SPIEGEL ONLINE

21. November 2011

Behörden-Trojaner

Firma will Späh-Software per iTunes installieren

Von Marcel Rosenbach

Eine Sicherheitslücke in der Musik-Software soll als Bresche dienen: Eine IT-Überwachungsfirma wirbt damit, Späh-Software für Behörden mittels gefälschter iTunes-Updates zu verteilen. Apple hat iTunes inzwischen nachgebessert und eine Sicherheitslücke geschlossen.

Es war eine verschwiegene Gesellschaft, die Ende September mitten in Berlin zu einem internationalen Stelldichein zusammenkam. In einem Hotel der gehobenen Kategorie trafen sich Militärs und Vertreter von Sicherheitsbehörden aus aller Welt, um über die Gefahren der digitalen Welt zu diskutieren: Cyber-Angriffe, elektronische Spionage, organisierte Kriminalität online. Vor allem ging es um die technischen Möglichkeiten, diese Gefahren zu bekämpfen.

Der martialische Titel der Veranstaltung lautete "Cyberwarfare Europe", doch viele der Teilnehmer kamen aus Übersee. Laut Teilnehmerliste waren unter anderem Staatsbedienstete und Industrievertreter aus den Vereinigten Arabischen Emiraten, Malaysia und Indonesien vertreten. Sie hatten bis zu 2700 Euro bezahlt, um während der vier Tage Fachvorträgen von IT-Experten und Militärs zu lauschen - etwa dem eines Rechtsexperten für laufende Operationen des US Cyber Command.

Im Foyer priesen einige Unternehmen den Kongressbesuchern ihre Überwachungstechnik an. Der auffallendste Stand war in blau-schwarz gehalten und warb für ein Produkt namens FinFisher. Die Visitenkarten der jungen Männer am Stand wiesen sie als Vertreter der Firma Gamma International GmbH in München aus. Die Gamma-Vertreter wollten allerdings nur potentiellen Kunden Auskunft über ihre Dienstleistungen geben, die sie mit "Governmental IT- Intrusion" überschreiben - also elektronische Einbruchswerkzeuge für Regierungen und Behörden. An Berichterstattung, sagte der Managing Director aus München dem SPIEGEL, habe man kein Interesse.

iTunes-Update soll Trojaner aufspielen

Anders als ihre italienischen Konkurrenten der Firma Hacking Team, die in Berlin ebenfalls um Neukunden warben, sorgten die Gamma-Leute sogar dafür, dass Journalisten vor dem Vortrag ihres "Managing Directors" den Saal verlassen mussten.

Die Scheu hat offenbar gute Gründe: Gamma scheint sich bei FinFisher dubioser Methoden zu bedienen - das legt Marketing-Material nahe, das dem SPIEGEL vorliegt. Danach funktioniert die angebotene Behörden- und Regierungs-Software ähnlich wie diejenige der Computerkriminellen, die damit bekämpft werden sollen.

Offenbar, so geht aus FinFisher-Werbevideos hervor, nutzt die Software beispielsweise Apples populären Medien-Supermarkt iTunes, um mit gefälschten Software-Updates eine FinFisher-Schnüffel-Software auf die Rechner von Verdächtigen zu laden.

Die Nachfrage nach Überwachungstechnik für das Internet, wie die Gamma International GmbH und Hacking Team sie in Berlin demonstrierten und feilboten, ist in den vergangenen Jahren international erheblich gestiegen. Sicherheitsbehörden sind weltweit mit dem Problem konfrontiert, dass Verdächtige zunehmend verschlüsselt über das Internet kommunizieren. Absprachen, die Verdächtige früher über vergleichsweise einfach abhörbare Festnetztelefone oder Handys trafen, laufen heute zunehmend über verschlüsselte Internet-Telefondienste wie Skype oder verschlüsselte Computer-Chats. Häufig bekommen Behörden nur noch mit, wie Verdächtige sich via Handy zum nächsten verschlüsselten Chat verabreden.

Dieses Problem versprechen Firmen wie die Gamma International GmbH und Hacking Team zu lösen. Allerdings sind derlei gezielte Überwachungsmassnahmen nicht einfach umzusetzen: Das Mithören verschlüsselter Kommunikation ist nur dann möglich, wenn es vor der Verschlüsselung stattfindet. Dazu muss eine Software auf dem Rechner der Verdächtigen installiert werden, die Gespräche, Mails oder Chats unbemerkt ausleitet - unverschlüsselt an die Sicherheitsbehörden. Im Klartext: Die Behörden müssen sich in die Rechner der Verdächtigen hacken.

Elektronisches Einbruchssystem

Wie schwierig und umstritten das rechtlich ist, hat in Deutschland gerade die Diskussion um den "Staatstrojaner" der Firma DigiTask gezeigt - der nach Analysen des Chaos Computer Clubs dazu noch mehr konnte, als das Gesetz erlaubt.

