

Referentie/Documentnummer: 002

Betreft: onderzoek data ten behoeve van digitaal onderzoek

Datum: 25-4-2024

Rapporteur: [REDACTED] Ivan [REDACTED]

Bevindingen Windows

De image is gebruikt die in het document ICT.AIS.ITF_rapportage_veiligstellen is gemaakt, de image is gekopieerd om het origineel te bewaren. Met FTK Imager 4.7.1.2 zien wij bij het uitvouwen van de image dat er naast de root map een [unallocated space] map staat. Na het verkennen van de image met FTK Imager, vonden we een verdachte map genaamd 'backup', waarin een submap genaamd '1t\$m3' zat, vermoedelijk gerelateerd aan het bedrijf in kwestie. Binnen deze map ontdekten we een submap met de naam 'caebe68d-065d-445d-a944-41955d23e0db', waarin zich een aantal cruciale bestanden bevonden.

Het bestand 'data.science.txt' leek een telefoonnummer te bevatten, '0651423256'. Daarnaast troffen we een gecomprimeerd bestand aan genaamd 'company_export.db.sql.tar.bz2', wat hoogstwaarschijnlijk een SQLite-database bevatte. Na het uitpakken met behulp van DB Browser for SQLite version 3.12.2 met SQLite Version 3.35.5 bleek dit inderdaad het geval te zijn, met een aanzienlijke hoeveelheid persoonsgegevens in de tabel 'personeel', inclusief wachtwoorden. Er was ook een tabel genaamd 'sqlite_sequence', waarvan de ID overeenkwam met een ID van een rij in de 'personeel' tabel. De betreffende rij bevatte vermoedelijk de persoonsgegevens en het wachtwoord van Mr. Wallet, dit is de naam weergegeven in de betreffende rij.

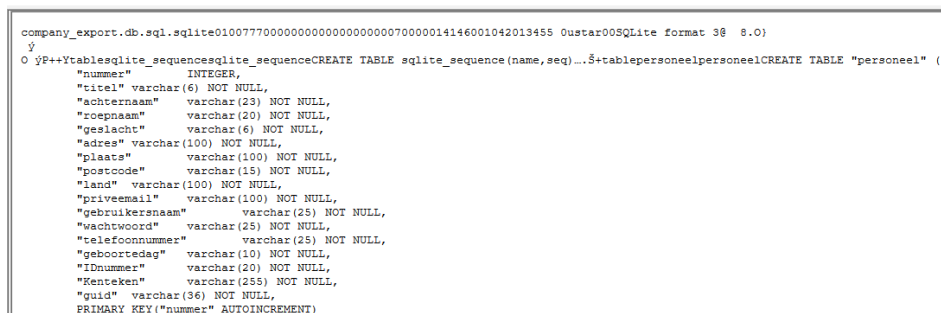
Een ander opvallend bestand was 'allebestanden.zip' in de map '2ba99e82-1946-435f-ad8a-239bb5241f94', vermoedelijk beschermd met een wachtwoord. De bestanden zijn encrypted, daarentegen zijn de bestandsnamen en extensies wel te zien. De volgende bestands extensies zijn wij tegengekomen: html, doc, pdf, ppt, xls, tekst, jpg, gif.

Binnen de 'hacking' map stuitte we op een verwijderd bestand genaamd 'ZAP_2_11_0_windows.exe', dat mogelijk verband houdt met beveiligingsscanners.

Daarnaast werden verschillende andere mappen aangetroffen, waaronder 'Vakantie2020', waarin zich jpg-bestanden bevonden die vermoedelijk afbeeldingen van een vakantie voorstelden. 'Bitcoin' bevatte PDF-bestanden, zoals "02 2019-1097-Anonymous Transactions with Revocation and Auditing in Hyperledger Fabricen.pdf" welke vermoedelijk van Boston University is.


Een map genaamd 'Downloads' bevatte een bitcoin-22.0-x86_64-linux-gnu.tar.gz bestand, waarin we een 'Readme.md' en een 'Bin' map aantreffen welke vermoedelijk een bitcoin wallet erin had, vanwege het bestand genaamd 'bitcoin-wallet' in deze map. De 'includes' map bevat vermoedelijke scripts.


De 'Fake' map bevatte een verwijderd bestand en een e-mail.




Figuur 2, Company_export.db.sql.tar bestand.

