Chinesische Pflichtsoftware mit Malware: Warum „GoldenSpy“ kein Einzelfall ist

Die Macht des Drachens

Rainer Burkardt, Tobias Glemser

Wer in China unternehmerisch tätig ist, kommt um das Installieren regierungsseitig vorgegebener Programme nicht herum – die manchmal mit Malware daherkommen. Betroffen sind auch zahlreiche deutsche Unternehmen.

Ende August 2020 warnten das Bundesamt für Verfassungsschutz (BfV) und das Bundeskriminalamt (BKA) vor „GoldenSpy“, einer Schadsoftware, die Hintertüren für Spionage öffnet. Die Malware wird innerhalb der obligatorischen chinesischen Steuersoftware „Golden Tax“ automatisch nachgeladen. Deutsche Unternehmen, die in China tätig sind, sollten sich daher dringend mit den rechtlichen Anforderungen und den technischen Absicherungsmöglichkeiten auseinandersetzen (zu den rechtlichen Anforderungen siehe auch Artikel „China first“ in *iX* 12/2020, S. 88). Laut Informationen des Deutschen Industrie- und Handelskammertags (DIHK) sowie der Auslandshandelskammer China sind dort rund 5200 deutsche Unternehmen mit eigenen Vertriebsstrukturen und Produktionsstätten aktiv (siehe ix.de/z8wq).

Im Sommer hatte SpiderLabs, das Sicherheitsforschungsteam von Trustwave, einen Untersuchungsbericht veröffentlicht (siehe ix.de/z8wq). Die Forscher berichteten vom Analysefall eines großen Kunden. Dieser verfügte bereits über Büros in den USA, dem Vereinigten Königreich und Australien und eröffnete erstmals neue Büros auf dem chinesischen Festland. Über die Methodik der Untersuchung ist nichts bekannt. Offensichtlich ging es darum, mögliche Schwachpunkte im Firmennetz auszumachen. Dazu hatten die Analysten unter anderem den Netzwerkverkehr mitgeschnitten.

Auffälliger Netzwerkverkehr

Aufgefallen waren dabei ungewöhnliche Verbindungen auf den Ports 9005 und 9006. Bei einer näheren Untersuchung konnten die Analysten eine ausführbare Datei ausmachen, die diese aufbaute. In Zusammenarbeit mit SpiderLabs-Kunden fanden sie heraus, dass die Datei von der Golden-Tax-Software geladen wurde.

Die Software wurde von der Golden-Tax-Abteilung der Firma Aisino entwickelt. Sie ist eine „offizielle“ Software der Steuerbehörden. Chinesische Unternehmen benötigen sie, um staatlich anerkannte Quittungen, sogenannte Fapiao, auszustellen. Die Unternehmen sind verpflichtet, die Fapiao bei jedem Empfang einer Zahlung auszugeben, und der jeweilige Geschäftspartner verlangt sie auch, denn nur so kann er gegenüber dem Finanzamt die Zahlung nachweisen. Bis auf wenige Ausnahmen ist die Nutzung der Golden-Tax-Software Pflicht.

Da in der Vergangenheit ein Computer zu den Steuerbehörden gebracht werden musste, um die Software zu installieren, befand sich die Software meist auf einem separaten Rechner. Seit einigen Jahren kann sie jedoch direkt heruntergeladen werden. Beim Installieren fordert die Golden-Tax-Software den Nutzer auf, den Virenscanner und die Firewall abzuschalten. Überdies funktioniert die Software nur, wenn eine Onlineverbindung besteht, damit sich die erstellten Steuerrechnungen sofort mit dem Server der Steuerbehörden synchronisieren lassen. Damit besteht das Risiko, dass mit der Software die Malware auf einem im Unternehmensnetzwerk integrierten Rechner installiert wird.

