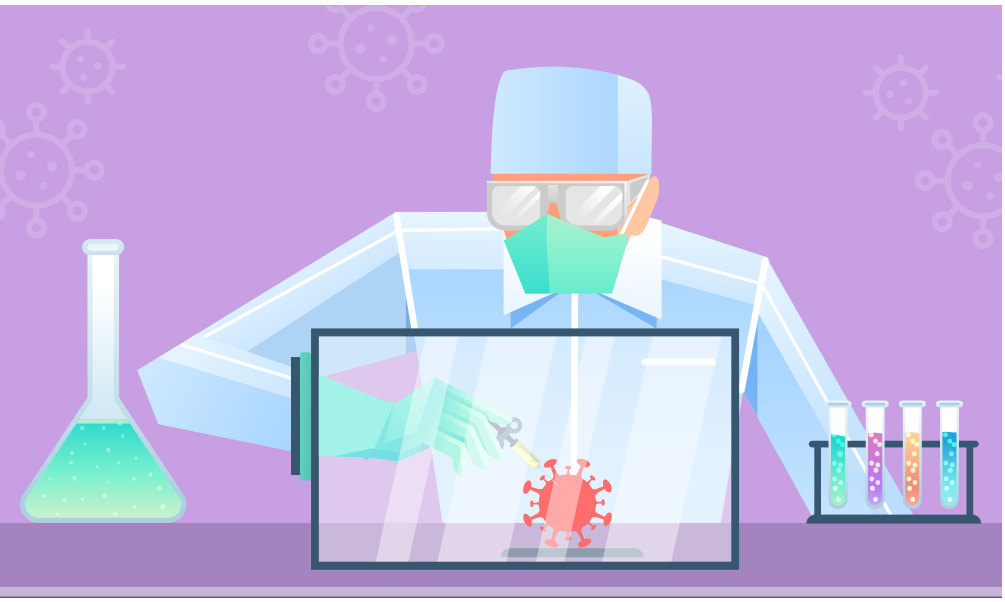


Malware-Analyse per OSINT und Sandbox

Öffentliche Informationen und frei zugängliche automatische Tools sind die ersten Anlaufstellen bei der Analyse von Schadsoftware. Sie sind zahlreich und in guter Qualität vorhanden und setzen nur wenig Vorwissen voraus.

Von Nadia Meichtry, Fabian Murer und Tabea Nordieker

Die einzelnen Stadien der Schadsoftwareanalyse unterscheiden sich im Detailgrad der Ergebnisse und im benötigten Vorwissen. Der erste Teil dieser Artikelserie hat sie im Überblick vorgestellt [1]. Die erste Phase ist fast immer eine Onlineanalyse, die schnell und mit relativ geringem Aufwand zu einer ersten Einschätzung gefundener potenzieller Schadsoftware führt. Dieses Hinzuziehen öffentlich zugänglicher Informationen gehört zu den Open Source Intelligence Techniques (OSINT), ein Begriff, der im Geheimdienstmilieu geprägt wurde, aber auch im Journalismus Verwendung findet.

Die Ziele von OSINT können sehr unterschiedlich sein: Finden personenbezogener Daten, Standortidentifikation per Bildersuche und vieles mehr. Einen allgemeinen Überblick dazu liefert das OSINT-Framework, eine umfangreiche Sammlung von Analysemöglichkeiten, sortiert nach der Art der Artefakte (Links zu allen erwähnten Tools und Websites sind unter ix.de/zsu5 aufgeführt). Bei der Malware-Analyse steht die Suche nach den Indicators of Compromise (IoCs) im Vordergrund, also nach allen Merkmalen, die auf eine Schadsoftware hinweisen. Ziel ist es, identifizierte Artefakte abzugleichen, um deren Gefährlichkeit zu prüfen und daraus neue Ansätze für die weitere Analyse zu gewinnen.

iX-TRACT

- OSINT (Open Source Intelligence), also die Suche in öffentlichen Quellen, ist die erste Stufe der Malware-Analyse und meist sehr ergiebig.
- Websites und Plattformen wie VirusTotal, Malpedia, abuse.ch oder MISP liefern aktuelle zuverlässige Informationen zu verdächtigen Dateien und zu Strategien der Angreifer.
- In Sandboxes lässt sich Schadsoftware gefahrlos ausführen und analysieren. Sie sind auch kostenlos online verfügbar und liefern umfangreiche Analyseergebnisse.
- Wer Onlinewerkzeuge benutzt, muss wissen, dass er möglicherweise Spuren hinterlässt, die auch dem Angreifer nützen.

Threat Intelligence als Vorsorge

Darüber hinaus kann OSINT ein Mittel sein, die aktuelle Bedrohungslage zu beobachten, um sich zukünftig besser vor Schadsoftware zu schützen, also Threat Intelligence zu betreiben und so Hintergrundinformationen zu aktuellen Malware-Angriffen und bekannten Tätergruppierungen zu sammeln. Hilfreich hierbei ist das MITRE ATT&CK Framework (MITRE Adversarial Tactics, Techniques, and Common Knowledge). Es handelt sich um eine Wissensdatenbank, die das Vorgehen von Cyberangreifern beschreibt, geordnet nach Phasen des Angriffs und Zielplattformen.

