The Golden Tax Department and the Emergence of GoldenSpy Malware | Trustwave

By Brian Hussey

Published: 2020-06-22 · Archived: 2026-04-05 14:29:20 UTC

June 22, 2020 3 Minute Read

Trustwave SpiderLabs has discovered a new malware family, dubbed GoldenSpy, embedded in tax payment software that a Chinese bank requires corporations to install to conduct business operations in China.

In April of 2020, the Trustwave SpiderLabs Threat Fusion Team engaged a customer to conduct a threat hunt. The company is a global technology vendor with significant government business in the US, Australia, UK, and recently opened offices in China. Our threat hunt produced several key findings important to the long-term security of their network, however, one key finding stood out as potentially impacting countless other businesses who currently operate in China. A full analysis of our findings is available for download in this report in which Trustwave SpiderLabs threat hunting experts investigate a malware campaign targeting corporations operating in China.

Investigation Details

We identified an executable file displaying highly unusual behavior and sending system information to a suspicious Chinese domain. Discussions with our client revealed that this was part of their bank's required tax software. They informed us that upon opening operations in China, their local Chinese bank required that they install a software package called Intelligent Tax produced by the Golden Tax Department of Aisino Corporation, for paying local taxes.

As we continued our investigation into the tax software, we found that it worked as advertised, but it also installed a hidden backdoor on the system that enabled a remote adversary to execute Windows commands or to upload and execute any binary (to include ransomware, trojans, or other malware). Basically, it was a wide-open door into the network with SYSTEM level privileges and connected to a command and control server completely separate from the tax software's network infrastructure. Based on this, and several other factors (described below) we determined this file to have sufficient characteristics to be malware. We've since fully reverse-engineered the files and named the family GoldenSpy.

GoldenSpy was digitally signed by a company called Chenkuo Network Technology and the signature used identical text for both the product and description fields; 认证软件版本升级服务 – which translates to "certified software version upgrade service". This name may sound like legitimate software, however, in this situation the tax software already has its own updater service that functions well, and in a way completely unrelated to GoldenSpy.

There were several other unusual aspects of this file, to include:

- GoldenSpy installs two identical versions of itself, both as persistent autostart services. If either stops running, it will respawn its counterpart. Furthermore, it utilizes an exeprotector module that monitors for the deletion of either iteration of itself. If deleted, it will download and execute a new version. Effectively, this triple-layer protection makes it exceedingly difficult to remove this file from an infected system.
- The Intelligent Tax software's uninstall feature will not uninstall GoldenSpy. It leaves GoldenSpy running as an open backdoor into the environment, even after the tax software is fully removed.
- GoldenSpy is not downloaded and installed until a full two hours after the tax software installation process is completed. When it finally downloads and installs, it does so silently, with no notification on the system. This long delay is highly unusual and a method to hide from the victim's notice.
- GoldenSpy does not contact the tax software's network infrastructure (*i-xinnuo[.]com)*, rather it reaches out to *ningzhidata[.]com*, a domain known to host other variations of GoldenSpy malware. After the first three attempts to contact its command and control server, it randomizes beacon times. This is a known method to avoid network security technologies designed to identify beaconing malware.
- GoldenSpy operates with SYSTEM level privileges, making it highly dangerous and capable of executing any software on the system. This includes additional malware or Windows administrative tools to conduct reconnaissance, create new users, escalate privileges, etc.

These factors have led us to the conclusion that GoldenSpy is a well-hidden and powerful backdoor that surrenders full remote command and control of the victim system to an unknown adversary.

The diagram below shows the network communication patterns of GoldenSpy installation via Intelligent Tax software.


Svmdiagram

The scope of this campaign is not currently known. For our client, GoldenSpy was secretly embedded within the Aisino Intelligent tax software, but we cannot determine if this was targeted because of their access to vital data, or if this campaign impacts every company doing business in China. We have identified similar activity at a global financial institution, but do not yet have further telemetry into this campaign.

The current GoldenSpy campaign began in April of 2020, however, our cyber threat intel analysts have discovered variations of GoldenSpy that date back to December of 2016. It is of interest that Chenkuo Technology's website announced a partnership with Aisino in October of 2016, two months prior to the original emergence of the GoldenSpy malware family. Their partnership is for "big data cooperation". GoldenSpy certainly could enable big data access and collection. Trustwave SpiderLabs has no current knowledge if GoldenSpy was active in the wild since 2016, our first identification of usage was April 2020. To be clear, we do not yet know the scope, purpose, or actors behind the threat. We do not know whether Chenkuo Technology or Aisino are active and/or willing participants or the extent of their involvement other than what is presented in the report.

Partnership

Recommendations

We believe that every corporation operating in China or using the Aisino Intelligent Tax Software should consider this incident a potential threat and should engage in threat hunting, containment, and remediation countermeasures, as outlined in our technical report (download link below).

Trustwave SpiderLabs is still actively investigating and seeking out more telemetry on the GoldenSpy campaign. If you have any information about this activity or feel you may have been victimized by this attack, please reach out to the Trustwave SpiderLabs Threat Fusion Team at GoldenSpy@trustwave.com.

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

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.

Stay Informed

Sign up to receive the latest security news and trends straight to your inbox from LevelBlue.
