Talha *et al.LGU (IJECI)* 2022

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 6 issue 3 Year 2022

Forensics Artifacts on Remote Desktop Protocol and Service.

Talha Ashfaq and Muhammad Shairoze Malik
School of Electrical engineering and computer Sciences, National University of Science and Technology, Islamabad.
Corresponding author: 13beemmalik@seecs.edu.pk

Abstract:

Remote Desktop Protocol provides user a graphical user interface to access system remotely and its implementation is called “remote desktop services”. This is widely used by network administrators and remote workers. Due to vulnerabilities and weak configurations, the protocol is hugely abused by threat actors and hackers to perform malicious acts as data infiltration, deploying backdoors, malwares and lateral movements. In this article, there will be discussion on importance of RDP in digital forensics, understanding RDP based artifacts and there use in forensics investigation where RDP was suspected to be involved.

Key words: RDP, artifacts, Log analysis, bitmaps, Registry artifacts

1. Introduction

Remote desktop protocol (RDP) is propriety Protocol developed my Microsoft which enables users to remotely access computers over the internet. [1][2] Operations sent to the remote server are executed as it was performed by the user (local) itself. The main focus of the protocol is the complete representation of the screen content of the remote-controlled computer [4]. This is widely used tool in areas where remote work, assistance and administration are required. The user use RDP client for remote connection to the RDP server. RDP Client exits on most of operating system such as Microsoft Windows, UNIX, macOS, IOS and android, while RDP servers are built on Microsoft Windows. [3] In order to establish RDP connection local and remote machines need to authenticate via username and password. Microsoft terms implementation of Remote Desktop Protocol (RDP) as “Remote Desktop Service”. [1] [3]

Importance of RDP in Forensics Investigation

As explained, RDP is very widely used proto-

col for employees and Administrators to provide graphical access to remotely connected devices. Despite providing useful features, RDP is abused very often by threat actors. Threat actors commonly target RDP as a primary method to gain access in an organization's network. Once initial foothold is achieved, threat actors or hacker(s) can deploy malwares, ransomwares, can perform data exfiltration or lateral movement without being detected. The Federal Bureau of Investigation (FBI) even released a warning in 2018 addressing dark markets selling RDP access. Threat actors can easily Weak password policies and misconfigured endpoint security play a big role in this. RDP is also prone to vulnerabilities and been exploited for reconnaissance, command and control and lateral movements. [11][10]. RDP was initial attack vector for 50% of the ransomware attack reported by unit 42. [12]. Reported by ESET telemetry, "In the first quarter of 2020, we saw 1.97 billion connection attempts. By the fourth quarter of 2021, that had jumped to 166.37 billion connection attempts, an increase of over 8,400%!" [18]

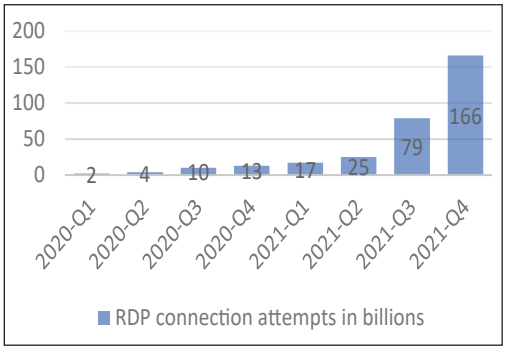

Figure 1 Malicious RDP connection attempts detected worldwide (source: ESET telemetry). Absolute numbers are rounded

Many sophisticated ransomwares such as Matrix, SamSam uses RDP vulnerabilities to gain initial foothold reported by Sophos [13]. In darknet, there are various marketplace that offers complete RDP data for low prices. [4] Thus it is important for a forensics analyst for analyse RDP connection and related artifacts in digital investigations.

RDP artifacts

RDP artifacts can have probative value when investigating a cyber-attack or incident, they include which user made connection to remote server on what time, what activity a user performed from the remotely established connection. These artifacts can be categorized in artifacts related to connectivity of remote server and artifacts for activity performed by the user using remote server.

