Velociraptor großflächig einsetzen

Bei einem Ransomwareangriff ist typischerweise nicht nur ein einzelnes System betroffen, sondern Hunderte oder sogar Tausende. Hier kann das Werkzeug Velociraptor bei einer großflächigen Triage und Analyse helfen.

Von Melanie Kubli und Nadia Meichtry

Für die Untersuchung eines einzelnen Systems gibt es verschiedene Werkzeuge, um schnell und effizient relevante Informationen zu sichern. Man stelle sich jedoch vor, man kommt an einem Montagmorgen ins Büro, schaltet seinen Laptop ein und es erscheint eine Meldung wie in Abbildung 1. Und sie erscheint nicht nur auf einem System, sondern auf allen Geräten der Mitarbeitenden und diversen Servern. Um die Frage zu beantworten, was genau passiert ist, muss man eine forensische Analyse durchführen. Doch wie lassen sich die Daten von dieser großen Anzahl von Systemen sammeln und untersuchen? Genau an dieser Stelle kommt Velociraptor ins Spiel.

Velociraptor ist ein forensisches Werkzeug zur Visualisierung und Datensammlung von verschiedenen Endpunkten. Die Informationen werden mithilfe einer eigenen Abfragesprache erfasst, der Velociraptor Query Language (VQL). Diese Abfragesprache ist in allen Artefakten enthalten und wird zum Sammeln und Überwachen von Daten auf den Clients verwendet. Velociraptor hat eine große Liste solcher vorinstallierter Artefakte, die auch angepasst werden können. Der Begriff „Artefakt“ aus Sicht von Velociraptor ist jedoch nicht gleichbedeutend mit einem Artefakt aus Sicht der Forensik. In der digitalen Forensik ist ein Artefakt ein beobachtbares Objekt, das durch menschliche oder automatische Aktivitäten auf einem Computer entsteht. Zum Beispiel die Windows-Ereignisprotokolle.

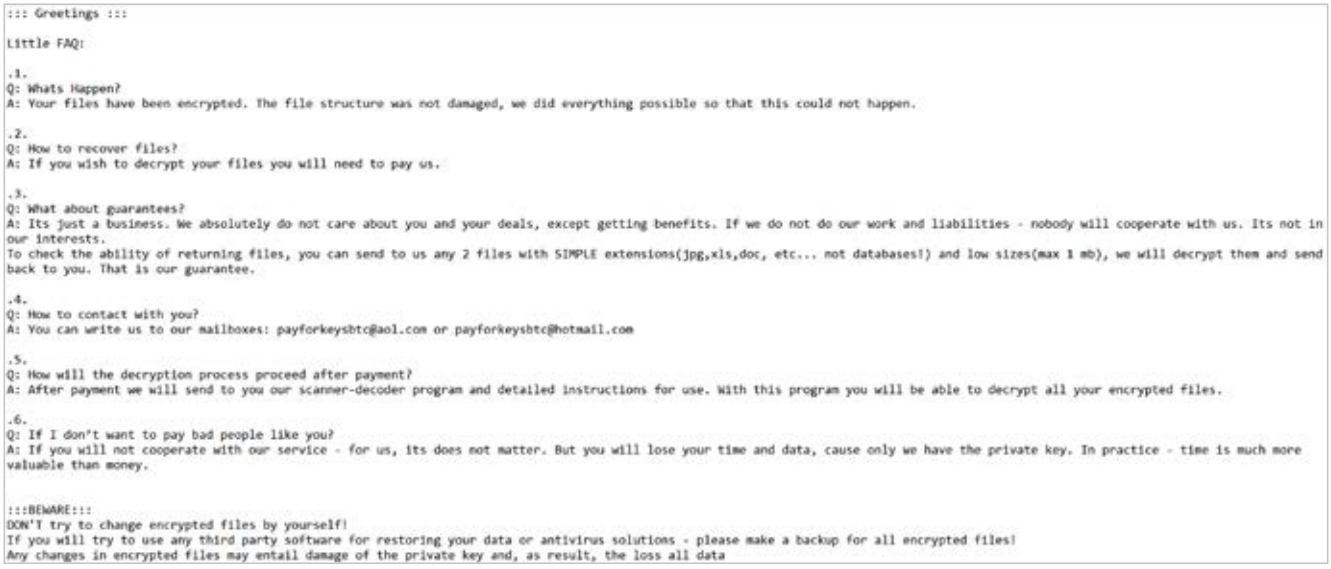
Mit Velociraptor lassen sich viele Systeme gleichzeitig und parallel durchsuchen, um Artefakte zu sammeln. Das bedeutet nicht nur eine erhebliche Zeitersparnis, sondern schafft auch Visibilität und damit einen Überblick über alle Systeme. Dadurch lassen sich infizierte Systeme schneller aufspüren und anschließend eingehender analysieren, was die Arbeit der Analysten erleichtert [1].

