KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Black Basta ransomware now deploys Brute Ratel C4

Tracker ID: TN1017 **Date:** 19/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Background

In recent attacks, threat actors associated with the Black Basta ransomware family have been observed using the QakBot malware to deliver the Brute Ratel C4 framework as a second-stage payload. Last month, a cracked version of Brute Ratel C4 began to circulate among cybercriminals, prompting its developer to change the licensing system to make it more difficult to hack. Based on infrastructure and overlapping TTP revealed in the Black Basta attacks, the Black Basta Ransomware group is related to the Qakbot-to-Brute Ratel-to-Cobalt Strike death chain.

While these authorized applications are intended for penetration testing, their capability to provide remote access has made them a valuable tool in the eyes of attackers aiming to discreetly probe the infiltrated environment without drawing scrutiny for prolonged periods. This is the first time that the growing adversary simulation software has been made available through a Qakbot infection. Qakbot, commonly known as QBot or QuackBot, is a financial and information-stealing virus that has been active since 2007. However, because of its modular structure and ability to function as a downloader, it has become a popular target for propagating further infections.

The initial vector in an identified campaign was a phishing email that contained a weaponized link leading to a ZIP archive and Cobalt Strike, which is utilised for lateral movement. The ZIP file in the email contains an ISO file, which in turn contains an LNK file that fetches the Qakbot payload, illustrating attempts by threat actors to adapt to alternative ways in the context of Microsoft's decision to block macros by default for web-based documents.

Brute Ratel and Cobalt Strike are retrieved following the Qakbot infection. It also used built-in command line functions such as arp, ipconfig, nslookup, netstat, and whoami to undertake automated reconnaissance. The threat actor's goal is considered to be the distribution of ransomware over the entire domain. Another Qakbot execution chain leads to the second-stage execution of Brute Ratel C4, in which the ZIP file is given using the relatively prevalent technique known as HTML smuggling.

The findings correlate with a recent spike in Qakbot attacks using a range of techniques such as HTML file attachments, DLL side-loading, and email thread hijacking, the latter of which involved capturing emails in bulk from successful ProxyLogon assaults aimed at Microsoft Exchange servers. Furthermore, intrusions via QAKBOT leading to Black Basta have been noticed previously. Organizations should be aware of the increasing use of Cobalt Strike in attacks, living-off-the-land binaries (LOLBins), and red team or penetration-testing tools that blend in with the environment, such as Brute Ratel C4.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Black Basta ransomware now deploys Brute Ratel C4

Tracker ID: TN1017 **Date:** 19/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Indicators of Compromise

Please refer to the attached sheet for IOCs.

MITRE ATT&CK Tactics

Initial Access , Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery, Lateral Movement, Command and Control.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Check the sender's identity, unfamiliar email addresses, mismatched emails, sender names, or spoofed company emails that are an indicator of malicious intent.
- Hover over the pointer above embedded links to verify the link's target. If the email claims to come from a legitimate user, verify if they sent it before taking any action.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Ravie Lakshmanan, Black Basta Ransomware Hackers Infiltrate Networks via Qakbot to Deploy Brute Ratel C4, The Hacker News, 17th October 2022, External Link (thehackernews.com)
- an Kenefick, Lucas Silva, Nicole Hernandez, Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike, TrendMicro, 12th October 2022, External Link (trendmicro.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Black Basta ransomware now deploys Brute Ratel C4

Tracker ID: TN1017 **Date:** 19/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: All

