FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Offene und verdeckte technische Ermittlungswerkzeuge zwischen Theorie und Praxis

Felix Freiling

Carl Friedrich von Weizsäcker Friedensvorlesung
Universität Hamburg, 30.10.2013

§5 Absatz 2 Nr. 11
Verfassungsschutzgesetz NRW vom 20.12.2006

- Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:

  [...]

  11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.

Fragenkatalog BVerfG, Frage 4

Wie sind die schon bisher durchgeführten "Online-Durchsuchungen" technisch durchgeführt worden und welche Schwierigkeiten und Erfolge hat es gegeben?

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Fragestellungen

- Welche Arten von verdeckten technischen Ermittlungsinstrumenten gibt es und wie funktionieren sie?
- Wann sind verdeckte technische Ermittlungsinstrumente angebracht?
- Gibt es Alternativen?

Fahnder: Massiver Eingriff - SPIEGEL ONLINE - Nachrichten - Netzwelt - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.spiegel.de/spiegel/0,1518,748110,00.html

spiegel lka bayern

Fahnder: Massiver Eingriff - SPIEGEL ...

28.02.2011

Drucken | Senden | Feedback | Merken

Fahnder

Massiver Eingriff

Von Steffen Winter

Thomas Einberger/ Argum

Rechtsanwalt Schladt: 60.000 Bildschirmfotos auf zwei DVDs

Das bayerische Landeskriminalamt setzte bei Ermittlungen ein rechtswidriges Spionageprogramm ein. Der Fall wird die Debatte über staatliche Cyber-Angriffe neu befeuern.

Fertig

Analyse und Vergleich von BckR2D2-I und II

Andreas Dewald[*], Felix C. Freiling[**], Thomas Schreck[**], Michael Spreitzenbarth[**], Johannes Stüttgen[**], Stefan Vömel[**], und Carsten Willems[***]

[*]Universität Mannheim
[**]Friedrich-Alexander Universität Erlangen-Nürnberg
[***]Ruhr-Universität Bochum

Abstract: Im Oktober 2011 erregte die Veröffentlichung von Details über die inzwischen meist als *BckR2D2* bezeichnete Schadsoftware öffentliches Aufsehen. Mitglieder des *Chaos Computer Club e.V.* veröffentlichten einen ersten Bericht über die Funktionsweise des Trojaners, dem weitere Analysen folgten. In dieser Arbeit geben wir einen Überblick über die bislang veröffentlichen Einzelberichte und über die verschiedenen Komponenten der Schadsoftware sowie deren Funktionsweise. Hierzu präsentiert diese Arbeit die wesentlichen Ergebnisse einer ausführlichen Analyse aller Komponenten des Trojaners und geht insbesondere auf Unterschiede zwischen den beiden bislang bekannten Varianten BckR2D2-I und II ein. Ziel dieser Arbeit ist auch die kritische Überprüfung der von anderen Autoren getroffenen Aussagen über die Schadsoftware.

1 Einleitung

Im Laufe des Jahres 2011 wurden verschiedene Versionen der inzwischen als *BckR2D2* bezeichneten Schadsoftware bekannt. Eine erste Analyse wurde Anfang Oktober 2011 durch den *Chaos Computer Club e.V.* (CCC) in Form einer Presseerklärung sowie eines dazugehörigen

