Vorgebliche Antiviren-Seite zockt Anwender ab

Anwendern wird mit geschickt gestalteten Werbebannern die Infektion des eigenen PC vorgetäuscht. Ein Klick darauf führt zu einem kostenpflichtigem Abo von eigentlich kostenlosen Versionen.

die News-Meldung vom 18.02.2009

G Data, Hersteller von Anvirensoftware, warnt vor einer aktuellen Kampagne eines unseriösen Security-Portals. Die Betreiber versuchen, Anwender in eine Abofalle zu locken: Besuchern der Streaming-Seite kino.to wird mit geschickt gestalteten Werbebannern die Infektion des eigenen PC etwa mit dem Wurm Blaster vorgetäuscht.

Ein Klick auf die gefälschte Sicherheitswarnung führt anschließend auf eine Webseite, die den Opfern nach erfolgter Registrierung eine kostenlose Vollversion von G Data AntiVirus zur Desinfektion des PC verspricht. Angeboten werden dann jedoch nur frei zugängliche Testversionen unterschiedlicher Antiviren-Hersteller, darunter auch G Datas Produkt. Wenn das Opfer dort nicht aufpasst, hat es nach der Registrierung ungewollt ein Zweijahresabo zum Preis von 316 Euro abgeschlossen.

G Data weist darauf hin, dass es in keinerlei geschäftlicher Verbindung zum Anbieter der Webseite steht und rechtliche Schritte gegen die in Dubai registrierte Firma prüft. Bislang haben derartige Anbieter mit einer vorgetäuschten Infektion eher versucht, mehr oder minder nutzlose Virenscanner, sogenannte Scareware, zu verkaufen. Wie man Schreck-Ware erkennt, sich davor schützt und sie im Fall der Fälle beseitigt, erklärt der Artikel "Scharlatane und Hochstapler" auf heise Security.

Gegen die neue Masche hilft nur Ruhe bewahren. So empfiehlt Nico Reiners vom Institut für Rechtsinformatik der Leibniz Universität Hannover Betroffenen, auf keinen Fall zu zahlen und gelassen zu bleiben, auch wenn Inkasso-Büros eingeschaltet werden. Selbst von der Androhung eines Schufa-Eintrags oder einer Klage solle man sich nicht beeindrucken lassen. "Die Abofallen-Betreiber haben kein Interesse an einer Klage, da sie Angst haben zu verlieren, und ein Schufa-Eintrag ist auch nicht ohne Weiteres möglich," erklärte der Jurist.

(c't)

"Scharlatane und Hochstapler – Zweifelhafte Antiviren-Produkte"

der Bericht von Daniel Bachfeld vom 25.10.2008

Mit gefälschten Meldungen über Infektionen des PCs erschrecken Betrüger arglose Anwender und versuchen, sie so zum Kauf dubioser Antiviren-Produkte ohne Funktion zu bewegen. Nicht selten kommt im Gefolge eines solchen Programms noch

ein Trojaner. heise Security zeigt, wie man solche Angriffe erkennt und abwehrt.

Die zweifelhaften Produkte kommen meist in prächtigen Gewändern und haben klangvolle Namen wie AntiMalware Guard, AntiSpyware XP 2008, WinDefender 2008, Total Secure 2009, WinAntivirus 2008 und XP Antispyware 2009. Die Nähe zu den Namen bereits etablierter Schutzprogramme soll die Opfer überzeugen, es handele sich um reguläre Produkte.

Die Verbreitung erfolgt über spezielle Seiten, die dem Anwender typischerweise einen Virenscan der Festplatte vorgaukeln, der dramatische Funde ergibt. Dabei ist die Oberfläche des vermeintlichen Scanners im Browser der Windows-Oberfläche so gut nachempfunden, dass unbedarfte Anwender selten Verdacht schöpfen, dass es nicht mit rechten Dingen zugehen könnte. So lügt etwa der vorgetäuschte Scan von AntiSpyware Expert dem Anwender vor, dass sein Windows-PC mit diversen Schädlingen – darunter Sobig, Sdbot und Mimail – infiziert sei, obwohl das System vollkommen sauber ist. Selbst wenn man die Seiten mit einem Linux-Rechner ansurft, erhält man die gleichen Meldungen.

Zur Abhilfe empfehlen die Seiten dann einen kostenlosen Virenscanner – und bieten diesen auch gleich zum Download an. Nach der Installation soll man zur Freischaltung freilich eine Lizenz erwerben. Andernfalls macht die Software regelmäßig mit nervenden Warndialogen darauf aufmerksam, dass der Rechner infiziert sei. Da sich die Software oft auch nicht auf normalem Wege über die Systemsteuerung deinstallieren lässt, geben einige Anwender schließlich nach und bezahlen den Kaufpreis für das aggressiv werbende Produkt.

