Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was sind Schadprogramme?
- Wer erstellt Schadprogramme?
- So schützen Sie sich

Schadprogramme

Überblick

Sie haben sicher schon Begriffe wie Virus, Trojaner, vielleicht auch Ransomware und Rootkit gehört, wenn über Cybersicherheit gesprochen wird. All diese Wörter beschreiben im Grunde genommen das Gleiche. Es sind Arten von Programmen, die von Kriminellen genutzt werden um Ihre Computer und Geräte zu infizieren. Ein gängiger Oberbegriff dafür ist Schadprogramme oder engl. Malware. In diesem Newsletter werden wir erklären, was Schadprogramme sind, wer sie erstellt, und natürlich wie Sie sich davor schützen können.

Gastautor

Lenny Zeltser legt sein Hauptaugenmerk auf den sicheren Betrieb der IT Systeme von Kunden der NCR Corp.und lehrt die Abwehr von Schadprogrammen am SANS Institute. Lenny ist auf Twitter als **@lennyzeltser** aktiv und schreibt ein Blog über IT Sicherheit unter **zeltser.com**.

Was sind Schadprogramme?

Ganz einfach gesagt sind Schadprogramme Computerprogramme, die darauf ausgelegt sind bösartige Handlungen durchzuführen. Im Deutschen wie im Englischen ist der Name eine Kombination der Wörter schadhaft (malicious) und Programm (software). Cyberkriminelle installieren Schadprogramme auf Computern und Geräten, um die Kontrolle über diese oder Zugang zu ihren Inhalten zu erlangen. Sobald sie installiert sind können die Angreifer die Schadprogramme nutzen um Sie bei Ihren Onlineaktivitäten zu beobachten, Ihre Passwörter oder Dateien zu stehlen, oder Ihr System nutzen um Andere anzugreifen. Schadprogramme können Ihnen sogar den Zugriff auf Ihre eigenen Dateien verwehren und erst nach Zahlung eines Lösegeldes an den Angreifer den Zugriff wiederherstellen.

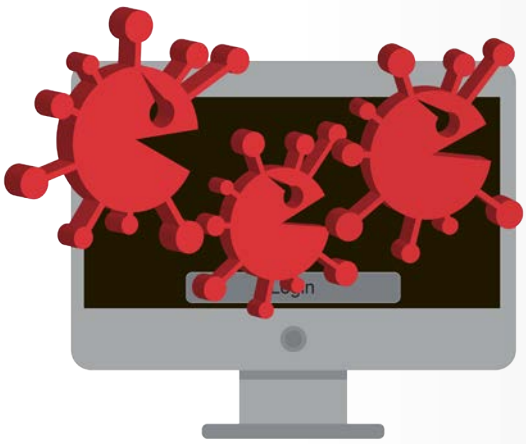
Bei vielen Menschen herrscht das Missverständnis vor, dass Schadprogramme nur auf Windows Computern ein Problem darstellen. Natürlich ist Windows weit verbreitet und daher ein großes Ziel, aber Schadprogramme können auch alle anderen Geräte infizieren, darunter Apple Mac Computer genauso wie Smartphones und Tablets. Je mehr Computer und IT Geräte die Cyberkriminellen infizieren, um so mehr Geld können sie verdienen. Jeder ist daher ein lohnendes Ziel, auch Sie.

Wer erstellt Schadprogramme?

Schadprogramme werden nicht mehr nur von neugierigen Amateur-Hackern oder Hobby-Programmierern erstellt, sondern von raffinierten Cyberkriminellen. Ihr Ziel ist ganz klar, Geld durch die Infektion Ihrer Geräte zu verdienen, vielleicht indem sie die von Ihnen gestohlenen Daten verkaufen, SPAM-E-Mail über Ihren Computer versenden, Attacken gegen Dritte darüber ausführen oder Erpressungen durchführen. Die Menschen, die Schadprogramme herstellen, verteilen und davon profitieren,

Schadprogramme

können Einzelpersonen sein, aber auch gut organisierte kriminelle Gruppen oder sogar Regierungsorganisationen. Oft ist das Erstellen von ausgefeilten Schadprogrammen eine Vollzeit-Beschäftigung für die Kriminellen. Ein einmal erstelltes Schadprogramm wird oft an andere Personen oder Organisationen verkauft, was dann sogar regelmäßige Updates und Unterstützung bei Problemen umfasst.



Schützen Sie sich vor Schadprogrammen, indem Sie vor allem gegenüber verdächtigen Nachrichten skeptisch sind, Ihre Geräte immer aktuell halten und wenn möglich eine Antivirus Software installieren.

