Update zu WannaCry: Schlimmster Ransomware-Angriff der Geschichte.

Jakub Křoustek
16 Mai 2017

Freitag der vergangenen Woche war zwar nicht der 13., aber es sah fast danach aus. PCs weltweit, einschließlich in Krankenhäusern und bei Behörden, waren von der **Ransomware WannaCry** (auch als WanaCrypt0r oder WCry bezeichnet) betroffen, die ein Chaos verursachte. Bis jetzt wurden 250.000 Fälle in 116 Ländern festgestellt. Das heißt, bei mehr als 250.000 Avast-Benutzern wurde ein Ransomware-Angriff durch WannaCry festgestellt, allerdings waren diese Nutzer geschützt, **da Avast eine Infizierung der PCs durch die Ransomware abgewehrt hat**. Während sich die Situation allmählich beruhigt, können wir schlussfolgern, dass dies der schlimmste Ransomware-Angriff aller Zeiten war.

Über unseren Avast WLAN-Inspektor, mit dem Benutzer ihre Systeme auf Sicherheitslücken hin überprüfen lassen können, sehen wir, dass etwa 15 Prozent der Nutzer keinen Patch für die Sicherheitslücke MS17-010 installiert hatten, wodurch sie durch diesen Angriff gefährdet gewesen wären, **wenn sie Avast nicht geschützt hätte**.

Bis Freitagnachmittag hatten wir mehr als 50.000 Vorfälle der Ransomware bei Avast-Nutzern festgestellt. Im späteren Tagesverlauf, gegen Mitternacht, war die Anzahl der Vorfälle auf mehr als 100.000 gestiegen.

Ein Bild der Zerstörung durch WannaCry

Die Übersicht auf:

https://blog.avast.com/de/update-zu-wannacry-schlimmster-ransomware-angriff-der-geschichte

zeigt die Zeitpunkte des Anstiegs und Abnahme der Angriffe, **die Avast abwehren musste**.
Avast kann alle WannaCry-Varianten ermitteln, nicht nur die Varianten mit der Wurmkomponente, sondern auch jene, die die Dateien einfach verschlüsseln und sich dann nicht weiter ausbreiten. Die Wurmkomponente bestimmt, wie WannaCry sich ausbreitet; dies beschreibe ich im Folgenden. Einige Forscher sagen, die Ausbreitung wäre vorüber, allerdings gilt dies nur für die WannaCry-Variante, die sich zuvor wie ein Wurm ausgebreitet hat.

Kurz nach dem Ausbruch haben wir 10.000 Vorfälle pro Stunde festgestellt, was eine sehr hohe Zahl für einen einzelnen Malware-Stamm ist.

Nachdem ein Malware-Forscher den Notausschalter aktiviert hat (dieser Vorgang wird weiter unten im Blog-Artikel beschrieben), reduzierte sich am späten Freitagnachmittag die Zahl der Erkennungen erheblich auf etwa 2.000 pro Stunde. Diese Zahl hat sich seitdem weiter verringert und wir hoffen, dass dieser Trend anhält.

Die zehn am stärksten von diesem Angriff betroffenen Länder sind - unseren Daten nach zu urteilen - in absteigender Reihenfolge: **Russland, Ukraine, Taiwan, Indien, Brasilien, Thailand, Rumänien, Philippinen, Armenien und Pakistan**. Mehr als die Hälfte der Angriffsversuche bei unseren Benutzern haben wir in Russland festgestellt und blockiert.

Gegen wen hat sich WannaCry gerichtet?

WannaCry richtete sich wie die meisten Ransomware-Varianten nicht gegen bestimmte Personen. Die Ransomware verwendete einen als ETERNALBLUE bekannten Exploit, der eine Sicherheitslücke (mit der Bezeichnung MS17-010) von Windows SMB (Server Message Block, einem Protokoll zur Dateifreigabe für Netzwerke) ausnutzt. WannaCry richtete sich wahllos und ziellos gegen die der **NSA** bekannten **Windows**-User, und davon dann insbesondere die nicht den im März von **Microsoft** für diese Sicherheitslücke veröffentlichten Patch (Flicken) installiert hatte.

WannaCry konnte sich deshalb so aggressiv ausbreiten, da jeder mit einem Netzwerk verbundene Windows-Computer, der die Sicherheitslücke MS17-010 aufweist, ohne Zutun seines Benutzers infiziert werden kann. Die bereits auf einem PC aktive Malware scannt sowohl das lokale Netzwerk als auch das Teilnetzwerk und wählt willkürliche IP-Adressen aus. Sobald ein anfälliger PC gefunden wurde, breitet sich die Ransomware auf diesem PC ebenfalls aus - wohl deshalb, weil WannaCry Wurmfähigkeiten enthält.

.

Windows XP-Benutzer waren dem Angriff **schutzlos** ausgesetzt. Microsoft hatte den Support für das alte Betriebssystem im Jahre 2014 eingestellt. Das heißt, dass auch wenn Windows-XP-Nutzer den Patch herunterladen wollten, konnten sie dies nicht. Microsoft hat nun einen speziellen Patch für ältere Betriebssysteme veröffentlicht.

.

Da dieser vor dem Angriff nicht verfügbar war, wurde Windows XP zwar das anfälligste Betriebssystem, dennoch trat die Mehrzahl der von uns abgewehrten Angriffsversuche auf Systemen wie **Windows 7** auf, das heißt auf Computern, auf denen man das Sicherheits-Update nicht installiert hatte, obwohl es längst verfügbar war. Falls Ihr den Patch noch nicht heruntergeladen habt, raten wir Euch dringend, dies nachzuholen; dies gilt insbesondere für Nutzer älterer Versionen von Windows-Betriebssystemen.

.

Große Unternehmen wie Telefonica und Deutsche Bahn waren von dem Angriff betroffen, aber weitaus schlimmer wirkte sich der Schaden auf Krankenhäuser weltweit aus. Krankenhäusern fehlen oft die finanziellen Mittel, um ihre Systeme auf dem neuesten Stand zu halten, daher waren sie am Freitag besonders schwer betroffen, was auch große Auswirkungen auf die Patientenversorgung hatte.

Entfernen von WannaCry

Das Entfernen der Ransomware WannaCry von einem PC ist nicht schwer, dazu sollte eine Antivirus-Software in der Lage sein, indem die gefährlichen Dateien in die Quarantäne verschoben werden. Jedoch wird das Problem dadurch nicht behoben, da die Dateien weiterhin verschlüsselt bleiben.

Derzeit gibt es keine kostenlosen Tools zur Entschlüsselung und nach unserer Analyse handelt es sich bei der verwendeten Verschlüsselung um eine sehr Starke (AES-128 kombiniert mit RSA-2048). Falls Euer PC infiziert wurde, solltet Ihr am besten Eure Dateien gegebenenfalls aus einem Backup wiederherstellen. Führt diesen Vorgang auf einem sauberen Rechner durch, auf dem alle Patches installiert wurden. Für maximale Sicherheit solltet Ihr diesen Vorgang offline durchführen, um das Risiko einer Verschlüsselung des Backup-Speichers so gering wie möglich zu halten.

Der Notausschalter

Ein auf Twitter als MalwareTech bekannter Forscher entdeckte einen Notausschalter, wodurch die Ausbreitung der häufigsten WannaCry-Varianten gestoppt werden konnte.

Der Grund, warum ein Notausschalter enthalten war, ist weiterhin unklar. Wir nehmen an, dass er in die Ransomware integriert wurde, falls die Gruppe hinter WannaCry die Ausbreitung stoppen wollte. Der Notausschalter funktioniert so: Wenn WannaCry eine Anfrage an eine bestimmte Web-Domain stellte (**www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**) und eine Antwort erhielt, was auf eine aktive Domain hinweist, wurde die Malware einfach beendet und so an einer weiteren Ausbreitung gehindert. Vor der Aktivierung des Notausschalters war die Domain nicht registriert und WannaCry konnte sich daher unkontrolliert ausbreiten.

.

Der 22-jährige britische Malwaretech-Forscher (…) fand die eigenartige Internetadresse im Code und registrierte die Domain für 10,69 US-Dollar. Er richtete dafür einen Server ein und hoffte so, weitere Informationen über den Kryptotrojaner sammeln zu können. Sofort entdeckte er 5000 bis 6000 Verbindungsversuche pro Sekunde. Zum Zeitpunkt der Guardian-Meldung waren es bereits 78.000 – inzwischen sind es mehr als 117.000.

(heise online, 13.05.2017, 12:11 Uhr)

Der Notausschalter ist vergleichbar mit der Handbremse eines Autos. Sie lässt sich im Notfall zum Anhalten verwenden, nicht aber zum Steuern des Fahrzeugs. Das Gleiche gilt für den Notausschalter – die Ausbreitung lässt sich sofort stoppen.

Dabei ist es wichtig zu wissen, dass der Notausschalter nur eine Variante von WannaCry an einer weiteren Ausbreitung gehindert hat. Dass die WannaCry-Variante gestoppt wurde hilft jedoch leider den Nutzern nicht, deren PC bereits infiziert wurde. Außerdem enthalten die tiefer liegenden Komponenten von WannaCry, beispielsweise die Dateiverschlüsselung, keine Wurmfunktion (wodurch so viele Computer angegriffen werden konnten); daher können diese nicht durch den Notausschalter gesteuert werden, sondern auch weiterhin Schäden verursachen. Wenn Ihr also auf die Ransomware selbst stoßt, beispielsweise von einem bereits infizierten Gerät, über das Kopieren einer Datei auf einen USB-Stick, dann kann Euer Gerät dennoch infiziert werden.

Seitdem der Notausschalter betätigt wurde, hat sich die Ausbreitung von WannaCry erheblich verlangsamt. Wir haben jedoch mindestens sechs weitere Varianten von WannaCry festgestellt, die andere Notausschalter, also URLs, enthalten.

Wir haben mehrere Muster festgestellt, bei denen der Notausschalter entfernt wurde, was bedeutet, dass die Personen hinter den Varianten wollten, dass ihre Versionen sich unkontrolliert ausbreiten. Aufgrund der Ähnlichkeit zwischen all diesen Varianten glauben wir, dass die späteren Versionen nur modifizierte Versionen der ursprünglichen Variante von WannaCry sind und wahrscheinlich von anderen Gruppen oder Personen verändert wurden.

