April, 2020

VPN SOLUTION SECURITY TESTING

LIFARS

your digital world, **secured**

Contents

Overview 3
VPN Solution testing..3
Discover 3
Impact 6
References...6

OVERVIEW

LIFARS frequently conducts penetration tests to ensure the effectiveness of our client's security implementations and to evaluate whether their systems can hold up to real world incident scenarios and stay resilient. Our cyber resiliency experts deliver calculated attacks against systems the same way black hat hackers.

In April, our client requested LIFARS Pen Testing Team to perform an authenticated black-box penetration test of the VPN solution and connection to the host through RDP. The client understands the risks they are daily facing as well as the importance of meeting compliance standards. Therefore, this client asked for an authenticated black-box penetration test.

The intent of this engagement was to identify weaknesses in the company's VPN solution and to detail how these vulnerabilities could impact the organization.

Our team found a critical vulnerability – Restricted RDP connection bypass which could help attacker mount other attacks. This security testing effort was conducted with emphasis on the actual state of the systems examined and no documentation to the client was provided.

Note: All information in this case study has been modified to maintain confidentiality of our client

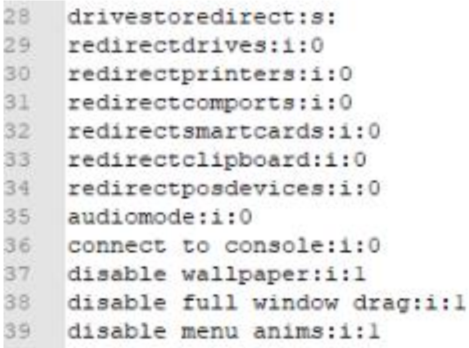
VPN SOLUTION TESTING

Client's VPN solution used web portal for authentication. After successful login, user could connect to the SSL VPN using MotionPro client (Array Networks) and then use RDP connection to the host in VPN.

This solution should allow safe connection from employees, without worrying about their current device as the data should not be leaving the corporate network. The RDP session was restricted and operations like clipboard, redirect drives/ports etc. were disabled.

DISCOVER

We have started with looking on files, which were created by MotionPro client when we were connecting to the VPN, such as logs, temporary files or configs. We went through the logs to see if there are any security issues or possible data leakage. In path "C:\Users\Name\AppData\Local\Temp\MotionPro" we saw hostname.rdp file which contained connection settings.

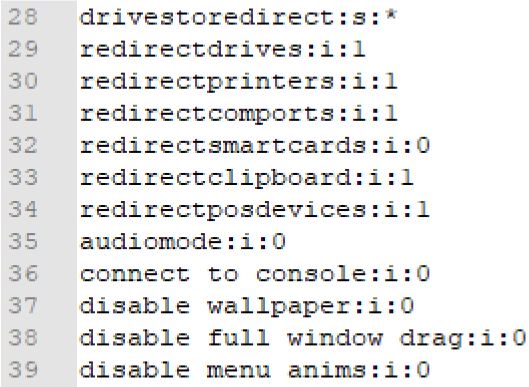


```
drivestoredirect:s:
redirectdrives:i:0
redirectprinters:i:0
redirectcomports:i:0
redirectsmartcards:i:0
redirectclipboard:i:0
redirectposdevices:i:0
audiomode:i:0
connect to console:i:0
disable wallpaper:i:1
disable full window drag:i:1
disable menu anims:i:1
```

Figure 1 content of the hostname.rdp file

The content of this file was interesting because, there was an IP address with port and strings like "redirectclipboard:i:0" or "redirectdrives:i:0" . These settings are used to disable clipboard and redirecting drives.

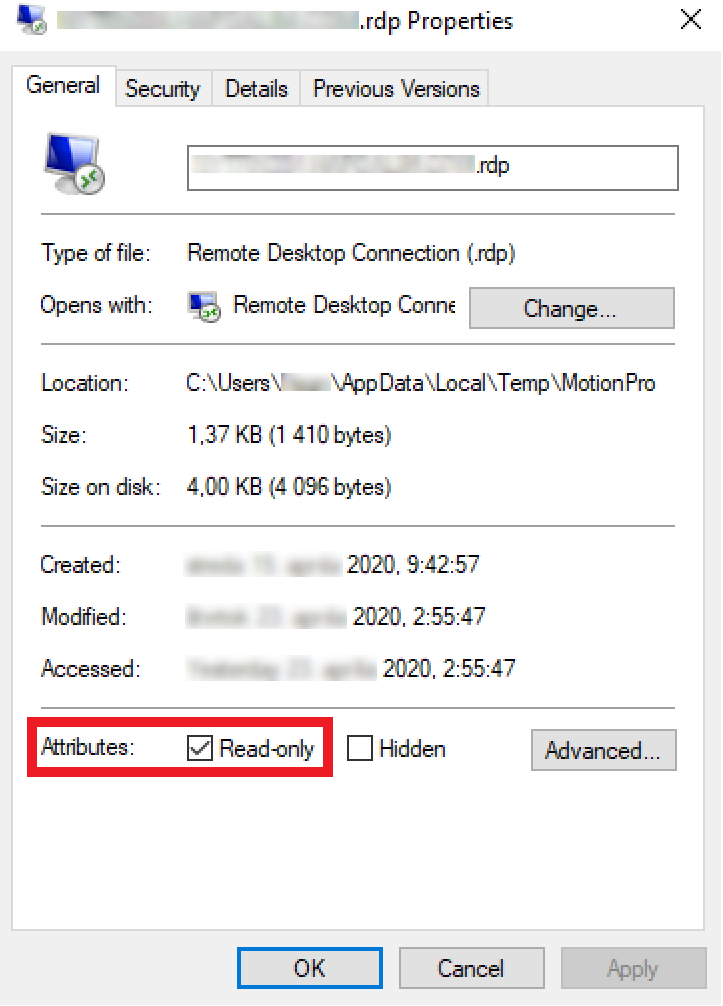
We have tried to modify content of this file, to see if this file is really used by the MotionPro client and what changes can be possibly made.



```
drivestoredirect:s:*
redirectdrives:i:1
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:0
redirectclipboard:i:1
redirectposdevices:i:1
audiomode:i:0
connect to console:i:0
disable wallpaper:i:0
disable full window drag:i:0
disable menu anims:i:0
```

Figure 2 modified hostname.rdp file

As the MotionPro client could rewrite our modified file, we had to use a file attribute read-only.



[redacted].rdp Properties

General | Security | Details | Previous Versions

[redacted].rdp

Type of file: Remote Desktop Connection (.rdp)

Opens with: Remote Desktop Conne Change...

Location: C:\Users\[redacted]\AppData\Local\Temp\MotionPro

Size: 1,37 KB (1 410 bytes)

Size on disk: 4,00 KB (4 096 bytes)

Created: [redacted] 2020, 9:42:57

Modified: [redacted] 2020, 2:55:47

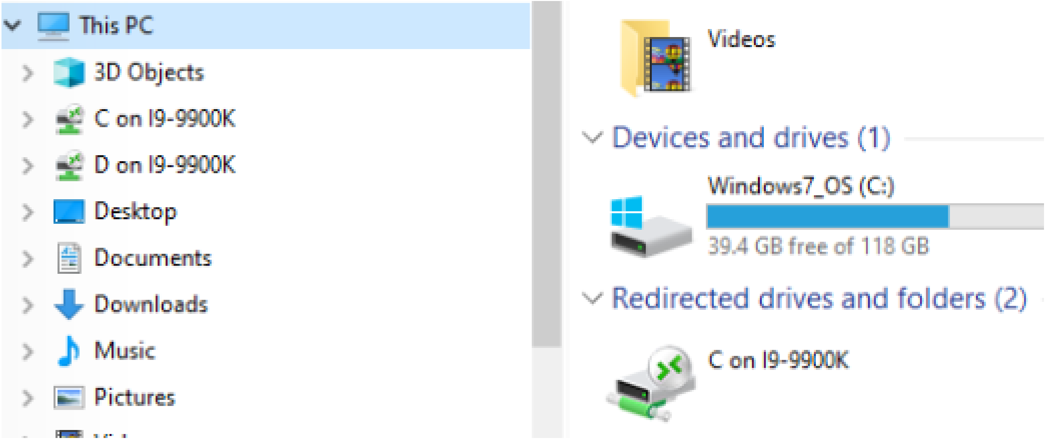
Accessed: [redacted] 2020, 2:55:47

Attributes: ☑ Read-only ☐ Hidden Advanced...