Hintertüre huckepack

Grundsätzlich funktioniert die obligatorische Steuersoftware, wie sie soll. Allerdings wird – erst zwei Stunden nach der Installation der eigentlichen Steuersoftware – weitere Software nachgeladen: eine Hintertür. Die Backdoor wird von dem Programm plugin.exe von einer fest codierten IP-Adresse heruntergeladen. Die Datei svminstall.exe wird ausgeführt und installiert svm.exe und eine identische Datei svmm.exe. Die Software hat es in sich: Sie läuft mit den höchsten Privilegien unter Windows im SYSTEM-Kontext. Sie

Gemeinsame Warnmeldung des Bundesamtes für Verfassungsschutz und des Bundeskriminalamtes zu möglicher Cyberspionage mittels der Schadsoftware GOLDENSPY

Bundesamt für Verfassungsschutz

Bundeskriminalamt

21.08.2020

Mögliche Cyberspionage mittels der Schadsoftware GOLDENSPY

Der Cyberabwehr des Bundesamtes für Verfassungsschutz (BfV) sowie dem Bundeskriminalamt (BKA) liegen Erkenntnisse vor, dass deutsche Unternehmen mit Sitz in China möglicherweise mittels der Schadsoftware GOLDENSPY ausgespäht werden. Ziel dieser gemeinsamen Warnmeldung ist es, deutsche Wirtschaftsunternehmen zu sensibilisieren und mit den notwendigen technischen Informationen zu versehen, um eine mögliche Infektion detektieren zu können.

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 July 2020

Alert Number

AC-000129-TT

**Note: this information is being provided by the FBI to assist cyber security specialists protect against the persistent malicious actions of cyber criminals. The information is provided without any guaranty or warranty and is for use at the sole discretion of the recipients.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats.

This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Chinese Government-Mandated Tax Software Contains Malware, Enabling Backdoor Access

Summary

Neben den deutschen Behörden warnte auch das FBI vor einem möglichen Ausspioniertwerden durch GoldenSpy.

sendet und erhält Informationen von zwei Webservices, die auf einer Zieladresse auf den Ports 9005 und 9006 laufen.

Über diese Backdoor lassen sich Windows-Befehle ausführen, Dateien hoch- und herunterladen und beliebige andere Programme ausführen. Die Backdoor hat eine legitime Softwaresignatur der Firma Chenkuo Network Technology. Damit wird die Software im Regelfall problemlos ausgeführt.

GoldenSpy installiert sich an zwei Stellen im Autostart. Stoppt man eine Datei, wird sie durch die identische zweite erneut gestartet. Löscht man eine Datei, wird sie von der anderen nachgeladen und neu installiert. Deinstalliert man die Steuersoftware, bleibt die Backdoor erhalten. svm.exe nimmt keinen Kontakt zur Infrastruktur der Steuersoftware auf, sondern zur Domain ningzhidata[.]com. Nach drei erfolglosen Kontaktversuchen würde die Anfrage zu randomisierten Zeiten wiederholt werden, um nicht zu auffällig im Netzwerkverkehr zu sein. GoldenSpy versucht also mit verschiedenen Methoden, sich selbst zu „schützen“.

Die Domain ningzhidata[.]com wurde am 22. September 2019 registriert. Anhand von Datenanalysen kommen die Analysten zu dem Schluss, dass sie seit April 2020 genutzt wird. Eine genaue Zuschreibung zu einem Urheber (Attribution) war hingegen nicht möglich. Die Einschätzung, ob dies rein technische Gründe hat, sei jedem Leser selbst überlassen. Das Forscherteam von SpiderLabs legt im Bericht großen Wert darauf, dass es nicht mit dem Finger auf irgendeinen Staat zeigen möchte. Die beiden im Bericht aufgeführten Firmen Aisino Corporation und Nanjing Chenkuo Network Technology wurden im Rahmen des Responsible-Disclosure-Prozesses kontaktiert, haben jedoch nicht geantwortet.

