Malware Found in Chinese Tax Software Used by Foreign Tech Firm

Posted on Jun. 29, 2020

By William Hoke

A cybersecurity firm said a global technology company that recently began operating in China was required by its bank there to install tax software containing malware that allowed intruders full access to the company's systems.

Chicago-based Trustwave Holdings Inc. said June 26 that it was hired in April by a global technology vendor with significant government business in Australia, the United Kingdom, and the United States. Trustwave said its client, which had recently opened offices in China, was informed by its bank there that it had to install the Intelligent Tax software program produced by Beijing-based Aisino Corp. for paying local taxes. Trustwave didn't disclose the names of either its client or the bank.

"Basically, it was a wide-open door into the network with system-level privileges, and [was] connected to a command-and-control server completely separate from the tax software's network infrastructure," Brian Hussey, Trustwave's vice president of cyber threat detection and response, said in a report posted to the firm's website. Hussey said the malware is part of a family of malicious software that it calls "GoldenSpy."

Trustwave said that even if the tax software program is uninstalled, the back door into the user's systems remains operational.

Hussey said there is evidence that early variations of the GoldenSpy family date back to 2016. He said his firm is unable to determine the extent to which the malware has been inserted elsewhere, but is aware of a "highly similar incident" that occurred at an unspecified major financial institution. "This could be leveraged against countless companies operating and paying taxes in China, or [it] may be targeted at only a select few organizations with access to vital information," he said.

An email sent by *Tax Notes* to the address indicated on Aisino's website came back as undeliverable.

Paolo Balboni, a professor of privacy, cybersecurity, and IT contract law at Maastricht University in the Netherlands, said an advanced cybersecurity analysis is usually needed to detect malware. "The problem is that not all organizations will run advanced cybersecurity analyses on software before it is installed," he said.

Trustwave said the GoldenSpy back door downloaded automatically two hours after its client installed the tax software package. "The two-hour delay in this process is highly unusual and may be to ensure [that] the covert installation is not identified by the victim," Trustwave said.

Adam Segal, a specialist in emerging technologies and national security and director of the digital and cyberspace policy program at the Council on Foreign Relations, a U.S. think tank, said the length of time it takes for cybersecurity software to detect malware depends on how badly the attackers want to avoid exposure. “For a high-value target, a sophisticated attacker might use what is called a ‘zero-day’ malware that no one has seen before, [which means] defenders have zero days to fix it,” he said. “But zero days are valuable, and there are lots of other known exploits to use, so it is unlikely to be used for an attack like this.”

Segal said the “Stuxnet” cyberattacks on Iran’s nuclear centrifuges in 2009-2010 — which were attributed to the United States and Israel — used five zero days, which he described as remarkable. “So it is not surprising that a cybersecurity [firm] found this, especially since they were looking for back doors,” he said.

Balboni said several cases of governments exploiting back doors in third-party software have been exposed in recent years. “The best way to prevent this is for companies to carry out a thorough cybersecurity risk assessment and relative analyses on any and all software that is to be installed,” he said.

Based on the information publicly available, there is no way to know whether the company that developed the tax software deliberately included the malware or whether it was instead secretly introduced into the software package by some other party, Segal said. “I saw on [U.S. television network] NBC that they were claiming it was a nation-state because it was extremely sophisticated malware," he said. "But one should always be skeptical of claims of sophistication, since cybersecurity firms do not make names for themselves discovering everyday spyware, so everything is almost always described as sophisticated in the press materials.”

Derek Scissors, a resident scholar at the American Enterprise Institute specializing in the Chinese economy, said the attempted cyberattack wasn’t a surprise. “There is no rule of law in China, and risks from illegal action are determined by political position,” he said. “Actors that feel politically safe frequently commit what are [considered] crimes. It's possible this particular activity was supported by Chinese security or intelligence agencies.”

Balboni said it is uncommon in Europe for a bank to require that customers install a specific type of tax software. “But this may be related to compliance with specific . . . Chinese legislation, e.g., regulating the banking and finance sectors or tax-related matters,” he said in an email.

But Scissors said it is not unusual for the Chinese government to require domestic companies to use locally developed software. “The companies then ask partner companies providing them [with] services to use compatible software,” he said. “It seems this can also be for the purposes of cyberintrusion.”