Quorum Cyber

Threat Intelligence Brute Ratel C4 Post-Exploitation Tool

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	12/02/2023	Initial Report Drafted
0.2	12/06/2023	Report Update
1.0	12/06/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

Brute Ratel C4

Overview

Brute Ratel C4 (Customised Command and Control Centre) is a commercial, full-featured, remote access tool that is incorporated as an adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. including APT29[1]. Brute Ratel's interactive post-exploit capabilities cover the full range of Mite ATT&CK techniques, all of which are executed within a single, integrated system.

Brute Ratel C4 is equipped with debugger programming that detects Endpoint Detection and Response (EDR) monitoring. The framework then takes action to avoid triggering detection, making the software particularly dangerous to network security. Additionally, Brute Ratel C4 is a malware as a service, therefore resulting in a vast scope of exploitability.

The malware is primarily distributed via phishing emails and exploiting Dynamic Link Library (DLL) hijacking vulnerabilities in Windows operating systems. Brute Ratel C4 has also been implemented in conjunction with other malware variants such as Cobalt Strike and Qakbot.

Impact

The Brute Ratel C4 framework contains a debugger component that recognises EDR hooks, thus preventing detection. Brute Ratel also incorporates a visual interface for LDAP queries. Upon execution of the software, malicious payloads are dropped via DLL search order hijacking.

The current version of the software offers the availability to form command-and-control channels via legitimate programmes, such as Microsoft Teams and Slack. The platform can leverage undocumented syscalls to avoid being detected and subsequently inject shellcode into process that have been previously activated[2]. Brute Ratel enables operators to deploy agents, called badgers, whilst in the realm of a target environment, that enable arbitrary command execution to perform lateral movement, privilege escalation, and establish additional channels of persistence.

Vulnerability Detection

Researchers at Palo Alto have documented[3] that the implant replaces a legitimate Microsoft library file with a malicious version. The original file is renamed, "vresion.dll", and function calls are proxied to it from the malicious library. A quick way to detect the implant is to look for the existence of this renamed .dll file.

Within the context of the Microsoft Defender suite, the following advanced hunting query can be implemented to detect the presence the associated Brute Ratel C4 malicious files:

```
DeviceImageLoadEvents
| where FileName == @"vresion.dll"
```

[1] APT 29 Using Brute Ratel (polyswarm.io)
[2] Brute Ratel-Powered Attacks Detection: Post-Exploitation Toolkit Leveraged by Adversaries - SOC Prime
[3] Brute Ratel C4 Red Teaming Tool Being Abused by Malicious Actors (paloaltonetworks.com)

Affected Products

- Windows Operating System

Containment, Mitigations & Remediations

Due to the nature of the Brute Ratel C4 framework being that of adversary emulation testing software, the following mitigation steps are recommended to be adhered to with regards to the potential malicious exploit of the software:

- Use strict password management and least privilege access policies.
- Reinforce social engineering and anti-phishing awareness training.
- Identify which systems, applications, and data lakes are mission-critical to your business and day-to-day operations.
- Implement frequent backups of crucial files and isolate them from local and open networks. Maintain offline backup copies of data stored in locations inaccessible from infected systems.
- Promptly patch software and applications and maintain awareness with regards to vulnerability advisories.
- Implement and practice a digital disaster recovery plan.

Indicators of Compromise

Brute Ratel C4 File Hashes (SHA-256):

- 973f573cab683636d9a70b8891263f59e2f02201ffb4dd2e9d7ecbb1521da03e
- 62cb24967c6ce18d35d2a23ebed4217889d796cf7799d9075c1aa7752b8d3967
- 3ed21a4bfcf9838e06ad3058d13d5c28026c17dc996953a22a00f0609b0df3b9
- 3ad53495851bafc48caf6d2227a434ca2e0bef9ab3bd40abfe4ea8f318d37bbe
- 3a946cba2ba38a2c6158fa50beee20d2d75d595acc27ea51a39a37c121082596
- 5f6e4617c2e716956eff9c704d294af6d933a8d9f78428f3231f005e4f34dc5
- c41f9d6bf97b9bf74ca62e8618f063d55fcb7d24d2ca76f1e3e16b475c1ac2a4
- e1a9b35cf1378fda12310f0920c5c53ad461858b3cb575697ea125dfee829611
- 09e48e03857a4c2c4b5b6997ce09c6b335c11da5bfb7cb562da113883a959a5e
- 2ddc77de26637a6d759e5b080864851b731fdb11075485980ece20d8f197104c
- 3ac2eadeca1c203cd66658f87997000f196737f789ce45cb4f0dd07a2d91ce34
- 59f6f217c4696ff6b93f268293cfa14536649ac57454b0db7f455cbfc55d2075
- 5e9ba02f4ce8c1c658fd631003a07a8d372d3a4e48bf09ffe5d001d2a145e54e
- 66155a82f70e078776e11d0d75ea77e7a2a71f633b0b2187f1064535bba3a9c5
- 75d190fe122709f7130cb8bfb61dc8a318cdfc208b653c0a0f829c8fa62d0e51
- 7982ad325c8f2f41d309c2f20bc7f45ee2fd0663d0273ecbc2050be8c5ddd5ba