iX-TRACT

- Velociraptor untersucht eine große Anzahl von Systemen parallel und gleichzeitig effizient auf Spuren eines Angriffs; so wird Visibilität geschaffen. Ebenfalls ist ein Echtzeitmonitoring möglich.
- Mit Velociraptor kann man eine Triage durchführen und damit die Daten für die weitere Analyse sichern. Dies spart gerade bei mehreren Systemen einiges an Zeit.
- Bei Hunderten oder sogar Tausenden von Systemen ist es nicht effizient und sinnvoll, eine komplette Triage auf allen Systemen durchzuführen. Mit Velociraptor kann man gezielt nach bestimmten Artefakten und Indicators of Compromise suchen.

Ein individuell anpassbares Werkzeug

Darüber hinaus gibt es eine Vielzahl typischer Artefakte, auch aus der Community.



```
::: Greetings :::

Little FAQ:

.1.
Q: Whats Happen?
A: Your files have been encrypted. The file structure was not damaged, we did everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay us.

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in
our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt them and send
back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailboxes: payforkeysbtc@aol.com or payforkeysbtc@hotmail.com

.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.

.6.
Q: If I don't want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause only we have the private key. In practice - time is much more
valuable than money.


:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data
```

Die Nachricht, die niemand auf dem eigenen Bildschirm lesen will: „Ihre Daten wurden verschlüsselt!“ (Abb. 1).

Es können auch eigene Abfragen, Artefakte et cetera erstellt oder bestehende an die eigenen Bedürfnisse angepasst werden. Mit dem Artefakt `Windows.System.PowerShell` kann beliebiger Code auf dem System ausgeführt werden. Dabei könnte man beispielsweise einen festen Befehl hinzufügen, der nach offenen RDP-Sitzungen sucht. Das Artefakt wird dann als `Custom.Windows.System.PowerShell` bezeichnet und kann über „Select Artefact“ ausgewählt werden.

Das sind aber nicht die einzigen Vorteile von Velociraptor. Neben der Datensammlung kann man die Systeme aktiv nach IOCs (Indicators of Compromise) durchsuchen, und zwar mit sogenannten Hunts (Jagden), die auf vorkonfigurierten Artefakten basieren; sie werden weiter unten erläutert. Des Weiteren erlaubt Velociraptor, die Ergebnisse der Hunts unter anderem über Notebooks gemeinsam zu bearbeiten und zu dokumentieren, was bei einer forensischen Analyse besonders wichtig ist.

Hunts werden nur einmal auf den Systemen ausgeführt. Um bestimmte Artefakte wie Protokolle kontinuierlich zu sammeln oder die Systeme gezielt und in Echtzeit mit bestimmten Abfragen auf Auffälligkeiten zu überwachen, bietet sich die Monitoringfunktion von Velociraptor an. Sitzt der Angreifer noch in der Umgebung und führt böswillige Aktivitäten aus, können diese zeitnah erkannt werden. Velociraptor kann auch Alarme auslösen (siehe ix.de/zj89). Dadurch werden Analysten sofort informiert und können schnellstmöglich reagieren. Alle Überwachungsergebnisse werden auf dem Velociraptor-Server gespeichert, sodass sie sich für historische Überprüfungen durchsuchen lassen. Beispielsweise kann man das Ausführen von Prozessen überwachen. Wird eine bestimmte Datei ausgeführt, wird man sofort benachrichtigt und kann nachforschen, ob dieser Prozess bereits zuvor auf dem infizierten Computer ausgeführt wurde. Außerdem kann der Analyst alle verbundenen Clients auf weitere Kompromittierungen durchsuchen.

Da Velociraptor mit den höchsten Privilegien auf den Systemen installiert wird, kann er Schutz- oder Behebungsmaßnahmen einleiten, zum Beispiel die Isolation (Quarantäne) von Systemen oder das Entfernen von Persistenzmechanismen, mit denen sich ein Angreifer auf dem System festgesetzt hat. Er ist daher in allen Phasen der Incident Response von großem Nutzen. Seine Stärke ist gleichzeitig aber auch seine Schwäche: Velociraptor läuft eben mit höchsten Privilegien. Wenn ein Angreifer Zugang zum Velociraptor-Server erlangt, kann er alle angebundenen Rechner kompromittieren. Außerdem besteht die Gefahr, dass aufgrund der erhöhten Rechte unerwünschte Änderungen vorgenommen werden. Es ist daher Vorsicht geboten, wenn man Suchabfragen mit Velociraptor startet.

Triage mehrerer Systeme

In zeitkritischen Momenten wie bei Cybervorfällen kann eine Triage im Vergleich zu einer klassischen, umfassenden forensischen Analyse massiv Zeit sparen. Dies ist insbesondere bei Ransomwarevorfällen wichtig.

Wie im vorhergehenden Artikel beschrieben, ist die Triage bei einer Handvoll Systemen sinnvoll und einfach. Ein Triage-Werkzeug ist KAPE [2], mit dem man Daten auf dem System sammeln und aufbereiten kann. KAPE lässt sich analog zum Einsatz in Einzelsystemen mit Velociraptor flächendeckend nutzen. Über den

Das Werkzeug Hayabusa

Hayabusa ist ein Werkzeug zum Erkennen verdächtiger Aktivitäten in den Ereignisprotokollen von Windows. Dazu verwendet es unter anderem öffentlich verfügbare Sigma-Regeln, anhand derer sich Anomalien erkennen lassen. Das Werkzeug kann für ein proaktives Threat Hunting oder für Einsätze digitaler Forensik und Incident Response verwendet werden. Ein positiver Nebeneffekt von Hayabusa ist, dass es nützliche Informationen aus den Windows-Ereignisprotokollen extrahiert und in einem lesefreundlichen Format ausgibt.

Die gefundenen Events werden in die Kategorien Critical, High, Medium, Low und Informational eingeteilt. Dies erlaubt es, sich zuerst auf die kritischen Events zu konzentrieren. Durch das Betrachten der Ereignisse gewinnt man eine erste Vorstellung davon, was während des Angriffs passiert sein könnte. Zudem gibt es Anhaltspunkte dafür, wonach man suchen oder was man weiter überprüfen sollte. Ein ähnliches Werkzeug zum Aufdecken von Angriffstechniken ist das von WithSecure veröffentlichte Chainsaw [3].

Exchange.Windows.EventLogs.Hayabusa/Results

Timestamp	RuleTitle	Level	Computer	Details
2022-11-02 15:07:45.480 +00:00	PW Guessing	med	-	[condition] count() by IpAddress >= 5 in timeframe [result] count:23 IpAddress:192.168.56.200 timeframe:5m
2022-11-02 15:09:10.430 +00:00	Unusual File Download from Direct IP Address	high	win10.windomain.local	Path: C:\Users\HAL_CONNER\Downloads\file.exe:Zone.Identifier ¦ Proc: C:\Program Files\Google\Chrome\Application\chrome.exe ¦ PID: 2224 ¦ PGUID: 344AF5AD-8814-6362-FB08-000000001700 ¦ Hash: SHA1=DC99C95D1031DACDA71E9E3EF9CC26DD3106CBA7,MD5=D0FD60E91E00B5444AC8CFA72439D6C1,SHA256=0BC920BC9BC90DA9B68B59778522CDB15B8C02AC41FF70D371438FFA4CAED729,IMPHASH=00000000000000000000000000000000
2022-11-02 15:31:50.594 +00:00	CurrentVersion Autorun Keys Modification	med	win10.windomain.local	EventType: SetValue ¦ TgtObj: HKU\S-1-5-21-1195756633-318299051-153033282-2629\Software\Microsoft\Windows\CurrentVersion\Run\Updater ¦ C:\ProgramData\updater.exe /q /n ¦ Proc: C:\Windows\system32\dllhost.exe ¦ PID: 10616 ¦ PGUID: 344AF5AD-8D66-6362-3209-000000001700

Die verdächtigen Hayabusa-Funde sollten weiter untersucht werden (Abb. 2).

