January 14, 2021

Industry Expert Report

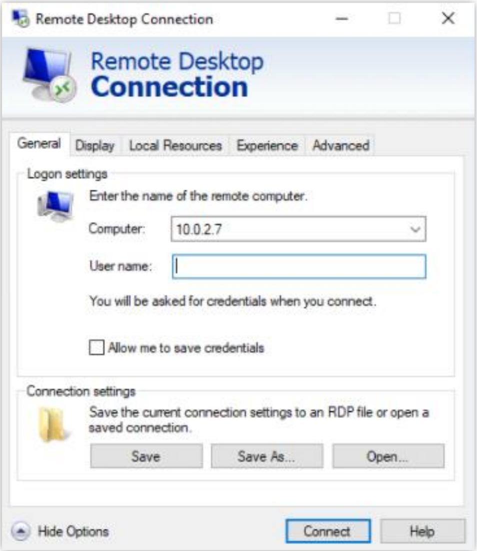
Remote Access to Company Server Offered for Sale

Cyberint

Background

Remote Desktop Protocol (RDP) is a communication protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection[1]. Once connected, the remote user will be able to communicate with the machine using their input devices, keyboard and mouse, and to have their screen displaying the output of their actions – as if they were physically connected.

Common use of this protocol would be IT personnel performing maintenance, or support teams providing training and assistance to end-users. It is also a useful tool for remote employees who want to connect the organization's resources.



Logon settings

Enter the name of the remote computer.

Computer: 10.0.2.7

User name:

You will be asked for credentials when you connect.

☐ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

RDP login interface

The protocol gained popularity, that naturally increased[2] during COVID-19 as most organizations moved to working from home; however, it was also noticed by malicious actors, who saw this as an opportunity to access organizations' internal networks, steal or corrupt information.

RDP AS A VULNERABILITY

As a result of the exclusive capabilities RDP enables once in-use, RDP servers became an attractive target for cybercriminals. The first stage of an attack in which this protocol is leveraged must include the detection on an internet-connected RDP server. The selection for detection tools is large, ranging from legitimate PT port scanning tools such as Nmap, to shady port scanners shared within the threat actors' community[3]. These scanners flag IPs that have an open port 3389, the default RDP port. Then, the vulnerable server will face 1 out of 3 main attack vectors, depending on the sophistication and experience level of the attacker:

- In the past few years, the cyber-security community discovered several critical **exploits** (risk rate is 9.8), that render RDP servers vulnerable to remote code execution:

  May 2019: BlueKeep (CVE-2019-0708)[4]

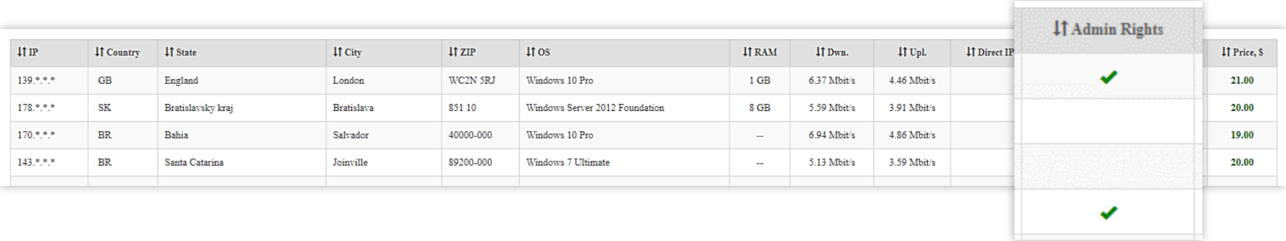
  August 2019: DejaBlue (CVE-2019-1181 and CVE-2019-1182)[5]

  January 2020: BlueGate (CVE-2020-0609 and CVE-2020-0610)[6]

[1] https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol
[2] https://www.trustradius.com/vendor-blog/remote-desktop-buyer-statistics-and-trends#:~:text=Between%20April%202019%20%E2%80%93%20February%202020,per%20week%20with%2046%2C363%20pageviews.
[3] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/rdps-in-the-world-of-cybercrime-darknet/
[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708
[5] https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0610