Wie viel die Internetbetrüger verdient haben

Das von WannaCry geforderte Lösegeld liegt zwischen 300 und 600 US-Dollar (300 US-Dollar entsprechen 0,17222 Bitcoin; Stand: 16. Mai 2017) und die Forderungen steigen laufend. Die Ransomware droht, alle verschlüsselten Dateien zu löschen, wenn das Lösegeld nicht innerhalb von sieben Tagen gezahlt wird; diese Behauptung stimmt jedoch nicht.

Wir haben die Bitcoin-Zahlungsadressen überwacht, die von der Gruppe verwendet werden, die hinter dem Angriff steht. Es wurden mehr als 260 Zahlungsvorgänge durchgeführt, was einem Gesamtbetrag von 41 BTC entspricht (Stand ist der Zeitpunkt, zu dem dieser Blog-Artikel verfasst wurde). Dies entspricht etwa 70.000 US-Dollar, was nicht besonders viel ist, verglichen mit dem entstandenen Schaden.

Während im WannaCry-Fenster der Countdown abläuft, die den Opfern zur Zahlung bleibt, bevor sie angeblich ihre Daten verlieren (was nicht stimmt, wie wir wissen), werden in den nächsten ein oder zwei Tagen wahrscheinlich noch mehr Zahlungen eingehen. Wir raten dringend von einer Bezahlung ab, da es keine Garantie dafür gibt, dass Eure Dateien entschlüsselt werden. Stattdessen werden die Autoren der Ransomware ermutigt, weitere Ransomware-Angriffe zu starten.

Es sieht aus wie WannaCry, benimmt sich wie WannaCry, aber es ist nicht WannaCry

Sobald WannaCry bekannt wurde, sind andere Cyberkriminelle auf den Zug aufgesprungen, um Geld zu verdienen. Wir haben mehrere minderwertige bösartige Anwendungen festgestellt, die WannaCry nachbilden.

Abschließende Bemerkungen

Am Freitag haben meine Kollegen und ich am CARO-Workshop teilgenommen, einer großartigen Antiviren-Konferenz, bei der ein Vortrag über die neue Ransomware Spora gehalten wurde, die sich ebenfalls wie ein Wurm ausbreitet. Während des Workshops haben wir uns mit Forschern aus anderen Unternehmen über die neuesten Trends und die Virenausbrüche der letzten Jahre wie Loveletter, Blaster oder Nimda ausgetauscht.

Diese Rückschau nahm ein abruptes Ende, als „Wannageddon“ eintrat. Das hektische Treiben, das in diesem Moment losbrach, ist nur schwer zu beschreiben. Am Ende des Tages wurde es klar, dass wir gerade den schlimmsten Ransomware-Angriff der Geschichte erlebten.

Wir werden sehen, was die nächsten Tage bringen. Über den Ursprung des Angriffs gibt es bereits Spekulationen. Außerdem treten auch andere Bedrohungen auf, die den gleichen Infektionsverlauf aufweisen.

Quelle:
https://blog.avast.com/de/update-zu-wannacry-schlimmster-ransomware-angriff-der-geschichte

(Ransomware-Angriff.odt/pdf)

Nach der Attacke durch Erpressersoftware gibt die ARD den Anwendern die Schuld

(15 *Montag* Mai 2017, Posted by Dok in ARD)

Die seit Freitagabend grassierende Epidemie mit der „*wannacry*“ getauften Erpressermalware (zu den bisher bekannten Fakten) hat in den vergangenen Tagen weltweit Tausende Computer mit veralteten **Microsoft-Betriebssystemen** befallen.

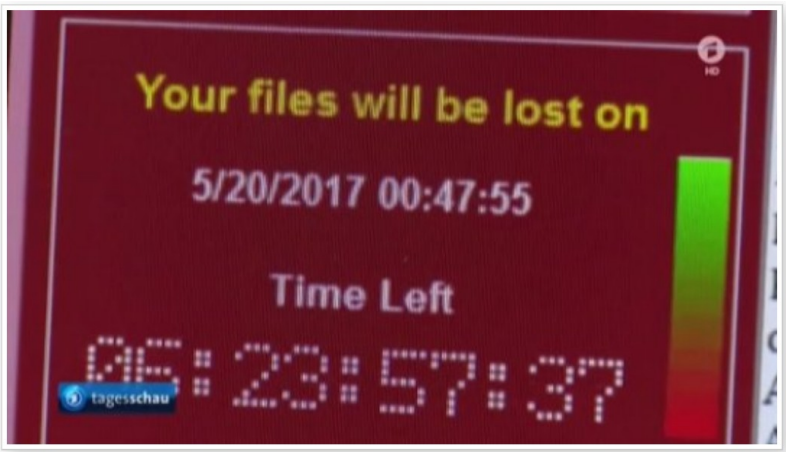
Auch wenn die Ausbreitung erstaunlich schnell etwas eingedämmt werden konnte, zeigt der Fall einmal mehr die Gefahren für eine auf unsicherer IT aufgebauten Infrastruktur sowie durch die kriminelle Energie staatlicher Geheimdienste, die Softwarelücken als Waffen sammeln und bei Bedarf für eigene Zwecke nutzen, anstatt sie zu stopfen.