IP	Domain	SHA256 Hash
197[.]204[.]227[.]155:443	symantecuptimehost[.]com	01fd6e0c8393a5f4112ea19a26bedffb31d6a01f4d3fe5721ca20f479766208f
123[.]23[.]64[.]230:443	sentisupport[.]com	2d1e93d28bf349a412bda7668536c4dc197cb12e020a5355f2d305ecac3ba458
173[.]218[.]180[.]91:443	near-org[.]top	f56d25cf9f20f2040b2ec14f769f36aa14819f56f6b254c0831c9b2a024b8c8d
111[.]125[.]157[.]230:443	teenieshopus[.]com	582a5e2b2652284ebb486bf6a367aaa6bb817c856f08ef54db64c6994c5b91bd
70[.]49[.]33[.]200:2222	hxxps://fewifasoc[.]com	f32b4407f51f1407bf4261c49ad940712b0e3777a5f7365ba6b485a163361d3b
149[.]28[.]38[.]16:995	hxxps://hadujaza[.]com	a0a0f07ffbede4772ef04ce7c7e98b77ad0d5e2b2f391d8d26dcc96c289469c4
86[.]132[.]13[.]105:2078	hxxps://himiketiv[.]com	e9e214f7338c6baefd2a76ee66f5fadb0b504718ea3cebc65da7a43a5ff819a4
149[.]28[.]38[.]16:443	hxxps://davalibapa[.]com	a0a0f07ffbede4772ef04ce7c7e98b77ad0d5e2b2f391d8d26dcc96c289469c4
45[.]77[.]159[.]252:995	halasaloon[.]com	d44b05b248f95986211ab3dc2765f1d76683594a174984c8b801bd7eade8aa47
45[.]77[.]159[.]252:443	edmor-p[.]com	06c4c4d100e9a7c79e2ee8c4ffa1f7ad165a014f5f14f90ddfc730527c564e35
149[.]28[.]63[.]197:995	growin[.]ro	5510ff3cb4b8b344b0ee70b80266d3b497afd9ec423183917983e8bb36ff7c25
144[.]202[.]15[.]58:443		62cb24967c6ce18d35d2a23ebed4217889d796cf7799d9075c1aa7752b8d3967
45[.]63[.]10[.]144:443		ab88d558ff0ae35860f6ba1ceab6ec3302ace9dc7e957940c053f85b4dc17e78
45[.]63[.]10[.]144:995		726bce40d17b3f9b245af6b78251469b89cde4d3428187f5c11ed4c3f5b58ed4
149[.]28[.]63[.]197:443		a7d6cd8209eea40a9bcf32e923b7723d8724895f5d1084605a64651c3a811b03
144[.]202[.]15[.]58:995		94392d757ba3526c3dcd5c3ddcb3f005c6330ef075dc246d08a8b79e017c0c01
39[.]121[.]226[.]109:443		9efbc691d53ea9aa1eef245da23e197310bf266b0223ae1af8035bf854782edd
177[.]255[.]14[.]99:995		c545541fecd97b2c46ab0c6db25a2f87b48ffadbd2c75ad65c7ce2781a8de491
134[.]35[.]10[.]30:443		a0adcd303fdff7747ab93df07b0722eab9890ba9deab7d322f077d6774ef6bc0
99[.]232[.]140[.]205:2222		66ff672282b02f4796e006f2cfef125cccfd542b65eb3fbc728badf09cb94202
180[.]180[.]132[.]100:443		74da9610cb92a5a6fc15c856d3af73ff2b069f23d5a9712e48b6fd40b52fc744
86[.]176[.]180[.]223:993		6f9e9137a014b29f47722dbbb7a290eff11a9da3226af01bb2ecb78116dcb607
41[.]98[.]11[.]74:443		1751c378e2b14bd6238c3189e13501d191c117fdfe65e4e0ea1cb5829cce2bb9
196[.]64[.]230[.]149:8443		16738ffeb00a849af4f24b6faee00d9d8e2b0247621d01718895dac5cc99fd8a
68[.]224[.]229[.]42:443		64a95de2783a97160bac6914ee07a42cdd154a0e33abc3b1b62c7bafdce24c0c
41[.]111[.]72[.]234:995		54e844b5ae4a056ca8df4ca7299249c4910374d64261c83ac55e5fdf1b59f01d
196[.]64[.]237[.]130:443		01af5478e290bfcd23eeb39ff3af8802ab11a410038cae957ccb56de45d90ac0
190[.]44[.]40[.]48:995		f2fe89d8de9dc29ddca56918beb652df1b3d44218bf5e084c4d0de7325ec54f5
70[.]51[.]132[.]197:2222		31103788fae9b988d9d4362b848249b49ea60e15fc5982f26b13447064a13325
88[.]232[.]207[.]24:443		ce01002614eb7029131a73769db721ac68ef47989d7a8022980d3ae22c82b6f7
115[.]247[.]12[.]66:443		48976d7bf38cca4e952507e9ab27e3874ca01092eed53d0fde89c5966e9533bb
189[.]19[.]189[.]222:32101		
72[.]88[.]245[.]71:443		
217[.]165[.]97[.]141:993		
191[.]97[.]234[.]238:995		
119[.]82[.]111[.]158:443		
88[.]237[.]6[.]72:53		
100[.]1[.]5[.]250:995		
96[.]234[.]66[.]76:995		
186[.]64[.]67[.]34:443		
66[.]181[.]164[.]43:443		
193[.]3[.]19[.]37:443		
197[.]94[.]84[.]128:443		
41[.]96[.]130[.]46:80		
187[.]205[.]222[.]100:443		
139[.]228[.]33[.]176:2222		
88[.]245[.]168[.]200:2222		
110[.]4[.]255[.]247:443		
89[.]211[.]217[.]38:995		
23[.]225[.]104[.]250		
186[.]125[.]93[.]28		
149[.]126[.]159[.]254		
189[.]79[.]27[.]174		
41[.]96[.]18[.]5		
197[.]204[.]126[.]136		
105[.]108[.]255[.]165		
41[.]105[.]54[.]8		
78[.]162[.]213[.]155		
154[.]183[.]135[.]35		
41[.]108[.]175[.]56		
94[.]52[.]127[.]44		
160[.]179[.]220[.]87		
45.153.242[.]251		
45.153.241[.]88		
45.153.241[.]64		
45.153.242[.]250		