Hunt-Manager kann man eine neue Jagd mit dem Artefakt `Windows.KapeFiles.Targets` starten. Mit diesem Artefakt werden die relevanten Daten auf den Clients gesammelt. Auf Linux- oder macOS-Rechnern sammelt Velociraptor die wichtigsten Artefakte mit dem Artefakt `Exchange.Generic.Collection.UAC`. UAC ist ein Skript (siehe ix.de/zj89) zum Sammeln von Artefakten und weiteren Informationen auf Unix-basierten Systemen. Neben der Sicherung ganzer Datenpakete sammelt Velociraptor auch gezielt einzelne Artefakte. Ein Beispiel dafür ist das Sichern der Windows-Ereignisprotokolle.

Eine Herausforderung bei der Triage ist, dass man genügend Speicherplatz braucht, um die gesammelten Daten zu speichern, und dass sie anschließend offline verarbeitet und ausgewertet werden müssen. Bei einem Großvorfall mit Hunderten oder Tausenden betroffenen Systemen ist eine Triage aller Systeme nicht praktikabel wegen des Zeitaufwands, da die Analyse Monate dauern würde, und des Speicherplatzes, da der Velociraptor-Server schnell volllaufen könnte. Es ist auch nicht zielführend, alle Systeme zu sichten, da sich darunter Systeme befinden, die bei einem Ransomwareangriff nur mitverschlüsselt wurden, aber keine besonders wichtigen Informationen zur Rekonstruktion des Angriffs liefern – und somit nur wertvolle Zeit verloren geht.

Flächendeckende Analyse mit Velociraptor

Im vorgestellten Szenario, das auf einem realen Beispiel beruht, sind praktisch alle Systeme des Unternehmens verschlüsselt worden und sollen nun untersucht werden. Um diese Herausforderung zu meistern, kann der Velociraptor diverse Jagden starten, die nach einem bestimmten Artefakt oder IOC suchen, und die Resultate gleich aufbereiten sowie gewisse Artefakte überwachen. Man kann direkt in der Weboberfläche die Ergebnisse durchgehen und auf Auffälligkeiten prüfen. Die mit Hunts gewonnenen Daten werden direkt auf den Endpunkten verarbeitet und analysiert, das löst das Speicherplatzproblem bei der Triage.

Wie erwähnt ist es bei dieser großen Anzahl von Systemen nicht möglich, die mit der Triage gesammelten Daten effizient zu sichten. Auch hier kann Velociraptor einen entscheidenden Vorteil bei der Klärung des Falles bieten, indem man gezielt nach Artefakten sucht und diese direkt in der Weboberfläche anzeigen lässt. Doch wo soll die Suche starten?

Bei den meisten Ransomwarevorfällen gibt es von Anfang an mehrere Ansatzpunkte für eine Analyse. Dazu gehören in unserem Szenario die Lösegeldforderung oder die Erweiterung der verschlüsselten Dateien (in diesem Fall .makop), die Informationen über die Angreifergruppe liefert. Damit kann man nach bekannten Artefakten/IOCs suchen, die damit in Verbindung stehen. Die Analyse kann auch auf Basis der bereits bekannten betroffenen Systeme oder Benutzer gestartet werden. Eine weitere Möglichkeit ist der Einsatz von Hayabusa (siehe Kasten „Das Werkzeug Hayabusa“), um damit nach Anomalien in der Windows-Umgebung zu suchen. Beim Ausführen des Artefakts `Exchange.Windows.EventLogs.`

2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:45Z	win10.windomain.local	WINDOMAIN	HAL_CONNER	3	192.168.56.200	LOGON_SUCCESSFUL
2022-11-02T15:07:45Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:46Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED
2022-11-02T15:07:46Z	win10.windomain.local		HAL_CONNER	3	192.168.56.200	LOGON_FAILED

Ausgabe des RDPAuth-Artefakts, das Erfolg oder Misserfolg bei RDP-Anmeldungen anzeigt (Abb. 3)

2022-11-02T15:08:21Z	win10.windomain.local	WINDOMAIN	HAL_CONNER	10	192.168.56.200	RDP_LOGON_SUCCESSFUL_NEW
2022-11-02T15:08:26Z	win10.windomain.local	WINDOMAIN	HAL_CONNER		192.168.56.200	RDP_REMOTE_RECONNECTION
2022-11-02T15:10:52Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL
2022-11-02T15:10:52Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL
2022-11-02T15:10:54Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL
2022-11-02T15:10:54Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL
2022-11-02T15:10:54Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL
2022-11-02T15:10:55Z	dc.windomain.local	WINDOMAIN.LOCAL	HAL_CONNER	3	192.168.56.104	LOGON_SUCCESSFUL

Laterale Verbindung auf den Domänencontroller: Diese verdächtige Aktivität sollte weiter untersucht werden (Abb. 4).

Windows.Analysis.EvidenceOfExecution/UserAssist

Name	User	LastExecution	NumberOfExecutions	Fqdn
C:\Users\HAL_CONNER\Downloads\file.exe	HAL_CONNER	2022-11-02T15:09:47Z	1	win10.windomain.local

Die Ausgabe des UserAssist-Artefakts belegt, dass die Datei file.exe ausgeführt wurde (Abb. 5).

Windows.Sysinternals.Autoruns

Time	Entry Location	Entry	Enabled	Category	Profile	Image Path	Launch String	Fqdn
20221026-114957	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Updater	enabled	Logon	WINDOMAIN\HAL_CONNER	c:\programdata\updater.exe	C:\ProgramData\updater.exe /q /n	win10.windomain.local
20221026-114957	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Updater	enabled	Logon	WINDOMAIN\MILLIE_CHARLES	c:\programdata\updater.exe	C:\ProgramData\updater.exe /q /n	dc.windomain.local

Die Ausgabe des Autoruns-Artefakts mit der Datei updater.exe liefert Indizien, die auf einen persistenten Zugriff hindeuten (Abb. 6).

`Hayabusa` läuft Hayabusa auf den jeweiligen Systemen. Hier lohnt es sich, die Ausgabe von Velociraptor zu betrachten, um erste schnelle Ergebnisse zu erhalten, die man weiterverfolgen und in die weitere Analyse einbeziehen kann.

Das Überprüfen der Hayabusa-Resultate offenbart ein Erraten des Passworts ausgehend von der IP-Adresse 192.168.56.200 (Abbildung 2). Dies könnte ein Hinweis auf einen möglichen Einstiegspunkt sein. Gefunden wurden ebenfalls der Download der Datei file.exe und eine Änderung in den Autostarts (Autoruns). Das muss man weiterverfolgen und auf Legitimität prüfen.

Zum Verfolgen des Password Guessing kann man die Windows-Ereignisprotokolle einsehen. Das Artefakt `Windows.EventLogs.RDPAuth` sammelt Windows-Ereignisprotokolle im Zusammenhang mit Remote-Desktop-Sitzungen sowie erfolgreichen oder fehlgeschlagenen An- und Abmeldungen. Velociraptor bereitet die Ereignisprotokolle auf und zeigt sie direkt in der Weboberfläche an, reduziert auf die relevanten Daten. Abbildung 3 zeigt, dass innerhalb eines kurzen Zeitraums ausgehend von der IP-Adresse 192.168.56.200 mehrere fehlgeschlagene Anmeldeversuche stattfanden. Es gibt auch einen erfolgreichen Anmeldeversuch, was darauf hinweisen könnte, dass das Passwort erraten wurde. Eine Möglichkeit ist ein Brute-Force-Angriff.

