Fraunhofer FKIE

Übungen zu ClamAV

Organisatorisches:
Zur Lösung der folgenden Aufgaben haben wir eine virtuelle Maschine vorbereitet, die ihr unter der folgenden Adresse herunterladen könnt:
`https://itsec.cs.uni-bonn.de/depot/?g=xdp5g`
Zum Ausführen der virtuellen Maschine benötigt man VirtualBox, welches auf `www.virtualbox.org` kostenlos angeboten wird.
Wir werden zeitnah eine Musterlösung auf der CTF-Gruppen-Seite (`http://net.cs.uni-bonn.de/wg/cs/projects/student-ctf-group/`) bereitstellen. Ansonsten seit ihr herzlich eingeladen zum nächsten Treffen der CTF-Gruppe am kommenden Dienstag (18.02.) zu kommen und dort mit uns über die Aufgaben, Lösungen, Erfahrungen und alles, was sonst noch mit Signaturen zu tun hat, zu diskutieren.

Nützliche Links:
ClamAV Homepage: `http://www.clamav.net`
Creating Signatures for ClamAV: `https://github.com/vrtadmin/clamav-devel/raw/master/docs/signatures.pdf`

Fragen und Anmerkungen an:
Peter Weidenbach: `weidenba@cs.uni-bonn.de`
Julian Dammann: `dammannj@cs.uni-bonn.de`

In den folgenden Übungsaufgaben sollen ClamAV-Signaturen erstellt werden, die anschließend am Ordner `~/suspiciousFiles` zu testen sind.

Aufgabe 1: Erstellt statische Signaturen von `~/samples/Hello_World.exe` und `~/samples/HeLLo_WoRld_1.exe`.

Aufgabe 2: Erstellt eine Signatur, die den String „I am Malware“ findet.

Aufgabe 3: Schreibt eine Signatur, die „I am Malware“ sowie ihre 1337-Abwandlungen findet. Dabei können die folgenden Buchstaben ersetzt sein:

$$\begin{aligned} A \mid a &\rightarrow 4 \\ E \mid e &\rightarrow 3 \\ I \mid i &\rightarrow ! \\ L \mid l &\rightarrow 1 \\ T \mid t &\rightarrow 7 \end{aligned}$$

Aufgabe 4: Schreibt eine Signatur, die „I am Malware“ findet und Groß- und Kleinschreibung ignoriert. (Nicht nur am Wortanfang!)

Aufgabe 5: Erstellt eine Signatur, die Dateien findet, in denen alle der folgenden Wörter in beliebiger Reihenfolge vorkommen: „I<space>“, „am“ und „Malware“.

Aufgabe 6: Erstellt eine Signatur, die Dateien findet, in denen alle der folgenden Wörter in der richtigen Reihenfolge vorkommen: „I<space>“, „am“ und „Malware“.

Aufgabe10: Bei einer Analyse mehrerer Samples einer Malware konnte der folgende charakteristische Code

extrahiert werden:

Assembler	**HEX**
zwischen 5 und 12 Bytes nach EP	
mov edi, edi push ebp	8B FF 55
beliebige Anzahl beliebiger Bytes	
push 1	6A 01
5 beliebige Bytes	
pop ecx push 0	59 6A 00

Des Weiteren kommt immer entweder der String „Hello World!“ oder der String „I am Malware“ vor.

Aufgabe 11: Erstellt eine Hash-basierte Signatur für das *.rdata* Segment der Datei
`~/samples/trojan.swizzor.exe`
(Tipp: Schaut euch `~/help/Trojan.swissor.analysis.pdf` an.)

Aufgabe 13: Im Ordner `~/analyses` befinden sich 25 Malware-Samples inklusive ihrer Cuckoo-Sandbox-Analysen. Erstellt zu jeder Malware eine Signatur. Versucht (sofern möglich) bei unterschiedlichen Samples der gleichen Malware-Familie ($< name > [A - Z]$) nur eine Signatur für alle Versionen zu erstellen.