Die immer häufigeren Leseranfragen an c't und heise Security belegen, dass immer wieder Anwender auf solche Täuschungen hereinfallen. Der Antiviren-Hersteller Panda bestätigt, dass die Zahl dieser als Scare-Ware bezeichneten Betrugsprogramme derzeit rasant zunimmt und bereits einen beträchtlichen Teil der täglich neu erstellten Signaturen ausmache. Der deutsche Hersteller G Data verzeichnet ebenfalls einen enormen Anstieg der Schreck-Ware ohne echte Schutzfunktion in den letzten Wochen und Monaten. Das sei ein eindeutiger Beleg, dass es sich für die Täter um ein lukratives Geschäft handle. Während man im September 2007 knapp 30 neue Signaturen für dubiose Programme erstellte, waren es im September 2008 fast 2100 – also rund siebzig Mal mehr. Aufgrund der zunehmenden Attacken hat kürzlich Microsoft in den USA sogar eine Klage gegen Hersteller gefälschter Antivirenprodukte angestrengt.

Trojaner inklusive

Längst nicht alle dieser dubiosen Antiviren-Programme sind harmlos. Nicht selten sperrt das Programm nach der Installation etwa die Webseiten von seriösen Anbietern von Antivirenprodukten. Immer öfter schleicht sich Schreck-Ware auch über Sicherheitslücken im Browser per Drive-by-Download in den Rechner und nervt den Anwender anschließend mit Meldungen über den angeblich schlechten Sicherheitsstatus des Systems.

Und war bislang das Geschäftsmodell zumeist nur der gewinnbringende Verkauf der wertlosen Software, infizieren solche Programme immer öfter den PC mit echten Schädlingen, um ihn in einen Bot zu verwandeln und anschließend darüber Spam zu versenden. Typische Vertreter dieser Schädlinge sind die Mitglieder der Familie "Trojan-Downloader.FraudLoad", bei denen die AV-Hersteller bereits Signaturen mit vierstelligem Suffix (.vcca und so weiter) vergeben. Es ist auch nicht auszuschließen, dass die Betrüger es auch auf die Kreditkartendaten beim Online-Kauf abgesehen haben.

Abhilfe

Die zahmen Vertreter der Gattung wird man vergleichsweise einfach los. So weisen etwa neuere Versionen des AntiMalware Guard und von An-

tispyware Express mittlerweile sogar Uninstall-Funktionen auf. Vermutlich wollen die Anbieter damit ihren wertlosen Programmen einen seriöseren Anstrich geben und eine Aufnahme in die Virensignaturen der AV-Hersteller vermeiden. Bietet die Scare-Ware keine solche Option, muss man sie wohl oder übel manuell entfernen. Dazu genügt es oft bereits, die dazugehörigen Prozesse zu beenden und die Dateien sowie die vom Programm vorgenommen Registry-Einträge zu löschen. Einschlägige Foren zum Entfernen von Spyware und sonstigen Programmen enthalten oft aktuelle Beschreibungen zu gerade grassierender Spyware und gefälschten Antiviren-Produkten.

Leider lesen die Entwickler dieser Programme diese Anleitungen ebenfalls und ändern die Installationspfade und Namen der Dateien, damit sie nicht mehr ohne weiteres funktionieren. Im schlimmsten Fall muss man also selbst erkunden, welche Prozesse und Dateien für die nervigen Meldungen verantwortlich sind. Oft reicht dazu bereits der Task Manager von Windows. Mehr Informationen, um die verantwortlichen Programme ausfindig zu machen, liefert das Tool Process Explorer von Microsoft [2]. Das Tool Autoruns spürt zudem die Start-Einträge in der Registry auf, mit dem sich die Schreck-Ware nach dem Booten aktiviert. Mit Autoruns lassen sich die Einträge auch deaktivieren, ohne mit Regedit in der Registry rumfummeln zu müssen [3]..

Schutz

Den besten Schutz vor nachgemachten Antivirenprogrammen bietet ein gesundes Maß an Misstrauen gegenüber unaufgefordert angebotener Software auf zufällig angesurften Webseiten. Wie solche Seiten und die angebotenen Produkte aussehen und arbeiten, illustriert die Bilderstrecke am Anfang des Artikels.

Im Zweifel sollte man den Programm-Download von unbekannten Webseiten einfach ablehnen und interessante Software lieber von größeren Software-Portalen beziehen, da es dort in der Regel auch ein Anwenderfeedback gibt. Dies gilt umso mehr, da bei einem Kurztest von heise Security längst nicht alle regulären Virenscanner die ScareWare-Produkte als Bedrohung erkannten. Vor echter Schadsoftware wie Trojan-Downloader.FraudLoad warnen sie nur, wenn sie schon die Signatur für die jeweils aktuelle Variante aufweisen. Problematischer sind oft die Programme in der Grauzone, die wenn überhaupt als Fälschung oder Risk-Ware gemeldet werden.

Gegen ungewollte Drive-by-Downloads via Browser-Lücken hilft es, immer die aktuelle Version einzusetzen und darüber hinaus auch alle eingesetzten Plug-ins wie den Flash Player und Adobe Reader auf dem neuesten Stand zu halten.

(dab)