Einstieg in die Malware-Analyse

Wer eine Schadsoftware analysieren will, kann auf reichlich Ressourcen und Werkzeuge zurückgreifen – braucht aber einen Plan. Der Auftakt einer vierteiligen Reihe zur Malware-Analyse zeigt, in welchen Phasen sie abläuft und wie man seine IT dabei schützt.

Von Nadia Meichtry, Fabian Murer und Tabea Nordieker

Was vor zehn Jahren noch vereinzelt und oft im Verborgenen stattfand, ereignet sich heute täglich und vor aller Augen: Hacker greifen Unternehmen und IT-Infrastrukturen an, um sie mit Malware zu infizieren. Nicht nur große Konzerne, auch KMU werden regelmäßig Opfer von Cyberattacken. Organisationen wie die European Union Agency for Cybersecurity (ENISA) geben dazu jährlich eindrückliche Statistiken heraus (siehe ix.de/zk5s).

Wer sich schützen will, muss die Ziele der Angreifer und die Funktionsweise ihrer Werkzeuge kennen. Dieser Auftakt einer vierteiligen Artikelserie zur Analyse von Schadsoftware erklärt, wie man sicher mit Malware umgeht, seine Infrastruktur vor ihr abschirmt und in welchen Phasen die Analyse abläuft.

iX-TRACT

- IT-Professionals müssen keine Sicherheits- oder Forensikspezialisten sein, um in die Analyse von Schadsoftware einzusteigen.
- Malware-Analyse umfasst fünf Phasen, die in der Praxis ineinandergreifen.
- Um die Infrastruktur nicht zu gefährden, muss die Analyse auf gut isolierten Systemen stattfinden, virtuelle Maschinen sind dafür geeignet.
- Eine Kombination aus Linux- und Windows-basierten VMs bietet sich an, da es auch zur Analyse von Windows-Schadsoftware viele Linux-Werkzeuge gibt.

Die Serie wird sich hauptsächlich mit der Analyse von Windows-Malware beschäftigen. Mit mehr als 70 Prozent Marktanteil ist Windows das lukrativste Ziel. Daher korreliert die Anzahl der für Windows, Linux und macOS erstellten Schadsoftware eng mit deren Marktanteilen. Das heißt jedoch nicht, dass es für andere Betriebssysteme wie macOS oder Linux keine Malware gibt oder dass diese Betriebssysteme nicht anfällig für Schadsoftware sind. Immer mehr Schadsoftware läuft auch auf Unix-basierten Betriebssystemen.

Wer steckt hinter einer Malware?

Die Verbreitung von Schadsoftware ist mittlerweile ein Geschäftsmodell. Die meisten Cyberangriffe sind also finanziell motiviert. Daher sind viele Schadprogramme so programmiert, dass sie auf möglichst vielen Zielsystemen erfolgreich sind. Solche nicht gezielten Attacken können dann beispielsweise durch Phishing oder andere Angriffsvektoren an viele potenzielle Ziele verteilt werden. So optimieren die Kriminellen ihr Kosten-Nutzen-Verhältnis.

In anderen Fällen sucht sich ein Angreifer sein Ziel spezifisch aus. Der Grund kann reine Neugier sein, häufig steckt aber Spionage oder eine politische Motivation dahinter. Eine Besonderheit sind Advanced Persistent Threats (APT). Hier verfügt der Angreifer über ein hohes Maß an Fachwissen und erhebliche Ressourcen, dank derer er sich über einen längeren Zeitraum in einem Netzwerk festsetzen und es ausspähen kann. APTs kommen in der Regel von nationalstaatlichen oder staatsnahen Gruppen. Das Ziel ist die Informationsgewinnung oder die Störung kritischer Infrastruktur.

Ob APT oder nicht, häufig führen nicht Einzelpersonen Malware-Angriffe durch, sondern eine organisierte Tätergruppe. Diese Organisationen nutzen eigene Werkzeuge, entwickeln eigene Techniken und Taktiken und verwenden jeweils die gleiche Infrastruktur. Um die Gruppen eindeutig benennen zu können, haben zwei der großen Cybersecurity-Anbieter Namenskonventionen herausgegeben. Mandiant verwendet nummerierte APT-, FIN- und UNC-Gruppen (siehe Tabelle „Tätergruppen nach Mandiant“). CrowdStrike orientiert sich für die Benennung einer Tätergruppierung an Tieren. Angreifer, die aus einer ähnlichen Motivation heraus handeln oder aus dem gleichen Ursprungsland agieren, werden dem gleichen Tier zugeordnet.

Tätergruppierungen nach CrowdStrike

Angreiferbezeichnung	Nationalstaat oder Kategorie
Bear	Russland
Buffalo	Vietnam
Chollima	Nordkorea
Crane	Südkorea
Jackal	Hacktivismus
Kitten	Iran
Leopard	Pakistan
Lynx	Georgien
Ocelot	Kolumbien
Panda	Volksrepublik China
Spider	E-Crime
Tiger	Indien
Wolf	Türkei

Tätergruppen nach Mandiant

Namenskürzel	Erläuterung
APT	Advanced Persistent Threats, die als solche identifiziert sind, z. B. APT19
FIN	Financial Threads: Gruppierungen, die Angriffe auf die Finanzwelt und das Zahlungswesen verüben, z. B. FIN6
UNC	Uncategorized Groups: Cluster von Angriffsaktivitäten, die beobachtbare zu einer Gruppierung gehörende Artefakte umfassen, aber nicht als APT oder FIN klassifizierbar sind

Eine konkrete Gruppierung bekommt ein zusätzliches Adjektiv oder Substantiv, zum Beispiel Cozy Bear oder Hammer Panda (siehe Tabelle „Tätergruppierungen nach CrowdStrike“).

Warnung: Infektionsgefahr

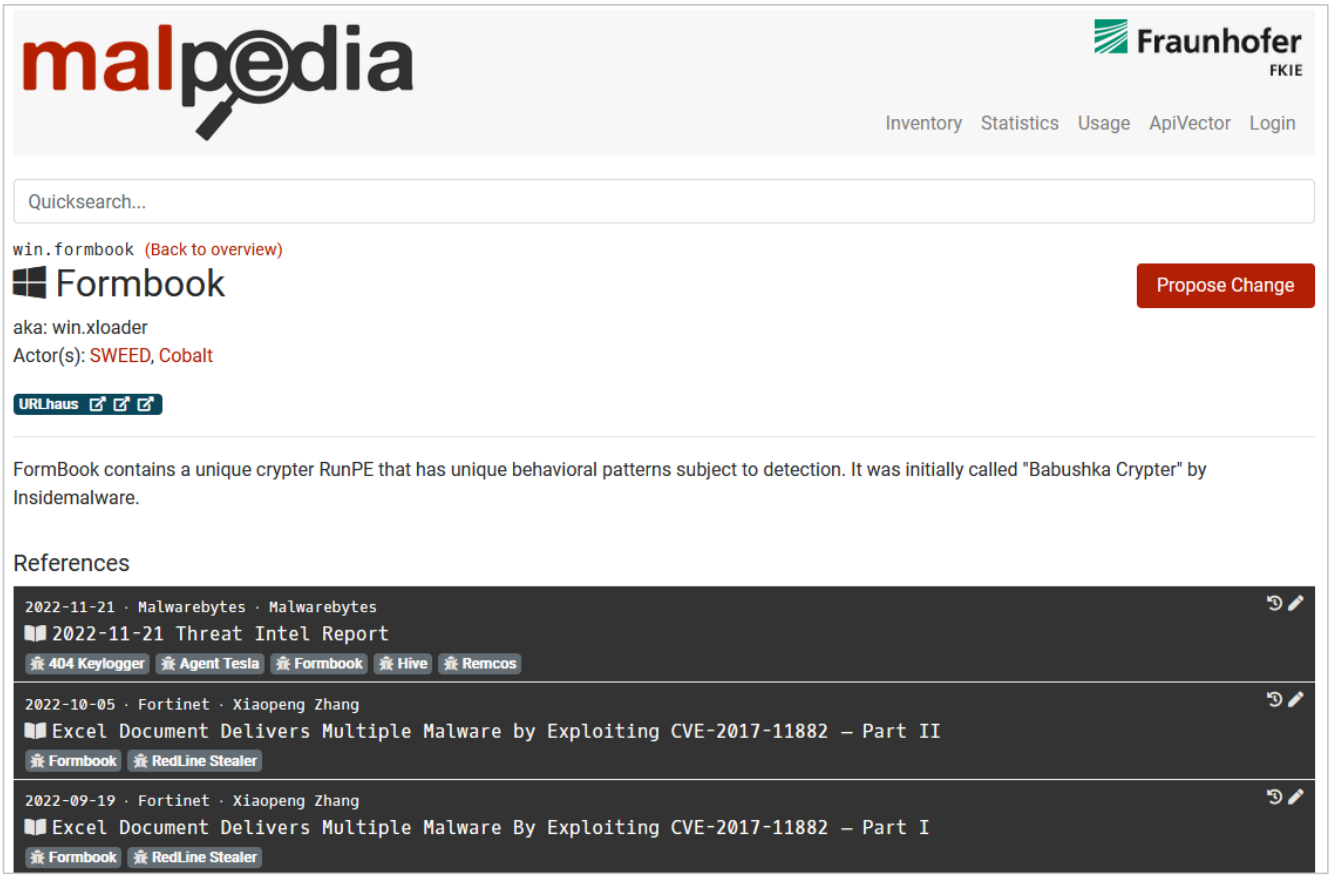
Im Umgang mit Malware, wie auch im Umgang mit biologischen Viren, ist stets Vorsicht geboten und es ist dringend anzuraten, sie so weit entfernt von Unternehmens- oder sonstigen Arbeitssystemen wie möglich zu halten. Je nach Art und Typ der Malware kann das versehentliche Ausführen auch schon von Teilen der Schadsoftware verheerende Folgen haben.

