



Dynamische Malware-Analyse

Die statische Analyse verdächtiger Dateien führt zu Hypothesen, die Forensiker handfest prüfen müssen. Sie beobachten den Schadcode in voller Aktion – und zeichnen seine Aktivitäten auf.

Von Nadia Meichtry

■ Digitale Forensiker – oder auch Reverse Engineers – analysieren Schadsoftware in vier Phasen. In der vierten und letzten Phase, der dynamischen Analyse, wird die Malware in Aktion beobachtet. Der vierte Teil unserer Artikelserie zur Malware-Analyse erklärt also, welche Werkzeuge dafür notwendig sind und wie Forensiker in dieser Phase vorgehen. Eine vorausgehende OSINT-Analyse (Open Source Intelligence) schaffte zuerst ei-

nen Überblick darüber, womit man es überhaupt zu tun hat [1], danach folgte eine vollautomatische Analyse mit entsprechender Software in einer Sandbox-Umgebung [2]. Im dritten Teil ging es an die statischen Eigenschaften der Schadsoftware [3]. Alle drei vorherigen Schritte dienten dazu, Hypothesen über die Art und Wirkungsweise der Malware aufzustellen. Der letzte Teil der Artikelreihe befasst sich nun mit der dynamischen

Analyse – dem Beobachten der Malware in Aktion –, um die formulierten Hypothesen zu überprüfen.

Infektion zulassen

Während der dynamischen Untersuchung führt man die verdächtige Datei in einer virtuellen Maschine aus und zeichnet ihre Aktivitäten mit diversen Werkzeugen auf. Alle im Artikel erwähnten Tools sind auch unter ix.de/z48a zu finden. Analysten sollten jedoch nur die notwendigen Anwendungen starten, um keine unnötigen Interaktionen zu erzeugen. Sie überwachen unter anderem gestartete Prozesse, aufgebaute Netzwerkverbindungen, abgelegte Dateien sowie neu erstellte oder geänderte Registrierungsschlüssel und Dienste. Dabei läuft die virtuelle Maschine ohne Schutzmechanismen, sodass die Malware freies Spiel hat und nicht blockiert oder entfernt wird.

Dadurch will man Hinweise auf das Verhalten der zu analysierenden Datei gewinnen, um ihre Natur und die Bedrohung, die sie für das Unternehmen darstellen kann, zu verstehen. Die Beobachtungen können die vorherigen Hypothesen weiterentwickeln, die Liste der gefundenen Indicators of Compromise (IOCs) erweitern, die bei der Analyse der statischen Eigenschaften festgestellt wurden, oder zuvor identifizierte IOCs bestätigen. Es ist natürlich absolut notwendig, die Operation in einer virtuellen Maschine durchzuführen – handelt es sich tatsächlich um Schadsoftware, infiziert sie schließlich das System. Vorher erstellt man am besten einen sauberen Speicherpunkt, um das System gegebenenfalls zurückzuspielen und eine erneute Analyse durchführen zu können. Das Starten der Schadsoftware kann die Auf-

Malware-Analyse in vier Schritten

Teil 1: Einstieg – Grundlagen und Ablauf der Malware-Analyse

Teil 2: OSINT – Abfragen von öffentlichen Informationen, vollautomatische Analyse in der Sandbox

Teil 3: Statische Eigenschaften – Hypothesen anhand der Beschaffenheit von Malware aufstellen

Teil 4: Dynamische Eigenschaften – Aktivitäten der Malware aufzeichnen und auswerten

EXTRACT

- Bei der dynamischen Malware-Analyse überwachen Forensiker Prozesse, Netzwerkaktivitäten und Änderungen an der Registry von Windows-Systemen. Dafür müssen sie genau wissen, was zu den normalen Systemaktivitäten gehört, um Auffälligkeiten zu erkennen.
- Schadsoftware verfügt über unterschiedliche Fähigkeiten, zum Beispiel Prozessinjektion oder die Kommunikation mit einem C2-Server (Command and Control). Diese Fähigkeiten wollen Forensiker aufdecken.
- Die Analyseumgebung muss akribisch vorbereitet sein: Weder dürfen eigene Prozesse die Aufzeichnung stören, noch darf die Umgebung zu leer sein – denn manche Malware erkennt, ob sie sich in einer Laborumgebung befindet.

Process Hacker [DESKTOP-2C3IQHO\REM] - (Administrator)								
Hacker View Tools Users Help								
Refresh Options Find handles or DLLs System information Search Processes								
Processes Services Network Disk								
Name	PID	ASLR	Integrity	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0			50.88		52 kB	NT AUTHORITY\SYSTEM	
System	4		System	0.23		156 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	496	ASLR	System			364 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1360		System			100 kB	NT AUTHORITY\SYSTEM	
Interrupts				3.53		0		Interrupts and DPCs
csrss.exe	592	ASLR	System	0.03		1.46 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	660	ASLR	System			1.2 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	784	ASLR	System			3.35 MB	NT AUTHORITY\SYSTEM	Services and Controller app
lsass.exe	792	ASLR	System			5.22 MB	NT AUTHORITY\SYSTEM	Local Security Authority Proce...
fontdrvhost.exe	872	ASLR	Low			1.26 MB	Font Driver Host\UMFD-0	Usermode Font Driver Host
csrss.exe	672	ASLR	System	0.48	2.11 kB/s	1.56 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	720	ASLR	System			2.14 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
fontdrvhost.exe	864	ASLR	Low			3.43 MB	Font Driver Host\UMFD-1	Usermode Font Driver Host
dwm.exe	516	ASLR	System	1.64		104.16 MB	Window Manager\DWM-1	Desktop Window Manager
explorer.exe	3292	ASLR	Medium	7.77	712 B/s	45.34 MB	DESKTOP-2C3IQHO\REM	Windows Explorer
vmtoolsd.exe	4828	ASLR	Medium	0.09	608 B/s	23.29 MB	DESKTOP-2C3IQHO\REM	VMware Tools Core Service
Autoruns64.exe	4840	ASLR	Medium			13.86 MB	DESKTOP-2C3IQHO\REM	Autostart program viewer
ProcessHacker.exe	3584	ASLR	High	0.76		11.92 MB	DESKTOP-2C3IQHO\REM	Process Hacker
Form.exe	1724		Medium			5.3 MB	DESKTOP-2C3IQHO\REM	
aziztwhel.exe	4368		Medium			1.74 MB	DESKTOP-2C3IQHO\REM	
aziztwhel.exe	888	ASLR	Medium			5.18 MB	DESKTOP-2C3IQHO\REM	

Process Hacker zeigt bereits, dass Form.exe verdächtige Prozesse startet (Abb. 1).

merksamkeit der Angreifer wecken und ihnen mitteilen, dass sie untersucht werden. Grund dafür ist die Kommunikation mit ihrem Server, beispielsweise über den Aufruf ihrer Domänen oder IP-Adressen. Um das zu verhindern, sollte man entweder die Netzwerkverbindung der virtuellen Maschine unterbrechen oder die Verbindung in eine andere virtuelle Maschine weiterleiten, die einen Internetzugang nur simuliert. Das beeinflusst allerdings auch, was gemessen wird: Will die Schadsoftware etwa zusätzliche Dateien he-

runterladen und ausführen, so ist dies bei deaktivierter Netzwerkverbindung nicht mehr möglich und wird auch nicht erfasst. Der Mittelweg ist die Nutzung eines VPN oder des TOR-Netzwerks, um die eigene Herkunft zu verbergen und sich so zu schützen.

Malware-Fähigkeiten

Malware hat bestimmte Fähigkeiten, die man mit der dynamischen Analyse ermitteln kann. Sie könnte beispielsweise

mit einem Command-and-Control-Server (C2-Server) kommunizieren oder Dateien herunterladen und ablegen. Außerdem setzt Malware verschiedene Techniken ein, um sich der Erkennung zu entziehen – zum Beispiel Prozessinjektion. Ein C2-Server ist ein Server, der von den Angreifern kontrolliert wird, um die Kommunikation mit dem kompromitierten System aufrechtzuerhalten und es im schlimmsten Fall fernzusteuern. Meist wird HTTPS als Protokoll für C2-Server benutzt. Dass andere Protokolle wie DNS

Process Monitor - Sysinternals: www.sysinternals.com				
File Edit Event Filter Tools Options Help				
Time of Day	Process Name	PID	Operation	Path
10:27:20 2766042 AM	Form.exe	5044	CreateFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 276612 AM	Form.exe	5044	QueryBasicInformationFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2766303 AM	Form.exe	5044	CloseFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2767903 AM	Form.exe	5044	CreateFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2768049 AM	Form.exe	5044	QueryBasicInformationFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2768132 AM	Form.exe	5044	CloseFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2768531 AM	Form.exe	5044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
10:27:20 2768610 AM	Form.exe	5044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\aziztwhel.exe
10:27:20 2768717 AM	Form.exe	5044	RegOpenKey	HKLM\Software\Microsoft\Wow64\Wow64
10:27:20 2769689 AM	Form.exe	5044	CreateFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2769993 AM	Form.exe	5044	WriteFile	C:
10:27:20 2797055 AM	Form.exe	5044	SetEndOfFileInformationFile	C:
10:27:20 2797311 AM	Form.exe	5044	CreateFileMapping	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2797545 AM	Form.exe	5044	CreateFileMapping	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2797639 AM	Form.exe	5044	QueryStandardInformationFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2798090 AM	Form.exe	5044	CreateFileMapping	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2798358 AM	Form.exe	5044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\aziztwhel.exe
10:27:20 2798591 AM	Form.exe	5044	QuerySecurityFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2801207 AM	Form.exe	5044	QueryNameInformationFile	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2800962 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-1866265027-1870850910-1579135
10:27:20 2801065 AM	Form.exe	5044	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-1866265027-1870850910-1579135
10:27:20 2801207 AM	Form.exe	5044	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-1866265027-1870850910-1579135
10:27:20 2801294 AM	Form.exe	5044	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM
10:27:20 2801196 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM
10:27:20 2801610 AM	Form.exe	5044	Process Create	C:\Users\REM\AppData\Local\Temp\aziztwhel.exe
10:27:20 2801657 AM	aziztwhel.exe	3532	Process Start	
10:27:20 2801708 AM	aziztwhel.exe	3532	Thread Create	
10:27:20 2802025 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
10:27:20 2802096 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
10:27:20 2802238 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
10:27:20 2802297 AM	Form.exe	5044	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
10:27:20 2802408 AM	Form.exe	5044	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safe\CodeIdentifiers

In Process Monitor kann man das Verhalten der untersuchten Malware genauer nachverfolgen (Abb. 2).

No.	Time	Source	Destination	Protocol	Length	Info
2150	464781	192.168.198.130	192.168.198.129	DNS	77	Standard query 0x28d7 A www.3bmbc6t.life
2250	464883	192.168.198.129	192.168.198.130	DNS	93	Standard query response 0x28d7 A www.3bmbc6t.life A 192.168.19...
2550	617089	192.168.198.130	192.168.198.129	DNS	86	Standard query 0x4ee4 A win1718.ipv6.microsoft.com
2650	617425	192.168.198.129	192.168.198.130	DNS	102	Standard query response 0x4ee4 A win1718.ipv6.microsoft.com A 1...
3753	652711	192.168.198.130	192.168.198.129	DNS	77	Standard query 0xefb1 A www.3bmbc6t.life
3853	652805	192.168.198.129	192.168.198.130	DNS	93	Standard query response 0xefb1 A www.3bmbc6t.life A 192.168.19...
4961	568614	192.168.198.130	192.168.198.129	DNS	80	Standard query 0x622a A www.soyoutextile.net
5061	568770	192.168.198.129	192.168.198.130	DNS	96	Standard query response 0x622a A www.soyoutextile.net A 192.168...
6364	778845	192.168.198.130	192.168.198.129	DNS	80	Standard query 0x6a72 A www.soyoutextile.net
6464	779185	192.168.198.129	192.168.198.130	DNS	96	Standard query response 0x6a72 A www.soyoutextile.net A 192.168...
7372	662603	192.168.198.130	192.168.198.129	DNS	74	Standard query 0xb7a4 A www.pwcgov.net
7472	662821	192.168.198.129	192.168.198.130	DNS	90	Standard query response 0xb7a4 A www.pwcgov.net A 192.168.198.1...
8775	856706	192.168.198.130	192.168.198.129	DNS	74	Standard query 0xb65a A www.pwcgov.net
8875	856970	192.168.198.129	192.168.198.130	DNS	90	Standard query response 0xb65a A www.pwcgov.net A 192.168.198.1...
9783	772973	192.168.198.130	192.168.198.129	DNS	81	Standard query 0xcab0 A www.senhongtea.online
9883	773256	192.168.198.129	192.168.198.130	DNS	97	Standard query response 0xcab0 A www.senhongtea.online A 192.16...

Wireshark stellt die Kommunikationen von Form.exe zwischen der infizierten virtuellen Maschine und dem Linux-System dar (Abb. 5).

hinweisen, weil sie auf dem System eines typischen Opfers nicht installiert sind.

Prozessanalyse

Um der Malware nun endgültig auf die Schliche zu kommen und ihre bösartigen Prozesse zu erkennen, müssen Analysten zunächst wissen, wie der Prozessbaum auf einem System im Normalfall aussieht. Dazu hat bereits das SANS-Institut ein Poster für Windows-Systeme veröffentlicht (siehe ix.de/z48a). Unter dem Titel „Evil Hunt 1“ erklärt es, welche Elternprozesse welche Kindprozesse starten. Beispielsweise sollte es nur eine Instanz von lsass.exe geben, mit wininit.exe als Elternprozess. Bei der Analyse ist es daher wichtig, die Beziehungen zwischen den Prozessen und ihre Prozesspfade zu überprüfen. Dafür kann man verschiedene freie Werkzeuge für Windows verwenden, wie Process Hacker und Sysinternals Process Explorer von Microsoft. Sie überwachen unter anderem die Systemressourcen sowie den Prozessbaum, die Prozessnamen und -kennungen (PID). Die Tools zeigen die von den Prozessen geöffneten oder geladenen Handles und DLLs an. Darüber hinaus listet Process Hacker Dienste und aktive Netzwerkverbindungen auf, ähnlich wie Sysinternals TCPView4. Prozesse werden auch farblich hervorgehoben: Grün steht für gestartete Prozesse, Rot für beendete und Blau für System- und Dienstprozesse.

Neben diesen beiden Werkzeugen gibt es Sysinternals Process Monitor. Er überwacht in Echtzeit die Prozessaktivitäten und Interaktionen mit anderen Prozessen, der Registry, dem Dateisystem und dem Netzwerk und protokolliert sie in einer Datei. Process Monitor erfasst Prozessdetails, einschließlich Befehlszeile und Operationen. Man kann Filter defi-

nieren, um sich beispielsweise auf einen Prozess zu konzentrieren oder normale Aktivitäten auszuschließen. Das Tool verfügt auch über eine Funktion zum Zeichnen des Prozessbaums, der alle im Protokoll referenzierten Prozesse in einer Eltern-Kind-Hierarchie anzeigt. Prozesse mit demselben Elternteil sortiert es nach ihrer Startzeit. Process Monitor gibt dabei auch einige Daten aus: den Pfad der ausführbaren Datei, das Benutzerkonto und die Startzeit. Solche Protokolle können anschließend mit ProcDOT visualisiert werden, indem man ein Aktivitätsdiagramm für den gewählten Prozess erstellt. Dadurch lassen sich Anomalien leicht aufdecken.

Um die vorgestellten Werkzeuge zu veranschaulichen, kann man innerhalb einer virtuellen Windows-Maschine die Malware-Datei Form.exe ausführen, die bereits in Teil 2 der Reihe vorgestellt wurde [2]. Der Prozessbaum in Process Hacker zeigt, dass der Prozess Form.exe unterhalb von explorer.exe läuft (siehe Abbildung 1). Das bedeutet, dass dieses Programm durch den Benutzer per Doppelklick ausgeführt wurde, in diesem Fall vom Desktop aus. Form.exe verwendet außerdem das Logo von Adobe, um legitim zu wirken. Ebenso kann man sehen, dass Form.exe azitwhel.exe aufruft, das dann eine weitere Instanz von sich selbst startet (in Abbildung 1 grün hervorgehoben). Das deutet auf eine Prozessinjektion hin. Ein solcher Prozessname aus zufälligen Charakteren ist besonders auffällig und legt nahe, dass es sich um einen bösartigen Prozess handelt – ein Eindruck, der sich dadurch verstärkt, dass sich alle drei Prozesse in weniger als einer Sekunde beendeten, um unentdeckt zu bleiben.

In Process Monitor ist das noch einmal detaillierter zu sehen, denn das Tool

zeigt an, welche Operationen konkret durchgeführt wurden. Wie in Abbildung 2 zu sehen, legt Form.exe zuerst die Datei azitwhel.exe unter C:\Users\REM\AppData\Local\Temp mit der Operation CreateFile an (zu sehen in der ersten roten Box in Abbildung 2). Der Pfad AppData\Local\Temp ist als Ablageort von Malware beliebt, da er zuverlässig vorhanden ist und keine erhöhten Rechte zum Schreiben benötigt. Außerdem ist er ein unauffälliger Bereich, den viele Opfer von Malware-Angriffen übersehen, da er nicht zwingend von Antivirenlösungen gescannt wird.

Anschließend öffnet die Schadsoftware den Registrierungsschlüssel HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\azitwhel.exe mit der Operation RegOpenKey (siehe zweite rote Box in Abbildung 2), um den Wert abzufragen.

Mit so einem Vorgehen versucht Malware üblicherweise, Persistenz herzustellen und Privilegien zu erhöhen. MITRE ATT&CK beschreibt, dass es die Image File Execution Options (IFEO) ermöglichen, einen Debugger an eine Anwendung anzuhängen. Beim Erstellen eines Prozesses wird ein Debugger, der in den IFEO einer Anwendung konfiguriert ist, dem Namen der Anwendung vorangestellt – der neue Prozess startet effektiv unter dem Debugger. Diese Optionen können direkt über die Registry unter HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable> eingestellt werden, wobei <executable> die Binärdatei ist, an die der Debugger angehängt ist. In diesem Fall handelt es sich um die Datei azitwhel.exe. Die Malware verschafft sich so einen Hintertürzugang als „Debugger“. Nachdem die Malware die Registry geändert hat, wird das Debugger-Programm

mit Systemrechten ausgeführt. Form.exe startet dann mit der Operation Process Create azizthwel.exe (siehe dritte rote Box auf Abbildung 2).