- 9d2d583a31e3f65675ac3ef863e31a792c6cf8f6671ee7d194d244fff7c0cf0b
- a4cac4a93cfb04af5740327e1efb915c5ef6833d3fdf107c89601e5afb7d8e0e
- b37396d224275110f26940f1748faef43a716cd7d641cc5dcc8f3e75da800b12
- d133cdc924035ec3088dc708fa63f9ce69b5353cb6aa3a35de019639e442e1f4

Brute Ratel C4 Associated IP Addresses:

- 149[.]28[.]251[.]203
- 159[.]65[.]186[.]50
- 37[.]119[.]57[.]195
- 13[.]82[.]141[.]216
- 18[.]163[.]6[.]122
- 167[.]71[.]62[.]156
- 13[.]114[.]48[.]174
- 167[.]99[.]137[.]218
- 52[.]68[.]31[.]77
- 35[.]79[.]109[.]52
- 107[.]148[.]27[.]54
- 54[.]168[.]127[.]93
- 52[.]194[.]85[.]123
- 54[.]248[.]200[.]60
- 35[.]72[.]100[.]201
- 54[.]95[.]222[.]110
- 51[.]77[.]112[.]254
- 159[.]203[.]77[.]32
- 172[.]105[.]235[.]229

Brute Ratel C4 Associated Domains

- symantecuptimehost[.]com

Threat Landscape

Brute Ratel C4 is a standardised post-exploitation framework that that can be used by threat actors to target the majority of organisations within both the public and private sectors. Threat actors has been reported to have bypassed the software licensing verification system, for Brute Ratel version 1.2.2, in order to implement it for malicious purposes. The uncracked version has been detected to have been cracked by the Russian group, "Molecules"[4]. This cracked version has since been distributed across popular cybercrime forums, within which various entities reside. These include data brokers, malware developers, initial access brokers, and ransomware affiliates. It is likely that, as with alternative exploited red team testing frameworks such as Cobalt Strike, the cracked version of Brute Ratel will become an attractive tool for ransomware affiliates moving forward.

[4] Cracked Brute Ratel C4 framework proliferates across the cybercriminal underground | SANS

Threat Group

The BlackBasta ransomware group have been linked to the utilisation of the Brute Ratel C4 malware. Despite the groups relatively recent formation, it is highly likely that the group is composed of experienced cyber criminals who have experience with attack vectors, such as ransomware extortion tactics. This would be due to the fact that the double extortion technique is implemented, as well as the groups observed significant rise to notoriety. Moreover, researchers as Sophos reported that the framework was used in a ransomware engagement correlating to the BlackCat (ALPHV) ransomware group[5].

Brute Ratel C4 Mitre Methodologies

Resource Development
T1588.002 - Obtain Capabilities: Tool[6]

Initial Access
T1566.001 - Spearphishing Attachment[7]

Execution
T1204 - Malicious File[8]

Privilege Escalation
T1055 - Process Injection[9]
T1055.001 - Dynamic-link Library Injection[10]

Defence Evasion
T1027 - Obfuscated Files or Information[11]
T1036.004 - Masquerade Task or Service[12]
T1036.005 - Match Legitimate Name or Location[13]
T1055 - Process Injection[14]
T1055.001 - Dynamic-link Library Injection[15]
T1140 - Deobfuscate/Decode Files or Information[16]
T1497.003 - Virtualization/Sandbox Evasion: Time Based Evasion[17]
T1564 - Hide Artifacts[18]
T1620 - Reflective Code Loading[19]

