Cuckoo Sandbox

Ein Open Source
Automatisiertes Malware Analyse System

https://www.cuckoosandbox.org/

Claudius Link @realn2s

Logo GPL http://bit.ly/2eFk238

Disclaimer

- Vortrag gibt meine Meinung wieder
- Nicht zwingend die Meinung meines Arbeitgebers (IBM)

Folien CC BY unter

https://goo.gl/y6cMSF

Was is Cuckoo?

Aktuell Cuckoo Sandbox v2.0

Automatisiertes Malware Analyse System???

- Bereitstellung der Sandbox
- Ausführen des “Code”
- Beobachtung
- Aufräumen

das alle automatisiert

Warum Cuckoo

Use Case 1:

Malware Analyse

Details zum Attack Chain

Vulnerable Guest

Use Case 2:

Sandbox Automatisierung

Verdächtige Dateien/Webseiten “sicher” öffnen

Standard Guest

Was

- Call Traces
- Dateien
- Memory dumps
- Network Traffic
- Screenshots

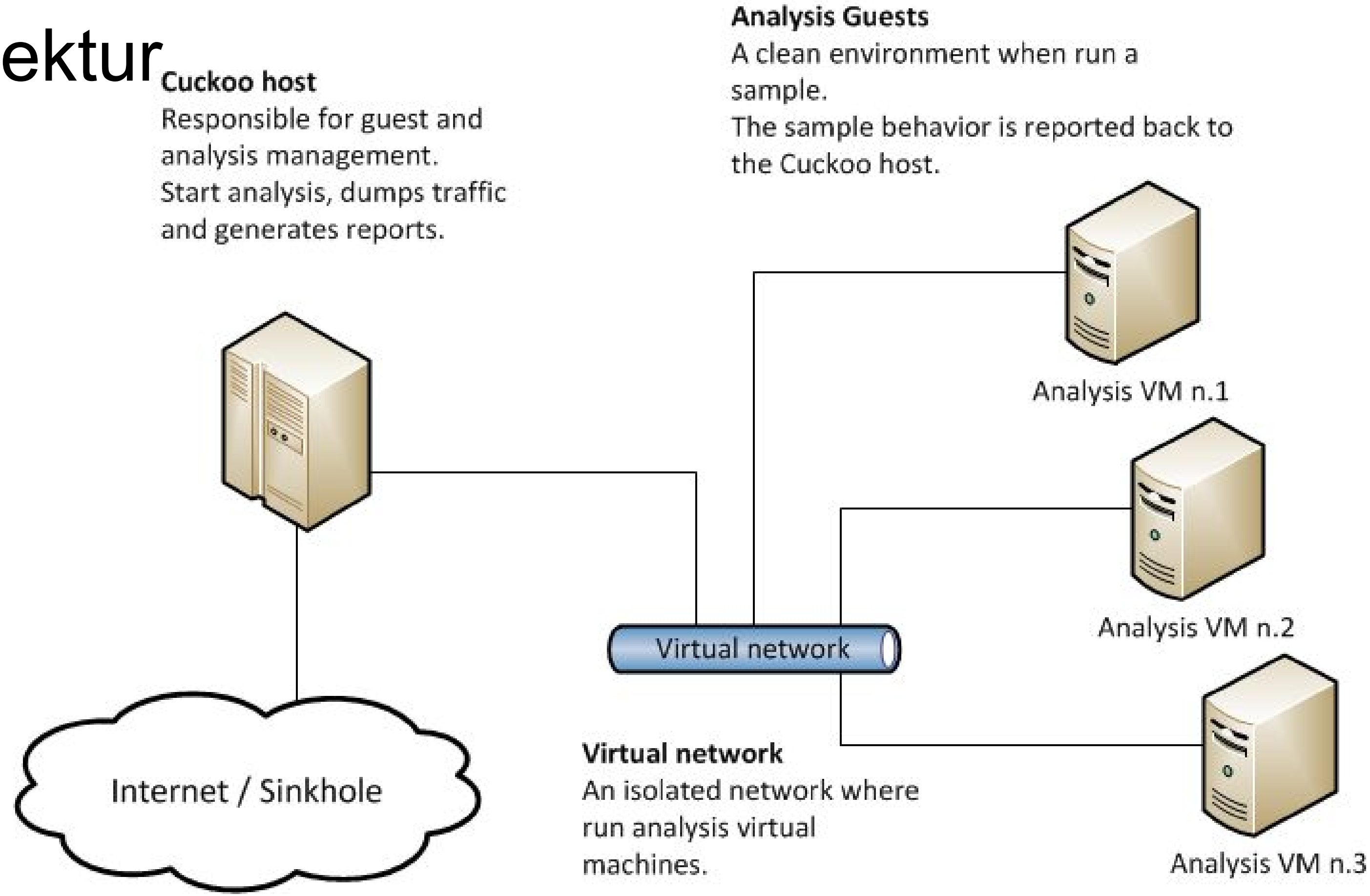
Unter

- Windows
- OS X
- Linux
- Android

Unterstützt

- Executables
- DLLs
- PDF
- Microsoft Office Dokumente
- URLs und HTML Dateien
- PHP Skripte
- CPL Dateien
- Visual Basic Skripte
- ZIP Dateien
- Java JAR
- Python Dateien
- ...

Architektur



Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.

Virtual network
An isolated network where run analysis virtual machines.

GPL http://bit.ly/2fFkqv8

Unterstützt

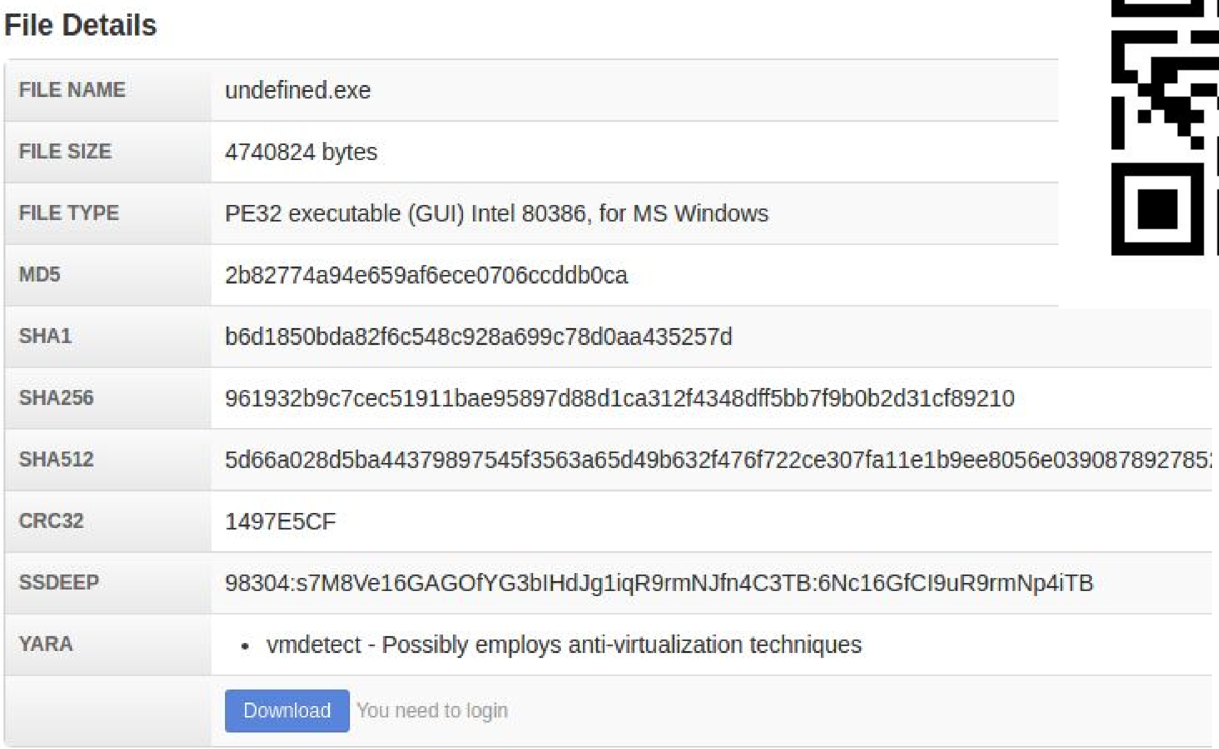
- VirtualBox
- VMWare
- QEMU/KVM
- Generic LibVirt