Der kriminelle Angriff war nur durch die 3 Voraussetzngen möglich:

1.) ein marktdominierendes Betriebssystem, das anstatt auf Sicherheit auf kommerziellen Erfolg hin konzipiert ist,

2.) Geheimdienste, die Sicherheitslücken sammeln und benutzen, anstatt sie zu stoppen,

3.) arglose Verbraucher.



— Die Erpressersoftware verschlüsselt Dateien auf dem Computer des Opfers und verlangt eine Lösegeldzahlung, um diese wieder freizugeben.

Wundert es jemanden, dass der Staatssender ARD gemeinsam mit der Regierung den Verbrauchern die Schuld zuschieben will?

Aufgeklärte Bürger wird es kaum wundern, denn der Staatssender agiert regelmäßig als Organ der Bundesregierung und vertritt im Zweifelsfall nicht die Interessen der Bürger, sondern jene von Wirtschaft und Regierung. Propaganda für TTIP und CETA oder die – milde ausgedrückt – industriefreundliche Berichterstattung über den VW-Skandal sind da nur die aktuellsten Beispiele. ARD und ZDF haben u.a. die Funktion, Unmut in der Bevölkerung anzufachen, gegen Russland, gegen AFD, gegen kritische Künstler, siehe auch Edward Snowden, 9.2.2017 by acTVism Munich:

https://www.youtube.com/embed/iA7V6goJXYk?rel=0&autoplay=1

zu kanalisieren, oder herunterzukochen, wenn es im Regierungsinteresse ist.

Was für jeden Hersteller gilt, dass er Verantwortung für die Sicherheit seines Produktes trägt, gilt im Falle globaler US-amerikanischer Großkonzerne, zu deren Kunden die Bundesregierung zählt, nicht gleichermaßen. Microsoft kann Betriebssysteme auf den Markt bringen, die schon am Tag der Auslieferung unsicher sind, regelmäßig mit Patches gefüttert werden müssen und deren Updates man schlicht und einfach einstellt, wenn man es für wirtschaftlich geboten hält.
In gewisser Weise erinnert das Geschäftsmodell von Microsoft an das der *wannacry*-Erpresser: Entweder du kaufst innerhalb eines Zeitraumes unser neues System, oder deine Daten sind verloren!

Bereits am Samstag Abend begann die ARD tagesschau ihr *„blame game“* gegen die betroffenen Verbraucher damit, dass sie ihnen zu allem Ärger, den sie hatten, auch noch in Person des **Präsidenten des BSI, Arne Schönbohm**, die Schuld an dem erpresserischen Einbruch zuschieben ließ. Der hatte kein Wort der Kritik in Richtung des US-amerikanischen Softwaregiganten **Microsoft**, schon gar nicht in Richtung der **NSA**,

aus deren Arsenal die zur Cyberwaffe aufgemotzte Sicherheitslücke in ihren Grundzügen stammte, sondern zeigte mit dem Finger einseitig in Richtung jener Bürger und Organisationen, die – aus welchen Gründen auch immer – keine Sicherheitspatches auf ihrem Rechner hatten.

Tatsächlich gab es für die neueren MS-Betriebssysteme seit März einen Patch, jedoch nicht für die vielen nach wie vor am Netz hängenden Versionen *Windows XP* und *Server 2003*. Diese Patches hat Microsoft erst nachgeliefert, als das Kind in den Brunnen gefallen war. Schön für Microsoft, wenn man Leute wie Arne Schönbohm und Staatssender wie die ARD hat.

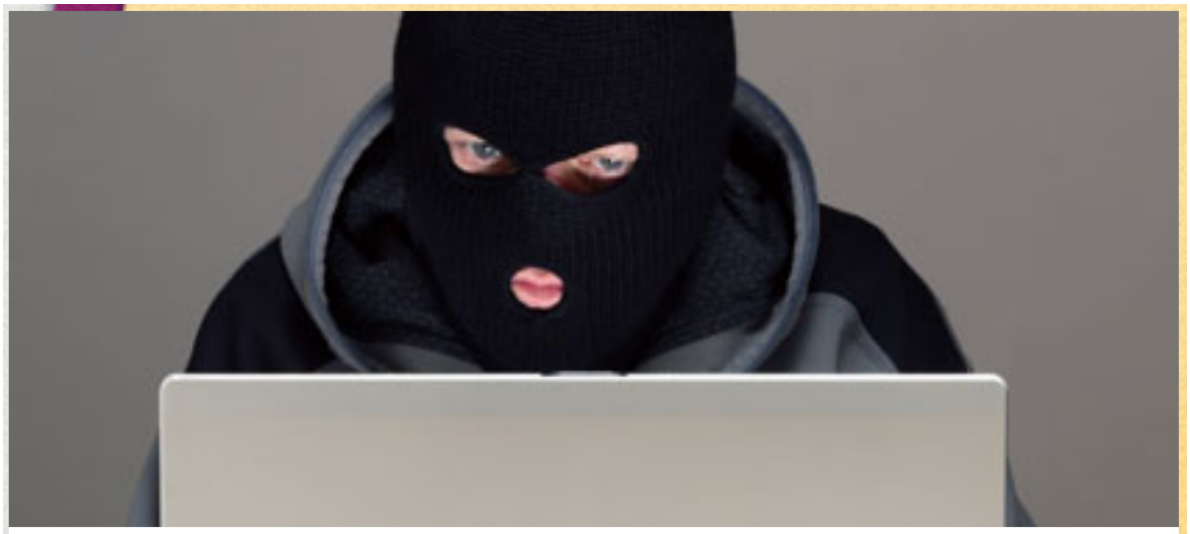
Diese Schuldzuweisung ist besonders hanebüchen, wenn man bedenkt, dass auch die Deutsche Bahn erheblich betroffen war. Dass der Präsident des BSI hier nicht die Interessen der Bürger, der Bahn oder auch die der Gesellschaft als vernetzte und verletztliche Gemeinschaft vertritt, die durch einen nächsten Angriff möglicherweise erheblich höheren Schaden erleiden kann, ist geradezu erschreckend und zeigt vor allem, mit wem Politik und Medien sich verbunden fühlen: der Wirtschaft und **nicht** dem Bürger.

