CASE STUDY

The Threat Hunt That Uncovered Novel Malware

What do you do when a required software program, recommended by a trusted member of your supply chain, comes inadvertently bundled with sophisticated malware? A global technology company came into such a predicament after opening operations in China. A routine threat hunt led to the discovery of an entirely novel malware campaign — identified as GoldenSpy by Trustwave SpiderLabs — and was extracted from the client's network before any nefarious activity could occur. Like all other malware, the Trustwave SpiderLabs team reverse engineered the threat, applied indicators of compromise to Trustwave tools and shared this information with the community to protect global organizations from this aggressive threat.

Trustwave®

Client Spotlight

A UK-based technology vendor that does significant business with high-profile clients across the globe.

The Challenge

As a multinational technology software vendor, this client, while launching operations in China, was working with a local Chinese bank. The bank required use of Intelligent Tax software package produced by the Golden Tax Department of Aisino Corporation to pay local taxes. What this client didn't realize was that, bundled inside the tax software package, the malware family — later named GoldenSpy — was also installed. This malware provided complete remote command and control of the system.

Industry Threat

The story of GoldenSpy is not an unusual one. Multinational companies exchange goods, intellectual property, and currency across borders and complex networks at a rapid pace. Today's threat actors are highly motivated by the multi-trillion-dollar industry and target companies of all sizes and types. These sophisticated attackers are breaching networks, and going unnoticed by security technologies. By leveraging a Managed Detection and Response (MDR) solution equipped with continuous threat hunts, this global technology company was able to rely on Trustwave threat hunters and digital forensic experts to protect their environment while they focused on growing their business and satisfying their customers.

The Solution

During a routine threat hunt, several unusual characteristics of the tax software tipped off the Trustwave SpiderLabs team to the threat: an executable that was silently installed two hours after install completion for the tax software, randomized and continuous beaconing to a remote server, and provided system-level access privileges upon install. When the Trustwave SpiderLabs team originally noticed the hidden svm.exe threat, the client assured the threat hunters that the tax software in question was trusted and required by their local Chinese bank. Despite the assumption of legitimacy, however, the Trustwave SpiderLabs team continued to probe.

Upon further digging, the Trustwave team found that it was also set up with triple persistence, meaning the upgrade software service — found to be the malware itself — was built to resist deletion. When downloaded and installed, it created two versions of itself that would monitor one another so that if one was killed, the other one would automatically initiate; furthermore, it was loaded with an ExeProtector module to automatically download and restart the program if both original versions were to be shut down together.

Once the remediation was complete and recommendations were published, the threat actors silently pushed an update in an effort to delete all signs of itself. This uninstaller was designed to evade antivirus software: when updated; a second version was designed to avoid even YARA detection rules. Trustwave experts, however — despite intricately compounded obstacles — were able to successfully shut it down.

Trustwave®