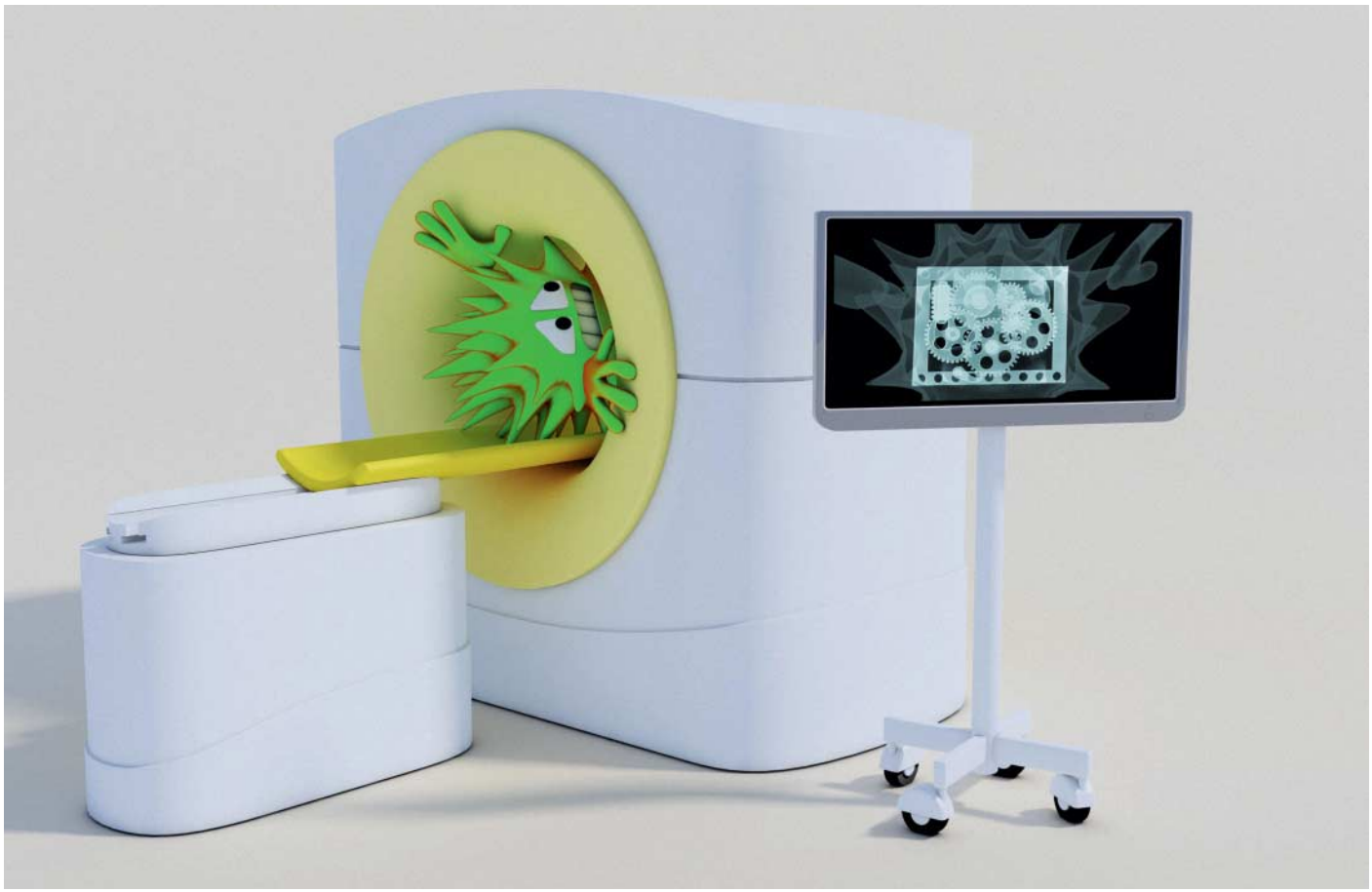


Blick hinter die Kulissen

Schädlingsanalyse mit Cuckoo Sandbox

Sei es zweifelhafte Herkunft, ein möglicher Fehlalarm des Viren-Scanners oder einfach nur Neugier: Manchmal will man genauer wissen, was ein Programm wirklich treibt. Die kostenlose Sandbox Cuckoo liefert da innerhalb von Minuten aufschlussreiche Einblicke. Und das Beste: Man kann sie ganz einfach als Online-Dienst nutzen.

Von Olivia von Westernhagen

Die Cuckoo Sandbox führt Dateien in einer virtuellen Umgebung aus, analysiert ihr Verhalten und liefert viele nützliche Informationen zurück, die die Einschätzung potenzieller Gefahren erleichtern. Das Open-Source-Projekt wurde bereits 2010 ins Leben gerufen. Dank kontinuierlicher Weiterentwicklung durch ein vierköpfiges Team sowie der Beiträge einer engagierten Community hat es sich in den letzten Jahren zu einem stabilen und leistungsfähigen Malware-Analyse-System entwickelt, das auch im Werkzeugkasten kommerzieller AV-Hersteller seinen festen Platz hat.

Wer sich privat mit Malware beschäftigt oder in der Unternehmens-IT öfter mal mit verdächtigen Dateien konfrontiert wird, kann sich mittels lokaler Cuckoo-Installation völlig kostenlos eine sichere und anpassbare Analyseumgebung zusammenbasteln. Cuckoo ist aber auch für den Gelegenheitsnutzer verfügbar: Auf malwr.com kann man verdächtige Dateien einfach hochladen und testen lassen. Den generierten Report präsentiert der Dienst wenig später direkt im Browser.

Für die Analyse führt Cuckoo das zu untersuchende Programm tatsächlich aus und sammelt dabei alle möglichen Informationen. Das Zentrum der Infrastruktur samt Programmlogik bildet der Cuckoo-Host. Dieser Computer stellt das Interface für die Dateiübergabe bereit und ist folglich auch der Ort, an dem (Malware-)Samples, Berichte, Log- und Konfigurationsdateien verwaltet werden.

Aufbau und Funktionsweise

Bei einer lokalen Installation fungiert der eigene Rechner als Host, auf dem logischerweise kein Schadcode ausgeführt werden soll. Hier kommen die Guests ins Spiel, bei denen es sich entweder um virtuelle Maschinen – etwa VirtualBox oder VMWare – oder um separate physische Systeme handelt.

Die Guests sind über ein virtuelles isoliertes Netz mit dem Host verbunden

(Host-only). Der Host kann dabei als Internet-Router seiner Guests agieren und deren Verbindungen etwa ins Internet weiterleiten (via IP Forwarding und Masquerading/NAT). Optional kann er dabei auch ein VPN oder Tor nutzen.

Im ersten Schritt der Analyse verpackt der Cuckoo-Host das Sample zunächst in ein ZIP-Archiv – und zwar zusammen mit der vorgefertigten Analyse-Komponente (Analyzer) und einigen Konfigurationsdateien. Anschließend nimmt er Kontakt zu einer Agent-Komponente auf, die auf dem Guest-System auf eingehende Verbindungen wartet. Der Agent nimmt das Zip-File entgegen, entpackt es und startet dann den enthaltenen Analyzer. Dieser wählt auf Basis der Config-Informationen sowie des Typs der übergebenen Datei ein Analyse-Paket aus, welches für die Dateiausführung zuständig ist.

Ausführbare Dateiformate startet das zuständige Python-Skript einfach direkt; Word-Dokumente, PDF-Dateien oder DLLs öffnet es mit einer passenden Hilfsanwendung. Aktuell kann man mit Cuckoo mehr als 20 Dateitypen analysieren, darunter außer herkömmlichen EXE-Dateien (PE32) auch Office-Dokumente, PDFs und JavaScript.

Während der Ausführung überwacht der Analyzer alle relevanten Funktionsaufrufe des gestarteten Samples. Dazu injiziert er nach dessen Laden, aber noch vor dem Start eine Monitor-DLL in den Prozess und leitet alle überwachten Systemaufrufe auf deren Funktionen um. Techniker sprechen dabei von Instrumentierung via DLL Injection und Inline Hooking.

Die Monitorfunktionen führen dann vor und nach dem Aufruf der eigentlichen Systemfunktionen fleißig Buch, welche Dateien oder Registry-Einträge das Sample anfasst und über vieles mehr. Beispielsweise verrät ein Hook auf der Funktion `RegCreateKey` dem Monitor nicht nur, dass das Programm einen neuen Registry-Eintrag erstellen wollte und ob das geklappt hat: Aus den Parametern des Funktionsaufrufs entnimmt er auch den Pfad, die Bezeichnung sowie den Inhalt des neuen Schlüssels.

Kapert oder startet das Programm einen anderen Prozess, sorgt die Monitor-DLL dafür, dass der dann ebenfalls „instrumentiert“ wird. Insgesamt überwacht Cuckoo etwa 300 verschiedene Systemaufrufe unter anderem aus den Bereichen Prozess-Management, Datei-, Registry-Netzwerk- und GUI-Operationen.

Der Cuckoo-Monitor verzichtet zugunsten der Stabilität auf das Anlegen einer Logdatei auf dem Guest. Stattdessen schickt er die protokollierten Aktivitäten per TCP/IP direkt an den Host, wo sie in einem speziell für die aktuelle Analyse angelegten Ordner gespeichert werden. Dort wird später auch der abschließende Report hinterlegt.

Netzwerkverkehr

Ein wichtiger Bestandteil der Analyse ist die Auswertung des Netzwerk-Traffics. Nahezu jede Malware kommuniziert zu irgendeinem Zeitpunkt ihrer Ausführung mit einem entfernten Server, um gesammelte Informationen zu übermitteln, Befehle zu empfangen oder weitere Komponenten nachzuladen.

Da alle Pakete der Guests ohnehin beim Host vorbeikommen, kann dieser den kompletten Netzwerkverkehr einfach mitschneiden. Cuckoo macht dies mit tcpdump, das eine PCAP-Datei im Analyse-Ordner erstellt. Aus dieser Kopie lässt sich der komplette Netzwerkverkehr rekonstruieren. Im gleichen Verzeichnis legt Cuckoo übrigens auch Kopien aller neu erstellten Dateien ab.

Will man auch via TLS verschlüsselte Daten etwa aus HTTPS-Verbindungen analysieren, muss man den Cuckoo-Host als „Man in the Middle“ einrichten. Dazu kann man eine Root-CA des Hosts in den Guests als vertrauenswürdigen Zertifikatsherausgeber installieren. Ein Tool wie mitmproxy kann sich damit dann in die TLS-Verbindungen einklinken. Außerdem extrahiert Cuckoo seit Version 2.0 die sogenannten TLS Master Secrets seiner Windows Guests in eine Datei namens tlsmaster.txt, die im gleichen Verzeichnis wie die PCAP-Datei landet. Damit kann dann etwa Wireshark auch die verschlüsselten HTTPS-Daten dechiffrieren.

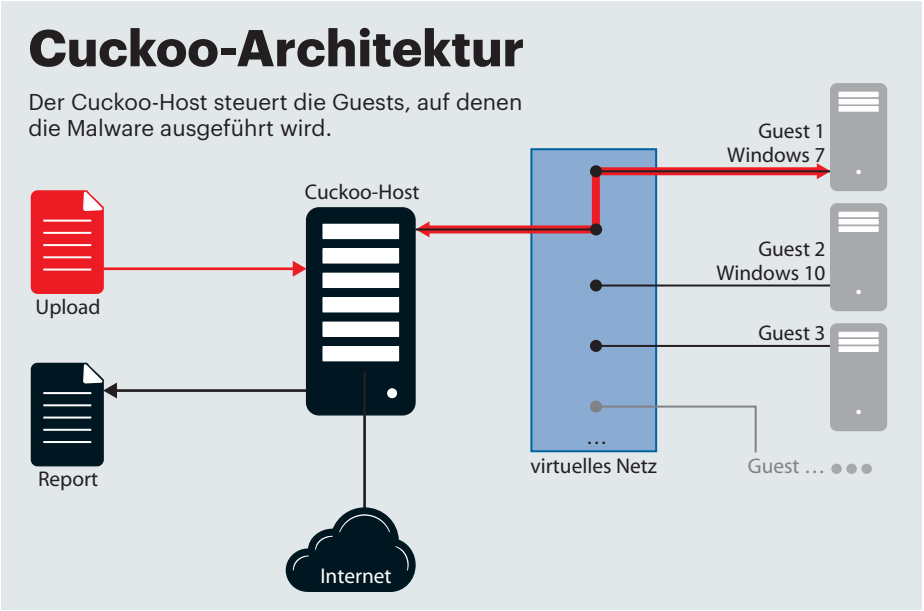
Oft sagt ein Bild mehr als 1000 Worte. So lässt ein Fenster mit Erpresser-Botschaft nebst verschlüsselten Dateien auf dem Desktop wenig Zweifel an den Absichten der analysierten Datei. Cuckoo gewährt im Rahmen jedes Reports Einblicke in die Sandbox – und zwar anhand mehrerer Screenshots, die ein Hilfsmodul während der Dateiausführung anfertigt.