Muss ich da als Beitragzahler stillhalten?

Wird der Verbraucher da zum Prügelknaben gemacht? (siehe links Schreibers Forderung)

(Geringfügig kommentierte Wiedergabe. 12. Juni 2017)

ARD: Auf den Gesprächsteilnehmer kommt es an. Was ist schon Bundeskriminalamt, wenn ich den Präsidenten des BSI, Arne Schönbohm, oder einen (fragwürdigen) Insider mit Vermarktungsinteresse die Bühne geben bzw. zitieren kann?



http://www.hr-online.de/website/fernsehen/sendungen/index.jsp?rubrik=55353&key=standard_document_61652022

Information

Gast im Studio:

Heiko Löhr
Kriminaloberrat – Referatsleiter Cybercrime
Bundeskriminalamt
65173 Wiesbaden
Telefon: 0611 550
Internet: www.bka.de

Sendung vom 17. August 2016:

Cybercrime - Betrug im Netz

Übersetzt bedeutet "Cybercrime" Computerkriminalität. Kriminelle nutzen das Internet für ihre betrügerischen Aktivitäten. Allein in Deutschland gibt es jährlich rund 45.000 bekannte Fälle (Dunkelziffer: 15 Millionen) mit einem Schadensvolumen von geschätzten 40 Millionen Euro.

Redaktion: juvo / svca Bild: © Imago (Letzte Aktualisierung: 17.08.2016, 20:36 Uhr)

Übersicht

- Was ist Malware?
- Auf welchen Wegen gelangt Malware auf den Rechner, das Tablet oder das Handy?
- Was bedeutet 'Pishing'?
- Wie erstellen Sie sichere Passwörter?
- Was sind Botnetze?
- Was ist das Darknet?

In den kommenden Jahren geht das Bundeskriminalamt davon aus, dass diese Zahlen noch dramatisch steigen werden, denn das kriminelle Milieu hat sich deutlich verändert. Es wird nicht mehr in Kleingruppen operiert, sondern es gibt eine organisierte Kriminalität, die "gewerbemäßig" und international vernetzt vorgeht. Vergleichbar mit einem Franchise-Unternehmen gehen die Täter arbeitsteilig vor, einige stellen die technischen Mittel zur Verfügung, andere sorgen für die Verbreitung der Schadsoftware. Die Beute wird anschließend aufgeteilt, z.B. 30 Prozent bekommen die Entwickler, 70 Prozent die Verbreiter.

Was ist Malware?

So erkennen Sie Phishing-Mails. Beim Surfen im Internet, beim Abrufen von E-Mails, beim Ausprobieren kostenloser Apps und Spiele, überall lauert die Gefahr sich mit bösartigen Malware (schädlicher Software wie Viren, Würmer und Trojaner) zu infizieren. Sie merken es vielleicht nicht sofort, aber genau das ist es, worauf diese Schadsoftware abzielt: Unbemerkt in ein System eindringen und die Schadfunktion ausführen.

Ein **Virus** ist ein nicht selbständig lauffähiges Programm. Es benötigt ein sogenanntes Wirtprogramm zur Ausführung. Es ist die älteste Art von Schadsoftware und kann sich selbst reproduzieren.

Ein **Wurm** ist ein selbstständiges Programm, das sich ohne große Hilfe des Anwenders auf dem PC verbreitet und dann versucht größtmöglichen Schaden anzurichten.

Ein **Trojanisches Pferd oder Trojaner** ist ein Programm, dass sich weder vervielfältigt noch kopiert. Es gefährdet aber die Sicherheit des Computers, indem es schädliche Funktionen unabhängig vom Anwender und ohne dessen Wissen ausgeführt. Trojaner gehören heutzutage zu der am meist verbreiteten Malware.

Spyware werden Programme genannt, die verschiedene Informationen über Sie als Anwender eines Computersystems sammeln und diese an Dritte weiterleiten. Zum Beispiel gehören Benutzernamen und Passwörter zu den gesammelten Informationen dieser Malware. Aber auch die Zugangsdaten Ihres Online-Bankings können Ziel dieser Schadsoftware sein.

Adware sind Programme, die ohne eine Nachfrage beim Anwender, zusätzlich zu gewünschten Programmen oder Tools installiert werden und dem Zweck der Marktforschung oder Werbung dienen.

