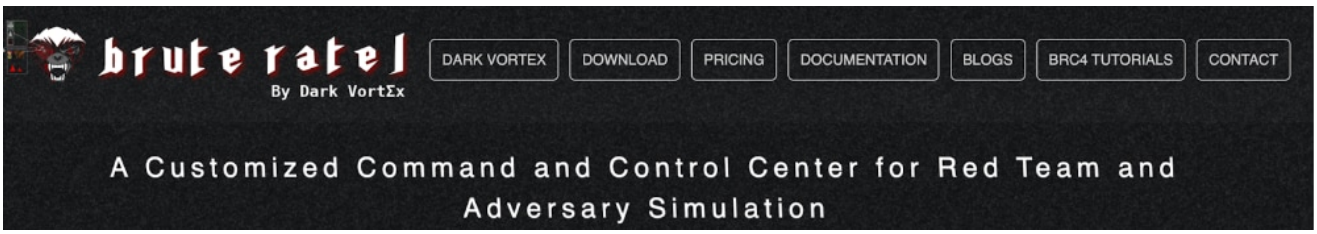
How to detect Brute Ratel activities

andreafortuna.org/2023/02/23/how-to-detect-brute-ratel-activities

Andrea Fortuna February 23, 2023

Feb 23, 2023

Brute Ratel (BRc4) is a *Command and Control* (C2) framework designed to help attackers evade defence systems and remain undetected while executing malicious commands. Used in simulations of real-world attacks, this tool helps red team members deploy badgers on remote hosts. Badgers are similar to **Cobalt Strike** beacons and connect attackers to a remote command and control server, providing them with remote code execution capabilities.



The current version of Brute Ratel allows users to create command-and-control channels using legitimate tools such as **Microsoft Teams**, **Slack** and **Discord**. It also uses undocumented syscalls instead of standard Windows API calls to avoid detection, and injects shellcode into running processes. **BRc4** includes a debugger capable of detecting and bypassing **EDR** hooks and detections, as well as an easy-to-use visual interface to assist with **LDAP** queries across domains.

Similar to what I did in a previous post focusing on the ***Sliver framework***, I try to outline a multi-layered approach to detecting malicious activity related to this tool, focusing on use of endpoint detection and response (EDR) tools, network traffic analysis, and file system monitoring.

Network Traffic Analysis

The detection of Brute Ratel traffic patterns is not easy, because the framework allows attackers to hide malicious traffic into communications with legitimate tools such as **Microsoft Teams**, **Slack** and **Discord**.

