CSI: INTERNET

Spion in der Post

Diesmal sind die CHIP-Experten einem Angreifer auf der Spur, der nicht mal eine Software-Lücke brauchte. Der Hacker legte sein Opfer ganz anders rein. *Von Valentin Pletzer*

Als der Virenscanner Alarm schlug, war es bereits zu spät. Der Zeitstempel des gemeldeten Trojaners zeigt, dass das Tool schon seit mehr als zwei Wochen seine bösartige Aufgabe erfüllt hat. Wie es auf seinen PC gekommen ist und warum der Scanner den Eindringling jetzt erst meldet, kann sich Vermögensberater Rainer B. nicht erklären. „Meine Security-Suite ist auf dem neuesten Stand", sagt er. „Und so naiv, dass ich jeden E-Mail-Anhang öffne, bin ich auch nicht."

DER EXPERTE

Steve Stasiukonis
ist Geschäftsführer des
Secure Network Te
Sein Team findet Daten
in großen Unternehmen

Höhe des Schadens – ungewiss. Vor allem, weil der Virenscanner keine genaueren Angaben über die Art der Schad-Software macht. Deshalb bittet Herr B. das Forensik-Team von CHIP, der Sache nachzugehen. Nach dem Vorbild des CSI-Teams („Crime Scene Investigation") suchen wir den Tatort auf: das Büro des Vermögensberaters.

Gleich zu Beginn ein Rückschlag: Auf dem Laptop wird immer noch gearbeitet. Unter Umständen wurden dadurch wichtige Spuren verwischt, der Hacker könnte aufschlussreiche Log-Files und temporäre Dateien gelöscht haben. Um weitere Veränderungen zu vermeiden, ziehen wir zuerst ein Image der Festplatte. Dann analysieren wir den Trojaner, den Herr B. glücklicherweise nicht gelöscht hat, sondern vom Virenscanner in Quarantäne verschieben ließ.

Schnell stellen wir fest, dass es sich bei dem Trojaner um eine modifizierte Version von »BackOrifice 2000« handelt. Ein alter Bekannter, der bereits 1998 erschienen ist, aber bis heute nichts an Attraktivität für Hacker verloren hat. Durch den Quellcode und das Baukastenprinzip, mit Plugins wie dem Remote Desktop und dem Password Extractor, können die Internet-Gangster diese Malware ihren Bedürfnissen anpassen. In unserem Fall reduzierte der Hacker das Tool auf das Nötigste – und schrieb sogar den Quellcode teilweise um. Dadurch änderte sich die Signatur des Schädlings, der Angreifer konnte die Erkennung des Virenkillers zwei Wochen lang austricksen. Dass das Anti-Virus-Programm überhaupt angeschlagen hat, verdankt Herr B. einem Zufall: Eine andere Variante des Trojaners, die inzwischen entdeckt wurde, ähnelt dem Eindringling so sehr, dass die Signatur passte.

Um zu bestimmen, worauf der Hacker aus war, müssen wir herausfinden, welche Funktionen der Trojaner ausführt. Das Ergebnis: Das Tool nimmt nur einen einzigen Befehl an. Aber der hat es in sich. Auf Kommando des Hackers schickt ihm der Trojaner alle Dokumente, die sich auf dem befallenen PC befinden. Für Opfer Rainer B. ein Horrorszenario, hat er doch sensible Kundendaten gespeichert. Ob und welche Dateien tatsächlich geklaut wurden, lässt sich aufgrund der verwischten Spuren nicht mehr nachvollziehen. Herr B. muss davon ausgehen, dass alle seine Kunden betroffen sind.