2. RDP Log analysis

To establish a remote desktop connection, RDP uses user's credential to authenticate login in the remote server. Windows event logs is an audit feature by Microsoft to record user events and activities on a system, also are potential source of evidence for forensics investigations [20]. Event logs resides usually at location C:\Windows\System32\winevt\Logs. RDP connection usually follows a uniform flow chart and they also leave traces in term of events in Windows Event logs. Here, some forensically relevant field of Windows event logs pointing RDP connection, Login, Session disconnection and Logoff, these events are chronologically ordered as [4]:

Event ID	Network Connection
1149	This Event log does not actually indicates remote controlled system but recorded only when network connection between the client and server is successfully connected. This would initiates login prompts for authentication. Event ID 1149 will only initiate when Network level Authentication is enabled.
	Authentication
4624	This event log occurs when a user is successfully authenticated on the server. If Logon Type 10, 7 is observed means the user is reconnected to the server. Type 3 would be observed when NLA (network level authentication) is enabled.
4625	Type 3 if NLA is enabled and/or type 10
	Login
21	If source network address is “LOCAL”, this is not an indication of an RDP login. “LOCAL” is also generated at PC start/reboot.
22	This event follows immediately after event 21. This event indicates a successful RDP login and starting a shell. Unless the source network is “LOCAL”, this login shows RDP login.
	Session Disconnect/reconnect
24	This event shows the user disconnected from an RDP session if source network address is not “LOCAL”. This event usually appears with event ID 40.
25	This event shows the user has reconnected to an RDP session if source network is not “LOCAL”. This also appears with event ID 40.
39	Connection formally ended, not just closed the window
40	Connection was terminated for reason code X.
4778	This event occurs when user connects to ongoing RDP session. Session name, client address and login ID can be used to identify the source will. This event often connects with event id 25.
4779	Occurs when a user disconnects from an RDP session. Often in connection with event ID 24 and with 39 and 40.
	Logoff
23	user initiated a system logoff, usually with connection with event ID 4634
4634	This event occurs when a user terminates an RDP connection or log out from the remote system.
9009	“Desktop Windows Manager” has ended occurs when an RDP connection is lost, which terminates the RDP desktop interface.

2. RDP bitmaps

According to Microsoft "Bitmap caches are used by the client and server to store graphic bitmaps. Each bitmap cache holds bitmaps of a specified size in pixels (known as the “tile size”). If a bitmap does not fit into a single cache entry, the server uses a tiling algorithm to divide the bitmap into tiles that will fit into the cache entries so that they can be stored separately into the cache" [14].

When a user connects to other system using RDP, small bitmaps images are created in the Client's (user's) system. If same image is used in the session it can be quickly retrieve and preventing same images to load once again. This caching can provide efficiency in performance even over low-bandwidth connections [7]. While analysing RDP, this can help investigators what the user was seeing in their RDP

session.

As said this artefact is stored on the client system on the server, so if an attacker uses RDP session to a victim, these bitmap cache would not be present on the victim's machine. However if attacker used victim's RDP connection for Lateral Movements in the Victim's network then it can be analyse by reconstructing RDP bitmapped cache stored on the attacker system, to translate what was actually being visualized by the malicious actor. Location for RDP bitmap caches are at C:\Users\<USER>\AppData\Local\Microsoft\Terminal Server Client\Cache\

Figure 2 RDP cache files in user profile

In this folder, you can see different files such as Bcache.bmc, Cache###.bin where # is the numbers append. Bcache is older version .From the bcache, number can be 2, 22 or 24 shows the quality of the bitmaps, higher the number higher the bitmap quality. Bcache2.bmc stores images in 8 BPP, Bcache22.bmc stores bitmap images in 16 BPP and bcache24.bmc stores bitmap images in 32 BPP [14].

"BMC-tools" is python script [15] by ANSSI (agence nationale la sécurité des systèmes d'information) to parse rdp Bcache.bmc and Cache###.bin to represent what was going on the client's connected screen. The script is written in python so can be used in any environment, windows, Linux etc.

Syntax to parse out bitmap cache from "bmc-tool" ./bmc-tools.py [-h] -s SRC -d DEST [-c COUNT] [-v] [-o] [-b] [-w WIDTH] After the remote connection, the cache files were exported to Kali virtual machine, however the script can also be run on windows environment where python is installed.

Figure 3 Using bmc-tools.py to parse RDP cache bitmaps

Here, -s flag for the source, -d for the destination directory where to export the bitmaps from the source directory. Here "files" folder is the source folder where bitmaps cache are present. -b will provide one bitmap image which aggregates all bitmap images. Once the cache are parsed, you could notice multiple png images created in output directory.

Figure 4 RDP bitmaps parsed from cache files

From here, we can manually rearrange individual bitmap images to reconstruct the possible "screen-shot" that was stored in the session.

For manually stitching the RDP bitmaps "RDPCacheStitcher" is a helpful tool to ease the tedious process. This supports output from ANSSI-FR/bmc-tools as input, provides a GUI and several placement heuristics for stitching the tiles together [17] Also some open source scripts exists where you can attempt to automatically parse extracted RDP bitmaps, such a "RDPPieces". [16].

3. Registry artifacts

Remote desktop protocol does leave artifacts in system registry under HKCU\Software\Microsoft\Terminal Server Client\Default. Under this key, history of clients private IP addresses are listed. RDP also leaves username used for the connection and also with the client PC names under the registry key HKCU\Software\Microsoft\Terminal Server Client\Servers. [6]

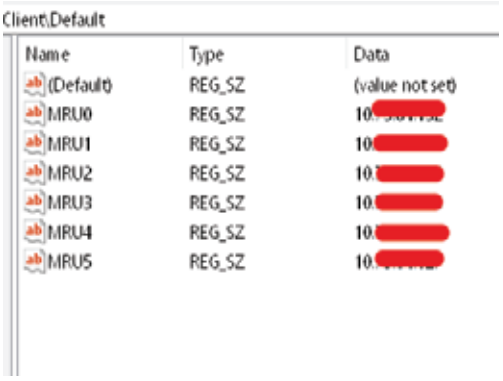

Figure 5 list of IP servers connected with client in registry

Figure 6 Username hint with IP address Server's in Windows Registry

4. Correlating RDP artifacts

RDP artifacts can help the forensics examiner to reconstruct events happened on the system. As explained, remote connection times, RDP client's IP, logon patterns and what a user was visualised on the remote desktop client can be retrieve from windows event logs, windows registry and remote desktop bitmap cache resident on user's profile. To prove a suspected logon initiated from system being analysed, Client IP, and username can be seen from Windows Registry. For a successful RDP logon, Event ID 1149 from remoteConnection-Manager.evtx is recorded, followed by ID 4624 (Security.evtx), 21 (LocalSessionManager.evtx) and event id 22 (LocalSessionManager.evtx).

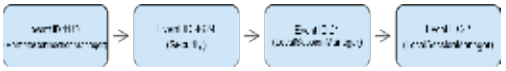

Figure 7 Event logs on Successful RDP Logon

Similarly, for RDP session logoff, find event log 23, 4634, 4647 and 9009 respectively.

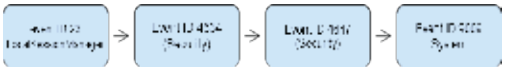

Figure 8 Event logs on RDP Session Logoff

RDP Session disconnect will generate following event ID as Event ID 24, 39, 40, 4779 and event ID 4634.

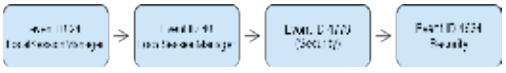

Figure 9 Event Log on RDP Session Disconnect

Logon times are important to be view here as they can used to find specific RDP bitmap

caches from client's system. RDP cache files (bcache.bmc and cache###.bin) created for each session at the time of RDP connection logon. After finding related bitmap cache then you can parse out bitmaps from the cache file to view activity done using RDP client. Bitmaps extracted from cache are usually in large numbers and analysing them is tedious process, as explained you can limit the search by correlating logon time from event logs with RDP cache creation times. Remote Desktop service also does leaves artifacts in windows registry where you can confirm IP and computer name of RDP server the client connecting to.

5. Summary

Remote Desktop Protocol is propriety of Microsoft Windows to provide GUI access to remote device. RDP follows client server model, where multiple clients exists on different operating systems, while the device to be remotely connected (remote desktop server) is usually on Windows environment. Threat actors uses RDP as their favourite initial attack vector in there malicious activities, various vulnerabilities also exists for remote desktop protocol. This makes RDP an important aspect to investigate in forensics investigations. Artifacts related to RDP can be retrieve from Windows Event logs, Windows Registry and RDP bitmap cache files to prove or disprove malicious activity attempted with the remote protocol. Differing usual Windows events from suspicious RDP activity can be tedious and difficult to understand. In this article system locations, Event Log Fields, tools and methods are discussed to understand RDP related activities.

6. References

1. Understanding Remote Desktop Protocol (RDP) - Windows Server. (2021a, September 24). Microsoft Learn. https://learn.microsoft.com/en-us/troubleshoot/windows-server/ remote/understanding-remote-desktop-protocol

2. Paubox. (2022, September 14). What is a remote desktop protocol attack? https://www.paubox.com/resources/what-is-remote-desktop-protocol-attack/

3. Remote Desktop Services (Remote Desktop Services) - Win32 apps. (2020, December 10). Microsoft Learn. https://learn.microsoft.com/en-us/windows/win32/termserv/terminal-services-portal?source=recommendations

4. Lauckner, K.N., 2020. Forensischer Nachweis eines Lateral Movement nach unberechtigtem RDP Zugriff (Doctoral dissertation).

5. Duranec, A. & Gruicic, Savina & Zagar, Marinko. (2020). Forensic analysis of Windows 10 Sandbox. 1224-1229. 10.23919/MIPRO48935.2020.924522

6. Kerai, P., 2010. Remote access forensics for vnc and rdp on windows platform.

7. ANSSI-FR/bmc-tools: RDP Bitmap Cache parser (github.com)

8. Chan, J. (2020, March 13). Do You Even Bitmap Cache, Bro? All Things DFIR. https://www.allthingsdfir.com/-

do-you-even-bitmap-cache-bro/

9. Swoboda, Andrew, Lane Thames, and Tyler Reguly. "RDP Fuzzing.

10. Ingalls, S. (2022, March 26). Addressing Remote Desktop Attacks and Security. eSecurityPlanet. https://www.esecurityplanet.com/threats/rdp-attacks/

11. Remote Desktop Protocol Use in Ransomware Attacks. (2022, May 6). RH-ISAC. https://rhisac.org/ransoware/remote-desktop-protocol-use-in-ransomware-attacks/

12. 2020 Unit 42 Incident Response and Data Breach Report. (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/resources/research/2020-unit42-incident-response-and-data-breach-report

13. Mark Loman, SOPHOS, How Ransomware attacks

14. [MS-RDPEGDI]: Bitmap Caches. (2021, June 24). Microsoft Learn. https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpegdi/2bf92588-42bd-4527-8b3e-b90c56e292d2

15. ANSSI-FR/bmc-tools: RDP Bitmap Cache parser (github.com)

16. brimorlabs/rdpieces: The home of the BriMor Labs rdpieces Perl script that tries to rebuild parsed RDP Bitmap Cache images (github.com)

17. BSI-Bund/RdpCacheStitcher: RdpCacheStitcher is a tool that supports forensic analysts in reconstructing useful images out of RDP cache bitmaps. (github.com)

18. Goretsky, A., & Goretsky, A. (2022b, September 13). RDP on the radar: An up-close view of evolving remote access threats. WeLiveSecurity. https://www.welivesecurity.com/2022/09/07/rdp-radar-up-close-view-evolving-remote-access-threats/

19. Schatz, Bradley. (2007). Digital evidence: representation and assurance.

20. Do, Quang, et al. "Windows event forensic process." IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, 2014.