BRANDEFENSE
CYBER THREAT INTELLIGENCE

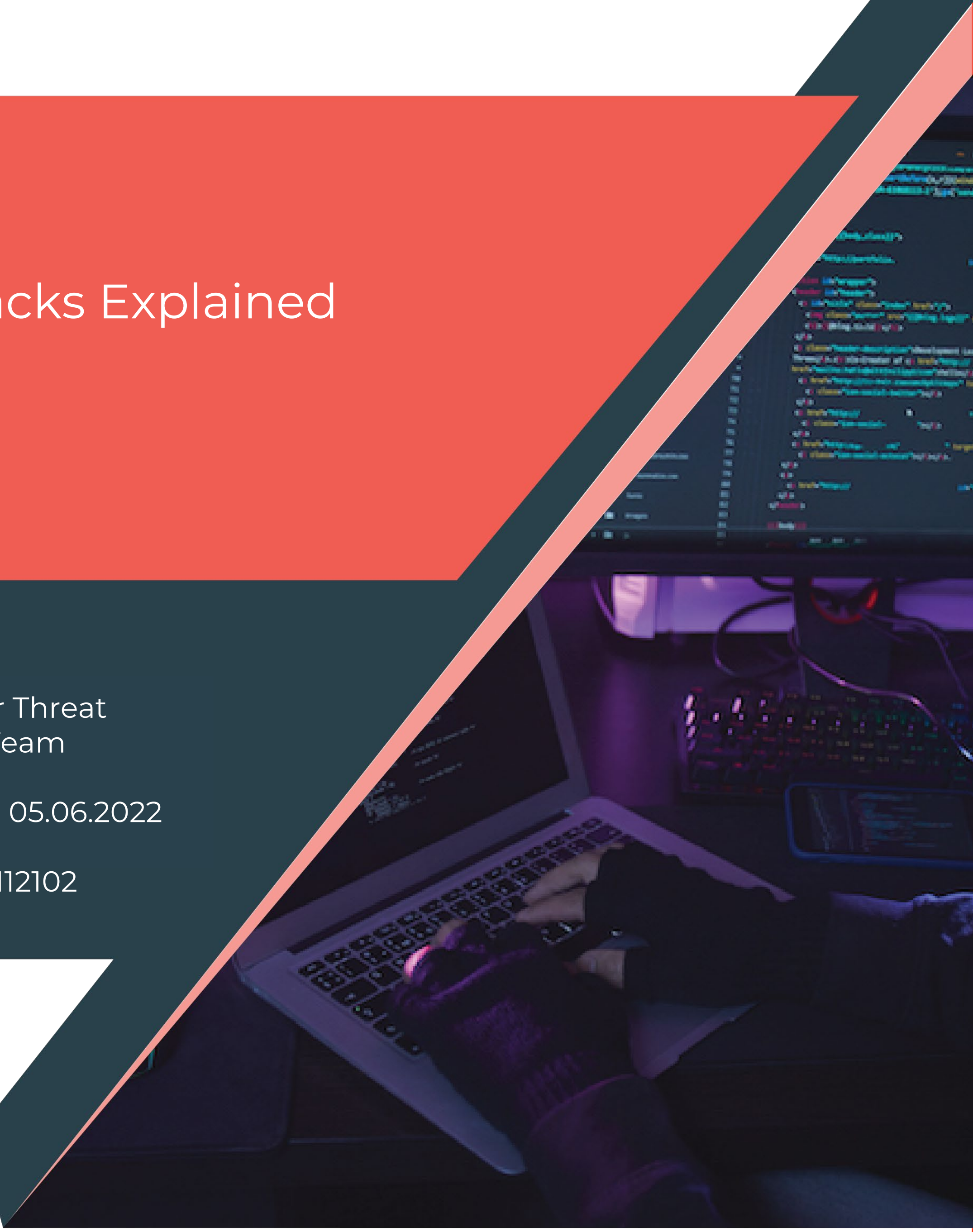
RDP Attacks Explained

—

Author: Cyber Threat Intelligence Team

Release Date: 05.06.2022

Report ID: 02112102



What is RDP?