So schützen Sie sich

Ein naheliegender Schritt, sich gegen Schadprogramme zu schützen, ist die Installation eines Antivirus-Programms von einem vertrauenswürdigen Hersteller. Solche Programme, oft auch Anti-Malware genannt, sind darauf ausgelegt, Schadprogramme zu erkennen und zu bekämpfen. Jedoch kann keines der Antivirus-Produkte alle bösartigen Programme erkennen oder blockieren. Cyberkriminelle erfinden ständig neue, fortgeschrittenere Methoden, die Erkennung Ihrer Schadprogramme zu umgehen. Gleichzeitig aktualisieren Antivirus-Hersteller fortwährend ihre Produkte mit neuen Möglichkeiten zur Erkennung von Schadprogrammen. Es ist in vielerlei Hinsicht zu einem Rüstungswettstreit geworden, bei dem beide Seiten versuchen den Anderen zu überlisten. Leider sind die bösen Jungs üblicherweise einen Schritt voraus. Sie können sich daher nicht allein auf Antivirus-Produkte verlassen und sollten die folgenden Punkte verinnerlichen, um sich besser zu schützen:

- Cyberkriminelle infizieren Geräte häufig durch das Ausnutzen von Schwachstellen in deren Software. Je aktueller die Programme auf Ihren Geräten sind, desto weniger bekannte Schwachstellen weisen diese auf und um so schwieriger ist es für die Kriminellen, sie zu infizieren. Stellen Sie daher für jedes Gerät sicher, dass Betriebssystem und Anwendungen automatisch aktualisiert werden.
- Eine gängige Methode zur Infizierung von Mobilgeräten ist die Erstellung einer gefälschten App, die irgendwo im Internet zum Download bereitgestellt wird. Nutzer werden dann dazu verleitet, diese herunterzuladen und auszuführen. Laden Sie nur Programme und Apps aus vertrauenswürdigen Quellen, und achten Sie darauf nur Apps zu wählen die schon vor längerer Zeit veröffentlicht wurden, von vielen anderen Menschen bereits heruntergeladen wurden und möglichst viele positive Bewertungen erhalten haben.
- Nutzen Sie auf Computern ein Standard-Benutzerkonto mit eingeschränkten Rechten, nicht die privilegierten Konten wie “Administrator” oder “root”. Das bietet einen zusätzlichen Schutz, weil es bei vielen Arten von Schadsoftware verhindert, dass diese sich unerkannt tief im System einnisten kann.
- Cyberkriminelle überlisten Nutzer häufig, damit diese ihre Schadprogramme unbeabsichtigt installieren. Sie könnten Ihnen z.B. eine E-Mail senden die legitim aussieht und einen Anhang oder einen Link enthält. Vielleicht scheint die E-Mail von Ihrer Bank oder einem Freund zu kommen. Wenn Sie jedoch die Datei öffnen oder den Link anklicken,

Schadprogramme

aktivieren Sie den bösartigen Programmcode, der ein Schadprogramm auf Ihrem System installiert. Wenn eine Nachricht eine große Dringlichkeit suggeriert, verwirrend formuliert ist oder einfach zu gut klingt um wahr zu sein, könnte es sich dabei um einen Angriff handeln. Seien Sie immer vorsichtig, der gesunde Menschenverstand ist oft Ihre beste Abwehr.

- Sichern Sie regelmäßig die Systemdateien und Ihre eigenen Daten zu Cloud-basierten Diensten oder speichern Sie die Sicherungen auf einem Medium, das nicht ständig mit Ihren Systemen verbunden ist. Das schützt die Sicherungen für den Fall, dass Schadprogramme versuchen all Ihre Dateien zu verschlüsseln oder zu löschen. Diese Datensicherungen sind unheimlich wichtig, sie sind oft der einzige Weg, nach einer Infektion mit einem Schadprogramm den Normalzustand wiederherzustellen.

Zusammengefasst kann man sagen, das Sie die Software auf Ihrem System immer auf dem aktuellsten Stand halten, ein Antivirus-Programm eines bekannten und vertrauenswürdigen Herstellers installieren und eine gewisse Vorsicht vor Versuchen, Sie hereinzulegen walten lassen sollten, um eine Infektion Ihres Systems zu vermeiden.

Weiterführende Informationen

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Sichere Nutzung Mobiler Apps:	https://securingthehuman.sans.org/ouch/2015#january2015
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup & Wiederherstellung:	https://securingthehuman.sans.org/ouch/2015#august2015

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

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

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