Standardmäßig lässt Cuckoo die zu testende Anwendung zwei Minuten laufen. Anschließend beendet der Analyzer sowohl das Programm als auch das Guest-System. Reagiert der Analyzer oder sogar die VM nicht mehr, erzwingt der Host nach weiteren 60 Sekunden deren Ende.

Anti- und Anti-Anti-Analyse

Malware kann folglich der Analyse entgehen, wenn sie zunächst zwei Minuten nur virtuelle Däumchen dreht. Der Analyst kann jedoch die Laufzeit global in der Cuckoo-Konfiguration oder temporär etwa durch einen Kommandozeilenparameter für einen Analyselauf beliebig verlängern.

Auch gegen andere Anti-Analyse-Techniken hat die Sandbox Strategien auf Lager. So simuliert ein Modul namens human.py menschliche Interaktionen wie Mausbewegungen oder Tastatureingaben. Außerdem kann es auch beschriftete But-



tons anklicken und so etwa Nachfragen vor dem Ausführen von Makros „beantworten“.

Nach dem Abschluss der dynamischen Analyse wertet Cuckoo die gesammelten Daten aus und bereitet sie zu einem übersichtlich strukturierten Analysebericht auf. Außerdem versetzt der Host nach jedem Scan das Guest-System wieder in den Ursprungszustand zurück, um für jede weitere Analyse unverfälschte Resultate auf einem sauberen System zu gewährleisten. Bei VMs geht das über Wiederherstellungspunkte; bei physischen PCs kommt dazu Software wie FOG, Clonezilla oder Deep Freeze zum Einsatz. Da werden dann zumeist SSDs genutzt, mit denen auch das Zurückspielen eines Komplett-Images nur noch Minuten und nicht mehr Stunden dauert.

ZLoader im Online-Check

Wer so schnell wie möglich sehen will, wie eine Analyse aussieht, kann ein (Schad-)Programm beim Online-Service malwr.com hochladen. Wie bei Cuckoo handelt es sich hier um ein nichtkommerzielles Projekt, das von zwei Cuckoo-Entwicklern in ihrer Freizeit betrieben und regelmäßig auf den neuesten Entwicklungsstand gebracht wird.

Beim Übermitteln einer Datei kann man übrigens durch Entfernen des Häkchens bei „Share the sample“ erklären, dass man die Datei nicht an Dritte weitergeben möchte. Belässt man es bei der Standard-Einstellung, versieht der Dienst die auf dem Server dauerhaft verfügbaren Reports mit einem Download-Link für andere. Nach dem Upload erhält man einen Link zum Report; typischerweise dauert es einige Minuten, bis die Ergebnisse vorliegen.

Die rohen Daten eines Analyse-Laufs sind wirklich harte Kost für Insider. Doch Cuckoo bemüht sich nach Kräften, die ermittelten Informationen mit Kontext zu versehen und damit eine Bewertung zu erleichtern. Dazu gehören unter anderem sogenannte „Signatures“, die man nicht mit den Signaturen einer Antiviren-Software verwechseln darf. Sie besagen, dass das untersuchte Programm auffällige Verhaltensweisen an den Tag legt.

Wichtig für die Interpretation ist, dass auch diese Signaturen keinen eindeutigen Beweis für Schadhaftigkeit darstellen. Besonders gelbe Hinweise wie „Performs HTTP requests“ sind wenig aussagekräftig. Auch wenn beim von uns für Tests ausgewählten ZLoader-Sample mindestens ein AV-Programm von Virustotal anspringt und das Programm Ressourcen in Russisch nutzt, kann es dafür harmlose Erklärungen ergeben.

Rot markiert der Report deutlich verdächtige Aktivitäten wie das Anlegen eines Autorun-Eintrags oder – wie bei ZLoader – den Versuch, sich der Analyse durch das Hooking zu entziehen. Besonders wertvoll sind konkrete Informationen wie „Contacts C&C server HTTP check-in (Banking Trojan)“, die das ZLoader-Sample schon recht deutlich als Banking-Trojaner klassifizieren. Schließlich gibt es wenig legitime Gründe für ein Programm, mit dem bekannten Command & Control-Server einer Betrügerbande zu reden.

Die Übersichtsseite verrät auch gleich, dass es sich dabei um die Domain tohinwithec.com handelt, sodass man weitere Nachforschungen dazu anstellen kann. In einem eigenen Reiter zu „Network Analysis“ finden sich mehr Details zu den Netzwerkaktivitäten, also etwa die komplette Liste der kontaktierten Hosts und die einzelnen HTTP-Requests.

Wichtige Informationen für die weitere Bewertung versammelt der Reiter „Behavioural Analysis“. Hier verbergen sich, getrennt nach Prozessen, die aus dem API-Hooking gewonnenen Informationen. Dazu gibt es auch eine nach Kategorien sortierte grafische Übersicht über Events wie Prozess- und Service-Starts, Datei- und Registry-Zugriffe sowie Netzwerkaktivitäten.

Zur Interpretation der Verhaltensinformationen benötigt man mitunter einiges an Hintergrundwissen oder alternativ Zeit für eine zusätzliche Online-Recherche. So kann man den dokumentierten Funktionsaufrufen des ZLoader-Samples dann etwa entnehmen, dass es eine Instanz von explorer.exe im Suspended State startet, in den es eine DLL mit eigenem Code injiziert. Das ist eine bekannte Technik, um Schadcode unter dem Deckmantel eines legitimen Programms auszuführen.

Interessant ist übrigens auch der Reiter „Static Analysis“. Dort listet Cuckoo alle importierten Windows-Funktionen

Sandbox im Eigenbau

Die Installation der aktuellen Cuckoo-Version 2.0.3 ist sowohl unter Linux und macOS als auch unter Windows möglich, auch wenn die Installationsanleitung für Windows im offiziellen Manual bislang noch fehlt. Unabhängig vom Betriebssystem besteht der erste Schritt im Herunterladen und Installieren diverser Pakete und Bibliotheken sowie (teilweise optionaler) Zusatzkomponenten wie MongoDB, PostgreSQL und tcpdump.