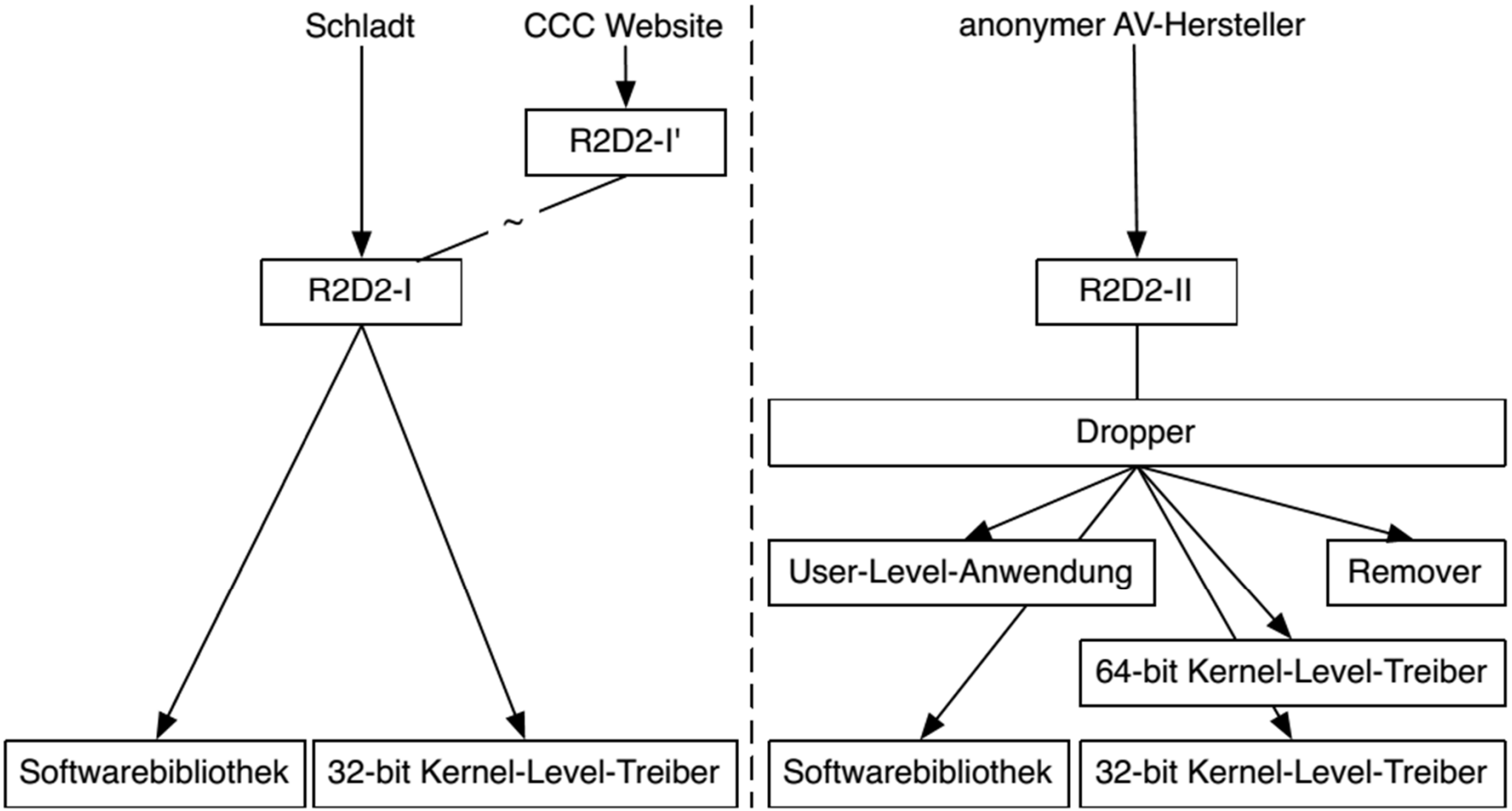


Abbildung 1. Herkunft und Komponenten der unterschiedlichen Versionen von *BckR2D2*.

Überwachte Anwendungen

R2D2-I (2009)

- skype.exe
- skypepm.exe
- msnmsgr.exe
- x-lite.exe
- yahoomessenger.exe
- explorer.exe

R2D2-II (2010)

- skype.exe
- skypepm.exe
- msnmsgr.exe
- x-lite.exe
- yahoomessenger.exe
- explorer.exe
- paltalk.exe
- voipbuster.exe
- simppro.exe
- simplite-icq-aim.exe
- icqlite.exe
- firefox.exe
- opera.exe
- lowratevoip.exe.

Interaktionsmöglichkeiten von Außen

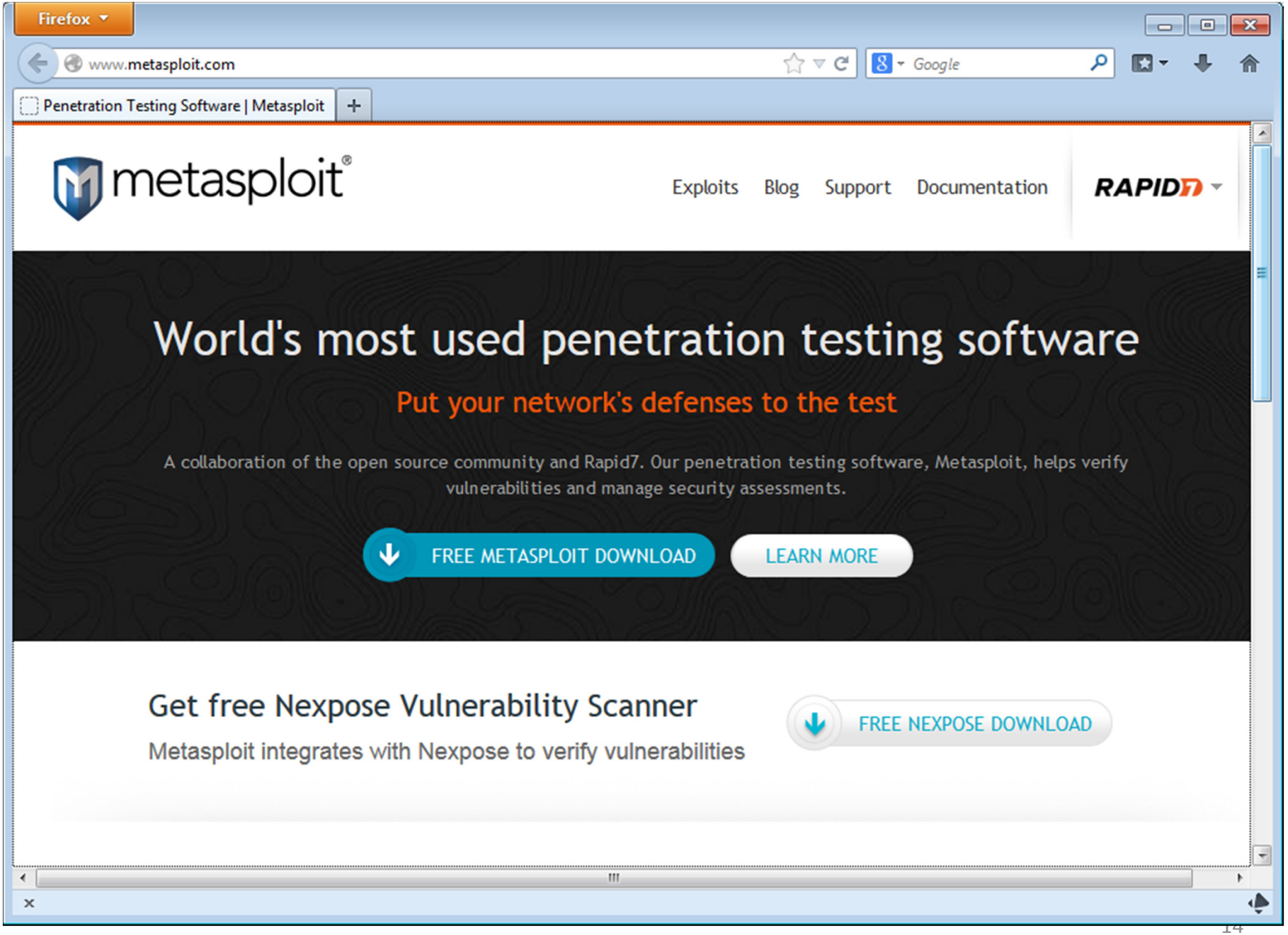
Kommando	Beschreibung	I	II
0x02	Anfertigung von Bildschirmschnappschüssen von aktiven Fenstern eines Internetbrowsers	x	
0x03	Erstellung eines dedizierten Threads, der periodische Bildschirmschnappschüsse des kompletten Bildschirms anfertigt	x	
0x04	Entfernung des Kernel-Level-Treibers, Einrichtung der Schadsoftware im Applikationsverzeichnis des Benutzers	x	x
0x05	Aktualisierung der Schadsoftware über das Netzwerk	x	x
0x06	Herunterfahren des Systems per `ExitWindowsEx()` (`EWX_SHUTDOWN`, `EWX_FORCE`)	x	x
0x07	Herunterfahren per `KeBugCheckEx()` (erzeugt einen *Blue Screen of Death*)	x	x
0x08	Abfrage der installierten Anwendungen und Programme	x	
0x09	Erstellung eines weiteren Threads, der periodische Bildschirmschnappschüsse anfertigt (Code ähnlich zu Kommando `0x03`)	x	
0x0C	Entgegennahme mehrerer (unbekannter) Parameter über das Netzwerk	x	x
0x0D	Anfertigung von Bildschirmschnappschüssen von bestimmten Fenstern im Vordergrund, unter anderem auch Internetbrowsern (ähnlich zu Kommando `0x02`)	x	
0x0E	Übertragung und Ausführung einer beliebigen Datei	x	x
0x10	Noch unbekannt	x	x
0x11	Noch unbekannt	x	x
0x12	Null-Rückgabe	x	