Lateral Movement: sich ausbreiten im Netz

Das Remote Desktop Protocol (RDP) wird auch für laterale Bewegungen (Lateral Movement) im Netzwerk verwendet. Es lohnt sich, dieses Artefakt ebenfalls auf eine mögliche Verbreitung zu überprüfen. Lateral Movement umfasst Techniken, mit denen Angreifer tiefer in ein Netzwerk eindringen und nach sensiblen Daten oder anderen wertvollen Ressourcen suchen, zum Beispiel nach einem Domänencontroller (DC), auf dem wertvolle Informationen wie Authentifizierungsdaten gespeichert sind [4]. Abbildung 4 zeigt, dass sich das System Win10 mit der IP-Adresse 192.168.56.104 erfolgreich mit dem Benutzer HAL_CONNER am DC anmelden konnte. Das könnte ein Hinweis auf eine laterale Bewegung sein und sollte auf Legitimität geprüft werden.

Neben den Artefakten, die nur Daten aus einer Quelle sammeln, gibt es diejenigen, die zu einem Sammelartefakt zusammengefasst wurden und daher mehrere Datenquellen nutzen. Ein Beispiel hierfür ist `Windows.Analysis.EvidenceOfExecution`. Es sammelt die Daten von UserAssist, Amcache, Shimcache und Prefetch. Damit lässt sich überprüfen, ob die Datei file.exe auf dem System ausgeführt wurde. Dieses Artefakt liefert auch Informationen darüber, ob andere verdächtige Programme zum Zeitpunkt des Angriffs ausgeführt wurden.

Angreifer verwenden Schadsoftware unter anderem, um ihre Privilegien zu erhöhen, Sicherheitssysteme zu umgehen oder Systeme zu verschlüsseln. Abbildung 5 zeigt die Ausgabe des UserAssist-Artefakts und beweist, dass die Datei file.exe einmal ausgeführt wurde. UserAssist zeichnet Metadaten wie den Pfad der Anwendung, das Datum der letzten Ausführung und die Anzahl der Ausführungen über die GUI-basierte Programmausführung auf.

Wie bereits bei Hayabusa gesehen, kann Velociraptor zusätzliche Programme auf den Systemen ausführen und die Ergebnisse in der Weboberfläche anzeigen. Dies geschieht auch mit dem Artefakt `Windows.Sysinternals.Autoruns`, das zum Auffinden von Persistenzmechanismen dienen kann. Autoruns ist ein Hilfsprogramm von Microsoft zur Anzeige der aktuellen Autostart-Anwendungen und -Konfigurationen. Eine Änderung der Autostarts war bereits in den Hayabusa-Ergebnissen sichtbar.

Abbildung 6 zeigt die Ergebnisse von Autoruns. Die Datei updater.exe wird jedes Mal ausgeführt, wenn sich ein Benutzer anmeldet. Das kann darauf hindeuten, dass der Angreifer eine Persistenz eingerichtet hat, die auch nach einem Neustart permanenten Zugriff auf das System gewährt. Das kann der Schadsoftware-Beacon sein, das heißt das Programm, das für die Kommunikation mit dem C2-Server (Command and Control) zuständig ist. Auf diese Weise meldet sich der infizierte Rechner regelmäßig beim C2-Server, um Befehle zu empfangen und Informationen zu senden. Diese müsste man zur weiteren Analyse sammeln, um genau zu überprüfen, was die Datei macht. Dies wird in einem späteren Abschnitt behandelt.

Die gezeigten Artefakte sind nur ein Bruchteil der Daten, die mit Velociraptor erfasst und verarbeitet werden können. Es ist möglich, Velociraptor zu nutzen, um externe Tools wie Hayabusa oder Autoruns auf den Systemen laufen zu lassen und ihre Ergebnisse anzuzeigen. Es stehen auch Artefakte zur Verfügung (zum Beispiel RDPAuth), mit denen spezifische Informationen aus einer Datenquelle angezeigt werden können. Damit

Zu überprüfende Pfade lassen sich im FileFinder-Artefakt konfigurieren (Abb. 7).

lässt sich ein großer Datensatz effizienter reduzieren und überprüfen. Schließlich kann eine Reihe von spannenden Artefakten mithilfe eines Sammelartefakts zusammengefasst und gemeinsam gesammelt werden.

Suche nach gezielten IOCs

Die vergangenen Abschnitte haben die Möglichkeiten von Velociraptor zur Triage und flächendeckenden Analyse vorgestellt. Darüber hinaus kann das Werkzeug bei einem Ransomwareangriff auch bei der Suche nach IOCs unterstützen und helfen, kompromittierte Systeme zu identifizieren.