RDP (Remote Desktop Protocol) is a protocol which provides connection to a remote machine. It is a service built for Windows, but anyone can connect to an RDP port via such tools from different operating systems. You can have a control of a remote machine from its Graphical User Interface, unlike telnet or SSH. Telnet and SSH provides you to control a remote machine from its Command Line Interface. Therefore, RDP is more comfortable to connect and having the control of a remote machine. You need to know the name or IP address of the remote machine, username and password in order to connect to it.

RDP is mostly used in corporate networks. Employees who want to do their job remotely, connect to their work computer via RDP. As the remote jobs are more prevalent nowadays, employees tend to work from remote locations and thus, RDP becomes more important. Another usage reason is that an IT employee may want to log into your computer remotely to fix an issue.

Attack Types and Vulnerabilities

- Brute force attacks on RDP can be done via automated tools, if the RDP port is open. This attack is useful when the usernames and passwords are easy to guess and related to the target's private life (name, city, pet name, etc.).
- BlueKeep vulnerability (CVE-2019-0708) provides attackers to execute commands remotely on the target machine. This vulnerability is popular and can be found in the metasploit exploit module.
- There are 103 CVE Records for RDP vulnerabilities. You may want to look at them: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rdp

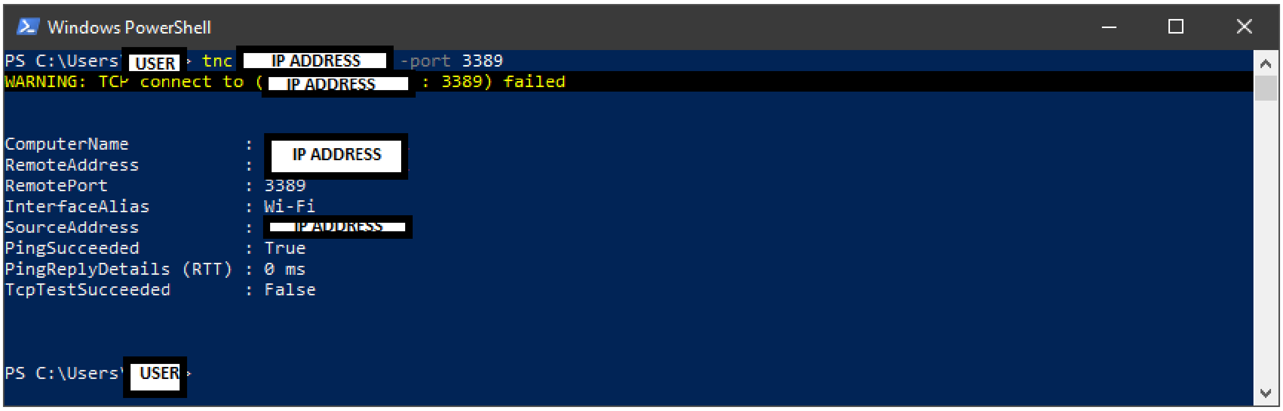
BlueKeep Mechanism

Since BlueKeep is very popular, it would be beneficial to known the mechanism behind the exploit. RDP connects two machines via RDP through 32 virtual channels. One of the channels named MS_T120 does not require to be connected by the client. However, if it is used for connection by the client, memory corruption occurs and the attacker will be able to execute commands remotely on the target machine.
BlueKeep vulnerability is wormable. This means that it can replicate itself and spread to other machines in the network. Wormable vulnerabilities may create a massive damage, especially to the companies because companies have a lot of machines connected to the same network.

Mitigation Methods

There are many ways for taking measures; however, none of them can be efficient to prevent the user from the attacker, when only one of them is taken. These measures are basic ones and can be done by a non-IT person. You should consider taking as many measures as you can.