Tabelle III
UNTERSTÜTZTE KOMMANDOS DER SCHADSOFTWAREBIBLIOTHEK IN DEN BEIDEN TROJANER-VARIANTEN (X = FUNKTIONALITÄT VORHANDEN)

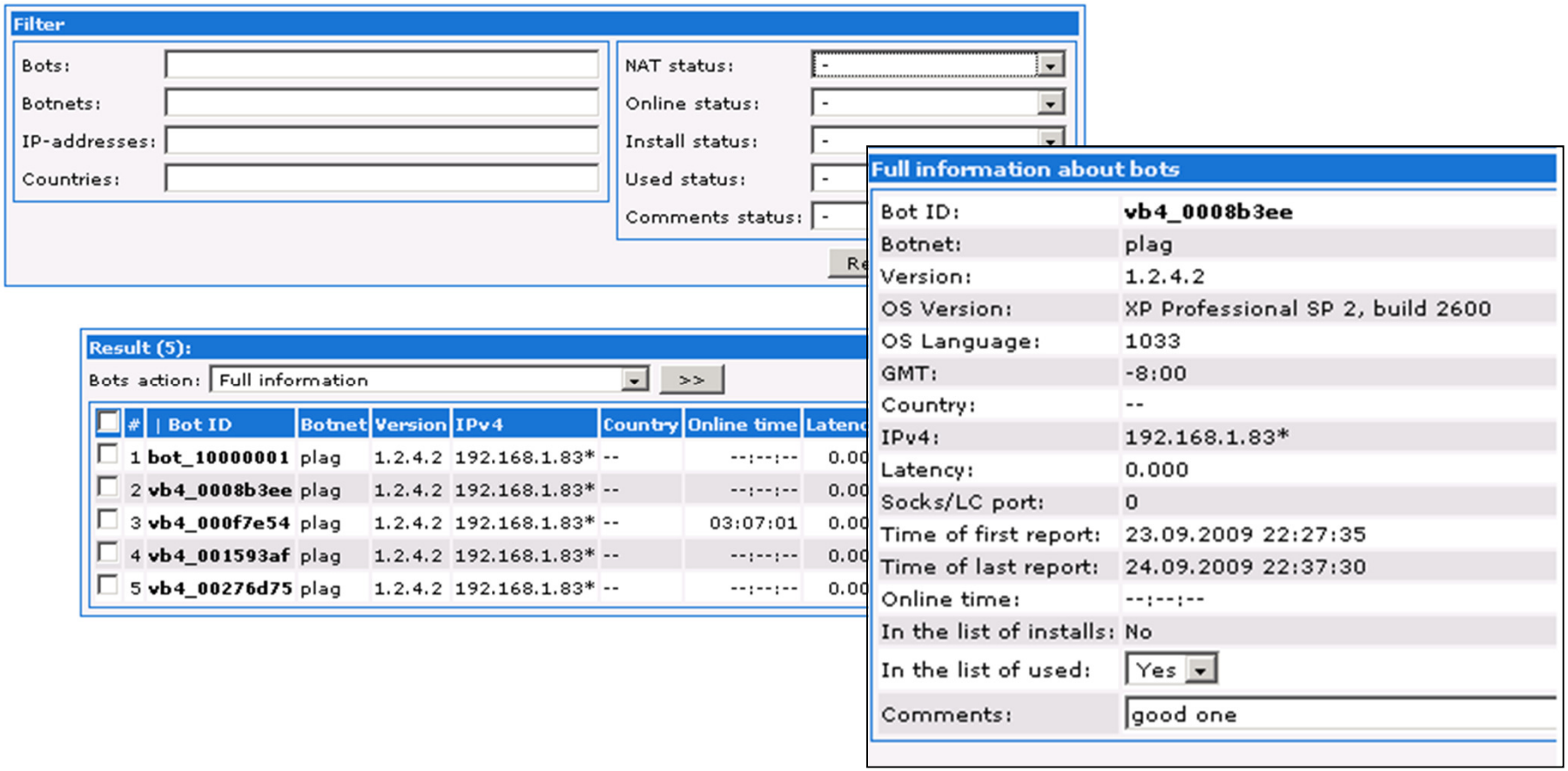
Verdeckte technische Ermittlungsinstrumente

