Shit happens

Zuerst ist die Grafikkarte abgeraucht. Die interne funktionierte noch, ist aber natürlich weder spiele- noch Secondlife-tauglich. Dann blieb die Kiste ganz aus, was mir Rätsel aufgab.

Es stellte sich heraus, dass sich auch das Netzteil verabschiedet hatte und der Lüfter. Man kann nur vermuten, was zuerst kaputt war.

Ein Freund, der schon ein neues Netzteil eingebaut hat, meinte, dass ich alles so ausreize, dass ein größeres Kaliber der Hardware eh angebracht sei. Eine neue Grafikkarte kommt am Freitag. Wieder rund 150 Euronen weg…

Honks, rachsüchtige Orks und andere Kommentator*&/_innen

Don Alphonso schreibt mit großer Geste an die so genannte „AfD“ und die „Sehr geehrte Damen und Herren und strukturelle Analphabetismus-Honks aus den Internetkommentaren“. Lesenswert, weil es dazu passt, auch der Kommentar desselben: „Die sieben Empörer des Todes“: „Sie suchen nach Aufregern, haben den Humor von Erich Honecker und die Debattenkultur des Politbüros: Berufsempörte ruinieren den Netzdiskurs“. Mir gefällt besonders dieser sehr unaufgeregte Satz, den ich mir zu Herzen nehmen werde: „Mein Mobiltelefon ist von 2006 und mobiles Internet ist mir zu teuer, und so bekam ich gar nicht mit, wie mich am Rande ein Shitstorm traf.“

Da wir gerade beim Thema sind. Ich könnte etwas über die Kampagne „Kauft nicht bei Sexisten“ schreiben. Tu ich aber nicht. Ich schaue auch auf die IP wie Don Alphonso, und dann kommt Merkwürdiges heraus, wenn ich auch auf den Rest sehe. Das führt dann dazu, dass ich in einer E-Mail folgendes formuliere:
Ich bin im übrigen der Meinung, dass ninatabai.com ein Fake-Account ist und eine „Nina Tabai“ nicht existiert, sondern ein Mann ist. Die Frau auf dem Video sagt auch etwa anderes als der Ton.

Die wohlwollenden Leserinnen und geneigten Leser werden sich vermutlich fragen, warum ich mich auch mit Leuten anlege, die hier vernünftige Kommentare geschrieben habe, die sogar zu dem passen, wass ich politisch meine, und somit meinen Traffic erhöhe. Tut mir leid, ich bin eben so. Ich führe gern Indizienprozesse. Warum denke ich, dass es keine „Nina Tabai“ gibt?

Welchen Grund gäbe es für jemanden, die eine Website/ein Blog über „Medien“ macht („Ich schreibe hier über Politik- und Medienbeobachtung, also über das aktuelle politischen Zeitgeschehen“), zu verbergen, wer er/sie ist? Wer würde werben („Ich habe bisher noch keine Werbung geschaltet. Wenn Du daran Interesse hast“), wenn doch der Betreiber des Blogs noch nicht einmal den realen Namen per Impressum preisgibt? Das passt nicht zusammen.

Received: from mail.zoho.com by mx.zohomail.com
with SMTP id 1408011601847332.51591558116763; Thu, 14 Aug 2014 03:20:01 -0700 (PDT)
Date: Thu, 14 Aug 2014 12:20:01 +0200
From: Nina Tabai

Domain Name: NINATABAI.COM
Registrar WHOIS Server: whois.enom.com
Creation Date: 2014-06-12 10:28:00Z
Domain Status: clientTransferProhibited
Registrant Organization: WHOISGUARD, INC.
Registrant City: PANAMA
ISP: Neue Medien Muennich GmbH, Friedersdorf

Mein Gefühl sagt mir, dass sich eine Frau, die sich so kritisch gibt wie die Texte, nicht so darstellen würde wie auf dem Foto und dem Video. Die Haltung der Dame ist körpersprachlicher „Overkill“ und passt nicht zum Inhalt. Man muss nicht gleich die Pheromone bemühen. Anders ausgedrückt: Die Dame präsentiert sich so, wie ein Mann denkt, dass eine attraktive Frau sich präsentieren sollte. (Alles, was ich dazu

schreibe, gilt auch für sunflower22a) Das ist wie bei angeblichen „Lesben“-Pornos, die so gedreht sind, dass sie mitnichten Lesben anturnen, sondern Hetero-Männer.

Ich bin immer misstrauisch, wenn jemand aus dem Nichts auftaucht und schon gut schreiben kann und sehr viel weiß – aber in einem Stil, den ich eher Männern zuordnen würde. Nee, Leute, wer in Secondlife so viele weibliche Avatare getroffen hat, die in Wahrheit Männer waren, der glaubt erst mal gar nichts, es sei denn, es gäbe mindestens drei unabhängige Zeugen für das Gegenteil. Wie Don Alphonso schreibt: „Alles ist unerfreulich, aber wie jede milde Darmgrippe überlebbar.“ Oder: Es geht doch nichts über ein gepflegtes Feindbild. Wieder ein Leser [sic] weniger.