Ausprobieren unter:

https://malwr.com/

Nur Dateien, keine URLs

Beispiel

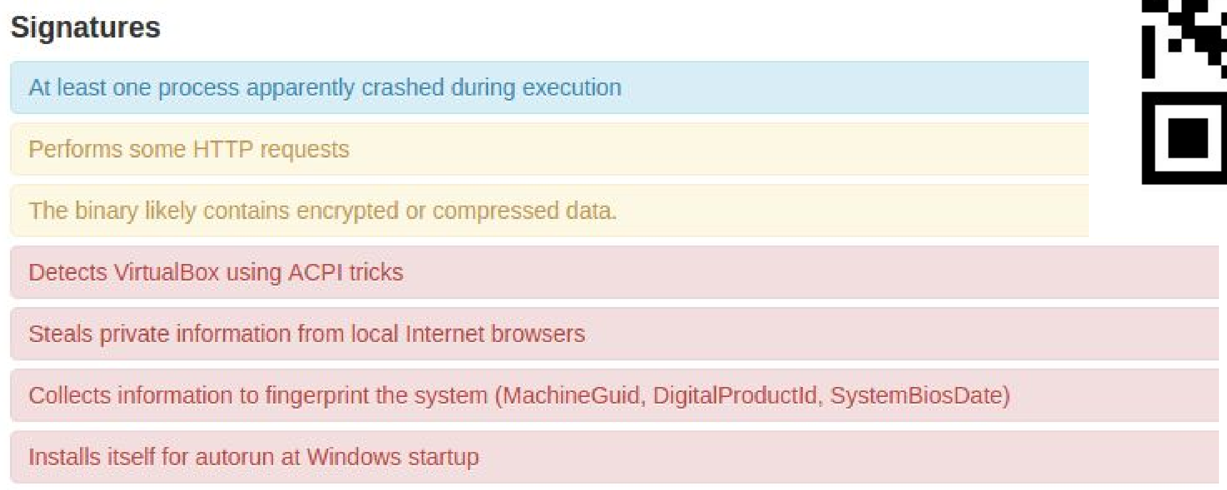


File Details

FILE NAME	undefined.exe
FILE SIZE	4740824 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	2b82774a94e659af6ece0706ccddb0ca
SHA1	b6d1850bda82f6c548c928a699c78d0aa435257d
SHA256	961932b9c7cec51911bae95897d88d1ca312f4348dff5bb7f9b0b2d31cf89210
SHA512	5d66a028d5ba44379897545f3563a65d49b632f476f722ce307fa11e1b9ee8056e039087892785
CRC32	1497E5CF
SSDEEP	98304:s7M8Ve16GAGOfYG3bIHdJg1iqR9rmNJfn4C3TB:6Nc16GfCI9uR9rmNp4iTB
YARA	- vmdetect - Possibly employs anti-virtualization techniques
	Download You need to login

https://malwr.com/analysis/OTk1Njg5YzBjNzBhNDYyMWJkYmM2NTFhNTdkNjkyZmM/

Beispiel



Signatures

At least one process apparently crashed during execution

Performs some HTTP requests

The binary likely contains encrypted or compressed data.