RAPPORTAGE INZAKE IT FORENSISCH ONDERZOEK

Table: **personeel** 


 **personeel**

 **sqlite_sequence**

Figuur 3, Tabellen binnen het vermoedelijk SQLite bestand.

























	postcode	land	privemail	gebruikersnaam	wachtwoord	telefoonnummer	geboortedag	IDnummer	Kenteken	guid
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	8274 AH	Netherlands	MaryantSenia@fleckens.hu	Plefuspritr	zie0eXc3	06-68298955	5/12/1984		2001 Opel Meriva	03793705-208a-458f-9c8a-5d3ac52339e5
2	1422 LB	Netherlands	ReyhanDiepenhorst@rhyta.com	Hicuregary	Oithuha9j	06-91422582	4/7/1961		2007 Ford Five Hundred	a74a0f10-758b-4d3c-acac-8d292b6cec72
3	9298 RV	Netherlands	ImreVoorneveld@rhyta.com	Sitherad	phohGh2Chai	06-89154239	10/6/1962		2005 Audi A4	2ed17558-ecb6-4834-9abd-6fcc4af59fbc
4	1945 NG	Netherlands	EcomOphorst@dayrep.com	Culd1985	Biefee1alei	06-41759288	11/11/1985		1994 Ferrari 512 TR	de613bc7-b9b4-4892-e41e-26a99d9d8121
5	4834 XK	Netherlands	MarisDiallo@rhyta.com	Vinter	veilNu9Tiep	06-27373730	12/5/1974		2009 Renault Modus	564559ae-0926-4a41-a845-eedca82177d7
6	3081 XP	Netherlands	MetehanBaker@armyspy.com	Evisshade	Aebae4koosae	06-75131937	12/26/1972		2001 Nissan GT-R	68a41b46-8871-46b6-8747-c7a98a64840d
7	1964 HH	Netherlands	SiljaGeilen@einrot.com	Vagind1972	hiaSoo6oor	06-16912764	2/27/1972		1998 Ford Ranger	ddffdd87-bda3-4ffc-b14e-a5578dffdb9e
8	4191 KV	Netherlands	PascalevanderHoef@rhyta.com	Yunchants	ohK0ahmie	06-55705247	7/14/1994		1995 Infiniti Q45	8c3f4443-712a-4462-a2e4-ee7a75d87cd6
9	3768 AE	Netherlands	AntoonMeppelink@armyspy.com	Lingovensids	Aboo8ith	06-73505448	9/20/1954		1993 Oldsmobile Achieva	7f2ed889-16c2-436e-9eb0-ebf2fa5f269b
10	3818 GT	Netherlands	DeaconHorst@fleckens.hu	Leng1961	LaFeilleeva9	06-95068666	10/30/1961		1998 Lotus GT 1	c73b62ba-537f-4d98-92a1-27e5baf3a576
11	6662 EA	Netherlands	SyNijgh@fleckens.hu	Tonlefor	reicoeo6O	06-63400240	5/17/1985		2014 Audi S8	98c3dead-1bca-4bcd-8a15-ceae937cb21e
12	1452 PE	Netherlands	CarlynHommes@armyspy.com	Sampriscrom	ahth3Eiquoa	06-64476226	8/4/1977		2003 Buick Rendezvous	8b498f73-303e-4346-969d-c9aaf297665d
13	7462 HP	Netherlands	ShauniSchakelaar@fleckens.hu	Thouturs	tjae53hee	06-58553298	6/11/1979		1999 Buick Century	869ded0d-a2c6-4349-a00f-3dcab7dc7bea
14	6991 HL	Netherlands	FlynnKoeleman@dayrep.com	Ancess	Zeil2ohh	06-26806145	6/11/1960		2009 Subaru Outback Sport	08d2d4ed-734d-4c22-81c2-9387e69fee1c
15	6466 HG	Netherlands	LesleyWijman@armyspy.com	Recare	ohtaeYe4oor	06-12194269	6/15/1982		1996 GAZ 3110	b2765110-406b-40a5-b59a-21e25942fd95
16	2992 RA	Netherlands	NouryFriesen@einrot.com	Whissind	oa3ahChoh	06-11931483	8/24/1999		2010 Mercedes-Benz Vito	89f79110-2e85-4ef3-af6e-36676e7071f1
17	5665 ES	Netherlands	FerrieKoolhaas@rhyta.com	Crypedged	aeWu7kxhk	06-71709988	6/13/1978		2001 Oldsmobile Alero	1bdf39be-d5f9-495e-a9f9-d81adaf81b8c
18	2312 AH	Netherlands	JiaDoodeman@jourrapide.com	Youlp1967	ahcie4Eew	06-42288125	7/10/1967		1994 Ford Versailles	38e80a53-f48d-4139-a8b5-6f63e9d4cd7
19	6001 EN	Netherlands	DjonnoGrootenboer@jourrapide.com	Orlintands	Ush9eeju8	06-69966321	11/2/1972		1999 Daihatsu Sirion	b6bdbbc4-7d02-4895-b12e-7c8844371db9
20	6883 HK	Netherlands	LeontinaRibberink@einrot.com	Theamed	lGH2eetho8i	06-47254044	7/7/1962		2001 Cadillac Escalade	c17d6826-3924-4840-b7d8-cae39c72f8bd

Figuur 4, Vermoedelijk personeel persoonsgegevens.

Table: **sqlite_sequence** 

	name	seq
	Filter	Filter
1	personeel	16984

Figuur 5, SQLite_sequence tabel inhoud.