Will man also einen genaueren Blick auf die Malware und ihre Funktionsweise werfen, muss man das auf einem dedizierten System tun. Digitale Forensiker, Reverse Engineers und Malware-Analysten haben hierzu in der Regel für jede Analyse eine eigene virtuelle Maschine, die im Optimalfall komplett isoliert, also ohne Netzwerk- und Internetverbindung betrieben werden kann. Ist eine Verbindung zum Internet nötig, darf keine Verbindung in das Firmennetz entstehen. Auch ist eine Internetverbindung über ein VPN oder das Tor-Netzwerk empfehlenswert, um keine Rückschlüsse über das Unternehmen zuzulassen (siehe ix.de/zk5s).

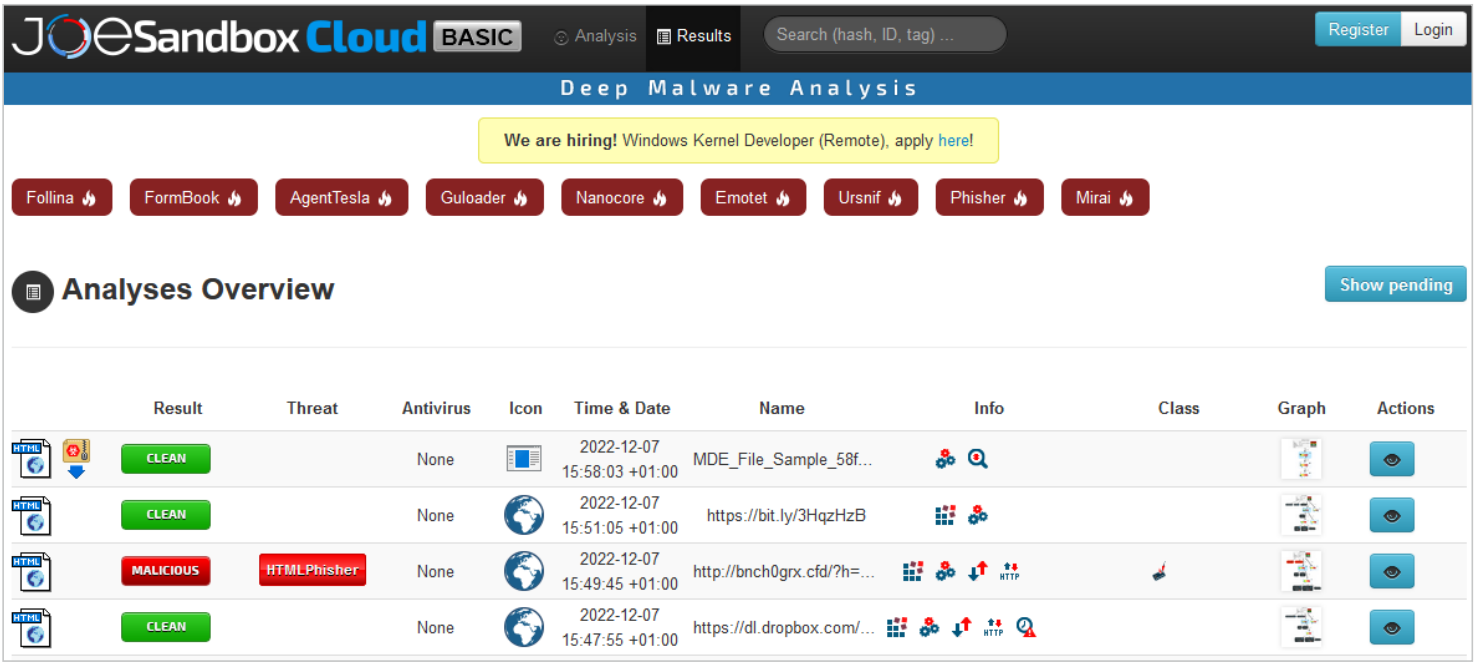
Zum sicheren Umgang mit Schadsoftware gehört auch der Austausch mit anderen Malware-Spezialisten. Will man sie an andere Analysten weiterleiten, sollte man sie stets in ein verschlüsseltes Archiv packen, damit Antivirenlösungen die darin verpackte Schadsoftware nicht erkennen und den Anhang löschen. Hier hat es sich eingebürgert, als Standardpasswort „infected“ zu verwenden. Der Name des Archivs sollte darauf hinweisen, dass es Malware enthält, beispielsweise durch die Dateierweiterung .vir.

