Brute Ratel Utilized By Threat Actors In New Ransomware Operations

Published: 2022-07-07 · Archived: 2026-04-05 19:24:37 UTC

When Brute Ratel first appeared in the wild, almost no security solutions could detect it. To avoid being discovered by EDR and antivirus programs, hacking groups and ransomware operations are switching from Cobalt Strike to the more recent Brute Ratel post-exploitation toolkit.

One of the most popular toolkits in red team engagements is Cobalt Strike, which enables attackers to install beacons on compromised devices to conduct remote network surveillance or send commands.

Hacker groups and ransomware attacks also use this tool to expand laterally through infected corporate networks.

To replace Cobalt Strike for red team penetration testing engagements, ex-red team member Chetan Nayak published Brute Ratel Command and Control Center (BRc4) in 2020.

About Brute Ratel

Brute Ratel is the most advanced red team simulation software at the moment. It can provide a structured timeline and simulate the cyber kill chain. Cybersecurity teams can use it to validate cyberattacks and strengthen their defenses. Despite being a post-exploitation tool, it does not assist in creating exploits.

Brute Ratel enables the red team to deploy badgers on remote hosts. Badgers function similarly to Cobalt Strike beacons and connect to the attacker's C2 server for RCE.

Brute Ratel's features and more details can be found on the software's official site.

Threat Actors Were Able To Acquire Licenses

Despite Cobalt Strike being a legal piece of software, threat actors have been spreading cracked versions of it online, making it one of the most widely utilized tools by hackers and ransomware operations.

Brute Ratel is currently only available to verified companies at a cost. Chetan Nayak, the developer of Brute Ratel, stated that the license was leaked by a customer's employee, explaining how the attackers could use it in their operations.

Although Nayak could revoke the license afterward, former Conti ransomware members were discovered using fake company profiles to gain access to the software's license.

"In one case, they have gained access to the Brute Ratel kit used for post-exploitation in targeted attacks from BumbleBee loader. The ultimate goal of the Brute Ratel usage was the post-exploitation framework for lateral movement and subsequent network encryption via ransomware payload." AdvIntel's CEO said.

Threat actors spread malicious ISOs that appear to include submitted resumes (CV) in attacks thought to be connected to the Russian state-sponsored hacking organization APT29 (also known as CozyBear and Dukes).

Malicious ISO file's contents (Source: Bleeping Computer)

However, as seen in the file's properties below, the Roshan-Bandara_CV_Dialog resume file is a Windows shortcut that will start the included OneDriveUpdater[.]exe file.

Windows shortcut disguised as CV to launch a program (Source: Bleeping Computer)

Upon clicking **Roshan-Bandara_CV_Dialog, cmd[.]exe** is launched:

/c start OneDriveUpdater[.]exe (Using the Windows start command, the executable is launched from the current directory)

Microsoft's executable is used to sync data to Cloud servers. It is used in this instance to load the attacker's DLL.

version.dll, a dependency of **OneDriveUpdater[.]exe**, is in the same directory. The actors modified this DLL to load an encrypted payload file (**OneDrive.update**).

The file is subsequently decrypted, and the modification's first stage of the shellcode is loaded into memory. To preserve code capabilities, threat actors also use DLL proxying technique (**vresion.dll for version.dll**).

The in-memory code, Brute Ratel C4, starts to communicate with **IP 174.129.157[.]251** on TCP port 443 as a Windows thread while running in the RuntimeBroker[.]exe process space.

The below image shows how ISOs would look if the show hidden files option were enabled.

ISOs appear when "Show hidden files" is enabled (Source: Unit42)

OneDriveUpdater[.]exe is a legal Microsoft executable, but the **version[.]dll** it loads has been altered to serve as a loader for a Brute Ratel badger that is loaded into the **RuntimeBroker[.]exe** process.

The threat actors can remotely access the infected device once the Brute Ratel has been loaded in order to run commands and spread farther throughout the compromised network.

Brute Ratel C4 ISO Samples:

1FC7B0E1054D54CE8F1DE0CC95976081C7A85C7926C03172A3DDAA672690042C

X64 Brute Ratel C4 Windows Kernel Module:

31ACF37D180AB9AFBCF6A4EC5D29C3E19C947641A2D9CE3CE56D71C1F576C069

APT29 ISO Samples:

F58AE9193802E9BAF17E6B59E3FDBE3E9319C5D27726D60802E3E82D30D14D46

X64 Brute Ratel C4 Samples:

3ED21A4BFCF9838E06AD3058D13D5C28026C17DC996953A22A00F0609B0DF3B9
3AD53495851BAFC48CAF6D2227A434CA2E0BEF9AB3BD40ABFE4EA8F318D37BBE
973F573CAB683636D9A70B8891263F59E2F02201FFB4DD2E9D7ECBB1521DA03E
DD8652E2DCFE3F1A72631B3A9585736FBE77FFABEE4098F6B3C48E1469BF27AA
E1A9B35CF1378FDA12310F0920C5C53AD461858B3CB575697EA125DFEE829611
EF9B60AA0E4179C16A9AC441E0A21DC3A1C3DC04B100EE487EABF5C5B1F571A6
D71DC7BA8523947E08C6EEC43A726FE75AED248DFD3A7C4F6537224E9ED05F6F
5887C4646E032E015AA186C5970E8F07D3ED1DE8DBFA298BA4522C89E547419B

Malicious DLLs:

EA2876E9175410B6F6719F80EE44B9553960758C7D0F7BED73C0FE9A78D8E669

Malicious Encrypted Payloads:

B5D1D3C1AEC2F2EF06E7D0B7996BC45DF4744934BD66266A6EBB02D70E35236E

X.509 Cert SHA1s:

55684a30a47476fce5b42cbd59add4b0fbc776a3
66aab897e33b3e4d940c51eba8d07f5605d5b275

Infrastructure linked to X.509 Certs or Samples:

104.6.92[.]229
137.184.199[.]17
138.68.50[.]218
138.68.58[.]43
139.162.195[.]169
139.180.187[.]179
147.182.247[.]103
149.154.100[.]151
15.206.84[.]52
159.223.49[.]16
159.65.186[.]50
162.216.240[.]61
172.105.102[.]247
172.81.62[.]82
174.129.157[.]251
178.79.143[.]149
178.79.168[.]110
178.79.172[.]35
18.133.26[.]247
18.130.233[.]249
18.217.179[.]8

18.236.92[.]31
185.138.164[.]112
194.29.186[.]67
194.87.70[.]14
213.168.249[.]232
3.110.56[.]219
3.133.7[.]69
31.184.198[.]83
34.195.122[.]225
34.243.172[.]90
35.170.243[.]216
45.144.225[.]3
45.76.155[.]71
45.79.36[.]192
52.48.51[.]67
52.90.228[.]203
54.229.102[.]30
54.90.137[.]213
89.100.107[.]65
92.255.85[.]173
92.255.85[.]44
94.130.130[.]43
ds.windowsupdate.eu[.]org
