KAPE-Einführung, Teil 1:
Installation, Konfiguration und Ausführung

Vorsortieren im Schnelltempo

Gregor Wegberg

Cyberangriffe, Schadsoftwareinfektionen und unerlaubte Aktionen gehören zum Alltag von Admins und Sicherheitsverantwortlichen. Zur Minimierung des Schadens müssen sie schnell und situationsgerecht auf solche Vorfälle reagieren. Der erste Teil des neuen Tutorials führt den Kroll Artifact Parser and Extractor als IT-forensisches Triage-Werkzeug zum Vorsortieren der relevanten Daten ein.

Für die Bewältigung eines Informationssicherheitsvorfalls müssen die Verantwortlichen die betroffenen Computer und Nutzerkonten, die potenziell involvierte Schadsoftware und alle mit dem Vorfall zusammenhängenden Aktivitäten in der IT-Umgebung identifizieren und analysieren. Erst diese Informationen erlauben es, die Ausbreitung des Schadens zu verhindern und anschließend den Vorfall durch die Säuberung und Wiederherstellung der IT-Systeme zu beenden.

IT-forensische Prozesse und Werkzeuge ermöglichen es, solche zentralen Informationen zu finden und auszuwerten. Im Normalfall werden zunächst die flüchtigen Daten gesichert, zum Beispiel der Inhalt des Arbeitsspeichers. Anschließend wird ein Abbild, also eine Eins-zu-eins-Kopie, der Datenträger erstellt.

Erst danach findet die eigentliche Analyse auf einer Kopie dieses Abbilds und der flüchtigen Daten statt. Mit der Kapazität der Speichermedien ist auch die Dauer einer solchen IT-forensischen Datenakquise stark gestiegen.

Gleichzeitig müssen die Zuständigen immer schneller auf Informationssicherheitsvorfälle reagieren, um den Schaden klein zu halten und die schnelle Rückkehr in den Normalbetrieb sicherzustellen. Aus diesem Grund eignen sich lang dauernde IT-forensische Datensicherungen nicht für die Bewältigung vieler Informationssicherheitsvorfälle, mit denen Organisationen heutzutage konfrontiert sind. In solchen zeitkritischen Situationen kommt der Kroll Artifact Parser and Extractor (KAPE) bei Windows-Systemen ins Spiel (das Werkzeug sowie weitere im Text genannte Quellen sind über ix.de/zv1c zu finden). KAPE darf außer bei bezahlten Kundenprojekten oder in Netzwerken Dritter frei genutzt werden.

Daten sammeln und auswerten

Während der Untersuchung eines Computers übernimmt das Werkzeug zwei Aufgaben: Es sammelt für die Analyse relevante Dateien („Triage“) und verarbeitet sie mit Drittsoftware, die daraus die IT-forensisch bedeutenden Informationen extrahiert und zur Analyse und Bewertung aufbereitet. Die beiden Arbeitsschritte können getrennt voneinander stattfinden und sind durch „Targets“ und „Modules“ abgebildet.

Jedes Target enthält eine Liste von Datei- oder Ordnerpfaden, die KAPE für die spätere Verarbeitung kopieren soll. Bei diesen Pfaden handelt es sich oft um Muster, die es dem Tool beispielsweise erlauben, in allen Nutzerprofilen nach Dateien oder Ordnern zu suchen. Module abstrahieren den Aufruf von Drittanwendungen zur Verarbeitung der gesammelten Dateien. Jedes Modul beschreibt den Aufruf einer Drittanwendung, inklusive der nötigen Parameter und Optionen.

So gibt es beispielsweise ein Target für den Microsoft-Edge-Browser, das KAPE dazu veranlasst, sämtliche von Edge genutzten Dateien in den Nutzerprofilen zu sammeln. Diese enthalten Cookies, den Browserverlauf, Metadaten zu Downloads und mehr. Anschließend kann eine Drittanwendung mithilfe eines Moduls diese Daten durch Zusammenfassen des Browserverlaufs und Downloads in CSV-Dateien verarbeiten. Anhand einer solchen CSV-Datei kann man beispielsweise den Besuch einer Phishing-Webseite oder das Herunterladen unerwünschter Software nachvollziehen. Im dritten Teil dieser Tutorialreihe werden wir die Browser-bezogenen Targets und Module vertieft kennenlernen.

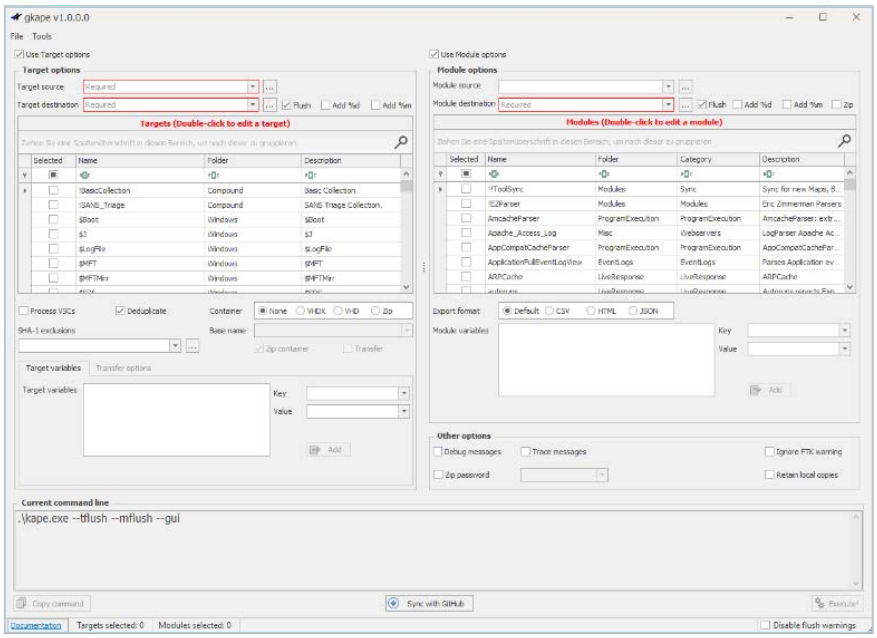
Läuft KAPE direkt auf einem zu untersuchenden System, können Module auch Applikationen zum Sammeln von Informationen der Laufzeitumgebung ausführen. Solche Module sind Teil der Live-Response-Kategorie und erlauben es zum Beispiel, den Inhalt des DNS Cache, die aktuell offenen TCP- und UDP-Verbindungen oder die laufenden Prozesse festzuhalten.

Mehrere Aufgaben zusammenfassen

Zur einfacheren Nutzung können mehrere Targets in einem Compound Target zusammengefasst werden, das alle in ihm gelisteten Targets ausführt. So verfügt KAPE über ein Standard-Compound-Target Web-Browsers, das die Dateien aller KAPE bekannten Browser sammelt. Compound Targets sind besonders nützlich, um ein persönliches Standardset von Targets für übliche Situationen zu definieren oder alle Targets auszuführen, die sämtliche Dateien verschiedener Softwareprodukte der gleichen Kategorie (Browser unterschiedlicher Hersteller) sammeln. KAPE behandelt Compound Targets als Target, wodurch mehrere Ebenen von Compound Targets möglich sind.

Jedes Target, Compound Target und Modul ist eine eigene Textdatei und aufgrund ihrer Struktur relativ einfach zu verstehen. Die Dateien lassen sich entweder mit einem Texteditor oder durch einen Doppelklick auf die Tabellenzeile in der grafischen KAPE-Anwendung ansehen (siehe Abbildung 1).

Trotz der vermeintlich einfachen Aufgabenstellung bietet das Werkzeug eine Vielzahl von Einstellungen. Die vorliegende Tutorialreihe konzentriert sich deshalb auf einen typischen Einsatz: Ein Windows-System soll aufgrund eines Verdachts schnellstmöglich untersucht werden. Ein weiteres System, das in den Vorfall nicht involviert ist, steht für die Vorbereitung und anschließende Analyse zur Verfügung. Für den Datentransfer zwischen den beiden Systemen wird ein externer Datenträger genutzt.



In der grafischen Oberfläche (gkape.exe) lässt sich KAPE einfach konfigurieren. Die (Compound-)Target- und Modul-Dateien können per Mausklick eingesehen werden (Abb. 1).

Aus den genannten Gründen müssen bei vielen Sicherheitsvorfällen erste Informationen schnellstmöglich als Entscheidungsgrundlage bereitstehen. In solchen Fällen führt der Forensikexperte KAPE direkt auf einem potenziell betroffenen System aus und sammelt Dateien mit Targets und flüchtige Informationen mit Modulen der Kategorie „LiveResponse“. Die Informationen werden danach auf ein anderes System überführt, auf dem weitere Module sie verarbeiten und die Resultate auswerten.

Vorsicht vor Beweisveränderung

Bei einer solchen Live-Forensics-Untersuchung muss der Verantwortliche darauf achten, möglichst wenige Änderungen am untersuchten System vorzunehmen, damit keine Spuren verwischt werden. Aus diesem Grund werden KAPE, der Kommandozeilenaufruf sowie sämtliche benötigten Drittanwendungen vorab vorbereitet und auf dem zu untersuchenden System nur noch ausgeführt.

KAPE wird von Eric Zimmerman für das Unternehmen Kroll entwickelt und muss beim ersten Mal von der Unternehmenswebseite heruntergeladen werden. Das ZIP-Archiv enthält die grafische Oberfläche zur Konfiguration und Ausführung des Tools (gkape.exe), die Kommandozeilenanwendung (kape.exe), ein PowerShell-Skript zum Herunterladen der neuesten Version und für die Targets und Module je einen Ordner gleichen Namens. Compound Targets liegen als Spezialfälle von Targets im Unterordner Targets/Compound.

Ausführung erfordert Administratorrechte

Entpacken und ausführen lässt sich KAPE an einem beliebigen Ort, sofern mindestens Microsoft .NET in Version 4.52 installiert ist und das Werkzeug mit einem Administratorkonto ausgeführt wird. Im vorgestellten Szenario wird es auf einem externen Datenträger entpackt und mit dem für die Analyse bereitstehenden System vorbereitet.

X-TRACT

- Informationssicherheitsvorfälle gehören zum IT-Alltag und müssen zeitnah verstanden und bewältigt werden.
- Eine vollwertige IT-forensische Sammlung und Auswertung von Informationen auf potenziell betroffenen Systemen dauert für viele Sicherheitsvorfälle zu lange.
- Der Kroll Artifact Parser and Extractor (KAPE) erlaubt eine rasche IT-forensische Triage bei Sicherheitsvorfällen und liefert Informationen zu deren Bewertung und Bewältigung.

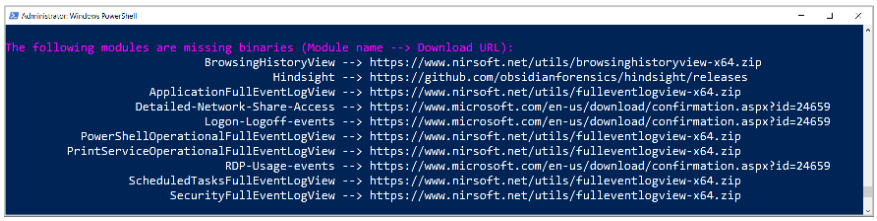
Tutorialinhalt

Teil 1: Installation, Konfiguration und Ausführung von KAPE

Teil 2: Autoruns-Artefakte auswerten und verstehen

Teil 3: Browserhistorie auswerten und verstehen

Teil 4: Was wurde von wem wann ausgeführt?



Per Befehl gibt KAPE eine Liste der Modul-Namen und die Links zu den von ihnen benötigten Drittanwendungen aus (Abb. 2).

Vor dem Benutzen der Software sollte sie einschließlich der Targets, Module und zum Einsatz kommenden Drittanwendungen auf den neuesten Stand gebracht werden: Mit dem Skript `Get-KAPEUpdate.ps1` wird die neueste Version heruntergeladen und entpackt. Die Targets und Module sind Teil eines öffentlichen GitHub-Projekts (siehe ix.de/zv1c) und können mittels Kommandozeilenbefehl `.\kape.exe --sync` oder mit dem „Sync with GitHub"-Knopf in der grafischen Oberfläche aktualisiert werden.

Die Aktualisierung der Drittanwendungen gestaltet sich etwas schwieriger. Alle von Modulen aufgerufenen Anwendungen müssen im Ordner Modules/bin liegen, damit KAPE sie finden und aufrufen kann. Die von Eric Zimmerman selbst entwickelten Drittanwendungen sind Teil des ZIP-Archivs und liegen bereits im besagten Ordner. Sie können ganz einfach mithilfe des Moduls !!ToolSync aktualisiert werden:

```
PS F:\kape> .\kape.exe --msource C:\ --mdest ↵
       C:\temp\null --module !!ToolSync -debug
```

Alle weiteren Anwendungen muss man manuell herunterladen. Welche für welches Modul benötigt wird, zeigt der folgende Befehl:

```
PS F:\kape> .\kape.exe --mlist . --mdetail
```

Welche Drittanwendungen werden benötigt?

Am Ende der Konsolenausgabe nennt KAPE eine Liste von Modul-Namen und die URL zum Download der Drittanwendung, sofern die erforderliche Anwendung im Modules/bin-Ordner fehlt (siehe Abbildung 2). In den kommenden beiden Tutorialteilen werden wir Module nutzen, die eine solche Drittanwendung benötigen, und auf das Identifizieren, Herunterladen und Einrichten dieser Anwendungen vertieft eingehen. Nach allen Aktualisierungen ist KAPE für den Einsatz bereit.

Bei der fiktiven Analyse sollen im ersten Schritt auf dem zu untersuchenden System Dateien für eine erste Triage gesammelt werden. Der einfachste Weg, den KAPE-Kommandozeilenaufruf vorzubereiten, ist die Nutzung der grafischen Oberfläche (Abbildung 1). In ihr kann man auf der linken Seite die Targets und auf der rechten Seite die Module konfigurieren. Anschließend führt man KAPE mit den gewünschten Einstellungen über die Kommandozeile im unteren Drittel unter „Current command line" aus.

Für das Sammeln der Dateien kommen Targets zum Einsatz, die sich unter „Use Target options" konfigurieren lassen. „Use Module options" bleibt deaktiviert, da das zu untersuchende System keine Drittanwendungen ausführen soll. Danach muss die „Target source" angegeben werden: Hierbei handelt es sich um das Laufwerk, von dem die Dateien gesammelt werden sollen. Das ist im Normalfall die Systempartition, also C:. Die Dateien werden in den „Target destination"-Ordner kopiert. Bis der externe Datenträger am zu untersuchenden System angeschlossen wird, ist sein Laufwerksbuchstabe unbekannt. Damit die „Target destination" vor der Ausführung angepasst wird, kann sie temporär TODO heißen.

Jetzt bleibt nur noch das Auswählen der auszuführenden Targets in der linken Tabelle. Für eine erste Triage eignet sich zum Beispiel KapeTriage, ein Compound Target, das viele typische IT-forensisch interessante Dateien sammelt, etwa die Windows-Ereignisprotokolldateien, die Registry Hives und vieles mehr. Die restlichen Einstellungen und Optionen bleiben in der Standardeinstellung (siehe Abbildung 3).

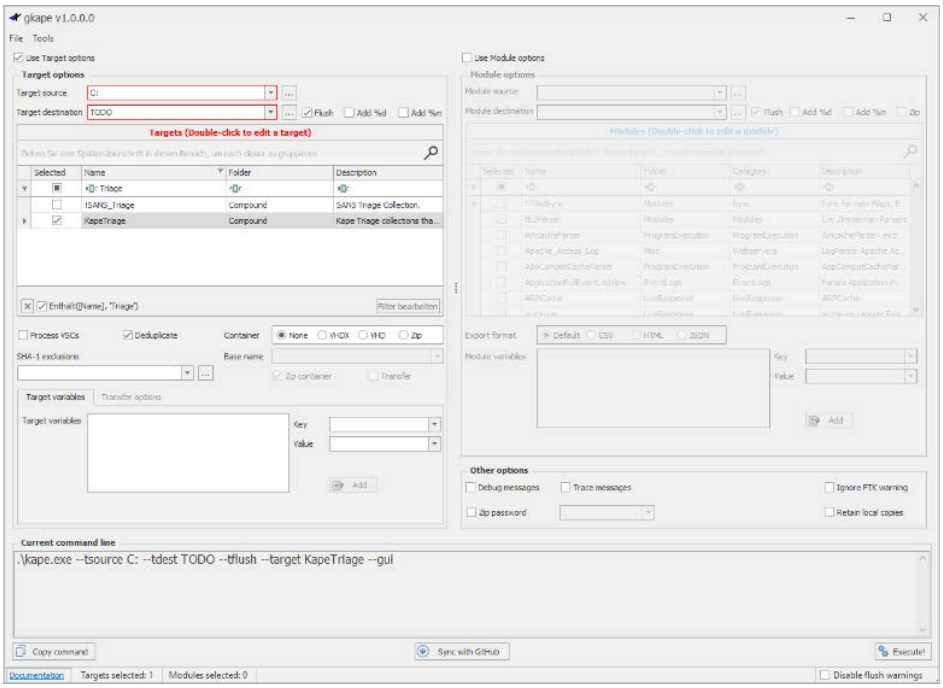
Die daraus resultierende Kommandozeile („Current command line") ist zu kopieren, zum Beispiel in eine Textdatei für den anschließenden Aufruf auf dem zu untersuchenden System. Damit ist die Konfiguration abgeschlossen, die grafische Oberfläche kann verlassen und der externe Datenträger mit KAPE und seinen Abhängigkeiten an das zu untersuchende System angeschlossen werden.

Nun startet man eine administrative Kommandozeile wie PowerShell und wechselt in den KAPE-Ordner auf dem externen Datenträger. Anschließend ist der vorbereitete Aufrufbefehl um das Ziel der Untersuchung zu ergänzen: Im vorliegenden Beispiel wurde dem externen Datenträger der Laufwerksbuchstabe F zugeordnet. Entsprechend wird das bisherige TODO durch einen gültigen Pfad auf dem externen Datenträger ersetzt, beispielsweise:

```
PS F:\kape> .\kape.exe --tsource C: --tdest ↵
            F:\TargetDestination\ --tflush --↵
                  target KapeTriage --gui
```

Mit dieser Änderung kann das Sammeln der Dateien durch die Ausführung des Befehls starten. Der Fortschritt ist dabei im Titel der Kommandozeile sichtbar.

Schließlich findet sich im Zielordner (hier F:\TargetDestination\) ein Ordner mit dem als „Target source" angegebenen Laufwerksbuchstaben (hier C), in dem die

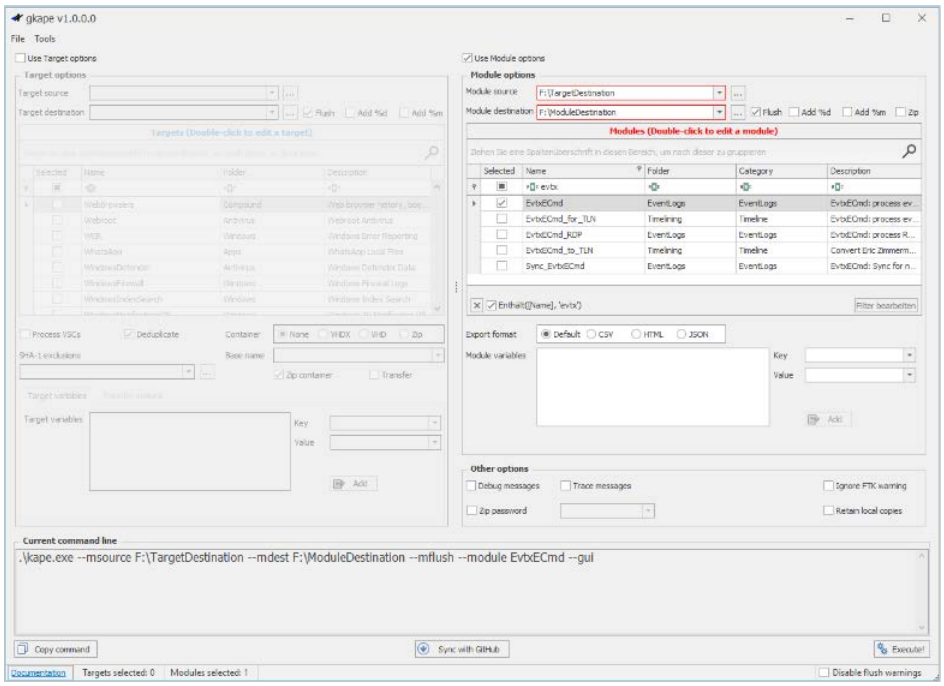


Beispielkonfiguration für die Dateisammlung für eine erste Triage (Abb. 3)

kopierten Dateien liegen, normalerweise unter Beibehaltung der ursprünglichen Dateipfade. Zusätzlich finden sich im Zielordner die Konsolenausgabe als Logdatei (Suffix _ConsoleLog.txt) und zwei CSV-Dateien mit einer Liste aller kopierten (_CopyLog.csv) und der übersprungenen Dateien (_SkipLog.csv). Nach dem Durchlauf beendet man die Konsole und schließt den externen Datenträger an den Analysecomputer an.

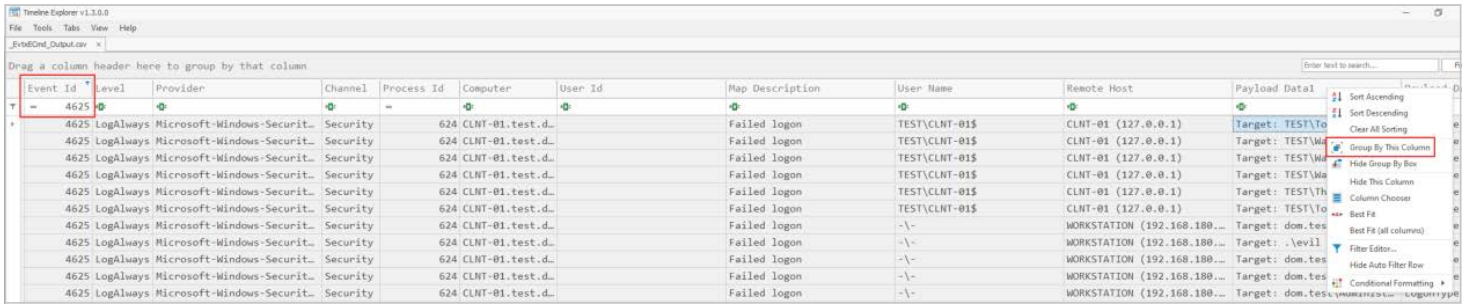
Auswertung der Dateien

Wie an der Konsolenausgabe, den kopierten Dateien oder dem ausgeführten Target KapeTriage zu sehen ist, hat KAPE unter anderem Windows-Ereignisprotokolldateien kopiert. Diese sind eine wertvolle Quelle zum Aufdecken diverser unerwünschter Aktivitäten. Auf einem Standard-Windows-System sammelt das Werkzeug schnell mehrere Hundert einzelne Ereignisprotokolldateien (siehe C\Windows\System32\winevt\logs im konfigurierten Zielordner). Jede einzelne von Hand durchzugehen, würde sehr viel Zeit in Anspruch nehmen.



Beispielkonfiguration für die Auswertung aller gesammelten Windows-Ereignisprotokolldateien mit EvtxECmd (Abb. 4).

Hier kommen die Module zur Auswertung und Aufbereitung der gesammelten Dateien zum Einsatz: Zur einfacheren Handhabung können diese beispielsweise mit dem Modul EvtxECmd in eine einzige CSV-Datei zur Auswertung zusammengefasst und zum einfacheren Verständnis normiert werden. KAPE nutzt für dieses Modul die gleichnamige EvtxECmd-Kommandozeilenapplikation von Eric Zimmerman (siehe ix.de/zv1c), die bereits beiliegt und ohne weiteren Aufwand einsetzbar ist.



Der erste Untersuchungsschritt besteht darin, nach fehlgeschlagenen Anmeldeversuchen (Ereignisnummer 4625) zu filtern und die Ereignisse nach Zielkonten (Spalte „Payload Data1“) zu gruppieren (Abb. 5).

Wie bei den Targets erfolgt auch die Konfiguration der Module über die grafische Oberfläche. Zuerst wird „Use Module options“ ausgewählt, „Module source“ soll der Zielordner der vorherigen Dateisammlung sein (entspricht „Target destination“ beziehungsweise `--tdest`) und als „Module destination“ dient ein neuer Ordner für die Resultate der Module. In der Tabelle auf der rechten Seite können analog zu den Targets die auszuführenden Module festgelegt werden – im vorliegenden Beispiel EvtxECmd. Nach diesen Voreinstellungen aktiviert man die Verarbeitung via Execute!-Button (Abbildung 4). Die Kommandozeilenapplikation startet mit dem unter „Current command line“ sichtbaren Befehl.

Sobald KAPE fertig ist, kann die Kommandozeile geschlossen werden. Im Ordner „Module destination“ finden sich erneut die Konsolenausgabe als Logdatei („_ConsoleLog.txt“-Suffix) und die von den gewählten Modulen abhängigen Unterordner mit den Resultaten der Auswertungen. Das EvtxECmd-Modul erstellt zum Beispiel den Unterordner EventLogs, in dem eine CSV-Datei mit dem Inhalt aller Ereignisprotokolldateien liegt (Suffix _EvtxECmd_Output.csv). Dessen Analyse gibt hoffentlich Hinweise zum vorliegenden Informationssicherheitsvorfall.

Im Normalfall generieren Module eine CSV-Datei, die mit den einschlägigen Tabellenkalkulationsprogrammen geöffnet und ausgewertet werden kann. Über diese Programme muss man wissen, dass sie gewisse Daten, zum Beispiel die Zeitstempel, nicht richtig darstellen und so die Auswertung deutlich erschweren. Oft kommen sie auch mit den großen Dateien nicht zurecht. Unter anderem aus diesen Gründen hat Eric Zimmerman den Timeline Explorer entwickelt (siehe ix.de/zv1c). Damit lassen sich die meisten von KAPE erstellten CSV-Dateien öffnen und dank einer Vielzahl von Funktionen detailliert auswerten.

Analyse der Windows-Ereignisprotokolle

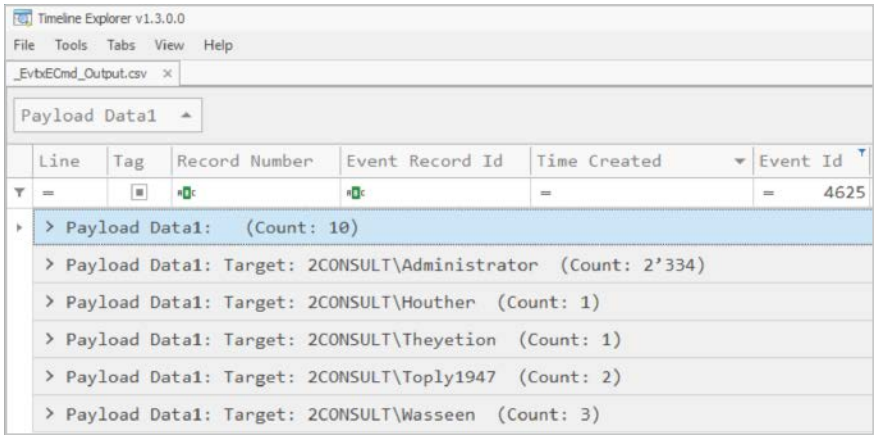
In unserem fiktiven Szenario möchten wir nun das vorhin von EvtxECmd generierte CSV-Dokument analysieren. Dazu öffnen wir die CSV-Datei im Timeline Explorer und klicken im Kontextmenü einer beliebigen Spaltenüberschrift auf den „Best Fit (all columns)“-Eintrag zur Steigerung der Lesbarkeit.

Bei Informationssicherheitsvorfällen ist es unter anderem interessant zu wissen, welche Nutzerkonten sich zu welchem Zeitpunkt auf einem untersuchten Gerät anzumelden versuchten. Zum Beispiel kann ein Blick auf die fehlgeschlagenen Anmeldungen Hinweise auf Brute-Force- oder Password-Spraying-Angriffe geben: Hierzu filtert man in der „Event Id“-Spalte nach der in der Windows-Dokumentation genannten Ereignisnummer 4625 (Ereignis „Fehler beim Anmelden eines Kontos“) und wählt im Kontextmenü der Spalte „Payload Data1“ den Eintrag „Group By This Column“ (siehe Abbildung 5). „Payload Data1“ enthält bei diesem Ereignis jeweils das vom fehlgeschlagenen Anmeldeversuch betroffene Nutzerkonto. Durchs Gruppieren erhält man einen ersten Überblick über die Anzahl fehlgeschlagener Anmeldeversuche pro Nutzerkonto.

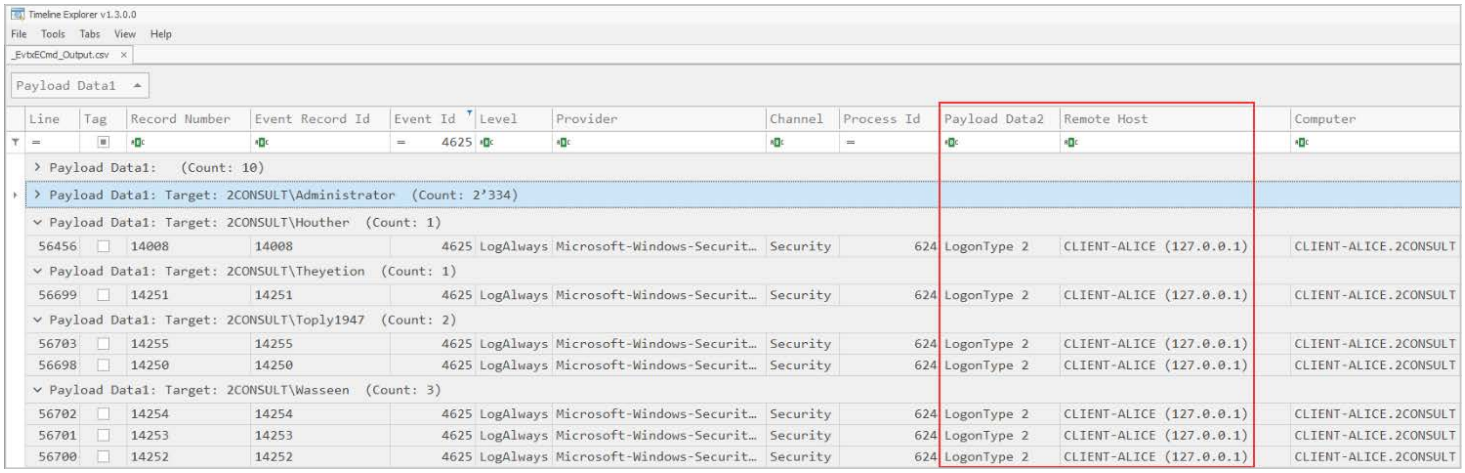
Im dargestellten Beispiel fallen sofort 2334 fehlgeschlagenen Anmeldeversuche beim Nutzerkonto 2CONSULT\Administrator auf (siehe Abbildung 6). Diese hohe Zahl ist gerade im Vergleich mit den restlichen Nutzerkonten besonders auffällig und muss bei einem Vorfall unbedingt genauer untersucht werden – bis man die Ursache dafür gefunden hat. Bei den restlichen Nutzerkonten lassen sich die niedrigen Zahlen mit mutmaßlichen Tippfehlern bei der Passworteingabe erklären.

Bei der vertieften Analyse dieser Anmeldeversuche helfen die Spalten „Payload Data2“ und „Remote Host“: „Payload Data2“ enthält bei diesem Ereignis den Anmeldetyp und „Remote Host“ das Quellsystem, von dem der Anmeldeversuch stammte. Beim Betrachten der Nutzerkonten mit den wenigen Ereignissen (Abbildung 7) zeigt sich sofort, dass sie alle vom Anmeldetyp 2 sind, der eine interaktive Anmeldung repräsentiert. Außerdem handelt es sich bei allen um lokale Anmeldungen auf dem untersuchten System (Spalte „Computer“). Dies bekräftigt die Vermutung, dass es sich hierbei um vorerst nicht weiter zu untersuchende Eingabefehler handelt.

Im Gegensatz dazu handelt es sich bei den Anmeldeversuchen für das Administratorkonto um Anmeldungen des Typs 3,



Fehlgeschlagene Anmeldeversuche gruppiert nach den betroffenen Nutzerkonten (Abb. 6)



Interaktive Anmeldungen vom untersuchten Gerät aus, die wahrscheinlich aufgrund von Tippfehlern fehlgeschlagen sind (Abb. 7)

also über das Netzwerk. Sie stammen allesamt vom gleichen Drittgerät mit der IP-Adresse 192.168.180.130 und es fanden mehrere Versuche pro Sekunde statt (siehe Abbildung 8). Dies kann auf einen Brute-Force-Angriff hindeuten oder einen fehlkonfigurierten Dienst, der sich fortlaufend mit einem falschen Passwort anzumelden versucht. Bei einem solchen Vorfall ist dieses Drittgerät zwingend näher zu untersuchen. Bis der Hintergrund der Ereignisse bekannt ist, sollte das Gerät als kompromittiert betrachtet und behandelt werden.