Analyseprozess – von statischer zu dynamischer Analyse

Die Analyse von Schadsoftware besteht aus fünf Schritten. Je nach eingesetzter Analysetechnik sind einige einfacher als andere – und nicht immer sind alle fünf erforderlich. Je weiter man im Analyseprozess voranschreitet, desto aufwendiger und anspruchsvoller wird er und verlangt bestimmte technische Fachkenntnisse. Bei der Malware-Analyse unterscheidet man folgende Schritte:



Die Malpedia des Fraunhofer FKIE liefert Informationen und Veröffentlichungen zu einer bestimmten Malware, hier als Ergebnis der Suche nach Formbook (Abb. 1).



JoeSandbox ist ein beliebtes Werkzeug, um online automatisch Schadsoftware zu analysieren (Abb. 2).

1. OSINT: Open Source Intelligence
2. vollautomatische Analyse
3. Analyse der statischen Eigenschaften
4. (interaktive) dynamische Analyse (Verhaltensanalyse)
5. statische Analyse (manuelles Reverse Engineering des Codes)

Im ersten Schritt, der OSINT-Suche, sammelt und analysiert man Daten aus öffentlichen Quellen. Viele Informationen über Malware tauscht die Community miteinander aus, daher ist eine solche Suche besonders interessant. Über öffentliche Plattformen lässt sich schnell feststellen, ob der Verdacht bei einer Datei tatsächlich angebracht ist, etwa mit VirusTotal. Wenn ja, bestimmt man die Art oder die Familie der Schadsoftware, beispielsweise mit der Malpedia von Fraunhofer FKIE (siehe ix.de/zk5s). Wie das Beispiel in Abbildung 1 zeigt, gibt Malpedia Informationen über die Schadsoftware (hier über Formbook) aus und listet Artikel auf, die damit in Verbindung stehen. Auch eine einfache Google- oder Twitter-Suche kann bereits viele nützliche Hinweise liefern. Mehr dazu in Teil 2 dieser Serie.

Während der Analyse können die von der Malware hinterlassenen Spuren – also die identifizierten Artefakte – dazu beitragen, einen Angriff besser zu verstehen und Rückschlüsse auf die Täter zu ziehen. Solche Merkmale, die auf eine Kompromittierung eines Netzwerks oder Computersystems hinweisen, werden als Indicators of Compromise (IOCs) bezeichnet. Sie sind nützlich für das Auswerten aktueller Angriffe und können dazu beitragen, Netzwerke oder Systeme sicherer zu machen. Durch das Überwachen der Infrastruktur auf bekannte IOCs hin kann man frühzeitig Anzeichen einer Attacke erkennen und sie gegebenenfalls verhindern. Ferner bestimmen IOCs die Techniken und Verhaltensweisen einer bestimmten Malware und lassen sich einfach innerhalb der Community teilen. Beispiele für IOCs sind ungewöhnlicher Netzwerkverkehr in Form von IPs und URLs, Registry-Einträge oder Hashwerte von Dateien.