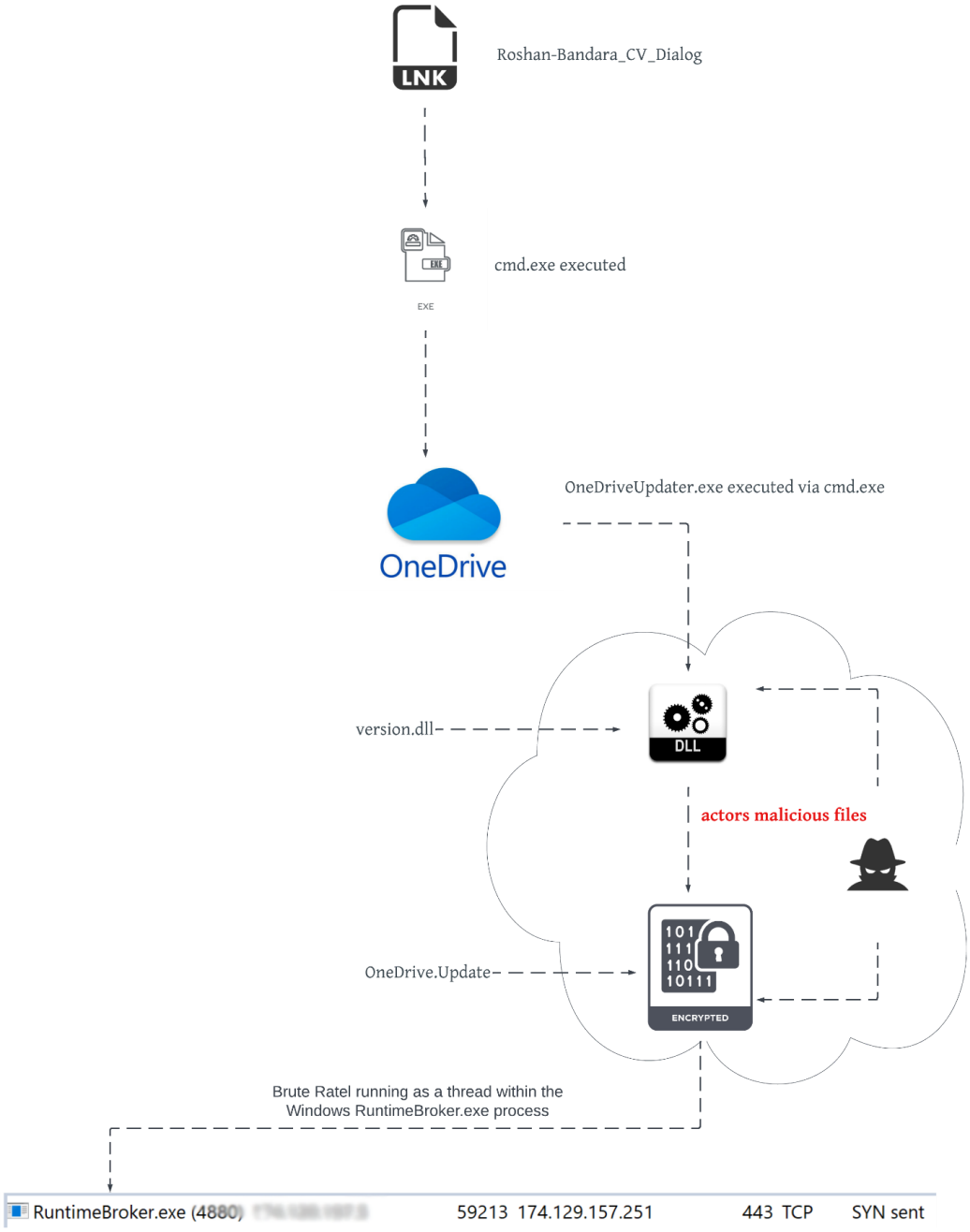
However, in this article the security firm **YOROI** suggests using the following Yara rule:

```
rule brute_ratel
{
    meta:
        author = "Yoroi Malware ZLab"
        description = "Rule for BruteRatel Badger"
        last_updated = "2023-02-15"
        tlp = "WHITE"
        category = "informational"

    strings:
        $1 =
{8079ffcc74584585c075044883e920448a094180f9e9740a448a41034180f8e97507ffc24531c0ebd731
c04180f94c752f8079018b7529807902d175214180f8b8751b8079060075170fb64105c1e0084189c00fb
641044409c001d0eb0231c0c3} // Checks Breakpoint (DLL)
        $2 = {565389d34883ec2885db74644889cee8????????31c9ba????????4989c0e8????????
448d430165488b142530000000488b5260488b4a30ba08000000ffd04885f6741c4885c0742731d20f1f4
400000fb60c16880c104883c2014839d375f04883c4285b5ec3} // Shellcode
    condition:
        (uint16(0) == 0x5A4D or uint16(0) == 0x00E8 or uint16(0) == 0x8348) and ($1
or $2)
}
```

File System Monitoring

According to article by **Unit42** and **Splunk**, recent campaigns using **Brutal Rater** have exploited fake **Microsoft OneDrive** installers encapsulated in .iso files to minimise detection by antivirus software.



This information can be used to create a hash list of possible files associated with payload implantation attempts:

SHA
1FC7B0E1054D54CE8F1DE0CC95976081C7A85C7926C03172A3DDAA672690042C
31ACF37D180AB9AFBCF6A4EC5D29C3E19C947641A2D9CE3CE56D71C1F576C069