Im Laufe einer Untersuchung identifizieren Analysten verschiedene IOCs. Gerade wenn die Ransomwaregruppe bekannt ist, lohnt es sich, vorhandene Ressourcen zu dieser Ransomware zu recherchieren. Wie erwähnt lässt sich die Ransomwaregruppe oft an der Erweiterung der verschlüsselten Dateien oder an der Lösegeldforderung erkennen. Eine Möglichkeit, an Informationen zu kommen, bietet die Seite Malpedia des Fraunhofer FKIE [5] (siehe ix.de/zj89). Die in den Ressourcen gefundenen IOCs können für gezielte Suchabfragen über Velociraptor genutzt werden.

Im vorgestellten Szenario hat die Recherche zur Ransomware gezeigt, dass die Angreifergruppe häufig Cobalt Strike als Command and Control (C2) verwendet [6]. Cobalt Strike ist eine kommerzielle Software zur Simulation von Angriffen. Sie wird in erster Linie von Red Teams oder Sicherheitsingenieuren eingesetzt, um die Verteidigung der Infrastruktur eines Unternehmens zu testen. Bedrohungsakteure verwenden Cobalt Strike jedoch auch häufig, um eine C2-Kommunikation aufzubauen. Diese Informationen lassen sich gezielt für die IOC-Suche mit Velociraptor nutzen. Das Artefakt `Windows.Carving.Cobalt Strike` dient zur Suche nach Beacons auf den Clients. Seine Ergebnisse zeigen, dass ein Cobalt-Strike-Beacon auf dem Win10-System und auf dem DC gefunden wurde und dass der Angreifer möglicherweise damit Befehle auf dem jeweiligen System ausgeführt hat.

Die Dateien file.exe und updater.exe wurden in der Untersuchung aus dem vorherigen Abschnitt identifiziert. Das Artefakt `Windows.Search.FileFinder` sammelt sie für die weitere Analyse und ermittelt die Systeme, auf denen diese Dateien noch vorhanden sind. Bei der Konfiguration der Parameter können Pfade angegeben werden, die geprüft werden sollen (siehe auch Abbildung 7). Dabei ist es möglich, Platzhalter (*) zu verwenden. Die gefundenen Dateien kann man auch mit Upload_File auf den Server hochladen oder die Hashwerte der gefundenen Dateien direkt mit Velociraptor berechnen.

In Abbildung 8 ist die Ausgabe des FileFinder-Artefakts zu sehen: Die Datei updater.exe ist auf dem DC sowie auf dem Win10-System vorhanden.

Bekannte Bedrohungen überprüfen

Zusätzlich zu Dateinamen sind Hashwerte in der Securitywelt häufig geteilte IOCs. Zu diesem Zweck kennt Velociraptor das Artefakt `Generic.Detection.HashHunter`, das den angegebenen Dateipfad mit den mitgegebenen MD5-, SHA1- und SHA256-Hashwerten vergleicht und im Falle einer Übereinstimmung die passende Datei zurückgibt. Es ist jedoch ratsam, die Suche wenn möglich mit dem Hashwert einer Datei zu beginnen, da sich Dateinamen selbst innerhalb derselben Ransomwaregruppe unterscheiden können, was die Suche erschwert.

Besonders wenn die Ransomware schon länger im Umlauf ist, gibt es oft bereits YARA-Regeln (siehe Kasten „YARA und Sigma“), mit denen sie auf den Systemen identifiziert werden kann. YARA kann auch mit Velociraptor verwendet werden. Wie das Zusammenspiel funktioniert, zeigt ein Artikel (siehe ix.de/zj89). Mit dem Artefakt `Windows.Detection.`

Die Ausgabe des FileFinder-Artefakts offenbart das Vorhandensein der Datei updater.exe (Abb. 8).

YARA und Sigma

YARA ist ein Open-Source-Framework [7]. Es durchsucht Dateien oder den Speicher von Prozessen nach übereinstimmenden Mustern anhand von YARA-Regeln.