Name	Size	Type	Date Modified
 000001.doc	40	Regular File	15/11/2021 14:59:30
 000002.doc	57	Regular File	15/11/2021 14:59:30
 000003.doc	55	Regular File	15/11/2021 14:59:30
 000004.doc	172	Regular File	15/11/2021 14:59:30
 000005.doc	177	Regular File	15/11/2021 14:59:30
 000006.doc	66	Regular File	15/11/2021 14:59:30
 000007.doc	175	Regular File	15/11/2021 14:59:30
 000008.ppt	298	Regular File	15/11/2021 14:59:30
 000009.pdf	39	Regular File	15/11/2021 14:59:30
 000010.pdf	118	Regular File	15/11/2021 14:59:30
 000011.pdf	31	Regular File	15/11/2021 14:59:30
 000012.pdf	23	Regular File	15/11/2021 14:59:30
 000013.pdf	38	Regular File	15/11/2021 14:59:30
 000014.pdf	3,691	Regular File	15/11/2021 14:59:30
 000015.pdf	55	Regular File	15/11/2021 14:59:30
 000016.pdf	148	Regular File	15/11/2021 14:59:30
 000017.pdf	1,056	Regular File	15/11/2021 14:59:30
 000018.pdf	93	Regular File	15/11/2021 14:59:30
 000019.pdf	122	Regular File	15/11/2021 14:59:30
 000020.pdf	5	Regular File	15/11/2021 14:59:30
 000021.pdf	5	Regular File	15/11/2021 14:59:30
 000022.pdf	21	Regular File	15/11/2021 14:59:30
 000023.pdf	20	Regular File	15/11/2021 14:59:30
 000024.pdf	44	Regular File	15/11/2021 14:59:30

Figuur 6, Inhoud allebestanden.zip.

```
Bitcoin Core integration/staging tree
=====

https://bitcoincore.org

For an immediately usable, binary version of the Bitcoin Core software, see
https://bitcoincore.org/en/download/.

Further information about Bitcoin Core is available in the [doc folder] (/doc).

What is Bitcoin?
-----

Bitcoin is an experimental digital currency that enables instant payments to
anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate
with no central authority: managing transactions and issuing money are carried
out collectively by the network. Bitcoin Core is the name of open source
software which enables the use of this currency.

For more information read the original Bitcoin whitepaper.

License
-----

Bitcoin Core is released under the terms of the MIT license. See [COPYING] (COPYING) for more
information or see https://opensource.org/licenses/MIT.

Development Process
-----

The 'master' branch is regularly built (see 'doc/build-*.md' for instructions) and tested, but it is not guaranteed to be
completely stable. [Tags] (https://github.com/bitcoin/bitcoin/tags) are created
regularly from release branches to indicate new official, stable release versions of Bitcoin Core.

The https://github.com/bitcoin-core/gui repository is used exclusively for the
development of the GUI. Its master branch is identical in all monotree
repositories. Release branches and tags do not exist, so please do not fork
that repository unless it is for development reasons.

The contribution workflow is described in [CONTRIBUTING.md] (CONTRIBUTING.md)
and useful hints for developers can be found in [doc/developer-notes.md] (doc/developer-notes.md).
```

Figuur 7, Bitcoin-22.0 README.md file.

```

// Copyright (c) 2009-2010 Satoshi Nakamoto
// Copyright (c) 2009-2018 The Bitcoin Core developers
// Distributed under the MIT software license, see the accompanying
// file COPYING or http://www.opensource.org/licenses/mit-license.php.

#ifndef BITCOIN_SCRIPT_BITCOINCONSENSUS_H
#define BITCOIN_SCRIPT_BITCOINCONSENSUS_H

#include <stdint.h>

#if defined(BUILD_BITCOIN_INTERNAL) && defined(HAVE_CONFIG_H)
#include <config/bitcoin-config.h>
#if defined(_WIN32)
#if defined(HAVE_DLLEXPORT_ATTRIBUTE)
#define EXPORT_SYMBOL __declspec(dllexport)
#else
#define EXPORT_SYMBOL
#endif
#elif defined(HAVE_DEFAULT_VISIBILITY_ATTRIBUTE)
#define EXPORT_SYMBOL __attribute__((visibility("default")))
#endif
#elif defined(MSC_VER) && !defined(STATIC_LIBBITCOINCONSENSUS)
#define EXPORT_SYMBOL __declspec(dllimport)
#endif

#ifndef EXPORT_SYMBOL
#define EXPORT_SYMBOL
#endif

#ifdef __cplusplus
extern "C" {
#endif

#define BITCOINCONSENSUS_API_VER 1

typedef enum bitcoinconsensus_error_t
{
    bitcoinconsensus_ERR_OK = 0,
    bitcoinconsensus_ERR_TX_INDEX,
    bitcoinconsensus_ERR_TX_SIZE_MISMATCH,
    bitcoinconsensus_ERR_TX_DESERIALIZE,
    bitcoinconsensus_ERR_AMOUNT_REQUIRED,
    bitcoinconsensus_ERR_INVALID_FLAGS,
} bitcoinconsensus_error;

