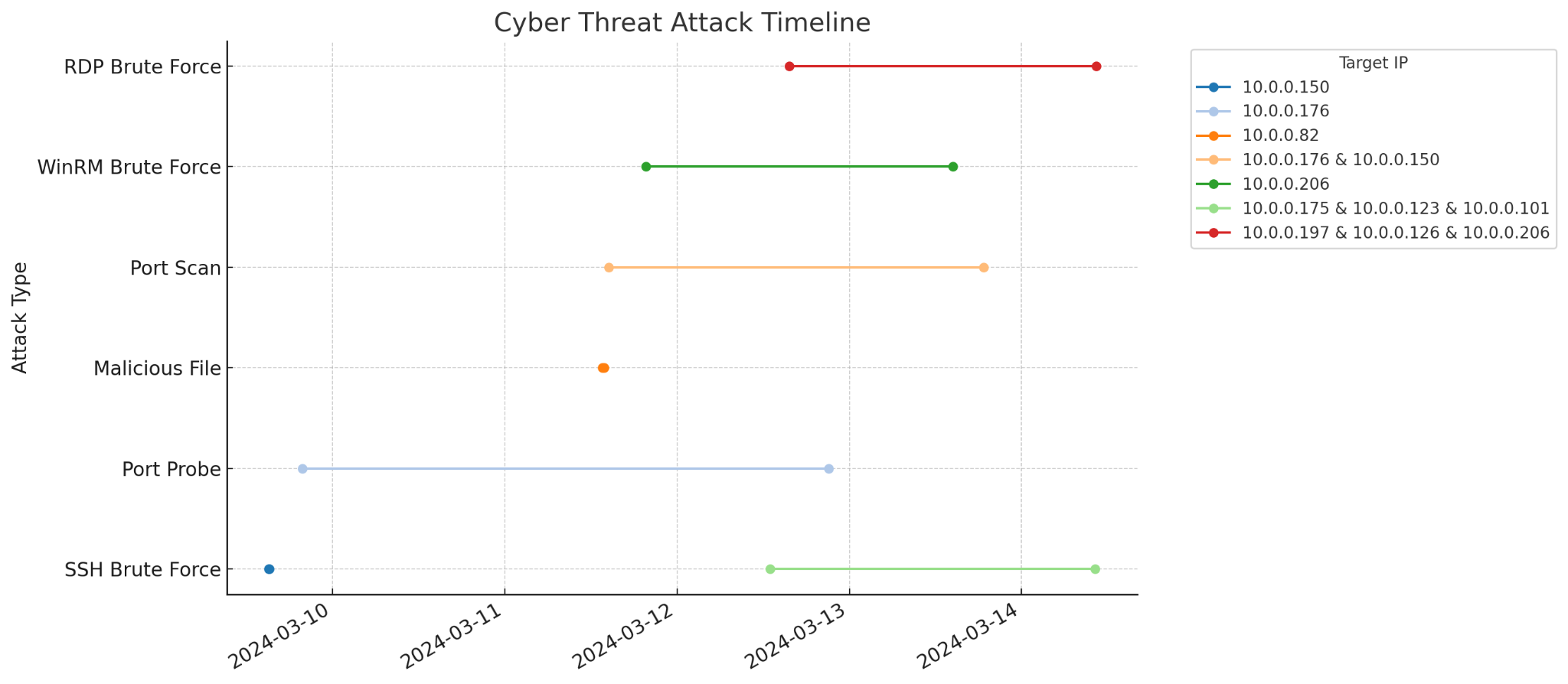
BT2 Cyber Threat Attack Timeline:

This timeline reveals a pattern of escalating attacks, starting with reconnaissance activities like port probes and scans, followed by brute force attacks leveraging both SSH and RDP, and culminating in the execution of a malicious file. It highlights the attackers' focus on identifying vulnerable targets, gaining unauthorized access, and potentially delivering payloads for further exploitation.



03-09-2024

15:02:26: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.150 | Last 03-09-2024 15:09:26

19:47:03: Recon:EC2/PortProbeUnprotectedPort | Target 10.0.0.176 | Last 03-12-2024 21:07:23

03-11-2024

13:35:09: Execution:EC2/MaliciousFile | Target 10.0.0.82 | Last 03-11-2024 13:51:10

14:26:13: Recon:EC2/Portscan | Target 10.0.0.176 | Last 03-13-2024 18:40:57

19:36:32: Impact:EC2/WinRMBruteForce | Target 10.0.0.206 | Last 03-13-2024 13:16:34

21:08:38: Impact:EC2/WinRMBruteForce | Target 10.0.0.206 | Last 03-13-2024 14:28:03

20:00:35: Recon:EC2/Portscan | Target 10.0.0.150 | Last 03-13-2024 12:34:31

03-12-2024

12:55:24: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.175 | Last 03-13-2024 22:44:46

12:55:34: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.175 | Last 03-13-2024 22:45:13

13:36:51: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.175 | Last 03-14-2024 10:16:11

15:38:01: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.197 | Last 03-14-2024 10:16:11

15:39:14: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.197 | Last 03-14-2024 10:23:14

18:46:46: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.101 | Last 03-12-2024 19:47:17

19:23:01: UnauthorizedAccess:EC2/SSHBruteForce | Target 10.0.0.123 | Last 03-14-2024 04:51:01

03-13-2024

01:15:17: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.126 | Last 03-13-2024 19:35:18

14:32:45: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.206 | Last 03-13-2024 15:30:46

14:33:03: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.206 | Last 03-13-2024 15:33:06

15:11:46: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.206 | Last 03-13-2024 19:58:45

19:28:03: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.126 | Last 03-14-2024 10:16:11

19:28:24: UnauthorizedAccess:EC2/RDPBruteForce | Target 10.0.0.126 | Last 03-14-2024 10:23:24

03-14-2024

04:51:01: End of the last reported attack incident targeting 10.0.0.123 with SSH brute force.

10:16:11 to 10:23:24: Concluding activities with RDP brute force attacks on targets 10.0.0.197 and 10.0.0.126.

Reference

<https://chat.openai.com/share/5c9688d5-1ec0-4da5-b8cb-6e356dd96703>

This report outlines a series of unauthorized access and reconnaissance attempts targeting various IP addresses within an EC2 network over several days. The incidents involve SSH brute force attacks, port probes, execution of malicious files, port scans, and WinRM brute force attacks. Notably, IP addresses 10.0.0.206 and 10.0.0.175 were frequently targeted, with 10.0.0.206 facing multiple WinRM and RDP brute force attempts. The activity spanned from March 9, 2024, with the last reported incident occurring on March 14, 2024, marking the end of the reported attacks with SSH brute force targeting 10.0.0.123 and concluding RDP brute force activities on 10.0.0.197 and 10.0.0.126.