IBM Sicherheitsforscher entdecken extrem gefährlichen Banking-Trojaner

IBM Sicherheitsforscher entdecken extrem gefährlichen Banking-Trojaner

Shifu-Trojaner attackiert derzeit Banken aus Japan, Österreich und Deutschland / "Monster-Malware": neues, bisher nicht gekanntes Gefährdungspotential
"Shifu" nennen die Japaner einen Dieb und ein solcher ist der gleichnamige Trojaner, den IBM (NYSE: IBM) Sicherheitsexperten jetzt entdeckt haben. Momentan hat es die Malware, die Code mit kyrillischen Schriftzeichen enthält, auf 14 japanische Banken sowie auf Banking-Plattformen in Europa abgesehen - zwölf Prozent der Angriffsziele liegen in Deutschland und Österreich. Aktiv attackiert hat Shifu aktuell japanische Geldinstitute. Der Trojaner ist die erste von IBM entdeckte Malware, die befallene Systeme mittels einer Antivirus-Software nach anderen Schädlingen scannt und diese aus dem eigenen Revier verbannt. Von Passwörtern, über EC-Karten bis hin zu Bezahlterminals ist wenig vor Shifu sicher - auch Software der Banken nicht.
"Eine Malware, die andere Malware daran hindert, auf den gekaperten Systemen zu wildern, ist uns noch nicht begegnet", sagt Gerd Rademann, Business Unit Executive, IBM Security Systems für Deutschland, Österreich und die Schweiz. "Der jetzt von unseren Sicherheitsexperten entdeckte Shifu-Trojaner bringt seinen eigenen Viren-Scanner mit, um sich die Beute nicht mit anderen Angreifern teilen zu müssen."
Japan und Europa im Visier
Schon seit April 2015 versuchen Cyberkriminelle mit dem Shifu-Trojaner die Systeme von japanischen Banken sowie Banking-Plattformen in Europa zu durchdringen - zwölf Prozent der potenziellen Ziele liegen in Deutschland und Österreich. Aktiv attackiert wurden bisher japanische Geldinstitute. Das haben die Sicherheitsexperten der IBM X-Force herausgefunden und auf ihrem Security Blog gepostet.
Bei Kunden eingesetzte IBM Lösungen zum Schutz vor Malware hatten Angriffe entdeckt, die neben Quellcode von bekannten Banking-Trojanern wie Shiz, Gozi, Zeus oder Didrex auch völlig neue Eigenschaften aufwiesen. Dazu gehört die Fähigkeit von Shifu, die von ihm befallenen Systeme mittels einer Art Anti-Virus-Software vor weiterem Befall zu schützen.
Vom Passwort bis zum Bezahlterminal
Shifu stiehlt auf den befallenen Systemen nach Möglichkeit Zugangsdaten, darunter über einen Key-Logger auch Passwörter, sowie private Zertifikate und Authentifizierungstoken. Diese Daten nutzen die Cyberkriminellen, um sich als die rechtmäßigen Inhaber von Bankkonten auszugeben. Auch der Inhalt von Chipkarten, etwa EC-Karten, ist nicht vor ihnen sicher, sofern diese über einen Kartenleser an ein befallenes Gerät angeschlossen sind. Dazu zählen auch mit dem Netz verbundene Verkaufsterminals, die Shifu befällt, um die darüber laufenden Bezahlinformationen auszulesen.
Mehrere Fliegen mit einer Klappe
Während viele Trojaner Websites von Banken befallen, gibt es wenige, die es auf die zugrunde liegende Banking-Plattform abgesehen haben. Zur letzteren Gruppe zählt auch der Shifu-Trojaner, der gezielt nach den Authentifizierungstoken sucht, die für den externen Zugriff auf diese Plattformen benötigt werden. Mit diesem Vorgehen schlagen die Hacker mehrere Fliegen mit einer Klappe, denn Banking-Applikationen werden meist von mehreren Banken genutzt. Ist eine Plattform gehackt, sind damit die Systeme auch anderer Geldinstitute verwundbar.
Falsche Fährten im Code
Auf der Suche nach dem Ursprung des Shifu-Trojaners sind die IBM Sicherheitsexperten in dessen Skripten auf Kommentare in russischer Sprache gestoßen. Andere Zeichenketten wiederum sind zwar nicht in kyrillischem Schriftcode geschrieben, haben jedoch eine russische Bedeutung, darunter Begriffe wie "Buchhaltung" oder "Kasse". Ob diese Indizien auf einen Ursprung der Hacker aus Russland oder einem anderen russischsprachigen Land schließen lassen, ist nicht geklärt. Möglich ist auch, dass die Cyberkriminellen versuchen, ihre Spuren zu verwischen.
Der komplette IBM Security Blog Post zu Shifu: http://ibm.co/1VsImAO

Kontaktinformation
Hans-J Rehm
IBM Kommunikation
07034-151887
0171-5566940
hansrehm@de.ibm.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=596057" width="1" height="1">

Pressekontakt

IBM Deutschland

71137 Ehningen

Firmenkontakt

IBM Deutschland

71137 Ehningen

IBM gehört mit einem Umsatz von 95,8 Milliarden US-Dollar im Jahr 2009 zu den weltweit größten Anbietern im Bereich Informationstechnologie (Hardware, Software und Services) und B2B-Lösungen. Das Unternehmen beschäftigt derzeit 399.400 Mitarbeiter und ist in über 170 Ländern aktiv.Die IBM in Deutschland mit Hauptsitz bei Stuttgart ist die größte Ländergesellschaft in Europa.Mehr Informationen über IBM unter: ibm.com/de/ibm/unternehmen/index.htmlIBM ist heute das einzige Unternehmen in der IT-Branche, das seinen Kunden die komplette Produktpalette an fortschrittlicher Informationstechnologie anbietet: Von der Hardware, Software über Dienstleistungen und komplexen Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten.