



itrust
consulting



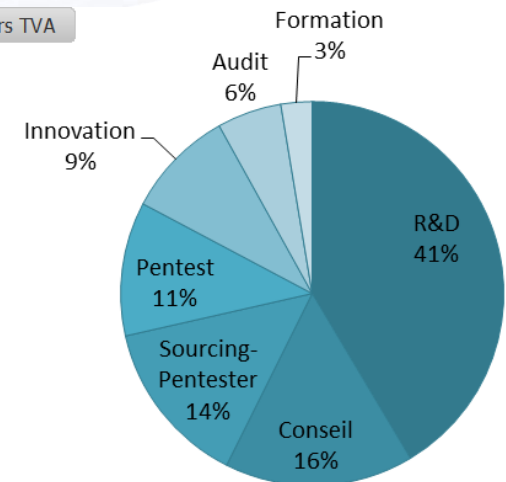
Anwendertag IT-Forensik

V1.1 2013_10_01
Carlo Harpes

Erfahrungen eines privaten CSIRT, malware.lu

- **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€

hors TVA

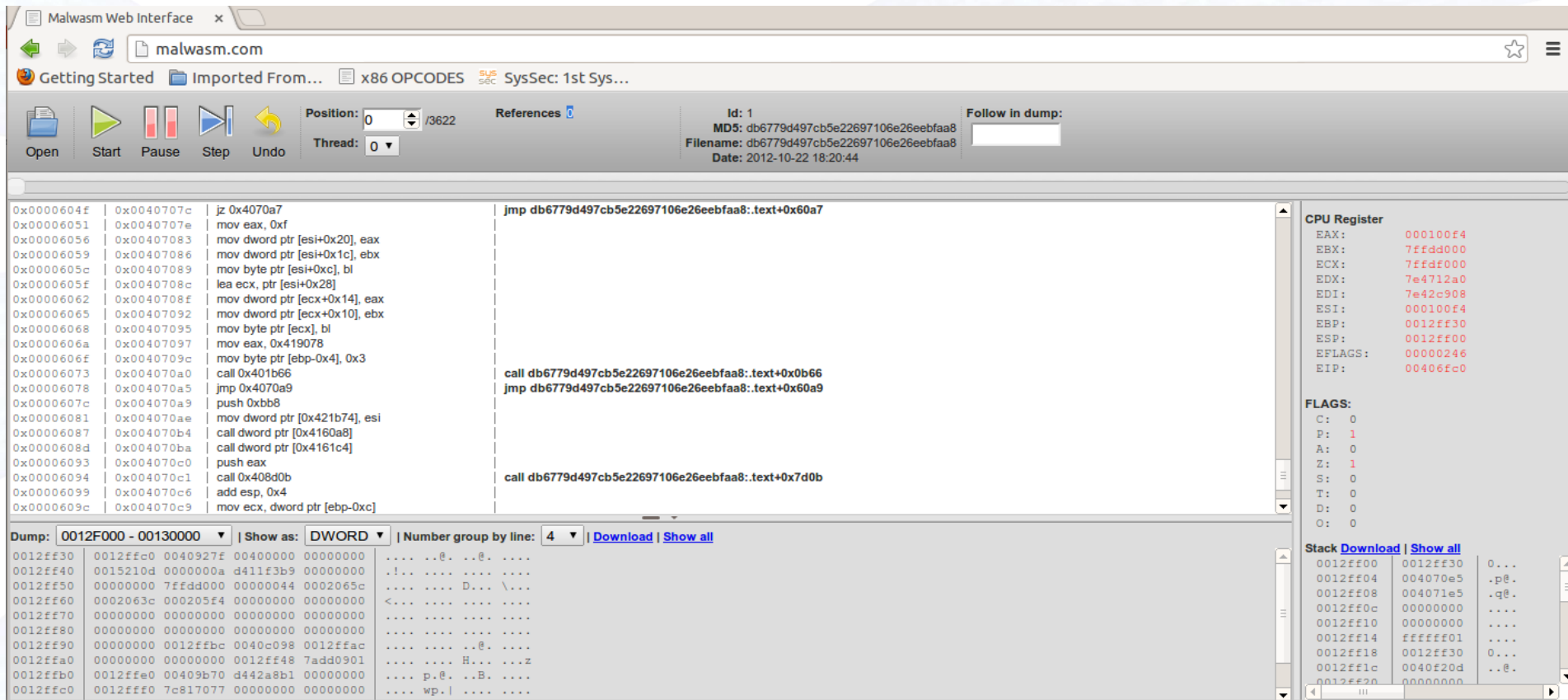


Entstehung Projekt ITEA2/diamonds



- 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%)

Reverse Engineering Tool Add-on auf Cuckoo Sandbox



Malwasm Web Interface x

malwasm.com

Getting Started Imported From... x86 OPCODES SysSec: 1st Sys...

