and approval and properly conduct legitimate tax operations.
- Hidden malware is installed alongside the legitimate tax software.
- Hidden malware utilizes separate network command and control infrastructure than used by the tax software.
- Hidden malware has the ability to remotely download and execute arbitrary code at SYSTEM level privilege.
- Hidden malware uses obfuscation techniques to hide deployment and communication methodologies.

## Corporate Profiles:

**Golden Tax Project (GTP)**: Project established in 1994 to monitor and administer VAT collection across the People's Republic of China. It obligates companies to utilize state approved software in order to perform VAT operations. The project aims to support counter fraud detection by adding heuristic and AI cloud modeling.

**Aisino Corporation:** (Aerospace Information Joint Stock LLC. - 航天信息股份有限公司) Listed IT company specializing in information security. Their website states they are owned by the state company CASIC (China Aerospace Science & Industry Corporation Limited - 中国航天科工集团公司).

**Zhejiang NouNou Network Technology Co., Ltd.(** 浙江诺诺网络科技有限公司)[1]: Integrates social resources, gathers third-party professional services, builds bridges, and provides comprehensive services in the fields of individual finance, taxation, and supply chain. NouNou is an Aisino subsidiary.

Services provided by NouNou:

**Baiwang Cloud (百望云):** As per their company web page, "*leading provider of smart taxation and electronic invoice services in China. Baiwang Cloud is committed to realize the closed loop of business transactions in a digital way, so that every link in the business transaction chain can enjoy the benefits of digitization and build an open digital business platform*."[2] Baiwang provides SaaS for industry finance and tax integration.

## Detailed Malware Analysis:

Analysis is of two files, JSKP_BWB_1.0.4.0.exe and skpc.dll. JSKP_BWB_1.0.4.0.exe is the installer for an older version of Baiwang edition tax software available from nuonuo[.]com. Recent versions of this software do not contain the DLL files described in this analysis.

**JSKP_BWB_1.0.4.0.exe**

Analysis of this file has been limited to installation and update mechanisms.

Update traffic flow:

Initial update check-in in via unencrypted HTTP traffic:

hxxp://update.jss[.]com[.]cn/interfaceCtr/version.do?version=1.0.4.2.01&type=18&orgcode=

Update download:

{"auto":0,"downUrl":"
hxxp://update.axnfw[.]cn/JSKP_BWB_1.0.4.2.01.exe","enforce":0,"result":"true","text":"","update":1,"version":"1.0.4.2.01"}

The updater file "update_bak.exe" will check for updates via HTTP periodically after installation

hxxp://xz.jskp.jss[.]com[.]cn/BwJskp.dat?21105437

Further updates are downloaded from xz.asnfw[.]cn

{"DownList":
[{"DownModel":0,"EndFile":"","FileCmd":"/S","FileMd5":"40A84B78944235850690C7873924282E","FileName":"JSKP_BWB_1.0.4.0.exe","FileSiz

During installation, the next file in our analysis, skpc.dll, is dropped on disk and is executed by software component kp.exe. It should be noted that during our dynamic analysis kp.exe was not dropped by the installer, we have not determined whether this is because it was designed to be retrieved as an update or whether a packed version requires a specific trigger to drop.

**skpc.dll**

We are specifically analyzing version 2.1.0.13 of this file with hash 99244e4186047a6531177fd189b3c299efa7db869db7ed307e3afa372913f306. Version 2.1.0.16 has a similar behavior while version 2.1.0.17 has this behavior removed.

skpc.dll is launched by the sc.exe component of the tax software. As noted, we are analyzing version 2.1.0.13 but during execution it writes the following entries to the file nisec_yyyy-mm-dd.log. We believe this is referring to an earlier version of skpc.dll from 2018 since the copy of regsvr32.exe on our test machine is from a different year.

