Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was ist Schadsoftware?
- Hintergründe
- Schützen Sie sich

Schadsoftware

Überblick

Sie haben sicher bereits Begriffe wie Viren, Würmer, Trojaner oder Rootkits gehört, wenn über Cyber-Sicherheit gesprochen wird. Diese Begriffe beschreiben Arten von Programmen, die von Cyberkriminellen verwendet werden um Computer und mobile Geräte zu infizieren und zu übernehmen. Heutzutage werden diese verschiedenen Begriffe meist einfach als „Schadsoftware“ bzw. englisch „Malware“ bezeichnet. In diesem Newsletter werden wir erklären, was Malware ist, wer es entwickelt und warum, und was Sie tun können um sich davor zu schützen.

Gastautor

Lenny Zeltser konzentriert sich auf die Sicherung des IT Betriebs bei NCR Corp und lehrt Malware-Bekämpfung am SANS Institute. Lenny ist aktiv auf Twitter als **@lennyzeltser** und schreibt einen Sicherheitsblog unter **blog.zeltser.com**.

Was ist Malware

Einfach ausgedrückt bezeichnet man als Malware Computerprogramme, die dazu ausgelegt sind schädliche Aktionen durchzuführen. Das deutsche „Schadsoftware“ drückt das ebenso aus wie der englische Begriff „Malware“, eine Kombination aus den Worten „boshaft“ und „Software“. Das endgültige Ziel der meisten Cyber-Kriminellen ist es, Malware auf Ihrem Computer oder mobilen Geräten zu installieren. Einmal installiert, können diese Angreifer potenziell die vollständige Kontrolle über die Geräte erlangen. Vielfach ist die falsche Vorstellung verbreitet, dass Malware nur ein Problem für Windows-Computer ist. Während Windows aufgrund seiner weiten Verbreitung ein großes Ziel ist, kann Malware prinzipiell jede Art von Computer infizieren, einschließlich Smartphones und Tablets. In der Tat nimmt die Bedeutung von Schadsoftware für mobile Geräte stetig zu. Darüber hinaus ist prinzipiell jedermann ein Ziel, denn je mehr Computer und mobile Geräte Cyber-Kriminelle infizieren, desto mehr Geld können sie verdienen. Diese Kriminellen kümmern sich in der Regel nicht darum, wen bzw. was sie infizieren, solange es nur so viele Geräte wie möglich sind.

Wer und Warum

Malware ist nicht mehr einfach nur von neugierig Hobbyisten oder Amateur-Hackern gemacht, sondern von anspruchsvollen Cyber-Kriminellen um deren hochgesteckte Ziele zu erreichen. Zu diesen Zielen gehören Diebstahl vertraulicher Daten, Sammeln von Logins und Passwörtern, das Versenden von Spam-E-Mails, Starten von Denial-of-Service-Attacken, Erpressung und Identitätsdiebstahl. Bekannt ist zum Beispiel die Malware Cryptolocker, die von Cyberkriminellen verwendet wird um Computer zu infizieren und alle Dateien zu verschlüsseln. Einmal infiziert und verschlüsselt fordern die Cyber-Kriminellen dann ein Lösegeld im Austausch für die Entschlüsselung Ihrer Dateien.

© The SANS Institute 2014

Schadsoftware

Die Verantwortlichen, die vom Erstellen und dem Einsatz der Malware profitieren, können von eigenständig handelnden Einzelpersonen über gut organisierte kriminelle Gruppen bis hin zu Regierungsorganisationen reichen. Darüber hinaus haben sich diejenigen, die die heutige hochentwickelte Malware geschaffen haben meist vollständig diesem Thema verschrieben; die Entwicklung von Malware ist ihr Vollzeit-Job. Malware, die sie entwickeln, verkaufen sie häufig an andere Personen oder Organisationen und bieten sogar regelmäßige Updates und Unterstützung für ihre "Kunden". Die kriminellen Käufer verdienen ihr Geld zum Beispiel durch die Installation der Malware auf Millionen von Systemen ahnungsloser Opfer. Die so geschaffenen Botnetze aus infizierten Systemen können die Cyber-Verbrecher wie eine ferngesteuerte Armee für eigene Zwecke gebrauchen, oder als Dienstleistung an andere Cyberkriminelle verkaufen.

Der beste Weg, um sich vor Malware zu schützen, ist Ihre Geräte immer zu aktualisieren und mit einer Antivirus-Software auszustatten. Seien Sie sich zudem immer bewusst, dass Sie dennoch angreifbar sind, und handeln Sie vorsichtig.

