

Raport 12: Wybrane artefakty użytkownika

Wstęp

To laboratorium ma na celu zapoznanie się z niektórymi artefaktami użytkownika, sposobami wyszukiwania tych informacji z użyciem programu Autopsy. Ponadto stanowi ono pewną (bardzo przybliżoną) symulację pracy analityka, którego zadaniem jest odpowiedzenie na konkretne pytania dotyczące zebranych materiałów cyfrowych.

1 Wprowadzenie do historii

organizacji wyciekły poufne dokumenty, co naraża firmę na ogromne straty. W ramach działań wyjaśniających skonfiskowany został komputer podejrzanego pracownika. Twoim zadaniem jest przeanalizowanie obrazu dysku i dostarczenie informacji potrzebnych do dalszego śledztwa. Ze względu na to, że jest to Twoja pierwsza sprawa otrzymasz też kilka wskazówek.

2 Krok zero – przygotowanie obrazu i analiza w Autopsy

Po etapie konfiguracji środowiska powinniśmy dysponować zarówno programem Autopsy jak i rozpakowanym obrazem dysku. Na początku musimy:

1. Otworzyć nową sprawę w Autopsy.
2. Dodać nasz obraz do Autopsy jako źródło danych
3. Na etapie dodawania będziemy mogli także wybrać jakie moduły analizujące chcemy uruchomić. Na nasze potrzeby wystarczą:
 - Recent Activity
 - File Type Identification
 - Extension Mismatch Detection
 - Embedded File Parser
 - Picture Analyzer
 - Email Parser.
4. Po uruchomieniu analizy będziemy mogli obserwować jej postęp w prawym dolnym rogu – może ona chwilę zająć, przed rozpoczęciem dalszej pracy musimy poczekać aż się zakończy. Jeśli będą pojawiały się problemy to można spróbować uruchamiać każdy moduł osobno klikając prawym przyciskiem myszy na źródle danych i wybierając Run ingest modules .

3 Krok pierwszy – wiadomości e-mail

Zacznijemy od sprawdzenia korespondencji mailowej podejrzanego pracownika, ponieważ jest to jedno z miejsc, w których mogły prawdopodobnie zostać potencjalne ślady przestępstwa. W związku z tym spróbuj odpowiedzieć na następujące pytania:

- Czy w wiadomościach mailowych na skonfiskowanym komputerze znajduje się jakakolwiek podejrzana korespondencja?

- Czy pracownik przysyłał jakieś załączniki za pomocą maila?

Odpowiedź: Duża część analizowanych wiadomości email jest co najmniej podejrzana. W wiadomościach możemy napotkać na dowody przestępstw cyfrowych, wiadomości nakazujące usuwanie po sobie śladów, wiadomości na temat nielegalnych logowań z nieautoryzowanych urządzeń, czy też wiadomości ukazujące wskazówki ukrycia pewnych typów danych. Pracownik przesłał 4 załączniki za pomocą maila, które zostały umieszczone na dole w tabeli.

Podejrzana korespondencja

Treść maili jest nieco obszerna dlatego, dane zostały umieszczone w dwóch tabelach. W jednej znajdują dane dotyczące tematu maila i jej treści, natomiast w drugiej znajdziemy temat maila, e-mail adresata oraz datę przesłania wiadomości. Maile są umieszczone według daty przesłania maila. W tabeli znalazły się tylko maile wzbudzające pewne podejrzenia.