Der aus den Logs von Process Monitor erstellte Prozessbaum (siehe Abbildung 3) sieht genauso aus wie der von Process Hacker. Man kann feststellen, dass die Lebensdauer (mit grüner Markierung) der Prozesse Form.exe und azizthwel.exe recht kurz war. Beide azizthwel.exe-Prozesse rufen außerdem die Datei nydkr.nr in Temp-Ordner auf.

Mit ProcDOT ist das Starten der beiden azizthwel.exe-Prozesse ebenfalls deutlich sichtbar. Es zeigt im Ereignisbaum an, dass temporäre Dateien erstellt wurden: nydkr.nr, gdeinuzidby.smf, syDOB8.tmp und syDOB9.tmp. Die zwei tmp-Dateien wurden dann gelöscht – bei tmp-Dateien ist das zu erwarten, da sie in der Regel entfernt werden, wenn der Prozess sich beendet.

Die Gesamtheit der Resultate stimmt mit den Informationen im Behavior Graph von Joe Sandbox und mit dem beschriebenen Verhalten in VirusTotal überein (siehe ix.de/z48a). Das stärkt natürlich das Vertrauen in die vorangegangenen Untersuchungsergebnisse. Und auch die von der Malware abgelegten Dateien findet man bei Joe Sandbox und VirusTotal unter „Dropped files“. Joe Sandbox berichtet, dass die nr-Datei eine COM-Datei ist – ausführbare Dateien, die in der Regel für das Ausführen einer Reihe von Befehlen verwendet werden.

Analyse von Netzwerkverbindungen

Nachdem man beobachtet hat, was die Malware im System anstellt, kann man sich der Kommunikation widmen, die sie nach draußen aufbaut. Um Netzwerkverbindungen zu untersuchen, empfiehlt es sich, die Internetressource, auf die die Datei zugreifen möchte, im Labor zu simulieren. Indem man die bösartige Netzwerkverbindung auf einen kontrollierten Server und Dienst umleitet, gibt man der Malware die Möglichkeit, Daten

mit dem Server auszutauschen. Dadurch lassen sich mehr Informationen über die netzwerkbezogenen Aktivitäten des Programms gewinnen, wie die Kommunikation zu C2-Servern, Datenexfiltration und Versuche, andere Software herunterzuladen. Verdächtig ist zum Beispiel der Verbindungsaufbau zu IP-Adressen oder Domänen, die bereits als bösartig bekannt sind, zu IP-Adressen aus unüblichen Ländern, zu auffälligen Ports oder über ungewöhnliche Protokolle.

Zum Überwachen der Netzwerkverbindungen eignen sich Tools wie Wireshark, TCPLogView oder Sysinternals TCPView (siehe ix.de/z48a). Der Network-Tab von Process Hacker kann auch weiterhelfen. Das Tool zeigt allerdings nur aktive Verbindungen an, eine Historie gibt es nicht. Die Überwachungswerkzeuge sollte man prinzipiell auf einem anderen System als dem infizierten ausführen, denn so ist es für die Malware schwieriger zu entdecken, dass sie beobachtet wird – sie könnte versuchen, die Analysetools zu stören. Ein Sniffer zur Netzwerkanalyse kann auf jedem Rechner innerhalb des Labornetzwerks eingesetzt werden, vorausgesetzt, er arbeitet im promiskuitiven Modus. Dafür stellt man die Netzwerkschnittstelle so ein, dass sie alle Pakete im zugewiesenen Netzsegment erfasst und jedes empfangene Paket im Detail aufzeichnet.

Wireshark eignet sich gut zum Überwachen des Labornetzwerks. Der Netzwerk-Sniffer erfasst Pakete und speichert sie. Dabei gibt er die Quell- und die Ziel-IP-Adresse, das verwendete Protokoll, die Paketlänge und den Inhalt der Pakete an. Die erfassten Pakete kann man dann nach jeder Komponente filtern. Sie werden auch eingefärbt, in der Regel entsprechend dem verwendeten Protokoll. Wireshark gibt jedoch nicht an, welcher lokale Prozess an der Verbindung beteiligt war – an dieser Stelle können aber TCPLogView oder TCPView helfen, da sie ein Protokoll der lokalen TCP-Verbindungen speichern. Das zeigt, welcher Prozess welche Verbindung hergestellt hat.

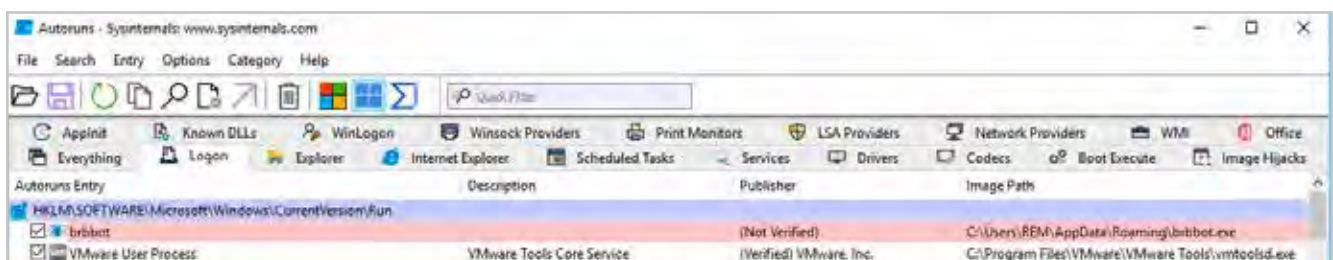
Damit die Malware auf die benötigten Ressourcen zugreifen kann, startet man eine interaktive dynamische Analyse mit Werkzeugen wie FakeDNS. FakeDNS löst alle Domänen auf, die von der Malware kontaktiert werden, wenn sie das System infiziert. Es beantwortet alle Anfragen nach Domännennamen mit einer konfigurierbaren IP-Adresse im Antwortdatensatz. Bei der Analyse enthält der Datensatz von FakeDNS die IP-Adresse der virtuellen Maschine, auf der er läuft.

FakeDNS und Wireshark zeigen beide deutlich, welche Domänen von Form.exe kontaktiert wurden, darunter www.3bmbc6t.life und www.pwcgov.net (siehe Abbildung 4 und 5). In Abbildung 4 ist auch erkennbar, dass FakeDNS mit der IP-Adresse der Linux-Maschine antwortet (192.168.198.129). In Abbildung 5 ist zu sehen, dass die Resultate von Wireshark gefiltert wurden, um nur DNS-Anfragen anzuzeigen, bei denen die Kommunikation zwischen der infizierten Windows-Maschine (IP-Adresse 192.168.198.130) und der Linux-Maschine sichtbar ist.

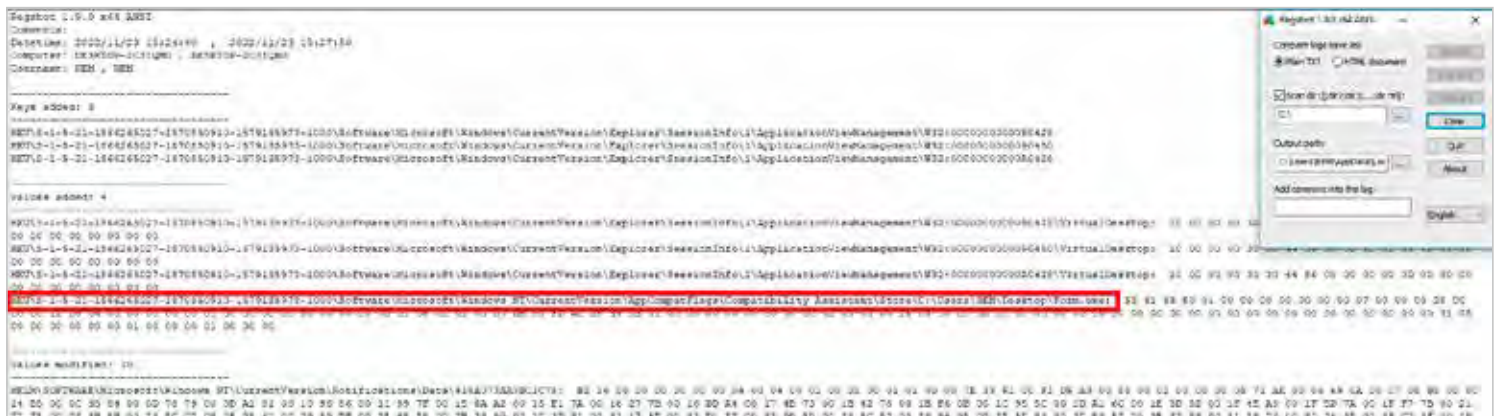
Hierbei handelt es sich um die Kommunikation mit einem C2-Server, schließlich hat Joe Sandbox www.pwcgov.net bereits als C2 aufgelistet. Die anderen Domänen sind auch unter „Domains and IPs“ in Joe Sandbox und unter „Relations“ auf VirusTotal zu finden. Die Anfragen an die Microsoft-Domänen sind hingegen legitim und entsprechen dem normalen Betrieb des Systems.

