Black Basta Ransomware Operators Expand Their Attack Arsenal With QakBot Trojan and PrintNightmare Exploit

We look into a recent attack orchestrated by the Black Basta ransomware group that used the banking trojan QakBot as a means of entry and movement and took advantage of the PrintNightmare vulnerability to perform privileged file operations.

June 30, 2022

By: Kenneth Adrian Apostol, Paolo Ronniel Labrador, Mirah Manlapig, James Panlilio, Emmanuel Panopio, John Kenneth Reyes, Melvin Singwa Read time: 4 min (955 words)

Since it became operational in April, Black Basta has garnered notoriety for its recent attacks on 50 organizations around the world and its use of double extortion, a modern ransomware tactic in which attackers encrypt confidential data and threaten to leak it if their demands are not met. The emerging ransomware group has continued to improve its attacks: We recently caught it using the banking trojan QakBot as a means of entry and movement, and taking advantage of the PrintNightmare vulnerability (CVE-2021-34527) to perform privileged file operations.

In the case of a Trend Micro customer, its system was infected with Black Basta ransomware that was deployed by QakBot (Figure 1). This behavior is typical of the QakBot malware family, which has served as a key enabler of ransomware families like MegaCortex, PwndLockerm, Egregor, ProLock, and REvil (aka Sodinokibi). QakBot, which was discovered in 2007, is known for its infiltration capabilities and has been used as a "malware-installation-as-a-service" for various campaigns. Over the years, this banking trojan has become increasingly sophisticated, as evidenced by its exploitation of a newly disclosed Microsoft zero-day vulnerability known as Follina (CVE-2022-30190).

5/2/2022	C:\Users\ \Downloads\c_3855059153.xlsb	Trojan.X97M.QAKBOT.YXCFH
	c:\ \beunsea.ooooooocccccccxxxxxxxx	
	c:\ \beunseb.ooooooocccccccxxxxxxxx	TrojanSpy.Win32.QAKBOT.YACEJT
5/2/2022	c:\ \beunse.ooooooocccccccxxxxxxxx	
5/2/2022	c:\Users\Public\spider.dll	Trojan.Win64.QUAKNIGHTMARE.YACEJT
	-nop -w hidden -encodedcommand	
5/2/2022	JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0A...	FILELESS COBEACON
5/2/2022	C:\Windows\150f1e6.exe	Trojan.Win32.COBEACON.SMYXBE2.hp
5/4/2022	c:\users\public\runtimelisten.exe	Backdoor.Win32.COROXY.YACEKT
5/4/2022	c:\windows\cps1.dll	Trojan.Win32.BLACKBASTA.YXCEJ
5/4/2022	c:\windows\cps.exe	Ransom.Win32.BLACKBASTA.YACEJ
5/4/2022	C:\\Users\\vadmin\\Downloads\\nmap-7.91-setup.exe	PUA.Win32.Netcat.B
5/5/2022	C:\Program Files\Broadcom\BACS\readme.txt	Ransom.Win32.BLACKBASTA.A.note

Figure 1. A timeline of the files detected on the infected machine

QakBot's infection chain

QakBot is distributed using spear-phishing emails (Figure 2) that contain Excel files with Excel 4.0 macros. The emails entice the recipient to enable macros, which download and execute the QakBot DLL files (Figures 3 and 4). The downloaded QakBot DLL is dropped onto a specific file path and file name, and is executed via regsvr32.exe (Figure 5). The QakBot DLL performs process injection using explorer.exe (Figure 6), after which the injected Explorer process creates a scheduled task to maintain the malware's initial foothold in the infected system (Figure 7).