```

Figuur 8, Bitcoinconsensus.h vermodelijke bitcoin script.

```

.\" DO NOT MODIFY THIS FILE! It was generated by help2man 1.47.13.
.TH BITCOIN-CLI "1" "September 2021" "bitcoin-cli v22.0.0" "User Commands"
.SH NAME
bitcoin-cli \- manual page for bitcoin-cli v22.0.0
.SH SYNOPSIS
.B bitcoin-cli
[\fI\,options\/\fR] \fI\,<command> \/\fR[\fI\,params\/\fR] \fI\,Send command to Bitcoin Core\/\fR
.br
.B bitcoin-cli
[\fI\,options\/\fR] \fI\,-named <command> \/\fR[\fI\,name=value\/\fR]... \fI\,Send command to Bitcoin Core (with named arguments)\/\fR
.br
.B bitcoin-cli
[\fI\,options\/\fR] \fI\,help List commands\/\fR
.br
.B bitcoin-cli
[\fI\,options\/\fR] \fI\,help <command> Get help for a command\/\fR
.SH DESCRIPTION
Bitcoin Core RPC client version v22.0.0
.SH OPTIONS

```

Figuur 9, Vermoedelijk commando's voor bitcoin script.

```

Delivered-To: br_pro@gmail.com
Received: by 10.112.15.111 with SMTP id w15csp505741bc;
Tue, 20 May 2014 13:12:20 -0700 (PDT)
X-Received: by 10.66.182.69 with SMTP id ec5mr23877909pac.125.1400616739811;
Tue, 20 May 2014 13:12:19 -0700 (PDT)
Return-Path: <info@limberry.us>
Received: from p3plwbeout22-02.prod.phx3.secureserver.net (p3plsmtp22-02-2.prod.phx3.secureserver.net. [68.178.252.56])
by mx.google.com with ESMTP id bjl1si3218316pbb.77.2014.05.20.13.12.18
for <br_pro@gmail.com>;
Tue, 20 May 2014 13:12:19 -0700 (PDT)
Received-SF: none (google.com: info@limberry.us does not designate permitted sender hosts) client-ip=68.178.252.56;
Authentication-Results: mx.google.com;
spf=neutral (google.com: info@limberry.us does not designate permitted sender hosts) smtp.mail=info@limberry.us
Received: from localhost ([68.178.252.117])
by p3plwbeout22-02.prod.phx3.secureserver.net with bizsmtp
id 4LCH1o0032YkKj001LCHpw; Tue, 20 May 2014 13:12:17 -0700
X-SID: 4LCH1o0032YkKj001
Received: (qmail 32123 invoked by uid 99); 20 May 2014 20:12:17 -0000
Content-Type: multipart/mixed;
boundary="=_0e030a3e0a0974e8f278310a4a7de3ab"
X-Originating-IP: 41.151.128.162
User-Agent: Workspace Webmail 5.6.48
Message-Id: <20140520131215.a118017471fe6fce587e5957b36083d4.739d55bbd5.wbe@email22.secureserver.net>
From: <info@limberry.us>
To:
Subject: NEWYORKUK55/3XA87-2PYJACPUK***
Date: Tue, 20 May 2014 13:12:15 -0700
Mime-Version: 1.0

--=_0e030a3e0a0974e8f278310a4a7de3ab
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"

```

Figuur 10, Gegevens van een vermoedelijke mail.



15 Beaver Street, New York, NY 10004
 Ref: EAASL/941OYI/02/SHYN
 Batch: 12/25/0034
 WEB SITE: WWW.NYLOTTERY.NY.GOV

Attention: Email Account Holder

Congratulations!! Congratulations!!

Are you the correct owner of this email? If yes, then, be glad this day as the result of the New York Online Lotto and email address free-ticket draws of the 22nd, April 2014 Promotion Award has been released and we are glad to announce to you that your email address came out in the first category and entitles you to claim the sum of **\$1,500,000.00**.

It is a promotional Program to encourage the use of Microsoft and Internet Programs. Your email address was entered for the online draw on this free ticket number: **B55607545 6152** with reference number **UK/JA2C110P5** and Serial number **UK5365/3**, Batch number **XA87-2PY**, drew the lucky numbers: 13-20-24-27-33-39- **Bonus 06**. This subsequently won you the lottery in the 1st category i.e. matches 6 lucky numbers Plus Bonus number.

You have therefore been allocated to claim a total sum of **\$1,500,000.00 (One Million Five Hundred Thousand, United States Dollars.)** in cash is credited to file **UKPC/9080144308/05**. This is from a total cash prize of **\$5,250,000.00** Shared amongst the 1691 with (2) lucky winner in "1st" category.

This promotion was drawn based on email address as the key identification for setting up online accounts. All valid email addresses in the World Wide Web Draw used/participants for the online email promotion version were selected randomly via computer balloting from a global website collaboration with internet companies like eBay, pay pal, liberty reserve, and Google whom also built their systems and based their membership registration identity on email addresses supporting this computer draw system done by extracted email addresses from over 100,000 unions, associations, and corporate bodies and affiliated members to the National Lottery website and their advertisers listed online. This Online promotion takes place via virtual ticket balloting and it is done Bi-annually.

