2018

c't Security

Sicherheitsratgeber 2018 für Internet & PC

Die Waffen der Hacker

Ihr PC in fremder Hand:
So leicht werden Sie zur Beute

Hardware absichern

Wie Profis Einbrüche verhindern

PC & Identität schützen

Tipps gegen den Account-Missbrauch

Die neue Passwort-Strategie

Eine Passphrase ersetzt Zeichensalat

Windows abhärten

Zum Download: c't-Tool mit Microsoft-Technik

Hacking-Gadgets ausprobiert

Keylogger, TV-Jammer und USB-Zerstörer im Einsatz

MAXIMALE LEISTUNG. PREMIUM SCHUTZ. TOP ENTSCHEIDUNG.

SG UTM & XG Firewall jetzt mit neuer Hardware

SG UTM und XG Firewall:

Jetzt mit Deep Learning – integriert in Sophos Sandstorm.

- Weitaus effektiver als herkömmliches Machine Learning
- Erkennt Malware komplett ohne Signaturen
- Schützt selbst vor völlig unbekannten Bedrohungen

www.sophos.de/firewalls

SOPHOS

Prämierte Firewalls mit Spitzentechnologie

Business Antivirus – PLATIN – Readers' Choice Security Insider AWARD 2017
Platin-Award „Business Antivirus" von SecurityInsider

Enterprise Firewalls – PLATIN – Readers' Choice Security Insider AWARD 2017
Platin-Award „Enterprise Firewalls" von SecurityInsider

SOPHOS NEXT GENERATION FIREWALL NSS RECOMMENDED
Sophos XG Firewall – Beste Firewall im Test der unabhängigen NSS Labs

Produkt des Jahres
ITK-Produkt des Jahres im Bereich „Cybersecurity" von der Funkschau

Readers' Choice eGovernment AWARDS 2017 Identität & Sicherheit – PLATIN –
Platin-Award „Identität und Sicherheit" von eGovernment Computing

SEE THE FUTURE

Sophos Dialog für IT-Sicherheit 2018 – Roadshow in DE | AT | CH
Jetzt anmelden und mehr erfahren: www.sophos-events.com/security

Liebe Leserinnen, liebe Leser,

Meltdown & Spectre, Yahoo-Hacks, WannaCry, Crypto-Trojaner … – allen, die heute mit moderner Technik umgehen, muss bewusst sein, dass sie an vielen Fronten bedroht werden. Computerkriminalität ist ein einträgliches, vielseitiges und professionell organisiertes Geschäft: Der Handel mit erbeuteten Identitäten blüht. Gekaperte Rechner werden untervermietet. Gezielte Angriffe richten sich gegen große Organisationen und Regierungen. Die Tricks und Werkzeuge sind mittlerweile auch für Nicht-Profis zugänglich und nutzbar.

Einblicke in derlei Treiben, wie sie das Heft mit den Waffen der Hacker und den ausprobierten Hacking-Gadgets gibt, sind eine Momentaufnahme. Die stillt hoffentlich nicht nur die technische Neugierde, sondern sie sollte zugleich auch Motivation sein, das eigene Handeln zu hinterfragen: Schützen Sie Ihre eigene digitale Identität hinreichend? Genügen die gewählten Passwörter? Welche Technik schützt eigentlich wovor? Was können Sie tun, wenn der Schutz nicht gereicht hat?

Konkrete Tipps liefert dieses Heft auch für die Konfiguration der Hardware – wir zeigen, was Profis tun und was davon Sie auch auf Ihrem PC umsetzen können. Mit dem c't-eigenen Werkzeug Restric'tor erreichen Sie darüber hinaus einen hohen Schutz, den Microsoft selbst in Windows zwar eingebaut, aber nur für professionelle Nutzung vorgesehen und nutzbar gemacht hat.

Ein Tipp vorab: Kombinieren Sie die für Ihre Nutzungsgewohnheiten passenden Techniken zu einem eigenen Schutzkonzept, das sich im Alltag immer aufrecht halten lässt – manchmal ist weniger mehr.

Peter Siering

INHALT

Gefahren verstehen

Jeden Tag entdecken Experten neue Lücken, oft solche, die jahrelang vermeintlich unbemerkt geblieben sind. Solche Fälle sollten die Augen öffnen, dass Sicherheit heutzutage kein dauerhaft erreichbarer Zustand ist.

PC und Identität schützen

Techniken, um die Sicherheit zu erhöhen, gibt es wie Sand am Meer. Wir wägen ab, welche unter welchen Umständen hilft. So finden Sie das für Sie geeignete Maßnahmenbündel.

Windows abhärten

Microsoft hat viele Sicherheitsverbesserungen für Windows entwickelt. Doch manche Technik lässt sich erst im professionellen Umfeld nutzen. Unser Restric'tor aktiviert diese Funktionen auch auf Ihrem PC zuhause.

Hardware absichern

Nicht nur Software ist angreifbar, sondern auch die Hardware. Wir haben Tipps von Profis, wie auch PCs und Notebooks sicherer werden, und zeigen Abhilfen gegen die größeren Eseleien von zentralem Verwaltungswahn.

Passwort-Strategie

Die Empfehlungen für Passwörter ändern sich alle paar Jahre, einfach anwendbar sind sie nicht immer. Wir gehen von der Richtlinie der Passwortpropheten des NIST für die US-Behörden aus und leiten daraus ein sicheres und zugleich pragmatisches Vorgehen ab.

Schaden begrenzen

Wer trotz aller Bemühungen Opfer von Sicherheitslücken oder Identitätsdiebstahl wird, sollte zügig die richtigen Schritte unternehmen, um den Schaden zu begrenzen.

Hacking-Gadgets

Böse, billig und leicht zu erwerben: Der Markt für Hacker-Werkzeuge floriert. Wir haben die spannendsten Produkte ausprobiert und erklären, wie sie funktionieren.

Die Waffen der Hacker

Ohne eine gewisse Sicherheitshygiene auf Ihren digitalen Begleitern haben die Geschäftemacher im Netz leichtes Spiel. Unser Blick hinter die Kulissen zeigt, wie diese die Schutzfunktionen überwinden, um die gekaperten Geräte in ihre Bot-Netze einzubinden.

Zum Heft

Christof Windeck, Olivia von Westernhagen, Axel Vahldiek

Sicherheitslücken in modernen Prozessoren

Unter dem Namen Meltdown und Spectre sind seit Anfang Januar 2018 gravierende Fehler in Prozessoren von Intel, AMD und vielen anderen Herstellern bekannt. Sie stellen, was ungewöhnlich ist, keine konkreten, sondern konzeptionelle Lücken dar. Mit Updates für die meisten aktuellen Betriebssysteme, für Browser und andere Software versucht man, mögliche Angriffe zu erschweren. Dennoch dürften die Auswirkungen die IT noch lange auf Trab halten.

Es ist eine Katastrophe für die Hersteller von Prozessoren, Betriebssystemen, Browsern, Computern, Servern und Smartphones: Sicherheitsforscher haben drei kritische Lücken in den meisten aktuellen Intel-Prozessoren ausgemacht und Anfang Januar Details dazu veröffentlicht; zwei betreffen auch die Prozessoren von AMD sowie einige mit ARM-, POWER- und SPARC-Mikroarchitektur.