2020-07-07 12:09:21:0070 00000928 this dll make datetime is : Dec 27 2018 09:20:29

2020-07-07 12:09:21:0070 00000928 exe this dll is : C:\Windows\SysWOW64\regsvr32.exe

2020-07-07 12:09:21:0070 00000928 this dll version is : 2.1.0.8

Inside skpc.dll another library is embedded, wmiasssrv.dll. This library (also referred to as WMI Assistant Patch) exports a number of functions and contains a further embedded dll. skpc.dll calls the WriteLibrary function from wmiasssrv.dll to install this third nested dll as a service. There are several aspects of this installation process which raise red flags.

The first suspicious aspect is that the third dll is not named as such but rather is given a random name using the format ms{aaa}s{999}.dat. This file is dropped in C:\Windows\system32 and installed as a service with full system privileges using a UAC bypass technique.

The specific UAC bypass used is documented at https://msitpros.com/?p=3960 and abuses a COM elevation moniker technique by creating an inf file and launching the inf file using the COM CMSTPLUA object. The contents of the inf file are below. An interesting note is that the second dll in this chain is named wmiasssrv, which appears to be named after Windows Management Instrumentation, while the service created as a result is named WMPAssis, which appears to be named after Windows Media Player.

[version]

signature = $Windows NT$

[DefaultInstall]

addREG = WMPAssis_AddReg

[WMPAssis_AddReg]

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","Type",0x11001,20,00,00,00

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","Start",0x11001,02,00,00,00

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","ErrorControl",0x11001,01,00,00,00

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","DisplayName",0x1000,"WMPAS"

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","ObjectName",0x1000,"LocalSystem"

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","Description",0x1000,"WMP Assistant Patch"

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis","ImagePath",0x21000,"%systemroot%\system32\svchost.exe -k WMPAG7600"

hklm, "SYSTEM\CurrentControlSet\services\WMPAssis\Parameters","ServiceDll",0x21000,"C:\Windows\system32\msfils945.dat"

hklm, "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost", "WMPAG7600", 0x11000, "WMPAssis"

Once this randomly named dll is installed as a service it attempts to download and install further software using the following process.

1. Resolve the following domains until a resolution succeeds. The IP address returned by this step will be used in following steps. It should be noted that traffic is never actually sent to this IP address, it is used purely as a way to control how the software behaves.
2. Take the IP address from step one, a.b.c.d, and either sleep or download the next payload using the algorithm:

***a* - main action:**

1: download file if local taxver.exe does not already exist

2: update delay time, where b.c.d is number of hours to sleep, e.g. 2.0.1.1, sleep for 11 hours

3: download file, force download even if taxver.exe already exists

***b* - determines which host to download from:**

1: info.tax-assistant.com

2: info.tax-assistant.info

3: info.tax-helper.ltd

4: tip.tax-helper.ltd

5: bbs.tax-helper.info

6: update.tax-helper.ltd

7: download.tax-helper.com

8: tools.tax-helper.info

9: update.tax-helper.com

default: info.tax-assistant.com

***c* - what to download:**

0: /app/taxver.jpg

1: /app/tps32.gif

2: /data/msabs.dat

3: /data/msabb.rar

4: /data/tax32.zip

default: /data/taxver.jpg

***d* - where to save download, note that file is always renamed to taxver.exe**

0: "%WINDIR%\system32\taxver.exe

1: "%WINDIR%"\debug\wia\taxver.exe

2: "%WINDIR%"\debug\taxver.exe

3: "%ALLUSERPROFILE%"\taxver.exe

4: "%WINDIR%"\taxver.exe

5: "%COMMONPROGRAMFILES%"\taxver.exe

From this analysis we can see that the software exhibits the following unusual behaviors:

- Ability to sleep indefinitely while waiting to download
- Executable is downloaded with a disguised extension
- The ability to switch download domains using an IP-based DGA (Domain Generation Algorithm)
- The ability to place the downloaded executable in a variety of locations