Nicht zu viel gestatten

Auf Netzwerkebene erfolgt der Schutz in vielen Unternehmen häufig immer noch ausschließlich gegen Eindringlinge von außen. Selbstverständlich werden von außen nur die Dienste zugelassen, die auch wirklich erreichbar sein sollen. Das

macht sogar jeder Heimrouter seit vielen Jahren in der Standardkonfiguration. Bei den ausgehenden Diensten wird hingegen auch in großen Firmennetzen sehr lax mit den Regeln umgegangen. Ein Großteil der Kommunikation – gerade für Audio- und Videoverbindungen – findet über nicht „vorhersehbare" Ports statt. So wird gerne nach außen sehr viel Kommunikation zugelassen.

Im vorliegenden Fall waren die Ports 9005 und 9006 für das Funktionieren der Backdoor notwendig. Ebenfalls Port 9002, der vom Updater genutzt wurde. Port 8090 könnte in anderen Fällen ebenfalls eine Rolle gespielt haben. Port 33666 ist für das Funktionieren der Steuersoftware Golden Tax notwendig. Nimmt man eine neue Software aus potenziell nicht vertrauenswürdigen Quellen in Betrieb, kann dies zunächst in einem isolierten Netz geschehen, bei dem keine Verbindungen nach außen möglich sind. Anhand der Dokumentation können dann die notwendigen Ports freigeschaltet werden. Parallel geben die Firewallprotokolle Aufschluss, ob noch anderer Verkehr aufgebaut wird.

Eine tiefere Analyse von Datenströmen hilft ebenfalls, verdächtige Verbindungen zu identifizieren. So wurden die HTTP- (nicht etwa HTTPS-)Verbindungen mit ungewöhnlichen User Agents aufgerufen: entweder Accept: */* (was für einen fehlenden Zeilenumbruch im Code spricht) oder Agent0 oder Ryeol HTTP Client Class.

Auf Systemebene hilft Application Whitelisting, also das Ausführen ausschließlich erlaubter Anwendungen, nachhaltig gegen Bedrohungen aller Art. Ransomware wäre kein sonderlich erfolgreiches Geschäftsmodell, würden saubere Whitelists der zugelassenen Programme gepflegt.

Vielfältige IT-Sicherheitsrisiken

Golden Tax ist nicht die einzige Software, die zwangsweise auf chinesischen Computern läuft. So muss man beispielsweise auch für die Einkommenssteuererklärung eine Software auf ein Mobiltelefon herunterladen. Jede nicht selbst ausgesuchte und nicht freiwillig installierte Software bedeutet ein zusätzliches Risiko, da man ihre Funktionen nicht genau kennt.

Hinzu kommt, dass chinesische Mitarbeiter oft zusätzliche Software von privaten Anbietern für die Arbeit benötigen oder aber gerne nutzen möchten. Anders als nichtchinesische Anbieter sind Firmen in China häufig mit dem Staat eng verwoben, wie das GoldenSpy-Beispiel zeigt. Die grundsätzliche Risikolage ist daher höher einzuschätzen.

So ist eine Software zur Meldung bei den Aufsichts- und Sozialversicherungsbehörden Pflicht oder aber die Mitarbeiter nutzen integrierte englische Wörterbücher oder Eingabemethoden für chinesische Schriftzeichen. Auch das allgegenwärtige WeChat wird gerne auf Arbeitsrechnern genutzt. Während offensichtlich „westliche" Software hohe weltweite Verbreitung erfährt und damit auch weltweit von Analysten untersucht wird, verbleibt speziell chinesische Software im chinesischen Markt.

Software wird kaum getestet

Es gibt daher vergleichsweise wenige (bekannte) Analysen chinesischer, lokal in China im Einsatz befindlicher Software. Die Sicherheitsaspekte von Messagingdiensten für den Firmeneinsatz wie MS Teams, Zoom, Wire oder WhatsApp werden gründlich untersucht, wohingegen WeChat in westlichen Analysen nicht auftaucht. Es ist daher davon auszugehen, dass Risiken sowohl durch Qualitätsmängel der ungeprüften Anwendungen bestehen als auch durch bewusst eingebaute Hintertüren.

