itrust consulting

Anwendertag IT-Forensik

V1.1 2013_10_01

Carlo Harpes

Erfahrungen eines privaten CSIRT, malware.lu

itrust consulting s.à r.l.
6 Z.I. Bombicht
L-6947 Niederanven

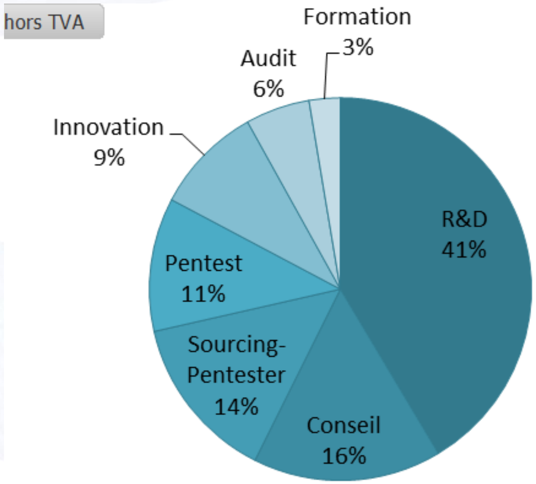
Tel: +352 26 176 212

Web: www.itrust.lu

Einführung

Allgemeines über itrust consulting s. à r. l.

- itrust : Akronym steht für
  “Information: Techniques and Research for Ubiquitous Security and Trust”
- Gegründet 2007, 4 Partner seit Sommer 2013
- Start-up des Jahres (ICT Awards 2008)
- 16 Angestellte zur Zeit
- Umsatz 2012 > 700k€



START-UP OF THE YEAR

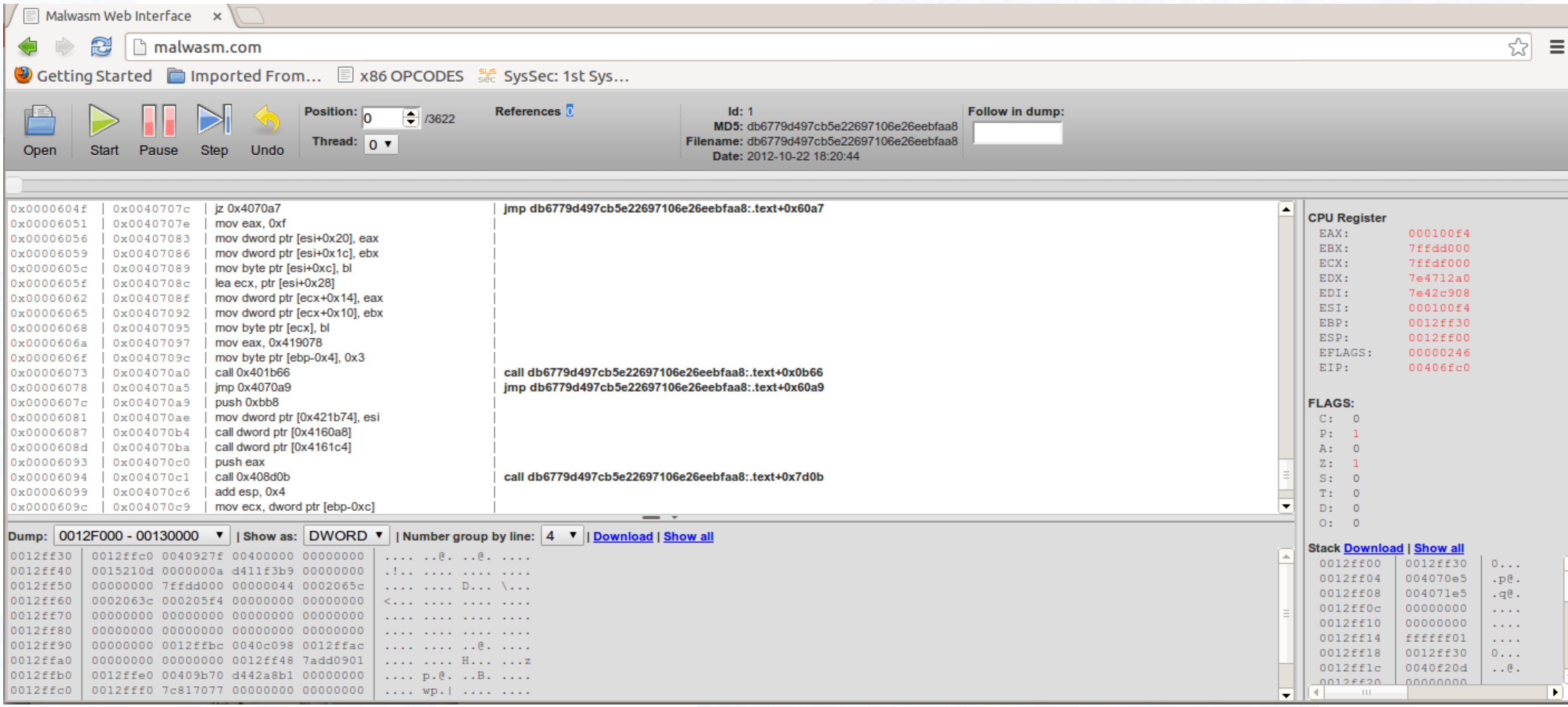
Entstehung
Projekt ITEA2/diamonds

- Nationale Förderung (60%) im Rahmen des ITEA1 Projektes “diamonds”
- Koordination: Fraunhofer Fokus, Prof Ina Schiefenecker
- diamonds = Development and Industrial Application of Multi-Domain Security Testing Technologies
- Dauer: 2010-2013
- Kosten: 14,2 Mio, davon 304 k€ für itrust zu 60% gefördert
- itrusts ursprüngliches Ziel: Erweiterung einer Managementplattform für sicherheitsrelevante Informationen mit Anforderungen und Ergebnissen von automatisierten Sicherheitstest zwecks automatischer Anpassung der Risikoanalyse.
- Zu anspruchsvoll, daher alternative Ziele und neue Ausrichtung auf Malware:
  - Malware Sammelstelle: malware.lu (30% der Projektkosten)
  - Malware Untersuchungsinstrument: malwasm (Open Source) (20%)
- Erreichte Ziele:
  - Pentest Distribution TRICK Tester (10%)
  - Malware.lu CERT (5%)
  - LASP Absicherung (Pentest, Security Target) (7%)

malwasm

itrust consulting

Reverse Engineering Tool Add-on auf Cuckoo Sandbox



malware.lu
Website

malware.lu

Inhalt

- 5,5 Mio Malware Samples
- 3000 (eingetragene) Benutzer
- 25 technische Analyseberichte
  - Duqu, Flame, Red October,…
  - Demo eine Smartcard Angriffs mit Malware (BE eID Karte)
    - Cf. Hack.lu (2012), Mexico, Corea

List of articles and technical analyses by date:

- 12/06/2013 : Analysis of KimJongRAT/stealer
- 13/05/2013 : Analysis of the sample cdorked.A
- 08/04/2013 : APT1: technical backstage
- 20/02/2013 : ZeroAccess statistics
- 11/02/2013 : Analysis of the sample blackenergy
- 08/02/2013 : Update of the technique used by Rannoh/Matsnu to store the images (version of January 2013)
- 16/01/2013 : Home made Red October C&C
- 16/01/2013 : Analysis of the malware of Red October - Part 3
- 15/01/2013 : Analysis of the malware of Red October - Part 2
- 15/01/2013 : Analysis of the malware of Red October - Part 1

malware.lu

malware.lu CERT

- Aufsetzen der Prozesse
- Registrierung durch Trusted Advisor
- Dienstleistungen
  - Weiterbildungen
  - Malware Analysen
  - Incident Response
  - Hilfe für Betrugsopfer (nicht nur Kunden)
  - Forensische Untersuchungen
  - Live-Untersuchung
- Business Model
  - Security-as-a-Service, d.h. Kompetenzen an öffentliche CERTs vermieten
  - …. im Aufbau…..
  - Pentest zum Kennenlernen, Incident Management Prozess aufsetzen
  - Auf Abruf bei Problemen, vor Ort ermitteln
  - Sektorielles Information Sharing, z.B. für Phishing

Sichtbarkeit von malware.lu

Luxembourg: The Steve McQueen of Cybersecurity

- Artikel vom 12. April von Stewart Baker, ehem. “first Assistant Secretary” des US Department of Homeland Security unter George W. Bush
- Er gibt eine politische Interpretation einer technischen Analyse von **Paul Rascagnerès, itrust consulting**, vom 8. April 2013.

Stewart Baker schließt:

- “Now we owe a lot to Paul Rascagnères, though he seems to have treated the Justice Department’s line the way Steve McQueen treated the fence in The Great Escape.
- Well, God bless him, he’s showing us a new path to cybersecurity.”

Paul Rascagnerès, “APT1: technical backstage”, Einstieg

Ausgangspunkt:

- Die US Firma Mandiant beschuldigt eine Gruppe, APT1 genannt (die erste ständig aktive (Spionage-)Bedrohung) hunderte Firmen von China aus zu bespitzeln.
  ATP1 soll dabei das Remote Administration Tool Poison Ivy einsetzen.

Ethische Einschränkungen:

- Kein Angriff auf Opfer von APT1, nur auf APT1 Systeme.
- Informationsweitergabe an Opfer, wenn möglich über nationale CERTs.

Source: http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf

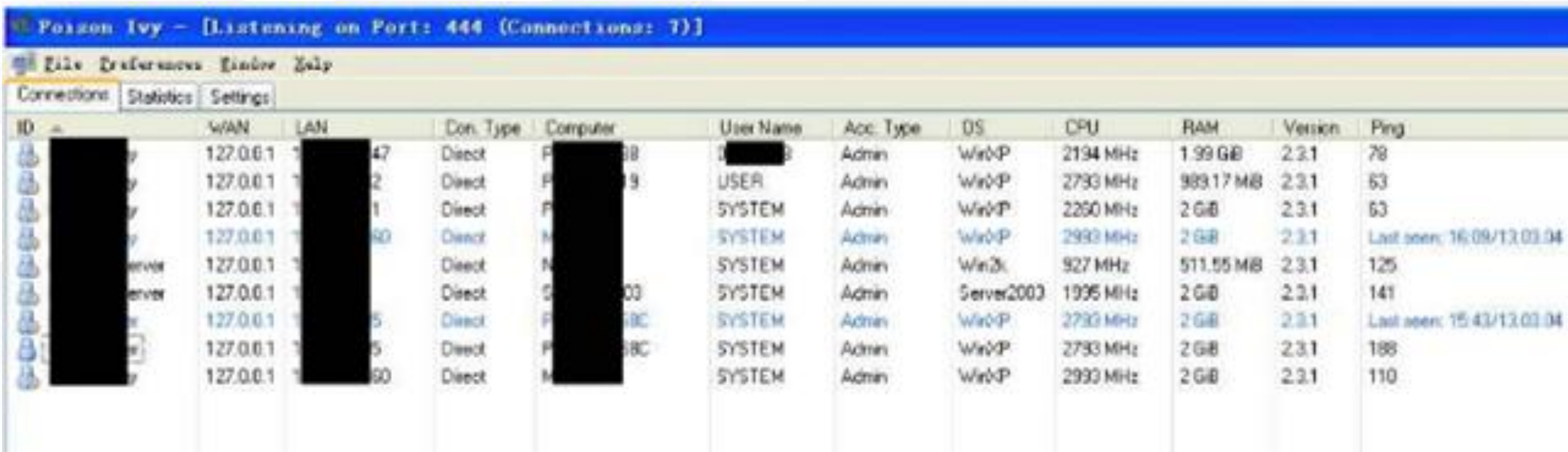
Paul Rascagnerès, “APT1: technical backstage”, Gegenangriff

Schritt 1:

- Paul entwickelt einen “passiven Scanner”, um Poison Ivy Server auf chinesischen IP-Ranges zu orten, dank bekannter Schwachstellen von Poison Ivy, mit neu entwickeltem Exploit.
- 300 Rechner, verteilt auf 6 Hoster wurden gefunden.
- Online Zeiten = Büro Öffnungszeiten in Hong Kong, d.h. keine privaten Hacker…

Schritt 2:

- Angriff auf diese Rechner, um die Netzwerkstruktur herauszufinden.
- Kopieren von etwa 20 hauseigenen Angriffstools, darunter “Terminator”.



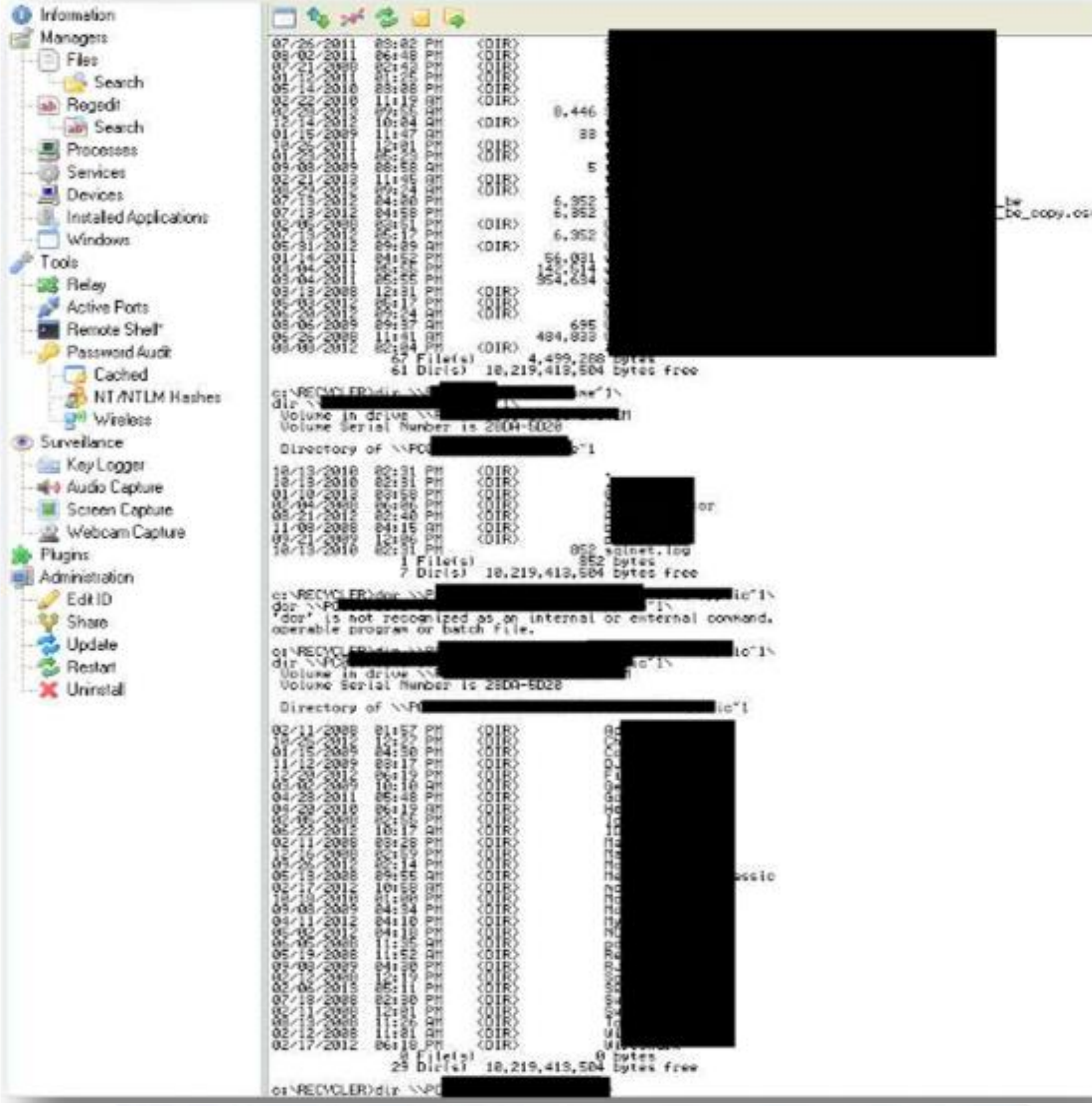
ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	[redacted]	Admin	WinXP	2194 MHz	1.99 GB	2.3.1	78
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	USER	Admin	WinXP	2793 MHz	989.17 MB	2.3.1	63
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2260 MHz	2 GB	2.3.1	63
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2993 MHz	2 GB	2.3.1	Last seen: 16:09/13 03:04
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	Win2k	927 MHz	511.55 MB	2.3.1	125
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	Server2003	1995 MHz	2 GB	2.3.1	141
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2793 MHz	2 GB	2.3.1	Last seen: 15:43/13 03:04
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2793 MHz	2 GB	2.3.1	188
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2993 MHz	2 GB	2.3.1	110

Paul Rascagneres, “APT1: technical backstage”, Gegenangriff

Schritt 3:

- Untersuchung und Entdeckung einer Schwachstelle in Terminator, welche das Root-Recht bringt, und Einsicht in die von APT1 gestohlenen Daten gibt.

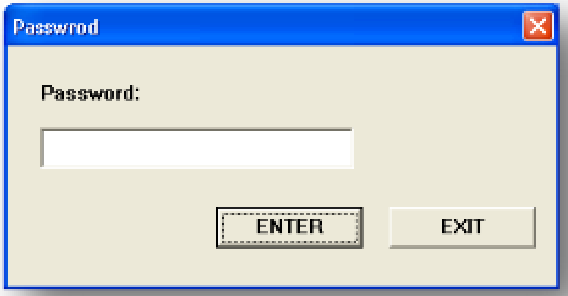
- Ziel waren Regierung-IPs, private und öffentliche Organisationen, Aktivisten und Journalisten (außerhalb der EU).



Screenshot vom APT1 Attacker
mit Fernzugriff auf die Besucherzeiten

APT1
Technical Backstage

- Das zweite benutzte RAT, “Terminator” genannt, wurde vorher als “Fakem” von TrendMicro identifiziert.
- Der Server wurde von einem Password geschützt, über welches wir logischerweise nicht verfügten:



- Nach einer Analyse des Code Zusammensetzers (Reverse Engineering) konnten wir diese Schutzfunktion umgehen.
- Durch eine tiefgehende Analyse des Code Zusammensetzers, entdeckten wir einen verwundbaren Punkt. Dieser erlaubte es uns ein Ausnutzungsmodul fürs Metasploit-Framework herzustellen.
- Dieses Modul ermöglichte uns den Zugriff auf den “Terminator” beherbergenden Server.

Paul Rascagneres, “APT1: technical backstage”, Enthüllungen

Vorgehensweise von APT1

- Einsatz von Proxyserver zur Verschleierung der Angriffs
- Ein Server pro Angriffsziel
- Hauseigene Malware
- Ausgezeichnete Organisation

Veröffentlichung

- itrust wurde erst nach der Veröffentlichung informiert – der Angriff wurde NICHT gebilligt.
- 50 Organisationen (mit über 300 Servers) wurden informiert, in der Regel über nationale CERTs.
- Die Veröffentlichungsabsicht von Paul Rascagneres wurde mit den CERTs besprochen.
- Der Artikel ging, viel später, am 8 April online auf malware.lu
- Er wurde über 50.000 mal angeklickt.

Source: http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf

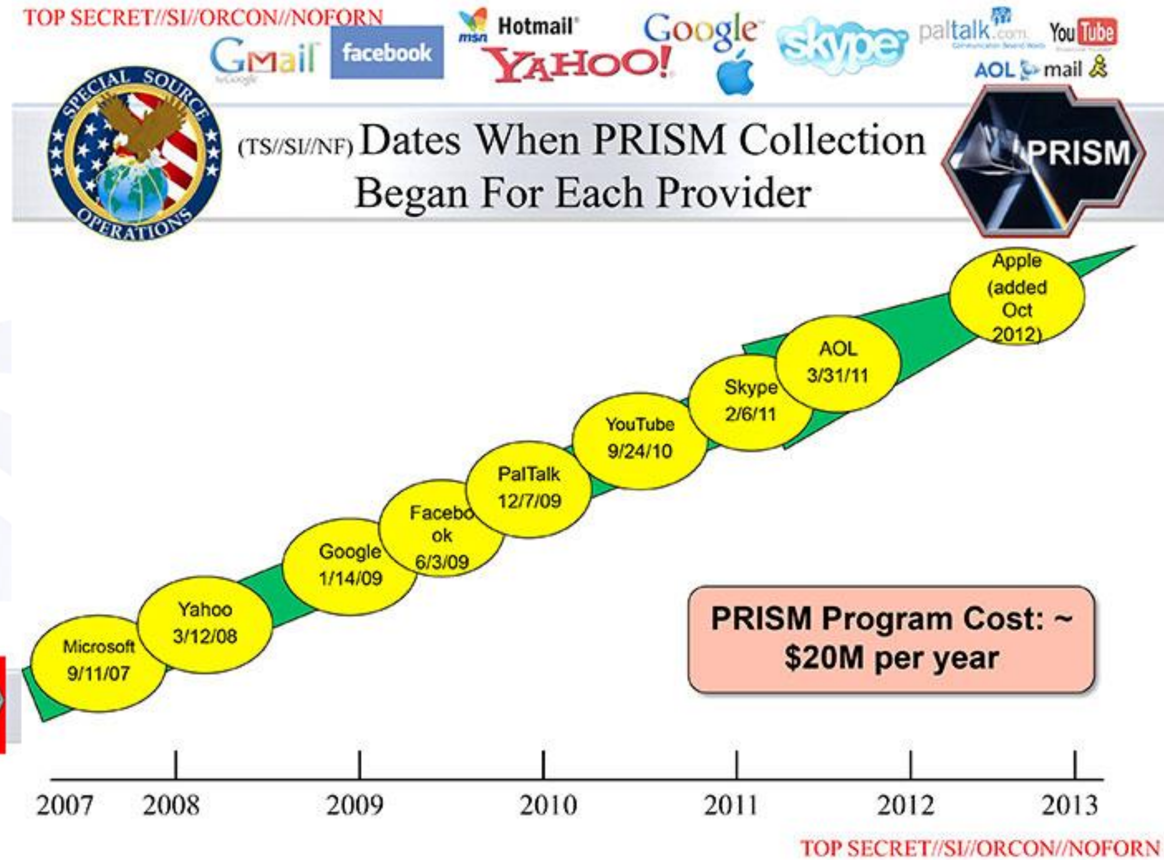
Luxembourg: The Steve McQueen of Cybersecurity
Schlussfolgerungen

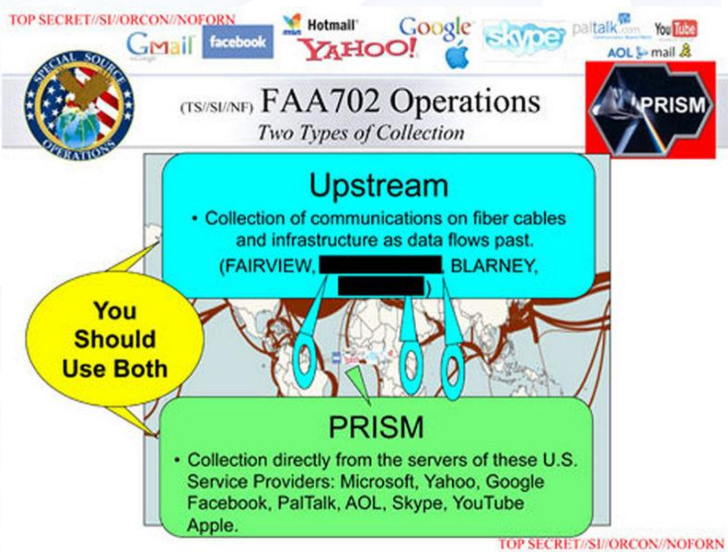
Stewart Baker schlussfolgert:

- “It’s getting harder for attackers to hide.”
- “Justice couldn’t be more wrong. This kind of tactic is absolutely essential if we want to create an effective defense against cyberespionage. Thanks to Luxembourg’s machismo, we won’t have to learn Unit 61398’s new tactics by trial and error; and we already have ways to thwart the new tactics, plus a store of tools and stolen data.”
- “Perhaps the Justice Department thinks that the government could have found all of this out on its own. Maybe the government already knows all this from its own supersecret penetrations of Chinese hacker networks, achieved without any help from vigilantes like Rascagnères. I kind of doubt it, but the more important fact is that it doesn’t really matter to all the private victims in this country what the government knows. We need to know it too.”

Source: http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf

PRISM
… nach Snowden…





PRISM
Politische Reaktionen

- **Viviane Reding**, Vizepräsidentin der Europäischen Kommission, kommentiert: “Wir können nicht über einen großen transatlantischen Markt verhandeln, wenn es auch nur den kleinsten Verdacht auf Spionage der Partner in den Büros der europäischen Verhandler gibt.”

- **Martin Schulz**, Präsident des Europäischen Parlamentes sagt er sei: “zutiefst beunruhigt und schockiert über die Behauptungen der US Spionage in EU Büros. Falls diese Behauptungen der Wahrheit entsprechen, wäre dies ein schwerwiegendes Problem das den Beziehungen zwischen den Vereinigten Staaten und Europa erheblich schaden würde.”

- “My job is to ensure people in Germany know that German law applies on German soil, and that applies to everyone here,” **Merkel** said. Still, she added, “it is not my job to familiarize myself with the details of PRISM,” referring to one of the NSA programs. Merkel has also sought to keep the issue from damaging relations with the U.S. “With every day it becomes clear to the United States that this is important for us,” she said. “Germany is not a nation of surveillance. Germany is a nation of freedom.”

- Auf die Frage “Ist EX-US-Agent Snowden für Sie ein Held oder Verräter?”, antwortet die luxemburgische EU-Justizkommissarin **Viviane Reding** wörtlich: “Weder noch. Er ist ein **'Whistleblower**' und ich habe Respekt vor seinem Mut. Ich nehme an, dass er eines Tages hier in Europa mit dem Durchbruch für einen starken Datenschutz sowohl gegenüber den öffentlichen Behörden als auch gegenüber Internetunternehmen in Verbindung gebracht wird.” (Tageblatt)

PRISM
Einstufung der Reaktionen

An die Philosophie des französischen Schriftstellers Albert CAMUS angelehnt:

Revolte	Verbesserung des Datenschutzes, Zurückgreifen auf nicht überwachte IT, Selbstschutz der Firmen (und Regierungen) gegen Spionage.
Absurdität	Schutz gegen Terrorismus ist notwendig, aber Überwachung äußerst ineffektiv (vgl. Boston Marathon). Die USA ändern ihre Haltung nicht.
Scheinheiligkeit	Wenn wir gewusst hätten, dass …
Sorglosigkeit	Nichts aus Echelon und SWIFT gelernt, Die amerikanische Absichten sind offensichtlich. Schlecht vorbereitete Regierungen und Firmen.

Fragen

Danke für Ihre
Aufmerksamkeit

Carlo Harpes
harpes (at) itrust.lu