Informationen über die Schadsoftware selbst liefern zahlreiche offen zugängliche Plattformen, die IoCs prüfen. Eine gute erste Anlaufstelle ist VirusTotal, eine Plattform, die gefundene IoCs und Dateien mit einer Vielzahl von bekannten und bereits analysierten Malware-Samples abgleicht. Ist der gesuchte IoC noch nicht bekannt, bietet VirusTotal die Möglichkeit, das Malware-Sample selbst hochzuladen. Dabei wird die Malware von mehreren Antivirenlösungen gescannt und die Resultate werden im Anschluss der Datenbank hinzugefügt.

Die Suchmaschine Malpedia des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE ist eine gute Adresse für die Recherche nach technischen Berichten zu einer Art von Schadsoftware, wenn man bereits eine Idee hat, worum es sich bei der Datei handeln könnte.

Das Ziel der Malware-Analyse ist es, IoCs zu identifizieren, um das Verhalten der Schadsoftware zu beschreiben und Sicherheitsmaßnahmen daran auszurichten. Ein Projekt, das den Austausch von IoCs fördert, ist die in Europa als Open Source entwickelte Malware Information Sharing Platform (MISP). Innerhalb der eigenen Organisation kann eine MISP-Plattform auf einem beliebigen Linux-System installiert werden, wobei

Ubuntu empfohlen wird. Die Installation enthält bereits einen öffentlich zugänglichen Satz an Threat Intelligence, der mit individuellen Einträgen ergänzt werden kann. Es gibt zahlreiche themen- oder organisationsspezifische Communitys, die in der Regel für Interessierte offen sind. MISP definiert auch eine Reihe von Datenmodellen und Formaten für den Austausch von IoCs und Threat Intelligence, richtet Events aus und bietet Trainings an.

Spielen wir die Nutzung solcher öffentlichen Plattformen an einem Beispiel durch. Ein Malware-Analyst wurde zu einem Cybervorfall gerufen und damit beauftragt, eine auf einem kompromittierten System identifizierte Datei mit dem Namen Form.exe zu analysieren. Er soll herausfinden, ob diese Datei mit dem Angriff zu tun haben könnte, ob es eine schädliche Datei ist und, wenn ja, was sie bei der Ausführung tut.

Sicher suchen mit dem Hashwert

Es beginnt mit der Suche nach Metainformationen und eindeutigen Identifikatoren der potenziellen Malware. Ein eindeutiges Erkennungsmerkmal einer Datei ist der kryptografische Hash, der sich unter Windows mit dem PowerShell-Befehl `Get-FileHash` (siehe Abbildung 1) ermitteln lässt.

Eine einfache Suche nach diesem Hashwert auf VirusTotal liefert bereits innerhalb von Sekunden die Erkenntnis, dass es sich bei der Datei sehr wahrscheinlich um eine Schadsoftware handelt. Mehr als die Hälfte aller in VirusTotal registrierten Antiviren- und Securityprogramme haben genau diese Datei schon einmal gesehen und als Malware eingestuft (siehe Abbildung 2). Obwohl man sieht, dass diese Datei wohl bösartig ist, steht noch nicht zweifelsfrei fest, um welche Art von Schadsoftware es sich handelt. So wird die Datei als Trojaner, generell als „malicious“ oder als Injector eingestuft, lediglich zwei Malware-Scanner nennen eine konkrete Malware-Familie, in diesem Fall FormBook.

Weitere Plattformen wie Malpedia liefern mehr Informationen über FormBook. Auf Malpedia werden verschiedene Veröffentlichungen im Zusammenhang mit Malware-Typen und -Familien verlinkt, so auch über bereits durchgeführte Analysen dieser Schadsoftware. Diese Informationen können dabei helfen, die richtigen Sofortmaßnahmen während eines Sicherheitsvorfalls einzuleiten, oder sie dienen als Ausgangspunkt für die tiefere Analyse.

Wie in Abbildung 2 zu sehen, bietet auch VirusTotal selbst diverse weitere Informationen über das Malware-Sample. Unter dem Reiter Details sind verschiedene statische Informationen wie zusätzliche kryptografische Hashwerte oder Versionsinformationen zusammengefasst.

VirusTotal geht ins Detail

Der Reiter Relations listet Artefakte auf, die mit dem zu analysierenden Beispiel in Verbindung stehen: IP-Adressen, die das Malware-Sample zu kontaktieren versucht, oder URLs, von denen diese Schadsoftware heruntergeladen wird. Im Reiter Behavior finden sich, wie der Name schon sagt, Informationen über das Verhalten der Schadsoftware, etwa Änderungen der Registry und Programmaufrufe. Daraus ergeben sich bei einem laufenden Cyberangriff oft Sofortmaßnahmen, etwa das Sperren der genannten IP-Adressen oder URLs auf der Firewall oder dem Webproxy.

Die Fähigkeiten der analysierten Datei sind dabei den verschiedenen Techniken aus dem MITRE ATT&CK Framework zugeordnet (siehe Abbildung 3). So ist im gezeigten Beispiel die Wahrscheinlichkeit groß, dass die Zugangsdaten und Passwörter des betroffenen Benutzers gestohlen und/oder geknackt wurden, da die Schadsoftware offenbar die Fähigkeit besitzt, diese zu sammeln und zu stehlen (OS Credential Dumping). Ein schneller Passwortwechsel ist also unumgänglich.

Im Reiter Community finden sich Kommentare von Nutzern mit Hinweisen zur analysierten Datei. In manchen Fällen sind an diese Stelle auch bereits Reports von Sandboxes verlinkt. Eine solche automatisierte Analyse ist ein

Google Dorks

Wenn im Bereich Cybersecurity von Onlinerecherchen und OSINT die Rede ist, darf auch Google Dorking (oder Google Hacking) nicht fehlen: eine Google-Suche mit fortgeschrittenen Suchparametern. Damit können explizit spezifische Bereiche einer Webseite abgefragt werden und die Ergebnisse werden dementsprechend um einiges relevanter. Die folgende Liste zeigt einige der zahlreichen Anwendungsmöglichkeiten:

- intitle: sucht nach dem Suchbegriff im Titel einer Webseite.
- inurl: sucht nach dem Suchbegriff in der URL.
- intext: sucht nach dem Suchbegriff im Text der Seite.
- * ist ein Wildcard-Charakter.
- - schließt das folgende Suchwort aus.

Diese Technik nutzen auch Angreifer gern, um nach verwundbaren Seiten zu suchen. Im Netz sind zahlreiche Sammlungen von Security-relevanten Google Dorks verfügbar.

Twitter

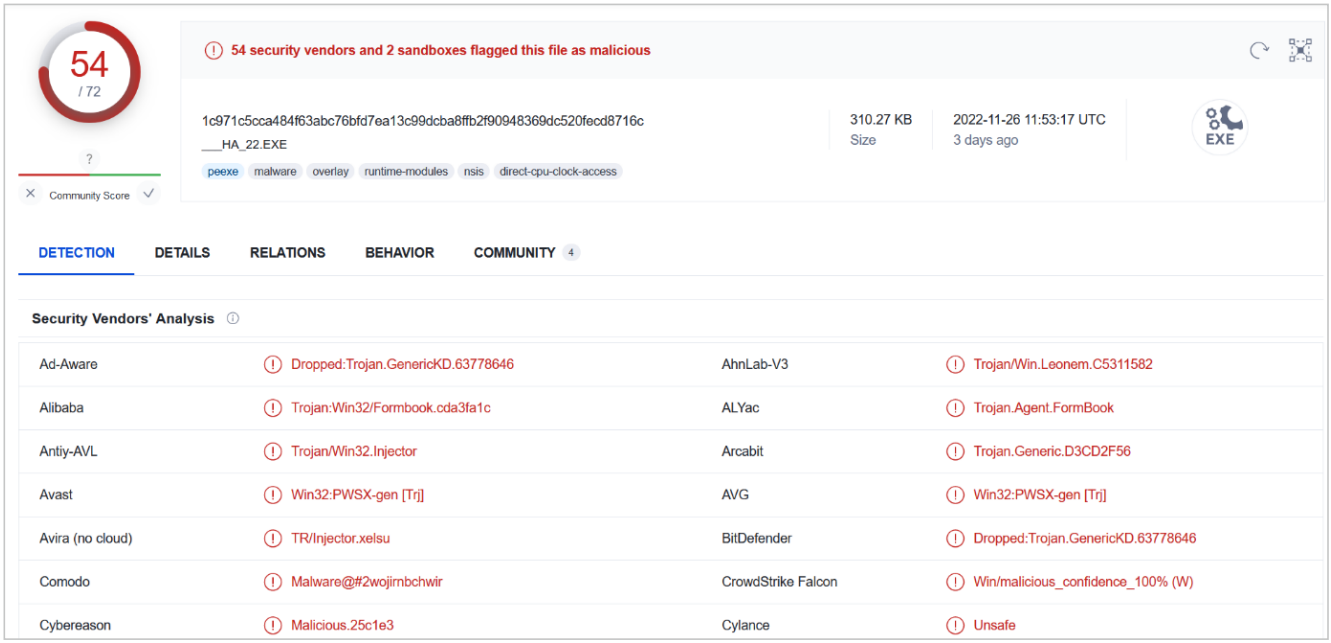
Auch Social Media eignet sich für Threat Intelligence. Vor allem auf Twitter teilen viele Securityforscher und Organisationen Schwachstellen mit der Community und liefern Hintergründe zu gängigen Angriffstaktiken. Einige interessante Twitter-Konten sind:

- SANS Internet Storm Center @sans_isc
- BleepingComputer @BleepinComputer
- The DFIR Report @TheDFIRReport
- Florian Roth @cyb3rops
- US-CERT @USCERT_gov

```
PS C:\Users\REM\Desktop> Get-FileHash -Algorithm SHA256 .\Form.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          1C971C5CCA484F63ABC76BFD7EA13C99DCBA8FFB2F90948369DC520FECD8716C       C:\Users\REM\Desktop\Form.exe
```

Ein kryptografischer Hash als eindeutiges Merkmal potenziell gefährlicher Dateien ist schnell erzeugt, hier unter Windows mit dem PowerShell-Befehl Get-FileHash (Abb. 1).



VirusTotal schlägt bei der Suche nach dem Hashwert von Form.exe Alarm. Bei 54 Scannern ist die Datei bekannt (Abb. 2).

nächster Schritt in der Malware-Analyse, wenn das Resultat nicht bereits bekannt ist.

Vielseitige Alternative aus der Schweiz

Eine Alternative oder Ergänzung zu VirusTotal ist abuse.ch mit seinen Unterprojekten. Auch hier lässt sich mit dem Hashwert oder anderen Artefakten wie IP-Adressen oder URLs die Reputation eines Samples überprüfen. Zusätzlich stellt abuse.ch mit dem MalwareBazaar eine Plattform zum Teilen von Malware-Samples bereit, sodass die Community, Hersteller von Antivirenlösungen, aber auch Anbieter von Threat-Intelligence-Diensten von aktuellen Samples profitieren können.

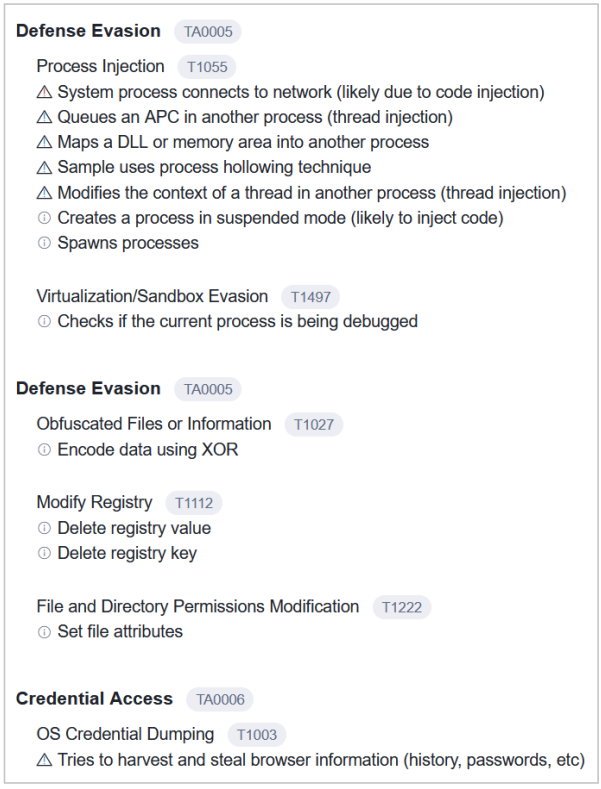
Der Feodo Tracker hingegen versucht Infrastrukturen von Command-and-Control-Servern (C2) im Zusammenhang mit verschiedenen Malware-Familien zu verfolgen. Zusammen mit dem URLhaus (Sammlung von Webservern, die Schadsoftware verteilen) und ThreatFox (Teilen von IoCs) bietet abuse.ch eine stets aktuelle Plattform, um sich schnell Informationen über ein vorhandenes Malware-Sample oder andere IoCs zu verschaffen.

Um die verschiedenen durch abuse.ch angebotenen Plattformen effizient zu nutzen, eignet sich das Tool AbuseLookup-GUI von Alexander Hübert. Damit lassen sich verschiedene Arten von IoCs wie IP-Adressen, Domains, URLs oder kryptografische Hashwerte auf den zuvor genannten Plattformen suchen und grundlegende Informationen anzeigen.

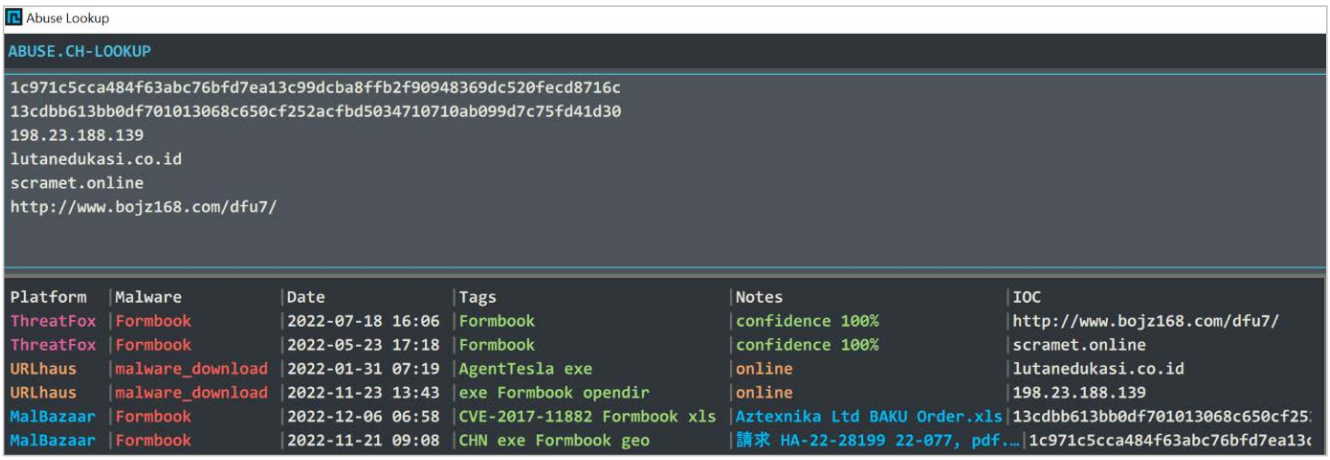
Im folgenden Beispiel hat der Analyst zusätzlich zum Hashwert bereits verdächtige Domains und IP-Adressen in Erfahrung gebracht. Eine schnelle Überprüfung dieser IoCs mit AbuseLookup-GUI (siehe Abbildung 4) zeigt, dass alle diese IoCs mit der Schadsoftware FormBook in Verbindung stehen. Die Wahrscheinlichkeit einer Kompromittierung mit FormBook ist also hoch, sodass weitere Maßnahmen, wie die Blockierung dieser IoCs, sinnvoll sind.

Über VirusTotal, abuse.ch oder andere Plattformen, aber auch über Google oder Twitter lassen sich oft grundlegende Informationen zu einer bestimmten Malware finden. Ist der Angriff jedoch etwas gezielter, kann es schnell vorkommen, dass die eingesetzte Malware der Öffentlichkeit oder den Malware-Spezialisten noch nicht bekannt ist und deshalb auf diesen Plattformen noch keine Informationen zu finden sind.

Eine solche Malware muss man genauer analysieren, um herauszufinden, wie sie funktioniert, wo sie sich einklinkt, wie sie sich auf einem System einnistet oder verbreitet und vieles mehr. Mithilfe einer ersten automatisierten Analyse der Malware lassen sich in der zweiten Stufe der Malware-Analyse in der Regel ohne großen Aufwand bereits einige grundlegende Informationen über die Malware ermitteln, wie die Malware-Familie oder



VirusTotal ordnet die Fähigkeiten der analysierten Datei den Techniken aus dem MITRE ATT&CK Framework zu (Abb. 3).



Das Programm AbuseLookup-GUI gestattet die Suche nach mehreren IoCs auf einmal und liefert auch Informationen aus den Tochterprojekten von abuse.ch zurück (Abb. 4).

die Art der Malware (Trojaner, Ransomware, Wurm et cetera). Je nachdem, wie und mit welchen Werkzeugen diese automatisierte Analyse durchgeführt wird, können diese Informationen mit beliebigen weiteren Informationen angereichert werden.

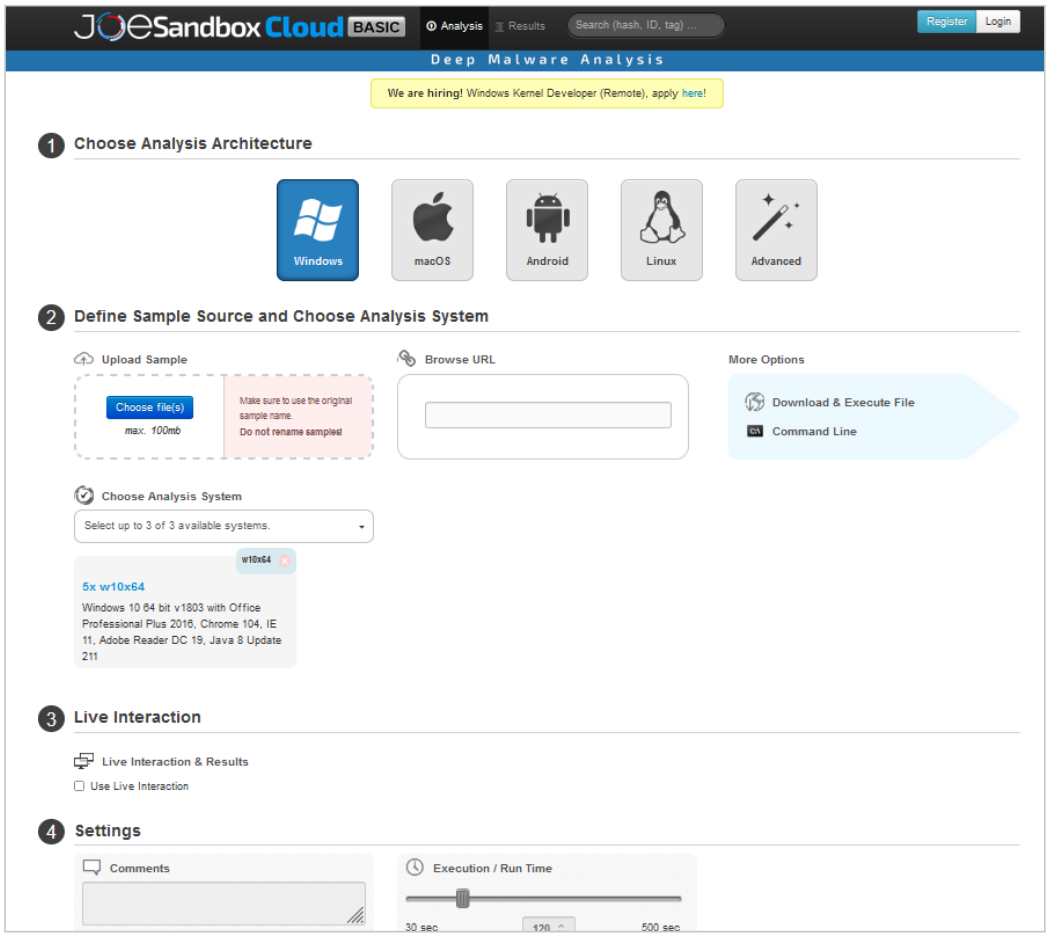
Sandboxes für die schnelle Analyse

Eine Möglichkeit der automatisierten Analyse einer Schadsoftware ist die Verwendung von Sandboxes. Eine Malware-Analyse-Sandbox ist ein speziell präpariertes System oder eine speziell präparierte Umgebung. Diese Umgebung kann dabei physisch sein, ist in der Regel jedoch eine virtuelle Maschine. Eine solche Sandbox simuliert die Umgebung eines möglichen Ziels der Schadsoftware. Die Schadsoftware wird also in einer solchen Sandbox zur Ausführung gebracht, um ihr Verhalten live zu beobachten. Um jedes Verhalten und jede Änderung am System zu registrieren, sei es die Erstellung oder Manipulation von Dateien, die Veränderung der Systemeinstellungen, das Aufrufen von Webseiten oder das Kontaktieren weiterer Systeme im Netzwerk oder im Internet, ist das Sandbox-System mit einer Vielzahl an Überwachungssystemen ausgerüstet. Sie dokumentieren alle Aktivitäten und Verbindungen auf dem System und analysieren sie.

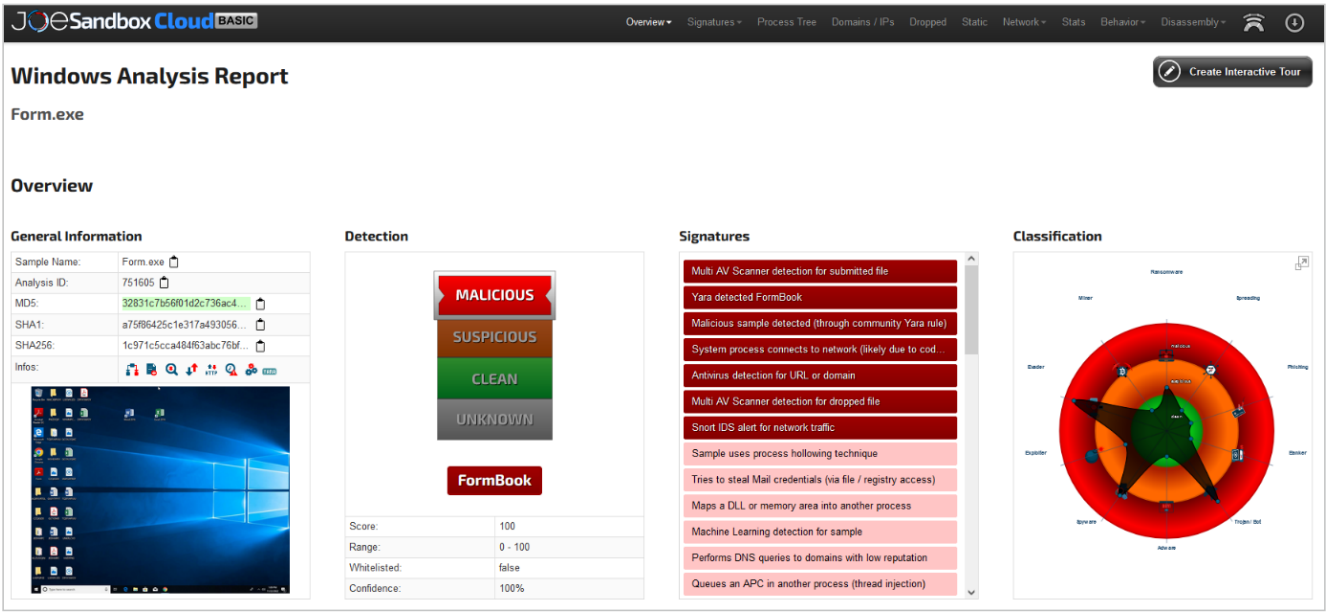
Wie bei den OSINT-Plattformen bietet auch die Welt der Sandboxes eine Vielzahl an verschiedenen Produkten und Diensten. Von kostenlos zu lizenzpflichtig, von Cloud-Diensten zu lokal installierbarer Software ist so gut wie für alle Anforderungen eine Möglichkeit dabei. Zu den bekannteren Sandboxes gehören JoeSandbox, Hybrid-Analysis oder die Cuckoo-Sandbox.

Was alle Produkte eint: Zum Schluss stellen sie eine mehr oder weniger detaillierte Auflistung an Aktivitäten, Indikatoren, Metadaten und Analyseresultaten zur Verfügung, manchmal sogar schon aufbereitet als PDF-Bericht. Die meisten Plattformen erlaube es auch, zusätzliche Daten für eine weitere und vertiefte Analyse, wie beispielsweise eine Aufzeichnung des Netzwerkverkehrs oder das Abbild des Arbeitsspeichers zum Zeitpunkt der Ausführung, zu extrahieren und herunterzuladen.

Um Möglichkeiten und Grenzen der Sandboxes zu zeigen, soll JoeSandbox die Datei Form.exe analysieren. Diese Sandbox erlaubt es, nach Erstellung eines entsprechenden Kontos die zu analysierende Schadsoftware über ein Webportal hochzuladen. Zusätzlich kann die Analyseumgebung bei JoeSandbox noch genauer definiert werden. So kann zum Beispiel das Betriebssystem, aber auch die Sprache, das Tastaturlayout oder das Netzwerk konfiguriert werden. Darüber hinaus lassen sich in der Regel noch ver-



JoeSandbox erlaubt weitreichende Konfigurationen der Umgebung, in der die Malware laufen soll (Abb. 5).



Nach der Analyse erzeugt JoeSandbox einen ausführlichen, grafisch aufbereiteten Bericht (Abb. 6).

schiedene Verfahren wie beispielsweise statische und dynamische Analyse auswählen (siehe Abbildung 5).

Nachdem das Sample hochgeladen wurde, führt JoeSandbox die Analyse durch und liefert nach deren Abschluss einen Bericht (siehe Abbildung 6). In der Übersicht unter den allgemeinen Informationen sind zuerst die Hashwerte zu finden. Unter Detection stellt JoeSandbox klar, dass es sich hierbei um die Malware FormBook handelt. Die Signaturen zeigen außerdem, was zu diesem Ergebnis geführt hat, insbesondere die Erkennungen von Antivirus- und YARA-Scans (mehr dazu in Teil 3) und die Fähigkeiten, die häufig mit Malware in Verbindung gebracht werden, wie das Process Hollowing, bei dem die Malware einen bestehenden Prozess mit ihrem schädlichen Code infiltriert (weitere Details in Teil 4). Dies ermöglicht es JoeSandbox auch, die Art der Malware zu bestimmen, hier vor allem Trojaner und Evader.

Umfangreiches Berichtswesen

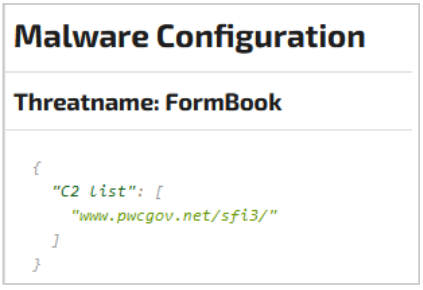
Zudem enthält der Bericht die MITRE-ATT&CK-Matrix mit den Taktiken und Techniken, die JoeSandbox für die Malware entdeckt hat. Dies ermöglicht ebenfalls eine schnelle Einschätzung ihrer Fähigkeiten. In diesem Fall kann sich die Malware insbesondere in Prozesse einschleusen, um ihre Privilegien zu erhöhen und die Erkennungstools zu umgehen. Sie kann auch Zugangsdaten dumpen und Daten vom lokalen System sowie E-Mails sammeln.

JoeSandbox versucht auch, Konfigurationsdaten der Malware auszulesen, im Beispiel die Domäne des C2-Servers (Command and Control), über den die Angreifer mit der Schadsoftware kommunizieren (siehe Abbildung 7).

Eine Verhaltensgrafik zeigt die Aktivitäten der Malware während der Laufzeit sehr anschaulich (siehe Abbildung 8). JoeSandbox kennzeichnet die als bösartig erkannten Elemente mit einem roten Symbol. Weitere Details zu den Aktivitäten, die von jedem Prozess ausgeführt werden, einschließlich der Interaktion mit Dateien und der Registry, werden im Bereich Behavior aufgeführt.

Malware unter Aufsicht

In Abbildung 8 sieht man, dass Form.exe zwei temporäre Dateien ablegt und einen weiteren Prozess aziztwhel.exe startet, bis er sich in explorer.exe injiziert. Dieser Prozess kontaktiert dann mehrere Domänen, darunter auch die in der Konfiguration gefundene, um unter anderem



JoeSandbox ermittelt auch Konfigurationsdaten wie hier die Domäne des C2-Servers (Abb. 7).

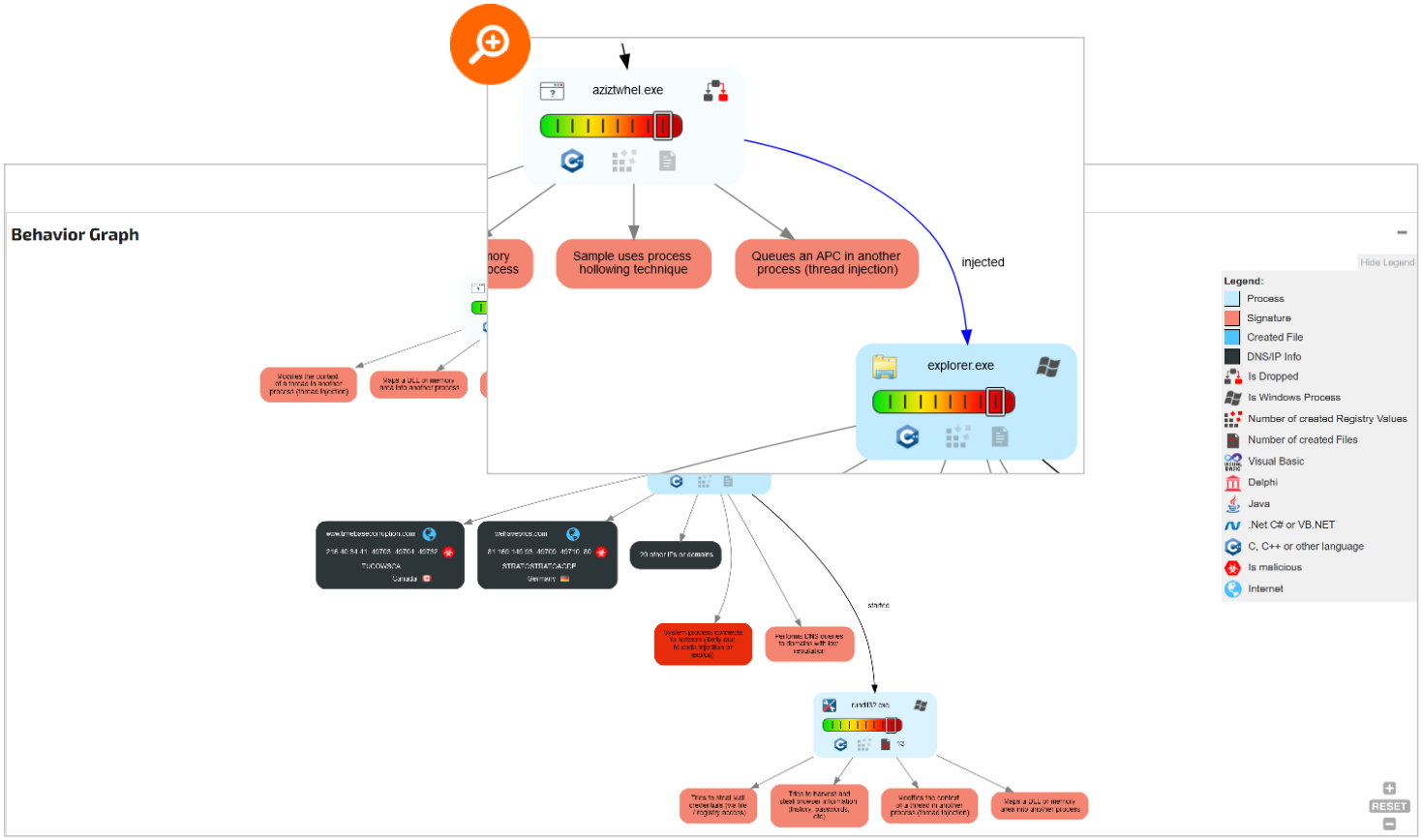
E-Mail-Zugangsdaten und Browserinformationen zu stehlen. Die Liste aller kontaktierten Domänen und URLs findet sich im weiteren Verlauf des Berichts unter „Domains and IPs“ aufgelistet, die Details über den Netzwerkverkehr unter Network, statische und für das Reverse Engineering wichtige Funktionen unter Static sowie Disassembly.

Damit liefert JoeSandbox bereits sehr wertvolle Informationen. Sie korrelieren auch mit den zuvor mithilfe von VirusTotal gefundenen Erkenntnissen. Dies schafft bereits zusätzliches Vertrauen in die gewonnenen Resultate. Es ist jedoch empfehlenswert, den Analyseprozess mit der Analyse der statischen Eigenschaften und einer dynamischen Analyse fortzusetzen, um die von JoeSandbox erhaltenen Resultate zu überprüfen und eventuell zu ergänzen. Dies wird in den folgenden Teilen dieser Artikelreihe behandelt.

Die Möglichkeiten der Onlinerecherche und die öffentlich zugänglichen Werkzeuge sind auf den ersten Blick sehr hilfreich. Es genügt, eine Abfrage zu tätigen oder eine Datei hochzuladen, und schon erhält man einen Schatz an wertvollen Informationen zurück. So verlockend diese Onlineanbieter auch sein mögen, sollte man ein paar Dinge zum Thema Sicherheit beachten.

Angreifer liest mit

In solchen Zusammenhängen fällt oft der Begriff Operations Security (OPSEC), der seinen Ursprung im militärischen Umfeld hat. Er beschreibt den Prozess, wich-



Ein Ausschnitt aus der Verhaltensgrafik zeigt, wie Form.exe neue Prozesse startet und sich in explorer.exe injiziert (Abb. 8).

tige Informationen zu identifizieren und diese einem potenziellen Gegner vorzuenthalten, um ihn über eigene Fähigkeiten und Absichten im Dunkeln zu lassen. Da es sich bei den in diesem Artikel genannten Anbietern grundsätzlich um kostenfreie, öffentlich zugängliche Lösungen handelt, sind auch die geteilten Informationen bei zukünftigen Aufrufen der Webseite öffentlich zugänglich. Somit ist darauf zu achten, dass keine sensiblen Daten hochgeladen werden. Bei Dateien lässt sich dies relativ einfach umgehen, wenn man anstelle der Datei immer ihren Hashwert benutzt.

Ein weiterer Punkt: Die Analysetools sind selbstverständlich auch den Angreifern bekannt. Das Abgleichen einer potenziell infizierten Datei kann ihnen zeigen, dass ihre Schadsoftware entdeckt wurde. So könnten sie ihre Spuren vertuschen oder auf einen neuen Angriffsvektor ausweichen. In manchen Fällen kann es auch von Vorteil sein, den Angreifer in Sicherheit zu wiegen, indem beispielsweise die Chatkonversation zur Verhandlung des Lösegelds am Laufen gehalten wird, um die Zeit zu nutzen, das Verhalten des Angreifers genauer zu analysieren und daraus detaillierte Erkenntnisse zum Angriff zu erlangen.

Fazit

Eine Vielzahl an Malware-Analysemöglichkeiten ist online verfügbar. Das Internet hält eine Menge an Datenquellen bereit, die sich zur Informationsgewinnung verwenden lassen. Mit OSINT-Techniken können explizit IoCs abgefragt und Hintergrundinformationen zu Tätergruppen und Malware-Familien gesammelt werden. Eine breite Community fördert den Austausch über Sicherheitsrisiken, aktuelle Angriffstaktiken und Analyseansätze. Auch soziale Medien werden gerne verwendet, um Threat Intelligence zu betreiben.

Diverse Onlinetools liefern erste Einschätzungen, ob es sich um eine bösartige Datei handelt, und erfordern kein tieferes Wissen. Selbstverständlich müssen Analysten das automatisch generierte Ergebnis verstehen, um die richtigen Schlüsse ziehen zu können.

Auch wenn das Internet eine große Hilfe darstellen kann, sollte man sich im Voraus Gedanken machen, was das Ziel der Analyse ist und wie viel man bereit ist über sich preiszugeben. Bei jeder getätigten Abfrage hinterlässt der Analyst Informationen auf der besagten Webseite. Das ist oft hilfreich für die Community, aber auch Angreifer können dann feststellen, dass ihre Schadsoftware entdeckt wurde, und ihr Verhalten ändern. (ulw@ix.de)

Quellen

[1] Nadia Meichtry, Fabian Murer, Tabea Nordieker; Einstieg in die Malware-Analyse; iX 2/2023, S. 98

[2] Links zu den erwähnten Projekten, Websites und Werkzeugen: ix.de/zsu5

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.