Cracked Brute Ratel C4 framework proliferates across the cybercriminal underground

By Will Thomas

Published: 2022-10-05 · Archived: 2026-04-05 14:32:28 UTC

Since mid-September, English-speaking and Russian-speaking cybercriminal underground forums having been buzzing with activity following the leaking and cracking of the Brute Ratel C4 (BRC4) post-exploitation toolkit.

This significant event is exemplary of the type of underground forum activity that the SANS FOR589: Cybercrime Intelligence course will cover, and this blog highlights key aspects of how FOR589 will teach students to generate actionable intelligence via monitoring the cybercriminal underground. This includes:

- How to identify what is actionable and what is noise within the cybercriminal underground
- How to spot significant evolutions and changes within the underground ecosystem
- How to act as an early warning system for defenders and responders about imminent threats to organizations

Practitioners can sign up for the BETA of this course on the SANS website by selecting 'FOR589: Cybercrime Intelligence' and by registering with their information.

Et tu Brute Ratel?

For those unacquainted with Brute Ratel, it was developed by Chetan Nayak, a former offensive security professional who previously worked for Mandiant and CrowdStrike. It is an emerging Red Teaming framework, similar to Sliver, Mythic, and Covenant, that all lag behind the most popular tool, which has been Cobalt Strike for several years. Much like Cobalt Strike, Brute Ratel enables operators to deploy agents, called badgers, while inside a target environment that enable arbitrary command execution to perform lateral movement, privilege escalation, and establish additional avenues of persistence.

The leak of a cracked version of Brute Ratel proves to be a significant event when we reflect on the precedent set by the leak of a cracked version of Cobalt Strike, back in November 2020, when the source code for Cobalt Strike 4.0 was shared via GitHub. Consequently, that leak bolstered free access to Cobalt Strike for threat actors within the cybercriminal underground; since then, Cobalt Strike has been widely adopted by threat actors, particularly ransomware affiliates, as well as nation state advanced persistent threat (APT) groups.