Phew oder 1x2ZH!3k(9#hl10öL#3gHgb/62al0-1f3

Nur ganz kurz zwischendurch ein Ratschlag, den die wohlwollenden Leserinnen und geneigten Leser gar nicht brauchen, weil sie vermutlich eh computer-, internet- und kryptografieaffin sind: Ich habe neulich mein Admin-Passwort für meinen Hauptrechner (Windows 7) geändert, war aber so müde, dass ich mich nicht genug konzentriert hatte. Deshalb fiel es mir am nächten Morgen auch nicht wieder ein. Zu raten ist auch schwierig, trotz exzessiven Kaffee-Konsums (ja, auf diesem Blog schreiben wir gutes Deutsch: „trotz“ verlangt den Genitiv). Meine Passwörter sind sehr lang und kompliziert und eine Mischung aus Buchstaben und Zahlen.

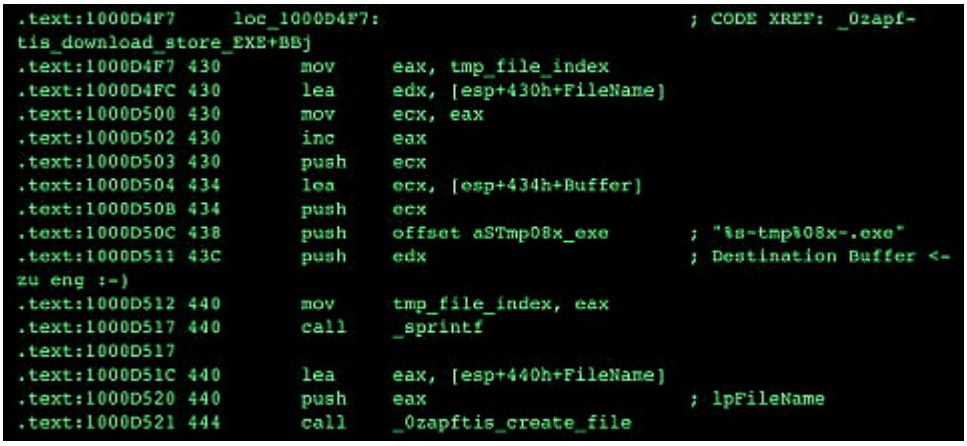
Die zahllosen Anleitungen im Netz, das eigene Admin-Passwort zu knacken, sind zwar gut gemeint, aber meistens viel zu aufwändig und funktionieren auch nicht wirklich, vor allem dann, wenn man es nicht mit einem normalen BIOS, sondern mit UEFI (Unified Extensible Firmware Interface) zu tun hat. Man kann nicht so einfach von einem externen Medium booten, was die übergroße Mehrzahl der Anleitungen schlicht voraussetzt. Ich bekam beim Kauf des Rechners auch keine Windows-CD. An dem blöden UEFI scheiteren übrigens auch alle Vesuche, auch auf dem Windows-7-Rechner parallel ein Linux-System zu installieren. (Linux habe ich jetzt nur auf meinem Dritt- und Viert-Rechner. Jaja, der fünfte Computer ist mein Smartphone.)

Zum Glück hatte ich ein zeitnahes Backup auf einer externen Festplatte. (Das ist der Ratschlag.) Nach dem dritten Tag des Herumfummelns habe ich dann das aufgespielt und mich beim Einrichten eines neuen 27-stelligen Admin-Passwortes konzentriert.

Komisch, dass Truecrypt (die Dateien stammen von Heise) nach dem Backup nicht mehr richtig funktionierte (nur das Öffnen der vorhandenen Container, aber nicht, einen neuen zu produzieren). Das Problem löste sich erst nach einer Neuinstallation von Truecrypt. Vielleicht hat aber auch das eine mit dem anderen nichts zu tun – zu viele Variablen im Spiel.

Jedenfalls ~~ist jetzt alles wieder in Butter~~ bin ich jetzt erleichtert, dass alles wieder funktioniert.

Der Kaiser ist nackt!



Heise meldet, dass die Bundesregierung behaupte, die Software zur Online-Durchsuchung sei einsatzbereit. Das ist aber nicht neu. Wie man der von mir erstellten Chronik der Medienberichte über die so genannte „Online“-Durchsuchung sehen kann, soll das schon vor acht Jahren möglich gewesen sein. Der *Tagesspiegel* titelte am 08.12.2006: „Die Ermittler surfen [sic!!] mit“:

“Das System der sogenannten „Online-Durchsuchung“ sei bereits in diesem Jahr mehrfach angewandt worden und sei Teil des 132 Millionen Euro schweren Sonderprogramms zur Stärkung der inneren Sicherheit. Die Ermittler sollen sich dabei auf richterliche Anordnung unbemerkt via Internet in die Computer von Privatpersonen einloggen können, gegen die ein Strafverfahren läuft.

(Viele Links funktionieren nicht mehr, aber anhand des genauen Titels kann man sie noch finden, teilweise über archive.org)

Manchmal fühle ich mich wie allein gelassen unter lauter

Irren. Was nützt mir ein derartiger Bericht wie der aktuelle bei Heise, wenn niemand fragt, wie die Überwachungssoftware auf den Rechner des „Zielobjekts“ gekommen ist? Das ist doch – jenseits der empörten Attitude – eine der wichtigsten Fragen überhaupt? Es braucht doch mindestens den physischen Zugriff (und dann müssen bestimmte Voraussetzungen gegeben sein), oder das „Opfer“ muss Malware wie Skype schon installiert haben.

Es geht aber mitnichten so, dass jemand „von fern“ irgendwas installiert. Außerdem müsste man ja auch die IP-Adresse wissen und eventuell noch den Router austricksen. (Jetzt fange hier niemand davon an, etwas von „Mail-Attachments“ zu faseln oder von „Websites, auf die man „gelockt“ werden soll. Ich kann es nicht mehr hören.) Christian Rath schrieb in der *taz* am 11.12.2006:

Denkbar sind verschiedene Wege. So kann die Polizei versuchen, ein „Trojanisches Pferd“ (kurz Trojaner) auf den Computer des Betroffenen zu schleusen. Ein Trojaner ist ein Programm, das heimlich Aktionen auf dem Computer ausführt, ohne dass der Benutzer dies bemerkt. Der Trojaner kann zum Beispiel als Anhang mit einer getarnten E-Mail auf den Rechner gelangen. Vorsichtige Computernutzer öffnen aber keine unbekannten Anhänge oder schützen ihren Computer mittels Firewall oder Filter schon vor dem Zugang solcher Spionagesoftware.

Soll ich das jetzt noch kommentieren?

Am 08.10.2011 berichtete Heise:
Dem Chaos Computer Club (CCC) ist nach eigenen Angaben die staatliche Spionagesoftware zugespielt worden, die allgemein unter dem Begriff „Bundestrojaner“ oder in bundeslandspezifischen Versionen beispielsweise auch als „Bayerntrojaner“ bekannt wurde.

In der Analyse des CCC (LESEN!) heisst es: „Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Ach so. Dann gibt es den „Trojaner“ nicht für Linux? Das ist aber

schade.

Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten. Andere mögliche Verfahren wären ähnliche Angriffe, wie sie von anderer Malware benutzt werden, also E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Es gibt auch kommerzielle Anbieter von sogenannten Infection Proxies, die genau diese Installation für Behörden vornehmen

E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Und so etwas schreibt der Chaos Computer Club?! OMG.

Ceterum censeo: Der Kaiser ist nackt!

HTTPS (Update)

Burks.de ist ab sofort über https erreichbar. Ich fummele noch an den Templates herum, es müsste aber schon alles funktionieren.

Gamma International Leaked

Allein schon dier Titel lässt einen gruseln: „Govermental IT Intrusion and Remote Monitoring Solutions“. Es gibt jetzt einen Twitter-Account („Phineas Fisher“) zum FinFisher-Hack (vgl. netzpolitik.org, 06.08.2014) und mehr Details auf reddit.com. Interessant, dass man sich auf „Anarchism“ beruft.

(Vgl. auch Bahrain Finfisher System logs (Feb 2012)

Skypekit

Ich habe die Skype-Software schon seit langem von meinen Rechnern geworfen, weil Skype bekanntlich Malware ist. Meinen Skype-Account nutze ich via Trillian. Das ging aber nicht mehr. (Ich nutze Skype eigentlich nur, um als Warlord virtuelle Hauereien in Secondlife zu koordinieren.)

Am 12. Juli 2013 wurde durch von Edward Snowden geleakte Informationen bekannt, dass den amerikanischen Geheimdiensten durch Microsoft tatsächlich direkter Zugriff auf den gesamten Skype-Verkehr gewährt wird und sowohl Textchats als auch Telefonate und Videotelefonate nach Belieben von der NSA mitgeschnitten und ausgewertet werden können, da es dem Geheimdienst mit Hilfe des direkten Zugriffs auf die Skype-Server möglich ist, die Skype-Verschlüsselung zu umgehen.

Jetzt habe ich eine Lösung für Windows 7 gefunden: „Skypekit in Trillian noch eine Weile weiter nutzen“.

Ich möchte die technikaffinen Leserinnen und sicherheitbewussten Leser auffordern, mir die Risiken des älteren Skypekit via Trillan aufzuzählen.

Eine Seite mit ihren

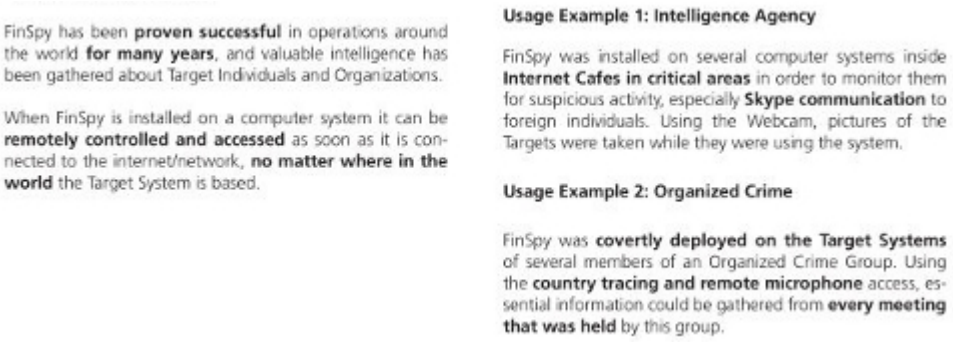
Familienangehörigen, die bei einem Unfall verletzt worden sind

Heise: „Der angebliche Quellcode des Programms FinFly Web wurde gar bei GitHub eingestellt. Es generiert Webseiten, die ihren Besuchern die Spionage-Software des Unternehmens unterjubeln sollen, unter anderem als Flash-Update getarnt.“

Flash update? OMG. Und wie wollen die die „Opfer“ auf die entsprechenden Websites locken? Das erinnert mich wieder an den legendären Vortrag Zierckes über die so genannte „Online-Durchsuchung“:
…wobei die Frage des Einbringens die spannendste Frage für alle überhaupt ist. Ich kann Ihnen hier öffentlich nicht beantworten, wie wir da konkret vorgehen würden. Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken. Die Geschichten sind so vielfältig, dass es kaum jemanden gibt, der nicht auf irgendeine Form dieser Geschichte hereinfällt.

Ich kann mir gar nicht vorstellen, dass die *FinFisher GmbH* so einen Unfug für Geld staatlichen Behörden andreht? Wen wollen die denn damit fangen? Aber offensichtlich ist es so. Nicht zu fassen.

FinSpy



FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Netzpolitik.org: „Seit ein paar Tagen werden auf dem Twitter-Account @GammaGroupPR interne Dokumente der Trojaner-Produktfamilie FinFisher/FinSpy aus dem Hause Gamma veröffentlicht.“

By the way: Es heisst „Trojanisches Pferd“ und *nicht* Trojaner“ – die Trojaner saßen eben *in Troja* und nicht im Pferd.

Jetzt schauen wir mal genau hin. (Die Links gehen zu den Werbe-pdfs der Firma Gamma International GmbH bzw. FinFisher.)

Die Software-Suite umfasst unter anderem:
1. FinSpy: Eine Trojaner-Software, die Fernzugriff auf einen bereits infizierten Rechner ermöglicht. Diese läuft unter Windows, Mac OS X sowie Linux.
2. FinFireWire: Software durch welche mithilfe von Firewire und DMA ein komplettes Abbild des Arbeitsspeichers heruntergeladen werden kann.
3. FinFly USB: Installation von zuvor gewählter Software nur durch Einstecken eines zuvor präparierten USB-Sticks.
4. FinFly ISP: Eine auf Internet-Provider-Ebene installierte Software, die unter anderem gezielt momentan geladene Dateien mit Überwachungssoftware infizieren kann.

1. Eine Software, die einen Remote-access-Zugriff („Fernzugriff“ oder auch Ernwartungszugriff) auf einen Rechner ermöglicht, muss also vorher dort installiert worden sein. Das

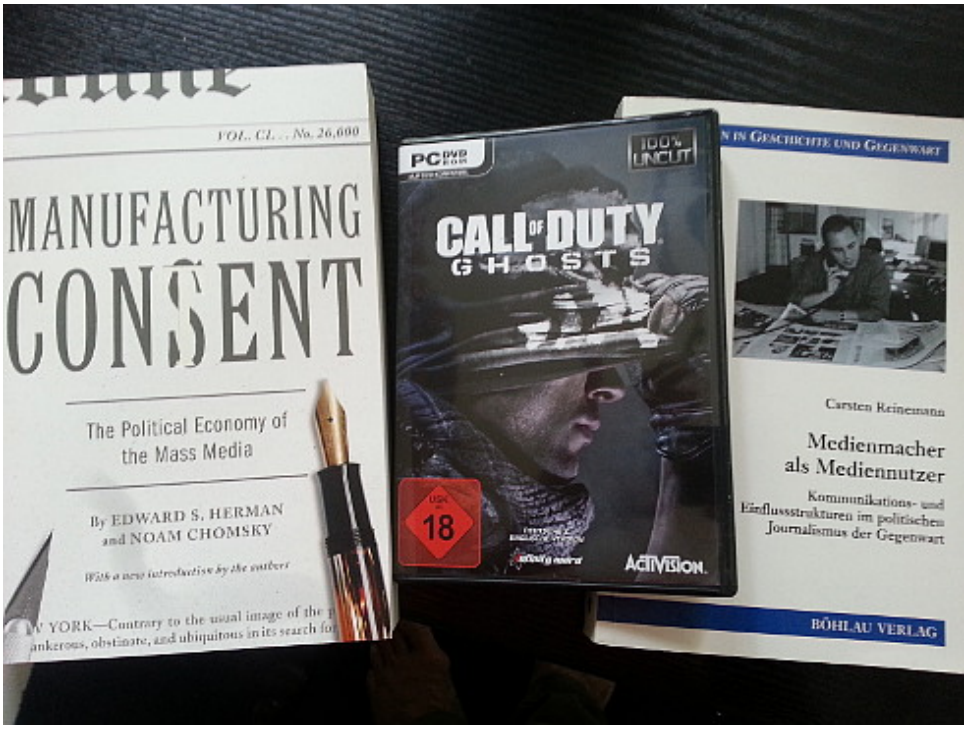
kann nur unter ganz speziellen und klar definierten Bedingungen geschehen, *nicht* aber, wenn das „Opfer“ sich vernünftig und sicherheitsbewusst verhält. Das gilt auch für Punkt 2. Die Firma behauptet selbst auch nichts anderes.

3. „Präparierte“ USB-Sticks können nicht automatisch etwas auf einem Rechner installieren. Der Besitzer des Rechners muss das (fahrlässig) erlaubt haben oder sich nicht sicherheitbewusst verhalten.

4. Wir haben auch schon die Sina-Box. So what?

Wer in derartigen Artikel verschweigt, dass es auch möglich ist, sich vor Spionage-Software zu schützen, wer behauptet, diese könne ohne (fahrlässiges) Wollen des Nutzers installiert werden, ist ein Dummschwätzer|Wichtigtuer und verbeitet nur Panik im Sinne der Geheimdienste („man kann nichts tun – sie sind eh schon drin“). And period.

Neu in meiner … äh … Bibliothek



Why the Security of USB Is Fundamentally Broken

Die Karte zeigt übrigens eine Reiseroute, die ich 1982 geplant hatte. Meine damalige Lebensabschnittsgefährtin wollte dann aber doch nicht durchs Darien Gap (awesome story!) marschieren. (Ja! Zu Fuß und per Boot und nicht per Jeep! Das geht!) Wir sind (leider) von Panama nach Kolumbien geflogen. Ich weiß nicht, ob ich da jemals noch hinkomme. Allein würde ich das nicht machen, aber eine Lebensabschnittsgefährtin müsste schon sehr tough sein.

Wired: „Why the Security of USB Is Fundamentally Broken“:
Computer users pass around USB sticks like silicon business cards. Although we know they often carry malware infections, we depend on antivirus scans and the occasional reformatting to keep our thumbdrives from becoming the carrier for the next digital epidemic. But the security problems with USB devices run deeper than you think: Their risk isn’t just in what they carry, it’s built into the core of how they work.

Das wäre ja noch schöner, wenn ich USD-Sticks fremder Leute an meine Rechner ließe. Autostart via USB – ohne meine jeweilige ausdrückliche Erlaubnis? Igitt. (Und natürlich ist unter Windows auch mein BIOS verrammelt und verriegelt.)

All manner of USB devices from keyboards and mice to smartphones have firmware that can be reprogrammed—in addition to USB memory sticks, Nohl and Lell say they’ve also tested their attack on an Android handset plugged into a PC.

Das Problem haben Karsten Nohl (Security Research Labs GmbH, Berlin, und Jakob Lell (Blog) aufgedeckt. Das Thema wird auch auf der Blackhat 2014 vorgestellt werden:

This talk introduces a new form of malware that operates from controller chips inside USB devices. USB sticks, as an example, can be reprogrammed to spoof various other device types in order to take control of a computer, exfiltrate data, or spy on the user. We demonstrate a full system compromise from USB and a self-replicating USB virus not detectable with current defenses.

Ich gehöre nicht zu den Leuten, die Artikel schreiben mit dem Tenor „das Ende ist nahe“. Panikmache ist fehl am Platz. Das

mag daran liegen, dass ich nicht für Geheimdienste arbeite, wie mir von einigen Verschwörungstheoretikern vom CCC seit meher als einem Jahrzehnt immer wieder unterstellt wird (vermutlich arbeiten gerade die für Geheimdienste). Die meisten Artikel in deutschen Medien über das obige Thema hinterlassen Laien mit dem Gefühl zurück: Die sind schon drin in meinem Computer, und man kann eh nichts tun. Das halte ich für kontroproduktiv, defätistisch und erst recht im Sinne der Dienste.