Bei **Ransomware** (ransom=Lösegeldforderung) handelt es sich um eine Erpressersoftware. Die kriminellen Schädlinge heißen Locky, TeslaCrypt, Crytolocker oder Cryptowall. Sie arbeiten alle nach dem gleichen Prinzip: die Malware wird meist über eine E-Mail mit schädlichem Anhang eingeschleust. Danach werden die Daten auf der Festplatte verschlüsselt und Lösegeld für eine Software gefordert, die die Daten wieder entschlüsselt. In der Regel in der schwer rückverfolgbaren Digitalwährung ‚Bitcoins'. Manchmal bieten die Erpresser sogar Hilfestellung beim Umgang mit Bitcoin an. Wer nicht zahlen kann, soll Mittäter werden und wird aufgefordert zur Begleichung der "Schulden" die Malware weiter zu verbreiten. Schätzungsweise werden täglich 17.000 deutsche Rechner mit Ransomware infiziert und nicht nur Privatrechner, sondern Krankenhäuser, Behörden und Unternehmen dadurch lahm gelegt. Die Polizei ist weitgehend machtlos, da die Täter das Verschlüsselungsnetzwerk 'Tor' nutzen und dadurch ihre Identifikation verhindern. Einziger Schutz: machen Sie in regelmäßigen Abständen Backups Ihrer Dateien, z.B. auf einer USB Festplatte, die nicht permanent ans Netz angeschlossen ist.

Auf welchen Wegen gelangt Malware auf den Rechner, das Tablet oder das Handy?

1. Gefälschte Online-Shops
Kopierte und teilweise eigens dafür programmierte Online-Shops sollen Verbraucher dazu bewegen, ihre Daten preiszugeben. Die betrügerischen Internetseiten lassen die Käufer nicht nur ohne ihre Ware zurück, sie entwenden auch ihr Geld und ihre Daten.

Unser Tipp: *Seien Sie misstrauisch, wenn eine Ware sehr viel billiger ist als üblich, oder, wenn Sie ein Angebot bei einem Shop entdecken, den sie gar nicht kennen. Dann sollten Sie im Internet forschen, welche Erfahrungen andere Nutzer mit diesem Anbieter gemacht haben.*

2. Fingierte Versandbenachrichtigungen
Wenn Internetnutzer auf Pakete warten, sind sie ein leichtes Angriffsziel für Betrüger. Diese versenden getarnte Update-E-Mails zum Versand. Diese gefälschten Lieferhin-weise informieren die Versender über den Versandstatus, während sie aber tatsächlich Schadsoftware installieren.

Unser Tipp: *Sie sollten unbedingt immer den Domainnamen auf den Versandbestätigungen überprüfen und besondere Vorsicht bei solchen walten lassen, die sie nicht angefordert haben.*

3. Grußkarten
E-Cards oder elektronische Grußkarten, sind beliebt – bei Unternehmen, bei Verbrauchern und auch bei Hackern. Neben netten Wünschen können sich in Anhängen oder hinter Links Trojaner und Viren verstecken. Was besonders gemein ist, denn die nichtsahnenden Nutzer tragen fleißig zur Verbreitung bei. Denn nebenbei greifen Kriminelle die privaten Zugangsdaten ab und richten mit der gestohlenen Identität weiteren Schaden an.

Unser Tipp: *Achten Sie auf verdächtige Rechtschreibfehler im Namen des Absenders oder Unternehmens. Häufig verbergen sich dahinter Betrüger.*

4. Anti-Viren-Programme

In einem separaten Browserfenster erscheint in regelmäßigen Abständen eine Virus-Warnung. Um die angebliche Gefahr zu beseitigen, wird der Anwender dazu aufgefordert, ein angebotenes, seriös erscheinendes Anti-Virenschutzprogramm herunterzuladen. Nach Installation der vermeintlichen Antivirenlösung erscheint eine Aufforderung zum Erwerb des Programms oder auch zum Erwerb einer Lizenz. Verweigert der Nutzer dies, öffnen sich in gewissen Zeitabständen immer wieder falsche Virenwarnungen, verbunden mit einer Zahlungsaufforderung. Die angebotenen Programme haben jedoch häufig überhaupt keine Funktion. Sie dienen lediglich dazu, den Nutzer zum Kauf zu bewegen, um dadurch an die Kreditkartendaten zu gelangen.

5. SMS

Schadsoftware wie "FakeInstaller", die sich als harmloses Installationsprogramm ausgibt, gefährdet besonders Android-Smartphones. Den uneingeschränkten Zugriff auf das Betriebssystem nutzt der Trojaner dann zum massenhaften Versand von SMS an kostenpflichtige Dienste ohne die Zustimmung des Nutzers.

Unser Tipp: *Spiele und Apps nur aus vertrauenswürdigen Quellen herunterladen.*

6. Apps

Hacker nutzen täuschend echt gestaltete Apps, nicht selten mit angeblichen Empfehlungen von Prominenten oder bekannten Unternehmen. Mit diesen Apps schöpfen sie private Daten ab oder leiten Anrufe und Nachrichten um. Im schlimmsten Fall können Kriminelle so selbst gut gesicherte Systeme wie das SMS-TAN-Verfahren im Online-Banking knacken.