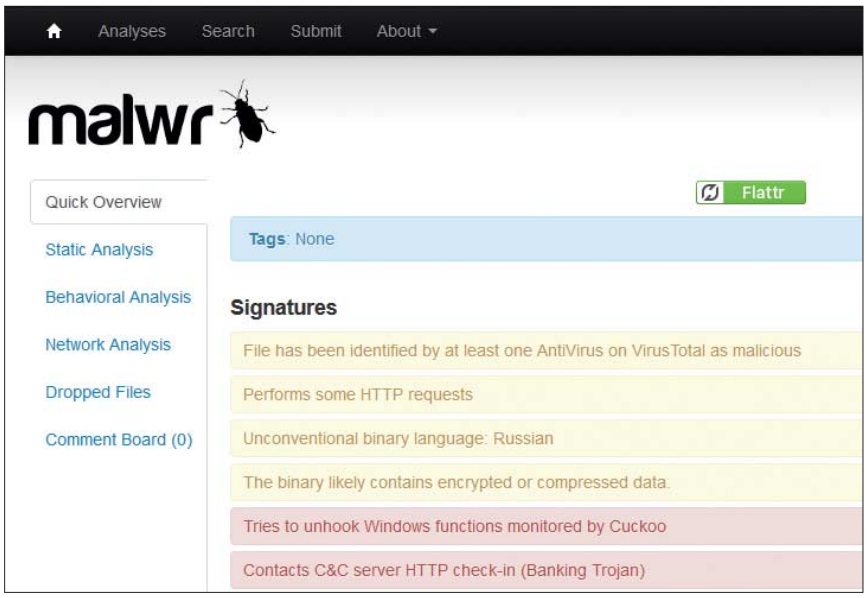
Auf Linux-Systemen muss anschließend ein neuer User hinzugefügt werden, um Cuckoo das eigenständige Starten der Guest-VM(s) zu ermöglichen. Die eigentliche Cuckoo-Installation funktioniert am bequemsten mit dem Python-eigenen Installationsmanager PIP. Daran schließen sich Anpassungen in mehreren Cuckoo-Konfigurationsdateien an, um Rahmenbedingungen der Kommunikation zwischen Host und Guest, des Analysevorgangs sowie der Speicherung der Ergebnisse festzulegen.

Die Installation der gewünschten Virtualisierungssoftware erfolgt unabhängig von der Cuckoo-Installation. Im Manual werden VirtualBox als Standard-VM und die Nutzung von Windows 7 (64 Bit) oder alternativ Windows XP als Analyseumgebung empfohlen. Um unverfälschte Ergebnisse zu erhalten, sollte man in den Guests User Account Control (UAC), Firewall und automatische Updates deaktivieren. Die Verknüpfung von Host und Guest(s) erfolgt mittels Installation der Agent-Komponente und der Konfiguration des verbindenden Netzes.

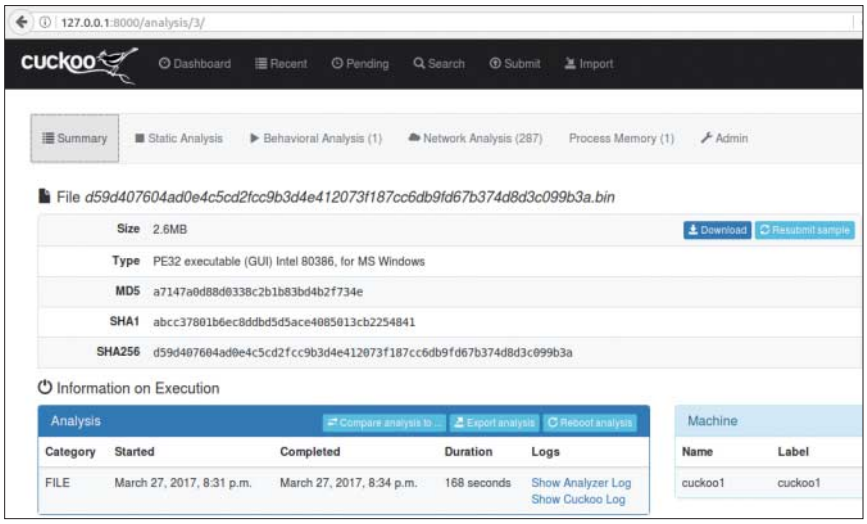
Nach Erstellen eines Sicherungspunkts und dem Klonen der VM ist Cuckoo im Wesentlichen einsatzbereit. Um wirklich von der Installation zu profitieren, sollte man die Sandbox allerdings noch um Signaturen und optionale Zusatzmodule erweitern. Des Weiteren gibt es eine ganze Reihe beliebter Analyse-Werkzeuge wie YARA oder Volatility, die sich in die Sandbox und teilweise auch ins grafische Interface integrieren lassen. Einen guten Startpunkt für die Suche nach möglichen Erweiterungen bietet das GitHub-Repository der Cuckoo-Community und das detaillierte Handbuch – beides finden Sie über ct.de/ycyy.

auf. Das ist nützlich, weil das dynamische API-Hooking nur die während des Testlaufs genutzten Funktionen zeigt. Die statische Liste gibt hingegen einen schnellen Überblick über den kompletten Funktionsumfang des Programms. Praktisch auch, dass Cuckoo weniger versierten Analysten die weitere Recherche durch passende Links zu Microsofts Dokumentation der Funktionen erleichtert. So erfährt man mit wenigen Mausklicks, dass und wie etwa `VirtualProtect` Speicherschutz-Optionen ändert.