Analyse in der Sandbox

Der einfachste Weg, die Funktionen einer verdächtigen Datei zu beurteilen, besteht darin, sie mit vollautomatischen Tools wie Sandboxes zu analysieren – insbesondere wenn nur wenige oder gar keine Informationen über die Malware vorliegen. Diese Werkzeuge sind darauf ausgelegt, schnell zu ermitteln, was die Datei tun könnte, wenn sie auf einem System läuft. Sie überwachen das Verhalten der Schadsoftware und erstellen Reports für eine schnelle Auswertung. Moderne Sandboxes generieren in der Regel Berichte mit vielen Details zu den Aktivitäten der Malware (Netzwerkverkehr, Änderungen an Dateien usw.). Hierzu gibt es zahlreiche Produkte, darunter Online-Sandboxes wie JoeSandbox (siehe ix.de/zk5s und Abbildung 2). Der zweite Teil dieser Reihe geht ausführlicher auf sie ein.

Vollautomatische Tools liefern meist nicht so viele Einsichten wie eine manuelle Analyse. Deswegen werden in der nächsten Phase die statischen Eigenschaften der Datei analysiert, wobei unter anderem die Gesamtstruktur, die Strings und die importierten Funktionen untersucht werden. Ziel ist es, Hypothesen über die Fähigkeiten der Datei zu entwickeln. Die Analyse statischer Eigenschaften kann manchmal ausreichen, um grundlegende IOCs zu definieren.

Hier spielt das PE-Format (Portable Executable) für ausführbare Dateien unter Windows eine wichtige Rolle. Eine PE-Datei besteht aus Headern (Kopfzeilen) und Sektionen. Header enthalten die Angaben, die das Betriebssystem benötigt, um die Datei in den Speicher zu laden und die Laufzeitumgebung für den Prozess einzurichten, damit er ordnungsgemäß ausgeführt werden kann. Der eigentliche Code und die Daten, aus denen die ausführbare Datei besteht, sind in Sektionen unterteilt. Sie haben spezielle Namen, die ihren Zweck angeben. Zum Beispiel enthält die Sektion .text den ausführbaren Code, .data die initialisierten Daten und .rsrc die vom Programm verwendeten Ressourcen, darunter Bilder oder eingebettete Binärdateien.

Die ebenfalls im PE-Header gespeicherte Importadresstabelle (IAT) verwendet Windows, um zum Ausführen benötigte Funktionen in externen Dynamic Link Libraries (DLLs) zu finden. Die importierten Funktionen vermitteln einen ersten Eindruck davon, was die Datei tun wird, wenn man sie ausführt – entsprechend hilfreich ist die Analyse der PE-Header für das Beurteilen eines Verdachts. Ein nützliches Tool zu diesem Zweck ist pestudio (siehe ix.de/zk5s). Es parst den PE-Header und liefert die

kryptografischen Hashwerte der Datei (MD5, SHA256) sowie viele andere Informationen wie Sektionen, Imports und Strings (siehe Abbildung 3). Die Analyse der statischen Eigenschaften von Malware beschreibt der dritte Artikel der Reihe näher.

Die dynamische Analyse in Phase 4 ist eine Technik, bei der man Malware ausführt und ihr Verhalten während der Laufzeit analysiert. Das geschieht in einer isolierten Umgebung wie einer virtuellen Maschine, die verschiedene Tools überwachen. Neben dem reinen Beobachten ihrer Aktivitäten ist es auch möglich, während der dynamischen Analyse mit der Malware zu interagieren. So lassen sich zusätzliche Fähigkeiten entdecken. Beispielsweise können Werkzeuge den Zugriff auf bestimmte Ressourcen, die die Schadsoftware benötigt, simulieren, etwa das Netzwerk durch die Simulation von Diensten wie HTTP/S oder DNS. Dies kann vorherige Hypothesen über ihre Fähigkeiten bestätigen oder negieren. Der vierte Artikel der Reihe steigt tiefer in die dynamische Analyse ein.

Ein Verständnis dafür, wie die Malware den Arbeitsspeicher nutzt, kann ebenfalls bei der Verhaltensanalyse zusätzliche Erkenntnisse bringen. Eine Speicheranalyse führt beispielsweise das Tool Volatility durch (siehe ix.de/zk5s).

