CSI: INTERNET

Folge 6

Rosenkrieg am PC

Die Worte Stalking und Spyware fallen selten in ein und demselben Satz. Der neue Fall unseres Computerkriminalisten-Teams verbindet jedoch beides. *Von Valentin Pletzer*

Es ist gerade so, als würde er noch einen Schlüssel zu meiner Wohnung besitzen und meine E-Mails lesen“, sagt Daniela R. verzweifelt. Vor etwa einem Monat hat sich die 26-Jährige von ihrem Freund, einem 34-jährigen Computerspezialisten, getrennt. Kurz darauf verwandelte er sich in einen Stalker: Immer wieder meldet er sich und macht ihr Vorwürfe zu allem, was sie aktuell getan oder gesagt hat, taucht sogar überraschend bei Treffen mit ihren Freundinnen auf. Dabei dürfte er doch von allem gar nichts wissen, die Termine etwa hatte die junge Frau nur per E-Mail mit ihren Freundinnen ausgemacht. Inzwischen ist ein wahrer Rosenkrieg entbrannt und Daniela R. seelisch am Ende. Schon mehrfach hat die junge Frau alle Passwörter an ihrem PC gewechselt, hat sich aktuelle Virenscanner und Anti-Spyware gekauft. Doch der Terror geht weiter.

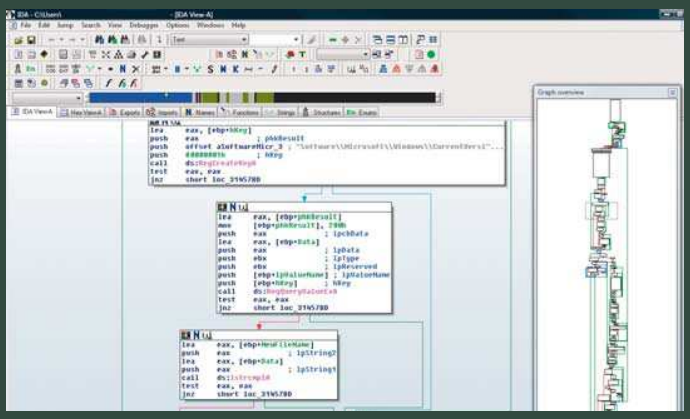
Als sie sich an das CHIP-Team wendet, machen wir uns gleich an die Arbeit. Zuerst checken wir den PC. Ein typisches System: Windows XP als Betriebssystem. Outlook Express, Internet Explorer und ein Instant Messenger sind die meistgenutzten Programme. Hinzu kommt gelegentlich Word 2003. Der Virenscanner läuft im Hintergrund. Er wird automatisch über das Internet aktualisiert, also scheint der Computer ausreichend vor Spyware, Trojanern und Viren geschützt. Deshalb überprüfen wir zunächst das Netzwerk: Der Router ist aber in Ordnung und weist keinerlei Anomalien in der Konfiguration auf. Da Rechner und Router per Kabel verbunden sind, scheidet ein Abhören per W-LAN auch aus. Noch scheint der Vorwurf von Daniela R. gegen ihren Ex-Freund unhaltbar.

Wir nehmen „Fingerabdrücke“

Zurück zum Rechner. Hier nehmen wir als erstes die aktiven Prozesse unter die Lupe. Ein einfaches Forensik-Tool, der Process Explorer von Sysinternals, hilft dem CSI-Team, sämtliche aktiven Prozesse zu erfassen. Wir können die Checksummen jedes aktiven Programmes nehmen und mit einer umfangreichen Datenbank vergleichen. Die Datenbank enthält für alle bekannten Dateien und Programme einen jeweils einzigartigen Wert – so wie ein Fingerabdruck. Angefangen von den Systemdateien bis hin zu Anwendungen wie Nero oder die T-Online-Software. Prozesse, deren Checksummen nicht in der Datenbank enthalten sind, kommen auf eine gesonderte Liste. Das passiert zum Beispiel, wenn ein Programm entweder völlig unbekannt ist oder aber eine bekannte Datei modifiziert wurde.

Danach würde normalerweise der mühsamere Teil kommen. Denn bisher musste man verdächtige Prozesse einzeln von Hand analysieren. Doch wir nutzen den Prototyp eines neuen Analysetools, dessen Heuristik ähnlich wie die eines Anti-Viren-Scanners arbeitet. Spezielle Algorithmen analysieren Programmabläufe und können Verwandtschaften selbst dann erkennen, wenn der Hacker versucht, sie zu verschleiern. Und natürlich versuchen die Profis der

Sezierter Trojaner



SPEZIAL-TOOLS **Programme wie der Disassembler IDA helfen dem Team bei der detaillierten Analyse des Trojaners und seines Inhalts.**

Fotos: Vox aus „CSI“; CHIPimages

CHIP-Serie

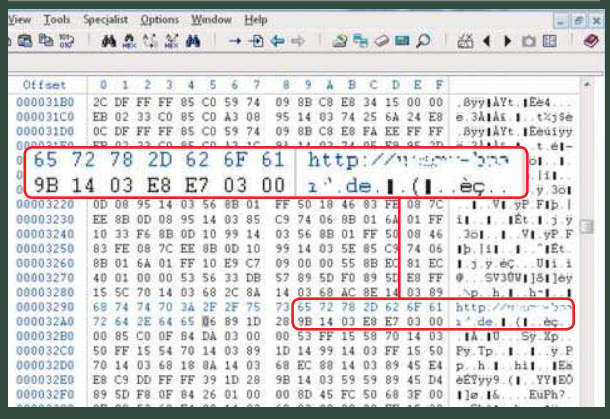
In der US-Krimireihe CSI (in Deutschland bei RTL, VOX und 13th Street zu sehen) klären Forensiker Verbrechen mit wissenschaftlichen Methoden auf. CHIP nimmt CSI zum Vorbild für eine Serie, die zeigt, wie Profi-Ermittler die ausufernde Computer-kriminalität bekämpfen.

Internet-Mafia alles, um die Virenscanner auszutricksen. So ist es üblich, dass Hacker ihre Angriffsprogramme solange verändern und modifizieren, bis sie der Virenscanner nicht mehr erkennt. Das können kleinere Veränderungen am Programmcode sein oder aber einfach das Packen der Dateien mit einem unbekannten Algorithmus. Die grundsätzliche Arbeitsweise, die Reihenfolge der einzelnen Funktionen, bleibt jedoch dieselbe wie beim ursprünglichen Spionage-Tool – und genau das entlarvt unser Spezialprogramm.

Und tatsächlich: Das Analyse-Programm schlägt an. Es zeigt, dass ein angebliches Instant-Messenger-Plugin etwas ganz anderes ist, als es vorgibt zu sein. Es weist deutliche Ähnlichkeiten mit einem Baukasten-Trojaner auf, dessen Quellcode für jedermann frei zugänglich im Internet kursiert. Wir müssen davon ausgehen, dass jemand das Pseudo-Plugin bewusst auf dem Rechner installiert hat. Wenn Daniela R. Recht mit ihrer Vermutung hat, wohl ihr Ex-Freund, kurz bevor die Beziehung zu Ende ging. Da der Instant Messenger bei jedem Systemstart automatisch startet, konnte auch der getarnte Trojaner immer laufen, ohne Aufsehen zu erregen.

Das Forensik-Team beginnt nun, den Trojaner im Detail zu untersuchen. Mit dem professionellen Disassembler IDA von DataRescue, wird das Programm in Maschinencode (Assembler) umgewandelt und durchschaubar dargestellt. Für Profis liest sich der Trojanercode dann fast so einfach wie der Originalquelltext. Sie können die Funktionsweise des Eindringlings ganz genau bestimmen. So überraschend der Fund auch ist, der Trojaner selbst ist wenig innovativ. Wir entdecken typische Elemente, wie etwa Keylogger, Screenshot-Funktion und weitere Spyware-Funktionen. Das zeigt: Der Urheber hat sich reichlich aus vorhandenen Baukästen bedient.

Der Beweis



FUNDSTÜCK Eine Stelle im Code des Trojaners weist dem CSI-Team den direkten Weg zum Angreifer.

Die Spur des Spions

Und dann finden wir die entscheidende Spur: Im Programmtext versteckt sich ein Domainname! Eigentlich wird der größte Teil der ferngesteuerten Trojaner und Bots über einen IRC-Server kontrolliert. Dort melden sich die Bots wie Chatprogramme an und der Hacker gibt seine Kommandos. Aber die Heuristik vieler Virenscanner erkennt die IRC-Kommandos. Das, so scheint es, wollte unser Hacker unter allen Umständen vermeiden. Doch dass er nun ausgerechnet einen Webserver mit de-Domain als Kommandozentrale ausgewählt hat, war sein entscheidender Fehler. Eine einfache Whois-Anfrage bei DENIC (**www.nic.de**), und wir wissen, wer der Angreifer ist: Tatsächlich der Ex-Freund unserer Auftraggeberin! Wir entfernen den Trojaner und empfehlen Daniela R., mit den gefunden Fakten zur Polizei zu gehen. Dafür geben wir ihr unsere lückenlose Dokumentation in die Hand. Mit diesen Beweisen dürfte es ein Leichtes sein, den Spion rechtlich haftbar zu machen.

DER EXPERTE

Eugene Kaspersky (41) ist Anti-Viren-Spezialist und Gründer der Kaspersky Labs. Er beobachtet immer mehr gezielte Hacker-Angriffe auf Einzelpersonen und Firmen.

Schutz vor erneuten Angriffen

Während wir unsere Ausrüstung zusammenpacken, fragt uns Daniela R., wie sie sich in Zukunft gegen solche Angriffe schützen kann. Wir können ihr nur raten, vorsichtig mit unbekannten Dateien und E-Mails umzugehen und regelmäßig Updates zu laden – direkten Zugriff auf den PC hat ihr Ex ja nicht mehr. Jede andere Möglichkeit würde die Arbeit am PC für Laien stark verkomplizieren. „Einen perfekten Schutz gibt es nicht“, sagt auch Anti-Viren-Experte Eugene Kaspersky, den wir nach seiner Meinung fragen. „Der Trend geht zu immer gezielteren Angriffen. Und je besser der Angreifer sich vorbereitet, umso größer ist auch seine Erfolgschance. Ein Problem, das aber vor allem Firmen haben.“ *valentin.pletzer@chip.de*

MEHR INFOS

www.viruslist.com/weblog: Der Experten-Blog von Kaspersky erzählt vom ganz alltäglichen Malware-Wahnsinn.