Please note that you're lucky winning ticket file and number falls within our European booklet representative office in Watford (UK) as indicated in your ballot played coupon. In view of this, your **\$1,500,000.00** would be released to you by our payment department.

Kindly provide following information urgently:

1. Full Name: 2. Email Address: 3. Age/Occupation: 4. Reference Number/Ticket Number: 5. Phone Number: 6. Country: 7. Date of draw

Contact our Fiduciary agents immediately to commence release of your lottery prize by providing details below.

Contact Person: Mr. James Morrison

E-mail: nylclaim@outlook.com, nylclaim@aol.co.uk

Sincerely,
 Teresa Marie

Controller General Copyright (c) 1994-2013 The US Lottery International Promotion Inc.
 All rights reserved. Terms of Service -Guideline 77635 476378 265867460.

Figuur 11, Vermoedelijk phishing mail, .eml bestand inhoud.

Logging Windows Analyse

Datum/tijd	Handeling/Observatie/Resultaat
30-4-2024 11:40	Evidence tree uitgevouwen, alle mappen in kaart gebracht
30-4-2024 11:41	Image verkennen
30-4-2024 11:54	company_export.db.sql.sqlite downloaden
30-4-2024 12:00	company_export.db.sql.sqlite verkennen met DB Browser for SQLite
30-4-2024 12:09	Verkennen allebestanden.zip
30-4-2024 12:22	Verkennen Vakantie2020
30-4-2024 12:30	Verkennen Bitcoin map
30-4-2024 12:32	Downloaden en inzien "02 2019-1097-Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric.pdf"
30-4-2024 12:40	Verkennen bitcoin-22.0-x86_64-linux-gnu.tar.gz
30-4-2024 13:10	Verkennen hacking map
30-4-2024 13:40	Verkennen fake map
30-4-2024 13:50	Downloaden en inzien eml bestand met mail app van Windows 11

Bevindingen Linux

De image is gebruikt die in het document ICT.AIS.ITF_rapportage_veiligstellen is gemaakt, de image is gekopieerd om het origineel te bewaren. Via python-imagemounter 3.1.0-2 en eza 0.18.13-1 de image verkend en hacking folder gevonden. Deze bevatte twee exe files welke beiden een naam bevatten die overeenkomt met veiligheidsscanner software-installatie. Ook bevatte deze folder een bestand genaamd ceseruces zonder file extensie in de naam. Deze file bevatte alleen dit mogelijk email adres: "securesec <at> yopmail".

In de 'backup' folder een folder aangetroffen genaamd '1t\$m3' oftewel its me. Hierin zat een folder genaamd caebe68d-065d-445d-a944-41955d23e0db. Deze folder bevatte twee bestanden, een data-science.txt bestand welke een nummer bevatte van '0651423256'. En een company_export.db.sql.tar.bz2, dit is vermoedelijk een gezippte sqlite bestand. Na het kopiëren hiervan en het uitpakken hiervan bevestigde dat het een werkende sqlite bestand is met een grootte hoeveelheid aan persoonsgegevens in de tabel 'Persoonsgegevens'.

Hier was het ook mogelijk om te filteren op guid, welke soortgelijke patroon bevatte als de eerdergenoemde folder. De database filteren op 'caebe68d-065d-445d-a944-41955d23e0db' resulteerde inderdaad in een resultaat. Omdat deze folder in de '1t\$m3'(its me) folder zat, is de usb stick dus vermoedelijk van de persoon uit de gefilterde guid: Clara Hoevers.

Twee andere folders in 'back-up' bevatte soortgelijke guid namen, deze guid gaven ook resultaat terug. In totaal zijn er 3 guids gevonden zo, Allemaal gelinked aan vermoedelijk 1 row met persoonsgegevens. De andere tabel genaamd 'sqlite_sequence' bevatte een nummer: 16984. Dit nummer linkte ook aan 1 row met persoonsgegevens.

In de folder genaamd '2ba99e82-1946-435f-ad8a-239bb5241f94' zit een wachtwoord beschermde vermoedelijke zipfile genaamd 'allebestanden.zip'. Geen wachtwoord dat behoorde aan de eerder gevonden rows wordt geaccepteerd.













Het wachtwoord in 'allebestanden.zip' is niet te kraken; "John the Ripper" brute-force algoritme heeft het niet kunnen kraken voor 18 uur. Alle wachtwoorden uit de sqlite bestand werken ook niet.

Clamav heeft geen malware gedetecteerd in de gehele image.

