Threat Landscape 2013

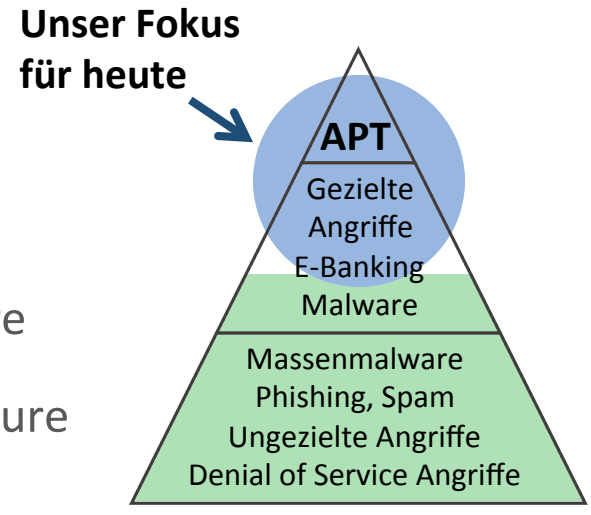
Fortgeschrittene Angriffe, Data Leakage
und Wirtschaftsspionage

ISACA After Hours Seminar, 25. Juni 2013
Renato Ettisberger & Adrian Leuenberger

IOprotect

Vergessen Sie für 1 Stunde...

- Aktivisten
- Skript Kiddies
- E-Banking Malware
- und ähnliche Akteure



IOprotect

Disclaimer

Das wollen wir nicht erreichen:

IOprotect

Bildquelle: [1]

Über IOprotect GmbH

2013 gegründet von Rolf Gartmann, Adrian Leuenberger und Renato Ettisberger.

Alles ehemalige Mitglieder eines Incident Response Teams.

Zusammen mehr als 35 Jahre Erfahrung im Bereich Informationssicherheit.

IOprotect

Background

- Beteiligung am Aufbau und Betrieb der Melde- und Analysestelle für Informationssicherung (MELANI).
- Weitere Stichworte:
  - Penetration Testing, Reviews und Audits, IT-Forensik, Reverse Engineering fortgeschrittener Malware, detaillierte Analyse von Schwachstellen, Exploit Entwicklung, Awareness Schulungen.

Inhalt

- Angriffe im 2013
  - Wer ist das Ziel,...
  - ...wie laufen die Angriffe derzeit ab und...
  - ...wieso sind sie erfolgreich?
- Umgang mit APT
  - Optimierung der Detektionsrate
  - Wie werden Sie Malware und Schwachstellen los?
  - Dos und Don‘ts im Umgang mit gezielten Angriffen

Definition – Advanced

Advanced

Means the adversary can operate in the **full spectrum** of computer intrusion. They can use the most pedestrian **publicly available exploit** against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and **develop custom exploits**, depending on the target's posture.

Quelle: [2]

Definition – Persistent

Persistent

Means the adversary is formally tasked to accomplish a **mission**. They are not opportunistic intruders. Like an intelligence unit they receive directives and work to **satisfy their masters**. Persistent does not necessarily mean they need to constantly execute malicious code on victim computers. Rather, they maintain the level of interaction needed to **execute their objectives**.

Quelle: [2]

Definition – Threat

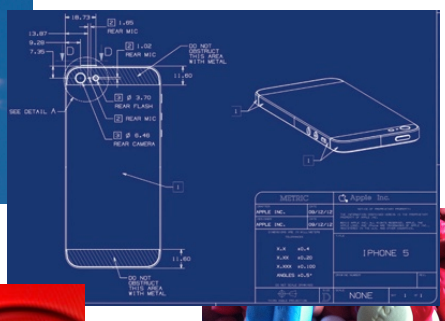
Threat

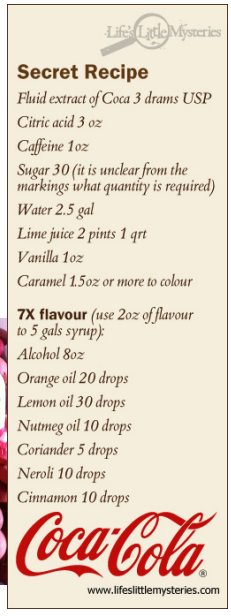
Means the adversary is not a piece of mindless code. […] Rather, the adversary here is a threat because it is **organized** and **funded** and **motivated**. Some people speak of multiple "groups" consisting of dedicated "crews" with various missions.

IOprotect

 Quelle: [2]

Ziele?





IOprotect

 Bildquellen: [3,4,5,6,7]

Angriffe 2013

ISACA After Hours Seminar, 25. Juni 2013

Entdeckung von APTs

APT werden entdeckt, weil

- Angreifer Fehler machen
- Zu „laut“ sind
- Kommissar Zufall

Aber:

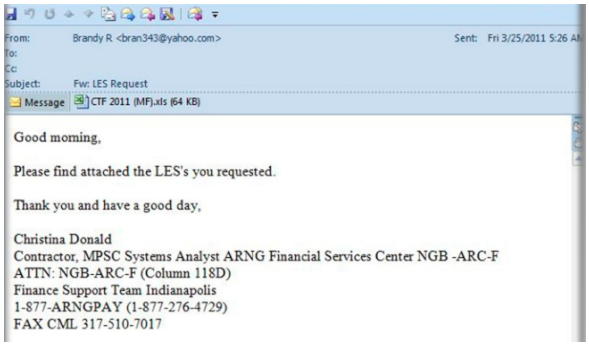
Sind üblicherweise bereits Wochen oder Monate aktiv!

Angriffsvektoren: Spam-Mail

E-Mails werden immer wieder über Wochen an beliebige Mitarbeiter einer Firma gesandt

Sollen in der üblichen Spam-Flut untergehen → Keine Mass-Mails

Hoffnung: Ein Mitarbeiter wird den Anhang schon öffnen



IOprotect

Bildquellen: [8]

Angriffsvektoren: Spear-Phishing

Gezielt verfasste und adressierte E-Mails

Meist Mailanhänge, vereinzelt URLs

Opfer werden über längeren Zeitraum ermittelt

Inhalt soll von Berufs wegen Interesse wecken

Absender häufig gefälscht

IOprotect

Angriffsvektoren: Watering Hole

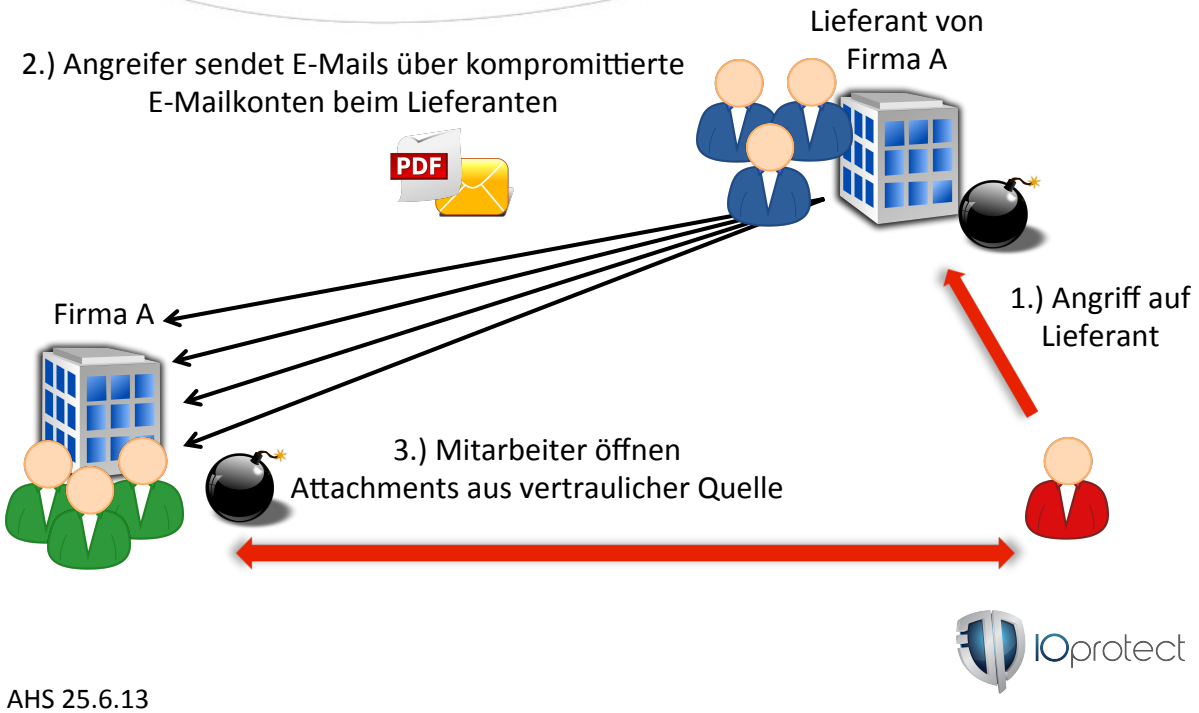
Angreifer kompromittieren Webseiten, die ihre Opfer mit hoher Wahrscheinlichkeit irgendwann besuchen

Bildquellen: [9,10]

Angriffsvektoren: Social Media

Bildquelle: [11]

Angriffsvektoren: Via Lieferanten



IOprotect

Häufig betroffene Applikationen

CVE-2011-2462
CVE-2011-0611
CVE-2013-0640
CVE-2013-0641
...

CVE-2011-0609
CVE-2011-0611
CVE-2012-0779
CVE-2013-0630

CVE-2010-0249
CVE-2012-4792
CVE-2012-1347
...

CVE-2012-0422
CVE-2013-1493
CVE-2013-2423
...

CVE-2010-3333
CVE-2012-0158

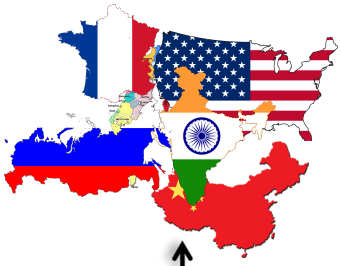
IOprotect

Kombinierte Angriffe

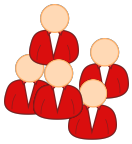
IOprotect

Wer steckt dahinter?

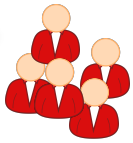
Staaten



Gruppierungen, die Infos an Staaten verkaufen



Gruppierungen, die Infos an Unternehmen verkaufen



Exploit-Seller

IOprotect

Exploit-Markt

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

VUPEN Security
@VUPEN

Next week, we will be attendi
Prague. Demo of our offensiv
will be held on Jun 5th, 2013
Govs only

Reply Retweet Favorite More

"My job was to have 25
defense contractor that
exploits for government use.

IOprotect

Bildquellen: [12,13]

Beispiel: ItaDuke/MiniDuke

Bekannt geworden im Februar 2013

Im Visier: Botschaften, Regierungsstellen, Think Tanks und Privatunternehmen in 23 Ländern

Angriffe erfolgten via PDF-Dateien

Später „geklaut“ und modifiziert von anderen APT-Gruppierungen

IOprotect

Beispiel: ItaDuke/MiniDuke

Sehr fortgeschrittener Angriff

- Unbekannte Schwachstelle in Adobe Reader/Acrobat
- Umgehen von Schutzmassnahmen auf OS-Ebene (DEP/ASLR-Bypass)
- Verschiedene Versionen von Adobe Reader unterstützt
- Ausbruch aus der Sandbox

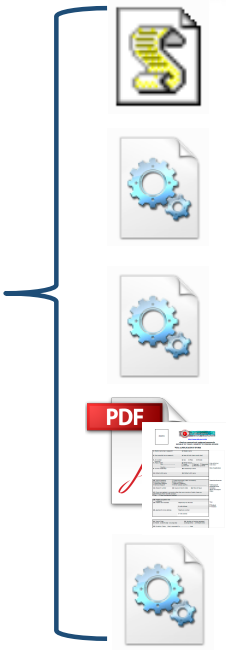
Zwei Gruppierungen nutzen gleichen Exploit

Unklar, ob vom gleichen „Lieferanten“ eingekauft

IOprotect

Inhalt des maliziösen PDF

CVE-2013-0640
CVE-2013-0641



JavaScript-Code

D.T (Windows-DLL)

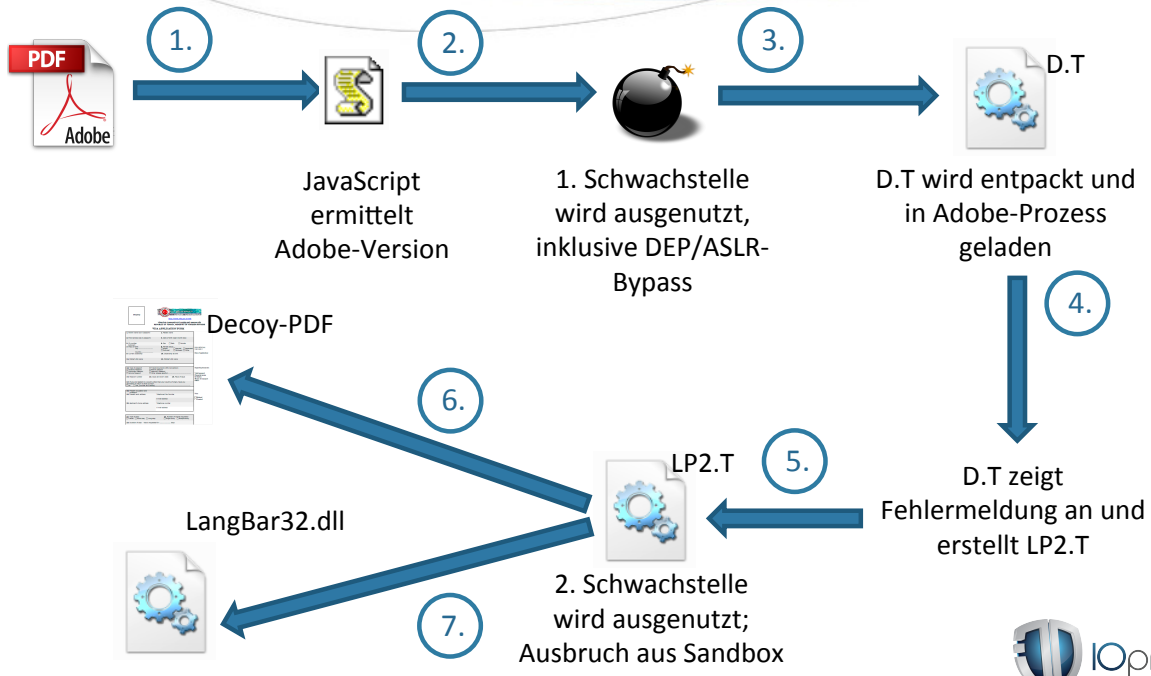
LP2.T (Windows-DLL)

Ablenkungs-PDF

LangBar32.dll (Windows-DLL)

IOprotect

Ablauf



IOprotect

Sandbox-Ausbruch notwendig

winlogon.exe		464		1'540 K	4'748 K
explorer.exe	Medium	1832	0.08	125'092 K	94'308 K
cmd.exe	Medium	1892		2'496 K	2'584 K
AcroRd32.exe	Medium	1276		5'212 K	12'004 K
AcroRd32.exe	Low	848	0.37	9'788 K	23'852 K

Renderer-Prozess läuft in einer „Sandbox“ (Low Integrity)

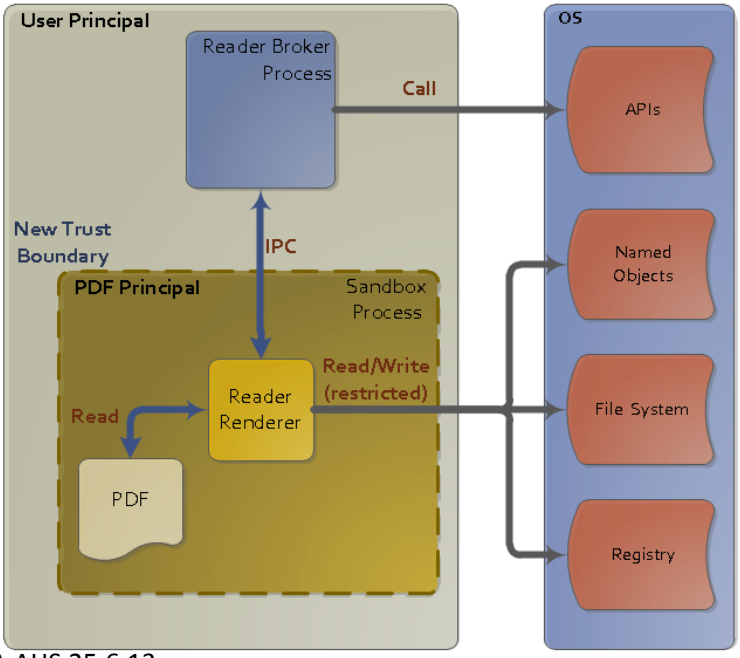
- Zugriff eingeschränkt auf bestimmte Verzeichnisse
- Wenig bis keine Rechte für Angreifer

Broker-Prozess hat Medium Integrity-Level

- Keine Einschränkungen bzgl. Verzeichnisse
- Angreifer hat Rechte des eingeloggten Benutzers

IOprotect

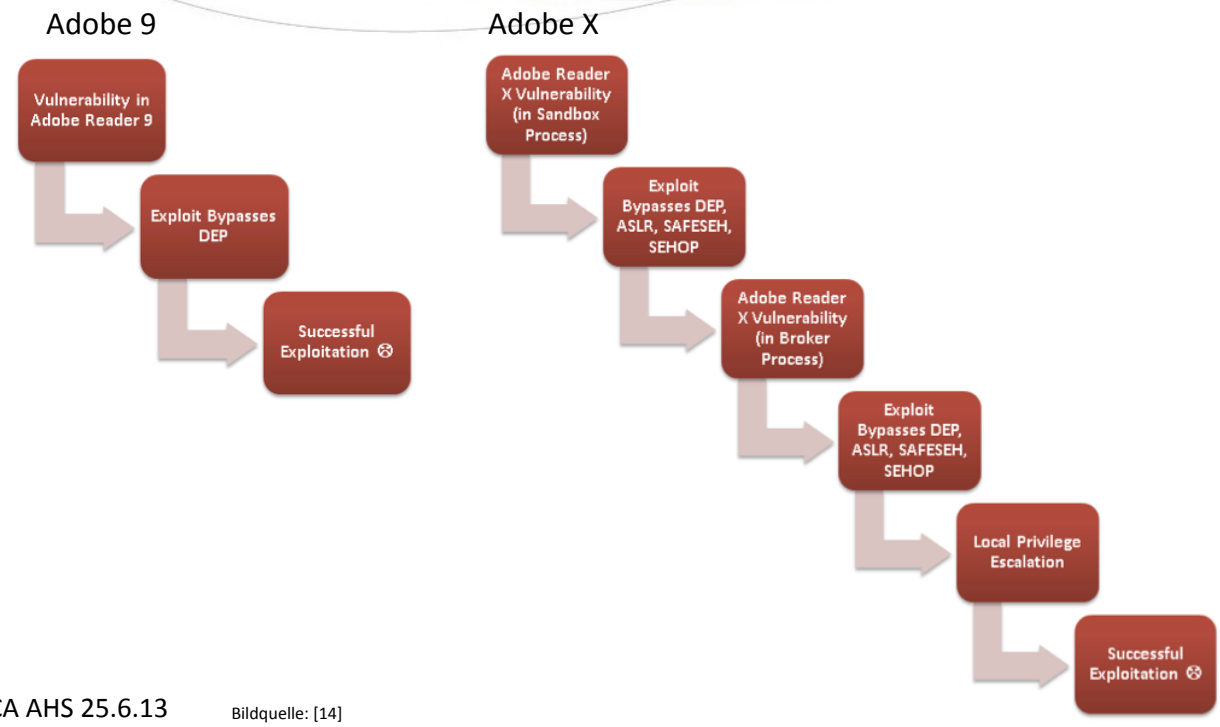
Sandbox-Architektur von Adobe



IOprotect

Bildquelle: [14]

Barriere für Angreifer drastisch erhöht



Bildquelle: [14]

Sandbox-Ausbruch via Call zu GetClipboardFormatName

```
0:003> kbc
ChildEBP RetAddr  Args to Child
0203fe00 00d3d749 0000c20e 02a9eaf4 0000009c USER32!GetClipboardFormatNameW
```

