INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2022-2023 – 1st Period

Digital Forensics Report

Afonso Lopes - 95526

Eduardo Claudino - 95567

Maria Campos - 95629

1 Do you find any traces of the Fake NASA files on Prof. Seagal's computers?

We found all the Fake NASA files on his computers. In backup_disk, inside folder /home/carlseagal/secrets/ we found the following artifacts:

- BuzzAldrin.mov
- letter.pdf
- Nevada.png
- top_secret
- polaroid

Also in backup_disk, inside archive /home/carlseagal/backup_1665190201.zip[1] we found all the above mentioned artifacts plus one:

- workmanship

This gives us all the 6 secrets. We also verified, and these artifacts had the same SHA256 fingerprint as the ones we found in the pen drive during the first part of the investigation.

2 If so, can you track the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.

This is the relative timeline of events regarding only the evidence files, from the moment they were received by Carl Seagal:

1. Source files were copied from a usb drive with serial number 14c0f244af16f6, which corresponds to the serial number of the apprehended usb drive.
2. Evidence files were extracted from those files one by one:
    a. letter.pdf was extracted from Corrupted.pdf using base64 and tool.py
    b. Nevada.png was extracted from Relativity.gif using exiftool

[1] To extract the archive, we had to provide a password. To know the password, refer to **Appendix D**.

c. BuzzAldrin.mov was extracted from Sports.zip using unzip
d. top_secret was extracted from Sports.zip/Golf by prepending PDF header to the file
e. polaroid was extracted from Dog.png using lsb.py
f. workmanship was extracted from Schedule.png using lsb.py

3. Evidence files (and browser files) were encrypted and sent to the backup_disk using backup.sh. This script was set to run every 10 minutes, by using the cron daemon.
4. Evidence files were erased from carl_disk using srm

For an absolute timeline of all relevant events we could find, refer to **Appendix A**.

3 Do you find any evidence of anti-forensic activity?

Yes, we did find evidence of anti-forensic activity. We found out that Carl was encrypting the documents before sending them to a backup server, in order to guarantee he was the only one that could read them (though unsuccessfully). The following files were used doing the backup process: pass_gen.sh, backup.sh and obfuscator. What these scripts do is i) generate a password based on a line from seeds.txt and the current timestamp; ii) create a zip of ~/Desktop/moon encrypted with said password; iii) send the zip file to backup_disk using rsync. We then managed to decrypt and unzip said files, where we found the "evidence" of the fake moon landing. We verified the files and they had the same SHA-256 fingerprint of the evidence we found in the pen drive (during the first report).

By looking at Carl's bash history, we can see, by the tools he used to process the files before opening them, that they were hidden inside other files. This means that steganography was being used in order to conceal those artifacts, making them difficult to find.

By analyzing the bash history, we also found that Seagal used srm to delete the files, which is a tool that overwrites deleted data to make it impossible to recover.

4 What can you tell about the identity of the person/people involved in the leakage of the files?

The emails and IRC chat logs we retrieved tell us that both Carl Seagal and Megan Polanski were involved. We learned that Megan and Carl knew each other and were once coworkers at least ten years ago, as they worked together on projects and papers at MIT.

We also know Megan is married to Chris Cox, the grandson of ex-president Richard Nixon, which is why she managed to obtain R. Nixon's letter and all the other classified documents. Megan was the one who got in touch with Carl with the intent to give him the documents she had collected, and it was also she who arranged their meeting to give him the usb drive.

Appendix A - Absolute timeline

#	Time	Timestamp	Event
1	2022-10-05 19:48		first email received from Megan Polanski
2	2022-10-07 15:08:42		first message sent on IRSSI to Megan
3	2022-10-07 15:17:08		chat closed (before meeting in person)

4	2022-10-07 15:27:02		inserted usb with serial number 14c0f244af16f6
5	2022-10-07 15:32:58	1665153178930794	python decompiler online - Google Search
6	2022-10-07 15:37:58	1665153478722887	ice baby lyrics - Google Search
7	2022-10-07 15:48:05		they start talking again through IRSSI
8	2022-10-08 01:26:43	1665188803	first backup to backup_disk
9	2022-10-08 01:44:06	1665189846397323	twitter - Google Search
10	2022-10-08 01:44:26	1665189866136247	expose a fraud - Google Search
11	2022-10-08 01:46:49	1665190009182258	safe delete - Google Search
12	2022-10-08 01:50:01	1665190201	last backup to backup_disk

Appendix B - Timeline sources

#	File
1	Inbox (line 2544)
2	irssi_mpolanski.10-07.log
3	irssi_mpolanski.10-07.log
4	kern.log (line 1174)
5	places.sqlite
6	places.sqlite
7	irssi_mpolanski.10-07.log
8	backup_1665188803.zip
9	places.sqlite
10	places.sqlite
11	places.sqlite
12	backup_1665188803.zip