### Domains referenced

There are three hard-coded domains which are the first stage of retrieving the final payload, shown in the first table below. These domains drive the download of taxver.exe according to the algorithm described above. During the period when the first version of this software was active, all of these domains were registered through the registrar Chengdu West Dimension Digital Technology Co., LTD. While the actual organization which registered the domains is hidden by a WHOIS privacy service, they were all registered at about the same time and the registration on each was allowed to expire about two years later. Based on this we believe that all were registered by the same organization and that the time they were registered is in the middle of the preparation period for this campaign.

| Domain | Actor registration | Deletion due to expiry |
|---|---|---|
| tax-helper.ltd | 3/8/18 | 2/5/20 |
| tax-assistant.com | 3/6/18 | 3/1/20 |
| tax-assistant.info | 1/27/18 | 2/4/20 |

The second set of domains are the ones used for the actual payload download. While the first set of domains are in our list of Indicators of Compromise (IOCs), we recommend not using the second set for this purpose because some of them belong to organizations we believe are not associated with the campaign. The purpose of the software including these unaffiliated domains is unclear.

| Domain | Actor domain registration | Deletion due to expiry | Owned by campaign |
|---|---|---|---|
| info.tax-assistant.com | 3/6/18 | 3/1/20 | Yes |
| info.tax-assistant.info | 1/27/18 | 2/4/20 | Yes |
| info.tax-helper.ltd | 3/8/18 | 2/5/20 | Yes |
| tip.tax-helper.ltd | 3/8/18 | 2/5/20 | Yes |
| bbs.tax-helper.info | n/a | n/a | No |
| update.tax-helper.ltd | 3/8/18 | 2/5/20 | Yes |
| download.tax-helper.com | n/a | n/a | No |
| tools.tax-helper.info | n/a | n/a | No |
| update.tax-helper.com | n/a | n/a | No |
| inf.tax-assistant.com | 3/6/18 | 3/1/20 | Yes |

## YARA Rule for Hunting:

As we have for every iteration of GoldenSpy, Trustwave SpiderLabs is providing the following GoldenHelper YARA rule to help with GoldenHelper hunting operations.

**YARA – GoldenHelper.yar**

```
 rule GoldenHelper
{
meta:
   author = "SpiderLabs"
   variant = "GoldenSpy"
   filetype = "exe_dll"
   features = "UAC bypass,Updater,Dropper,ServiceDLL"
   version = "2.0"
strings:
   $str1 = "WMPAssis_AddReg" wide ascii
   $str2 = "wmsma.inf" wide ascii
   $str3 = "taxhelper" wide ascii
   $str4 = "WMP Assistant Patch" wide ascii
   $str5 = "Elevation:Administrator" wide ascii
condition:
   (uint16(0) == 0x5A4D) and 4 of ($str*)
}
```

## Thank you to our Contributors:

When Trustwave SpiderLabs first published our research on the GoldenSpy campaign, on June 25, 2020, we set up an information sharing email address goldenspy@trustwave.com that is delivered directly to the security research team. Our hope was to confidentially crowdsource cyber threat intelligence sharing to expand our telemetry into the GoldenSpy campaign. This turned out to be enormously successful as many companies reached out to us to share their experiences and the impact of GoldenSpy within their environment.

This sharing led us to the discovery of GoldenHelper and allowed us to further our investigations into supply-chain compromises associated with the Chinese Golden Tax Project. We would like to thank everyone that contacted us, shared their experience, and enabled us to continually educate the public on this threat.  Your effort will benefit countless organizations in similar situations.

However, there is still a gap in this story. We have not yet identified a sample of the final GoldenHelper payload, taxver.exe. We do not know its purpose, capabilities, or IOCs. Therefore, we are keeping open the goldenspy@trustwave.com email address and welcome further intel sharing regarding GoldenSpy, GoldenHelper, or any other related compromise.

[1] https://www.jss.com.cn/Contents/portal/allow/aboutus/about.ftl

[2] http://www.baiwang.com/mainsite-new/about