Tatsächlich sind die oben genannten Maßnahmen nicht nur als Selbstschutz geboten. Es bestehen rechtliche Verpflichtungen, sie umzusetzen. So ist in China jeder Netzwerkbetreiber gesetzlich verpflichtet, ein internes Sicherheitsmanagementsystem (ISMS) einzuführen. Bei der aktuellen rechtlichen Interpretation ist wohl fast jedes Unternehmen als Netzwerkbetreiber zu klassifizieren.

Neben einem ISMS fordern die chinesischen Regelungen insbesondere Maßnahmen, die Sicherheit gewährleisten und dadurch unter anderem verhindern sollen, dass Systeme mit Computerviren infiziert werden oder das Netzwerk durch Malwareangriffe unterwandert wird. Dazu müssen die Unternehmen entsprechende Monitoringsysteme einrichten, um die Netzwerkaktivitäten zu überwachen. Die Protokolle sind mindestens sechs Monate aufzubewahren.

Sollte ein Unternehmen nach einer Warnung der Behörden keine ausreichenden Sicherheitsmaßnahmen treffen, kann es mit bis zu 100 000 RMB (ungefähr 12 000 Euro) pro Verstoß bestraft und die verantwortlichen Personen können mit einer Strafe von bis zu 50 000 RMB (ca. 6000 Euro) pro Verstoß persönlich belangt werden. Das kann auch das Management des Unternehmens treffen.

Sollte sich ein Unternehmen noch nicht mit den in China geltenden rechtlichen Datenschutz- und IT-Sicherheitsanforderungen auseinandergesetzt haben, ist es höchste Zeit. In einem ersten Schritt gilt es zu analysieren, welche Gesetze und Verordnungen anwendbar sind. Wer als deutsches Unternehmen in China ansässig ist oder auch nur mit chinesischen Unternehmen Geschäftsbeziehungen unterhält, ist beispielsweise vom Chinese Cybersecurity Law (siehe Artikel „China first") betroffen. Unabhängig von der rechtlichen und technischen Analyse ist Datensparsamkeit dringend anzuraten. Jeder Datentransfer nach und in China beinhaltet ein gewisses Risiko für einen ungewollten Abfluss von Daten.

Erstaunlich ist, dass eine Software wie GoldenSpy erfolgreich sein kann. Sie ist zwar einerseits sehr hartnäckig programmiert und nicht einfach zu entfernen, andererseits lässt sie sich mit den richtigen Maßnahmen – die sogar von den chinesischen Regularien gefordert werden – im Netzwerk leicht erkennen. Es brauchte aber erst eine gesonderte Analyse, damit GoldenSpy auffiel. Alle technischen Maßnahmen sind seit Langem bekannt und sicherlich keine Raketentechnik. In der Praxis erweisen sie sich leider dennoch als aufwendig bei der Einführung und auch im Betrieb. Solange IT- und Datenschutzbudgets nicht aufgestockt werden, ist es für Angreifer viel zu leicht, mittelprächtige Malware erfolgreich in Unternehmensnetzen zu persistieren. (ur@ix.de)

Quellen

[1] Tobias Haar; China first; Auswirkungen des chinesischen Cybersicherheitsgesetzes; *iX* 12/2020, S. 88

[2] Informationen zu deutschen Unternehmen in China sowie der Analysebericht von SpiderLabs sind über ix.de/z8wq zu finden.

Rainer Burkardt

lebt seit 23 Jahren in China und ist Gründungs- und Managingpartner von Burkardt & Partner Rechtsanwälte, die KMU aus dem D-A-CH-Raum bei ihren Geschäften in China beraten.

Tobias Glemser

ist BSI-zertifizierter Penetrationstester und Geschäftsführer der secuvera GmbH.