Foto's (indien van toepassing)

```
[root@kali ~]# fdisk -l /dev/sda1
[+] Mounting image ICA15C3_Image01 (1.001 using auto ...
affuse: error while loading shared libraries: libcrypt.so.1.1: cannot open shared object file: No such file or directory
affuse: error while loading shared libraries: libcrypt.so.1.1: cannot open shared object file: No such file or directory
[+] Mounted raw image [1/1]
Warning: Unable to open /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd read-write (Permission denied). /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd has been opened read-only.
Error: /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd: unrecognised disk label
Error: Unable to open /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd read-write (Permission denied). /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd has been opened read-only.
Error: /tmp/image_mounter_wmn9h9w/ICA15C3_Image01 (1).dd: unrecognised disk label
[+] Mounted volume 57.76 GiB @POS/MBR boot sector on /tmp/im_0_iv98avsp.
>>> Press [enter] to unmount the volume, or ^C to keep mounting...
```

Figuur 12, Mounting image

```
> z /tmp/im_0_2cdqft_7
> ll
drwxrwxrwx - root 10 nov 2021  backup
-rwxrwxrwx 1.3M root 2 sep 2021  CIS_Controls_v8_Guide.pdf
-rwxrwxrwx 710k root 5 sep 2021  CIS_Controls_v8_Mapping_to_SOC2_v21.08.xlsx
drwxrwxrwx - root 13 okt 2018  fake
-rwxrwxrwx 333k root 30 sep 2021  'Firefox Installer.exe'
drwxrwxrwx - root 8 nov 2021  hacking
-rwxrwxrwx 1.1k root 20 aug 2020  logon_without_pw_CH.crt
drwxrwxrwx - root 14 nov 2021  'System Volume Information'
-rwxrwxrwx 1.2M root 27 sep 2021  zero-trust-maturity-model.pdf
> z hacking
> ll
-rwxrwxrwx 224M root 8 nov 2021  burpsuite_community_windows-x64_v2021_9_1.exe
-rwxrwxrwx 22 root 8 nov 2021  ceseruces
-rwxrwxrwx 163M root 8 nov 2021  ZAP_2.11.0_windows.exe
```

Figuur 13, Verkenning gemounte image.

```
File: burpsuite_community_windows-x64_v2023_9_1.exe <BINARY>
```

Figuur 14, Header van eerste .exe bestand.

[illegible]

Figuur 15, Header van tweede .exe bestand.

```
> bat -A ceseruces
```

	File: ceseruces
1	securesec.<at>yopmail

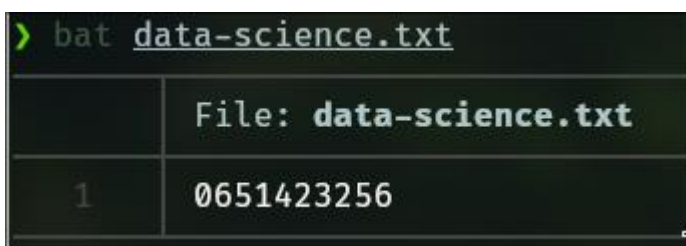
Figuur 16, ceseruces file inhoud.



Figuur 19, inhoud .eml bestand.



Figuur 20, folder inhoud.



Figuur 21, data-science bestand inhoud.

```
> ll
drwxrwxrwx - root 15 nov 2021 1t$m3
drwxrwxrwx - root 16 okt 2021 2ba99e82-1946-435f-ad8a-239bb5241f94
drwxrwxrwx - root 16 okt 2021 f0fa391f-b420-4fd3-afd9-f0ed1d56be52
> z 1t\$m3
> ll
drwxrwxrwx - root 15 nov 2021 caebe68d-065d-445d-a944-41955d23e0db
```

Figuur 22, guids als folder naam.

nummer	titel	achternaam	roepnaam	geslacht	adres	plaats	postcode	land	privemail	gebruikersnaam	wachtwoord	telefoonnummer	geboortedag	nummer	Kenteken	guid
1	1820	Mt.	Hoovers	Clara	female	Usselerweg 185	Enschede	7548 RZ	Netherlands	Clarahoovers@teleworm.us	Thentood76	up3a7Aph	06-29189467	4/21/1976	2012 Nissan Frontier	caebe68

Figuur 23, resultaat guid van folder naam in '1t\$m3'.

nummer	titel	achternaam	roepnaam	geslacht	adres	plaats	postcode	land	privemail	gebruikersnaam	wachtwoord	telefoonnummer	geboortedag	nummer	Kenteken	guid
1	358	Mt.	Rutgrok	Thije	male	Hen-Akker 25	Kaatsheuvel	5171 WR	Netherlands	ThijeRutgrok@dayrep.com	Selon1991	Dayrothlee	06-12553871	4/15/1991	1992 Buick Century	ca99e82-1946-435f-ad8a-239bb5241f94

Figuur 24, resultaat guid van tweede folder naam.

nummer	titel	achternaam	roepnaam	geslacht	adres	plaats	postcode	land	privemail	gebruikersnaam	wachtwoord	telefoonnummer	geboortedag	nummer	Kenteken	guid
1	1140	Mt.	Knigge	Wiebren	male	Blaauwweg 90	Dordrecht	3328 XN	Netherlands	Wiebrenknigge@teleworm.us	Kinnamny	Esoh3iek3	06-36644041	1/28/1960	2001 Proton Saloon	f0fa391f-b420-4fd3-afd9-f0ed1d56be52

Figuur 25, resultaat guid van derde folder naam.

Table: sqlite_sequence	
name	seq
Filter	Filter
1 personeel	16984

Figuur 26, inhoud 'sqlite_sequence' tabel.

nummer	titel	achternaam	roepnaam	geslacht	adres	plaats	postcode	land	privemail	gebruikersnaam	wachtwoord	telefoonnummer	geboortedag	nummer	Kenteken	guid
6084																
1	16984	Mt.	Walleit	Danië	male	Hub van der Cluizenstraat 157	Waalre	5581 CT	Netherlands	DanierWalleit@fleckens.hu	Fichave	ymn0Zu76i	06-32509958	10/2/1966	2006 Lexus SC	31fc791e-327f-48b6-8b8b-154f302148c3

Figuur 27, resultaat sequence filter nummer '16984'.

RAPPORTAGE INZAKE IT FORENSISCH ONDERZOEK

```

$ clamscan --recursive /tmp/im_0_iv98av9p
Loading: 6s, ETA: 0s [=====] 8.69M/8.69M sigs
Compiling: 1s, ETA: 0s [=====] 41/41 tasks

/tmp/im_0_iv98av9p/System Volume Information/WPSettings.dat: OK
/tmp/im_0_iv98av9p/System Volume Information/IdxrVolumeGuid: OK
/tmp/im_0_iv98av9p/backup/itlm3/caeb6e8d-0e5d-445d-a944-4195d23e0db/company_export.db.sql.tar.bz2: OK
/tmp/im_0_iv98av9p/backup/itlm3/caeb6e8d-0e5d-445d-a944-4195d23e0db/date-science.txt: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/documenten/allegebstanden.zip: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/vakantie2020/SLn5ACDj4yI.jpg: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/vakantie2020/9wgsViip524.jpg: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/vakantie2020/tc8PB6jUKDo.jpg: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/vakantie2020/WLzaZnXfno.jpg: OK
/tmp/im_0_iv98av9p/backup/2ba99e82-1946-435f-ad8a-239bb5241f94/vakantie2020_a6ERB7Nlfg.jpg: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/01 A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/02 2019-1897-Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/03 Blockchain technology for enhancing supply chain resilience.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/04 AICPA-implications-of-blockchain-web.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/05 Auditing Blockchain Solutions KPMG.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/06 Blockchain en assurance dec2019def NOREA.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/07 Blockchain-Framework-and-Guidance ISACA wbf6 res eng 1220(bram niet verspreiden).pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/08 Blockchainimpactauditingandaccounting_PermissionlessvsPermissioned.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/09 Permissioned Blockchains A Comparative Study.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/10 blockchain-maturity-model KPMG.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/11 enhancing due diligence in supply chain management kpmg C-2019-4-Antonovici.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/12 How Blockchain Enhances Supply Chain Management ASurvey.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/13 hyperledger fabric whitepaper.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/14 Toward a Policy-based Blockchain Agnostic Framework.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/15 internal-auditors-guide-to-blockchain Deloitte.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/16 Systemizing the Challenges of Auditing Blockchain-Based Assets AAA .pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/17 Norea presentatie blockchain.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/18 Audit-Programs_joa Eng 0717.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/19 Hyperledger-Fabric-2.0-Architecture-Security-Report.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/20 Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance (1).pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/21 Auditing and Examining Blockchain 10-1188 978-1-83982-198-120211027.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/22 Blockchain and Accounting Governance Emerging Issues and Considerations for Accounting and Assurance Professionals .pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/23 Auditing Mutual Distributed Ledgers aka Blockchains 2017.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/24 designing_and_auditing_accounting_systems_based_on_blockchain_and_dsl_principles.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/25 Asante et al Distributed Ledger Technologies 2021.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/26 An ISM Modeling of Barriers for BlockchainDistributed.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/27 Governance and control in distributed ledgers.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/28 Risks and Opportunities for Systems using blockchain and Smart Contracts by Data 61.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/29 gartner 3869088-evaluating-the-security-risks-to-blockchain-ecosystems.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/30 C-2019-4-Weerd.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/31 DBC-Cyber-Security-Framework-Final.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/bitcoin/32 2018-10-26-conceptualising-dlt-systems.pdf: OK
/tmp/im_0_iv98av9p/backup/f0fa391f-b420-4fd3-afd9-f0ed1d5b6e52/Downloads/bitcoin-22.0-x86_64-linux-gnu.tar.gz: OK
/tmp/im_0_iv98av9p/hacking/c0reutils: OK
/tmp/im_0_iv98av9p/hacking/ZAP_2.11.0_windows.exe: OK
/tmp/im_0_iv98av9p/hacking/burpsuite_community_windows-x64_v2021_9.1.exe: OK
/tmp/im_0_iv98av9p/CIS Controls_v8_Guide.pdf: OK
/tmp/im_0_iv98av9p/CIS Controls_v8_Mapping to SOC2_v21.08.xlsx: OK
/tmp/im_0_iv98av9p/Firefox Installer.exe: OK
/tmp/im_0_iv98av9p/logon_without_pw.CH.crt: OK
/tmp/im_0_iv98av9p/zero-trust-maturity-model.pdf: OK

----- SCAN SUMMARY -----
Known viruses: 8692057
Engine version: 1.2.1
Scanned directories: 13
Scanned files: 52
Infected files: 0
Data scanned: 548.02 MB
Data read: 1628.57 MB (ratio 0.34:1)
Time: 47.137 sec (0 m 47 s)
Start Date: 2024:04:28 18:56:05
End Date: 2024:04:28 18:56:53

```

Figuur 28, Clamav scan resultaten.

	File: wachtwoorden.txt
1	wachtwoord
2	zie0eiXe3
3	Oithuha9j
4	phohGh2Chai
5	Biefee1alei
6	veiNu9Tiep
7	Aebae4koosae
8	hiaSoo6oor
9	ohK0ahmie
10	Aboo8ith
11	LaFeileeva9
12	reico060
13	ahth3Eiquoa
14	IjaeS3hee
15	Zeil2ohh
16	ohdaeYe4oor
17	oa3ahChoh
18	aeWu7kohk
19	ahcio4Eow

Figuur 29, Wachtwoorden lijst vanuit sqlite tabel 'Personeel'.

Logging Linux Analyse

Datum/tijd	Handeling/Observatie/Resultaat
27-4-2024 21:19	Begonnen download image file genaamd ICTAISc3_Image01.001 vanuit OneDrive
27-4-2024 21:38	Download image file klaar
27-4-2024 21:40	Image gemount
27-4-2024 21:41	Image verkent
27-4-2024 21:41	Header geprint van exe bestand genaamd "burpsuite_community_windows-x64_v2021_9_1.exe"
27-4-2024 21:50	Header geprint van exe bestand genaamd "ZAP_2_11_0_windows.exe"
27-4-2024 21:59	Bestand genaamd "ceseruces" inhoud geprint
27-4-2024 22:02	Folder genaamd "Fake" geopend en enige bestand genaamd "NEWYORKUK55_3XA87-2PYJACPUK____.eml" geprint
27-4-2024 22:14	Bestand genaamd 'Firefox Installer.exe' header geprint
27-4-2024 22:15-23:10	Rond gekeken en bitcoin folder en files bestudeerd
27-4-2024 23:14	Bestand genaamd "NEWYORKUK55_3XA87-2PYJACPUK____.eml" geopend en bestudeerd in Thunderbird
27-4-2024 23:25	In een van de onderliggende folders zipfile gevonden op wat lijkt een sqlite database
27-4-2024 23:26	Data-science.txt bestand inhoud geprint
27-4-2024 23:31	Sqlite bestand geopend in sqlitebrowser
27-4-2024 23:32	Telefoonnummer opgezocht in sqlitebrowser, geen resultaten
27-4-2024 23:51	Guid van folder naam gezocht, 1 resultaat gevonden.
27-4-2024 23:53	Guids screenshot gemaakt
28-4-2024 00:04	Guid van tweede folder naam gezocht, weer 1 resultaat gevonden
28-4-2024 00:09	Wachtwoord beveiligde zip bestand genaamd 'allebestanden.zip' in '2ba99e82-1946-435f-ad8a-239bb5241f94' geprobeerd te unzippen met wachtwoord verkregen uit de sqlite bestand, was verkeerd wachtwoord.
28-4-2024 00:14	Guid van derde folder naam gezocht, weer 1 resultaat gevonden
28-4-2024 00:16	Wachtwoord geprobeerd van hiervoor gevonden sqlite resultaat, gaf weer verkeerd wachtwoord aan.
28-4-2024 00:21	Tweede tabel genaamd 'sqlite_sequence' inhoud gevonden
28-4-2024 00:21	Resultaat sqlite_sequence gefilterd in 'Personeel' tabel, gaf 1 resultaat
28-4-2024 00:35	Brute-force algoritme 'John the Ripper' aangezet om 'allebestanden.zip' wachtwoord proberen te kraken.
28-4-2024 18:55	John stopgezet na 18h 17m 55s, gaf helaas geen resultaten.
28-4-2024 18:56	Clamav antivirus gestart om hele image te scannen.
28-4-2024 18:56	Clamav antivirus klaar, niks gevonden.
28-4-2024 20:01	In SqliteBrowser de 'personeel' tabel geëxporteerd naar csv.
28-4-2024 20:03	Via xsv alle wachtwoorden in "wachtwoorden.txt" bestand gezet.
28-4-2024 20:07	Met John alle wachtwoorden in database uitgeprobeerd om 'allebestanden.zip' te openen, gaf geen resultaten.