Welche Bedrohungen von Viren und Schadsoftware gibt es?

Virus, Malware, Ransomware, Trojaner

Wie ist die Virus- und Malware-Bedrohung einzuschätzen?

Quelle: Emsisoft In Sicherheitswissen by Doreen on July 7, 2016
Haben Sie sich jemals gefragt, was Sie tun würden, wenn alle Daten auf Ihrem Laptop als „Geisel“ genommen werden? Was, wenn Sie Artikel online kaufen möchten und plötzlich grundlos Ihr Bankkonto leer ist? Das ist ein Albtraum, den viele von uns nur aus Gruselgeschichten anderer kennen. Leider sind dies nur zwei von eindeutig zu vielen Bedrohungen, denen wir mit der zunehmenden Internetkriminalität ausgesetzt sind.

Heutige Angreifer scheinen moderne Sicherheitsmaßnahmen überhaupt nicht zu beeindrucken. Der Einsatz bösartiger Software ist für Banken, Unternehmen und Privatanwender noch immer ein großes Problem.

Was ist Malware?

Der Begriff „Malware“ geht für eine Fülle an ausbeuterischen Programmen. In

einfachen Worten: Malware ist ein Schadprogramm, das speziell dafür ausgelegt wurde, ein Computersystem zu stören oder zu beschädigen.

Welche Arten von Malware gibt es?

Malware lässt sich in verschiedene Kategorien unterteilen, die wir hier in der Reihenfolge ihres Gefahrenpotenzials vorstellen werden.

Viren – heutzutage keine große Bedrohung mehr

Ein Virus verbreitet sich, indem er seinen Code in ein anderes Programm schleust. Der Einsatzbereich von Computerviren reicht dabei vom Stehlen vertraulicher Informationen und Übernehmen der Steuerung des Computers zum Durchführen unerlaubter Aktionen bis hin zum schlichten Beweis, dass es möglich ist (etwa das Hacken oder Deaktivieren einer Regierungswebsite). Wie die Namensverwandtschaft zur biologischen Version schon andeutet, benötigt ein Virus einen Wirt (ein sogenannter Host).

Würmer – weniger gebräuchlich

Diese Schädlinge ähneln Viren insofern, dass sie sich so schnell wie möglich verbreiten wollen. Allerdings benötigen Sie dazu kein Host-Programm. Würmer werden über Speichergeräte (wie USB-Sticks) und E-Mails verteilt. Erinnern Sie sich, als Ihnen Ihre Schwester den USB-Stick mit den Familienfotos gegeben hat und Ihr Computer plötzlich verrückt spielte? Genau, er war höchstwahrscheinlich mit einem Wurm infiziert.

Antivirus-Software, idealerweise mit einem **Dual-Engine-Dateischutz**, ist Ihre beste Verteidigung gegen jegliche Art von Malware, die über E-Mails, USB-Sticks oder Downloads verbreitet wird.

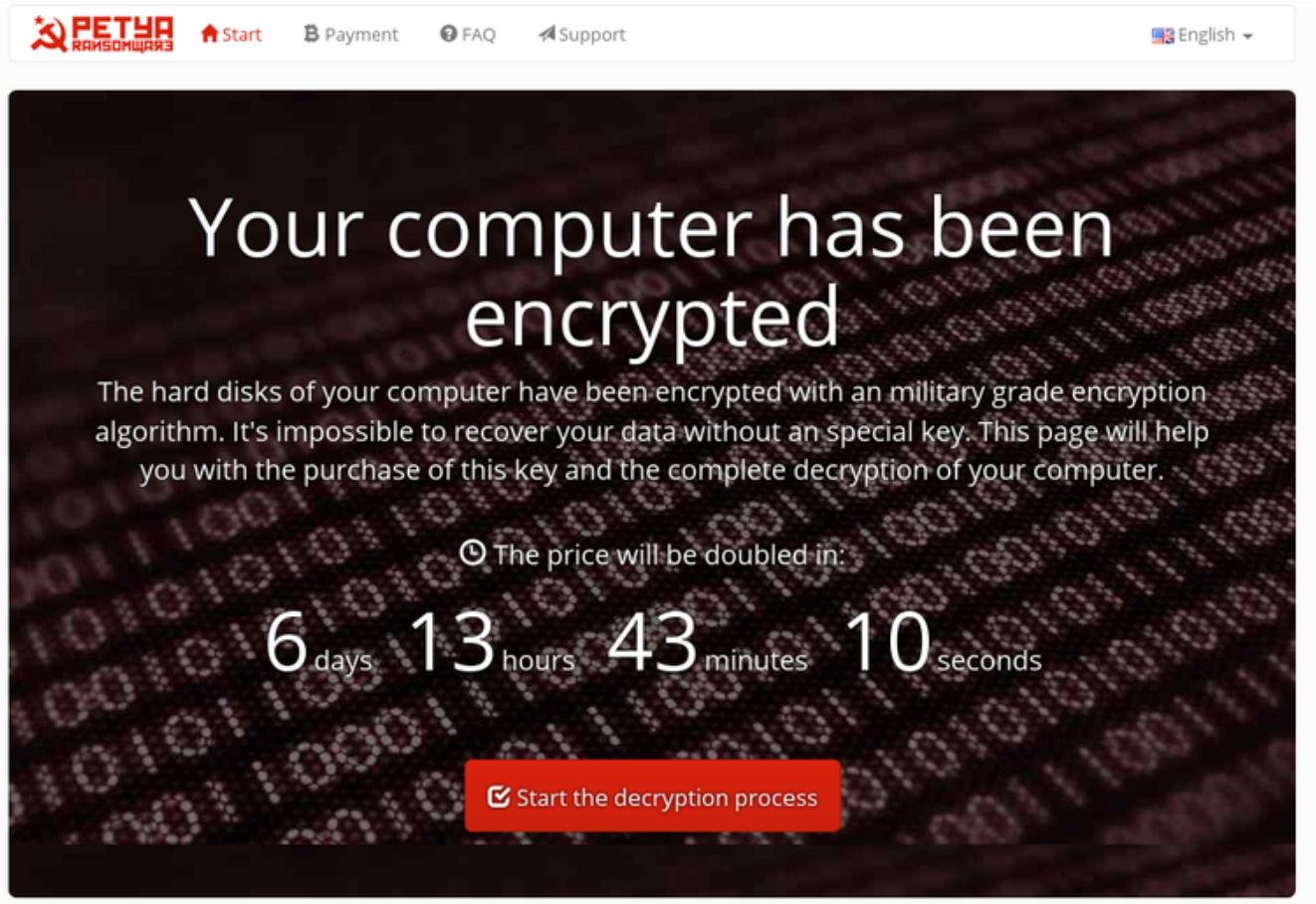
Spyware – nicht sehr störend, aber beängstigend

Diese Schadprogramme spionieren Sie aus und sammeln ohne Ihr Wissen alle Arten von Daten, die auf Ihrem Computer gespeichert sind. Innerhalb von Augenblicken nach der Installation haben Internetkriminelle Zugriff auf Ihre persönlichen Informationen, wie E-Mails, private Fotos und natürlich auch Ihre Kreditkartendaten. Spyware wird in Form von sogenannten *Keyloggern* auch zur Überwachung eingesetzt. Dabei werden alle auf der Tastatur gemachten Tastenanschläge überwacht und aufgezeichnet. Hier ist in den letzten Jahren

auch der Bedarf im privaten Bereich stark gewachsen. Eltern machen sich zunehmend Sorgen, was ihre Kinder im Internet treiben. Keylogger-Software hat sich daher zu einer neuen Form der elterlichen Kontrolle entwickelt, ähnlich der Kindersicherung am Fernseher. Mit einem schlichten Programm können Eltern die Eingaben ihrer Kinder überwachen und damit nachvollziehen, was sie in Foren schreiben und auf Google suchen, wenn sie sich unbeobachtet fühlen.

Ransomware – ein kostspieliges Problem

Ransomware ist ein kriminelles Schadprogramm, das Ihre privaten Daten verschlüsselt oder den gesamten PC sperrt. Sie werden dann aufgefordert, über einen anonymen Dienst ein „Lösegeld“ zu bezahlen, um den Computer oder die Daten wieder freizugeben. Ransomware ist inzwischen zu einer der größten Bedrohungen geworden, da sie sich als leichte Einkommensquelle für die Angreifer erwiesen hat. Andere Malware bringt den Entwicklern nur indirekt Geld (etwa durch die Verwendung oder den Verkauf der Computerleistung). Dieser Schädling fordert jedoch direkt Geld bei dem Opfer (Ihnen), damit es wieder Zugriff auf seine Daten oder seinen Computer erhält. Diese Forderung erfolgt meistens über einen Sperrbildschirm mit einem Countdown und dem Link zu der Seite, über die das Lösegeld gezahlt werden soll.



Beispiel für eine Ransomware-Sperre

Anfang des Jahres hat das Presbyterian Medical Center in Hollywood nach einem Malware-Angriff 17.000 USD an Lösegeld bezahlt, um Patientendaten wiederherzustellen. Diese Art von Malware wird in der Regel mithilfe eines Trojaners installiert, der wohl heimtückischsten Malware-Variante.

Trojaner – der ultimative Schädling

Das Hauptziel eines Trojanischen Pferds (kurz Trojaner) ist die Installation einer anderen Anwendung auf dem infizierten Computer, die dann ferngesteuert werden kann. Im Gegensatz zu Viren verbreiten sich Trojaner nicht selbstständig. Wie auch die Griechen beim Angriff auf die Stadt Troja mit ihrem Pferd versteckt sich in schädlichem Code ein zweites Programm, der eigentliche Trojaner. Diese Malware stellt auch weiterhin ein großes Problem dar, insbesondere für Geldinstitute. Sie ist bekannt dafür, Screenshots zu machen und an externe Server zu senden, zur Identifikation verwendete IP-Adressen zu sammeln, bösartigen Code einzuschleusen und jedermann den Zugriff auf den PC zu ermöglichen, der den Schlüssel dazu hat.

Trojaner sind so gefährlich, weil die Software aus zwei Teilen besteht: Der erste Teil infiziert Ihren Computer, während der zweite Teil im Hintergrund wartet, bis Sie die Website Ihrer Bank aufrufen, wo er dann Ihre Anmeldedaten aufzeichnet und Ihre Online-Identität klaut. Dasselbe Kennwort, das Sie für all Ihre Websites, E-Mail-Konten, Facebook, Online-Banking und dergleichen verwenden (wobei wir stark hoffen, dass Sie es besser wissen), wurde bequem mit Ihrem Benutzernamen aufgezeichnet. Mit auf diese Weise gestohlenen Kreditkartenangaben wird bereits genug Missbrauch betrieben. Da beim Online-Einkauf weder eine PIN noch eine Unterschrift erforderlich sind, reicht es schlicht, Namen, Kartennummern, Ablaufdaten und CVV-Nummern (Sicherheitsnummer auf der Rückseite) abzugreifen, während Sie sie auf der vorgeblichen eBay-Seite eingeben. Ein sehr lukrativer Betrug.

Trojaner können jedoch auch Dateien und Daten auf Ihren Festplatten zerstören oder vertrauliche Informationen erfassen und an externe Adressen weiterleiten. Durch das Öffnen von Kommunikationsports lässt sich Ihr Computer zu einem *Zombie* machen. Dabei handelt es sich um einen Teil eines sogenannten Botnetzes (Netzwerk aus mit Bots befallenen Rechnern), das von Kriminellen ferngesteuert wird.

Bots – einfach nur Furcht einflößend

Auch dieser Schädling besteht aus zwei Teilen:

Einem Dropper – ein Exploit oder Trojaner, der dafür sorgt, dass die tatsächlichen Malware heruntergeladen wird.

Der eigentliche Bot – eine Software zur Fernsteuerung, die sich mit einem Master-Server verbindet und auf Anweisungen wartet. Stellen Sie sich vor, Sie hätten einen Computer, mit dem Sie 100.000 Computer fernsteuern könnten, um eine Aktion auszuführen. Was sich damit anstellen ließe … Ein Beispiel: Sie könnten alle Computer eine Spam-E-Mail pro Stunde senden lassen. Das würde niemandem auffallen. Sie könnten aber auch innerhalb kurzer Zeit Millionen E-Mails verschicken, um Viagra zu verkaufen oder um amazon.com mit 1.000 Anfragen pro Minute gleichzeitig zu überschwemmen und damit deren Server zu überlasten, sodass sie nichts mehr verkaufen können. Sie könnten aber auch ein Lösegeld fordern, um diesen Angriff gar nicht erst zu starten.

Leider können diese Lösegeldforderungen in die Millionen reichen und die Bots

befallen trotzdem weiter immer mehr Computer, wo sie auf die Entdeckung neuer Sicherheitslücken warten und dann alle anderen Bots auffordern, weitere verletzliche Maschinen zu infizieren. Ein endloser Kreislauf.

Plötzlich ist aus dem Botnetz mit 100.000 Computern ein virtueller Monstercomputer geworden, der Kennwörter knacken, durch Mining Bitcoins sammeln oder andere rechenintensive Aufgaben kostenlos durchführen kann – und Ihr Computer wäre ein Teil davon.

Natürlich wollten Sie keine 10.000 USD aus Ihren Ersparnissen als Spende an eine Terrororganisation senden. Sicher haben Sie auch die Keylogger auf den Hunderten Computern nicht absichtlich installiert, die jetzt für Betrüger Daten sammeln. Leider müssen wir Ihnen jedoch sagen, dass diese Aktionen von Ihrem Computer durchgeführt wurden und Sie damit im Ernstfall zur Verantwortung gezogen werden können.

Beim Zugriff auf eine Website überprüft eine gute Anti-Malware-Software, ob diese Adresse bereits für das Verteilen von Malware bekannt ist. Sollte dies der Fall sein, wird Ihnen statt der Website eine Warnmeldung angezeigt. Vertrauen Sie also auf eine Antivirus-Lösung, die sich nicht allein auf die Erkennung von Signaturen verlässt, sondern auch das Verhalten Ihrer Programme auf Unregelmäßigkeiten überwacht.

Ein abschließender Hinweis zu Malware

Malware ist darauf ausgelegt, Ihr System zu stören oder zu beschädigen. Sie sollten sich jedoch bewusst sein, dass sich diese Bedrohungen nicht länger in nur eine Kategorie einsortieren lassen. Bots werden beispielsweise über Exploits und Trojaner installiert und ihre Verbreitung kann mitunter sehr sprunghaft erfolgen. Ransomware verhält sich hingegen manchmal wie ein Virus und manipuliert

Dateien. Malware ist also immer gefährlich – unabhängig von ihrer Art oder Verbreitung.

Noch eine Anmerkung zu *PUPs (potenziell unerwünschte Programme)*

PUPs oder sogenannte „Crapware“ (engl.: crap = Unsinn, Müll) hingegen ist normalerweise nicht gefährlich, sondern lediglich extrem störend. Sicher interessiert Sie eine permanente Wettermeldung von Aruba nicht im Geringsten. Dennoch kann es vorkommen, dass Ihnen plötzlich bei jedem Öffnen eines Programms diese oder andere nervige Meldungen angezeigt werden. PUPs gelangen ähnlich wie Malware auf Ihr System, etwa durch einen Fehler auf einer vertrauenswürdigen Website oder in ein tatsächlich erwünschtes Programm verpackt. Ein gutes Sicherheitsprogramm wird diese Eindringlinge jedoch erkennen und entfernen und darüber hinaus einen sicheren Surfschutz bieten. Eine Datenbank, die die Adressen der gefährlichen Websites enthält, sorgt dann dafür, dass Sie die Websites gar nicht erst aufrufen können.

Es gibt Schutz vor Malware und PUPs

Das klingt alles sehr beängstigend, allerdings können Sie mithilfe der richtigen Vorsichtsmaßnahmen Ihre Daten schützen und Ihr Surfvergnügen sicherer gestalten.

1. Stellen Sie sicher, dass Ihre Software auf dem neuesten Stand ist – insbesondere Ihr Betriebssystem, Ihre Webbrowser sowie alle Browser-Plug-ins, wie Adobe Flash Player oder die Java-Plattform von Oracle.
2. Bleiben Sie aufmerksam. Stellen Sie Fragen, bevor Sie klicken. Informieren Sie sich darüber, wie Bedrohungen (und Betrugsmaschen) funktionieren, um ihnen nicht zum Opfer zu fallen.
3. Stellen Sie sicher, dass Sie immer eine leistungsstarke Anti-Malware-Software mit Echtzeitschutz (egal ob beim Arbeiten, Spielen oder Surfen) verwenden, wie beispielsweise Emsisoft Anti-Malware.
4. Lassen Sie Ihr System für eine zweite Meinung gelegentlich von einem Scanner wie Emsisoft Emergency Kit, Malwarebytes Anti-Malware oder Hitman Pro überprüfen, um sicherzustellen, dass der Computer keinen Trojaner hat.

Egal, wie gut Sie sich auch mit Computern auskennen mögen, das Wichtigste beim Umgang mit dem PC bleibt das regelmäßige Aktualisieren einer

Sicherheitssoftware mit Echtzeitschutz. Der Schutz Ihrer Daten und Ihrer persönlichen Informationen ist von höchster Bedeutung. Welche weiteren Funktionen sollte ein gut abgestimmtes Sicherheitsprogramm noch haben?

Emsisoft Anti-Malware schützt Ihren Computer auf drei verschiedene Arten: Der **Surfschutz** sorgt dafür, dass Sie keine gefährlichen Websites aufrufen können. Der leistungsstarke **Dual-Engine-Scanner** findet Malware, sofern sie es doch auf Ihren Computer schaffen sollte, und dank der fortschrittlichen **Verhaltensanalyse** werden selbst unbekannte Schädlinge zuverlässig erkannt.

Wenn Sie sich schützen wollen schauen Sie bitte hier: Nicos Anti-Virusprogramme