Schon dieses kurze Beispiel mit ZLoader zeigt, wie sich eine Analyse mit Cuckoo von einem Check beim bekannten Online-Dienst Virustotal unterscheidet. Letzterer lieferte lediglich ein wenig aussagekräftiges Ergebnis. Ob sich etwa hinter McAfees „BehavesLike.Win32.BadFile.ch“ eine echte Gefahr verbirgt, kann man nur spekulieren. Mit der konkreten Analyse des Verhaltens, die malwr.com liefert, ist der Befund jedoch recht eindeutig: Das Sample führt ziemlich sicher Böses im Schilde. Auf Basis der präsentierten Informationen und etwas weiterer Recherche kann man das dann auch beliebig konkretisieren.



Der Dienst malwr.com liefert einen schnellen Einblick in das Verhalten eines Programms. Im Hintergrund arbeitet Cuckoo.



Eine lokale Cuckoo-Installation erlaubt gezieltere Analysen, etwa mit maßgeschneiderten VMs.

Eigener Nestbau

So komfortabel die Analyse des Online-Dienstes ist, hat sie doch einige Nachteile, die für den Betrieb einer eigenen Sandbox sprechen. Das beginnt mit dem oft nicht erwünschten Upload des Samples in die Cloud. Es geht weiter über die vielfältigen Erweiterungen, mit denen man die Analyse weiter verfeinern könnte – etwa zusätzliche Memory-Dumps mit dem Forensik-Tool Volatility.

Außerdem versuchen natürlich die Malware-Autoren immer wieder mit neuen Tricks, eine Analyse ihrer Machwerke zu verhindern. Profis pflegen deshalb ihre mit Anti-Anti-Analyse-Tricks handoptimierte Sandbox, die im Zweifelsfall dann auch auf echter Hardware und nicht in einer virtuellen Maschine läuft.

Zu den größten Stärken einer lokalen Cuckoo-Installation zählt die Individualisierbarkeit der Guest-Systeme. So kann man einen Schädling auf vordefinierte Umgebungen loslassen, um sein Verhalten besser zu verstehen oder sogar die Wirksamkeit bestimmter Schutzvorkehrungen zu testen. Man kann dazu auch ein ganzes virtuelles Netz hochfahren und dann etwa WannaCry bei der Ausbreitung beobachten. Für das Einrichten eines funktionsfähigen Basissystems sollte man etwa einen Arbeitstag veranschlagen; diverse Erweiterungen können dann beliebig mehr Zeit beanspruchen.

Antiviren-Software und Sandboxes wie Cuckoo stellen sich letztlich der gleichen Frage: „Ist dieses Programm böse?“ Doch die Art der Antworten unterscheidet sich fundamental. AV-Software beschränkt sich letztlich auf ein schlichtes „Ja“ oder „Nein“. Das ist in vielen Fällen ausreichend, doch man läuft damit natürlich immer Gefahr, dass der AV-Wächter auch mal falsch liegt. Kommen Zweifel auf, steht man ziemlich ratlos da. Denn selbst Experten können den Meldungen der AV-Software nicht entnehmen, was zu dieser Einschätzung führte.

Cuckoo hingegen versucht erst gar nicht, solch eindeutige Antworten zu geben, sondern liefert lediglich Indizien, die der Sandbox-Nutzer selbst interpretieren muss. Das ist nicht immer einfach und überfordert reine Computeranwender in vielen Fällen. Doch Cuckoo bemüht sich nach Kräften, die weitere Recherche zu unterstützen und ist damit durchaus auch für ambitionierte Noch-nicht-Experten ein toller Einstieg in die Analyse von Malware. *(ju@ct.de)* c't

Download und Doku: ct.de/ycyy