Die Entdecker haben die Lücken Meltdown und Spectre getauft; das bedeutet so viel wie (Kern-)Schmelze und Phantom, Schreckgespenst. Es geht um drei Angriffsmöglichkeiten, die sich ungefähr so beschreiben lassen: Eine laufende Anwendung kann RAM-Inhalte auslesen, auf die sie eigentlich keinen Zugriff haben sollte. Meltdown und Spectre hebeln die bisher als zuverlässig angenommene Trennung von RAM-Bereichen aus – allerdings auf Umwegen, etwa über Caches. Man spricht daher von Seitenkanalangriffen (Side Channel Attacks).

Die Sicherheitslücken ermöglichen es, vermeintlich gut geschützte Daten wie Passwörter abzugreifen. Deshalb sind – oft in Hauruckmanier – erste Updates erschienen für Betriebssysteme (Windows, macOS, Linux, iOS, Android, FreeBSD und so weiter), Browser, NAS-Speicherboxen, Grafiktreiber und manche Anwendungen.

Mehrere voneinander unabhängige Projektgruppen haben die beiden Sicherheitslücken entdeckt und detailliert in Blogs und Whitepapers beschrieben: Googles Project Zero, Mitarbeiter des Unternehmens Cyberus Technology und zwei Teams aus Mitarbeitern mehrerer Universitäten waren daran beteiligt – darunter auch Forscher von der TU Graz, die bereits zwei Jahre zuvor mit neuen Erkenntnissen zum RAM-Konstruktionsfehler Rowhammer auf sich aufmerksam gemacht hatten.

Gerüchte über eine schwerwiegende Sicherheitslücke in Intel-CPUs hatten schon um die Jahreswende die Runde gemacht. Auslöser war vor allem das hohe Tempo, mit dem Windows- und Linux-Kernel-Entwickler an der Implementierung eines Sicherheitsmechanismus namens „Kernel Page-Table Isolation“ (KPTI) arbeiteten. Die konkreten Angriffstechniken, die es abzuwehren galt, blieben zunächst geheim; erst am 3. Januar machten die Entdecker Details der Öffentlichkeit zugänglich. Später stellte sich heraus, dass die Forscher die betroffenen Hard- und Software-Hersteller bereits im Juni 2017 informiert hatten, um ihnen ausreichend Zeit für Reparaturen zu geben. Im Zeitraum bis zum offiziellen Bekanntwerden der Lücke haben AMD, Intel, Microsoft, Apple und zahllose andere Firmen demnach bewusst sicherheitsanfällige Chips und Geräte verkauft.

Meltdown & Spectre im Detail

Meltdown (CVE-2017-5754), von Google auch „Rogue Data Cache Load“ genannt, bringt die strikte Trennlinie zwischen User- und Kernel-Mode zum Schmelzen und ermöglicht unprivilegierten Angreifern bei den meisten Betriebssystemen Zugriff auf den gesamten Arbeitsspeicher. Voraussetzung für diese Angriffstechnik ist, dass Prozesse im User-Mode mit einer Seitentabelle arbeiten, die nicht nur ihre eigenen, sondern auch sämtliche virtuellen Speicheradressen des Kernels auflistet.

Das traf bis zur Veröffentlichung der Lücke und den ersten Patches auf alle gängigen Betriebssysteme zu. Die implementieren einen „Page Table Isolation“ (PTI) genannten Schutzmechanismus im Kernel (daher auch Kernel PTI/KPTI genannt). Er basiert auf einer von ihren Erfindern ursprünglich als KAISER (Kernel Address Isolation to have Side-channels Efficiently Removed) bezeichneten Technik. Diese vollzieht eine Trennung der Seitentabellen für Kernel- und User-Mode, auch „Page Table Splitting“ genannt. Hierzu dient eine Tabellen-Kopie („Shadow Page Table“), in der ein laufender Prozess nur noch seinen eigenen Speicherbereich sowie einige kleine Speicherbereiche des Kernels sieht, die für Systemaufrufe und Interrupts benötigt werden. Die Originaltabelle samt Mapping des vollständigen Adressraums ist nur noch im Kernel-Mode erreichbar.

Hinter der zweiten Lücke namens **Spectre** verbergen sich zwei unterschiedliche Angriffsszenarien. Variante 1 (CVE-2017-5753) wird von Google auch als „Bounds Check Bypass“, Variante 2 (CVE-2017-5715) als „Branch Target Injection“ (BTI) bezeichnet. Die Proof-of-Concept-Code-Veröffentlichungen zu den Spectre-Angriffstechniken zielen bislang zwar nur auf Programme im User-Mode ab. Es scheint jedoch nicht ausgeschlossen, dass auch der Kernel-Code gefährdet ist: Die Linux-Entwickler arbeiten bereits seit einiger Zeit an Patches, die das Betriebssystem absichern sollen. Anders als bei Meltdown löst der Spectre-PoC aber keine Exception aus. Stattdessen „trainiert“ er ein weiteres Feature moderner Out-of-Order-Execution-fähiger Prozessoren – die Branch-Prediction. Sie dient der Adress-Vorhersage von Sprungbefehlen anhand von Erfahrungswerten.

Ein Angreifer, der Spectre ausnutzen will, trainiert den Branch-Predictor mittels einer ausreichenden Anzahl von Wiederholungen so, dass der angegriffene Code bei bestimmten Programmverzweigungen einen für ihn vorteilhaften Zweig wählt. Ziel dieser Vorgehensweise ist es, ähnlich wie bei Meltdown, mittels spekulativer Befehlsausführung auf fremde Speicherinhalte zuzugreifen und dadurch Spuren im Cache zu hinterlassen. Dieser dient dem Angreifer dann wiederum als verdeckter Kanal, über den er die gewünschten Inhalte mittels zeitbasierter Side-Channel-Angriffe wie Flush & Reload oder auch Evict & Reload rekonstruieren kann.

Loch im RAM-Zaun

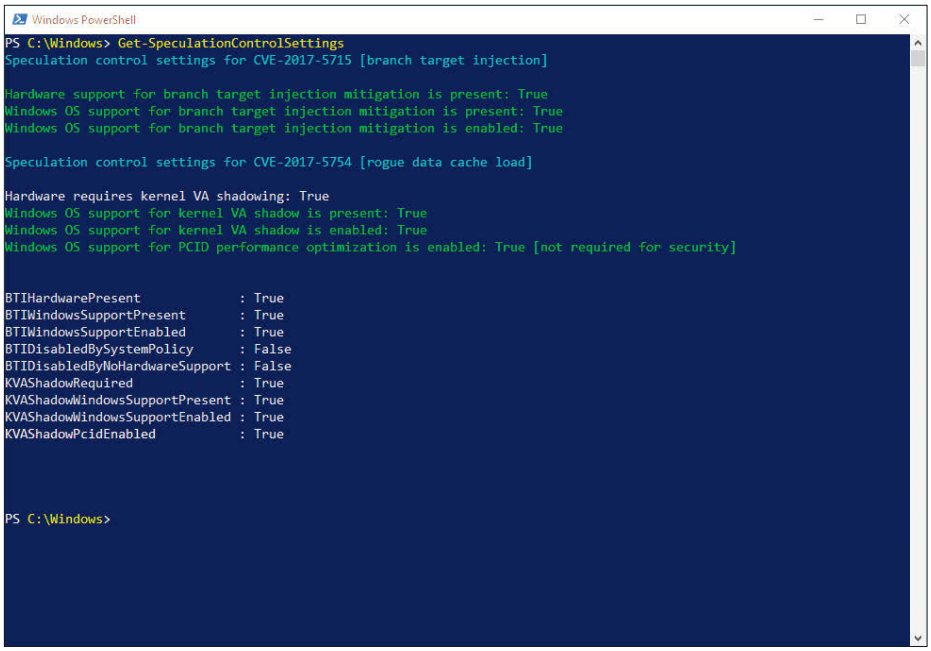
Die gegenseitige Abschottung von Speicherbereichen ist ein Grundpfeiler der IT-Sicher-

Die CPU-Sicherheitslücken Meltdown und Spectre

Google-Name	Kurzbezeichnung	CVE-Nummer	betroffene Prozessoren und jeweilige Patches			
			Intel	AMD	ARM1	IBM POWER
Spectre, Variante 1	Bounds Check Bypass	CVE-2017-5753	✓ (A, B)	✓ (A, B)	✓ (A, B)	✓ (A)
Spectre, Variante 2	Branch Target Injection (BTI)	CVE-2017-5715	✓ (A, B, C)	✓ (A, C[2])	✓ (A)	✓ (A, C[3])
Meltdown	Rogue Data Cache Load	CVE-2017-5754	✓ (D)	–	✓[4]	–

A: Updates für Betriebssystem und mitgelieferte Browser (IE, Edge, WebKit) vom Hersteller des Betriebsssystems
B: Updates von separaten Anwendung(en), Browsern, Virenscannern und/oder Treibern von den jeweiligen Herstellern
C: CPU-Microcode-Update, bei Windows via BIOS-Update, bei vielen Linuxen via Distributions-Update
D: Update für Betriebssystem (PTI); Prozessoren ab Haswell (Core i-4000/Xeon E5 v3) reduzieren PTI-Bremswirkung mit PCID

[1] betroffen sind Cortex-A8, -A9, -A15, -A17, -A57, -A72, -A73, -A57, -R7, -R8, also etwa nicht der Cortex-A53 im Raspi
[2] laut AMD nur geringes Risiko „nahe Null“, trotzdem „optionale“ Microcode-Updates für Ryzen/Epyc, später für ältere Prozessoren
[3] Firmware-Update für POWER7+, POWER8, POWER9
[4] nur Cortex-A75, der noch nicht in einem Chip erschienen ist



Windows-Nutzer können per PowerShell-Skript prüfen, wie Ihr PC hinsichtlich der Meltdown- oder Spectre-Lücken aufgestellt ist – alternative Prüfmethoden für Windows liefern oft unzutreffende Resultate.

heit. Passwörter und Verschlüsselung wären nicht mehr sicher, wenn ein Prozess einfach nach Belieben Daten im Hauptspeicher (RAM) auslesen könnte, also die anderer Prozesse und besonders die des Betriebssystems. Besonders hart treffen die Lücken Cloud-Rechenzentren, in denen virtuelle Maschinen Daten unterschiedlicher Kunden auf demselben Server verarbeiten.

Meltdown und Spectre missbrauchen Funktionen, die in Milliarden von Prozessoren stecken: Out-of-Order-Execution (OoOE), Speculative Execution und Branch Prediction. Intel hat OoOE vor rund zwanzig Jahren mit dem Pentium Pro eingeführt: Falls der Prozessor mit der Ausführung eines Befehls warten muss, etwa auf Daten aus dem RAM, verarbeitet er schon einmal einen anderen Befehl, der eigentlich erst später an der Reihe wäre. Er arbeitet Code also nicht in der Reihenfolge ab, wie sie im Programm steht (In Order), sondern in einer anderen, optimierten: Out of Order.

Aus demTritt gekommen

Programmcode enthält außerdem Bedingungen, durch die sich der Ablauf verzweigt (Branching). Sprungvorhersageeinheiten versuchen, die vermutlich als Nächstes wichtigen Speicheradressen zu erraten (Branch Prediction). Falls Ressourcen frei sind, führt die CPU Befehle schon einmal auf Verdacht aus (Speculative Execution), obwohl sie vielleicht doch nicht nötig sind – dann werden die Resultate verworfen. Doch unter anderem dank KI-Algorithmen wie neuronalen Netzen erzielen moderne Sprungvorhersageeinheiten hohe Trefferraten und steigern die Rechenleistung erheblich. Würde man OoOE, Branch Prediction und Speculative Execution abschalten, um Sicherheitslücken zu schließen, würde die Performance drastisch sinken.

Zum Schließen der Meltdown-Lücke, die nur Intel-Prozessoren betrifft, sind tiefgreifende Änderungen am Kernel des Betriebssystems nötig. Sie trennen die Speicher-Adressbereiche des privilegierten Betriebssystem-Kernels gründlicher von denen laufender Programme im sogenannten „User Space“. Die Technik nennt man auch Page Table Isolation (PTI). Jüngere Intel-Prozessoren ab der vierten Core-i-Generation (Haswell, Core i-4000, Xeon E5 v3) beherrschen eine Funktion namens Process-Context Identifier (PCID). Diese reduziert Leistungseinbußen durch PTI. Bei älteren (vor 2013) und schwächeren Prozessoren bremsen die Sicherheitsupdates stärker als bei modernen.

Sicherheitsforscher von AV-Test haben entsprechend Anfang Februar schon 140 verschiedene Malware-Samples gezählt, die darauf hindeuten, dass Malware-Autoren fleißig mit dem Proof-of-Concept-Code experimentieren. Konkrete Angriffe per Meltdown und Spectre sind auch im März noch keine bekannt. Die Lücken lassen sich auch nicht für Remote-Angriffe via Ethernet oder WLAN nutzen, weil der Schadcode auf dem angegriffenen System selbst laufen müsste. Deshalb sind viele Embedded Systems und Router nicht direkt angreifbar. Über sonstige Lücken lassen sich Meltdown und Spectre womöglich jedoch nutzen, um größeren Schaden anzurichten.

Linderung statt Heilung

Intel, Microsoft und die Entdecker der Lücken sprechen interessanterweise nicht davon, die Sicherheitslücken zu schließen. Stattdessen verwenden sie durchweg den englischen Begriff „Mitigation“, der so viel bedeutet wie Abschwächung oder Linderung. Die Spectre-Entdecker vermuten, dass noch weitere Schwachstellen in den erwähnten CPU-Funktionen schlummern, und sie erwarten, dass sich die Lücken erst mit künftigen, in der Hardware veränderten Prozessoren ganz schließen lassen werden.

Bei aktuellen Intel-Systemen lässt sich Branch Target Injection (BTI) nur dann erschweren, wenn der Prozessor ein sogenanntes Microcode-Update erhält. Es rüstet drei neue Funktionen nach, um Software robuster zu machen. Dieses Update hat Intel zuerst für Prozessoren geliefert, die seit 2013 ausgeliefert wurden. Solche Updates hängen oft vom jeweiligen Systemhersteller ab: Der muss die Microcode-Updates in neue BIOS-Versionen einfügen, die er dann als BIOS-Updates ausliefert. Die muss der Besitzer des PCs, Notebooks, Servers oder Mainboards dann einspielen.

Über ein optionales Update (siehe ct.de/wq8u) hat Microsoft in Windows 10 erstmals Microcode-Updates gegen die Spectre-Lücke ausgeliefert. Vorerst enthält das Update nur den Code für ausgewählte Skylake-Prozessoren. Linux-Nutzer sind etwas besser dran: Viele Distributionen bringen CPU-Microcode-Updates automatisch.

Besonders bedrohlich sind die Spectre-Lücken für Software, die einerseits Daten aus dem Internet lädt und andererseits sensible Informationen verarbeitet. Das gilt vor allem für Browser: Sie laden ausführbaren Code wie JavaScript und HTML5 von Webseiten und senden Passwörter – oder speichern sie sogar. Daher enthalten die Updates für Windows und macOS auch Updates für die integrierten Browser. Wer Chrome, Firefox oder andere Browser nutzt, muss auch hier auf Updates achten. Den Schutz verstärken Skriptblocker wie NoScript.

Meltdown und Spectre werden die IT-Branche noch eine Weile beschäftigen. Wann erste Prozessoren ohne diese Fehler erscheinen, lässt sich derzeit nicht einschätzen; es dürfte länger als nur ein paar Monate dauern. (ciw) c't

Prüfwerkzeug und optionales Update für Windows 10: ***ct.de/wq8u***

© fotolia, Kurt Kleemann

heise Security Tour

Thema 2018

Wissen schützt

10. April, **Stuttgart** • 12. April, **München** • 18. April, **Wien** • 24. April, **Köln** • 26. April, **Hamburg**

100 % unabhängig
hochkarätig • praxisrelevant

AUSZUG AUS DEM PROGRAMM

Gefahr erkannt, Gefahr gebannt –
Sinnvolle Reaktion durch Kenntnis der IT-Sicherheitslage
// Klaus J. Keus (D)

Malware-Analyse für Admins – Hilfestellung für die Praxis
// Christoph Fischer

Anforderungen der DSGVO an die IT-Sicherheit
// Joerg Heidrich (D) / Max Mosing (A)

Sicherheit beim Namen nennen – DNS als Sicherheitsinstrument
// Carsten Strotmann

Wie man Attribution richtig macht
// Tillmann Werner

Teilnahmegebühr (inkl. MwSt.): 599,00 Euro

© fotolia, honksantima

www.heisec.de/tour

Sponsoren

COMPASS SECURITY · CONSIST Business Information Technology · CROWDSTRIKE · mimecast · VARONIS

Eine Veranstaltung von heise Security

Organisiert von heise Events

Bild: Albert Hulm

Jürgen Schmidt

Die Tricks und Techniken aktueller Ransomware

Das Jahr 2017 hat einige entscheidende Neuerungen bei Erpressungstrojanern gebracht. WannaCry, Petya/NotPetya & Co. setzten beispielsweise auf neue Verbreitungswege und hatten zum Teil weitere Schädlinge im Gepäck. Insbesondere Firmen und Behörden stehen stärker im Fokus der Kriminellen als je zuvor.

Die Erpressung mit verschlüsselten Daten hat sich seit 2016 als einer der profitabelsten Geschäftsbereiche der Malware-Szene etabliert. Kein Wunder: Anders als etwa beim Online-Banking-Betrug sind sowohl die technischen als auch die organisatorischen Anforderungen so niedrig, dass auch minderbegabte Kleinkriminelle auf den Zug aufspringen können: Software, die Dateien verschlüsselt, und ein Bitcoin-Konto sind kein Hexenwerk – und außerdem im Rahmen von Angeboten zu „Ransomware as a Service“ bereits im Paket mit dabei.

Doch 2017 hat sich einiges getan. Die wohl größte Neuerung ist die Form der Verbreitung: Klassiker wie Locky & Co. landen primär über E-Mails bei den potenziellen Opfern; sogenannte Drive-by-Infektionen durch Webseiten mit Schadcode sind der zweite wichtige Weg, auf dem Ransomware Systeme der Opfer infiziert. WannaCry jedoch nutzte im Mai erstmals eine Windows-Lücke aus dem NSA-Arsenal (EternalBlue), um sich wie ein Wurm selbsttätig im Netz weiter zu verbreiten. Die Infektion erfolgte völlig ohne Zutun der Anwender. Noch hinterhältiger war NotPetya, der heimlich über den Update-Mechanismus einer legitimen Software auf das System kam. Von dort aus verbreitete er sich ebenfalls über die EternalBlue-Lücke im Windows SMB-Stack weiter. Doch diese beiden Formen der Verbreitung werden wohl die Ausnahme bleiben. Wurm-taugliche Sicherheitslücken in PCs sind sehr selten und Malware über reguläre Updates einzuschleusen lässt sich ebenfalls nicht beliebig wiederholen.

Erpressung und Spionage

Allerdings sehen Malware-Analysten mittlerweile vermehrt Angriffe auf Firmen, die primär das Ziel haben, dort Erpressungstrojaner zu platzieren. Das sind dann beispielsweise angebliche Bewerbungen, die sich auf tatsächliche Stellenanzeigen der Firma beziehen und an die Personalabteilung adressiert sind. Nachdem der Rechner des Personalers infiziert wurde, breiten sich die Angreifer von dort aus weiter im Netz aus, suchen und übernehmen Systeme mit wichtigen Daten und verschlüsseln Dateien dann sehr koordiniert überall gleichzeitig. Ein weiteres, aktiv genutztes Einfallstor sind Remote-Desktop-Dienste (RDP). Die Crysis-Gang sucht in großem Stil erreichbare RDP-Ports und versucht deren Zugangsschutz mit einfachen Passwörtern auszuhebeln. Haben sie damit Erfolg, laden sie die Crysis-Ransomware herunter und infizieren das System.

Ransomware-Angriffe auf Firmen ähneln in der Vorgehensweise und den eingesetzten Tools immer häufiger professionellen Spionage-Angriffen. In manchen Fällen sind sich die Forensiker, die die Vorfälle untersucht haben, sogar recht sicher, dass es den Angreifern eigentlich um Spionage ging. Die vorgefundene Ransomware war nur ein kleines „Abschiedsgeschenk“, das zwei Fliegen mit einer Klappe schlagen sollte: Zum einen vernichtet man damit Spuren und zum anderen ergibt sich ja vielleicht auch noch eine nette Nebeneinkunft.

Pay per Install

Außerdem bandeln die Ransomware-Autoren offensichtlich mit der etablierten Crimeware-Szene an. So erklärte uns Holger Unterbrink von Ciscos Threat-Research-Abteilung Talos, dass er bereits mehrfach Fälle gesehen habe, in denen die Opfer nach einer Bezahlung zwar den Schlüssel für den Zugang zu ihren Daten erhielten und ihre Daten auch zurück bekamen – sich aber weitere Schadsoftware auf dem System befand. Da hatte dann etwa ein Exploit Kit auf einer Website im Kombi-Pack mit dem Erpressungstrojaner einen Bitcoin-Miner geliefert, der dann natürlich nach der Datenwiederherstellung munter weiter schürfte.

Es ist durchaus üblich, dass Malware auf Befehl ihres Herrn und Meisters auch nachträglich noch andere Schadprogramme installiert. Da lädt dann etwa der Online-Banking-Trojaner nach getaner Arbeit noch Locky oder eine andere Erpressungssoftware nach.

WannaCry war der erste Erpressungstrojaner, der sich in Netzwerken wurmartig weiter verbreitete.

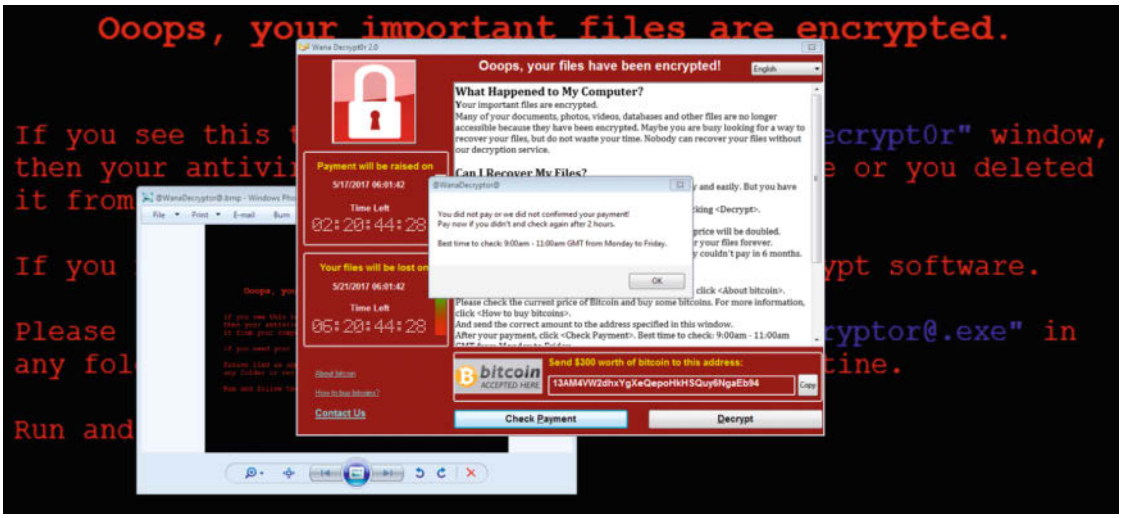


Bild: Checkpoint

„Pay per Install" nennt sich dieses ursprünglich aus der Freeware-Szene stammende Geschäftsmodell, das sich auch in der Malware-Community durchgesetzt hat. Wer eine große Zahl an Installationen vorweisen kann – also entweder beliebte Freeware vertreibt oder große Bot-Netze administriert –, hilft dabei Dritten gegen kleine Provision bei der Verbreitung ihrer Software.

Bröckelndes Image

Insgesamt hat die Ransomware-Szene sehr bewusst an dem Ruf gearbeitet, dass man nach dem Bezahlen des Lösegelds auch eine realistische Chance hat, wieder an seine Daten zu kommen. Die Jigsaw-Gang bot bei Problemen sogar einen Chat als Hotline-Service an. Das zahlt sich aus.

Auch wenn etwa das BSI nicht müde wird, vor den Risiken zu warnen, ringen sich vor allem Firmen und auch Behörden mittlerweile regelmäßig dazu durch, der Erpressung nachzugeben und die geforderte Summe zu bezahlen. Symantec ermittelte, dass in den USA rund 64 Prozent der Betroffenen das Lösegeld entrichten; für Deutschland konnten wir keine konkreten Zahlen finden, aber Insider schätzen, dass auch hier über die Hälfte der Firmen blecht.

Diese Zahlungsbereitschaft steht und fällt mit der Zuversicht, dass man eine reelle Chance hat, seine Daten zurückzubekommen. Und wenn man ehrlich ist, stimmt das in den meisten Fällen auch. Allerdings zeigt dieses Bild erste Risse. So gibt es immer mehr Erpresser, deren Software die technischen Voraussetzungen für eine Wiederherstellung gar nicht an Bord hat. Malware-Experten sprechen dann von Wipern, weil die Schadsoftware die Daten praktisch löscht. Der bislang prominenteste Wiper war NotPetya/Petya/Netya – je nach Namensgeber. Der überschrieb Daten des Boot-Sektors unwiederbringlich und machte sich nicht einmal die Mühe, eindeutige IDs für seine Opfer zu erstellen. Selbst wenn sie es wollten, könnten die Kriminellen einem Opfer keinen Schlüssel zu dessen Daten liefern. Nach aktuellem Kenntnisstand hat auch wirklich kein einziges NotPetya-Opfer seine Daten zurückbekommen. Bei NotPetya handelte es sich vermutlich um eine politisch motivierte Kampagne, bei der Erpressung nur als Kulisse diente. Doch dessen Vorgehen ahmen immer mehr Gauner nach, denen es vor allem um die schnelle Bitcoin geht, erklärt Unterbrink gegenüber c't. Sie sparen sich den ganzen Aufwand mit den Schlüsseln, kassieren ab und tauchen dann wieder unter. Dass sie damit das Image der Branche ruinieren und irgendwann darunter die Zahlungsmoral leiden wird, ist ihnen dabei egal.

Lukratives Millionengeschäft

Es ist schwer, die Schäden durch Ransomware zu beziffern. Klar ist, dass es sich für die Cyber-Kriminellen um ein äußerst lukratives Millionengeschäft handelt. Für die Opfer liegt der Schaden durch die von der Ransomware verursachten Verluste noch um ein vielfaches höher. Der deutsche Konzern Beiersdorf schätzt die eigenen NotPetya-Verluste durch Verzögerungen bei Versand und Produktion auf etwa 35 Millionen Euro; andere Firmen meldeten ähnliche Zahlen. Allein WannaCry und NotPetya verursachten somit Schäden im Milliardenbereich.

Zusammenfassend kann man feststellen, dass Ransomware zur beliebtesten Schädlingsgattung der Cyber-Kriminellen avanciert ist. Der Fokus der Angriffe hat sich ein wenig auf den Firmenbereich verschoben, weil dort angesichts des drohenden materiellen Schadens die Zahlungsbereitschaft größer ist als bei Privatpersonen. Außerdem kann man bei Firmen mit höheren Lösegeldforderungen weit über 1000 Euro operieren. Für Firmen ist Ransomware somit die derzeit größte Bedrohung für ihre Daten. Doch auch für Endanwender gibt es keineswegs Entwarnung: Die Macher von Locky, Cerber & Co. werden auch 2018 munter auf Sie losgehen.

Was tun?

Wenn es Sie erwischt hat, sollten Sie keinesfalls einfach zahlen. Erstatten Sie Anzeige und versuchen Sie auf jeden Fall zunächst, mehr über die Malware herauszufinden. Dienste wie ID Ransomware (siehe ct.de/whjy) helfen dabei, den Typ des Erpressungstrojaners zu identifizieren. Trauen Sie sich das nicht selbst zu, ziehen Sie Spezialisten zu Rate.

Bei einem bekannten Wiper ist der Fall hoffnungslos – das Geld wäre verschwendet. Auch nach einer Bezahlung bekommen Sie Ihre Daten nicht zurück. Bei manchen Erpressungstrojanern wurde die Verschlüsselung geknackt, sodass sich die Daten auch ohne Bezahlung wiederherstellen lassen. Die Macher von Crysis haben auch bereits mehrfach Master-Keys für ihre Software veröffentlicht. Warum, ist nach wie vor unklar. Vielleicht ging es einfach nur darum, den Kunden ein kostenpflichtiges Update der Mietsoftware aufzuzwingen. Jedenfalls kann man mit dem Master-Key ebenfalls ohne Lösegeld an die Daten kommen. Erst als allerletzte Option sollten Sie eine Bezahlung ins Auge fassen. Hat es Sie noch nicht erwischt, ist jetzt ein sehr guter Moment, sich über Schutzmaßnahmen Gedanken zu machen. Wie Sie speziell gegen Trojaner vorgehen können, erfahren Sie in den Artikeln ab Seite 24 und Seite 44. (des) c't

Ransomware identifizieren: ***ct.de/whjy***

Olivia von Westernhagen

Heimliches Krypto-Mining auf Webseiten

Seit einigen Monaten nutzen gewiefte Kriminelle die Rechenleistung fremder CPUs für ihre persönliche Bereicherung. Der neue Trend nennt sich „Cryptojacking" – und ein Ende ist nicht abzusehen.

Die Webseite „The Pirate Bay" experimentierte im Herbst 2017 mit einem JavaScript-Schnipsel, der CPU-Leistung der Besucher zum Schürfen einer Kryptowährung abzwackte, ohne um Erlaubnis zu fragen. Seitdem hat sich heimliches Mining im Web-Browser zu einem unerfreulichen Trend entwickelt, der auch mit dem Begriff „Cryptojacking" – einem Kofferwort aus Cryptocurrency Mining und Browser Hijacking – bezeichnet wird.

Aufgrund der Tatsache, dass sich „Cryptojacking" erst bei hohen Zugriffszahlen so richtig lohnt, missbrauchen die Kriminellen oftmals gut besuchte Webseiten für ihre Aktivitäten. Das funktioniert sowohl über legitim eingekaufte Werbeflächen (Malvertising) als auch mittels gezielter Einbrüche: So gelang es beispielsweise Online-Räubern im November, Mining-Code im beliebten deutschen Spielforum Minecraft.de zu verankern.

Besonders Videostreaming-Angebote sind dank langer Verweildauer der Besucher wie geschaffen für „Cryptojacking"-Angriffe. Im Dezember will der Adblocker-Hersteller AdGuard eingebetteten Mining-Code in den Video-Playern der Streaming-Websites Openload, Streamango, Rapidvideo und OnlineVideoConverter entdeckt haben. Allein die monatliche Besucherzahl von Openload schätzt AdGuard auf 330 Millionen.

Auch die Kaffee-Kette Starbucks sorgte kürzlich mit „Cryptojacking" für Schlagzeilen: Ein Kunde stellte in insgesamt drei Filialen in Buenos Aires Verzögerungen beim Verbinden mit dem kostenlosen WLAN fest. Als Auslöser entpuppte sich Mining-Code in der Landing-Page des verantwortlichen Internet-Providers Fibertel, der wiederum von Dritten eingeschleust worden war.

Coinhive und Monero besonders attraktiv

Nimmt man diese und ähnliche Beispiele genauer unter die Lupe, so fällt auf, dass bei einem Großteil – einschließlich Piratebay, Minecraft.de und Starbucks – Variationen desselben JavaScript-Codes zum Einsatz kommen. Es stammt von einem Anbieter namens Coinhive, der es seit September 2017 für den Einbau auf Webseiten zur Verfügung stellt. Seine Geschäftsidee: Das eingebundene Skript ruft den eigentlichen Mining-Code

von der Coinhive-Webseite ab, und die Code-Entwickler streichen letztlich rund 30 Prozent des resultierenden Gewinns ein. Ob das Anzapfen der CPU per Coinhive-Skript heimlich stattfindet oder ob der Nutzer darüber informiert wird, liegt in der Verantwortung desjenigen, der das Skript auf eigenen oder gehackten Webseiten einbaut.

Zahlen von AdGuard veranschaulichen die Beliebtheit von Coinhive. Demnach entdeckte AdGuard zwischen Oktober und November 2017 mehr als 33.000 Webseiten mit Mining-Skripten; bei mehr als 95 Prozent von ihnen soll es sich um Coinhive-Code gehandelt haben. In wie vielen Fällen das Mining ohne Zustimmung der Webseiten-Besucher (und vielleicht auch ohne Wissen der Webseiten-Betreiber) stattfand, geht aus AdGuards Statistiken allerdings nicht hervor.

Die Attraktivität des Coinhive-Codes für Kriminelle besteht einerseits in der einfachen Integrierbarkeit und öffentlichen Verfügbarkeit, andererseits aber auch in der mit ihm schürfbaren Kryptowährung Monero. Ähnlich wie ZCash gewährt sie ein höheres Maß an Anonymität als Bitcoin, da Transaktionen standardmäßig stark verschleiert stattfinden und durch Dritte nur schwer nachvollziehbar sind.

„Cryptojacking“ erfordert JavaScript

Das Deaktivieren von JavaScript im Browser schiebt jeglichen Krypto-Mining-Aktivitäten einen Riegel vor. Die Kehrseite dieser Vorgehensweise ist allerdings, dass viele moderne Webseiten ohne die Skriptsprache nicht mehr so funktionieren, wie sie sollten. Zielführender ist die Nutzung eines Adblockers nebst Filterregeln, die das Mining unterbinden. Adblock Plus beispielsweise veröffentlichte bereits Ende September 2017 als Reaktion auf den Coinhive-Code auf Piratebay eine Filterregel zum Blockieren des Mining-Skript-Anbieters.

Die Entwickler der Antimalware-Software von Malwarebytes entschieden sich im Oktober 2017 dafür, Coinhive-Aktivitäten im Browser als Bedrohung einzustufen und folglich zu unterbinden. In einem Blogpost begründeten sie diesen Schritt mit dem massenhaften Missbrauch des Mining-Codes durch Kriminelle.

Mining-Skripte statt Werbebanner

Malwarebytes argumentierte zudem, dass das rechenintensive Mining auf älteren Systemen nicht nur Performance-Einbußen mit sich bringe, sondern die Hardware dauerhaft beschädigen könne. Krypto-Mining im Browser sei jedoch nicht per se schlecht, sondern könne beispielsweise als Alternative zu aufdringlichen – und bisweilen auch Schadcode-verseuchten – Werbebannern zum Einsatz kommen. Dies erfordere allerdings das Einverständnis der Nutzer.

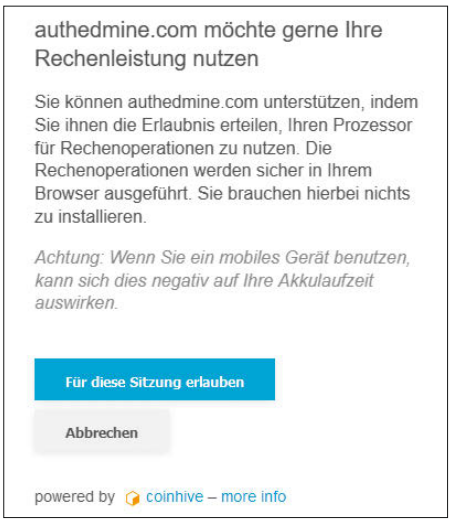
Die Coinhive-Entwickler selbst beteuern auf ihrer Webseite, dass sie keinerlei kriminelle Absichten verfolgen, sondern Krypto-Mining tatsächlich als Alternative zu herkömmlicher Werbung betrachten. Diese Aussage untermauern sie, indem sie neben dem eigentlichen, beliebig anpassbaren Mining-Code auch eine Variante mit vorgefertigter grafischer Oberfläche bereitstellen, die erst nach Anklicken eines Start-Buttons durch den Nutzer mit dem Schürfen von Moneros beginnt.

Da die gängigen Adblocker Coinhive jedoch unabhängig vom Vorhandensein einer Nachfrage beim Besucher blockieren, haben die Entwickler vor kurzem das AuthedMine-Projekt ins Leben gerufen. Dabei handelt es sich um eine Coinhive-Implementierung, die den Besucher in jeder Sitzung explizit um Zugriff auf die Rechenleistung der CPU bittet. Auf der Internetpräsenz des AuthedMine-Projekts betonen die Coinhive-Entwickler, dass es keinerlei Grund gebe, die neue Mining-Variante zu blockieren. Letztlich wissen aber nur sie selbst, ob sich hinter AuthedMine tatsächlich nutzerfreundliche Absichten oder nicht doch eher die Angst vor finanziellen Verlusten verbirgt.

Das Problem: Jede Nachfrage um Erlaubnis dürfte die Einnahmen schmälern. Denn viele Webseiten-Besucher schrecken vor dem Anklicken einer Einwilligung, wie sie etwa AuthedMine anzeigt, zurück – sei es nun aus Unkenntnis des Konzepts „Mining statt Werbung“, aus Passivität oder aus Sicherheitsbedenken. In der Konsequenz brüten Kriminelle lieber immer neue Taktiken aus, um ihre Aktivitäten zu verbergen – und untergraben damit jegliche Bemühungen, Krypto-Mining als vertrauenswürdige Alternative zu Werbebannern zu etablieren.

```
<script src="https://authedmine.com/lib/simple-ui.min.js" async></script>
<div class="coinhive-miner"
   style="width: 256px; height: 310px"
   data-key="YOUR_SITE_KEY">
   <em>Loading...</em>
</div>
```

Zur Integration eines Coinhive-Miners samt grafischer Oberfläche in eine Webseite benötigt man lediglich diesen simplen Code-Schnipsel nebst persönlichem Key.



AuthedMine bittet um Rechenleistung und gibt sich nebenbei besorgt um Energiereserven.

Kriminelle spielen weiterhin Verstecken

Eine besonders raffinierte „Cryptojacking“-Strategie entdeckte das Malwarebytes-Team Anfang Dezember 2017 auf der Porno-Webseite yourporn.sexy. Sie basiert auf Browser-Fenstern in Gestalt sogenannter „Pop-unders“, einer Popup-Variante, die sich nicht vor, sondern hinter dem aktuellen Fenster öffnet. Im Falle besagter Porno-Webseite ermittelt das Pop-under die Bildschirmauflösung, um die exakte Größe und Position der Taskleiste anzunehmen und sich anschließend dahinter zu verstecken.

Während der Webseiten-Besucher bereits die nächste URL ansteuert, läuft das Mining-Skript im Pop-under weiter – mit moderater CPU-Nutzung zugunsten einer möglichst perfekten Tarnung. Die ist zum Glück aber doch nicht so perfekt wie beabsichtigt: Malwarebytes zufolge kann man das Pop-under unter der Taskleiste erahnen, sofern diese dank des ausgewählten Windows-Themes transparent ist.

Das Pop-under enttarnt sich aber noch durch ein weiteres Merkmal – nämlich durch das Browser-Icon in der Taskleiste, das auch dann als aktiv gekennzeichnet bleibt, wenn der Nutzer glaubt, alle Fenster geschlossen zu haben. Per Rechtsklick auf das Icon („Fenster schließen“) oder durch Beenden des Browser-Prozesses im Taskmanager ist es dann ein Leichtes, den verborgenen Mining-Aktivitäten ein Ende zu bereiten. (ovw) c't

Dennis Schirrmacher

Online-Banking mit TAN-Apps

Viele Online-Banking-Apps sind verwundbar und Angreifer könnten etwa Überweisungen manipulieren. Eine derartige Attacke ist jedoch komplex. Sicherheitsforscher demonstrieren erfolgreiche Übergriffe und zeigen abermals die Gefahren das TAN-App-Ansatzes auf.

Transaktionsnummern, kurz TAN, sind beim Online-Banking unabdingbar. Man kann sie als einmaliges Passwort betrachten, das etwa die Ausführung einer Überweisung autorisiert. Anfangs las man die Transaktionsnummer von einem Zettel ab und gab diese auf dem Computer in das Formularfeld ein. Das ist quasi der Klassiker der Zwei-Faktor-Authentifizierung (siehe auch S. 100), bei dem das Bankgeschäft strikt getrennt mit zwei Medien abläuft. Selbst wenn sich ein Angreifer die PIN für das Banking-Konto erschleicht, kann er keine Überweisungen tätigen, da ihm der zweite Faktor fehlt. Aktuelle TAN-Konzepte setzen auf ein zweites Gerät. Bei mTAN ist das etwa ein Handy, das die TAN per SMS empfängt.

Heutzutage bieten jedoch immer mehr Banken neben der Banking-App auch TAN-Apps für Smartphones und Tablets an. Dabei findet neben der Überweisung auch die Generierung der TAN auf ein und demselben Endgerät statt. Man kann die TAN sogar oft direkt in die Banking-App übertragen. Das ist praktisch und äußerst bequem, aber ein gefundenes Fressen für Hacker, weil die beiden Faktoren nicht aus unterschiedlichen Quellen stammen.

Angriff nicht trivial

Die Kommunikation zwischen den Apps findet verschlüsselt statt und ein auf einem Smartphone installierter Trojaner kommt nicht ohne Weiteres an die Daten ran. Das Konzept ist aber durchaus angreifbar, wie die Sicherheitsforscher Vincent Haupert und Tilo Müller schon 2015 am Beispiel der TAN-App der Sparkasse demonstrierten. Ende 2017 haben sie erneut die Unsicherheit des bequemen Online-Bankings aufgezeigt und eigenen Angaben zufolge 31 Banking-Apps erfolgreich attackiert – darunter etwa die Comdirect, Commerzbank und Fidor-Bank. Eine vollständige Liste wurde bislang nicht veröffentlicht. Bei diesen Apps realisiert die Firma Promon die Absicherung und Verschlüsselung.

Doch um etwa Überweisungen mit ihrem Angriff zu manipulieren, mussten sie einige Hürden überwinden. Als Erstes sind sie über eine bekannte, aber nicht vollständig geschlossene Sicherheitslücke in ein Nexus 5X und Android 7.0 auf Patchstand Ende 2016 eingestiegen. Nach ihrem erfolgreichen Angriff auf das Smartphone befanden sich die Forscher in einer Position, in der sie die Banking-Apps über Sicherheitslücken attackieren konnten. Dabei haben sie die von der Firma Promon implementierten Sicherheitsmechanismen komplett umgangen. Das sei aber sehr aufwendig gewesen, schildern die Sicherheitsforscher. Promon ist im App-TAN-Bereich ein großer Fisch und hat eigenen Angaben zufolge rund 100 Kunden mit insgesamt 100 Millionen Nutzern.

Updates in Sicht, aber …

Promon versichert, dass es bisher keinem Hacker in freier Wildbahn gelungen ist, ihre Sicherheitsmechanismen auszuhebeln. Die Interessenvertretung der Kreditinstitute Deutsche Kreditwirtschaft (DK) unterstreicht diese Aussage und sie halten „die Sicherheit der von den Banken und Sparkassen angebotenen Banking-Apps weiterhin für gewährleistet“. Promon hat unterdessen eine neue Version seiner Schutzsoftware entwickelt und veröffentlicht, die nicht mehr anfällig für die Attacke ist.

Doch die Updates lösen nicht das Grundproblem: Finden das Banking und die TAN-Generierung auf ein und demselben Gerät statt, ist dies ein erfolgversprechenderes Angriffsziel, als wenn beide Vorgänge auf getrennter Hardware stattfinden. Wer die Sicherheit beim Online-Banking steigern will, sollte also auf Zwei-Faktor-Authentifizierung mit zwei Geräten setzen. Derartige Geräte haben im Grunde alle Banken im Programm. Zum Beispiel stellen die Commerzbank und einige Volksbanken den Kunden Lesegeräte für das photoTAN-Verfahren zur Verfügung. Damit scannt man einen farbigen Barcode von einem Bildschirm, um eine Transaktionsnummer zu generieren. Auch das chipTAN-Verfahren ist eine Alternative. Dabei generiert ein EC-Kartenleser die TAN. Am besten fragen Sie Ihre Bank, ob diese Extra-Hardware zur TAN-Generierung anbietet.

Am sichersten ist es, wenn man die TAN mit einem zweiten Gerät erzeugt.

Weit verbreitet ist das mTAN-Verfahren. Doch auch dieses Verfahren bietet Angriffspotenzial. Gängig ist etwa, dass Betrüger bei der Bank versuchen, die hinterlegte Nummer zu ändern.

Ernstfall

Man braucht vor dem Hintergrund der Analyse zur Sicherheit der TAN-Verfahren aber nicht in Panik zu verfallen: Letztlich ist die Bank dafür verantwortlich, dass die eingesetzten Verfahren ausreichend sicher sind. Ist das nicht der Fall und kommt es zu erfolgreichen Angriffen, muss die Bank für den entstandenen Schaden aufkommen. Das ist diesen auch durchaus bewusst. Etwa die in diesem Fall betroffenen Banken Comdirect und Commerzbank versicherten gegenüber c’t, dass sie im Schadensfall Privatkunden die vollständige Summe erstatten. (des) c't

03. MAI 2018 - HAMBURG
BLOCKCHAIN MASTERS

ES ERWARTEN SIE UNTER ANDEREM:

TAAVI KOTKA
HEAD OF ESTONIAN E-RESIDENCY
PROGRAM COUNCIL

KEYNOTE:
WINTER IS COMING:
WIE REGIERUNGEN DIE BLOCKCHAIN
NUTZEN KÖNNEN

FLORIAN GLATZ
PRÄSIDENT
BLOCKCHAIN BUNDESVERBAND

VORTRAG:
JURISTISCHE RAHMENBEDINGUNGEN
UND GESELLSCHAFTLICHE
AUSWIRKUNGEN

PROF. WOLFGANG PRINZ, PHD
VICE CHAIR / STELLV. INSTITUTSLEITER
FRAUNHOFER FIT

VORTRAG:
INTEROPERABILITÄT
VON BLOCKCHAINS

EXKLUSIVER WORKSHOP MIT PROF. ROMAN BECK

Als besonderes Highlight bieten wir am Folgetag, dem 4. Mai, einen exklusiven Blockchain Hands-on Workshop an. Professor Roman Beck von der IT University of Copenhagen leitet den Workshop "How to create your own Ethereum Dapp". Es sind nur wenige Plätze verfügbar.

TICKETS SICHERN!

www.blockchain-masters.com

eco VERBAND DER INTERNETWIRTSCHAFT

heise Events
Conferences, Seminars, Workshops

c't

iX

Uli Ries

Milliardenfacher Datenklau bei Yahoo, Dropbox & Co.

Sie nutzen Dropbox, haben eine Adobe-ID oder sind bei LinkedIn? Dann ist Ihr Passwort wahrscheinlich schon in den Händen von Kriminellen – vielleicht seit Jahren. In immer kürzeren Abständen werden immer größere Datenlecks bei prominenten Web-Unternehmen bekannt und Webseiten verkaufen den Zugang zu geklauten Datenbanken mit Milliarden von Benutzerkonten.

Ganz egal, ob Sie E-Mail-Dienste, Webhoster, Online-Speicher, Pornoangebote, Seitensprung-Vermittler, soziale Netzwerke oder Business-Netzwerke nutzen: Die Anmeldedaten für Ihr Konto kursieren wahrscheinlich im Netz. Seit Monaten oder sogar Jahren.

Die Zahlen über Datendiebstähle bei großen Websites sind in der Tat erschreckend. Die Website vigilante.pw behauptet, insgesamt über 3,8 Milliarden Datensätze mit geklauten Zugangsdaten zu besitzen; fast 5 Milliarden hat haveibeenpwned.com gesammelt. Allein Fahrdienstleister Uber hat sich 58 Millionen Datensätze entwenden lassen, 177 Millionen waren es bei LinkedIn, 152 Millionen bei Adobe, 69 Millionen bei Dropbox und beinahe unfassbare 3 Milliarden Einträge im Fall von Yahoo. Dies dürfte dem kompletten Kundenbestand entsprechen – inklusive längst inaktiver Konten. Selbst wenn bei-