Temat maila	Treść
New sign-in from Chrome on Linux	New sign-in from Chrome on Linux Hi EH, Your Google Account ehptmsgs@gmail.com was just used to sign in from Chrome on Linux. EH Techniques ehptmsgs@gmail.com Linux Tuesday, June 21, 2016 2:00 AM (Eastern European Summer Time) Jordan* Chrome (...) *The location is approximate and determined by the IP address it was coming from.
Your recovery email address changed	Your recovery email address changed Hi EH, The recovery email for your Google Account ehptmsgs@gmail.com was recently changed. Don't recognize this activity? Review your recently used devices now. (...)
New sign-in from Chrome on Windows	New sign-in from Chrome on Windows Hi EH, Your Google Account ehptmsgs@gmail.com was just used to sign in from Chrome on Windows. EH Techniques ehptmsgs@gmail.com Windows Tuesday, June 21, 2016 2:09 AM (Eastern European Summer Time) Jordan* Chrome (...) *The location is approximate and determined by the IP address it was coming from.
How to add contacts and start communicating at Sky	"e-mail powitalny dla nowego konta Skype w języku arabskim"
Re: TeamViewer	Okay, looking forward to that. On Mon, Jun 20, 2016 at 5:56 PM, Linux rul3z > wrote: Hello Hunter, I am currently at work. Let us meet after I finish work. I will ping you on Skype Thanks _____ From: ehptmsgs@gmail.com Date: Mon, 20 Jun 2016 17:53:13 -0700 Subject: TeamViewer To: linux-rul3z@hotmail.com Hello there, I just wanted to confirm the installation of Team Viewer as requested. When can we continue our discussion? Regards, Hunter

Pics	Hello, Attached is a 7z archive of some of the pictures I told you about. The password will be given to you using Skype :D Regards, Hunter
DNS Exfil Videos	Some Exfil videos you might want to check: https://www.youtube.com/watch?v=dYypZG6ueEY https://www.youtube.com/watch?v=AYpPOih64dY https://www.youtube.com/watch?v=eHjMJ9hnDC0 https://www.youtube.com/watch?v=UVYnVELzJk4 https://www.youtube.com/watch?v=7usXIUvIx2U https://www.youtube.com/watch?v=iokzWGWitws Happy hunting Hunter :)
New sign-in from Windows	New sign-in from Windows Hi EH, Your Google Account ehptmsgs@gmail.com was just used to sign in on Windows. EH Techniques ehptmsgs@gmail.com Windows Tuesday, June 21, 2016 4:54 AM (Eastern European Summer Time) Jordan* (...) *The location is approximate and determined by the IP address it was coming from.
Re: File Extensions	Check this :) On Mon, Jun 20, 2016 at 6:57 PM, EH Techniques > wrote: I will try that. Wait a minute. On Mon, Jun 20, 2016 at 6:57 PM, Linux rul3z > wrote: Hello Hunter, One of the basic techniques that could be used to disguise files, is to change their file extension. Check changing the extension of a PDF file and see :) Good luck... -- Regards, Hunter -- Regards, Hunter
Hangouts?	Hello, Got this email of yours. Lets connect using hangouts, ok? -- Regards, Hunter
Nice Pics	Hello, Just wanted to share these nice pics with you. Let me know if you liked them :D -- Regards, Hunter
Re: DNS Exfil Videos	Ok I will remove them now. I will wipe all those folders and info. On Tue, Jun 21, 2016 at 4:56 AM, Linux rul3z > wrote: No don't do that. It is bad and you will get detected! _____ From: ehptmsgs@gmail.com Date: Tue, 21 Jun 2016 04:51:04 - 0700 Subject: Re: DNS Exfil Videos To: linux-rul3z@hotmail.com Thank you ... I saved them for later watching. I must finish what I have now. On Mon, Jun 20, 2016 at 6:04 PM, Linux rul3z > wrote: Some Exfil videos you might want to check: https://www.youtube.com/watch?v=dYypZG6ueEY https://www.youtube.com/watch?v=AYpPOih64dY https://www.youtube.com/watch?v=eHjMJ9hnDC0 https://www.youtube.com/watch?v=UVYnVELzJk4 https://www.youtube.com/watch?v=7usXIUvIx2U https://www.youtube.com/watch?v=iokzWGWitws Happy hunting Hunter :) -- Regards, Hunter -- Regards, Hunter
Network Design	Hello, I have attached a sample of a network design. Is this what you need in order to understand our network and stuff? Please let me know as soon as possible. Can't wait to continue :D -- Regards, Hunter

Re: Network Design	Yes! Try to get the original print for your network. We need to know what systems, apps, tools, appliances are being used. Okay? Do your homework, and I will finish from there ;) On Tue, Jun 21, 2016 at 12:19 PM, EH Techniques > wrote: Hello, I have attached a sample of a network design. Is this what you need in order to understand our network and stuff? Please let me know as soon as possible. Can't wait to continue :D -- Regards, Hunter
Sign-in attempt prevented	Sign-in attempt prevented Hi EH, Someone just tried to sign in to your Google Account ehptmsgs@gmail.com from an app that doesn't meet modern security standards. Details: Tuesday, June 21, 2016 3:59 PM (Eastern European Summer Time) Jordan* (...) *The location is approximate and determined by the IP address it was coming from.
Synchronization Log:	6:07:07 Synchronizer Version 15.0.4569.1505 6:07:07 Synchronizing Mailbox 'ehptmsgs@gmail.com' 6:07:07 Synchronizing Hierarchy 6:07:35 Error in folder 'Inbox' 6:07:35 [800CCC0E-0-0-733] 6:07:35 Terminated in error 6:07:35 [800CCC0E-0-0-733]
Access for less secure apps has been turned on	Access for less secure apps has been turned on Hi EH, You recently changed your security settings so that your Google Account ehptmsgs@gmail.com is no longer protected by modern security standards. Please be aware that it is now easier for an attacker to break into your account. You can make your account safer again by undoing this change here, then switching to apps made by Google such as Gmail to access your account. (...)
Microsoft Outlook Test Message	This is an e-mail message sent automatically by Microsoft Outlook while testing the settings for your account.
Synchronization Log:	6:13:07 Synchronizer Version 15.0.4569.1505 6:13:07 Synchronizing Mailbox 'ehptmsgs@gmail.com' 6:13:07 Synchronizing local changes in folder 'Inbox' 6:13:09 2 item(s) updated in online folder 6:13:09 2 item(s) changed read-state in online folder 6:13:09 Error synchronizing folder 6:13:09 [80040109-0-0-560] 6:13:09 Done

	E-mail adresata	Data przesłania
Temat maila		
New sign-in from Chrome on Linux	ehptmsgs@gmail.com	2016-06-21 01:01:05 CEST
Your recovery email address changed	ehptmsgs@gmail.com	2016-06-21 01:01:29 CEST
New sign-in from Chrome on Windows	ehptmsgs@gmail.com	2016-06-21 01:09:34 CEST

How to add contacts and start communicating at Sky	ehptmsgs@gmail.com	2016-06-21 01:16:38 CEST
Re: TeamViewer	linux-rul3z@hotmail.com	2016-06-21 02:53:13 CEST
Pics	linux-rul3z@hotmail.com	2016-06-21 03:00:31 CEST
DNS Exfil Videos	ehptmsgs@gmail.com	2016-06-21 03:04:45 CEST
New sign-in from Windows	ehptmsgs@gmail.com	2016-06-21 03:54:21 CEST
Re: File Extensions	linux-rul3z@hotmail.com	2016-06-21 03:57:53 CEST
Hangouts?	linux4rulez@gmail.com	2016-06-21 13:32:14 CEST
Nice Pics	linux-rul3z@hotmail.com, linux4rulez@gmail.com	2016-06-21 13:50:24 CEST
Re: DNS Exfil Videos	linux-rul3z@hotmail.com	2016-06-21 13:56:39 CEST
Network Design	linux-rul3z@hotmail.com, linux4rulez@gmail.com	2016-06-21 14:19:33 CEST
Re: Network Design	ehptmsgs@gmail.com	2016-06-21 14:27:34 CEST
Sign-in attempt prevented	ehptmsgs@gmail.com	2016-06-21 14:59:04 CEST
Synchronization Log:	ehptmsgs@gmail.com	2016-06-21 15:07:35 CEST
Access for less secure apps has been turned on	ehptmsgs@gmail.com	2016-06-21 15:12:20 CEST
Microsoft Outlook Test Message	ehptmsgs@gmail.com	2016-06-21 15:12:22 CEST
Synchronization Log:	ehptmsgs@gmail.com	2016-06-21 15:13:09 CEST

Wszystkie wiadomości e-mail pochodzą z pliku /img item-10x1.E01/Users/Hunter/Documents/Outlook Files/backup.pst.

Analiza załączników

Nazwa załącznika	E-mail adresata	Data przesłania	Komentarz
Pictures.7z 1	linux-rul3z@hotmail.com	2016-06-21 03:00:31 CEST	Pracownik przesyła archiwum 7z zabezpieczone hasłem, które ma zostać wysłane przez Skype'a
Conf.jpg	linux-rul3z@hotmail.com	2016-06-21 04:01:17 CEST	Zostaje przesłany plik pdf z rozszerzeniem zmienionym na jpg
fakeporn.7z	linux-rul3z@hotmail.com linux4rulez@gmail.com	2016-06-21 13:50:24 CEST	Przesłane zostaje archiwum 7z zabezpieczone hasłem
home-network-design - networking-for-a-	linux-rul3z@hotmail.com	2016-06-21 14:19:33 CEST	Przesłany zostaje schemat sieci biurowej

single -family-home-case-house - arkko-1433-x-792.jpg	linux4rulez@gmail.com		
---	-----------------------	--	--

Źródłem wszystkich załączników i wiadomości e-mail jest plik /img item10x1.E01/Users/Hunter/Documents/Outlook Files/backup.pst.

Wnioski:

Na podstawie przeanalizowanych maili można stwierdzić, że doszło do popełnienia przestępstwa cyfrowego. Komunikacja pracownika z osobą z zewnątrz trwała około 1 dnia. Pracownik zainstalował program TeamViewer, który służy do zdalnego obsługiwanie komputera. Komunikacja następowała też przez Skype i Hangouts. W załącznikach do maili możemy znaleźć np. linki do filmów na Youtube oraz archiwa chronione hasłem czy też schemat sieci biura. Przestępstwo, którego dopuścił się pracownik to przede wszystkim udostępnianie poufnych danych firmy. Dalsze wnioski zostaną wysunięte na podstawie analizy artefaktów z programu Skype.

4 Krok drugi – rozmowy Skype

W poprzednim kroku w wiadomościach mailowych znaleźliśmy fragment prowadzący nas do rozmów przeprowadzanych za pośrednictwem Skype (jeśli tego nie odkryłeś spróbuj jeszcze raz przeanalizować wiadomości mailowe). W związku z tym chcielibyśmy dokonać analizy danych aplikacji Skype. Niestety Autopsy nie ma funkcjonalności przetwarzającej dane Skype. W związku z tym musimy do tego podejść trochę bardziej ręcznie. Aby to zrobić potrzebujemy dowiedzieć się gdzie i jakie dane przechowuje Skype – możemy zacząć od wpisania w Google frazy „Skype forensic”. Stąd możemy trafić na stronę:

<https://www.dataforensics.org/skype-forensic-analysis/>.

Zgodnie ze znalezionymi instrukcjami zaczynamy od znalezienia na dysku pliku File main.db – powinien się on znajdować pod taką ścieżką:

\\Users\\UserName\\AppData\\Roaming\\Skype\\SkypeUserName\\main.db. Odnaleziony plik File main.db to plik sqlite – prosta baza danych (ten typ plików został omówiony na wykładzie). Autopsy na szczęście dostarcza możliwość analizowania danych znajdujących się w takich plikach. Po otwarciu poglądu tego pliku w Autopsy w zakładce ”Application” będziemy mogli przeglądać zawartość różnych tabel znajdujących się w bazie (ich zawartość jest opisana w znajdującym się powyżej linku). Nas będzie interesować tabela zawierająca wiadomości – Messages, a przede wszystkim kolumny: author, dialog_partner, bodyxml oraz timestamp. Przeglądnij wszystkie wiadomości, a następnie korzystając z Autopsy posortuj je po dacie (timestamp) oraz wyeksportuj te kolumny do pliku csv.

Rozmowy wyeksportowane do csv:

[illegible]

author	dialog_partner	timestamp	body_xml
hunterehpt		1466469388	Hi Linux rul3z, I'd like to add you as a contact. I need your help with Data Exfiltration. Regards, Hunter
linux-rul3z	linux-rul3z	1466469408	
hunterehpt	linux-rul3z	1466469416	hello
linux-rul3z	linux-rul3z	1466469422	hello
hunterehpt	linux-rul3z	1466469457	I have some pics that need to send outside my network
hunterehpt	linux-rul3z	1466469474	but the problem is that our network is monitored
hunterehpt	linux-rul3z	1466469512	I need to bypass their censorships
hunterehpt	linux-rul3z	1466469533	also I need to get access to documents and send them
hunterehpt	linux-rul3z	1466469544	so I am asking for your help
linux-rul3z	linux-rul3z	1466469550	hmm
linux-rul3z		1466469556	what kind of pics?
linux-rul3z	linux-rul3z	1466469570	and what is the type of docs u need to send outside?
hunterehpt	linux-rul3z	1466469582	the pics are something special
hunterehpt	linux-rul3z	1466469603	some of the docs are for products
hunterehpt	linux-rul3z	1466469616	others are for other misc stuff
linux-rul3z		1466469630	no worries
linux-rul3z	linux-rul3z	1466469655	let us work on them separately
hunterehpt	linux-rul3z	1466469663	what do you mean?
linux-rul3z	linux-rul3z	1466469675	I mean, let us first find away to access your device
linux-rul3z	linux-rul3z	1466469691	and then, see what can we do in order to exfil the docs/pics outside ur network
hunterehpt	linux-rul3z	1466469693	ok
hunterehpt	linux-rul3z	1466469697	that sounds great
hunterehpt	linux-rul3z	1466469703	but is this truly doable?
linux-rul3z		1466469707	there is no limits
linux-rul3z		1466469711	sure it is <ss type="wink">-)</ss>
hunterehpt	linux-rul3z	1466469719	when shall we start

5 Krok trzeci – przeglądane strony

Przy przeszukiwaniu korespondencji mailowej trafiliśmy też na maila z linkami do filmów na YouTube (jeśli tego nie pamiętasz lub wcześniej nie zauważyłeś – przeglądaj jeszcze raz wiadomości mailowe). Teraz chcielibyśmy znaleźć odpowiedzi na pytania:

W historii przeglądania/wyszukiwania znalazło się wiele stron powiązanych w hasłem „eksfiltracja” (lub „exfil”), co jest kolejnym dowodem na złamanie prawa przez pracownika.

- Czy użytkownik oglądał na YouTube jakieś filmy związane z eksfiltracją?

Użytkownik obejrzał na Youtube jeden film powiązany z eksfiltracją.

Odwiedzone strony, które są podejrzone:

Adres strony	Data wizyty na stronie	Tytuł lub krótki opis strony
Google Image Result for http://www.filetransferconsulting.com/wp-content/uploads/2014/07/Exfiltration_Diagram.png	2016-06-21 11:37:09 CEST	data exfiltration - research
http://image.slidesharecdn.com/phdays-2012-miroslavstampar-dnsexfiltrationusingsqlmap-slides-120619030857-phpapp02/95/dns-exfiltration-using-sqlmap-18-728.jpg?cb=1340075384	2016-06-21 11:37:16 CEST	data exfiltration - research
https://www.google.jo/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&ved=0ahUKEwjB5d_34rfNAhVBmBoKH aF1DKoQjBwIBA&url=http%3A%2F%2Fwww.filetransferconsulting.com%2Fwp-content%2Fuploads%2F2014%2F07%2FExfiltration_Diagram.png&psig=AFQjCNHY4yTmq-jcahffslBwOl4lJ7qP4Q&ust=1466552230722116	2016-06-21 11:37:30 CEST	data exfiltration - research
https://www.google.jo/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj_tcT_4rfNAhXDyRoKHxg3CQEQQFggdMAA&url=http%3A%2F%2Fabout-threats.trendmicro.com%2Fcloud-content%2Fus%2Fent-primers%2Fpdf%2Fhow_do_threat_actors_steal_your_data.pdf&usg=AFQjCNEp0x-JVXIcVhcMvy11usXOSQE_ng&sig2=SZLlhyzBUGIPrplV3rAclw&bvm=bv.124817099,d.d2s	2016-06-21 11:39:15 CEST	data exfiltration - research
https://www.google.jo/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwj_tcT_4rfNAhXDyRoKHxg3CQEQQFggdMAI&url=http%3A%2F%2F	2016-06-21 11:39:25 CEST	data exfiltration - research
https://www.google.jo/webhp?sourceid=chrome-	2016-06-21 11:43:52 CEST	Data about hacking

instant&ion=1&espv=2&ie=UTF-8#q=hacking		
How to bypass strict firewalls on public wifi hotspots and restricted networks, by tunneling blocked ports and protocols - verot.net	016-06-21 01:56:15 CEST	bypassing firewalls
https://www.google.jo/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=bypass+firewall&start=10	2016-06-21 01:56:19 CEST	bypassing firewalls
TeamViewer Windows Download	2016-06-21 02:51:50 CEST	TeamViewer - download

Odwiedzane strony pozyskano z pliku /img item-10x1.E01/Users/Hunter /AppData/Local/Google/Chrome/User Data/Default/History.

Wyszukiwane frazy

Wyszukiwana fraza	Data wyszukiwania
exfiltration	2016-06-21 11:37:01 CEST
data exfiltration	2016-06-21 11:37:10 CEST
exfiltration	2016-06-21 11:37:19 CEST
How to exfiltrate data	2016-06-21 11:37:26 CEST
data exfiltration	2016-06-21 11:38:06 CEST
DNS Exfiltration Using sqlmap	2016-06-21 11:38:17 CEST
Data Exfiltration in Depth	2016-06-21 11:39:04 CEST
Detecting & Deterring Data Exfiltration	2016-06-21 11:39:21 CEST
dns data exfiltration	2016-06-21 11:39:33 CEST
hacking	2016-06-21 11:43:54 CEST Ta fraza była wyszukiwana ponad 10 razy po godzinie 11:43:54
9 Easy Ways to Bypass a Firewall or Internet Filter	2016-06-21 01:56:03 CEST
network design	2016-06-21 14:17:59 CEST

Wszystkie wyszukiwania pochodzą z pliku /img item-10x1.E01/Users/Hunter /AppData/Local/Google/Chrome/User Data/Default/History.

Odwiedzone filmy:

Adres filmu	Data wizyty na YouTube	Tytuł filmu
https://www.youtube.com/watch?v=dYypZG6ueEY	2016-06-21 13:50:19 CEST	DEFCON 16: New Tool for SQL Injection with DNS Exfiltration - YouTube

Dane odnośnie filmu użyksano z plki/img item-10x1.E01/Users/Hunter /AppData/Local/Google/Chrome/User Data/Default/History

6 Krok czwarty – pliki posiadający niezgodne typy

We wcześniej przejranych rozmowach na Skype widzieliśmy, że podejrzanemu pracownikowi zostało zalecona zmiana rozszerzenia plików, które chce przesłać, na jpg. W związku z tym odpowiedz na poniższe pytanie:

- Czy na zabezpieczonym dysku znajdują się pliki pdf, których rozszerzenie zostało zmienione na jpg?

Tak, znaleziono na dysku pliki pdf, których rozszerzenie zostało zmienione na jpg:

Podejrzane pliki:

Nazwa pliku	Ścieżka do pliku na dysku
Conf.jpg	/img item-10x1.E01/Users/Hunter/Dropbox/Outlook/backup.pst/Conf.jpg
Conf.jpg	/img item-10x1.E01/Users/Hunter/Documents/Conf.jpg
Conf.jpg	/img item-10x1.E01/Users/Hunter/Documents/Outlook Files/backup.pst/Conf.jpg