Gamma preist das FinFisher-System als das umfassendste elektronische Einbruchssystem auf dem Markt an. International in die Schlagzeilen geriet das Unternehmen, als im Frühjahr Revolutionäre die Büros des ägyptischen Staatssicherheitsdienstes stürmten und darin detaillierte Angebotsunterlagen für diverse Finfisher-Anwendungen auftauchten. Gamma International UK Limited liess daraufhin über Anwälte erklären, dass man keines der Produkte der FinFisher-Serie an die ägyptische Regierung geliefert habe. Das Unternehmen liefere nur an Regierungen, befolge dabei britisches Recht und alle andere relevante Vorschriften. Darüber hinaus könne das Unternehmen keine Auskunft über "vertrauliche Geschäftsbeziehungen und die Art der Produkte, die es anbietet", geben.

Spätestens seither geraten die verschwiegenen Geschäfte mit den Technologien für das sogenannte legale Abhören (Lawful Interception) zunehmend in die Kritik, denn auch in anderen autoritären Staaten wie Syrien, Libyen und Bahrain tauchten in den vergangenen Monaten modernste westliche Überwachungstechnologien auf. In den Händen von Diktatoren können sie leicht als Repressionsinstrumente gegen die eigene Bevölkerung eingesetzt werden.

Aus dem nun vorliegenden Material gehen erstmals Details über die FinFisher-Überwachungs-Software hervor. So bietet das Unternehmen ausweislich der eigenen Werbevideos gleich eine ganze Palette von Möglichkeiten, um die Späh-Software auf die Rechner von Verdächtigen zu bringen.

"Voller Zugang zum Zieltelefon"

Am einfachsten ist die Sache, wenn der "Agent" physischen Zugang zu dem Rechner der Zielperson hat. Dann reicht es, einen USB-Stick einzustecken ("FinFly USB"). Doch was, wenn das nicht geht? Auch dafür bietet das Unternehmen Lösungen - sogar für mobile Endgeräte. Im Werbevideo zu "FinSpy Mobile" etwa, das als kurzer Animationsfilm gestaltet und mit elektronischer Musik unterlegt ist, bekommt die Zielperson eine gefälschte Nachricht mit dem eingeblendeten Text: "Lieber Blackberry-Nutzer, bitte bringen Sie ihr Blackberry auf den neuesten Stand, indem sie auf den angezeigten Link gehen". Wenn der Nutzer das tut, sei "das Zielsystem mit der FinSpy-Software infiziert", heisst es im Video - und das "Hauptquartier" habe "vollen Zugang zum Zieltelefon".

Ganz ähnlich funktioniert die Infektion ausweislich der eigenen Werbematerialien auch mit "FinFly ISP" - im Werbevideo erhält die Zielperson "ein gefälschtes iTunes Update". Wird das Update angeklickt und heruntergeladen, habe das Hauptquartier vollen Zugriff auf das Zielsystem - so die Hersteller-Werbung.

Blackberry-Hersteller Research in Motion reagierte nicht auf die Frage, was das Unternehmen von den gefälschten Update-Nachrichten hält.

Bei Apple zeigt man sich auf Anfrage wenig erbaut über das Vorgehen der Münchner und zerknirscht über die Schwachstelle, die sie zum Verteilen ihrer Späh-Software nutzen. Offenbar machten sich die Münchner zunutze, dass Apple seine iTunes-Update-Nachrichten bislang nicht in einem sicheren Format verschickte; die FinFisher-Software konnte sich in die Kommunikation einklinken, Hacker nennen so etwas eine "Man in the Middle Attack".

Apple bestätigt, dass Angreifer Updates fälschen konnten

"Die Sicherheit und Privatsphäre unserer Nutzer ist uns extrem wichtig und wir arbeiten aktiv daran, alle Lücken zu finden und zu schliessen die ihre Systeme beeinträchtigen könnten", sagt ein Apple-Unternehmenssprecher auf SPIEGEL-ONLINE-Anfrage. Blackberry-Hersteller Research in Motion hat auf entsprechende Anfragen nicht reagiert. Vertreter der Münchner Gamma International GmbH verwiesen auf Anfrage auf die Limited-Gesellschaft in Grossbritannien. Auf eine Anfrage bei der britischen Gamma International hat das Unternehmen bis zur Veröffentlichung dieses Artikels nicht geantwortet.

Apple hat offenbar bereits reagiert und will die von der FinFisher-Lösung genutzte Schwachstelle dichtmachen. Vor wenigen Tagen brachten die Kalifornier das neue iTunes Update 10.5.1 heraus, es kommt diesmal tatsächlich von Apple selbst, nicht von den Späh-Software-Herstellern. Auf seiner Homepage verrät Apple einen Grund für das Sicherheits-Update. Ein "Man in the Middle Angreifer" habe bislang unter Umständen Software anbieten können, die von Apple zu kommen schien - diese Schwachstelle sei mit der neue iTunes-Version behoben.