... anlassunabhängige Überwachung
des Internet ...

... verdeckter Einsatz technischer Mittel ...

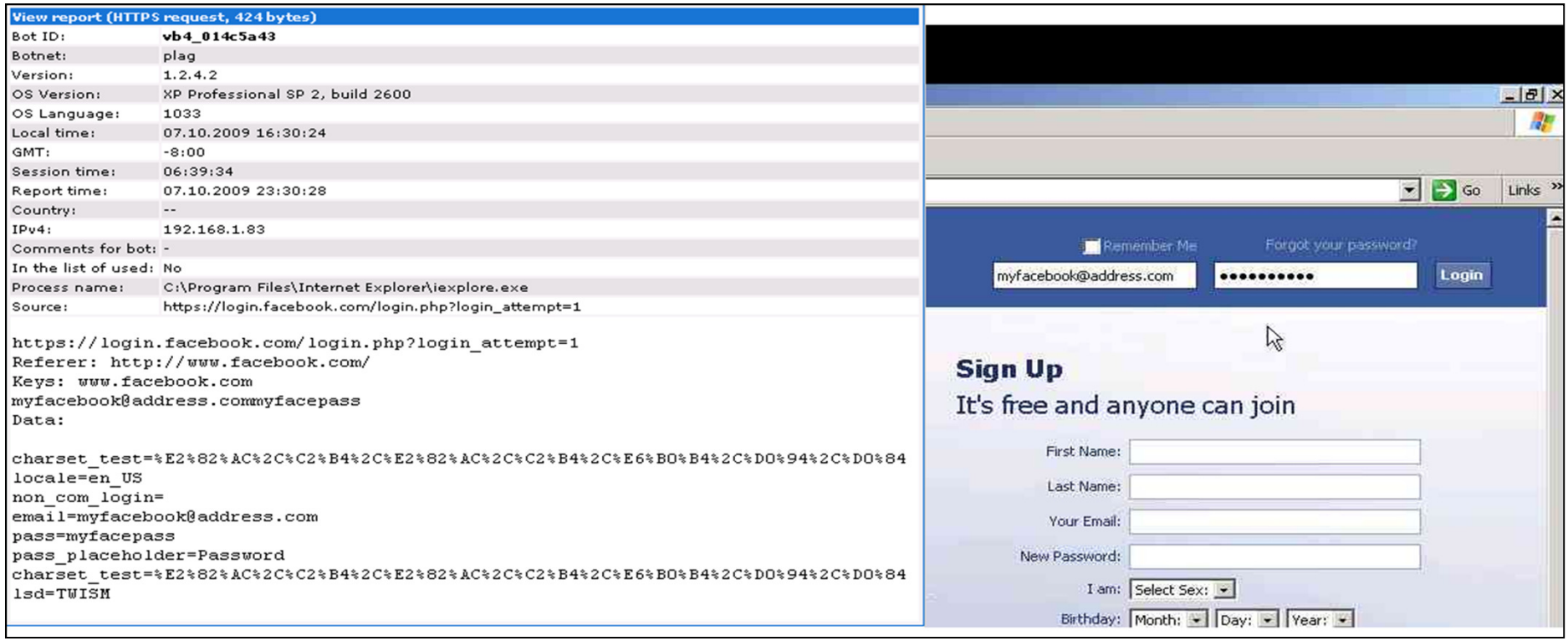

Firefox
www.metasploit.com
Google
Penetration Testing Software | Metasploit
metasploit
Exploits
Blog
Support
Documentation
RAPID7
World's most used penetration testing software
Put your network's defenses to the test
A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.
FREE METASPLOIT DOWNLOAD
LEARN MORE
Get free Nexpose Vulnerability Scanner
Metasploit integrates with Nexpose to verify vulnerabilities
FREE NEXPOSE DOWNLOAD

Moderne Trojaner: ZeuS



(Quelle: Fortinet, 2009))

ZeuS



View report (HTTPS request, 424 bytes)

Bot ID:	**vb4_014c5a43**
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	07.10.2009 16:30:24
GMT:	-8:00
Session time:	06:39:34
Report time:	07.10.2009 23:30:28
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	https://login.facebook.com/login.php?login_attempt=1

```
https://login.facebook.com/login.php?login_attempt=1
Referer: http://www.facebook.com/
Keys: www.facebook.com
myfacebook@address.commyfacepass
Data:

charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%BO%B4%2C%DO%94%2C%DO%84
locale=en_US
non_com_login=
email=myfacebook@address.com
pass=myfacepass
pass_placeholder=Password
charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%BO%B4%2C%DO%94%2C%DO%84
lsd=TWISM
```


(Quelle: Fortinet, 2009))

Gestaltungsvarianten

Verdeckte Existenz

Verdeckter Zweck

Ermittlungsziele: Zugriff auf ...

Datenverkehr		Gesamtsystem
„Quellen-TKÜ“	<	„Online-Durchsuchung“

Ermittlungsziele: Zugriff auf ...

Datenverkehr		Gesamtsystem
„Quellen-TKÜ“	$\leq$	„Online-Durchsuchung“

Wann sind verdeckte technische Zugriffe angebracht?

Welche Alternativen gibt es?

Zugriff auf verschlüsselte Datenträger

- Hardware Keylogger (verdeckt)
- offene Beschlagnahme im laufenden Zustand
  - Cold Boot (falls Rechner gesperrt, Standby oder gerade ausgeschaltet)
  - Hot Plug (falls gesperrt, Standby)
- Live-Durchsuchung (über das Netz)
  - Sofern durchsuchter Rechner nicht anderweitig infiltriert


http://citp.princeton.edu/memory

Zugriff auf verschlüsselte Kommunikation

- Herstellerkooperation, Verwendung eines modifizierten Clients
- Kommunikationsmetadaten und andere Seitenkanäle

- Nutzung gefälschter Zertifikate, falls keine Ende-zu-Ende-Verschlüsselung

Seitenkanal in Typo3

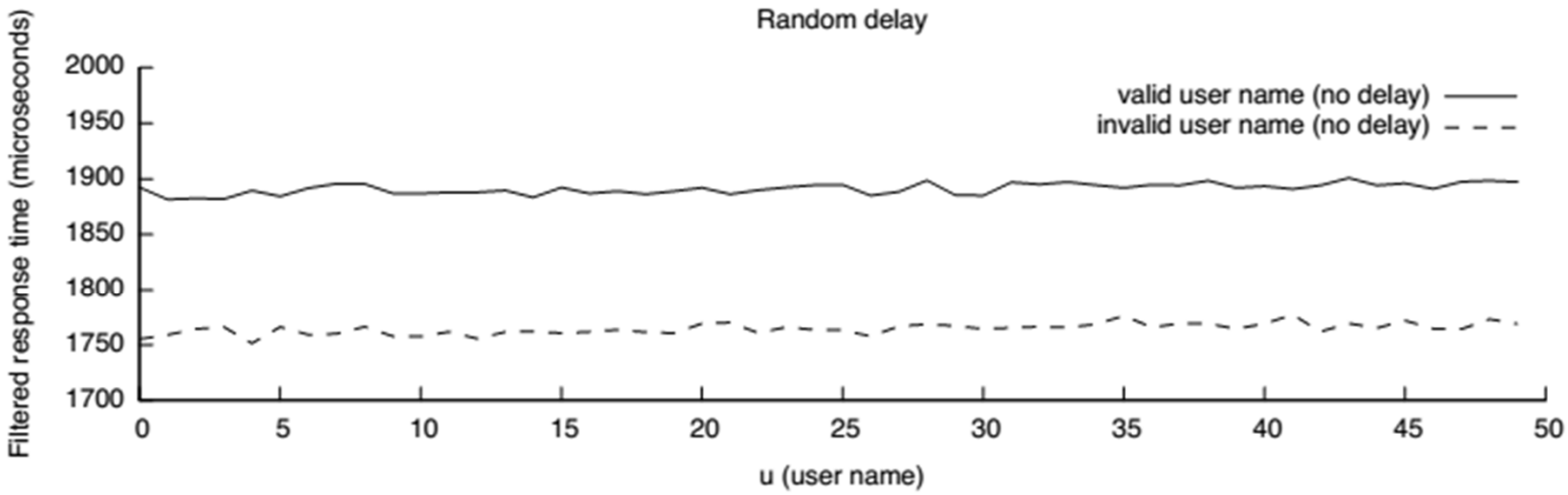


Fig. 5. Timing side channel in Typo3's login form leaks whether a user name exists or not.

Quelle: Sebastian Schinzel

Rückverfolgung

- Seitenkanäle in Verbindung mit Server-Überwachung
- Protokollschwächen

Übersicht über Alternativen

Datenträger	Kommunikation	Rückverfolgung
Hardware Keylogger	Herstellerkooperation	Seitenkanäle
Cold Boot	Seitenkanäle	Protokollschwächen
Hot Plug		
„offene Online-Durchsuchung“		

offene Maßnahmen

Maßnahmen ohne Infiltration

Nachrichtendienste


Josef Foschepoth
Überwachtes Deutschland
Post- und Telefonüberwachung in der alten Bundesrepublik
Fernsprecher
Vandenhoeck & Ruprecht

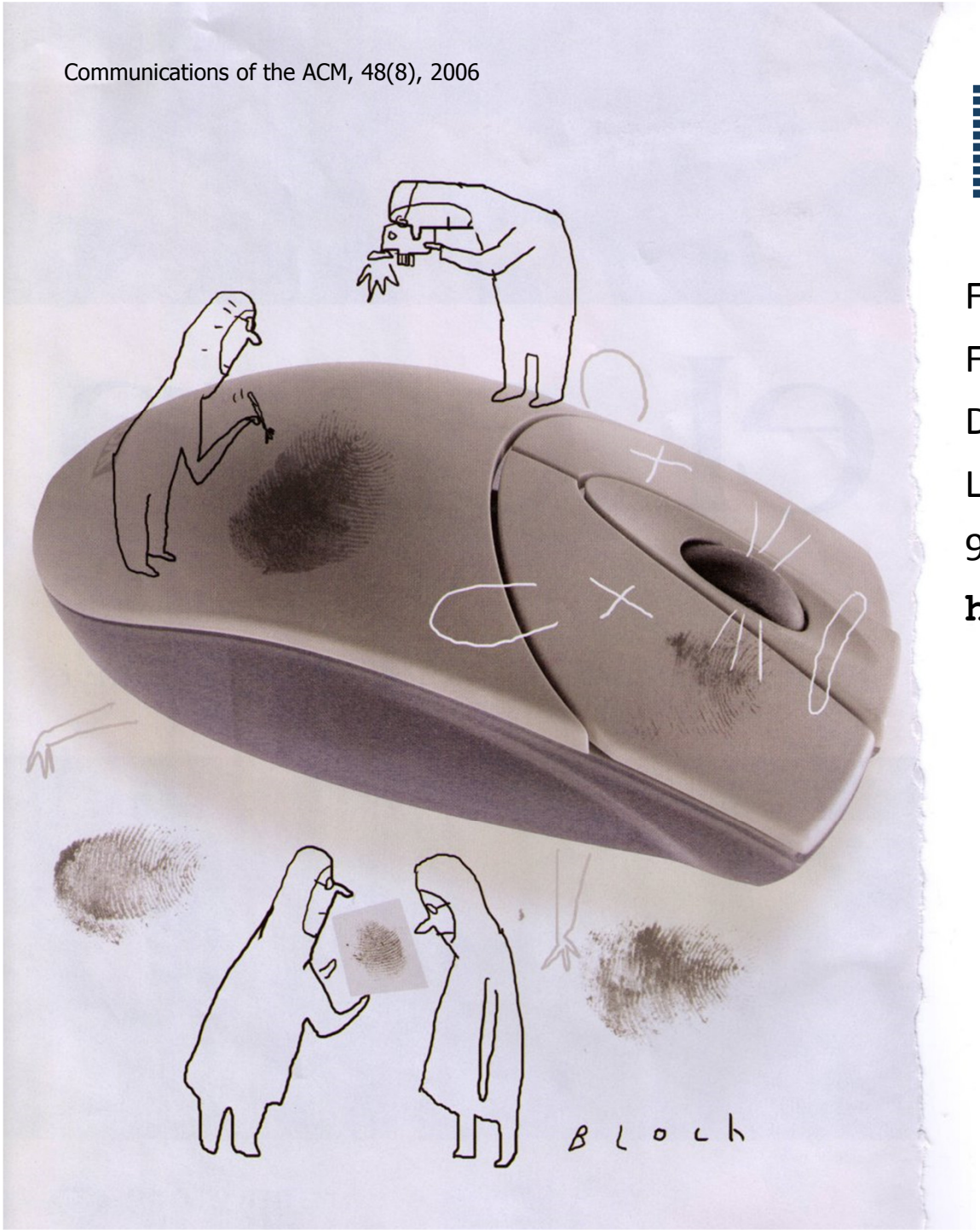
... und Internetunternehmen

- Zunehmende Datenanalyse großer Internetunternehmen (Facebook, Google, Apple, ...) zu Werbezwecken
- Nahezu unregulierte Erstellung von Benutzerprofilen
- Unmerkliche und massive Erosion der Privatsphäre mit unabsehbaren Folgen

- Universelles Ermittlungsinstrument der Zukunft? Für wen?

Technik ist ein Mittel des verständigen Willens. Soweit unsere Vernunft ausreicht, kann Technik gesteuert werden; Technik kann aber kein Versagen der Vernunft ausgleichen. Das Besondere der heutigen Lage ist, dass die Erhöhung der technischen Mittel Forderungen an die Vernunft stellt, die vorher unbekannt waren. Wir müssen das Ganze der technischen Zivilisation mit seinen Rückwirkungen aufs Leben des Menschen und der Natur, deren Kind der Mensch ist, wahrnehmen. Fraglich ist, ob wir das können. Gewiss ist, dass wir es nicht tun. Notwendig ist nunmehr, es zu versuchen.

Carl Friedrich von Weizsäcker, Wege in der Gefahr



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Felix Freiling

Friedrich-Alexander-Universität

Department Informatik

Lehrstuhl für Informatik 1

91058 Erlangen

https://www1.cs.fau.de

Abstract

Seit der Veröffentlichung des "Bayerntrojaners" durch den CCC im Jahr 2011 sind verdeckte technische Ermittlungsinstrumente wie die "Online-Durchsuchung" und die "Quellen-Telekommunikationsüberwachung„ in aller Munde. Wie funktionieren diese Technologien? Welche forensisch verwertbaren Spuren kann man mit ihnen erhalten? Unter welchen Bedingungen dürfen sie eingesetzt werden? Im Rahmen dieses Vortrages wird eine kritische Bestandsaufnahme dieser Technologien versucht. Im Ausblick werden auch Bezüge zu nachrichtendienstlichen und militärischen Handlungsoptionen aufgezeigt.