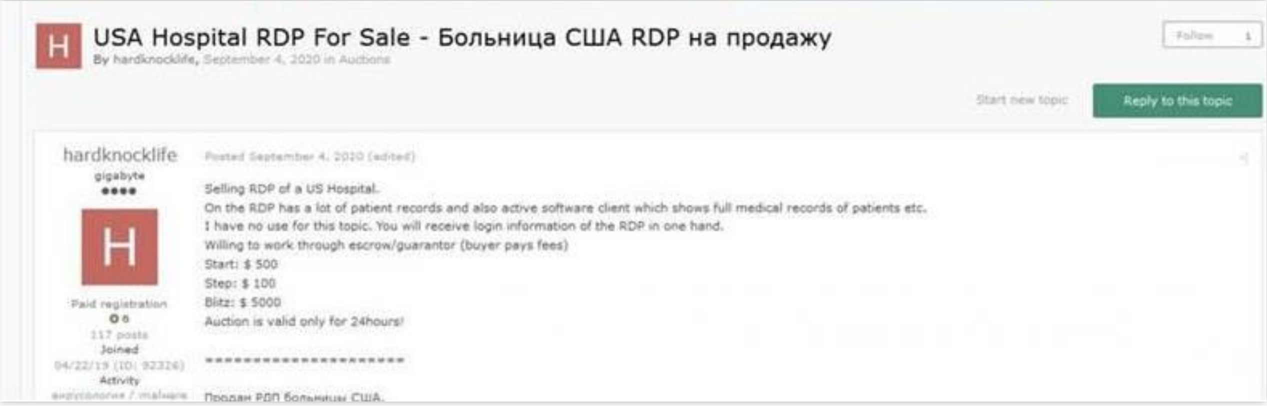
- From authentication perspective, obtaining the **credentials** of an RDP server is a similar effort to other ATO attempts, using brute-force tools and dictionary attacks. Threat actors that choose this methodology rely on the unfortunate habit of using default or weak passwords.

- Even with poor technical skills, a beginner could register to one of the many dark web marketplaces, and **purchase RDP access**. These were likely obtained through one of the methods above, and are sold for a limited timeframe. The listings start from surprisingly low prices, only a few dollars, and get higher according to machine's geo-location, its content, and what it has access to.



⇅ IP	⇅ Country	⇅ State	⇅ City	⇅ ZIP	⇅ OS	⇅ RAM	⇅ Dwn.	⇅ Upl.	⇅ Direct IP	⇅ Admin Rights	⇅ Price, $
139.*.*.*	GB	England	London	WC2N 5RJ	Windows 10 Pro	1 GB	6.37 Mbit/s	4.46 Mbit/s		✓	**21.00**
178.*.*.*	SK	Bratislavsky kraj	Bratislava	851 10	Windows Server 2012 Foundation	8 GB	5.59 Mbit/s	3.91 Mbit/s			**20.00**
170.*.*.*	BR	Bahia	Salvador	40000-000	Windows 10 Pro	--	6.94 Mbit/s	4.86 Mbit/s			**19.00**
143.*.*.*	BR	Santa Catarina	Joinville	89200-000	Windows 7 Ultimate	--	5.13 Mbit/s	3.59 Mbit/s		✓	**20.00**

RDP marketplace listings, specify whether the server has Admin privileges



USA Hospital RDP For Sale - Больница США RDP на продажу

By hardknocklife, September 4, 2020 in Auctions

hardknocklife
gigabyte
Paid registration
117 posts
Joined
04/22/19 (ID: 92326)
Activity
вирусология / malware

Posted September 4, 2020 (edited)

Selling RDP of a US Hospital.
On the RDP has a lot of patient records and also active software client which shows full medical records of patients etc.
I have no use for this topic. You will receive login information of the RDP in one hand.
Willing to work through escrow/guarantor (buyer pays fees)
Start: $ 500
Step: $ 100
Blitz: $ 5000
Auction is valid only for 24hours!

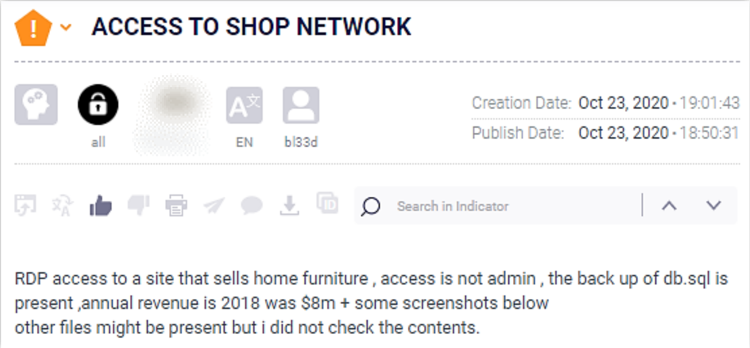
======================

Продан РДП больницы США.

Listing on an RDP designated section on an underground forum

Case Study – RDP Access for Sale

As part of its online monitoring, Cyberint identified an RDP access for a server of a home furniture retailer, which is offered for sale in an online marketplace.

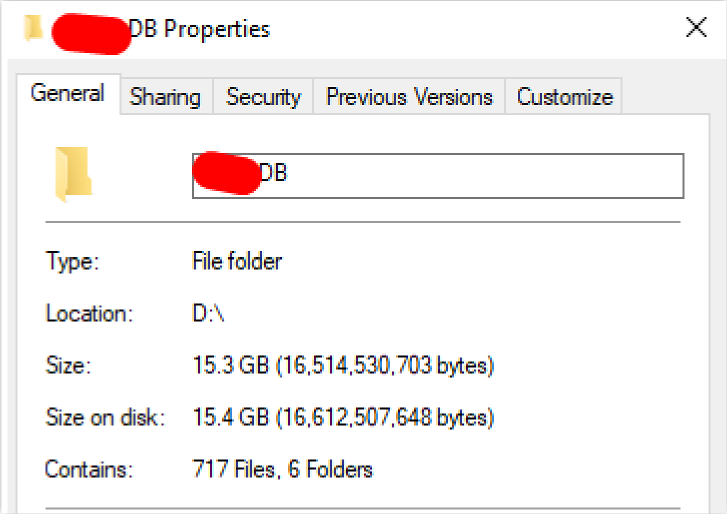


ACCESS TO SHOP NETWORK

Creation Date: Oct 23, 2020 - 19:01:43
Publish Date: Oct 23, 2020 - 18:50:31

RDP access to a site that sells home furniture , access is not admin , the back up of db.sql is present ,annual revenue is 2018 was $8m + some screenshots below
other files might be present but i did not check the contents.

In the listing, the threat actor mentions that the hacked RDP server in question contains a back-up database. Furthermore, the TA provides 3 screenshots allegedly taken from the compromised machine, as an evidence for the compromise; one of them shows the properties window of a 15.3 GB DB.



[redacted]DB Properties

[redacted]DB

Type: File folder

Location: D:\

Size: 15.3 GB (16,514,530,703 bytes)

Size on disk: 15.4 GB (16,612,507,648 bytes)

Contains: 717 Files, 6 Folders

Once purchased, the information disclosed by the screenshot and the rest of the machine's content are at risk of theft and/or corruption. It is worth mentioning that besides the business impact, such attack can also harm the customers of the retailer, which may result it customer churn and lawsuits.

Conclusions

Now more than ever, in the times of COVID-19, organizations around the world are relying on the RDP protocol for effective and productive work environment. Nevertheless, the protocol has several security flaws that make it a popular target of malicious actors. In order to avoid the potential risk of using RDP, Cyberint recommends taking the following precautions:

- Reduce the number of RDP servers which are internet-exposed to the possible minimum. As internet connection is the key for every RDP attack, it is highly recommended to restrict the access to the server only for whitelisted IPs. Organizations should pay extra attention to DMZ (demilitarized zone), non-compliant cloud environments and new machines deployed by non-security personnel.

- In case a server must be publicly available, it is recommended to implement another measure of multifactor authentication. Those servers should be vigilantly monitored, and any suspicious connection attempt should be flagged and analyzed within the organization. Please note that this practice may protect the server only from compromise credentials attacks. If a vulnerability exists, MFA would be useless.
- Make sure all in-use technologies are patched and in their latest version.
- Set high-quality password policy, instructing users to choose complex, long passwords.