Credential Access
T1056.001 - Keylogging[20]

---

[5] Cracked Brute Ratel C4 framework proliferates across the cybercriminal underground | SANS
[6] Obtain Capabilities: Tool, Sub-technique T1588.002 - Enterprise | MITRE ATT&CK®
[7] Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise | MITRE ATT&CK®
[8] User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®
[9] Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®
[10] Process Injection: Dynamic-link Library Injection, Sub-technique T1055.001 - Enterprise | MITRE ATT&CK®
[11] Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®
[12] Masquerading: Masquerade Task or Service, Sub-technique T1036.004 - Enterprise | MITRE ATT&CK®
[13] Masquerading: Match Legitimate Name or Location, Sub-technique T1036.005 - Enterprise | MITRE ATT&CK®
[14] Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®
[15] Process Injection: Dynamic-link Library Injection, Sub-technique T1055.001 - Enterprise | MITRE ATT&CK®
[16] Deobfuscate/Decode Files or Information, Technique T1140 - Enterprise | MITRE ATT&CK®
[17] Virtualization/Sandbox Evasion: Time Based Evasion, Sub-technique T1497.003 - Enterprise | MITRE ATT&CK®
[18] Hide Artifacts, Technique T1564 - Enterprise | MITRE ATT&CK®
[19] Reflective Code Loading, Technique T1620 - Enterprise | MITRE ATT&CK®
[20] Input Capture: Keylogging, Sub-technique T1056.001 - Enterprise | MITRE ATT&CK®

Discovery
T1046 - Network Service Discovery[21]
T1087 - Account Discovery[22]
T1497.003 - Virtualization/Sandbox Evasion: Time Based Evasion[23]

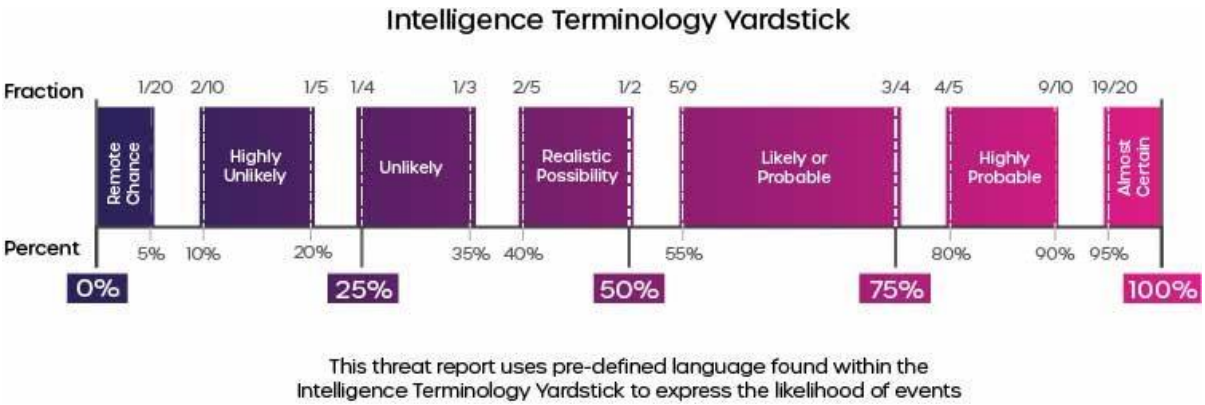
Collection
T1056.001 - Keylogging[24]
T1113 - Screen Capture[25]

Command and Control
T1104 - Multi-Stage Channels[26]

Further Information

- PolySwarm Blog: PolySwarm Article
- SOC Prime Report: SOC Prime Report
- Unit42 Report: Unit42 Report
- SANS Report: SANS Report

Intelligence Cut-off Date (ICoD): 12/06/2023 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

[21] Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®
[22] Account Discovery, Technique T1087 - Enterprise | MITRE ATT&CK®
[23] Virtualization/Sandbox Evasion: Time Based Evasion, Sub-technique T1497.003 - Enterprise | MITRE ATT&CK®
[24] Input Capture: Keylogging, Sub-technique T1056.001 - Enterprise | MITRE ATT&CK®
[25] Screen Capture, Technique T1113 - Enterprise | MITRE ATT&CK®
[26] Multi-Stage Channels, Technique T1104 - Enterprise | MITRE ATT&CK®