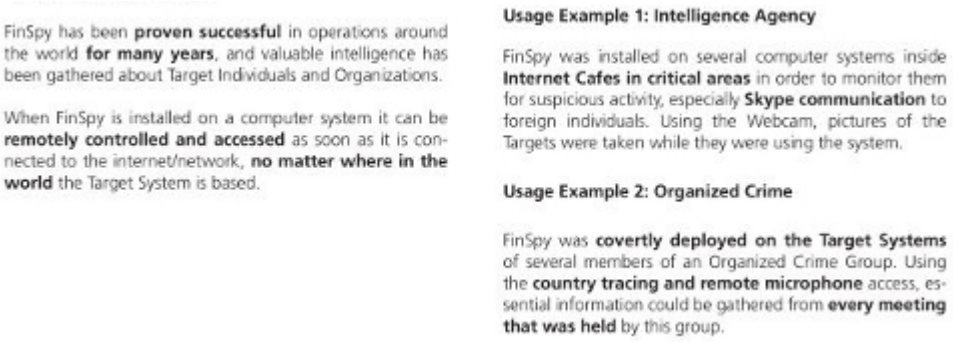
Eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind

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.

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.

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*

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)

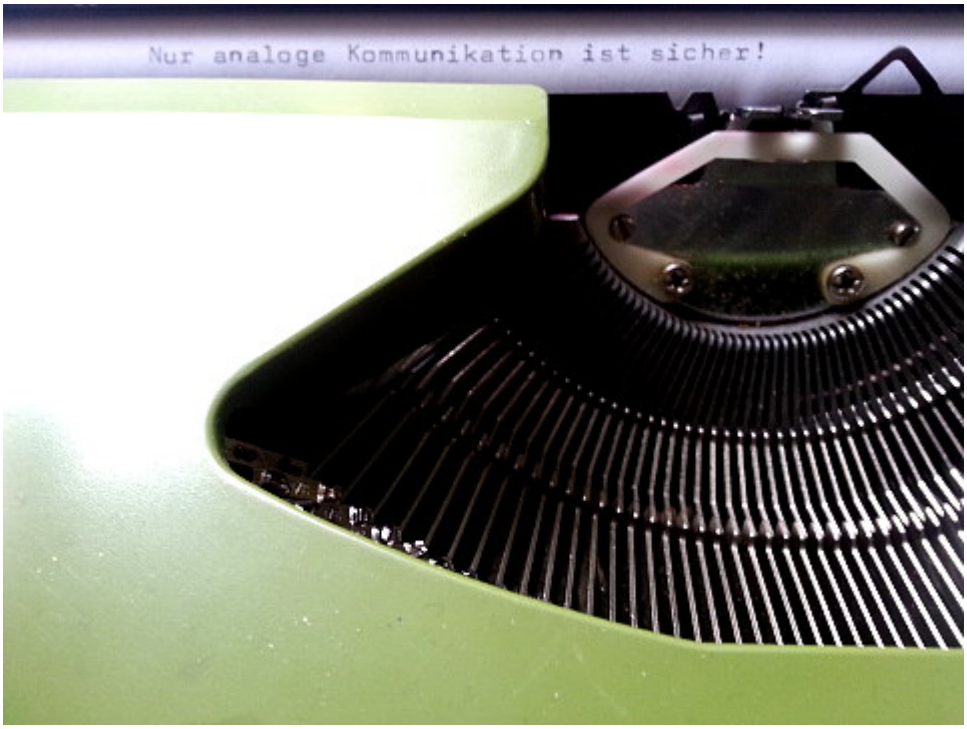
Bruhahahahaha. Vermutlich hat die externe Firma ihren Sitz in den Patch Barracks in Stuttgart-Vaihingen.

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.

Unter Torroristen

Aus der Tor-Mailingliste:

I would like to quote from the XKeyscore code (1)(2):

> *„// START_DEFINITION*
> */*
> *These variables define terms and websites relating to the*

*TAILs (The Amnesic Incognito Live System) software program, a comsec mechanism advocated by extremists on extremist forums. */*

$TAILS_terms=word(‚tails‘ or ‚Amnesiac Incognito Live System‘) and word(‚linux‘ or , USB , or , CD , or ’secure desktop‘ or , IRC , or ‚truecrypt‘ or , tor ,);
$TAILS_websites=(‚tails.boum.org/‘) or (‚linuxjournal.com/content/linux‘);*
// END_DEFINITION“

Obviously we on these lists belong to the most extreme dangerous people one can think of :-)) . Pirate Party Luxemburg thinks the same and offers for 20 EUR or 0.043 BTC a nice TORrorist Shirt (3). The profit will be donated to the Tor project.

Best regards and stay wiretapped!

Bange machen gilt nicht

Ein Kommentar von mir in der taz: „Wer hat Angst vor der bösen NSA? – Ja, ich bin ein Extremist – im Sinne der NSA. Ja, ich bekenne: Ich habe Tor und andere Anonymisierungsdienste genutzt und werde das weiterhin tun. Ich beschäftige mich oft mit dem Thema und suche im Internet danach. Deswegen bin ich in der NSA-Datenbank XKeyscore vermutlich schon gespeichert. Wenn nicht, wäre ich empört. Ich hielte es für unerträglich, wenn das Imperium des Bösen mich für harmlos hielte. [mehr…]

Sensationell ist, dass die taz mehr Links in den Artikel hineingedröselt hat als ich in das Original-Manuskript… Geht also.

In der Mitte meines Manuskripts hieß es: „Viel schlimmer als diejenigen, die keine Ahnung von Sicherheit im Internet haben wollen, sind die Defätisten, die mit geheimnisvoller Miene murmeln: „Die sind eh schon drin. Man kann nichts tun.“ Hier meine Verschwörungstheorie: Vermutlich werden gerade die von Geheimdiensten bezahlt. Das genau wollen die erreichen: Dass niemand mehr etwas unternimmt.“

Der letzte Satz sollte heißen: „Wer nach einer Reform oder gar einer Kontrolle der Dienste ruft, ist nicht nur naiv, sondern vergisst – oder ist nur zu feige – die Systemfrage zu stellen.“ (hat die taz mittlerweilie ergänzt).

Techniken der Datensammler: Was dagegen tun?

Jondonym stellt die Techniken der Datensammler vor, fasst die Risiken zusammen und gibt gleichzeitig Argumentationshilfen, warum man sicher und anonym surfen sollte:

– Tracking mit Cookies: Cookies sollte man ganz ausstellen!

– Flash-Cookies und EverCookies: Dagegen hilft z.B. das Firefox-Add-on Better Privacy.

– Fingerabdruck des Browsers: „Das Demonstrations-Projekt Panopticlick der EFF zeigt, dass mehr als 80% der Surfer anhand des Fingerabdrucks des Browsers eindeutig erkennbar sind. (…) Es werden die verwendete Software (Browser, Betriebssystem), installierte Schriftarten, Bildschirmgröße und Browser-Plugins ausgewertet. Zusätzliche Informationen werden mit einem Flash-Applet gesammelt. Bluecava erreicht damit bis zu 30% bessere Erkennungsraten, als Cookie-basierte

Lösungen.“

– Cache des Browsers: Cache beim Herunterfahren des Browsers löschen – das kann man so einstellen.

– Referer: Abhilfe z.B.: RefControl.

– Risiko JavaScript (ausschalten! Empfehlenswert: Noscript: „Das FBI nutzte im August 2013 bösartige Javascripte, die auf Tor Hidden Services platziert wurden, um durch Ausnutzung eines Bug im Firefox einen Trojaner zu installieren und Nutzer des Anonymisierungsdienstes zu deanonymiseren.“ (Sorry, aber wer Tor nutzt und gleichzeitig Javascript erlaubt, sollte geteert und gefedert werden – mein Mitleid hält sich da in Grenzen.)

– Risiko Plug-ins: „Der (Staats-) Trojaner der Firma HackingTeam wird beispielsweise mit einer signierten JAR-Datei auf dem Zielsystem installiert. Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln. Nur das Deaktivieren aller Plug-ins im Browser bringt Sicherheit.“ Java deaktivieren! Statt Adobe kann man auch den Foxit-Reader neben. Ich habe Adobe-Produkte übrigens komplett von meinen Rechnern entfernt.

– History-Sniffing: Abhilfe: keine History bzw. Browserverlauf anlegen.

– Webbugs, Werbebanner und Like-Buttons: „Eine andere unangenehme Eigenschaft von Webbugs ist, dass sie beim Abruf neben Cookies auch Ihre IP-Adresse automatisch an den Statistikdienst übermitteln. Selbst mit einer sehr guten Browserkonfiguration, dem Abschalten von Cookies und automatischen Webbug-Filtern können Sie dies niemals zuverlässig verhindern. Dagegen hilft nur die Verwendung eines Anonymisierungsdienstes.“

– TCP-Zeitstempel: Der Zeitstempel kann vom Client- und/oder

Server-Gerät eingesetzt werden, um die Performance zu optimieren. „Jedoch kann ein Internetserver Ihren Computer anhand der Zeitstempel wiedererkennen und verfolgen: Indem er die Abweichungen in der Uhrzeit misst, kann er ein individuelles Zeit-Versatz-Profil für Ihren Computer berechnen. Außerdem kann er die Zeit schätzen, zu der Ihr Rechner zuletzt neu gestartet wurde.“ Abhilfe nur per Anonymisierungsdienst.

– IP-Adresse: Die IP-Adresse offenbart zum Beispiel den aktuellen Aufenthaltsort, den Zugangsprovider, die Anbindung und Zugangstechnologie, das Unternehmen / die Behörde. Abhilfe nur per Anonymisierungsdienst.

– MAC-Adresse (kann man selbst ändern!).

Ich bekenne: Auch ich bin ein Extremist

NSA backdoors per default

Electronic Frontier Foundation (EFF): „Today, the US House of Representatives passed an amendment to the Defense Appropriations bill designed to cut funding for NSA backdoors.“

Vgl. auch Heise: „US-Repräsentantenhaus votiert gegen NSA-gesponserte Sicherheitslücken.“

Die Pointe an der Sache ist, dass der Foreign Intelligence Surveillance Act (Sektion 702), also das Gesetz (eines von mehreren), welches das Abhören regelt, nur Personen zu überwachen erlaubt, „die mit 51-prozentiger Sicherheit keine US-Amerikaner sind." Ab Werk eingebaute Sicherheitslücken und Schnittstellen zum Überwachen würden aber auch US-Amerikaner treffen. Heise: „Darüber hinaus schreibt der Gesetzestext vor, dass NSA und CIA kein Geld dafür benutzen, um Hersteller oder Anbieter dazu zu bringen, ein Produkt oder eine Dienstleistung so anzupassen, dass elektronische Überwachung ermöglicht wird."

Vermutlich wird der Senat das Gesetz wieder aufweichen.

Das BSI hat jetzt sehr kurze Beine

Spiegel online: „Interne Berichte beschreiben etwa die Kooperation der NSA mit den deutschen Diensten und sogar mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) – das die deutschen Nutzer eigentlich vor Cyber-Bedrohungen von außen schützen sollte. (…) Vor allem aber belegt das Deutschland-Dossier die enge Zusammenarbeit zwischen NSA und BND. Nicht nur abgefangene Informationen werden geteilt: Die NSA veranstaltet Lehrgänge, man zeigt sich gegenseitig Spähfähigkeiten und tauscht untereinander Überwachungssoftware aus. So haben die Deutschen das mächtige XKeyscore bekommen, die Amerikaner durften MIRA4 und VERAS ausprobieren."

Da bin ich jetzt aber mal gespannt. Am 26.07.2013 schrieb das BSI: „Eine Zusammenarbeit oder Unterstützung ausländischer Nachrichtendienste durch das Bundesamt für Sicherheit in der

Informationstechnik im Zusammenhang mit den Ausspähprogrammen Prism und Tempora findet nicht statt. Das BSI hat weder die NSA noch andere ausländische Nachrichtendienste dabei unterstützt, Kommunikationsvorgänge oder sonstige Informationen am Internet-Knoten De-CIX oder an anderen Stellen in Deutschland auszuspähen. Das BSI verfügt zudem nicht über das Programm XKeyscore und setzt dieses nicht ein.“

Tweet of the day 74

„Most commercial encryption products are junk.“ (Matthew Green)

Für ihn war das Neuland

„Wenn Sie innerhalb Deutschlands eine E-Mail verschicken, ist es durchaus denkbar, dass diese über die Vereinigten Staaten und wieder zurück läuft. (…) Für mich war das neu.“ (Hans-Peter Uhl, Bundestagsabgeordneter der CSU, Mitglied im Parlamentarischen Kontrollgremium zur Kontrolle der Nachrichtendienste (!!!), in der Frankfurter Allgemeinen Zeitung).

Schöne Zitatensammlung der Süddeutschen!

Vodafone reveals existence of secret wires that allow state surveillance

The Guardian (via Fefe): „Vodafone, one of the world's largest mobile phone groups, has revealed the existence of secret wires that allow government agencies to listen to all conversations on its networks, saying they are widely used in some of the 29 countries in which it operates in Europe and beyond."

Auch die Süddeutsche berichtet.

Ich überlege mir ernsthaft, ob ich meinen Vodafone-Vertrag für das Smartphone kündigen sollte.

Im Jahr eins nach Snowden

Lesenswert und informativ: Heise – „Was bisher geschah: Der NSA-Skandal im Jahr 1 nach Snowden".

Truecrypt, downloaded

Das komplette Archiv aller aktuellen Truecrypt-Versionen ist jetzt auch auf dem Webserver der GPF, zusätzlich ein Zip-Archiv (410 MB) aller Dateien.

Not Secure As

Fefe spekuliert über Truecrypt IMHO ganz richtig (via mathew).

It smelled like a warrant canary.