Systemänderungen überwachen

Schadsoftware nimmt häufig Änderungen am System vor, um einen Systemneustart zu überleben – oder unbemerkt auf dem System zu bleiben, indem sie beispielsweise Antivirenprogramme deaktiviert. Auf solche Maßnahmen können auch Änderungen an den Autostart-Speicherorten wie den Run-Registrierungsschlüsseln und im %AppData%\Roaming-Ordner hinweisen, die es der Malware ermöglichen, sich beim Anmelden des Benutzers oder beim Systemstart auszuführen.



Um persistent zu bleiben, kann Malware sich in den Autostart schleichen. Autoruns zeigt, dass brbbot.exe dafür einen Registrierungsschlüssel modifiziert (Abb. 6).



Regshot analysiert das Verhalten von Form.exe – die Malware nistet sich im Programmkompatibilitätsassistenten ein (Abb. 7).

Schadsoftware kann außerdem Dateien ablegen, wie nachgeladene Malware, Konfigurationsdateien oder Lösegeldforderungen von Ransomware als ReadMe-Textdateien.

Solche Änderungen kann man mit Werkzeugen wie Sysinternals Autoruns und Regshot überwachen. Autoruns zeigt Konfigurationen auf, die es erlauben, Malware persistent zu machen. Dazu gehören RunOnce-Registrierungsschlüssel, geplante Aufgaben und Dienste. Bei vie-

len schädlichen Programmen fehlen oft Angaben zum Herausgeber, eine Beschreibung oder die Version. Autoruns prüft die Signatur der Programme und kann auch Einträge mit VirusTotal abgleichen, wobei das Tool eine bestimmte Farbcodierung benutzt: Rosa bedeutet, dass keine Informationen zum Herausgeber gefunden wurden oder dass die digitale Signatur nicht existiert, bei gelber Färbung ist der Starteintrag vorhanden, aber die Datei, auf die er verweist, gibt es

nicht mehr, und Grün zeigt Elemente an, die beim letzten Mal nicht im Autostart vorhanden waren.

Bei der Analyse von Form.exe fand Autoruns keine Persistenzeinträge. Um sie dennoch zu veranschaulichen, kommt an dieser Stelle eine andere beispielhafte Schadsoftware zum Einsatz: brbbot.exe (siehe Abbildung 6). brbbot.exe erstellt einen Eintrag im Registrierungsschlüssel Microsoft\Windows\CurrentVersion\Run. Das ermöglicht es der Malware,

```

-----
Files added: 12
-----
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D33.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E1C.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E5C.tmp.txt
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER8D33.tmp.WERInternalMetadata.xml
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER8E1C.tmp.csv
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER8E5C.tmp.txt
C:\Users\REM\AppData\Local\Temp\aziztwheel.exe
C:\Users\REM\AppData\Local\Temp\gdeinuizidby.smf
C:\Users\REM\AppData\Local\Temp\nydkr.nr
C:\Users\REM\AppData\Local\Temp\RD8D32.tmp\empty.txt
C:\Windows\Prefetch\AZIZTWHEEL.EXE-72B7C94A.pf
C:\Windows\Prefetch\FORM.EXE-CAA82D32.pf

```

Mehrere Dateien wurden von der Malware neu angelegt. Dank Regshot können Forensiker sehen, wie sie an unverdächtigen Stellen auftauchen (Abb. 8).

dauerhaft auf dem System zu bleiben und bei jeder Anmeldung gestartet zu werden. Weil es weder eine Beschreibung noch einen Herausgeber gibt, hebt Auto-runs ihn in Rosa hervor.

Regshot vergleicht den Zustand des Systems vor und nach der Infektion, indem es Schnappschüsse erstellt und einen Bericht generiert, der die Änderungen am Dateisystem und der Registrierung wie neue Dateien oder Einträge in der Registrierung aufzeigt, die während der Infektion entstanden. Das liefert Hinweise auf Persistenzmechanismen der Malware. Regshot kann jedoch keine Informationen über die spezifische Abfolge von Ereignissen liefern oder angeben, welcher Prozess für die Änderungen verantwortlich ist. Dafür ist Process Monitor besser geeignet.

Im Beispiel von Form.exe zeigt Regshot aber, dass der Eintrag C:\Users\REM\Desktop\Form.exe dem Registrierungsschlüssel Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store hinzugefügt wurde (siehe rote Box in Abbildung 7). In diesem Registrierungsschlüssel erscheinen die Programme, bei denen der Programmkompatibilitätsassistent verwendet wird. Er verfolgt ein Programm, wenn es ausgeführt wird, und identifiziert alle Anzeichen bekannter Kompatibilitätsprobleme – Programme, die in diesem Registrierungsschlüssel auftauchen, sind also erst einmal unverdächtig.