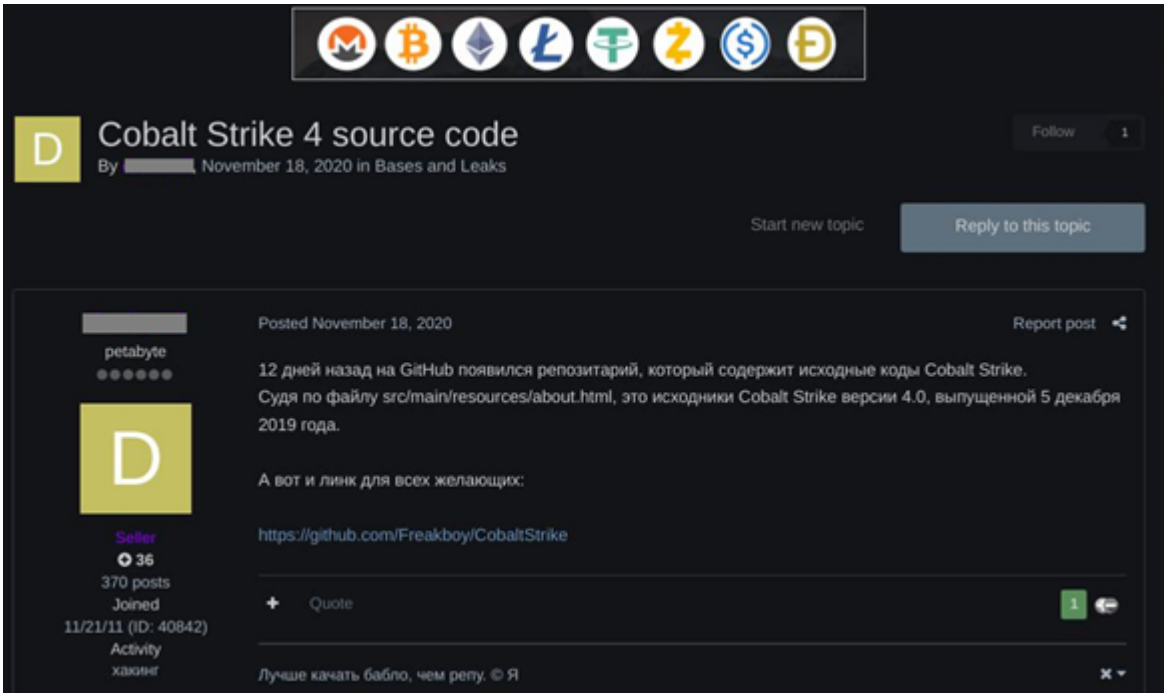

Figure 1: Cobalt Strike 4.0 source code offered on Exploit[.]in

Due to this, security products have heavily focused on detecting the tool and it is no longer as proficient as it once was for adversaries. As a result, it has been reported that some threat actors have gone as far as creating spurious US-based firms to be able to bypass Brute Ratel's licensing verification so they can leverage the new toolkit. The developer of Brute Ratel, Chetan Nayak, could then revoke these licenses for any malicious customers using the framework for cybercrime.

The newly cracked version of Brute Ratel 1.2.2, however, now means that that anyone can use the framework and bypass the license verification system. Chetan Nayak found that the uncracked version was uploaded to VirusTotal and was subsequently cracked by a Russian-speaking group called "Molecules" who reverse engineered and bypassed the license check.

A version of Brute Ratel was uploaded to VirusTotal at 19:59:20 UTC on 13 September 2022, via an archive file called "bruteratel_1.2.2.Scandinavian_Defense.tar.gz". Chetan Nayak confirmed this file contains a valid copy of BRC4 version 1.2.2/5. It was then cracked and was floating around private Telegram groups until it made its way to the mainstream cybercrime forums.

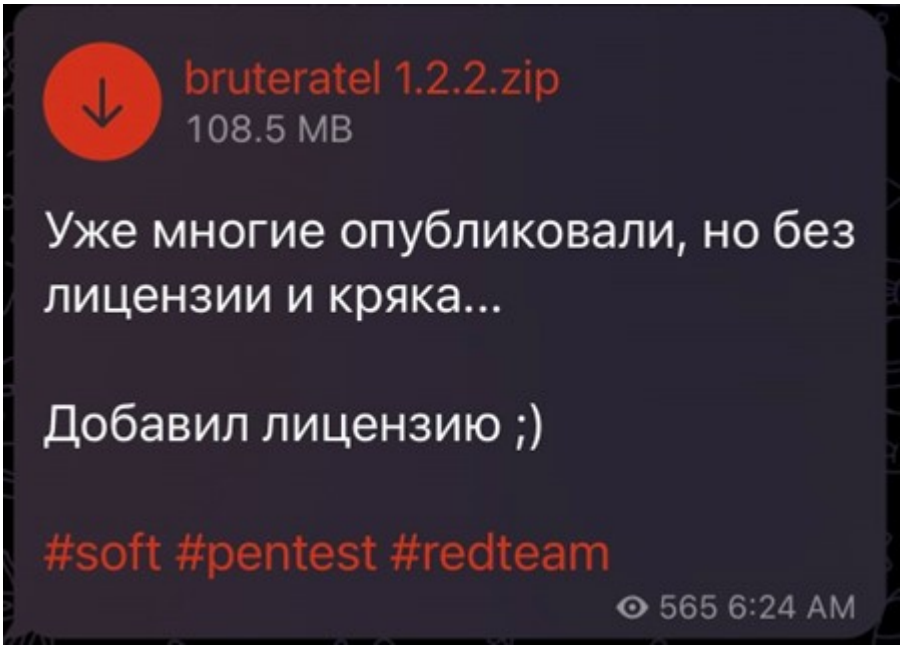

Figure 2: A cracked version of Brute Ratel v1.2.2 shared on a Russian-speaking Telegram channel (Source: Twitter)

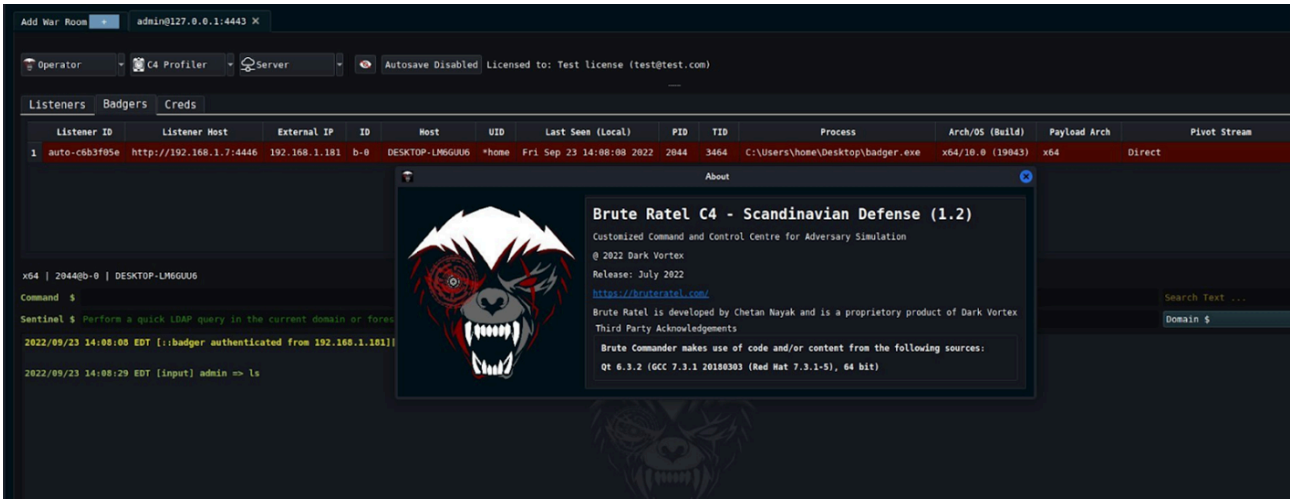

Figure 3: Screenshot of Brute Ratel C4 – Scandinavian Defense (1.2)

This cracked version has since been distributed across the popular cybercrime forums where data brokers, malware developers, initial access brokers, and ransomware affiliates all reside. This includes BreachForums, CryptBB, RAMP, Exploit[.]in, and XSS[.]is (aka DaMaGeLaB), as well as other communities on Discord and Telegram.