Detects VirtualBox using ACPI tricks

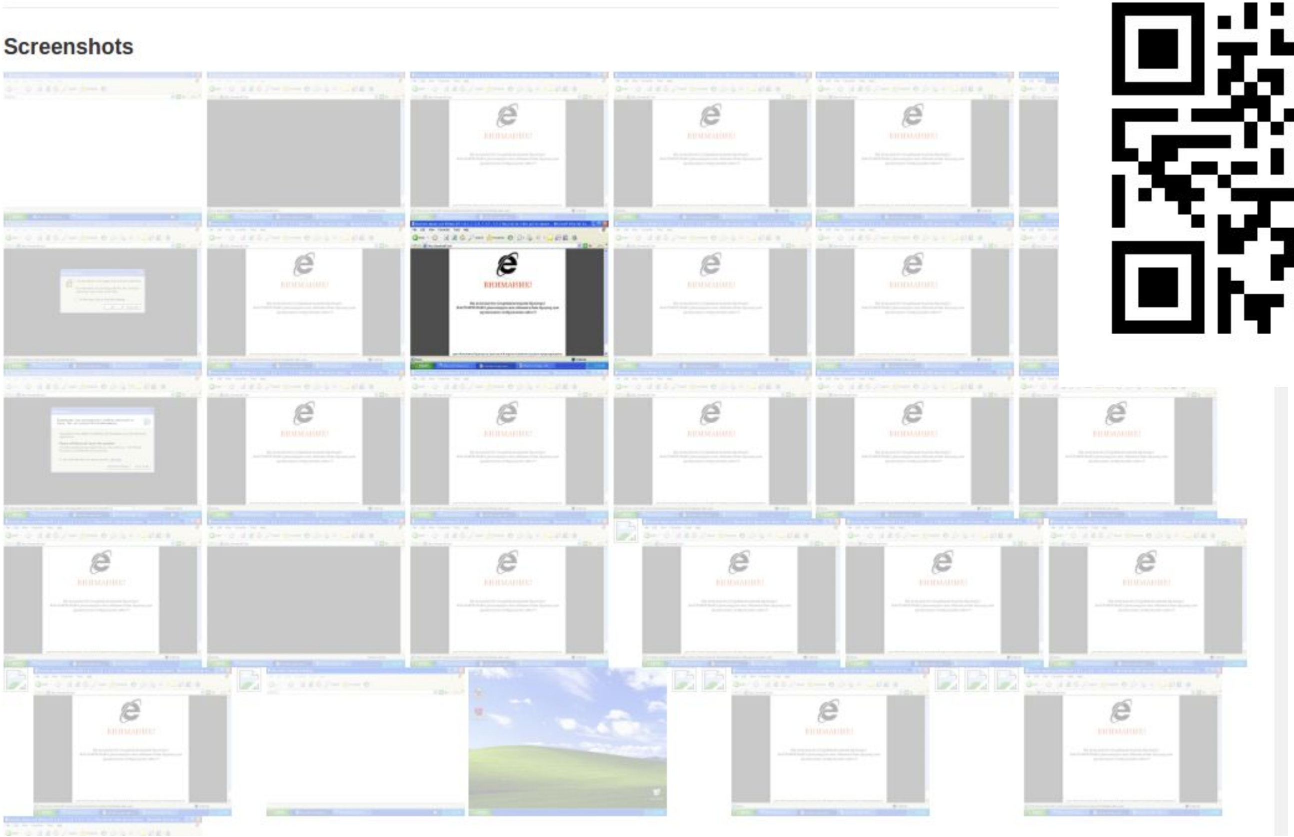
Steals private information from local Internet browsers