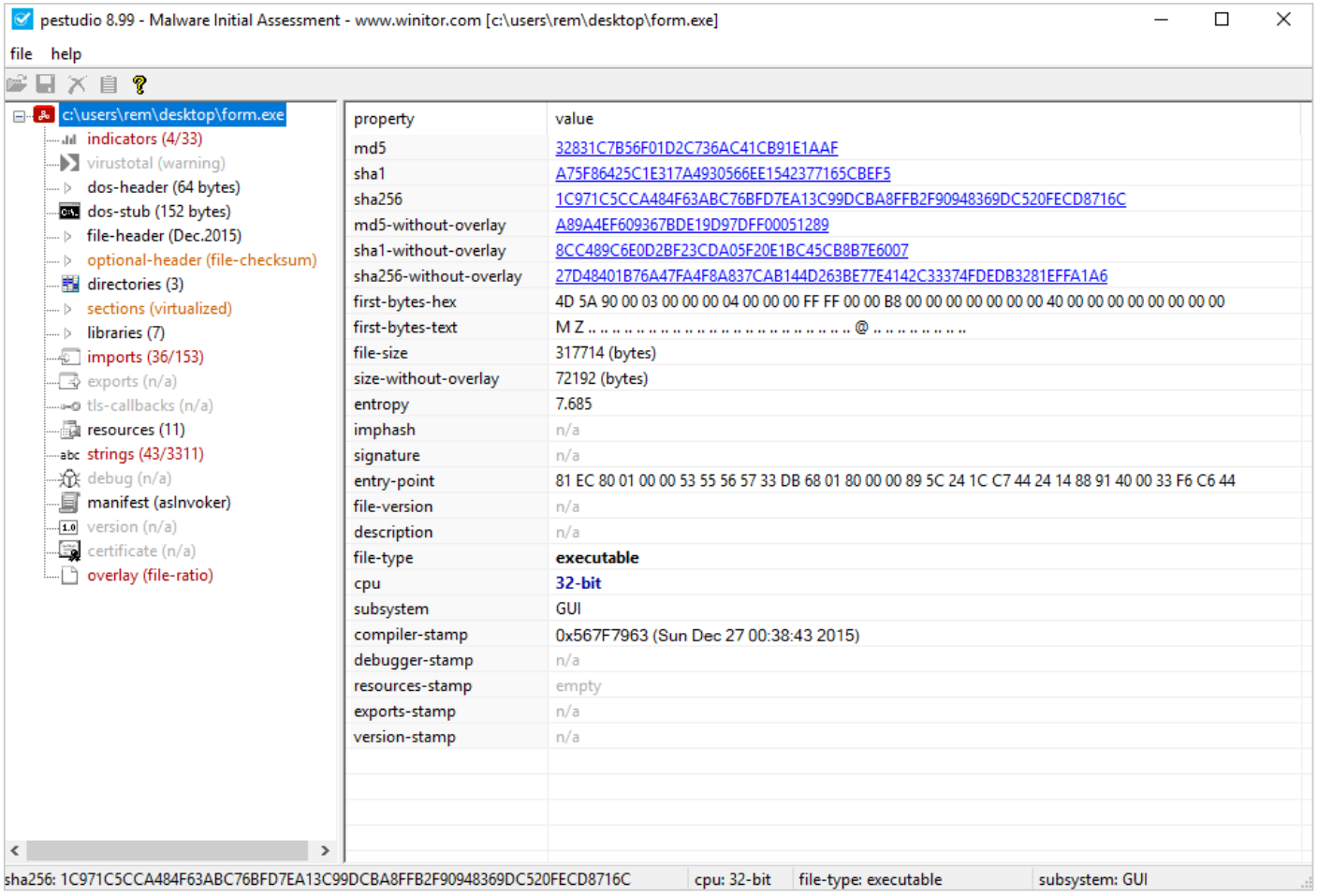
Wenn noch Zeit zur Verfügung steht, kann eine statische Analyse vorgenommen werden. Dabei wird die Malware analysiert, ohne dass sie ausgeführt wird. Stattdessen erfolgt ein manuelles Reverse Engineering des Codes mit Debuggern wie x64dbg oder anderen Disassembler-Tools wie Ghidra, um die inneren Abläufe besser zu verstehen. Manchmal kann ausschließlich eine statische Analyse bestimmte Informationen liefern, etwa über das Entschlüsseln von Daten, den Domaingenerierungsalgorithmus oder andere Aspekte, die bei einer dynamischen Analyse nicht ersichtlich sind.