- Windows publishes patches related to a specific vulnerability just after it is found. You need to keep your operating system updated, if you are using Windows.
- When you try to connect to other machines via RDP, it will ask you to enter a username and password. It would be beneficial to use second-factor authentication such as VPN, SSL or RDP gateway.
- You should enable NLA (Network Level Authentication) since it forces people to authenticate before connecting to any machine remotely.
- Disable RDP service, if it is not required too much. You can enable it, when it is needed.
- You can set a maximum limit of login attempts. This will prevent you from the brute force attacks.
- RDP uses 3389 as the default port number. An attacker might attack to this port blindly by guessing that port serves RDP. If you change the RDP's port number, it will be a little harder to hack into the system.
- You can use port scanners or some powershell/command-line tools (tnc, netstat, telnet, ...) for test purposes. This will make you to be sure if the port is open or not. Here is an example of how tnc tools is used (we will show closed port and opened port respectively).

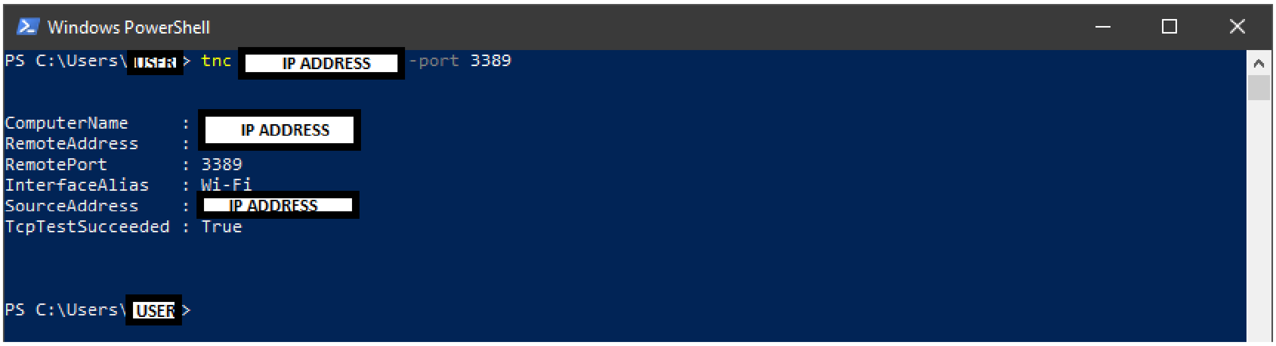


```
PS C:\Users\ USER > tnc  IP ADDRESS  -port 3389
WARNING: TCP connect to ( IP ADDRESS  : 3389) failed


ComputerName           :  IP ADDRESS
RemoteAddress          :
RemotePort             : 3389
InterfaceAlias         : Wi-Fi
SourceAddress          :  IP ADDRESS
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False



PS C:\Users\ USER >
```



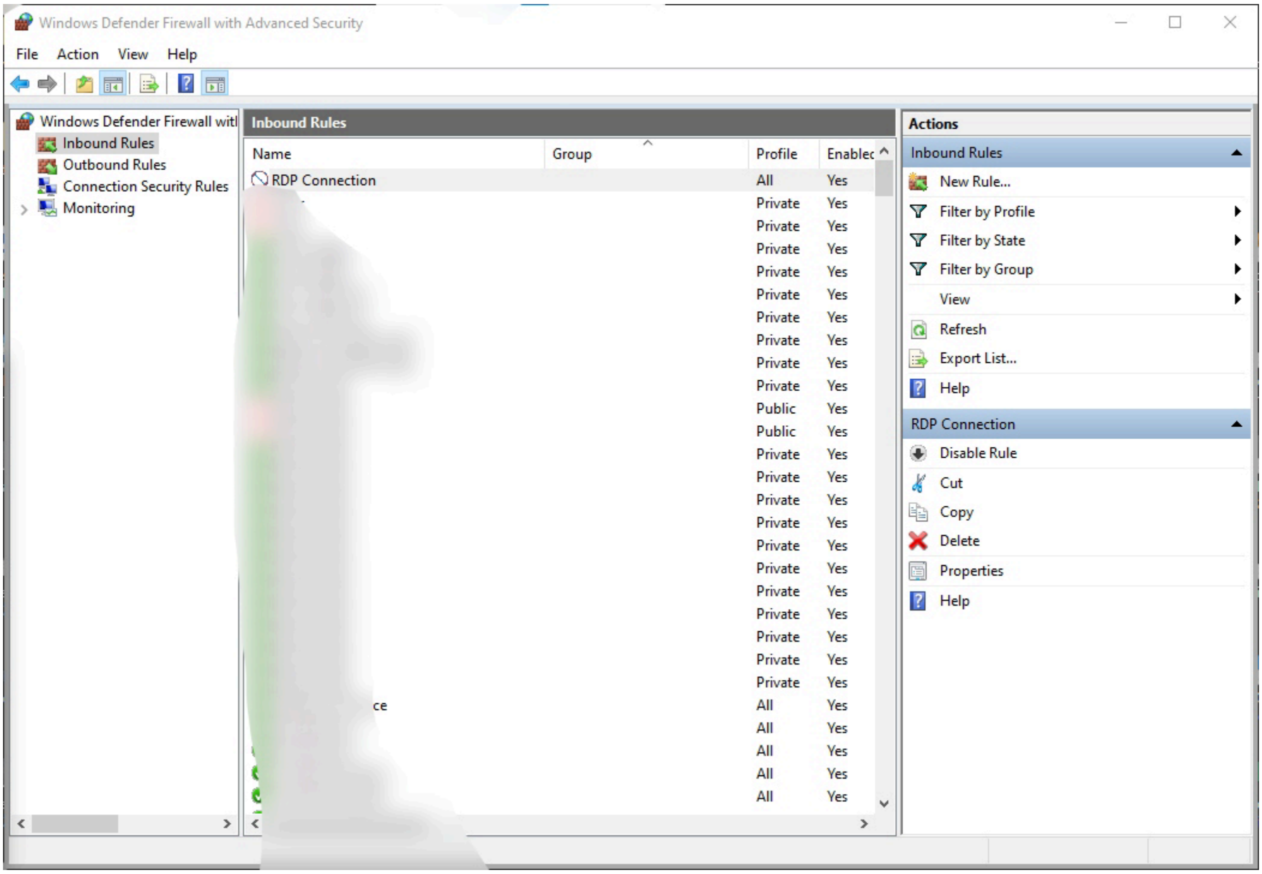
```
PS C:\Users\ USER > tnc  IP ADDRESS  -port 3389


ComputerName     :  IP ADDRESS
RemoteAddress    :
RemotePort       : 3389
InterfaceAlias   : Wi-Fi
SourceAddress    :  IP ADDRESS
TcpTestSucceeded : True



PS C:\Users\ USER >
```

- If you do not need to use RDP, you may want to close the port, not just the service. You can do that by writing an inbound rule to the Windows Defender Firewall. In the example below, you can see an already written inboud rule named «RDP Connection». You can set new rules by selecting «New Rule...» in the right panel.



Name	Group	Profile	Enablec
RDP Connection		All	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Public	Yes
[redacted]		Public	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted]		Private	Yes
[redacted] ce		All	Yes
[redacted]		All	Yes
[redacted]		All	Yes
[redacted]		All	Yes
[redacted]		All	Yes

Conclusion

RDP is widely used by remote workers. Its usage rate is increased because of the coronavirus. This is not the only reason why attackers prefer attacking to this service. Attackers are able to execute commands remotely or even sometimes gain control of the GUI of the target machine. Attackers are likely to target companies since they have a lot of computers in the same network and they are likely use RDP. Therefore, companies should set the authentication and autharization rules strictly. The measures mentioned above should also be considered to be taken.