OK Cancel Apply

Figure 3 file attribute Read-only

After setting read-only attribute, we managed to get successful connection through RDP to our host.



This PC
- 3D Objects
- C on I9-9900K
- D on I9-9900K
- Desktop
- Documents
- Downloads
- Music
- Pictures

Videos

Devices and drives (1)

Windows7_OS (C:)
39.4 GB free of 118 GB

Redirected drives and folders (2)

C on I9-9900K

Figure 4 mounted disks

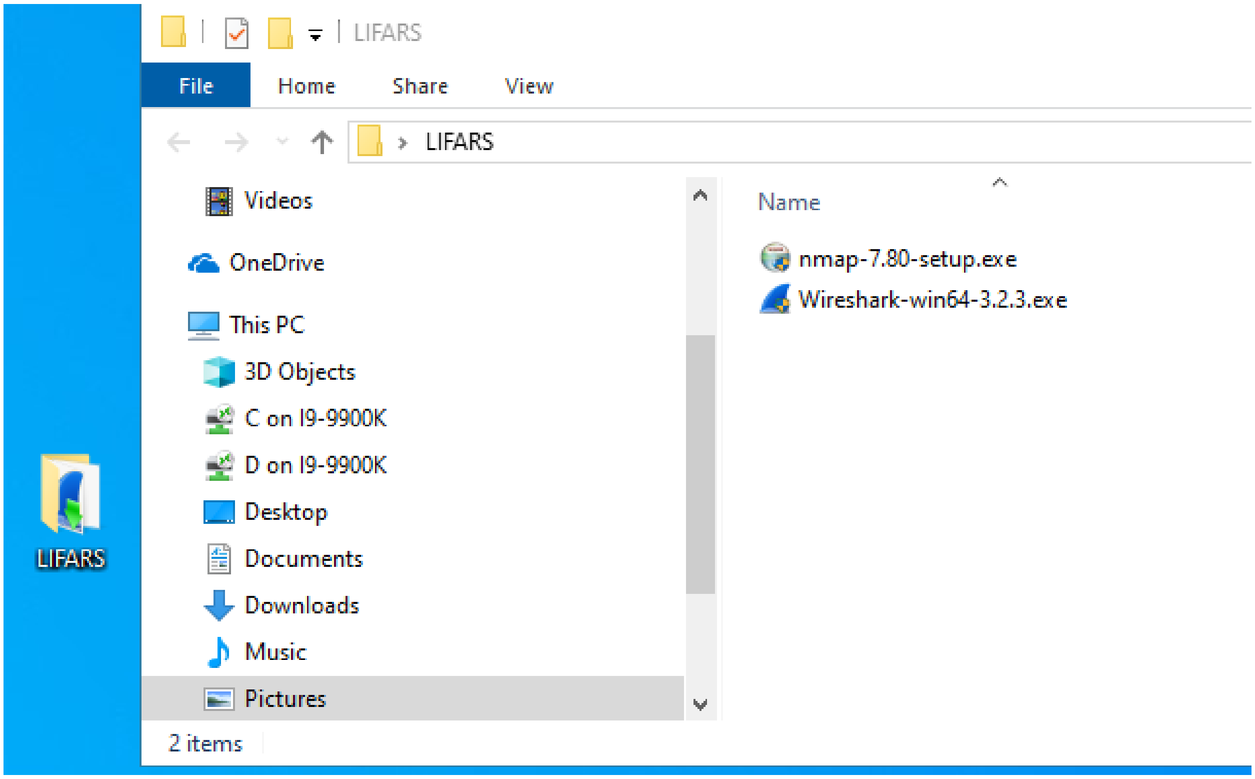


Figure 5 executables successfully uploaded

We saw redirected drives, allowed clipboard also the background and composition were changed. As a Proof of Concept (POC), we have uploaded executables to our directory "LIFARS" on desktop. MotionPro client seems to have used this hostname.rdp file, which as we could see, can be modified for bypassing any RDP restrictions.

IMPACT

Adversary could connect to the host machine without previous restrictions. He gained the possibility to upload malicious software to help him obtain additional information about the environment and mount other attacks such as privilege escalation or lateral movement. He could also exfiltrate data from his machine because of the mounted drives and allowed clipboard.

REFERENCES

[1] Array Networks, "SSL VPNs" Available: https://www.arraynetworks.com/products-ssl-vpns-features.html