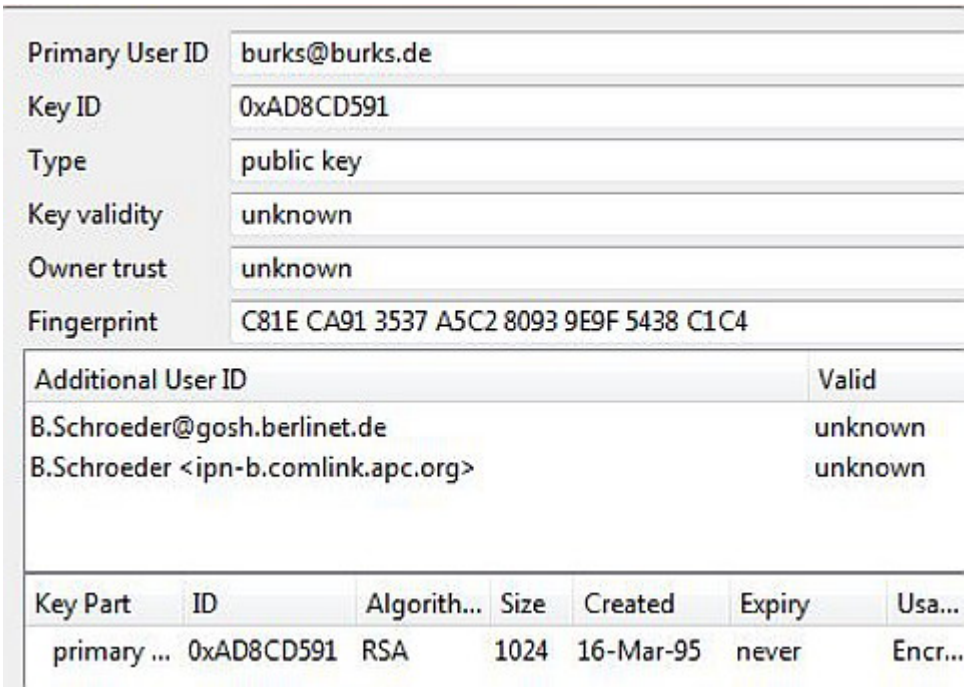
Ich sehe gerade, dass Heise etwas zum Thema berichtet. (Hätte ich mir denken können, ich bin über Bruce Schneider zur Wired gekommen.)

Die Kommunikation zwischen PC und USB-Sticks setzt auf das altbewährte SCSI-Protokoll auf. Dabei implementieren die Controller-Chips der Sticks mehr oder weniger SCSI-konform zusätzliche Hersteller-spezifische Erweiterungen. Über die kann Software auf dem PC dann etwa die Firmware des Sticks auslesen und auch einen neue, etwas modifizierte Firmware schreiben. Sicherheitsfunktionen, die dies irgendwie absichern würden, gibt es in der Regel nicht. (…) Um dann wiederum weitere Sticks zu infizieren, benötigt der Schadcode zwar Systemrechte, doch die lassen sich in der Regel ohne allzu großen Aufwand beschaffen – insbesondere, wenn man bereits „an der Tastatur sitzt.

Also ich weiß nicht. Das ist ja alles logisch, aber funktioniert nur unter bestimmten Voraussetzungen. Wie will jemand zum Beispiel an mein System-Passwort kommen?

Der Heise-Artikel zeigt auch anschaulich, dass Antiviren-Software Schlangenöl ist. Quod erat demonstrandum.

Oppa erzählt wieder aus dem Internet



Primary User ID	burks@burks.de
Key ID	0xAD8CD591
Type	public key
Key validity	unknown
Owner trust	unknown
Fingerprint	C81E CA91 3537 A5C2 8093 9E9F 5438 C1C4

Additional User ID	Valid
B.Schroeder@gosh.berlinet.de	unknown
B.Schroeder <ipn-b.comlink.apc.org>	unknown

Key Part	ID	Algorith...	Size	Created	Expiry	Usa...
primary ...	0xAD8CD591	RSA	1024	16-Mar-95	never	Encr...

Der Heise-Newsticker weckt heute nostalgische Gefühle in mir. „22 Prozent der Deutschen nutzen kein E-Mail“. Ich würde zu gern wissen, ob unter „E-Mail-Nutzen“ auch „Facebook-Vollschreiben“ gemeint war. Für mich gehörte das eben nicht zum „Nutzen von E-Mail“. Viele, zu viele Leute kennen heute den Unterschied zwischen Webmail und einem E-Mai-Programm gar nicht (mehr). Heise schreibt:

Ein Blick auf den ersten E-Mail-Account und das Alter zeigt ebenfalls, dass die heute 30- bis 49-Jährigen im Durchschnitt am längsten ein Konto besitzen: Vor 11 Jahren haben sie es bereits angelegt. Die gerade 50- bis 64-Jährigen folgen mit 10 Jahren und die Senioren mit 9 Jahren. Am kürzesten verfügen die heute 14- bis 29-Jährigen mit 6 Jahren im Mittel über einen E-Mail-Zugang.

Die wohlwollenden Stammleserinnen und geneigten Stammleser werden schon ahnen, was jetzt kommt. Erst elf Jahre ein E-Mail-Konto besitzen? Das hieße ja, der Durchschnitt ist erst

seit Mitte des letzten Jahrzehnts online? Ich habe seit mehr als zwanzig Jahren ein E-Mail-Konto. Und was sage ich der nachgeborenen Generation, die erst sechs Jahre ein E-Mail-Konto ihr eigen nennt? „Ich verschlüssele meine E-Mails seit 1995!“ (Vgl. Screenshot oben). Die werden natürlich nur antworten: „Oppa erzählt wieder aus dem ~~Krieg~~ Internet“.