Appendix C - Evidence artifacts

Appendix C.1 - Artifact checksum

Evidence Artifact	SHA-256 sum

backup_1665190201.zip	1d2b90f0786d5db9aeadb7f006e6f7a3ff1339038d610d81c5022f54beb8ee44 **Link to file:** https://drive.google.com/file/d/10-78PSUuD0F7qY9HR_ITPYQkQIrWWJXP/view?usp=sharing
backup.sh	de1307a1be0a72d8286d5804cba931f8259cf0b31c38599547b8abda0405ab50
bash_history	338d485d9ffb200e34abdb69e08d0c0a9eb962819146a710d935f224efa4dc82
Inbox	18d2d3616206771a8583de6fb3d4c0d4b82f175ffbee6102786c2ebe04303491
kern.log	94574dae9bf7566391ab1624440aff058990a737b18af8e5c5f998083f1479b0
mpolanski.10-07.log	870e71c0f270a0261631e882539ebd2972421ed391abbbf0d93fb9a8bf46c5b6
obfuscator	e3d217351855e3caab70c49f761816dc66f102f095d7391c08cbac5a743dd0bc
pass_gen.sh	535dafaf7e7f6eefa12ea6ae4b1d00e859c41adb683fc298387de38e151ebe8e
seeds.txt	3296b803bf327dfe9e26caf89df23f4d23ee6222871be80d4178fa2d1815cc70

Appendix C.2 - Artifact location

Evidence Artifact	Parent Folder[2]
backup_1665190201.zip	in backup_disk: /home/carlseagal/
backup.sh	/home/carlseagal/backup/
bash_history	/home/carlseagal/
Inbox	/home/carlseagal/snap/thunderbird/common/.thunderbird/weis2y1j.default/Mail/pop.mailfence.com/
kern.log	/var/log/
mpolanski.10-07.log	/home/carlseagal/snap/irssi/common/irclogs/2022/EFNet/
obfuscator	/home/carlseagal/backup/
pass_gen.sh	/home/carlseagal/backup/
seeds.txt	/home/carlseagal/

[2] By default assume we are referring to carl_disk

Appendix C.3 - Artifact inode

Evidence Artifact	Partition[3] and inode
backup_1665190201.zip	backup_disk.img1: 137626
backup.sh	carl_disk.img3: 674515
bash_history	carl_disk.img3: 674722
Inbox	carl_disk.img3: 674446
kern.log	carl_disk.img3: 540980
mpolanski.10-07.log	carl_disk.img3: 674246
obfuscator	carl_disk.img3: 675415
pass_gen.sh	carl_disk.img3: 675523
seeds.txt	carl_disk.img3: 674518

Appendix D - Decryption password for artifacts (where needed)

Artifact	Decryption password
backup_1665190201.zip	296c0a0eb14443561fa31256ab05a90fa3439e4b3c830a6971a4d87d20bfec56

Appendix E - Auxiliary items

Auxiliary Item	Description
obfuscator.py	obtained by decompiling obfuscator
deobfuscator.py	tool we created to decrypt backup archives found in backup_disk
places.sqlite	found in backup_1665190201.zip; contains firefox history

Appendix F - Email in readable format

[3] As described by fdisk utility

I knew you would be interested :) what if we continued this conversation in IRC just like the old times?

> **Sent:** Wednesday, October 05, 2022 at 8:17 PM
> **From:** "Carl Seagal" <prof.carl.seagal@mailfence.com>
> **To:** "Megan Polanski" <megan.polanski@mail.com>
> **Subject:** Re: Long time no see!
>
> Wow no way Meg! Was not expecting an email from you that's for sure!
> Yes at least 10 years... but how could I forget you? We worked together in quite a few course projects and papers at MIT. That paper we wrote on relativity even kick started my career.
>
> Well the Patriots ain't doing too well after Brady left, who would have thought...
>
> Anyway, you certainly got my attention what are you up to?
>
> Regards,
> Carl Seagal
>
> On 05/10/22 19:48, Megan Polanski wrote:
>
> > Hi Carl! This is Megan, We have not talked in years.
> > Do you still remember me ahah? How are you?
> >
> > I know that you are still going full speed at MIT. Your recent publications on black holes definitely made some heads turn.
> > Look, I have been "working" on something that might interest you even though it is no directly related to your research.
> >
> > If i have sparked you curiosity please email me back.
> >
> > Best regards,
> > Megan Polanski
> >
> > PS: How are the Patriots doing?

Obtained from Inbox (lines 2525 to 2577). To reproduce, copy target lines to a separate file and open it with a browser.