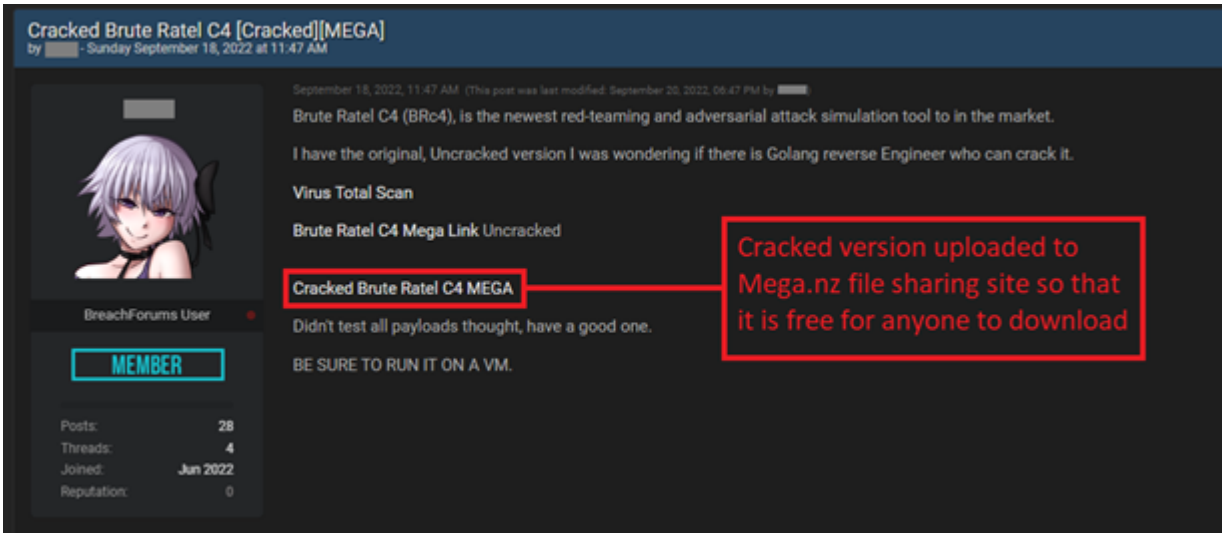

Figure 4: Cracked version of Brute Ratel shared to BreachForums

Figure 5: Cracked version of Brute Ratel shared to Exploit[.]in

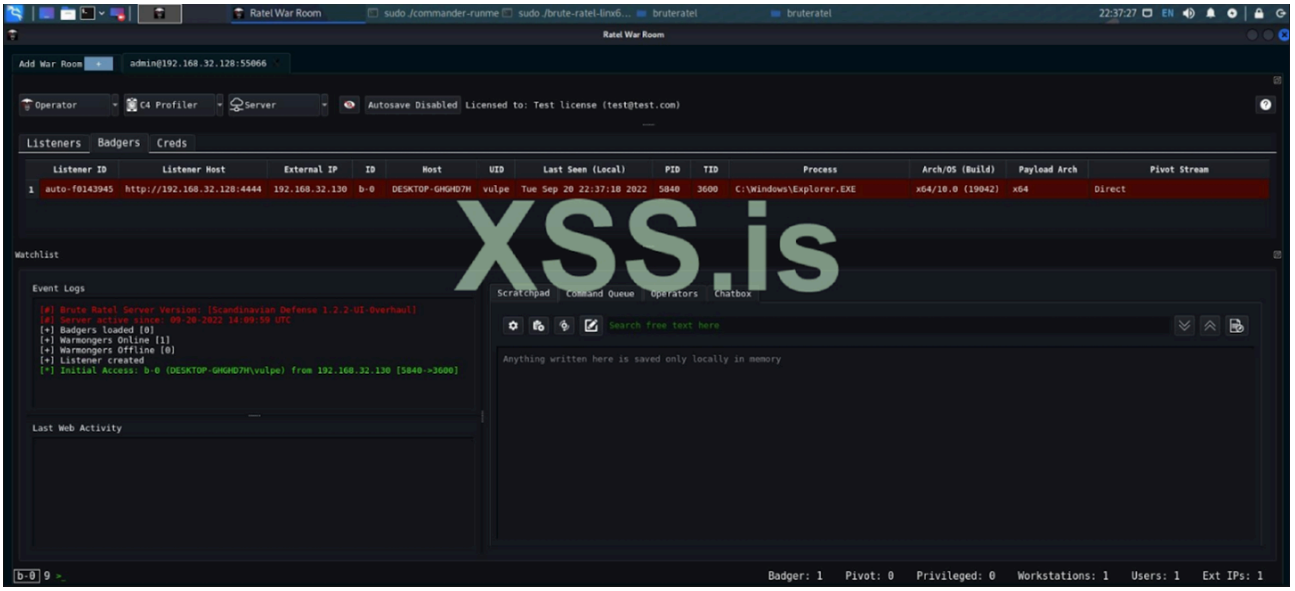

Figure 6: User of XSS[.]is testing the cracked version of Brute Ratel

So What?

One of the most concerning aspects of Brute Ratel for many security experts is its ability to generate shellcode that is undetected by many endpoint detection and response (EDR) and antivirus (AV) products. This means that every new attack creates unique indicators of compromise (IOCs). The developer of Brute Ratel has demonstrated the tool's proficiency at doing so; for example, on 29 September 2022, the developer shared a video on YouTube called "Evading Elastic EDR in Full Prevent Mode with Brute Ratel C4."

This extended window of detection evasion can give threat actors enough time to establish initial access, begin lateral movement, and achieve persistence elsewhere. Brute Ratel's capabilities closely align with the objectives of ransomware groups that are already highly active and looking for new windows of opportunity. In July 2022, Sophos incident responders confirmed they encountered Brute Ratel in the wild, alongside Cobalt Strike, at an ALPHV (aka BlackCat) ransomware engagement. This compounds our assessment that cybercriminals, especially ransomware affiliates, are going to be using this tool in the foreseeable future.

Further, to prevent Brute Ratel, defenders may try to gather and block related IOCs. However, due to Brute Ratel's unique generation of evasive new payloads, it makes the practise of blocking of file hashes an inadequate countermeasure. Therefore, It is recommended that defenders implement behavioral-based detection opportunities to thwart attempts, like those outlined in blogs by MdSec and Palo Alto Networks Unit 42.

Overall, enterprises and public sector organizations should recognize the imminent threat of the proliferation of this tool in the hands of organized cybercriminal groups.

Uncracked and cracked versions of Brute Ratel C4 shared on VirusTotal

- Uncracked: "BruteRatel_1.2.2.Scandinavian_Defense.tar.gz" - available here
- Cracked: "bruteratel 1.2.2-Cracked.zip" - available here
