TLP:CLEAR

INTEGRATION OF UNTRUSTED SOFTWARE

THE CASE OF GOLDENSPY

Version 2022/en

December 7, 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

TLP:CLEAR

Table of contents

1 Integration of untrusted software

The regulatory frameworks of some countries may require these companies to use specific software. While their integration does not usually present any technical concern, such software can entail some specific security risks. Furthermore, they represent an opportunity for attacks by adversaries who could target a software that is popular in the region to reach companies in a given country.

The installation of some versions of the Chinese software *GoldenTax* and *Beijing One Pass*, detailed below, reportedly resulted in the inclusion of hidden features that could be used as a backdoor. The first affected versions of this software were released in 2018, but the problem they illustrate persist. Thus, in 2022, French companies established in China reported to ANSSI that the installation of mandatory software led to multiple alerts from their security solutions. However, to date, no information has been published regarding the possible exploitation of accesses enabled by the affected versions of *GoldenTax* and *Beijing One Pass* software. The objectives of these backdoors are therefore unknown, but they could have been used as an entry point for wider compromises within the affected companies.

While the backdoor-like feature might have been included, they might also be the victim of a supply chain attack aimed at compromising their customers via its software. The NotPetya wiper was distributed through a malicious update of the Ukrainian accounting software M.E.Doc, which was widely used among companies operating in the country [1]. A compromise of Vietnam's government certification authority in 2020 also led to the distribution of a compromised version of software used for electronic document signatures [2].

1.1 GoldenSpy

For the digital processing of value-added tax (VAT) returns, the Chinese government has implemented the *Golden Tax* program. Companies operating in China are therefore required to use a *Golden Tax* software to file their VAT returns. The *Golden Tax* software is not, however, distributed directly by the State, but by two companies, Baiwang and Aisino, which integrate it into their products. It seems that the selection of one or the other of these publishers is decided by the companies' banks in China.

On 25 June 2020, Singaporean cybersecurity firm Trustwave published a report [3] revealing that the installation of China's Aisino Intelligent Tax VAT management software led to the deployment of what appears to be a backdoor dubbed "GoldenSpy" by Trustwave.

Two hours after the installation of the VAT management software, codes are downloaded and silently executed. They have persistence mechanisms, communicate with a remote server at a random frequency, and allow arbitrary code to be executed with system administrator privileges without user interaction. The presence of GoldenSpy is not mentioned in the documentation, and **it persists when the Aisino Intelligent Tax software is uninstalled.**

According to Trustwave's analysis, GoldenSpy's distribution would have started in April 2020. But on 28 June 2020, just as Trustwave's article was widely publicised, new code was silently downloaded and executed by the Aisino Intelligent Tax software. This code uninstalls GoldenSpy and erases all traces of its presence on the machine [4]. Finally, from 1st July, a new version of the uninstallation code was sent out, including a change that seems designed to evade detection by the YARA rule published by Trustwave [5].

GoldenSpy is not the first suspicious code distributed alongside software suites associated with *Golden Tax*.

A fourth Trustwave publication [6] details a campaign involving a separate code named "GoldenHelper", active from January 2018 to July 2019. This code would have been integrated into a different software: *Golden Tax Invoicing software (Baiwang Edition)*. However, although the tax information collected by this software is transmitted to Baiwang, *Golden Tax Invoicing software (Baiwang Edition)* was developed by the same subsidiary of Aisino as *Aisino Intelligent Tax*. While the final payload could not be investigated by Trustwave, the analysis of GoldenHelper determined that the payload was downloaded, stored in several directories and executed with system administrator privileges without triggering user alerts (*UAC bypass*). Such mechanisms are not expected features of legitimate

VAT management software, but are common for backdoors.

Trustwave also reports cases of physical workstations supplied for the use of *Golden Tax* on which GoldenHelper code was allegedly present upon delivery [6].

Several French companies operating in the People's Republic of China reported having detected the presence of GoldenSpy in their information systems.

Indicators of compromise have been published in the Trustwave reports mentioned in the bibliography.

1.2 Beijing One Pass

In July 2021, Recorded Future published a report stating that the *Beijing One Pass* software also exhibited features that could be used as a backdoor [7]. This software, distributed by the state-owned Beijing Certificate Authority, enables access to a digital platform to manage employee state benefits.

2 Recommendations

Beyond the situations illustrated by the malicious codes mentioned above, the installation of untrusted software can expose the business assets and the information system (IS) of an entity to numerous threats. In order to limit the impact of these threats, several recommendations should be followed to contain the software in an isolated area dedicated to this use. These recommendations cover the following topics:

- Infrastructure
- Access to the software
- Maintaining security measures
- Detection

In addition, it is recommended to update the network map to facilitate the oversight of the segmented areas and the identification of potential compromise paths.