Position: 0 / 3622 References 0

Id: 1
MD5: db6779d497cb5e22697106e26eebfaa8
Filename: db6779d497cb5e22697106e26eebfaa8
Date: 2012-10-22 18:20:44

Follow in dump:

Open Start Pause Step Undo

Thread: 0

0x0000604f 0x0040707c jz 0x4070a7 jmp db6779d497cb5e22697106e26eebfaa8:.text+0x60a7

0x00006051 0x0040707e mov eax, 0xf

0x00006056 0x00407083 mov dword ptr [esi+0x20], eax

0x00006059 0x00407086 mov dword ptr [esi+0x1c], ebx

0x0000605c 0x00407089 mov byte ptr [esi+0xc], bl

0x0000605f 0x0040708c lea ecx, ptr [esi+0x28]

0x00006062 0x0040708f mov dword ptr [ecx+0x14], eax

0x00006065 0x00407092 mov dword ptr [ecx+0x10], ebx

0x00006068 0x00407095 mov byte ptr [ecx], bl

0x0000606a 0x00407097 mov eax, 0x419078

0x0000606f 0x0040709c mov byte ptr [ebp-0x4], 0x3

0x00006073 0x004070a0 call 0x401b66 call db6779d497cb5e22697106e26eebfaa8:.text+0x0b66

0x00006078 0x004070a5 jmp 0x4070a9 jmp db6779d497cb5e22697106e26eebfaa8:.text+0x60a9

0x0000607c 0x004070a9 push 0xb8

0x00006081 0x004070ae mov dword ptr [0x421b74], esi

0x00006087 0x004070b4 call dword ptr [0x4160a8]

0x0000608d 0x004070ba call dword ptr [0x4161c4]

0x00006093 0x004070c0 push eax

0x00006094 0x004070c1 call 0x408d0b call db6779d497cb5e22697106e26eebfaa8:.text+0x7d0b

0x00006099 0x004070c6 add esp, 0x4

0x0000609c 0x004070c9 mov ecx, dword ptr [ebp-0xc]

CPU Register

EAX: 000100f4
EBX: 7ffdd000
ECX: 7ffdf000
EDX: 7e4712a0
EDI: 7e42c908
ESI: 000100f4
EBP: 0012ff30
ESP: 0012ff00
EFLAGS: 00000246
EIP: 00406fc0

FLAGS:

C: 0
P: 1
A: 0
Z: 1
S: 0
T: 0
D: 0
O: 0

Dump: 0012F000 - 00130000 | Show as: DWORD | Number group by line: 4 | Download | Show all

0012ff30 0012ffc0 0040927f 00400000 00000000e. .e.
0012ff40 0015210d 0000000a d411f3b9 00000000 .!..
0012ff50 00000000 7ffdd000 00000044 0002065c D... \..
0012ff60 0002063c 000205f4 00000000 00000000 <... ..
0012ff70 00000000 00000000 00000000 00000000
0012ff80 00000000 00000000 00000000 00000000
0012ff90 00000000 0012ffbc 0040c098 0012fface.
0012ffa0 00000000 00000000 0012ff48 7add0901 H... .z
0012ffb0 0012ffe0 00409b70 d442a8b1 00000000 p.e. .B.
0012ffc0 0012ff00 7c817077 00000000 00000000 wp. |

Stack Download | Show all

0012ff00 0012ff30 0...
0012ff04 004070e5 .p@.
0012ff08 004071e5 .q@.
0012ff0c 00000000
0012ff10 00000000
0012ff14 ffffffff
0012ff18 0012ff30 0...
0012ff1c 0040f20d ..e..
0012ff20 00000000

A screenshot of the malware.lu website. The header features a green and yellow abstract graphic above the "malware.lu" text. Below the header is a navigation bar with links: Search, Services, Malware.lu CERT, Articles, Events, Goodies, and About Us. The main content area includes a description of the site as a repository for malware and technical analyses, a disclaimer, and a login section for the "Samples repository". The login section prompts the user to enter a username and password, with a "Connect" button. At the bottom, there is a "Donate" button.

malware.lu

[Search](#) [Services](#) [Malware.lu CERT](#) [Articles](#) [Events](#) [Goodies](#) [About Us](#)

Malware.lu is a repository of malware and technical analyses for security researchers.

Malware.lu is a brand of [itrust consulting](#). We provides an expert team in malwares analyses and incident response for private and government entities.

Disclaimer:

Malware.lu contains malware samples. Malware.lu will not be held responsible for any damage brought to your equipment, including virus infection, caused by accessing, using or displaying this website or by downloading any information. You are accessing this website at your own risk.

If you would like to download or submit samples, you need to have an account. To request an account, please send an email to register@malware.lu with a username and a short explanation about "why you want an account". Currently the database contains **5,572,972** samples. The complete list of md5|sha1|sha256 can be found [here](#)

Samples repository

You are not connected, please enter your username and password

Username:

Password:

- 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](#)



- Aufsetzen der Prozesse
- Registrierung durch Trusted Advisor
- Dienstleistungen
 - Weiterbildungen
 - Malware Analysen
 - Incident Response
 - Hilfe für Betrugsoffer (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



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.”

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

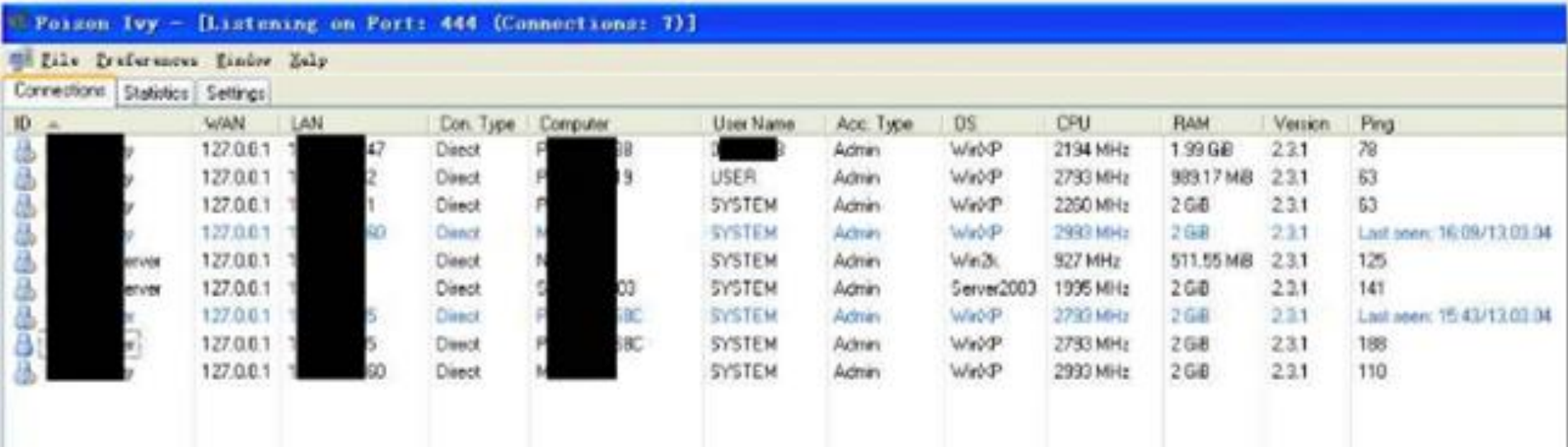
Paul Rascagnerès, “APT1: technical backstage”, Gegenangriff

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”.



Poison Ivy - [Listening on Port: 444 (Connections: 7)]

File Preferences Window Help

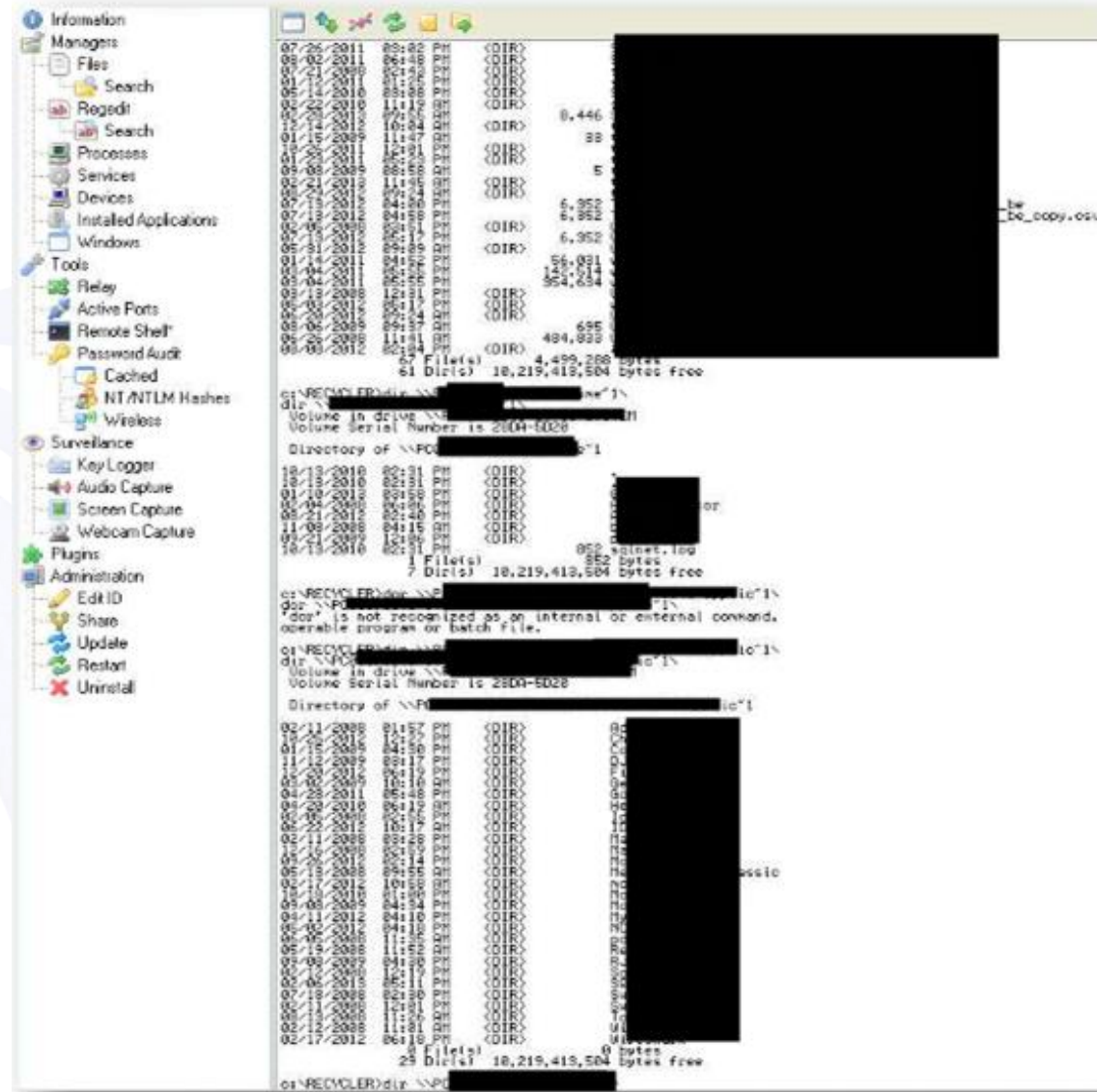
Connections Statistics Settings

ID	WAN	LAN	Con. Type	Computer	User Name	App. Type	OS	CPU	RAM	Version	Ping
	127.0.0.1	192.168.1.47	Direct	F...	...	Admin	WinXP	2194 MHz	1.99 GB	2.3.1	78
	127.0.0.1	192.168.1.2	Direct	F...	USER	Admin	WinXP	2793 MHz	989.17 MB	2.3.1	63
	127.0.0.1	192.168.1.1	Direct	F...	SYSTEM	Admin	WinXP	2260 MHz	2 GB	2.3.1	63
	127.0.0.1	192.168.1.50	Direct	M...	SYSTEM	Admin	WinXP	2993 MHz	2 GB	2.3.1	Last seen: 16:09/13.03.04
server	127.0.0.1	192.168.1.1	Direct	N...	SYSTEM	Admin	Win2k	927 MHz	511.55 MB	2.3.1	125
server	127.0.0.1	192.168.1.1	Direct	S...	SYSTEM	Admin	Server2003	1995 MHz	2 GB	2.3.1	141
	127.0.0.1	192.168.1.5	Direct	F...	SYSTEM	Admin	WinXP	2793 MHz	2 GB	2.3.1	Last seen: 15:43/13.03.04
	127.0.0.1	192.168.1.5	Direct	F...	SYSTEM	Admin	WinXP	2793 MHz	2 GB	2.3.1	188
	127.0.0.1	192.168.1.50	Direct	M...	SYSTEM	Admin	WinXP	2993 MHz	2 GB	2.3.1	110

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).

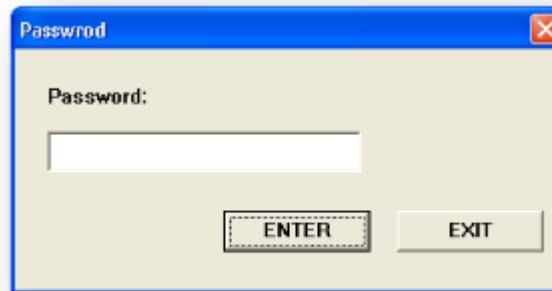
Screenshot vom APT1 Attacker
mit Fernzugriff auf die Besucherzeiten



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...



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) **FAA702 Operations**
Two Types of Collection

Upstream

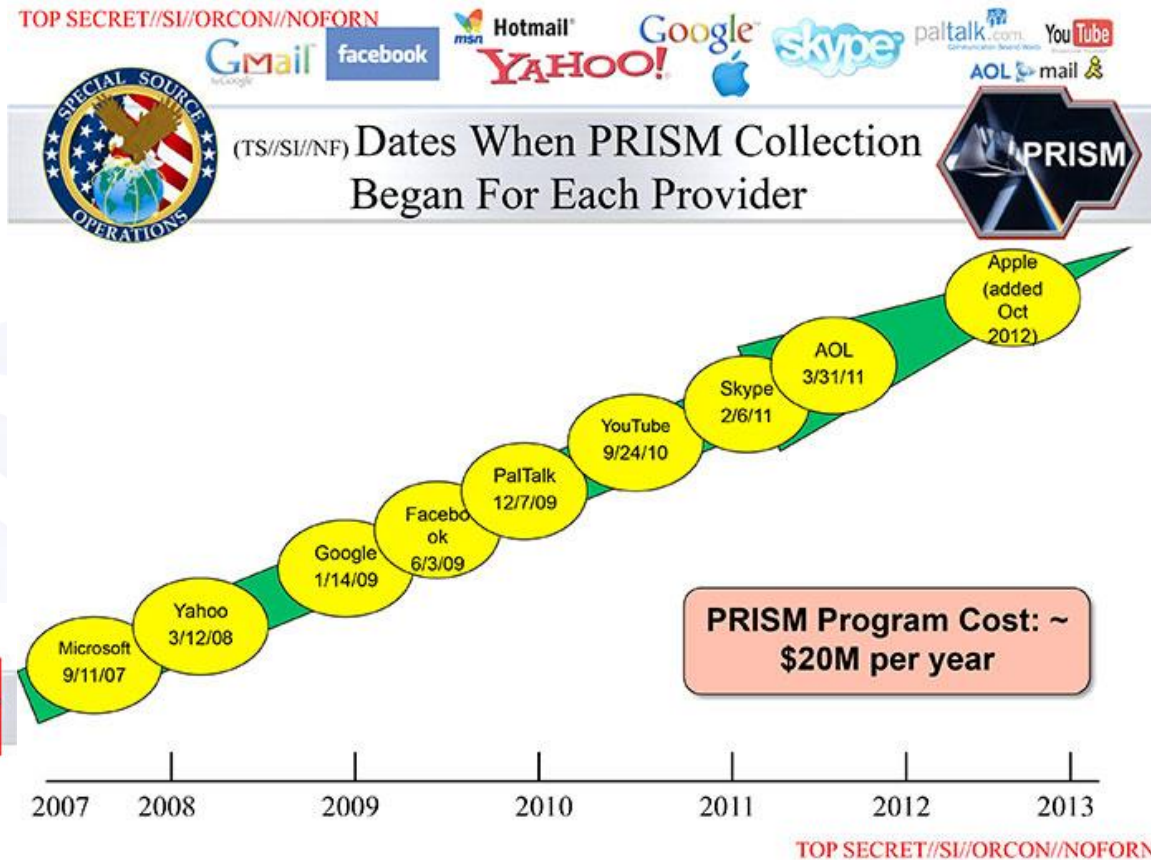
- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, [REDACTED], BLARNEY, [REDACTED])

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

You Should Use Both

TOP SECRET//SI//ORCON//NOFORN



- **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

Absurdität

Scheinheiligkeit

Sorglosigkeit

Verbesserung des Datenschutzes,
Zurückgreifen auf nicht überwachte IT,
Selbstschutz der Firmen (und Regierungen)
gegen Spionage.

Schutz gegen Terrorismus ist notwendig, aber
Überwachung äußerst ineffektiv (vgl. Boston
Marathon).
Die USA ändern ihre Haltung nicht.

Wenn wir gewusst hätten, dass ...

Nichts aus Echelon und SWIFT gelernt,
Die amerikanischen Absichten sind offensichtlich.
Schlecht vorbereitete Regierungen und Firmen.

Danke für Ihre
Aufmerksamkeit

Carlo Harpes
harpes (at) itrust.lu