Schützen Sie sich

Ein üblicher Schritt zum Schutz Ihrer Computer und mobiler Geräte vor Malware ist es, Anti-Virus-Software von vertrauenswürdigen Anbietern zu installieren. Anti-Virus-, manchmal auch als Anti-Malware-Software bezeichnet, wurde entwickelt um Schadsoftware zu erkennen und zu stoppen. Dabei ist sie jedoch nicht unfehlbar, denn die Cyber-Angreifer entwickeln ständig neue, anspruchsvollere Angriffe und Methoden um Anti-Viren-Programme zu umgehen. Im Gegenzug müssen Anti-Viren-Hersteller ihre Produkte ständig aktualisieren und mit neuen Funktionen versehen, teilweise mehrfach pro Tag. In vielerlei Hinsicht hat es sich zu einem Wettrüsten entwickelt bei dem beide Seiten versuchen den anderen zu überlisten. Leider haben Cyber-Kriminelle dabei fast immer die Oberhand. Denken Sie also daran, dass die beste Anti-Virus-Software keinen hundertprozentigen Schutz bieten kann und daher weitere Maßnahmen notwendig sind um Sie zu schützen.

Stellen Sie zunächst sicher, dass Ihr Betriebssystem und die Anwendungen so eingestellt sind Sicherheits-Updates automatisch zu installieren. Je aktueller Ihre Software ist, desto schwieriger ist es für Cyberkriminelle Ihren Computer oder mobile Geräte zu infizieren.

Denken Sie zudem daran, dass Sie selbst eine der besten Abwehrmechanismen gegen Malware sind. Malware-Infektionen sind oft mit Social Engineering verbunden, dem Versuch der Angreifer Sie zu überlisten um ihre Malware zu installieren. Ein häufiges Beispiel sind sog. Phishing-Attacken, das sind E-Mails die legitim erscheinen, aber in Wirklichkeit mehr oder weniger gut gemachte Fälschungen sind um sie zu betrügen und Ihren Computer zu infizieren. Ein oft zitiertes Beispiel ist eine E-Mail, die angeblich von Ihrer Bank stammt und Sie auffordert, auf einen Link zu klicken. Folgen Sie diesem Link

Schadsoftware

gelangen Sie zu einer Website die automatisch versucht Ihren Computer zu hacken und zu infizieren. Vielleicht enthält die E-Mail aber auch einen Hinweis, dass ein Paket nicht zugestellt werden konnte und bittet Sie das beigefügte Tracking-Dokument zu öffnen – und damit unbemerkt auch Ihren Computer zu infizieren.

Social-Engineering-Angriffe können aber auch mithilfe anderer Technologien, wie z.B. dem Telefon, durchgeführt werden. Der Angreifer ruft dabei auf Ihrem Firmentelefon an und gibt vor, vom technischen Support von Microsoft sein der festgestellt hat dass Ihr Computer infiziert ist. Natürlich ist diese Geschichte eine Lüge und Ihr Computer wahrscheinlich in Ordnung. Schafft es der Anrufer jedoch Ihnen glauben zu machen, dass Sie infiziert sind wird er Sie als nächstes anleiten ihm Remote-Zugriff auf Ihr System zu ermöglichen oder Ihnen eine Sicherheitssoftware verkaufen die nichts mehr als Malware ist. Nutzen Sie Ihren gesunden Menschenverstand. Wenn ein Anruf oder eine Nachricht seltsam, verdächtig oder zu gut ist um wahr zu sein erscheint, ist sie es wahrscheinlich auch nicht.

Letztlich ist der beste Weg sich gegen Malware zu verteidigen eine Strategie mit mehreren Elementen: halten Sie Ihre Software aktuell, installieren Sie vertrauenswürdige Anti-Virus- Software von namhaften Herstellern und seien Sie wachsam hinsichtlich Versuchen Ihren Rechner zu infizieren, Sie zu täuschen oder zu betrügen.

Weiterführende Informationen

OUCH „Phishing“:

www.securingthehuman.org/resources/newsletters/ouch/2013 # february2013

OUCH „Sichern Ihres Computers“:

www.securingthehuman.org/resources/newsletters/ouch/2012 # december2012

„Sie sind das Ziel“ Poster:

http://www.securingthehuman.org/resources/posters

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der Creative Commons BY-NC-ND 3.0 Lizenz vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis