

IOCS UND THREAT INTEL

SCHNELLERE AUFKLÄRUNG VON SICHERHEITSVORFÄLLEN

DATUM: OKT 04.OKTOBER 2016

Mathias Fuchs

Vorstellung

MATHIAS FUCHS

- Senior Consultant
 - Incident Response
 - Redteaming
 - QSA
- SANS Instructor
 - FOR508
 - Advanced Digital Forensics and Incident Response
- Twitter
 - @mathias_fuchs

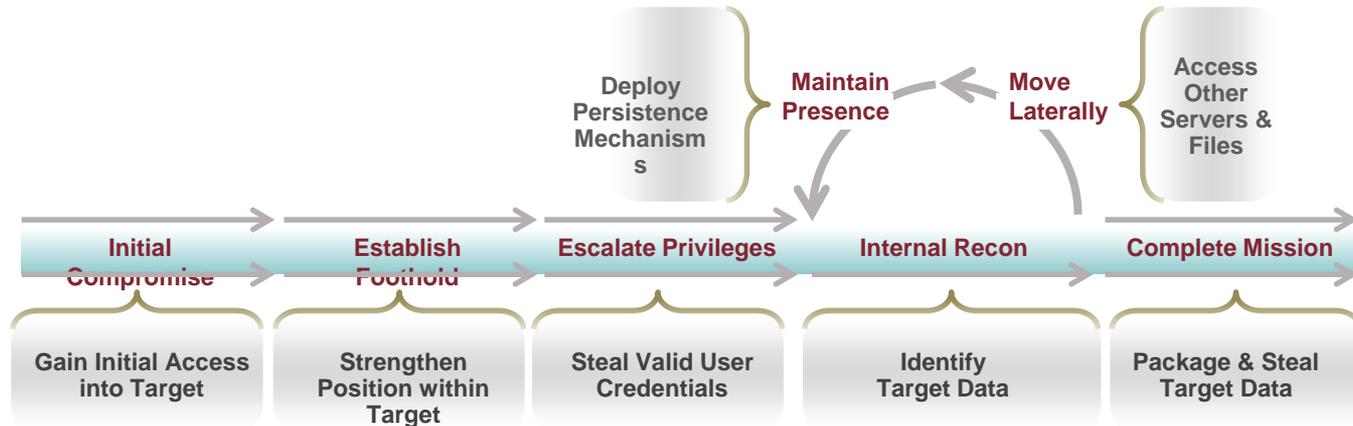


Übersicht

- *Was sind IOCs*
- *Aufbau von Threatintelligence*
- *Beispiele aus dem echten Leben*

Anatomie eines gezielten Angriffs

Attackers Move Methodically to Gain Persistent & Ongoing Access to Their Targets



Indicators of Compromise

Indicators of Compromise

Controller: Localhost | IOC Source: All IOCs (Default)

Name	UUID
6C.TMP (DROPPER)	e44952b0
133.EXE (BACKDOOR)	d986ab71
8088.EXE (DROPPER)	58eea985
A0104762.EXE (DROPPER)	428f4b42
ACEL.PVC (UNKNOWN)	36336491
ACRORD32.EXE (BACKDOOR)	5c620e1d
ACRORD32UPDATE.EXE (BACKDOOR)	e70502d3
ACRRD32.EXE (DROPPER)	759c7f18
AD (BACKDOOR)	134c225f
ADOBEARM (BACKDOOR)	060299cd
ADVAPI64.DLL (BACKDOOR)	02972bf
ADVAPI64.DLL (BACKDOOR)	c794c53b
AK.EXE (DROPPER)	5067f3cb
ALG (UNKNOWN)	39fb18ee
APPMGMT (BACKDOOR)	1d067037
APPMGMT.DLL (BACKDOOR)	6e486469
ATEXE (KEYLOGGER)	8968ef7
AUSOV (DOWNLOADER)	4967b944
AUSOV (DOWNLOADER)	17541a0b

6C.TMP (DROPPER)
e44952b0-1dee-4f1a-9a25-d700bf76b952

Description
This malware writes a malicious DLL to disk and launches it as a service on the infected machine. The malware may temporarily disable Windows File Protection on certain DLLs in the system folder, escalate its privileges using a known local kernel privilege escalation vulnerability on Vista systems.

Definition

OR:

- FileItem/FullPath contains '\system32\msimage.dat'
- FileItem/FullPath contains '\system32\msconfig.dat'
- FileItem/FullPath contains 'Program Files/Common Files\bak.dll'
- FileItem/Md5Sum is '449D85BC635CE778BC59C5D556BA4FAE'
- FileItem/Md5Sum is 'E0D1A07C2D55FDFAC3B8D7E75E44A326'
- FileItem/Md5Sum is '32D555F6F2F4625DE234C305CB0EC3CC'

AND:

- FileItem/PEInfo/DetectedAnomalies/string contains 'checksum_is_zero'
- FileItem/PEInfo/PETimeStamp is '2010-09-10T02:48:12Z'
- FileItem/SizeInBytes is '77924'

AND:

- FileItem/PEInfo/PETimeStamp is '2010-09-10T08:43:10Z'
- FileItem/SizeInBytes is '11002'

INFORMATION
Author: Mandiant
Authored On: 2010-11-10T09:46:32Z
Updated: 0001-01-01T00:00:00Z

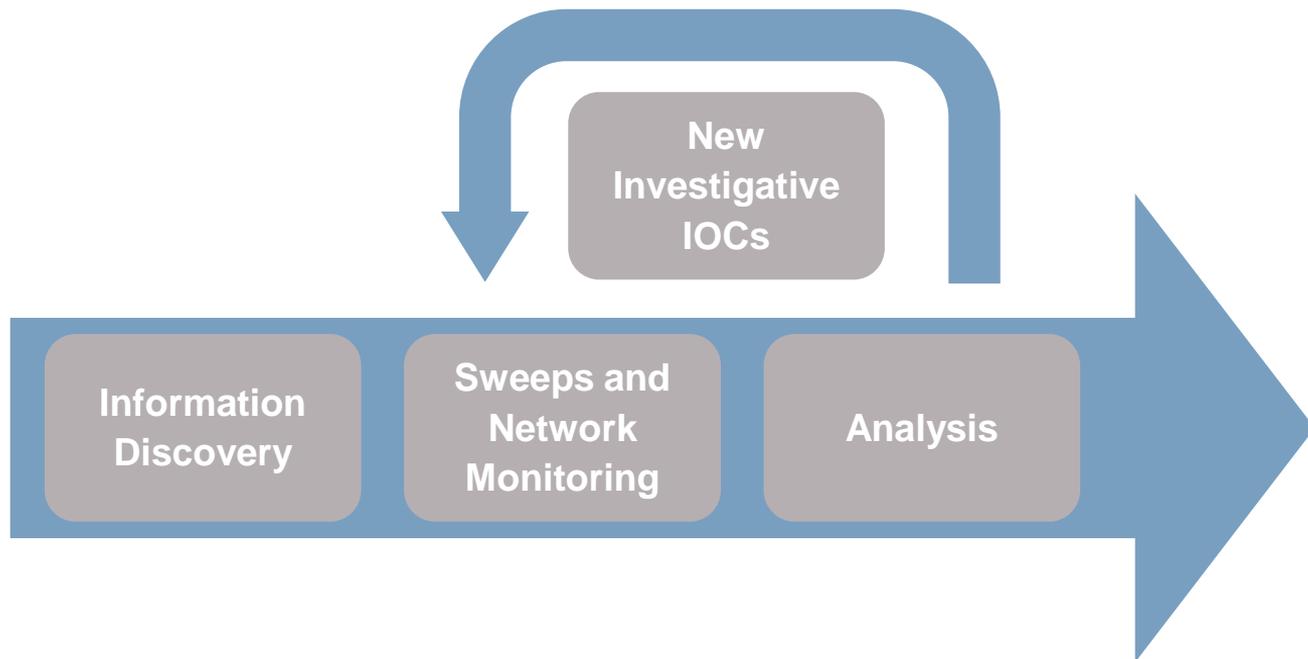
REFERENCES

KEYWORDS
dropper

Untersuchungszyklus

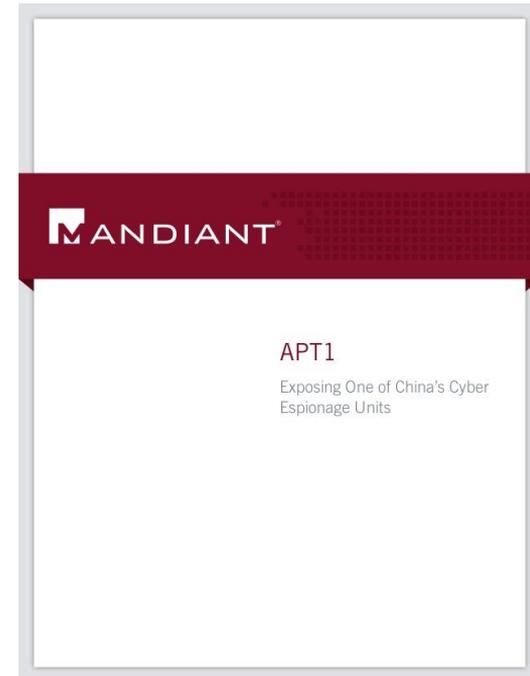
Informationsquellen

- Host Untersuchung
- Netzwerk Monitoring
- Log Analyse (SIEM)
- Malware Reverse Engineering



Threat Intelligence

- 3 Arten von Spuren
 - Atomic
 - Computed
 - Behavioural
- Hoher Informationsfluss
- Attributionsfehler
- Dynamisches Gegnerfeld
- Teuer
- Aktive vs. Passive Informationsgewinnung



Threat Intel Sharing

- Vielzahl an Plattformen
- Einbahnstraßen scheinen attraktiver für Unternehmen
- Interessensverbände
- CERTs



Ihr Intel Team

- Erfahrung im Intelligence/Ermittlungs Bereich
- Mindestens 2 Personen
- Verknüpft in Community
- Informationseingänge
 - Incident Response Untersuchungen
 - Internet & Darknet Analysen
 - Öffentliche Stellen
 - Malware Analysen
 - Hersteller
 - Certs
 - Medien, ...

Fallbeispiel APT3

- APT3 ist eine technische sehr ausgereifte Angreifergruppe
- Bekannt durch „Operation Clandestine Wolf“
- Ziel mit hohem wissenschaftlichen Wert

- Intelligence Einsatz um weitere infizierte Rechner zu finden
- Aufbau weiterer Intelligence durch Fehler der Angreifer



Incident Response Hotline

Phone

- Germany 0800 181 7231
- Switzerland 0800 848 030
- Austria: 0800 296 251
- International: +1 (703) 996 3012

Email

- To: investigations@mandiant.com
- CC: dachconsulting@mandiant.com

Kontakt Daten

Mathias Fuchs

MANDIANT, a FireEye Company

Senior Security Consultant

Mobile: **+43 660 31337 99**

Email: mathias.fuchs@mandiant.com

Jan Korth

MANDIANT, a FireEye Company

Director of Security Consulting Services

Mobile: **+49 (160) 2723362**

Email: jan.korth@mandiant.com

FRAGEN & ANTWORTEN