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Installs itself for autorun at Windows startup

https://malwr.com/analysis/OTk1Njg5YzBjNzBhNDYyMWJkYmM2NTFhNTdkNjkyZmM/

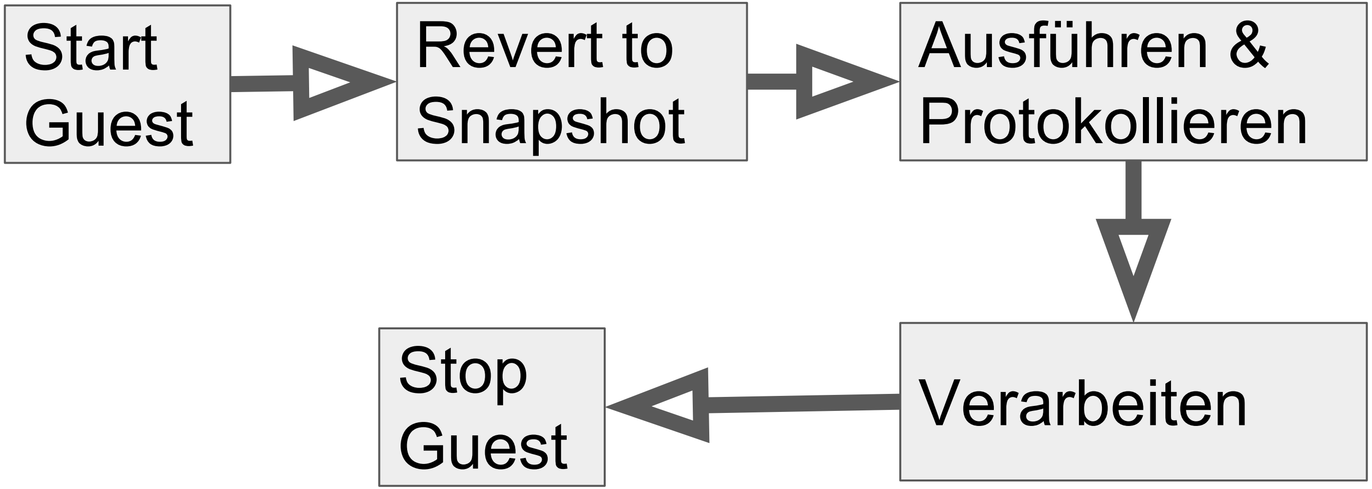
Beispiel



Screenshots

https://malwr.com/analysis/OTk1Njg5YzBjNzBhNDYyMWJkYmM2NTFhNTdkNjkyZmM/

Analyse



Start Guest

Revert to Snapshot

Ausführen & Protokollieren

Verarbeiten

Stop Guest

Langsam :-(

Installation: Host

1. Ubuntu (?)
2. Python
3. Cuckoo
4. Mongodb (für das Web-Interface)
5. Virtualisierungs Komponenten
6. TcpDump + Analyse Module

http://docs.cuckoosandbox.org/en/latest/installation/host/

Installation: Gast

1. Windows | Linux | Mac OS X | Android
2. Python
3. Netzwerkkonfiguration
4. Cuckoo Agent
5. Applikationen
6. Sauberen Snapshot

http://docs.cuckoosandbox.org/en/latest/installation/guest/

Geschichte

- Google Summer of Code project in 2010
  Als Teil vom Honeynet Project http://www.honeynet.org
- Google SoC 2011
- 2012 http://malwr.com Cuckoo as a service
- 2014 Cuckoo Sandbox 1.0 & Cuckoo Foundation
- 2015 Google SoC Mac OS X Malware Analyse
- 2016 Cuckoo Sandbox 2.0

Nutzt

- Volatility Framework - memory forensics
  https://www.volatilityfoundation.org/
- YARA - pattern matching swiss knife for malware
  http://virustotal.github.io/yara/
- VirusTotal - analyze suspicious files and URLs
  https://www.virustotal.com/
- ….

Weitere Information

- Cuckoo Sandbox Book
  http://docs.cuckoosandbox.org/en/latest/
- Mo’ Malware Mo’ Problems - Cuckoo Sandbox to the rescue
  Black Hat Las Vegas
  http://ubm.io/2fYYUT3