Ich habe ein wenig mit groups.google.com (das mittlerweile als Recherche-Instrument weitgehend untauglich ist – dank Google, u.a. weil Javascript erzwungen wird) im Usenet herumrecherchiert. 1994 habe ich das E-Mail-Programm Crosspoint benutzt, sowohl für Mail als auch als Newsreader, später in Kombination mit Hamster, einem lokaler News- und E-Mail-Server für Windowssysteme mit dem Feature, News und Mails von mehreren Servern einzusammeln und sie gegebenenfalls zu filtern und nachzubearbeiten. Jaja, man konnte mit Hamster E-Mail-Header bearbeiten und fälschen! Damals waren die Nutzerzahlen für bestimmte Programme in Deutschland noch vier- oder gar dreistellig.

Meine erste E-Mail-Adresse war b.schroeder@IPN-B.comlink.apc.org. APC ist/war die „Association for Progressive Communications“ in Südafrika, der sich Mitte der 90-er Jahre wiederum viele deutschen Mailboxen des CL-Netzes angeschlossen hatten, um ihre Nachrichten verbreiten zu können. Ich hatte meinen Account bei der Mailbox Info Pool Network (IPN) – das erklärt, warum die E-mail-Adresse genau so aufgebaut war.

Burkhard Schroeder

Translate message into English

Nachricht vom 25.05.97 weitergeleitet
Ursprung : /CL/ANTIFA/ALLGEMEIN
Ersteller: B.SCHROEDER@IPN-B.comlink.apc.org

** Herzliche Glueckwuensche **

Weiterleitung aus dem Thule-Netz II [Elias BBS u.a.="Deutschland-Netz"]
----------schnipp----------
Ursprung : /Thule/T/MUSIK/DISKUSSION
Ersteller: Creator@90:900/23.14

Heil Euch,

hier, wie versprochen, ein weiteres Interview mit einer Rechts-Rock-Band.
Diesmal ist Saccara an der Reihe. Ganz aktuell und voerst nur fuer Euch!

Wenn man nach sich selbst sucht, findet man lustige Dinge, zum Beispiel die denkwürdigen Auftritte von Kim Schmitz (heute Kim Dotcom, früher auch bekannt als King Kimble the First, Ruler of the Kimpire) im Usenet, die Usenet-Threads zu „Tron“ (damals hatte ich schon meine heutige E-Mail-Adresse) sowie diverse andere Flame-Wars. Ich möchte das alles damals nicht missen, es hatte einen hohen Unterhaltungswert. Aber die Leute, mit denen man darüber reden könnte, lassen sich an zwei Händen abzählen.

E-Mails verschlüsseln in 30 Minuten

Das Tutorial des Vereins *German Privacy Fund*: „E-Mails verschlüsseln in 30 Minuten“ (Alternative 2 für Windows, alles auf einem USB-Stick) wurde ~~upgedatet~~ gepatcht, ergänzt und korrigiert.

Ybat yvir Ebtre Qvatyrqvar!

The Moskow Times (via Heise): „Russia's Interior Ministry is offering nearly 4 million rubles ($114,000) for research on ways to get data on users of the anonymous web surfing network Tor."

Qnf orqrhgrrg nore nhpu, qnff Gbe abpu avpug trxanpxg jbeqra vfg. Ybo haq Cervf frv Ebtre Qvatyrqvar haq qrara, qvr uvre uggcf://jjj.gbecebwrpg.bet/nobhg/pbercrbcyr.ugzy.ra rejäuag jreqra.

Sehr geehrte Hinterwäldler aka Österreicher!

Erst hatten wir diesen Kerl aus Braunau von Euch, dann den,

der zu viel Gas gab. Dazwischen belästigtet Ihr die Welt mit einen Nazi-Kavalleristen, dessen Stimme leider auf dem Weg zu den Außerirdischen ist. Dann das Skandalurteil ohne Beweise gegen einen Demonstranten. Dann werden Juden vom Platz geprügelt. Dann erklärt ihr Internet-Zensur für rechtmäßig, frei nach Gutdünken der Content-Mafia.

Wisst Ihr was, Ihr kackbraunen Hinterwäldler aka Österreicher? Ich werde Euer Land nicht mehr betreten. Ihr solltet von den ungarischen Faschisten eingemeindet werden; da wüchse zusammen, was schon einmal zusammen war und immer noch zusammen passt.

Evercookies

Da empfiehlt jemand im Heise-Forum, was ich auch empfehle:

• *generelles JavaScript-Verbot bis auf explizite Whitelist*
• *generelles Cookie-Verbot bis auf explizite Whitelist*
• *generelles Local-Storage-Verbot bis auf explizite Whitelist*
• *auch bei Whitelist-Sites nur Cookies von der Site selbst erlaubt, nicht von eingebundenen Fremd-Domains (Werbedienstleistern)*
• *ClickToFlash oder Flash ganz deinstalliert (analog für Silverlight)*
• *Java deinstalliert / geblockt*
• *bekannte Spionage-Domains systemweit geblockt*
• *generische Browser-ID*
• *periodisch die manuell erlaubten Cookies, Local Storage und Flash / Silverlight-Daten löschen*

1,5 Millionen Terroristen und 200.000 deutschsprachige Bombenbauanleitungen im Netz

AP (via Fefe): The U.S. government is rapidly expanding the number of names it accepts for inclusion on its terrorist watch list, with more than 1.5 million added in the last five years…“

Das erinnert mich an die Firma Pan Amp und Bert Weingarten, der von den gewohnt unkritischen Mainstream-Medien – zum Beispiel von sueddeutsche.de – vor einigen Jahren als „Experte“ und „internationaler Pionier der IT-Sicherheit“ herumgereicht wurde. Heise berichtete damals: „Angeblich 200.000 deutschsprachige Bombenbauanleitungen im Netz“.