Tarnen und Täuschen

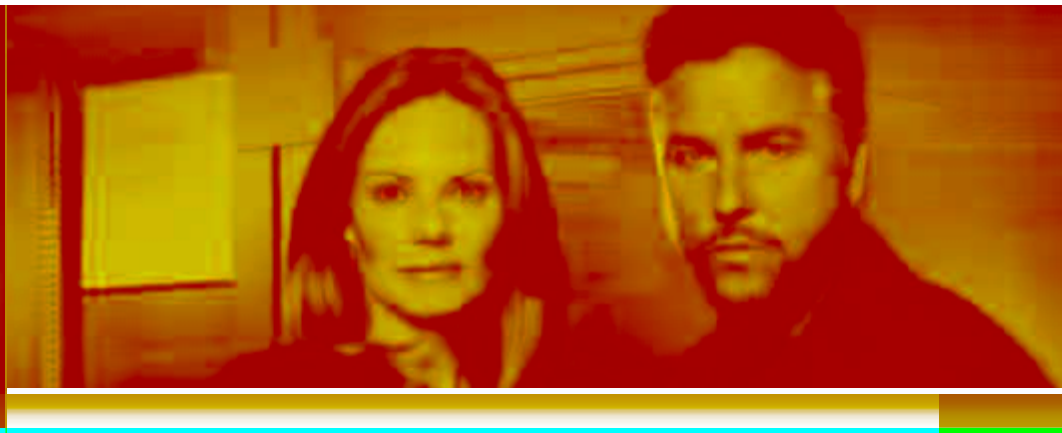
Um noch mehr über das Motiv des Hackers herauszubekommen, suchen wir nach der Quelle des Trojaners. Dafür nehmen wir zuerst den Browser unter die Lupe. Da fast jeder Angriff entweder über Webseiten oder E-Mails kommt, versprechen sich die Forensiker hier sehr viel. Leider eine Sackgasse: Ausgerechnet ein Sicherheits-Tool hat den Cache, den Verlauf und die Cookies des Browsers beim Schließen automatisch gelöscht.

Deshalb nehmen wir uns als Nächstes die Software vor, die Herr B. auf seinem Rechner installiert hat. Er selbst ist überzeugt, nichts Gefährliches installiert zu haben. „Ich habe sogar kürzlich erst eine neue Anti-Spyware-Software installiert, um Schädlinge fernzuhalten", sagt er – und lässt unser CSI-Team sofort aufhorchen. Denn wir kennen weder den Produkt- noch den Firmennamen! Also nehmen wir das Programm genauer unter die Lupe. Und werden fündig: Obwohl es sich dem Anschein nach um eine ganz gewöhnliche Sicherheitssoftware handelt, wird uns sofort klar: Rainer B. ist auf eine „Rogue-Anti-Spyware" reingefallen, eine Spyware, die sich ganz frech als Schädlingskiller tarnt.

Foto: Vox aus „CSI", N. Schäffler; K. Satzinger

Neue CHIP-Serie

In der US-Krimireihe „CSI" klären Forensiker Verbrechen mit wissenschaftlichen Methoden auf. CHIP nimmt „CSI" zum Vorbild für eine neue Serie, die zeigt, wie Profi-Ermittler und Spezialisten die rasant wachsende Computerkriminalität bekämpfen.



Die Angst vor Spyware hat Herrn B. direkt in die Falle des Hackers getrieben – wie viele andere auch. Natürlich gewähren die Opfer der vermeintlichen Sicherheitssoftware Administratorrechte, genau darauf sind die Hacker aus. Ihr trojanisches Pferd erhält alle Systemrechte.

Bleibt noch die Frage, wie die Software überhaupt auf den Rechner von Herrn B. gekommen ist. Zu unserer Überraschung zieht er einen USB-Stick aus der Schublade. „Da war sie drauf. Ein Werbegeschenk, das mir die Sicherheitsfirma geschickt hat." Das ist aber noch nicht alles, denn er fügt hinzu: „Ich hatte sogar mit jemandem telefoniert."

Nun wird die Sache richtig brisant: Herr B. ist nicht das Opfer eines breit gestreuten Angriffs auf beliebige Internet-Nutzer geworden. Er wurde gezielt attackiert! Unser Team will nun herausfinden, von wem. Wir versuchen unser Glück mit dem Trojaner und installieren ihn auf einem Testrechner. Kaum startet das Programm, lädt es ein Update aus dem Internet – so als würde es ein Signatur-Update für die Spyware-Suche installieren. Doch stattdessen lädt es den Trojaner.

Der Trick mit dem USB-Stick

Der Trick des Hackers ist keineswegs neu. Schon vor einiger Zeit demonstrierte der New Yorker Sicherheitsexperte Steve Stasiukonis von „Secure Network Technologies", dass die größte Schwachstelle der Mensch und seine Neugier ist. Eine Bank hatte seine Firma beauftragt einen gründlichen Sicherheitscheck durchzuführen und auch „Social Engineering" nicht auszulassen. Üblicherweise bedeutet das für den Sicherheitsexperten, mit der Sekretärin zu flirten oder in der Raucherecke zu lauschen, um so eine Schwachstelle im System auszumachen oder ein Passwort zu ergattern.

Doch ein einfacher Trick funktioniert noch besser: Steve Stasiukonis ließ USB-Sticks auf dem Firmengelände auslegen – ein speziell dafür programmierter Trojaner inklusive. Mitarbeiter fanden sie und schlossen sie neugierig an die Firmenrechner an. Von 20 ausgelegten Fallen schnappten 15 zu. Stasiukonis erhielt sowohl Logins und Passwörter als auch alle Informationen über das jeweilige befallene System.

Datenklau ohne Beweise

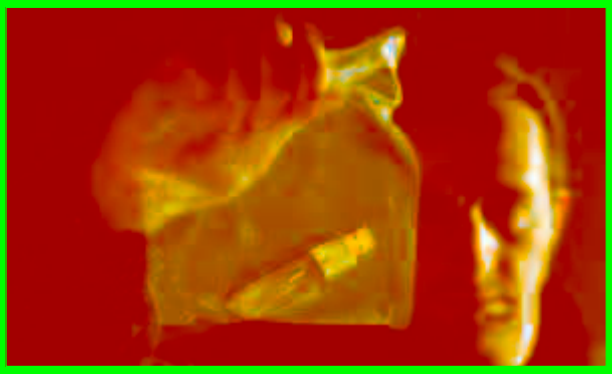
So einfach der Angriff ist, so schwer ist es im Fall von Herrn B. nachzuvollziehen, wer ihn ausgeheckt hat. Da der Virenscanner den Trojaner deaktiviert hat, ist der Hacker vorgewarnt, konnte seine Spur verwischen. Wahrscheinlich besitzt er jetzt Kopien aller vertraulichen Dokumente seines Opfers. Da es sich aller Wahrscheinlichkeit nach um Auftragsspionage mit hoher krimineller Energie handelte, ist das Desaster für Herrn B. doppelt groß. Seine Spur kann auch unser Forensik-Team nicht aufnehmen. Herrn B. bleibt nur die Lehre, nie wieder einem Werbegeschenk trauen.

valentin.pletzer@chip.de

MEHR INFOS

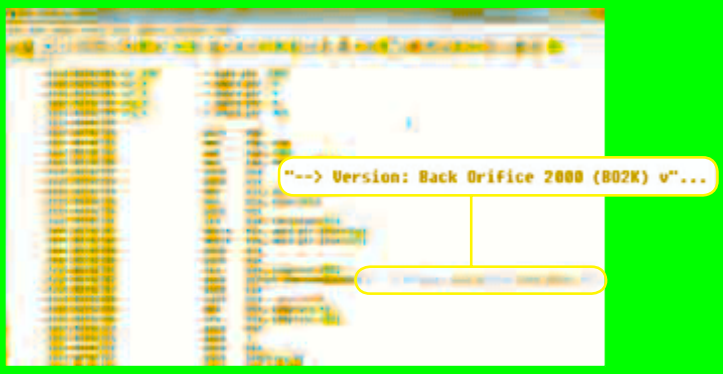
Die Kunst der Täuschung ISBN 3826615697, ca. 20 Euro: Hacker Kevin Mitnick zeigt in diesem Buch, wie man auch ohne Software Rechner knacken und in Netzwerke eindringen kann.

Beweis 1



GEFÄHRLICHE HARDWARE **Ein Stick in hübscher Verpackung lässt alle Vorsicht vergessen. Doch in dem vermeintlichen Werbegeschenk schlummert in diesem Fall bösartige Spyware.**

Beweis 2



ALTER BEKANNTER **Das Analyse-Tool Disassembler IDA enttarnt die Malware als alten Bekannten. Der Trojaner enthält sogar noch den Originaltext „Back Orifice 2000".**