Sigma ist ähnlich wie YARA ebenfalls ein Werkzeug zum Austausch von Erkennungsdaten. Im Vergleich zu YARA sind Sigma-Regeln jedoch mehr auf den Einsatz in SIEM-Systemen (Security Information and Event Management) ausgerichtet. Dabei ist Sigma ein generisches Format zur Beschreibung von Angriffen, die in Protokollen entdeckt werden können. Der Vorteil ist, dass sich Sigma-Regeln für unterschiedliche SIEM-Produkte konvertieren lassen [3].

`Yara.Process` wird eine YARA-Regel auf die laufenden Prozesse im Speicher angewendet.

Eine neue Funktion von Velociraptor ist das Anwenden einer großen Anzahl von Sigma-Regeln auf Protokolldateien. Mit diesen Regeln können potenziell interessante Rechner schnell und in großem Umfang eingegrenzt werden. Die erkannten potenziell bösartigen Aktivitäten können in die weitere Untersuchung einbezogen werden. Velociraptor bietet bereits ein Verzeichnis von Regeln; eigene Regeln lassen sich ergänzen. Mit dieser neuen Funktion kann auch eine Echtzeitüberwachung für Sigma-Regeln auf Livesystemen eingerichtet werden. Das zuvor vorgestellte Hayabusa verwendet ebenfalls Sigma-Regeln. Die nun native Unterstützung von Sigma (siehe ix.de/zj89) in Velociraptor ermöglicht es, die CPU- und Speicherkontrolle von Velociraptor zu nutzen, und ist wesentlich effizienter als Hayabusa. Die Prüfung mit Sigma-Regeln kann auch als Einstiegspunkt für die Analyse dienen.

Velociraptor bietet verschiedene Möglichkeiten, gezielt nach IOCs zu suchen. Diese IOC-Suchen können über eine große Anzahl von Systemen gestartet werden, was viel Zeit spart. So lässt sich auch feststellen, welche Systeme kompromittiert wurden und in den Wiederherstellungsprozess einbezogen werden müssen.

Weiterführende Quellen: Training und Herausforderungen

Für diejenigen, die noch tiefer in die Materie einsteigen und Velociraptor testen oder damit üben möchten, stehen auf der Velociraptor-Webseite Trainingsvideos zur Verfügung. Sie behandeln unter anderem das Installieren des Werkzeugs, die VQL-Sprache und die forensische Analyse einschließlich Triage. Das Tool wurde auf mehreren Veranstaltungen und Konferenzen vorgestellt; dabei wurden Fallbeispiele aus der Praxis gezeigt. Die Präsentationen finden sich ebenfalls auf der Webseite (siehe ix.de/zj89).

Auch diejenigen, die sich gerne Herausforderungen stellen, kommen nicht zu kurz. Einige sind auf Onlineplattformen wie HackTheBox oder TryHackMe (siehe ix.de/zj89) zu finden. Dazu gibt es Anleitungen im Internet, wie man diese Herausforderungen meistert. (ur@ix.de)

Quellen

[1] Markus Stubbig; Auf Spurensuche mit Velociraptor; iX 9/2023, S. 122

[2] Gregor Wegberg; KAPE-Tutorial Teil 1: Vorsortieren im Schnelltempo; iX 7/2021, S. 128

[3] Fabian Murer, Gregor Wegberg; AD-Sicherheit: Angriffsspuren analysieren; iX 1/2022, S. 124

[4] Frank Ully; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; iX 11/2020, S. 94

[5] Nadia Meichtry, Fabian Murer, Tabea Nordieker; Malware-Analyse per OSINT und Sandbox; iX 3/2023, S. 122

[6] Frank Neugebauer; Blue Teaming: Wie man die Verteidigung gegen Internetangriffe übt; iX 7/2019, S. 54

[7] Nadia Meichtry; Statische Malware-Analyse; iX 5/2023, S. 132

[8] Alle im Artikel genannten Quellen und Hilfestellungen sind über ix.de/zj89 zu finden.

MELANIE KUBLI

ist Digital-Forensics- und Incident-Response-Spezialistin bei der Oneconsult AG in Zürich. Sie unterstützt Kunden bei der Bewältigung und der Analyse von Informationssicherheitsvorfällen.

NADIA MEICHTRY

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