

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.

ür 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 bei-

Target o arget cour	andiana					2U	ise Module	options					
arget sour	ip ciona					M	odule opt	ions					
	ree Required					Mod	kile source			•			
arget dest	tination Required		- 2 R	lush 🔲 Add %sd 🔲 Ad	dd %m	Mod	kle destri	abon Required		ZFI	ush 🗌 A	dd 76d 🔲 Add 75m 🗍	1
	Tan	gets (Double-click to edit a t	target)					Modu	les (Double-click to a	edit a moduli	e)		
					Q		hen Sie en	ne Spaltenilberschrift in diesen B	ierekm, um nach dieser a	a anapieren			5
Selecto	ed Name	Tolder		Description	-		Selected	Name	Folder	Cabegory		Description	í
4 III	i or	r0r		101	•	4		•	-0-	101		-0:	
• E	BesicColecton	Compound		Basic Collection	-110		0	"ToolSync	Modules	Sync		Sync for new Maps, 8	8
1	15ANS_Triage	Compound		SANS Trage Collection.				12Parser	Modules	Modules		Enc Zmmerman Parse	85
E	\$Boot	Windows		\$Boot				AmcadheParser	ProgramExecution	ProgramEx	recubion	AncacheParser: extr	
Ē	40	Windows		\$3				Apache_Access_Log	Misc	Webserver	rs	LogParser Apache Ac	
Ē	\$Log=le	Windows		\$LogFile				AppCompatCacheParser	ProgramExecution	ProgramEx	necution	AppCompatCachePar	
	\$MFT	Windows		\$4FT				ApplicationPullEventLogView	EventLogs	EventLogs		Parses Application ev	
1	SMFTMin	Windows		\$4FTMin		10		ARPCache	LiveResponse	LiveRespo	rse	ARPCache	
1					and in the second se				LL Downson	LineD on the		Autoruna renorta Exe	1
Process	a VSCs 🛛 🖂 Dedupki usions	ate Container Base name	None (0	Exp Mod	ort format Iule variabi	estenzes estenzes]	Key		
Process	a VSCs 🖓 Dedupki usions	ate Container Base name) None (leme Owen Owen Olas ner ∐Transfer	p	Exp Mod	ort format Iule vəriab	Default CSV (]	Key Value		
Process HA-1 exck	atables	ate Container Base name) None (Lenne Diwebx Oweb Oas ner ∐Transfer	P	Exp Mod	ort format Iule variabi	Default () CSV ()			Key Value		
Process HA-1 exck Target vi	avisors Decor	ate Container Base name) None (2p conte	Lenne D'WEX O'WE O 2: rer D'Transfer	P	Exp	ort format Iule variabi	Default O CSV (Key Value		
Process HA-1 exck Target vi Target vi	ariables Transfer options	ate Container Base name	0 None (2p conta Key	Leron WHDX () WHD () 2; ner () Transfer	P	Dop	ort format Iule variab	Default O CSV			Key Value	📴 Ack	
Process HA-1 exck Target vi Target vi	ariables Transfer options	ate Contaner Base name	None (2p:conta Key Value	Lenne WHDX WHD 22 ner Inansfer	2	Exp Mod	ort format Iule variab	Default O CSV			Key Value	D AK	•
Process HA-1 excli Target vi Target va	artables	ate Contaner Base name) None (2p contai Key Value	_enne	P	Dep Mod	ort format kule variabi	Cathorne Default O CSV			Key [Value	📴 Add	
Process HA-1 exclu Target vi Target va	avatives Prove	ate Contaner Base name) None (2p conta Key Value	Lenne	2 	Exp Mod	ort format lule variab ther optic Debug mes	In data of the second s			Key [Value]	Add	
Process HA-1 excl Target vi Target va	artables Transfer options	ate Contane Base name	0 None (2p conta Key Value	ene WEX VHD 22 ner Itanifer	P	Mac	ort format Iule variab deer optic Debug mes	Bedraut CDV CDV es			Key [Value]	Add	
Process HA-1 exck Target vi Target via	atables Transfer options	ate Contane Base name	0 None (2p conta Key Value	ene 22	P	Mod	ort format fule variabl ther optic Debug mes 2p passivo	es Cobult COV (es	HINGS AND		Key [Value]	Acc Ignore FIK warni Retan local cope	ing 15
Process HA-1 exck Target va Target va	svides Productions	ate Container a Beee name .) None (2p contai Key Value	rene 2000	P	Mod	ort format kile variab dier optic Debug mer Zip passivi	Bedraute CDV (CD	HTML JJSON		Key [Value [Acc Ignore FTK wars Retan local cope	ing es

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

den Systemen wird ein externer Datenträger genutzt.

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.

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.

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.

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?

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 Z
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



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

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.

Disable flush warnings

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:

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 Dateisamm-
lung für eine erste Triage (Abb. 3)
```

r gka	pe v1.0	.0.0												×
le To	ols													
Z use	Target op	tions						e Module	options					
Terg	et option	15					He	dule op	3005					
Target	source	Ci				Module source								
Target	destinatio	In TODO	*		at Takisa Takisa		Mod	ule destra	stun			lush 🗌 a	dd fad Dade fan	120
-		Tarpets	(Double-click to edit a	target)	and the set of the set									
		Spatentiseruteitt in deum t	Sensidu, um rauth diesair au	oruppinno	Q									
9	slected	Name	♥ Folder		Description	-11								
4		(D: Triage	r@r		(D):			100						
	0	ISANS_Triage	Compound		SANS Triage Collection.	18								
6		KapeTriage	Compound		Kape Triage collectors that.									
														10.00
Twie -	7 6.00.000	(Name) Triane?)			(where have do not									
1×10	Citoraci	(mame), (hage)			Hiter ocerbeiten									
Pro	cess VSCs	s 🛛 🗹 Dedupikate	Container	None C	WHDX O WHD O Zp		Expe	et format	🖲 Default. 🔿 CSV	HTML O JEON]:			
SHA-1	exclusion	8	Base name				Not	de veriet	les .			hey T		
-			F.S.		10 11 10 10 10 10 10 10 10 10 10 10 10 1							Salar I		
proven		the state of the s		- op conse	C lines							tone 1		
Targ	jet variabl	es Transfer options												
Targe	st variable	8		in									Add	
					1									
				Value										
							Ot	her opti	ns					
					Eth m		1	bebug me	isages Trace messages				Ignore FTK wa	ning
							1.13	Dp passw	and [Retain local co	pies
Curre	ent comr	mand line												
,\kap	e.exe	tsource C:tdest	TODOtflushta	irget Kap	eTrlagegul									
					100									
Ct Ct	tak counti	and			()	Sync	with G	duHi					90	Executel

Targets selected: 1 Modules selected: 0

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

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.

	0.0.0									- 0
e Tools										
Use Target op	ptions			24	lse Module	options				
Target option	005			M	odule opt	ions				
arget source				Mor	iule source	F: (TargetDestination		-		
Carrat darbrate	lane l		TURN LARGE LAS	Max.	iule destru	tion E-Mark laDertmation			keh 🗆 se	
			and the same of the same of the same			M	whites (Double click to a	adit a modu	(m)	
							March (Contone Calen Co.	COR O MODO		
					and the et		en cereich, um nech deser :	au gruppieren		1
					Selected	Name	* Folder	Categor	Υ.	Description
9 H				7 9		*@* evb:	·0·	•0:		•0:
					2	EvistECnd	EventLogs	EventLo) grs	EvtxECmd: process e
						EvtxECmd_for_TUN	Timelining	Inelne		EvtoECmd: process e
						EvbdCmd_RDP	EventLogs	Eventio	ogs	EvtdECmd: process R
						EvtxECmd_to_TLN	Timelining	Timeline		Convert Eric Zimmern
						Sync_EvtxECmd	EventLogs	Eventio	ogs	EvtxECmd: Sync for I
				1-						
				1		Princemal Sectors				Eller handel
				10	() () failes	influence), enory				Trunt seamon
Process VSC	s Dedupicate	Container	None WHDX WHD 20	Dor	ort format	@ Default () CSV	O HTML O JSON			
PNA-1.exclusion	10	Sage name		Mod	kule variabi	es :			кеу	
	5		äp container 📃 Transfer						Value	
									104	
Target variable	HS .		Key						3 3	P Ack
			Value							
			In the second	0	ther optic	ns				
	÷.		Br Add		ther optic Debug mes	ns sages Trace messa	ges			C Ignore FTK warning
	1		B AG		<mark>ther optic</mark> Debug mes 2p pessive	ns sages Trace messa rd	9es			Ignore FTK warning Retain local copies
	÷.		BP AG		ther optic Debug mes 2ip passwo	ns sages Trace messa rd	905 [+]			C Ignore FTK warning

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.

155	Timeline Exp	plorer v1.1	3.0.0										- 0
Fili	Tools	Tabs)	View Help										
_F	txECind_Out	tput.cov	x										
Dr	ag a co	nul	header he	re to group by that column								Enter	lext to search
	Event	Id *	Level	Provider	Channel	Process Id	Computer	User Id	Map Description	User Name	Remote Host	Payload Data1	AL CONTRACTOR
т	-	4625	D:	-0=	-0:	-	-0:	-0:	+ O :	+D:	0	-O:	21 Sort Ascending
٠	1	4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\Te	Clear All Sorting @
		4625	LogAlways	Microsoft-Windows-Securit_	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\W	Genue By This Column
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\W	4" Hide Group By Bdy E
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\Wa	Hide The Column 9
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\T	e Column Chooser
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	TEST\CLNT-01\$	CLNT-01 (127.0.0.1)	Target: TEST\T	e Best Fit
		4625	LogAlways	Microsoft-Windows-Securit_	Security	62	4 CLNT-01.test.d.		Failed logon	-\-	WORKSTATION (192.168.180	Target: dom.te	Best Fit (all columns)
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	-1-	WORKSTATION (192.168.180	Target: .\evil	Titter Editor
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	-\-	WORKSTATION (192.168.180	Target: dom.te	Hide Auto Filter Row
		4625	LogAlways	Microsoft-Windows-Securit	Security	62	4 CLNT-01.test.d.		Failed logon	-\-	WORKSTATION (192.168.180	Target: dom.te:	· Conditional Formattion +
		4625	LogAlways	Microsoft-Windows-Securit_	Security	62	4 CLNT-01.test.d.		Failed logon	-\-	WORKSTATION (192.168.180	Target: dom.te:	Stynumanast. Logonrype

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 Zeit-

File	Time	eline Expl Tools	lorer v1.3. Tabs Vi	0.0 iew Help										
Ev	b/EC	Cmd_Out	put.csv 3	×										
P	ay]	load I	Data1	*										
	Li	Line Tag Record Number			r Event Record I	d Time Created	Ŧ	Event	Id T					
Ŧ	-			*Dc	# D c	=		=	4625					
•	>	Payl	oad Da	ata1: (Coun	t: 10)									
	>	> Payload Data1: Target: 2CONSULT\Administrator (Count: 2'334)												
	> Payload Data1: Target: 2CONSULT\Houther (Count: 1)													
	>	Payl	oad Da	ata1: Target: 2CONSULT\Theyetion (Count: 1)										
	> Payload Data1: Target: 2CONSULT\Toply1947 (Count: 2)													
	>	Payl	oad Da	ata <mark>1: Ta</mark> rget:	2CONSULT\Wasseen	(Count: 3)								

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

punkt 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,

🖏 Timeline	Explorer	v1.3.0	0.0								
File Tools	s Tabs	Vie	ew Help								
EvtxECmd	Output.c	sv >	c								
Pavloa	d Dat	a1									
1					7	-	1			1	
Line	Ta	g	Record Number	Event Record Id	Event Id Level	Provider	Channel	Process Id	Payload Data2	Remote Host	Computer
۳ =			*Dc	4Dc	= 4625	* D ¢	A C	-	* D ¢	* O ¢	a 🗖 c
> Pa	yload	d Da	ta1: (Count:	10)							
> Pa	yload	d Da	ta1: Target: 20	ONSULT\Administrat	or (Count: 2'334)						
✓ Pa	yload	d Da	ta1: Target: 20	ONSULT\Houther (C	ount: 1)						
564	56		14008	14008	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
✓ Pa	yload	d Da	tal: Target: 20	ONSULT\Theyetion	(Count: 1)						
566	99		14251	14251	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
v Pa	yload	d Da	tal: Target: 20	ONSULT\Toply1947	(Count: 2)						
567	03		14255	14255	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
566	98 [14250	14250	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
✓ Pa	yload	d Da	tal: Target: 20	ONSULT\Wasseen (C	ount: 3)						
567	02		14254	14254	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
567	01		14253	14253	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE.2CONSULT
567	00		14252	14252	4625 LogAlways	Microsoft-Windows-Securit	Security	624	LogonType 2	CLIENT-ALICE (127.0.0.1)	CLIENT-ALICE, 2CONSULT

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.

10	Tenelize Kap	sorer v 1.	3.0.0											- a	×.
2.0	e Tools	labs	View Help												
-	rb/EOnd_Out	put.csv	¥.												-
F	ayload	Datal	1 A									En	er text to search.	FP	nd
	Line	Tøg	Record Number	Event Record Id	Time Created -	Event Id Level	Provider	Channel	Process Id	Computer	Payload Data2	Remote Host	User Id	Map Descriptio	on.
τ	-		-0-	-0-	-	- 4625 🕫	•	-0:		-0-	-0-	4	-0-	* D *	-
	> Payl	load I	Data1: (Count:	10)											
	v Pavl	load I	Data1: Target: 2	CONSULT\Administr	ator (Count: 2'334)										
	SGASE		1/005	14006	2021-05-20 14-01-50	4626 1 0001000	r Mirporoft-Windows-Corupitu-Auditi	na Corunitu	67	CUTENT-AUTOR DOONSULT	LogonTune 2	WORKSTATTON (103 168 180 130		Eniled logen	
	56454		14005	14005	2021-05-30 14:01:50	4625 Lonàlway	Nicrosoft-Windows-Security-Auditi	ng Security	62	A CLIENT-ALICE 2CONSULT	LogonType 3	WORKSTATION (192.168.188.138)		Failed logon	
	56453		14004	14004	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALTCE. 2CONSULT	LogonType 3	WORKSTATION (192,168,188,138)		Failed logon	
	56452		14093	14003	2021-05-30 14:01-50	4625 LogAlway	s Nicrosoft-Windows-Security-Auditi	ng Security	62	A CLITENT-ALICE 2CONSULT	LogonType 3	WORKSTATION (192 168 188 138		Failed logon	
	56451		14992	14002	2021-05-30 14:01:58	4625 Logályay	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLITENT-ALTCE. 2CONSULT	LogonType 3	WORKSTATTON (192, 168, 188, 138)		Failed logon	
	56450		14001	14001	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192,168,180,130	i l	Failed logon	
	56449		14000	14000	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192,168,180,130)		Failed logon	
	56448		13999	13999	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130	i l	Failed logon	
	56447		13998	13998	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56446		13997	13997	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	5	Failed logon	
	56445		13996	13996	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56444		13995	13995	2021-05-30 14:01:58	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	j l	Failed logon	
	56443		13994	13994	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	5	Failed logon	
	56442		13993	13993	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	52	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56441		13992	13992	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130))	Failed logon	
	56448		13991	13991	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56439		13990	13990	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	5	Failed logon	
	56438		13989	13989	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56437		13988	13988	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130))	Failed logon	
	56436		13987	13987	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56435		13986	13986	2021-05-30 14:01:57	7 4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130))	Failed logon	
	56434		13985	13985	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56433		13984	13984	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	F	Failed logon	
	56432		13983	13983	2021-05-30 14:01:57	7 4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56431		13982	13982	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56430		13981	13981	2021-05-30 14:01:57	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130	1	Failed logon	
	56429		13980	13980	2021-05-30 14:01:56	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56428		13979	13979	2021-05-30 14:01:50	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56427		13978	13978	2021-05-30 14:01:56	5 4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56426		13977	13977	2021-05-30 14:01:56	5 4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	
	56425		13976	13976	2021-05-30 14:01:56	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	(Failed logon	
	56424		13975	13975	2021-05-30 14:01:50	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)		Failed logon	
	56423		13974	13974	2021-05-30 14:01:50	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	4	Failed logon	
	56422		13973	13973	2021-05-30 14:01:50	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	62	4 CLIENT-ALICE.2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	4	Failed logon	
	56421		13972	13972	2021-05-30 14:01:56	4625 LogAlway	s Microsoft-Windows-Security-Auditi	ng Security	.62	4 CLIENT-ALICE. 2CONSULT	LogonType 3	WORKSTATION (192.168.180.130)	1	Failed logon	100

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