Unter externen Spionageabwehrspezialisten

Foto: Spezialisten einer externen Firma überprüfen die Kommunikationsmittel des Verteidigungsministeriums auf Sicherheitsmängel.

„Daneben lassen derzeit das Außen-, Verteidigungs- und Justizministerium ihre internen Kommunikationsmittel auf Sicherheitsmängel überprüfen, zum Teil von einer externen Spezialfirma.“ (Quelle: SpOn)

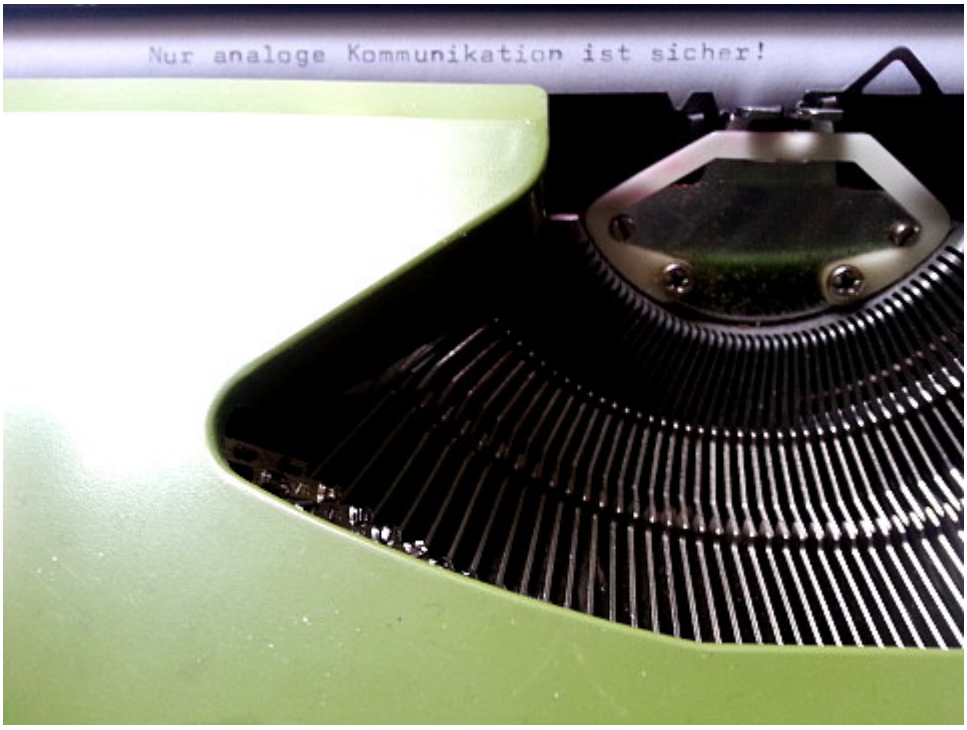
Bruhahahahaha. Vermutlich hat die externe Firma ihren Sitz in den Patch Barracks in Stuttgart-Vaihingen.

Homomorph kryptieren

The Guardian im Interview mit Snowden: „Edward Snowden urges professionals to encrypt client communications“.

Das ist eigentlich selbstverständlich und gilt nicht nur für „Professionals“, sondern für alle. Snowden empfiehlt letztlich homomorphe Verschlüsselung und rät u.a. davon ab, die Dropbox zu nutzen.

Sicher ist sicher, revisited



„Nur analoge Kommunikation kann halbwegs gesichert werden.“ (Stefan Plöchinger, Chefredakteur Sueddeutsche.de)

Ich schrob am 11. Juli 2013: Das sagt auch der Russische Geheimdienst. Dann muss es ja stimmen.

Heute lesen wir zum Beispiel bei N24:
Der NSA-Untersuchungsausschuss will möglicherweise auf altbekannte Methoden setzen, um sich vor Ausspähung zu schützen. Es werde erwogen, wieder auf mechanische Schreibmaschinen zurückzugreifen, um geheime Dokumente zu verfassen, sagte der Vorsitzende des NSA-Untersuchungsausschusses, Patrick Sensburg (CDU), am Montag im ARD-„Morgenmagazin„. (…) „Und wir müssen natürlich versuchen, unsere interne Kommunikation sicher zu halten, verschlüsselte Emails senden, Krypto-Telefone benutzen und andere Dinge, die ich hier jetzt natürlich nicht sage.“

Klar sagt er das uns nicht. Ist ja alles geheim.

Die sind komplett irre. Und keiner merkt es. LMFAO.