Die einzelnen Schritte des Analyseprozesses werden natürlich in den meisten Fällen kombiniert. So können die in einer Phase gesammelten Informationen die Bemühungen in einer anderen Phase unterstützen. Es handelt sich also um einen Zyklus, den Analysten nur dann unterbrechen, wenn ihnen keine Ressourcen mehr zur Verfügung stehen.

Sicher arbeiten mit VMs

Der Einstieg in die Malware-Analyse ist auch für Nicht-Spezialisten kein Ding der Unmöglichkeit, gute allgemeine IT-Kentnisse sind jedoch notwendig. Bereits mit ein paar einfachen Analysen und öffentlich verfügbaren Hilfsmitteln lässt sich ein erster Überblick gewinnen, mit welcher Art von Schadsoftware man es zu tun hat. Dafür braucht es eine geeignete Prüfumgebung. Hier sind zwei Punkte zentral: die eigene Sicherheit, um gesunde Systeme nicht ungewollt mit der Malware zu infizieren, und die nötigen Ressourcen, um einerseits ein performantes System mit den benötigten Tools zur Hand zu haben, das andererseits auch einfach wiederzuverwenden ist.

Virtuelle Maschinen bieten aus mehreren Gründen einen guten Schutz vor Infektionen. Beim Analysieren einer potenziellen Schadsoftware besteht immer



Die PE-Header von Windows-Binaries liefern wichtige Informationen zum Identifizieren von Schadsoftware. Das Programm pestudio wertet sie aus (Abb. 3).

die Gefahr, sie durch eine Unachtsamkeit auszuführen. Manche Analysen setzen dies gar voraus. Eine virtuelle, vom Firmennetzwerk isolierte Umgebung verringert die Wahrscheinlichkeit, dass die Malware das Hostsystem infiziert und sich womöglich weiter im Netzwerk verbreitet. Ist die Analyse abgeschlossen, setzt man die VM per Snapshot in einen sauberen Zustand zurück und sie ist sofort wieder einsatzbereit.

Virtualisierung erlaubt es, die benötigten Ressourcen der Testumgebung anzupassen und verschiedene Betriebssysteme parallel zu verwenden. Nicht zuletzt lassen sich in abgeschotteten virtuellen Umgebungen Sicherheitsmechanismen ohne Risiko deaktivieren – schließlich ist es beim Analysieren einer Malware hinderlich, wenn ein Antivirenprogramm ständig anschlägt und die zu untersuchende Datei in Quarantäne verschiebt oder sogar direkt löscht.

Doch Vorsicht: Fortgeschrittene Malware erkennt, ob eine virtuelle Umgebung sie ausführt – woraufhin sie ihr Verhalten ändert. Diese Technik nennt sich Virtualization/Sandbox Evasion. Dabei sucht die Schadsoftware auf dem infizierten Gerät nach Analysetools wie Sysinternals oder Wireshark, aber auch nach spezifischen Artefakten einer VM wie den Guest Additions für VirtualBox. Wenn die Malware vermutet, dass sie analysiert wird, kann sie versuchen, die Analysetools zu beenden, sich selbst zu beenden, sich selbst in den Schlafmodus zu versetzen oder ihre schädlichen Eigenschaften zu verbergen.

VMs gut abschotten

Nach dem Installieren der VM ist auf die korrekte Netzwerkkonfiguration zu achten. Erfordert die Analyse eine Verbindung ins Internet, empfiehlt sich ein eigenes Netzwerk für die VM. Noch sicherer ist es, alle anderen Verbindungen zum Host zu trennen, indem man beispielsweise geteilte Verzeichnisse oder die gemeinsame Zwischenablage nicht zulässt. Für eine spätere dynamische Analyse ist es wichtig, dass sich die Malware frei entfalten kann. Schutzmechanismen wie Firewalls und Antivirenprogramme sollten deshalb in den Analyse-VMs abgeschaltet sein. Ist es erforderlich, ein ganzes Opfernetzwerk nachzustellen, müssen sich alle Analyse-VMs im selben abgeschotteten Netzwerk befinden, damit sie untereinander kommunizieren können.

