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 evidence of transfers involving the documents in the analyzed network traces? What can you tell about the source and authenticity of these documents?

We now know that the source of the Fake Nasa Files was Chris' computer. These files were extracted from his computer by Megan, who used a computer virus to achieve such an end. Megan then contacted Prof. Seagal and gave him the files in person.

The virus worked by receiving external requests (from Megan), executing on Chris' computer and then sending the result back. The requests and replies were encrypted, so we had to use a script to decrypt them, `decoder.py`

However, not all of the files we extracted from the network capture match the files that showed up on Carl's computer. For example: the BuzzAldrin.mov we managed to export from Wireshark is three seconds long while the BuzzAldrin.mov from Carl's computer is ten seconds long. Also, we recovered a letter that would correspond to Richard Nixon's letter that Carl received, although it is corrupted, making it impossible to make out a signature. These differences imply that Carl did not receive authentic versions of these files. That being said, the other three files found through wireshark (poor workmanship, nevada and top secret) are the same files found in Carl's computer as comproved through the comparison of the SHA-256 of these documents.

2 What can you tell about the identity of the person/people responsible for leaking the secrets?

The person responsible for leaking the secrets was Megan Polanski, Chris Cox's wife. She leaked the files in a way to achieve revenge because of her husband, Chris, cheating on her. She achieved this by pretending to be Monica, and using that mistaken identity to infect Chris' computer with a virus.

She pretended to be Monica by creating an email account with an address which was almost identical to Monica's, so that an inattentive person wouldn't catch the difference.

3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Carl Seagal's computers?

- **Saturday, October 1st, 2022**
  - `At 11:46`, Chris searches on Quora "How can one hide an extramarital affair?".
  - `At 11:47`, Megan accesses the site www.survivedivorce.com.
  - `At 11:49`, Chris receives an email from monica.l.sky@mail.com talking about how amazing their vacation was. In reality the mail came from Megan's pc.
  - `At 11:51`, Chris replies to the email about the vacation with Monica.
  - `At 11:59`, Megan starts sending commands to the virus she put on Chris' computer, extracting the "fake landing evidence". See Appendix B.
  - `At 12:04`, Megan accesses the proton mail website.
  - `At 12:06`, Chris receives an extortion email from real.life.trinity@protonmail.com demanding money, threatening to release the documents of the supposed fake moon landing.
- **Wednesday, October 5th, 2022**
  - `At 19:48`, Megan contacts Carl by mail.
- **Friday, October 7th, 2022**
  - `At 15:08`, Carl begins talking to Megan on IRSSI.
  - `At 15:17`, the IRSSI chat is closed.
  - Carl receives the documents from Megan in person.
  - `At 15:27`, Carl inserts the USB in his computer.

4 From all the collected evidence in this investigation, what can you deduce about the motivation of the actor(s) responsible for the data exfiltration?

From all the collected evidence, we can deduce Megan Polanski found out Chris Cox, her husband, was having an affair (by her search "How to survive divorce" and her husband's search "How to hide an extramarital affair") . So to get revenge on him, she hacked his computer and downloaded all the files containing the supposed evidence of the fake moon landing, with the intent to blackmail/distribute.

To do this, she pretended to be Monica (the person Chris was having an affair with). We know this because Chris was receiving emails from a "Monica", whose email does not match the verified one (being monica.l.sky@mail.com instead of monica.lsky@mail.com). This is also supported by the fact that in the entire capture, Monica's ip never accesses any email services, and we can see Megan's ip retrieving this sequence of mails (see Appendix C).

A. Evidence and checksum

File Name	MD5 value
TopSecret.pdf	8abfb39c337351c7d6d264ba8b1d218d
Workmanship.pdf	7e474f88767396e73efe1358ccda4fda
Nevada.png	840b78ad9f51878db2d4bee1b8c70e42
Letter.pdf	79a3a2377d95b88f435f7b62d4603db2
BuzzAldrin.mov	2828c9cbc62fc19e17f8ae8b12582446
maldives-video.zip	e0f30369b54d6e19804a160c6c74736c
vacation_mail_1.html	1fa7a7278fb0220f55d314b7e0fa7806
vacation_mail_2.html	adb13eec7ba9dfcf99e4830733dcebb8
vacation_mail_3.html	6efafe5ded56391189a2a30b3d00f32e
extortion_mail_1.html	0082dc2a9938dfd5819cff45963ea33a
extortion_mail_2.html	caadd38e1ca47625623df728f6489ba5
maldives.desktop	ee6823f4b830c9bc9385efbf0279a23d
shell.py	3c0c99a4a6cc499884975eed94dc533a

B. List of commands executed by Megan on Chris' computer

TCP stream	Commands sent
7115	ls
7118	ls /home/chris
7121	ls /home/chris/Desktop
7124	ls /home/chris/Desktop/vacations
7127	ls /home/chris/Desktop/topsecret
7130	ls /home/chris/Desktop/topsecret/moon1969
7134	download /home/chris/Desktop/topsecret/moon1969/Buzz.mov
7138	download /home/chris/Desktop/topsecret/moon1969/Letter.pdf
7142	download /home/chris/Desktop/topsecret/moon1969/Nevada.png
7145	download /home/chris/Desktop/topsecret/moon1969/TOP_SECRET.pdf
7150	download /home/chris/Desktop/topsecret/moon1969/Workmanship.png
7153	quit

C. Relevant packet streams

TCP stream	Description
266	Chris searches on Quora how to hide an extramarital affair
310	Megan searches how to survive divorce
7086	Chris downloads infected zip file
7174	Megan connects to protonmail

TCP stream	Email
1052	vacation_mail_1
6658	vacation_mail_2
6659	vacation_mail_3
7510	extortion_mail_1
7759	extortion_mail_2