





CASE STUDY: WIFI RDP ATTACK DETECTION & RESPONSE

 Policy Action No Action	 Reputation Trusted White List
 Process State Ran	 Signature Verification Signed And Verified

**1st
Alert**

```
CMD C:\WINDOWS\System32\svchost.exe -k Net
workService -s TermService

SHA-256 dd191a5b23df92e12a8852291f9fb5ed59
4b76a28a5a464418442584afd1e048

MD5 9520a99e77d6196d0d09833146424113

PID 1212

Start time 10:21:22 am Sep 6, 2019
```

Preface

A customer's employee was visiting a hospital in New York. Like many of us do, she connected to the Hospital's WiFi public network to continue working - but she then experienced another issue while she was connected to this network.

The Case

Our endpoint computer agent detected a suspicious connection from another computer using Microsoft Remote Desktop Protocol (RDP), which allows users to access computers remotely. We then alerted the IT manager about this activity, and the IT Manager called the employee, advising her that a remote device was trying to access her laptop, and that she should stay off that network.

**2nd
Alert**

ALERT TRIAGE: NONRFDS6

NON-MALWARE

10:21:22 am Sep 6, 2019 **1**

A port scan was detected from null on an external network (off-prem).

In Conclusion

The client has achieved better security, and is now aware of the potential dangers of connecting to public networks.

An Email from IT Manager to Our SoC Team



Fri 9/6/2019 12:47 PM

Fritz

RE: **11-ASSISTANT-LT2** public IP:64.251. (Internal)
IP: 192.168.

To Security Operation Center-2Secure Corp

Good catch!

She is at Bellevue hospital. She complained about very slow Wi-Fi. I told her a device was trying to access her laptop and to stay off that network.

Fritz
IT Manager



About 2 Secure

2Secure is a Cyber Security firm which takes a PROACTIVE approach to solving network security problems. We provide the right strategy, people, and tools to fix problems the first time around – in fact, we guarantee it!