Immer wieder taucht Malware auf, die aus der virtuellen Umgebung ausbrechen kann, solche Fälle nennt man VM Escapes. Auch wenn dies nicht auszuschließen ist, handelt es sich doch um fortgeschrittene Angriffe – die daher nicht sehr wahrscheinlich sind, wenn man nicht ein besonders lukratives Ziel ist. Dennoch sollte die Virtualisierungssoftware immer aktuell und sauber konfiguriert sein.

Für den Einstieg in die Malware-Analyse kann man auf existierende VMs aus der Community zurückgreifen. Diese enthalten bereits eine gute Auswahl an Analysewerkzeugen und sind korrekt vorkonfiguriert. REMnux und FlareVM sind zwei solche Systeme.

REMnux, entwickelt vom Securityberater und Forensikspezialisten Lenny Zeltser, ist eine Ubuntu-VM mit einer Sammlung aus Open-Source-Werkzeugen zur Malware-Analyse und fürs Reverse Engineering. Die installierten Tools ermöglichen die folgenden Analysen:

- Untersuchung statischer Eigenschaften einer verdächtigen Datei;
- statische Analyse von bösartigem Programmcode;
- dynamisches Reverse Engineering;
- Memory-Analyse eines infizierten Systems;
- Untersuchung des Netzwerkverkehrs für die Verhaltensanalyse;
- Prüfen der Interaktionen von Malware auf Systemebene;
- Analyse bösartiger Dokumente;
- Sammeln und Analyse von Bedrohungsdaten.

Das Image enthält viele gute Analyseprogramme, die auf der Website des Projekts dokumentiert sind. Auch wer nicht plant, die VM einzusetzen, erhält so einen guten Überblick über die Werkzeuge für die Malware-Analyse unter Linux.

Das von Mandiant entwickelte FlareVM ist eine Windows-VM. Neben den Sysinternals-Tools bringt sie Disassembler, Debugger, Decompiler und weitere Programme für die statische und dynamische Malware-Analyse mit sowie einzelne von Mandiant entwickelte Werkzeuge. Eine Übersicht und einen kleinen Crashkurs zum Einsatz der VM gibt es in einem Blogbeitrag der Entwickler.

Diese beiden VMs ergänzen sich gut: Viele Analyseprogramme gibt es ausschließlich für Linux, jedoch braucht man für die dynamische Analyse ein Windows-System zum Ausführen der Malware. Zusätzlich enthält eine Windows-Installation die nützlichen Sysinternals.

Fazit

Malware-Angriffe gehören leider zum digitalen Alltag. Besonders für Firmen besteht ein reelles Risiko, Opfer einer Schadsoftware zu werden. Dies hat meist finanzielle Schäden, Imageschäden und den Verlust von Informationen zur Folge. Im Hintergrund agieren häufig gut organisierte Tätergruppen. Umso wichtiger ist, dass sich auch die Gegenseite vernetzt und vom geteilten Wissen profitiert.

Da potenziell verseuchte Dateien immer eine Gefahr bedeuten, hat die sichere Handhabung oberste Priorität. Das umfasst das sichere Ablegen solcher Dateien in einer verschlüsselten Zip-Datei und eine geeignete Analyseumgebung, vorzugsweise eine VM.

Der Malware-Analyseprozess umfasst fünf Schritte, die sich in der Komplexität und Analysedauer unterscheiden sowie in der Tiefe der Informationen, die man damit erlangt. Die Artikel in den nächsten iX-Ausgaben behandeln die Onlinerecherche, die statische und die dynamische Analyse im Detail. (ulw@ix.de)

Quellen

Informationen zur erwähnten Software und Vorgehensweise bei der Malware-Analyse: ix.de/zk5s

NADIA MEICHTRY

ist Digital-Forensics- und Incident-Response-Spezialistin bei der Oneconsult AG. Sie unterstützt bei der Bewältigung und Untersuchung von Cybervorfällen.

FABIAN MURER

ist Senior Digital-Forensics- und Incident-Response-Spezialist bei der Oneconsult AG. Er unterstützt Firmen bei der Bewältigung von Cyberattacken und untersucht die Methoden der Angreifer bis auf den letzten Befehl.

TABEA NORDIEKER

ist als Digital-Forensics- und Incident-Response-Spezialistin bei der Oneconsult AG in Zürich angestellt, wo sie Kunden bei der Behebung von Cybersicherheitsereignissen unterstützt.