2.1 Infrastructure

R1

Installing the software in an isolated area

It is recommended to install the software in an isolated area of the entity's IS and preferably with dedicated equipment assigned for this purpose.

R2

Filter network flows "from" and "to" the isolated area to the strict operational need

Network flows to and from the isolated area should be filtered by a firewall to restrict communications to defined IP addresses or ranges, limited to the strict operational needs. It should be noted that flows from the isolated area to the IS of the entity are to be prohibited insofar as possible.

R3

Filtering flows with a firewall device separate from the machine on which the software is installed

A firewall on a machine separate from the one on which the software is installed must be used to filter the flows. The aim is to prevent the software from disabling the firewall in the event of a privilege escalation.

Isolating a zone in an on-premise IS is a task that can be time-consuming and complex if the IS has not been designed to handle this case. When a connection to the internal IS is not necessary, outsourcing (e.g. use of a Cloud service) to an isolated and dedicated area is a possible option when the sensitivity of the data handled allows it. The following recommendations should be observed.

R4

Use a dedicated cloud account to isolate the area of least trust

If an isolated are is set up on the Cloud, it is recommended to use a dedicated account. The objective is to limit the risk of privilege escalation that could affect other resources and to avoid any lateral movement on other instantiated resources unrelated to the software.

The isolated area should not use the common infrastructure services of the entity (such as authentication system, DNS, etc.). The objective is to prevent a compromise or potential denial of service by prohibiting access to the entity's internal IS services.

R5

Apply the principle of least privilege to all services and equipments

The accounts used should have the lowest possible privileges appropriate to each operation and administration of the isolated area. If possible, the software should not be run with an account that has administrator rights. In general, user and administrator accounts should rely on local accounts.

2.2 Access to the software

Access to the software is carried out via direct access to the machine on which the software is installed. When the user needs to interact with the isolated area remotely, it is preferable to use a remote access solution (which can be a Cloud service) with the following precautions.

R6

Disabling clipboard sharing and disk redirection

Clipboard sharing and disk redirection in remote access solutions must be disabled.

When file exchange between the internal IS and the machine hosting the software is required, then a shared storage area can be considered if it is hosted in the isolated area.

R7

Setting up a dedicated and isolated file share

When a storage area between the internal IS and the isolated area is required, it should be set up in the isolated area. A possible alternative is the use of a SaaS service in a Cloud, which makes the storage area de facto separate from the internal IS.

2.3 Maintaining security measures

Although the area is isolated from the entity's IS, it is important to maintain the security of the software and hardware components. The administration of this isolated area, limited to a few of devices, should be done manually, directly on the devices or from a dedicated workstation.

R8

Maintaining security from the Internet

The repositories required to keep the isolated area up to date should not communicate with the entity's IS, but should access updates directly from the Internet. Firewall rules must only allow the network flows necessary for maintenance in secure condition.

When the need to use the software is occasional, additional measures can be implemented to limit the exposure of the isolated area.

R9

Turn off the service when not in use

It is recommended to switch off the service when not in use.

2.4 Detection

Event logging is a prerequisite for implementing a post-incident detection and analysis capability. For more information on good logging practices in environments with multiple levels of trust, see the ANSSI guide on “security recommendations for the architecture of a logging system” [8] (in French).

R10

Enable and configure logging

Logging of system and network components in the isolated area should be enabled and configured to detect and analyse security incidents. This logging is completed with the analysis of events from firewalls located at the edge of the isolated area.

R11

Set up a dedicated collector for logs in the isolated area

It is recommended to centralise the logs via a dedicated collector in the isolated zone and to regularly retrieve these logs from the entity’s internal IS. Thus, only the internal IS initiates connections to the zone of least trust, and not the other way around.

3 Bibliography

[1] ESET. *Analysis of TeleBots' Cunning Backdoor*. July 4, 2017.
URL: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.

[2] ESET. *Operation SignSight: Supply chain Attack against a Certification Authority in Southeast Asia*. December 17, 2020.
URL: https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/.

[3] Trustwave. *The Golden Tax Department and the Emergence of GoldenSpy Malware*. June 25, 2020.
URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/.

[4] Trustwave. *GoldenSpy: Chapter Two – The Uninstaller*. June 30, 2020.
URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/.

[5] Trustwave. *GoldenSpy Chapter 3: New and Improved Uninstaller*. July 2, 2020.
URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-3-new-and-improved-uninstaller/.

[6] Trustwave. *GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software*. July 14, 2020.
URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/.

[7] Recorded Future. "“Beijing One Pass” Employee Benefits Software Exhibits Spyware Characteristics". July 29, 2021.
URL: https://go.recordedfuture.com/hubfs/reports/cta-2021-0729.pdf.

[8] ANSSI. *Publication : Recommandations de sécurité pour l'architecture d'un système de journalisation*. January 28, 2022.
URL: https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/.

Version 2022/en - December 7, 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité