RdpMon - Server-side RDP monitoring tool

https://github.com/cameyo/rdpmon

Overview

A monitoring tool for RDS servers that shows real-time and past RDP connections along with source IP, success and failure counts, logins, active and past session, executed processes and more.

RDP security and brute-force attacks

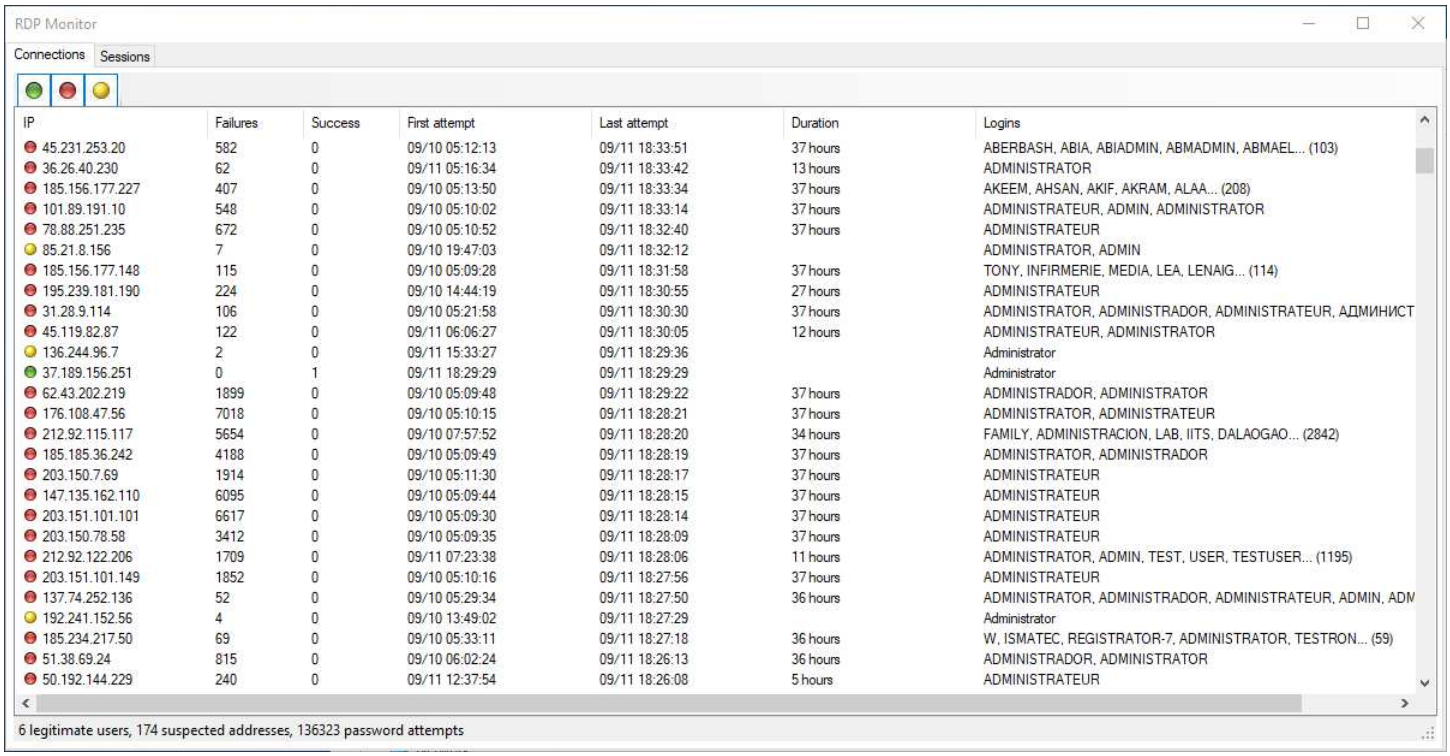
RDP is a fantastic technology, yet it brings some security challenges along, especially when it comes to cloud machines that are directly connected to the Internet. From our own observations once a cloud-connected machine with port 3389 is discovered by several bots, it undergoes **brute-force attacks** that amount to 100K - 200K password attempts per week. And in most cases it is difficult to even know about it. Also, security vulnerabilities that are discovered from time to time such as BlueKeep can make this even more challenging. Most RDP tools are designed to manage the Windows aspect of it such as users, quotas etc. But there is very little when it comes to cloud-oriented RDP security and management. RdpMon addresses the need of cloud-oriented RDP monitoring.

Usage

The first time you run RdpMon, it installs itself as a service named "RDP Monitor". The service part constantly logs in the background RDP activity targeted at the machine it runs on, even when you are logged off. The GUI part lets you view the logged activity as well as real-time connection and session events as they occur. Both parts are contained within the same executable: RdpMon.exe.

Connections

Under the Connections tab you can see RDP connections and connection attempts, grouped by IPs. IPs are marked by different colors: green=legitimate connections, red=high-intensity failed connections (likely brute-force attacks), yellow=low-intensity failed connections.



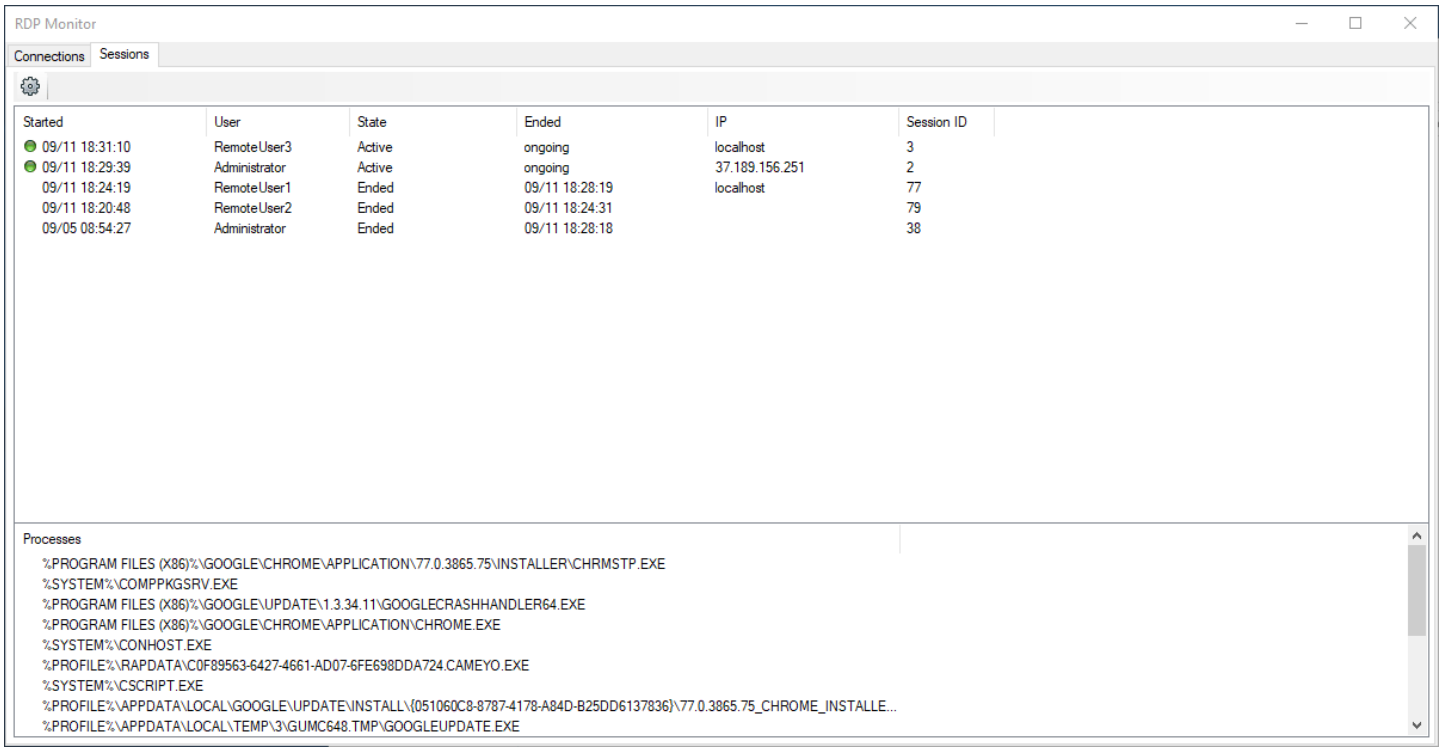
IP	Failures	Success	First attempt	Last attempt	Duration	Logins
45.231.253.20	582	0	09/10 05:12:13	09/11 18:33:51	37 hours	ABERBASH, ABIA, ABIADMIN, ABMADMIN, ABMAEL... (103)
36.26.40.230	62	0	09/11 05:16:34	09/11 18:33:42	13 hours	ADMINISTRATOR
185.156.177.227	407	0	09/10 05:13:50	09/11 18:33:34	37 hours	AKEEM, AHSAN, AKIF, AKRAM, ALAA... (208)
101.89.191.10	548	0	09/10 05:10:02	09/11 18:33:14	37 hours	ADMINISTRATEUR, ADMIN, ADMINISTRATOR
78.88.251.235	672	0	09/10 05:10:52	09/11 18:32:40	37 hours	ADMINISTRATEUR
85.21.8.156	7	0	09/10 19:47:03	09/11 18:32:12		ADMINISTRATOR, ADMIN
185.156.177.148	115	0	09/10 05:09:28	09/11 18:31:58	37 hours	TONY, INFIRMERIE, MEDIA, LEA, LENAIG... (114)
195.239.181.190	224	0	09/10 14:44:19	09/11 18:30:55	27 hours	ADMINISTRATEUR
31.28.9.114	106	0	09/10 05:21:58	09/11 18:30:30	37 hours	ADMINISTRATOR, ADMINISTRADOR, ADMINISTRATEUR, АДМИНИСТ
45.119.82.87	122	0	09/11 06:06:27	09/11 18:30:05	12 hours	ADMINISTRATEUR, ADMINISTRATOR
136.244.96.7	2	0	09/11 15:33:27	09/11 18:29:36		Administrator
37.189.156.251	0	1	09/11 18:29:29	09/11 18:29:29		Administrator
62.43.202.219	1899	0	09/10 05:09:48	09/11 18:29:22	37 hours	ADMINISTRADOR, ADMINISTRATOR
176.108.47.56	7018	0	09/10 05:10:15	09/11 18:28:21	37 hours	ADMINISTRATOR, ADMINISTRATEUR
212.92.115.117	5654	0	09/10 07:57:52	09/11 18:28:20	34 hours	FAMILY, ADMINISTRACION, LAB, IITS, DALAOGAO... (2842)
185.185.36.242	4188	0	09/10 05:09:49	09/11 18:28:19	37 hours	ADMINISTRATOR, ADMINISTRADOR
203.150.7.69	1914	0	09/10 05:11:30	09/11 18:28:17	37 hours	ADMINISTRATEUR
147.135.162.110	6095	0	09/10 05:09:44	09/11 18:28:15	37 hours	ADMINISTRATEUR
203.151.101.101	6617	0	09/10 05:09:30	09/11 18:28:14	37 hours	ADMINISTRATEUR
203.150.78.58	3412	0	09/10 05:09:35	09/11 18:28:09	37 hours	ADMINISTRATEUR
212.92.122.206	1709	0	09/11 07:23:38	09/11 18:28:06	11 hours	ADMINISTRATOR, ADMIN, TEST, USER, TESTUSER... (1195)
203.151.101.149	1852	0	09/10 05:10:16	09/11 18:27:56	37 hours	ADMINISTRATEUR
137.74.252.136	52	0	09/10 05:29:34	09/11 18:27:50	36 hours	ADMINISTRATOR, ADMINISTRADOR, ADMINISTRATEUR, ADMIN, ADM
192.241.152.56	4	0	09/10 13:49:02	09/11 18:27:29		Administrator
185.234.217.50	69	0	09/10 05:33:11	09/11 18:27:18	36 hours	W, ISMATEC, REGISTRATOR-7, ADMINISTRATOR, TESTRON... (59)
51.38.69.24	815	0	09/10 06:02:24	09/11 18:26:13	36 hours	ADMINISTRADOR, ADMINISTRATOR
50.192.144.229	240	0	09/11 12:37:54	09/11 18:26:08	5 hours	ADMINISTRATEUR

At the bottom, a status bar shows the overall counts:

6 legitimate users, 174 suspected addresses, 136323 password attempts

Sessions

Under the Sessions tab you can view both past and current RDP sessions. Clicking on a session in this list displays the processes that were / are used during this session. Live sessions are marked by a green bullet. Right-clicking on a live session allows shadowing it (=viewing the session in real time).



This project uses LiteDB for data storage.