Anhand der Windows-Ereignisprotokolle lassen sich viele weitere interessante Ereignisse studieren und Schlussfolgerungen ziehen. Auf der zweiten Seite des vom SANS Institute veröffentlichten Posters „Hunt Evil“ (siehe ix.de/zv1c) findet sich eine Übersicht typischer Techniken, die bei Angriffen genutzt werden, und in welchem Ereignisprotokoll welche Ereignisnummer auf die jeweilige Technik hindeuten könnte.

Ausblick

In den kommenden Tutorialteilen geht es um spezifische Fragestellungen während eines Informationssicherheitsvorfalls, zum Beispiel das Aufdecken typischer Schadsoftware-Persistenzmechanismen. Bis dahin sei Ihnen ans Herz gelegt, mit KAPE zu experimentieren, um das Werkzeug schon kennenzulernen: Es bietet eine Vielzahl von Einstellungen, die gut dokumentiert sind (siehe ix.de/zv1c), und kommt mit zahlreichen Targets und Modulen, die man durch einen Doppelklick auf die entsprechende Tabellenzeile in der grafischen Oberfläche näher betrachten kann.

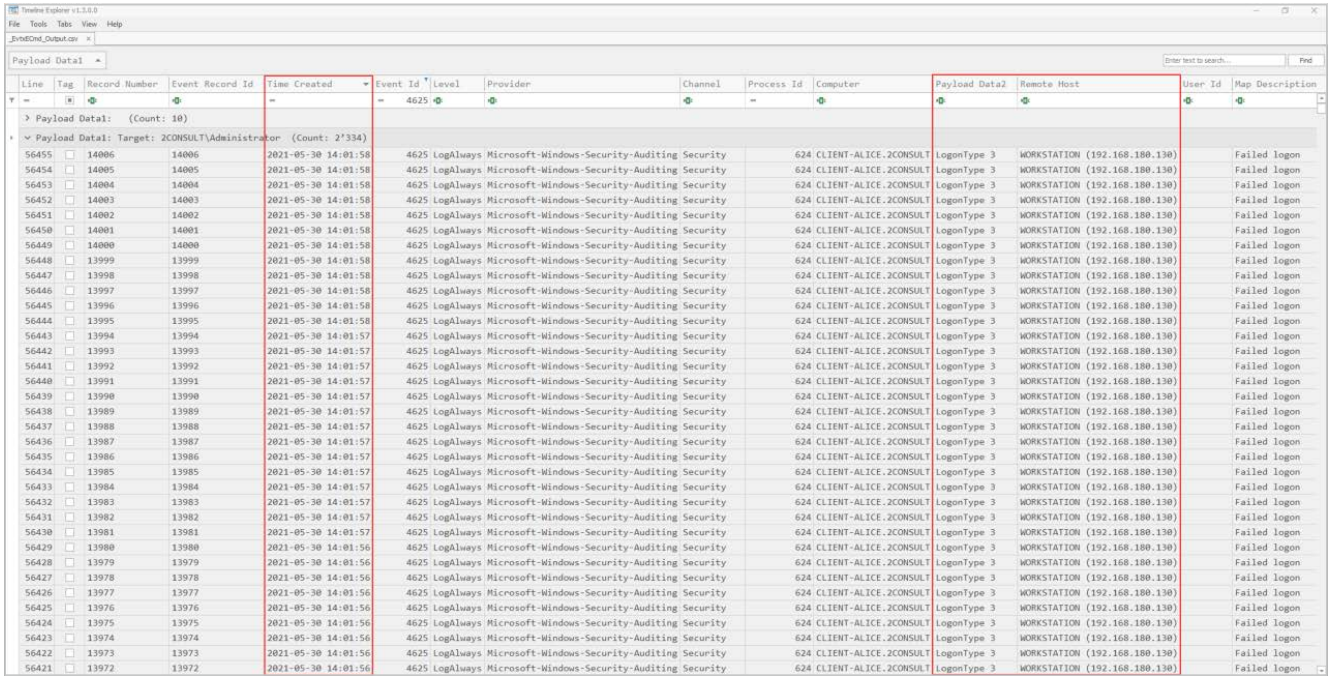
(ur@ix.de)

Quellen

Das Werkzeug KAPE, Informationen zu seinem Einsatz und den Targets und Modulen sowie weitere Quellen sind über ix.de/zv1c zu finden.

Gregor Wegberg

unterstützt mit seinem Team bei der Oneconsult AG Organisationen bei der Bewältigung von Cyberangriffen.



Die Ereignislogs in diesem Fall könnten auf eine Kompromittierung des untersuchten Geräts hinweisen und sollten weiter analysiert werden (Abb. 8).