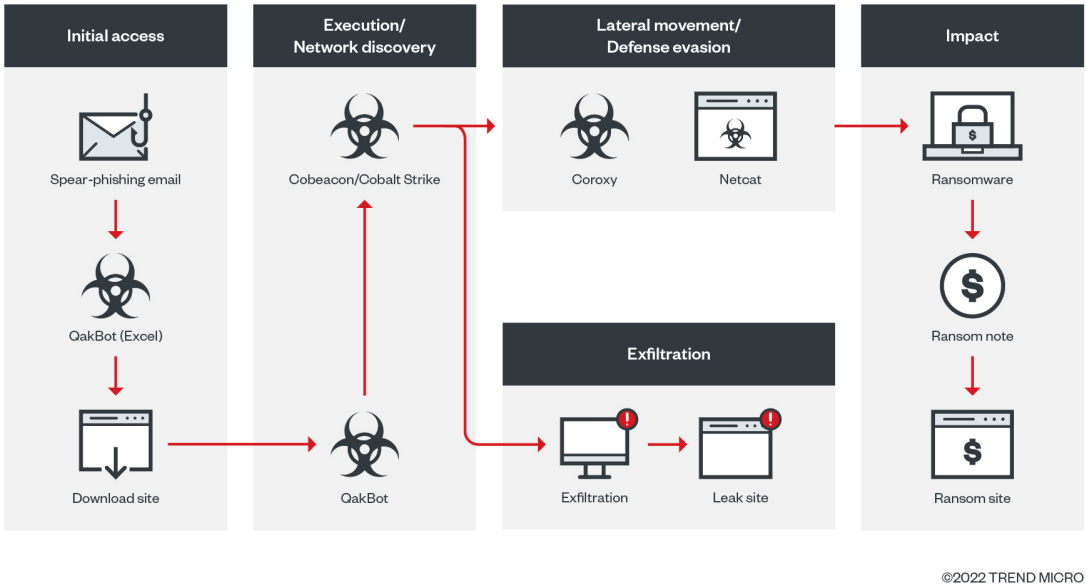

Figure 2. The infection chain from the point of entry to the Black Basta ransomware payload

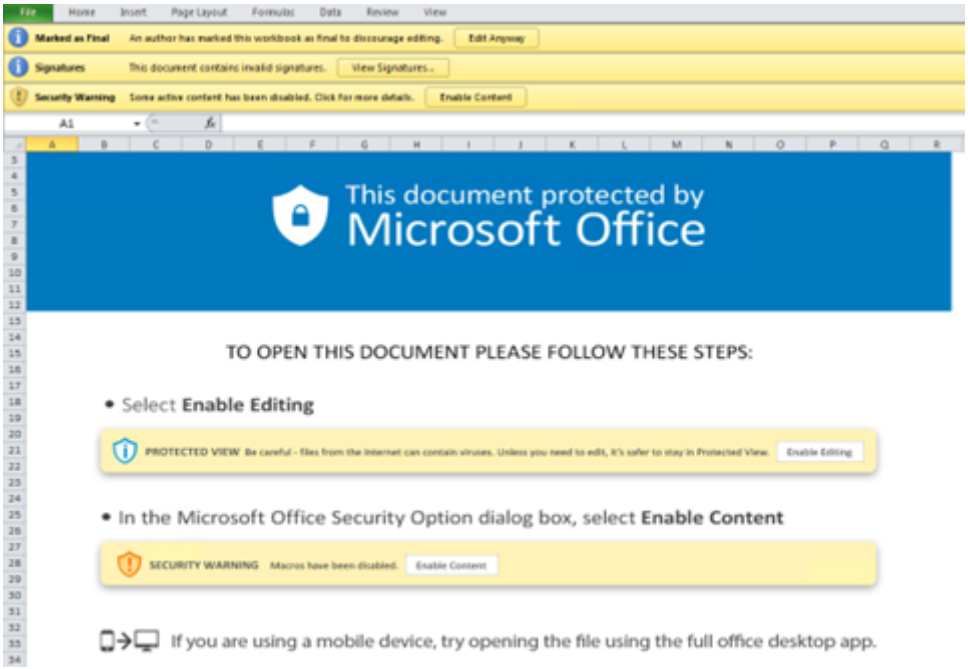

Figure 3. Instructions in the Excel file used by QakBot to lure a potential victim into enabling Excel 4.0 macros

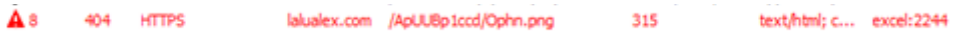

Figure 4. The malicious URL used to download the QakBot malware

Figure 5. The downloaded QakBot malware dropped onto a specific file path and file name

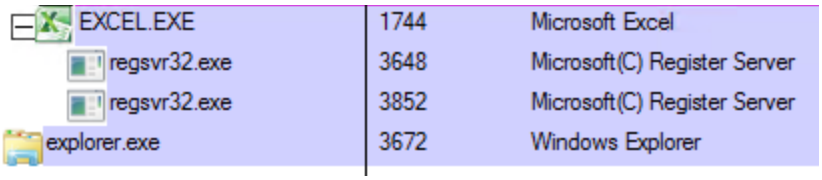

Figure 6. The explorer.exe process used in process injection

Figure 7. The scheduled task created by QakBot

Once QakBot is installed in a system, it proceeds to download and drop the other components in the infection chain, beginning with the Cobeacon backdoor. We have observed the execution of Cobeacon using a fileless PowerShell script with multiple layers of obfuscation (Figures 8 to 11). The Base64-encoded shellcode of the installed Cobeacon establishes and names a pipe for communication (Figure 12) that is possibly used for exfiltration purposes once information has been collected from a targeted system. The Black Basta ransomware group posts this information on its leak sites if the victim does not pay the ransom.

Figure 8. Cobeacon's first layer of obfuscation, a Base64-encoded PowerShell command

Figure 9. Cobeacon's second layer of obfuscation, the loading and reading of an archive file in memory

Figure 10. Cobeacon's third layer of obfuscation, the decoded script for running the Base64-encoded shellcode

```
0000000000000000 FC                   CLD
0000000000000001 E889000000           CALL 0000000-FFFFFF71
0000000000000006 60                   ???
0000000000000007 89E5                 MOV EBP,ESP
0000000000000009 31D2                 XOR EDX,EDX
000000000000000B 648B5230             MOV EDX,DWORD PTR FS:[RDX+30]
000000000000000F 8B520C               MOV EDX,DWORD PTR [RDX+0C]
0000000000000012 8B5214               MOV EDX,DWORD PTR [RDX+14]
0000000000000015 8B7228               MOV ESI,DWORD PTR [RDX+28]
0000000000000018 0FB74A26             MOVZX ECX,WORD PTR [RDX+26]
000000000000001C 31FF                 XOR EDI,EDI
000000000000001E 31C0                 XOR EAX,EAX
0000000000000020 AC                   LODS AL,BYTE PTR [RSI]
0000000000000021 3C61                 CMP AL,61
0000000000000023 7C02                 JL 0000000000000027
0000000000000025 2C20                 SUB AL,20
0000000000000027 C1CF0D               ROR EDI,0D
000000000000002A 01C7                 ADD EDI,EAX
000000000000002C E2F0                 LOOP 000000000000001E
000000000000002E 52                   PUSH RDX
000000000000002F 57                   PUSH RDI
0000000000000030 8B5210               MOV EDX,DWORD PTR [RDX+10]
0000000000000033 8B423C               MOV EAX,DWORD PTR [RDX+3C]
0000000000000036 01D0                 ADD EAX,EDX
0000000000000038 8B4078               MOV EAX,DWORD PTR [RAX+78]
000000000000003B 85C0                 TEST EAX,EAX
000000000000003D 744A                 JE 0000000000000089
000000000000003F 01D0                 ADD EAX,EDX
0000000000000041 50                   PUSH RAX
0000000000000042 8B4818               MOV ECX,DWORD PTR [RAX+18]
0000000000000045 8B5820               MOV EBX,DWORD PTR [RAX+20]
0000000000000048 01D3                 ADD EBX,EDX
000000000000004A E33C                 JRCXZ 0000000000000088
000000000000004C 498B348B             MOV RSI,QWORD PTR [R11+RCX*4]
```

Figure 11. Disassembly of the decoded shellcode

Figure 12. Shellcode containing the named pipe for communication

PrintNightmare and Coroxy

Upon further analysis of the system that was affected by Black Basta, we found evidence that points to the ransomware group's exploitation of the PrintNightmare vulnerability. Exploiting this vulnerability, Black Basta abused the Windows Print Spooler Service or spoolsv.exe to drop its payload, spider.dll, and perform privileged file operations. It also exploited the vulnerability to execute another file in the affected system, but samples of this file were no longer available in the system.

Additionally, our investigation found that the ransomware actors used the Coroxy backdoor. They used Coroxy in conjunction with the abuse of the computer networking utility tool Netcat to move laterally across the network. Once the attackers gained a wide foothold in the network, they executed the Black Basta ransomware, whose infection process we explained in more detail in a previous blog post.

Thwarting phishing attempts

Spear phishing is a common precursor to ransomware infection. Organizations can protect their data from threats that spread through emails by adhering to best practices such as:

- Ensuring that macros are disabled in Microsoft Office applications.
- Verifying an email's sender and content before opening or downloading any attachments.
- Hovering the pointer over embedded links to show the links' full addresses.

- Being wary of telltale signs of malicious intent, including unfamiliar email addresses, mismatched email and sender names, and spoofed company emails.

Businesses and their employees can safeguard sensitive company data from email-borne ransomware threats like Black Basta by turning to endpoint solutions such as Trend Micro's Smart Protection Suites and Worry-Free Business Security solutions, which are equipped with behavior-monitoring capabilities that are able to detect malicious files, scripts, and messages, and block all related malicious URLs. Trend Micro™ Deep Discovery™ also has a layer for email inspection that protects businesses by detecting any malicious attachments and URLs. Multilayered detection and response solutions like the Trend Micro Vision One™ platform provides companies with greater visibility across multiple layers — like email, endpoints, servers, cloud workloads, and networks — to look out for suspicious behavior in their systems and block malicious components early, mitigating the risk of ransomware infection.

Indicators of compromise

Hashes

SHA-256	Trend Micro detection
01fafd51bb42f032b08b1c30130b963843fea0493500e871d6a6a87e555c7bac	Ransom.Win32.BLACKBASTA.YXCEP
72a48f8592d89eb53a18821a54fd791298fcc0b3fc6bf9397fd71498527e7c0e	Trojan.X97M.QAKBOT.YXCFH
580ce8b7f5a373d5d7fbfbfef5204d18b8f9407b0c2cbf3bcae808f4d642076a	Backdoor.Win32.COROXY.YACEKT
130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007e1aed	Trojan.Win64.QUAKNIGHTMARE.YACEJT
c7eb0facf612dbf76f5e3fe665fe0c4bfed48d94edc872952a065139720e3166	TrojanSpy.Win32.QAKBOT.YXCEEZ
ffa7f0e7a2bb0edf4b7785b99aa39c96d1fe891eb6f89a65d76a57ff04ef17ab	TrojanSpy.Win32.QAKBOT.YACEJT
2083e4c80ade0ac39365365d55b243dbac2a1b5c3a700aad383c110db073f2d9	TrojanSpy.Win32.QAKBOT.YACEJT
1e7174f3d815c12562c5c1978af6abbf2d81df16a8724d2a1cf596065f3f15a2	TrojanSpy.Win32.QAKBOT.YACEJT
2d906ed670b24ebc3f6c54e7be5a32096058388886737b1541d793ff5d134ccb	TrojanSpy.Win32.QAKBOT.YACEJT
72fde47d3895b134784b19d664897b36ea6b9b8e19a602a0aaff5183c4ec7d24	TrojanSpy.Win32.QAKBOT.YACEJT
2e890fd02c3e0d85d69c698853494c1bab381c38d5272baa2a3c2bc0387684c1	TrojanSpy.Win32.QAKBOT.YACEJT
c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bf1fab6bb70	Ransom.Win32.BLACKBASTA.YACEJ
8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad	Trojan.Win32.BLACKBASTA.YXCEJ

0e2b951ae07183c44416ff6fa8d7b8924348701efa75dd3cb14c708537471d27	Trojan.Win32.BLACKBASTA.YXCEJ
0d3af630c03350935a902d0cce4dc64c5cfff8012b2ffc2f4ce5040fdec524ed	Trojan.Win32.BLACKBASTA.YXCEJ
df35b45ed34eaca32cda6089acbfe638d2d1a3593d74019b6717afed90dbd5f8	Trojan.Win32.BLACKBASTA.YXCEJ
3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc	Trojan.Win32.BLACKBASTA.YXCEJ
433e572e880c40c7b73f9b4befbe81a5dca1185ba2b2c58b59a5a10a501d4236	Ransom.Win32.BLACKBASTA.A.note
c4683097a2615252eeddab06c54872efb14c2ee2da8997b1c73844e582081a79	PUA.Win32.Netcat.B

URLs

24[.]178[.]196[.]44:2222
37[.]186[.]54[.]185:995
39[.]44[.]144[.]182:995
45[.]63[.]1[.]88:443
46[.]176[.]222[.]241:995
47[.]23[.]89[.]126:995
72[.]12[.]115[.]15:22
72[.]76[.]94[.]52:443
72[.]252[.]157[.]37:995
72[.]252[.]157[.]212:990
73[.]67[.]152[.]122:2222
75[.]99[.]168[.]46:61201
103[.]246[.]242[.]230:443
113[.]89[.]5[.]177:995
148[.]0[.]57[.]82:443
167[.]86[.]165[.]191:443
173[.]174[.]216[.]185:443
180[.]129[.]20[.]53:995
190[.]252[.]242[.]214:443
217[.]128[.]122[.]16:2222
elblogdeloscachanillas[.]com[.]mx/S3sY8RQ10/Ophn[.]png
lalualex[.]com/ApUUBp1ccd/Ophn[.]png
lizety[.]com/mJYvpo2xhx/Ophn[.]png