SHA
F58AE9193802E9BAF17E6B59E3FDBE3E9319C5D27726D60802E3E82D30D14D46
3ED21A4BFCF9838E06AD3058D13D5C28026C17DC996953A22A00F0609B0DF3B9
3AD53495851BAFC48CAF6D2227A434CA2E0BEF9AB3BD40ABFE4EA8F318D37BBE
973F573CAB683636D9A70B8891263F59E2F02201FFB4DD2E9D7ECBB1521DA03E
DD8652E2DCFE3F1A72631B3A9585736FBE77FFABEE4098F6B3C48E1469BF27AA
E1A9B35CF1378FDA12310F0920C5C53AD461858B3CB575697EA125DFEE829611
EF9B60AA0E4179C16A9AC441E0A21DC3A1C3DC04B100EE487EABF5C5B1F571A6
D71DC7BA8523947E08C6EEC43A726FE75AED248DFD3A7C4F6537224E9ED05F6F
5887C4646E032E015AA186C5970E8F07D3ED1DE8DBFA298BA4522C89E547419B
EA2876E9175410B6F6719F80EE44B9553960758C7D0F7BED73C0FE9A78D8E669
B5D1D3C1AEC2F2EF06E7D0B7996BC45DF4744934BD66266A6EBB02D70E35236E
55684a30a47476fce5b42cbd59add4b0fbc776a3
66aab897e33b3e4d940c51eba8d07f5605d5b275
b5378730c64f68d64aa1b15cb79088c9c6cb7373fcb7106812ffee4f8a7c1df7
cab0da87966e3c0994f4e46f30fe73624528d69f8a1c3b8a1857962e231a082b
392768ecec932cd22511a11cdbe04d181df749feccd4cb40b90a74a7fdf1e152
e549d528fee40208df2dd911c2d96b29d02df7bef9b30c93285f4a2f3e1ad5b0
a8f50e28989e21695d76f0b9ac23e14e1f8ae875ed42d98eaa427b14a7f87cd6
025ef5e92fecf3fa118bd96ad3aff3f88e2629594c6a7a274b703009619245b6
086dc27a896e154adf94e8c04b538fc146623b224d62bf019224830e39f4d51d
17decce71404a0ad4b402d030cb91c6fd5bca45271f8bf19e796757e85f70e48
17e4989ff7585915ec4342cbaf2c8a06f5518d7ba0022fd1d97b971c511f9bde
200955354545ef1309eb6d9ec65a917b08479f28362e7c42a718ebe8431bb15d
221e81540e290017c45414a728783cb62f79d9f63f2547490ec2792381600232
25e7a8da631f3a5dfeec99ca038b3b480658add98719ee853633422a3a40247d

SHA
28a4e9f569fd5223bffe355e685ee137281e0e86cae3cc1e3267db4c7b2f3bcd
2ddc77de26637a6d759e5b080864851b731fdb11075485980ece20d8f197104c
31fe821e4fac6380701428e01f5c39c6f316b6b58faff239d8432e821a79d151
331952c93954bd263747243a0395441d0fae2b6d5b8ceb19f3ddb786b83f0731
34c1d162bf17cdb41c2c5d220b66202a85f5338b15019e26dcab1a81f12fc451
38b3b10f2ddeecda0db029dacc6363275c4cdf18cc62be3cc57b79647d517a44
3a946cba2ba38a2c6158fa50beee20d2d75d595acc27ea51a39a37c121082596
3baace2a575083a7031af7e9e13ff8ed46659f0b25ce54abe73db844acfad11a
3f63fbc43fc44e6bf9c363e8c17164aeb05a515229e2111a2371d4321dcde787
4766553ce5ff67a2e28b1ee1b5322e005b85b26e21230ffba9622e7c83ed0917
4e5d89844135dca1d9899a8eedfbabc09bcb0fb5c5c14c29f7df5a58d7cf16d4
4f88738e04447344100bb9532c239032b86e71d8037ccb121e2959f37fff53cf
54e844b5ae4a056ca8df4ca7299249c4910374d64261c83ac55e5fdf1b59f01d
56ced937d0b868a2005692850cea467375778a147288ac404748c2dea9c17277
5f4782a34368bb661f413f33e2d1fb9f237b7f9637f2c0c21dc752316b02350c
6021d5500fdea0664a91bdd85b98657817083ece6e2975362791c603d7a197c7
62cb24967c6ce18d35d2a23ebed4217889d796cf7799d9075c1aa7752b8d3967
62e88163b51387b160e9c7ea1d74f0f80c52fc32c997aa595d53cbc2c3b6caf4
64a95de2783a97160bac6914ee07a42cdd154a0e33abc3b1b62c7bafdce24c0c
6a85451644a2c6510d23a1ab5610c85a38107b3b3a00238f7b93e2ce6d1ba549
6ade03a82d8bb884cae26c6db31cf539bec66861fc689cf1c752073fb79740c5
6fdd81e31f2bec2bdda594974068a69e911219d811c8de4466d7a059dd3183a3
74c00f303b87b23dffb59718187ff95c9d4d8497c61a64501166ac5dbed84b9f
7757a76ca945f33f3220ad2b2aa897f3e63c47f08e1b7d62d502937ba90360a7
7824197ad3b9c0981a1cdabf82940ac7733d232442bd31d195783a4e731845d2

SHA
79e232b2a08a2960a493e74ab7cba3e82c8167acc030a5ca8d080d0027a587fe
7fe1ff03e8f5678d280f7fd459a36444b6d816b2031e37867e4e36b689eccd33
83b336deca35441fa745cd80a7df7448ce24c09dd2a36569332ae0e4771f36a6
88249de22cefaf15f7c45b155703980fb09eb8e06b852f9d4a7c82126776ee7e
8b8f7e8030e2ba234a33bc8a2fa3ccb5912029d660e03ed40413d949142b98fe
8d979a1627dea58e9b86f393338df6aabfd762937e25e39f1d325fce06cf5338
8dd3faf0248890e8c3efb40b800f892989204ba3125986690669f0a914f26c5d
9521f51e42b8e31d82b06de6e15dbf9a1fa1bbff62cf6bc68c0b9e8fd1f8b2c5
97a00056c459a7ce38ad8029413bf8f1691d4ae81e90f0d346d54c91dd02a511
991f883556357a3b961c31e2b72f6246b52b27a5c45b72914abc61c5b5960cc3
9f06583bd4b8c4aefc470ef582ff685cd3d03b404e67ce8bf9dbbd5828c90c43
a0c3da2ebf94f6671537a80d26b3288f8fcdf845fe2780ef81fd9da48c0162bf
a8759ef55fed4a9410cc152df9ef330a95f776619901054715ed4721a414d15c
a8cc14bd56aa4a2da40717cb3f11ecb6aff4e0797a9cebcff51461db19eaf580
ae38ec0ddc58424bf6de8858c82c4c6902fc947604943d58d8cbca00991c7f7d
aeb82788aad8bdee4c905559c4636536fb54c40fdc77b27ba4308b6a0f24bedf
bdd028922220ff92acb8530c894e2705743a968a8159fe955c1057736c7e1ebd
c3cc43492d005b25fc2cc66f82a550420bb4c48b5aae0a77f1ccef0603a3e47c
c4f40e2eb029ef11be4ac43ccc6895af6fb6dabd3a5bcc02f29afb9553da625c
c6aa2c54eee52f99a911dadfbf155372bd9f43fb9f923500b0b374799204d7a3
c6e2562a2ae399a851b0e5bfb92011e9f97ab45fa536a61eb89b3aee062461f7
ca2b9a0fe3992477d4c87a6e2a75faaac9ea0f3828d054cb44371b3068b76ba5
cdc5e05843cf1904e145dad3ae6c058b92b1bc3cbffffc217884b7cc382172a1
cee890a9e7ab521125372c13b71fc154ef5332d333fe43798303b198e9314dcd
d90beab9a3986c26922e4107dccb0b725b8b0eea398f2aeb8848cbe25c3becee

SHA
db987749ef4a58c6a592a33221770d23adcb2efce4a5504aabc73d61cd356616
dc9757c9aa3aff76d86f9f23a3d20a817e48ca3d7294307cc67477177af5c0d4
dcb986e45f1cf38794acec5e7f576a8dff6fbec66e6a09e3cc92596c796ad0d3
e400a196e7128a3cf40085629db8f26b73b6980be7df3da60928a4a062bc85cb
e491d06e3a556c79e922274af04c1786a957775ba2d5d0b02d13bdee91bf5ce4
ea6d9ff8f768fc0132f9f543d9546744d04f9f83e2241950f63f60b520b9ece0
ead189bb18ee839db3d221701e208c4d2845c232cec66764bb3ea6c688ca18e8
ee035537c3b8fc54ca2e1fa98c18e2fb0e203d863005c878bc8ceaa690a6689f
ee53521e7d8b2b05fef77877440738ee169f3b75228931f9aaf96621a2f64c25
eef36bc6f208abd46541bac1b1de18bb3a69057b1a54e67d71d259cc0f1bef5b
f59fe0945f97df4e3d2efc9b31d00602fc5a16e05453e0d853e275cadb63a057
f875e68899afe172394176fa9cabededeaa19ad6816a90746bb630c064c69e6a
fdeb6a6aaee94fe204fb986f6d78e64a9086c5f64e315d8c5e90b590f0007af8

Endpoint Detection and Response (EDR) Tools

Using EDR tools it is possible to detect Brute Ratel activity by monitoring for specific behaviors, such as the use of specific network connections.

Using information provided by **Uni42**, **Yoroi** and **Splunk** it is possible to create a list of network indicator useful to spot malicious activities performed with the framework:

IP/Domain
104.6.92[.]229
137.184.199[.]17
138.68.50[.]218
138.68.58[.]43

IP/Domain
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

IP/Domain
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

References

- https://yoroi.company/research/hunting-cyber-evil-ratels-from-the-targeted-attacks-to-the-widespread-usage-of-brute-ratel/
- https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
- https://www.splunk.com/en_us/blog/security/deliver-a-strike-by-reversing-a-badger-brute-ratel-detection-and-analysis.html