Unser Tipp: *Die Legitimität und die Kommentare direkt bei den Herstellern prüfen und nur solche Apps auf das Smartphone oder Tablet laden. Auch für die kostenlose App des Mobile-Games Pokémon Go gibt es mittlerweile mehr als 200 Fake-Apps, die das Smartphone oder Tablet des Benutzers ausspionieren wollen, versuchen teure Pre-mium-SMS zu versenden oder das Gerät sperren, um Lösegeld vom Nutzer zu erpres-sen. Die Original-App vom Entwickler Niantic laden Sie am sichersten direkt bei Nintendo oder in einem offiziellen App-Store herunter.*

Was sind DDoS-Attacken?

Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf einen Computer mit dem Ziel dessen Verfügbarkeit außer Kraft zu setzen.
Im Gegensatz zur DoS (Denial of Service)-Attacke erfolgt der Angriff von vielen verteilten Rechnern aus. Das Opfer wird hierzu beispielsweise mit einer Vielzahl von fehlerhaften IP-Paketen bombardiert und stellt seinen Dienst wegen Überlastung ein.

Was bedeutet 'Pishing'?

Mit Hilfe gefälschter E-Mails oder Webseiten versuchen Betrüger, an vertrauliche Daten wie zum Beispiel die Kreditkartennummer, Kontodaten oder Passwörter zu gelangen. Phishing. Das klingt nach fischen gehen – und genau so ist es auch. Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln". Immer öfter fälschen Betrüger E-Mails und Internetseiten und haben damit einen neuen Weg gefunden, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heranzukommen – die Nutzer geben ihre Daten einfach freiwillig und bedenkenlos preis.

Beispiel für Phishing: In der E-Mail werden Sie aufgefordert, Ihr PayPal-Konto zu "aktualisieren" oder zu "verifizieren", da es einen Missbrauch gegeben habe. Sie werden zur Eile gedrängt, weil sonst Ihr Konto gesperrt werden würde. Zur "Aktualisierung" werden Sie aufgefordert, auf einen Link zu klicken, der Sie zu einer gefälschten Webseite bringt. Ähnlich wie die E-Mail, kann die Webseite dem Original täuschend ähnlich sehen. Auf der Webseite sollen Sie Konto-Informationen preisgeben, die dann den Online-Betrügern zugespielt werden. Eventuell werden Sie auch dazu aufgefordert, eine bestimmte Telefonnummer anzurufen.

Was passiert wenn Sie den Link einer Phishingmail geöffnet haben?
Auch wenn Sie "nur" auf einen Link klicken, ohne auf der präparierten Internetseite Daten preiszugeben, ist dies eine gefährliche Situation. Einige Kriminelle verstecken im Quellcode der Seite ein Schadprogramm. Falls Ihr Virenschutzprogramm, Ihr Internetbrowser und/oder Ihr Betriebssystem nicht auf dem neuesten Stand sind, kann es passieren, dass Sie sich durch den Besuch dieser Seite einen Virus oder ein troja-nisches Pferd einfangen.

Der nächste Schritt für Sie lautet daher: Aktualisieren Sie Ihr Virenschutzprogramm und lassen Sie den gesamten Computer untersuchen. Prüfen Sie bei der Gelegenheit, ob Virenschutzprogramm, Internetbrowser und Betriebssystem die erforderlichen automatischen Updates machen. Ziehen Sie gegebenenfalls einen Fachmann hinzu. Falls Sie sich ein Schadprogramm eingefangen haben, prüfen Sie, ob Sie eventuell per-sönliche Daten wie PINs, Passwörter oder Sicherheitsfragen ändern müssen.

Wie erstellen Sie sichere Passwörter?

- Es sollte mindestens zwölf Zeichen lang sein.
- Es sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.
- Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter.
- Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfgh oder 1234abcd und so weiter.

Was sind Botnetze?
Von Botnetzen spricht man dann, wenn sehr viele PCs, meist mehrere Tausend, es können aber auch mehrere Millionen sein, per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden. Die Folge: Durch Botnetze ist Ihr Rechner nicht mehr nur Opfer, sondern er wird gleichzeitig auch zum Täter. Er erhält die entsprechenden Befehle und führt diese ohne Ihre Kontrolle aus. Auch Ihre, auf dem PC gespeicherten persönlichen Daten sind nun nicht mehr sicher.

Was ist das Darknet?

"Darknet", das sogenannte 'Dunkle Netz' ist der Teil des Internets zu dem nicht jeder Zugang hat. Also Server und Foren, auf die es keine öffentlichen Links gibt und die man nur auf Einladung und mit speziellen Zugangsdaten findet. Unter der Oberfläche des WWW spannt sich daher ein tiefes, undurchsichtiges Netz. Es bietet einen Schutzraum und nahezu vollständiger Anonymität, die von Drogen- und Waffenhändlern ebenso genutzt wird wie von Andersdenkenden in totalitären Regimen. Die Technik bietet somit sowohl ein Höchstmaß an Privatheit, als auch eine ausgezeichnete Gelegenheit, diese kriminell zu missbrauchen. Um in das Darknet zu kommen, muss man sich eine spezielle Software, den "Tor"-Browser herunterladen. Durch Verwendung von Tor können die Netzaktivitäten eines Internet-Nutzers nicht nachverfolgt werden (anonymes Surfen).

Datenpakete werden nach dem Zwiebelschalenprinzip, der ursprüngliche Name TOR stand für "The Onion Router", verschlüsselt zwischen Tor-Servern weitergeleitet. Jeder Tor-Server kennt dabei nur seinen Vorgänger und seinen Nachfolger, aber nicht die gesamte Ende-zu-Ende Verbindung. So wird die wirkliche IP-Adresse eines Internet-Nutzers getarnt. Eine weitere Eigenschaft von Tor ist die Möglichkeit, Dienste versteckt bereitzustellen (Hidden Services im Dark Web). Dienstleistungen und Daten im Darknet findet man nicht bei gewöhnlichen Suchmaschinen sondern beispielsweise im Hidden Wiki, das eine Sammlung von speziellen Links (erkennbar an der Endung .onion) zu Angeboten und illegalen Marktplätzen umfasst.

Bezahlt werden die Leistungen und Waren ebenfalls anonym mit Krypto-Währungen wie Bitcoins. Es handelt sich um eine Währung, die weder Scheine noch Münzen kennt. Der Name ist ein Kunstwort aus "Bit" (kleinste Speichereinheit im Computer) und "Coin" (englisch für „Münze“). Sie besteht aus berechneten, verschlüsselten Datenblöcken. Das Bitcoin-Netzwerk entstand am 3. Januar 2009 mit der Berechnung der ersten 50 Bitcoin-Blöcke. Bitcoins kauft man entweder mit herkömmlicher Währung an Bitcoinbörsen oder man bietet Waren und Dienstleistungen an und akzeptiert Bitcoins als Zahlungsmittel.

Es gibt für PC und Handy kostenlose Programme, sogenannte "Bitcoin-Brieftaschen" (engl. "Wallets"). Dort können Bitcoins "gelagert", empfangen und gesendet werden. Will man unterwegs mit Bitcoins zahlen, muss man seine Bitcoin-Brieftasche entweder dabei haben (Handy, Laptop) oder den Betrag per Internet ab¬buchen lassen. Diese Art der Währung ist allerdings noch in der Entwicklung und star¬ken Währungsschwankungen ausgesetzt.

Die meisten Seiten des Darknets sehen eher spartanisch aus, wie das Internet der 90er Jahre. Da Darknet wird von Oppositionellen beispielsweise im Iran, in Ägypten oder China genutzt. Auch Whistleblower wie Edward Snowden konnten darüber sicher kommunizieren. Journalisten nutzen es, Menschenrechtsorganisationen und verfolgte Menschen in vielen Ländern. In Deutschland gibt es schätzungsweis einige Tausend Darknet-Nutzer. Wie viele es allerdings missbrauchen, um illegale Geschäfte zu tätigen ist unbekannt. Denn natürlich gibt es im Darknet einen offenen Handel mit Waffen, Falschgeld, Ausweisdokumenten, Kreditkartendaten, Drogen aller Art und Kinder¬pornografie. Trojaner-Entwickler, Betrüger oder Auftragsmörder bieten hier ihre Dienste gegen Entgelt an.

Danach werden in vielen EU-Staaten "Dekorations- und Salutwaffen" von Spezialisten bearbeitet und als scharfe Waffen im Darknet angeboten. Eine solche scharf gemachte Dekorationswaffe hatte sich der Amokläufer in München besorgt. Dabei hatte er offenbar im Darknet über ein Jahr nach exakt dem Modell gesucht, das der schwedische Rechtsterrorist Breivik bei seinem Massenmord benutzte. Bei einem zweiten Händler kaufte er sich Munition und ließ sich die Waren an eine Packstation liefern.

Warum ist das Surfen im Darknet gefährlich?
Die Anonymität der Untergrundseiten bietet eine ideale Möglichkeit, üble Geschäfte abzuwickeln. Das zeigen auch die Suchrubriken. Neben banalen Rubriken wie "Kochrezepte" finden sich hier solche wie "Killerdienste", "Geldwäsche", "Drogengeschäfte" – oder eben "Filme". Im Darknet sind beispielsweise illegale Film-Downloads und raubkopierte Musik nur einen Mausklick entfernt. Sie sind einer der Hauptgründe, weshalb auch "normale" Internet-Nutzer den Weg ins Darknet gehen. Wer sich allerdings auf das verlockende Angebot einlässt, riskiert hohe Geldstrafen und verseucht seinen PC möglicherweise mit Schadsoftware. Denn natürlich sind Kopien urheberrechtlich geschützter Materialien illegal und wer im Darknet unterwegs ist, macht sich nicht nur mit dem Download von Raubkopien strafbar.

Jeder kann unbewusst zum Mittäter krimineller Geschäfte werden. Die laufen nämlich über alle PCs, deren Tor-Browser-Einstellung "Relais-Verkehr" erlaubt. Welche Daten dann über den eigenen PC ge-schleust werden, lässt sich nicht mehr kontrollieren. So macht sich der Nutzer unter Umständen nichts ahnend zum Komplizen von Kinderschändern. Und noch weitere Gefahren drohen: Viren, Trojaner und andere Schädlinge sind im Darknet ebenfalls in großer Menge vorhanden.