Regshot macht aber auch sichtbar, dass mehrere Dateien durch das Ausführen von Form.exe geändert oder hinzugefügt wurden (in der oberen roten Box in Abbildung 8 zu sehen). aziztwheel.exe, nydkr.nr und gdeinuizidby.smf sind alle im Temp-Ordner gelandet, außerdem hat die Malware pf-Dateien (Prefetch) für Form.exe und aziztwheel.exe erstellt (siehe untere rote Box in Abbildung 8). Prefetch ist ein Prozess, bei dem das Betriebssystem wichtigen Code und Daten

von der Festplatte in den Speicher lädt, bevor sie benötigt werden. Der Prefetch-Ordner wird nach der ersten Ausführung eines Programmes mit einer .pf-Datei gefüllt. Auch das ist normales Systemverhalten.

Die Dateien im Temp-Ordner sind auch unter „Dropped files“ im Bericht von Joe Sandbox zu sehen, die Registrierungsschlüssel und andere Änderungen am Dateisystem findet man dort ebenfalls unter „Behavior“. Joe Sandbox und VirusTotal ließen bereits vermuten, dass es sich um eine Schadsoftware, höchstwahrscheinlich Formbook, handelt, und die Überprüfung der IOCs auf Online-diensten wie Malpedia deutet ebenfalls darauf hin. Statische und dynamische Analyse haben also vermitteln können, wie die Malware arbeitet – und erlauben es dadurch auch, Gegenmaßnahmen zu ergreifen.

Fazit

Durch das Überwachen von Prozessen, Netzwerkaktivitäten und Systemänderungen kann eine dynamische Analyse die Fähigkeiten einer Schadsoftware bestimmen, wie die Kommunikation mit einem Command-and-Control-Server oder die Injektion in andere Prozesse, um unentdeckt zu bleiben. Diese Aktivitäten können aber nur dann aufgedeckt werden, wenn bereits bekannt ist, wie das System normalerweise funktioniert. Die dynamische Analyse vervollständigt am Schluss die Liste der IOCs, die Forensiker in den vorherigen Analysephasen identifizierten.

Allerdings ist es kaum möglich, alles, was die Malware anrichten kann, nur mit einer dynamischen Analyse herauszufinden – insbesondere, wenn die Malware fähig ist zu erkennen, dass sie analysiert wird. Man kann zusätzlich noch eine Arbeitsspeicheranalyse durchführen, beispielsweise mit dem Speicherforensik-Framework Volatility. Codeanalyse (Re-

verse Engineering) führt ebenfalls zu einem tiefgreifenden Verständnis der Funktionsweise der Schadsoftware, ist jedoch zeitaufwendig. Beide Techniken bereiten zwar den Weg für weitergehende Analysen – die vier in der Artikelreihe genannten Schritte liefern aber bereits ein ziemlich klares Bild von der fraglichen Schadsoftware.

Malware stellt ein tägliches Risiko für Unternehmen dar und verschiedene Arten von Angreifern setzen verschiedene Arten von Schadsoftware ein. Hat man eine verdächtige Datei in den Händen, ist Vorsicht geboten – selbst Onlineplattformen und Sandboxes bergen Risiken. Angreifer setzen außerdem natürlich alles daran, ihre Software so gut wie möglich zu verbergen – eine statische Analyse kann zum Beispiel die Tarnung als Makro auffliegen lassen, mit der Schadsoftware in PDF- und Office-Dokumenten versteckt ist. Informationen, die man durch solche Analysen gewinnt, kann man in der dynamischen Analyse dann noch einmal erhärten und genau hinschauen: Wie verhält sich die Malware, wie kommuniziert sie? Sämtliche Erkenntnisse hängen aber von einem gut sortierten Werkzeugkasten ab – verschiedene Werkzeuge sind in unterschiedlichen Phasen der Analyse hilfreich.

Schlussendlich dürfen Forensiker aber bei aller Detektivarbeit nicht vergessen, dass Schadsoftware auch während der Analyse Risiken birgt. Oberste Maxime sollte daher sein, sich selbst entsprechend zu schützen. (kki@ix.de)

Quellen

- [1] Nadia Meichtry, Fabian Murer, Tabea Nordieker; Einstieg in die Malware-Analyse; iX 2/2023, S. 98
- [2] Nadia Meichtry, Fabian Murer, Tabea Nordieker; Malware Analyse per OSINT und Sandbox; iX 3/2023, S. 122
- [3] Nadia Meichtry, Statische Malware-Analyse; iX 5/2023, S. 132
- [4] Die Vorgestellten Tools und weitere Informationen finden sich unter ix.de/z48a.

NADIA MEICHTRY

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