Virtual: 02a9eaf4 | Display format: Byte | Previous | Next

```
02a9eaf4 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
02a9eb10 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
02a9eb2c 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
02a9eb48 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
02a9eb64 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
02a9eb80 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 0e c2 00 00 00 00 00 00 00 00 00 00  BBBBBBBBBBBBBBBB..............
02a9eb9c 00 00 00 00 59 7f 01 64 00 00 00 94 e8 47 dc 00 00 00 2f 70 00 00 00 00 00 00 00 00  ....Y..d.....G..../p........
02a9ebb8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................................
02a9ebd4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................................
```

IOprotect

Downloader LangBar32.dll

Process Explorer Search

Handle or DLL substring: LangBar32.dll | Search

Process	PID	Type	Name
procexp.exe	808	DLL	C:\Users\user\AppData\Local\cache\LangBar32.dll
iexplore.exe	1276	DLL	C:\Users\user\AppData\Local\cache\LangBar32.dll
iexplore.exe	2208	DLL	C:\Users\user\AppData\Local\cache\LangBar32.dll
explorer.exe	3984	DLL	C:\Users\user\AppData\Local\cache\LangBar32.dll

C:\Windows\system32\cmd.exe

```
 Directory of C:\Users\user\AppData\Lo

27.05.2013  13:16    <DIR>          .
27.05.2013  13:16    <DIR>          ..
27.05.2013  13:16    <DIR>          jkduwjvfh
               0 File(s)              0 bytes
               3 Dir(s)  22'106'513'408 bytes free

C:\Users\user\AppData\Local\cache>dir /ah
 Volume in drive C has no label.
 Volume Serial Number is B4DB-D41E

 Directory of C:\Users\user\AppData\Local\cache

14.07.2009  04:37           250'880 LangBar32.dll
               1 File(s)        250'880 bytes
               0 Dir(s)  22'106'513'408 bytes free

C:\Users\user\AppData\Local\cache>_
```

IOprotect

Kommunikation mittels Twitter und Google

Edith Albert
@EdithAlbert11

Follow

Albert, my cousin. He is working hard.
uri!wp07VkkxYmfNkwN2nBmx4ch/Iu2c+G
Jow39HbphL

Reply Retweet Favorite More

2:03 p.m. - Feb 19, 201

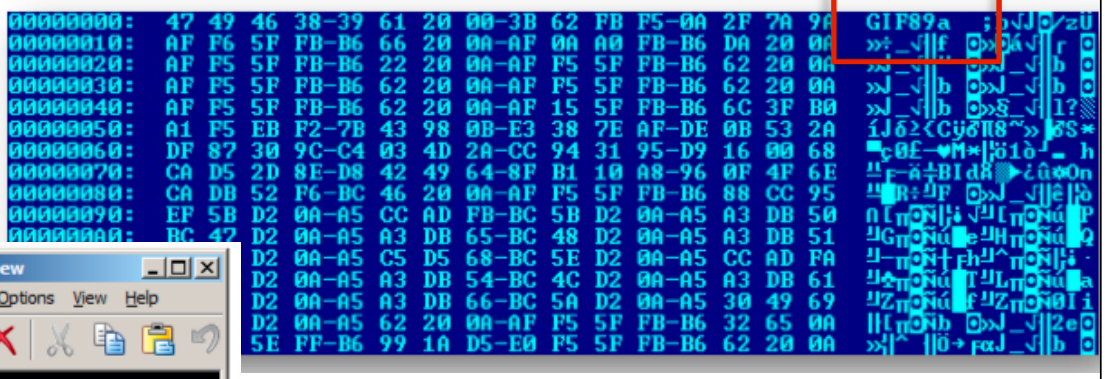
The search looks for a specific binary pattern in Google results, and by following these results the malwar
can find the files to download. Here are some example of such queries:

```
GET /search?q=3\277\200\230\345\215\017\370\274\251\215\216\364\275\307\262 HTTP/1.1
GET /search?q=3\277\200\230\345\215\017\370\274\251\215\216\364\275\307\262 HTTP/1.1
GET /search?q=\027\201\277\270\352\255\003\370\221\251\215\216\364\275\307\262 HTTP/
GET /search?q=\027\201\277\270\352\255\003\370\221\251\215\216\364\275\307\262 HTTP/
GET /search?q=3\277\200\230\345\215\017\370\274\251\215\216\364\275\307\262 HTTP/1.1
GET /search?q=3\277\200\230\345\215\017\370\224\261\204\216\336\241\316\222 HTTP/1.1
GET /search?q=3\277\200\230\345\215\017\370\274\251\215\216\364\275\307\262 HTTP/1.1
```

IOprotect

Bildquellen: [15]

Schadcode getarnt in Bildern



IOprotect

Bildquellen: [16,17]

Sicht des Opfers

IOprotect

ISACA AHS 25.6.13

Umgang mit APT

IOprotect

ISACA After Hours Seminar, 25. Juni 2013

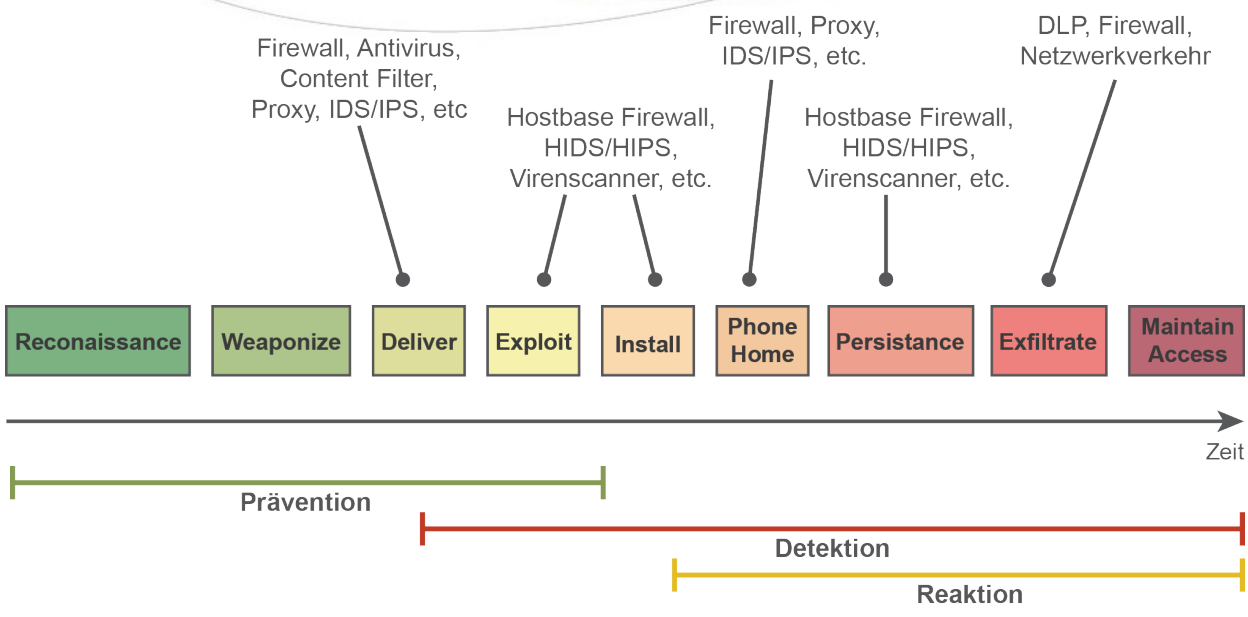
Wiederholung...

Das wollen wir nicht erreichen:

IOprotect

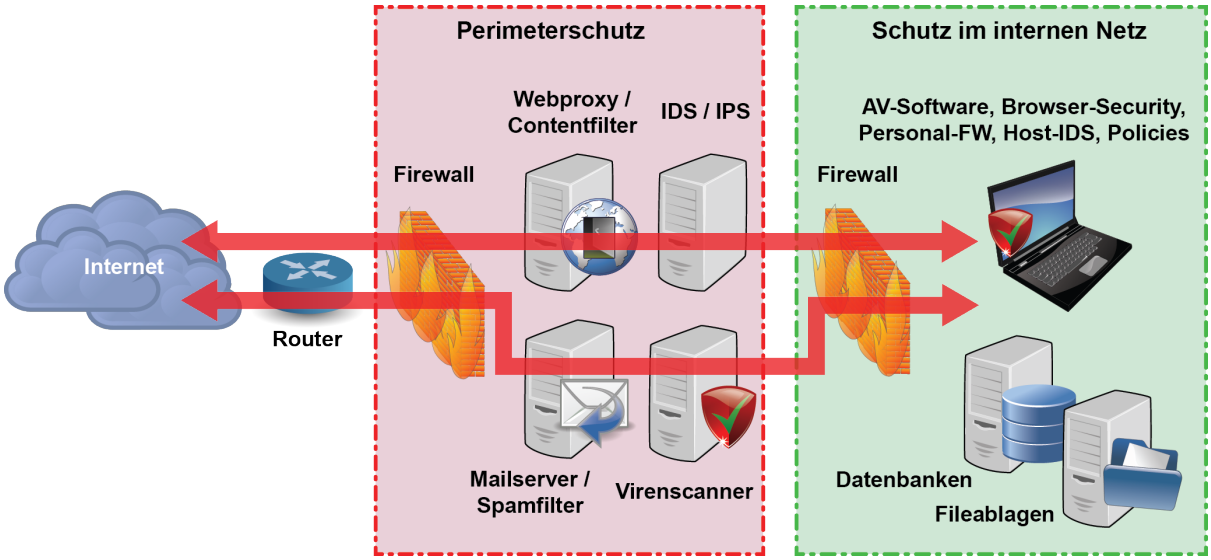
Bildquelle: [1]

"Cyber Kill Chain"



IOprotect

Prävention



IOprotect

Prävention

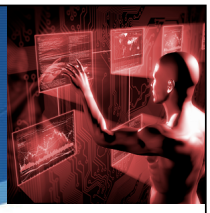
Test der eigenen Infrastruktur durch Simulation:

→ Kenntnis zu Grenzen der eingesetzten Produkte

→ Nicht blind auf die Hersteller vertrauen

IOprotect

Trigger für Detektion



- Zufall & Fehler der Akteure
- User
  - Kenntnis Helpdesk Nummer?
  - Helpdesk geschult?
- Eigene Schutzsysteme haben angeschlagen
  - Firewalls, IDS/IPS, Content Filter, DLP, SIEM, etc.

IOprotect

Trigger für Detektion

- Externe Stellen
  - Sind sie erreichbar?
  - Gibt es eine bekannte Anlaufstelle?

```
Whois für www.admin.ch:

role:    Bundesamt fuer Informatik und Telekommunikation
Address: Monbijoustrasse 74
Address: CH-3003 Bern
phone:   +41 31 325 9011
fax-no:  +41 31 325 9030
remarks:
------------------------------------------------------------
Remarks: For spam/abuse contact only abuse@bit.admin.ch
Remarks: For generall support contact noc@bit.admin.ch
Remarks: For 7*24h emergency support contact +41 31 325 8888
Remarks: E-mails to the persons below will be IGNORED!!
------------------------------------------------------------
```

IOprotect

Detektion

- Pattern basierter Ansatz sehr oft unzureichend
- Was ein Dokument bzw. ein E-Mail Anhang auf einem System auslöst ist üblicherweise nicht klar

→ Bsp. Sandbox-Ansatz zur raschen Analyse

IOprotect

Detektion

- Informationen unter anderem zu:
  - Detaillierter Ablauf nach Öffnung eines E-Mail Anhangs
  - Veränderungen am Filesystem (Modifikationen, neue Dateien etc.)
  - Veränderungen an den Einstellungen (Registry)
  - Netzwerk-Verkehr
  - Etc.

IOprotect

ISACA AHS 25.6.13

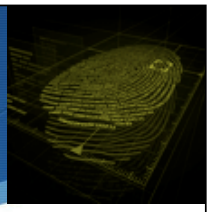
Detektion

Beispiel einer Sandbox-Analyse:

Classification / Threat Score	
Persistence, Installation, Boot Survival:	
Hiding, Stealthiness, Detection and Removal Protection:	
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:	
Spreading:	
Exploiting:	
Networking:	
Data spying, Sniffing, Keylogging, Ebanking Fraud:	

IOprotect

Reaktion



Wie ist das weitere Vorgehen nach der Detektion?

- Reine Abwehrmassnahmen
  - Eingeschränkte Analyse-Möglichkeiten
  - Weniger Chance auf Erkennung zukünftiger Incidents, weil kein Lerneffekt
- Abschottung und weitere Überwachung / Analyse
  - Stichwort: Finden des „Modus Operandi“

IOprotect

“Falsche” Reaktion

Bekannte Prozedur, wenn es rasch gehen muss:

1. Malware identifiziert
2. Betroffener Computer platt machen und neu installieren
3. Alles in Ordnung…

Probleme damit:

- Man findet nicht alles → Weiterhin Datenabfluss
- Bsp. Sample an AV-Hersteller geschickt → Globales Pattern

IOprotect

“Richtige” Reaktion

- Nötige Voraussetzungen (Forensic Readiness) vorgängig schaffen
  - Zuständigkeiten geklärt
  - Prozesse definiert
  - Datenquellen identifiziert
  - Hilfsmittel bereitgestellt
  - Kontaktnetz etabliert
  - Erfahrung durch Übung

IOprotect

“Richtige” Reaktion

- Strategie: Überlegtes und zielgerichtetes Vorgehen
- Triage & Sofortmassnahmen einleiten
- Detaillierte Analyse
- Aufarbeitung und Dokumentation
- Lessons Learned → In Forensic Readiness einfliessen lassen

Schadcode-Analyse

- Verschiedene Ebenen
  - Virenscanner
  - Malware-Sandboxen
  - Reverse Engineering (statisch und dynamisch)
- Resultate
  - Wie und wo ist die Malware auf dem System installiert?
  - Netzwerkkommunikation (Kommandopfad, Daten Exfiltration)
  - Erkenntnis: Nach was muss gesucht werden auf weiteren Systemen im Netzwerk?

Auffinden infizierter Systeme

- Suche nach weiteren Systemen mit identischem Kommunikationsverhalten
  - Netflow Daten
  - Firewall-, Proxy Logs und Mailserver Logs
- Suche auf Client-Systemen → Live Forensik
- Setzt voraus, dass die Daten vorhanden sind.
  - Stichwort „Forensic Readiness“

IOprotect

Forensic Readiness
Bsp. Forensik-Framework

Ermöglicht:

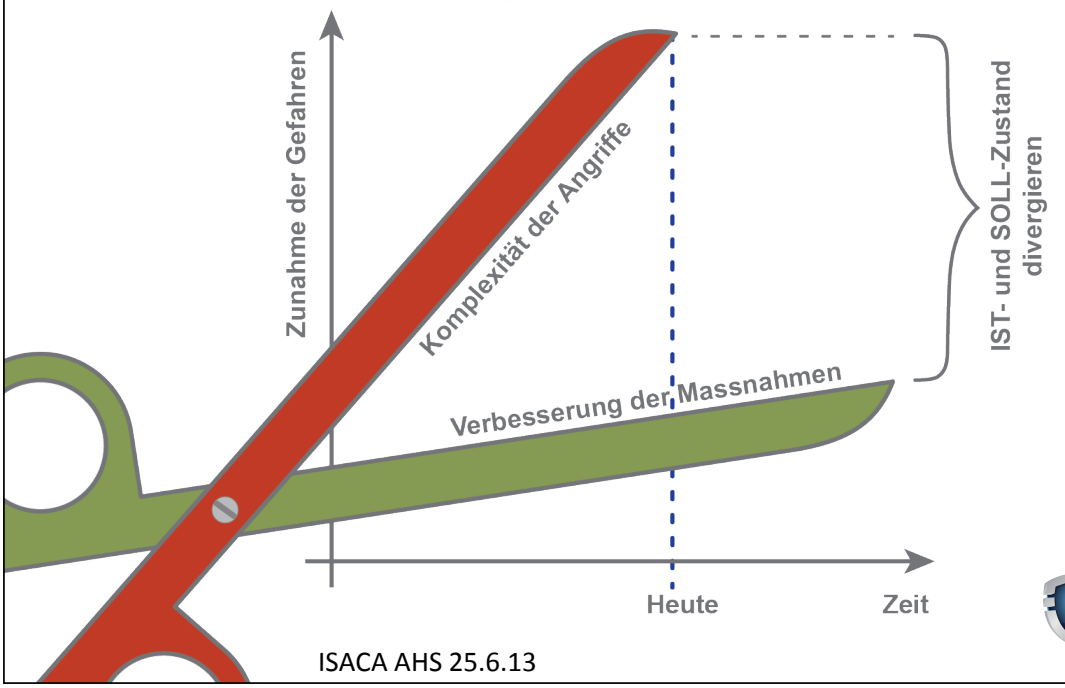
- Live Memory Analyse von Endgeräten
- Gezielte Suche nach Files

Anforderungen an ein Forensik-Framework:

- Fernzugriff auf zu untersuchende Systeme. Agent muss vorher ausgerollt sein.
- Skalierbarkeit, Erweiterbarkeit, Anpassungsmöglichkeiten
- Unterstützung verschiedener Betriebssysteme
- Automatisierung

IOprotect

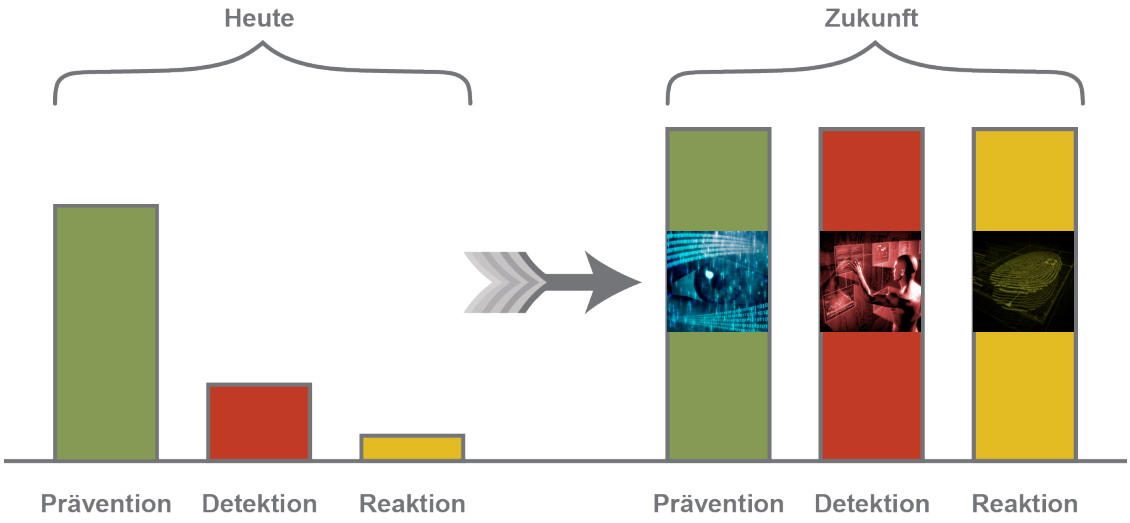
Summary



IOprotect

ISACA AHS 25.6.13

Summary



IOprotect

ISACA AHS 25.6.13

Fragen?

IOprotect GmbH
Huobstrasse 14
CH-8808 Pfäffikon SZ
+41 44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

ISACA After Hours Seminar, 25. Juni 2013

Quellangaben

[1] http://www.straussenfarm-riederfelde.de/mediapool/128/1285102/resources/24478409.jpg
[2] http://taosecurity.blogspot.ch/2010/01/what-is-apt-and-what-does-it-want.html
[3] https://en.wikipedia.org/wiki/File:Lockheed_Martin_F-22A_Raptor_JSOH.jpg
[4] https://commons.wikimedia.org/wiki/File:Assorted_Pills_3.JPG
[5] http://www.irepairvero.com/wp-content/uploads/2011/07/iRepairIT-iPhone5-Blueprint.jpg
[6] http://www.thelocal.ch/userdata/images/article/0084f730e5e4dc474cb3df10991d0ad688be8b8bbe9aa8ce9bd5dbb57b8ecd53.jpg
[7] http://i.livescience.com/images/i/000/048/362/i02/cokerecipe.jpg?1324346893
[8] http://contagiodump.blogspot.com
[9] http://1funny.com/wp-content/uploads/2009/06/water-hole.jpg
[10] http://blogs.scientificamerican.com/tetrapod-zoology/2013/02/04/crocodiles-attack-elephants/
[11] http://www.cybersquared.com/apt_targetedattacks_within_socialmedia/
[12] http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews
[13] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
[14] http://blogs.adobe.com/asset/2010/10/inside-adobe-reader-protected-mode-part-1-design.html
[15] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24297/en_US/McAfee_Labs_Threat_Advisory_MiniDuke.pdf
[16] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24297/en_US/McAfee_Labs_Threat_Advisory_MiniDuke.pdf
[17] http://www.securelist.com/en/downloads/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf