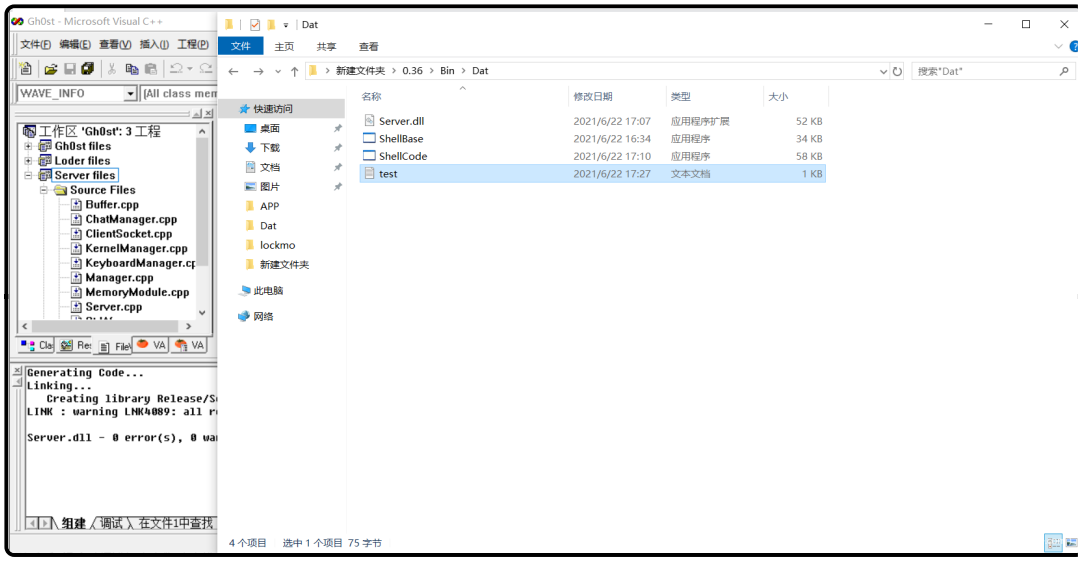
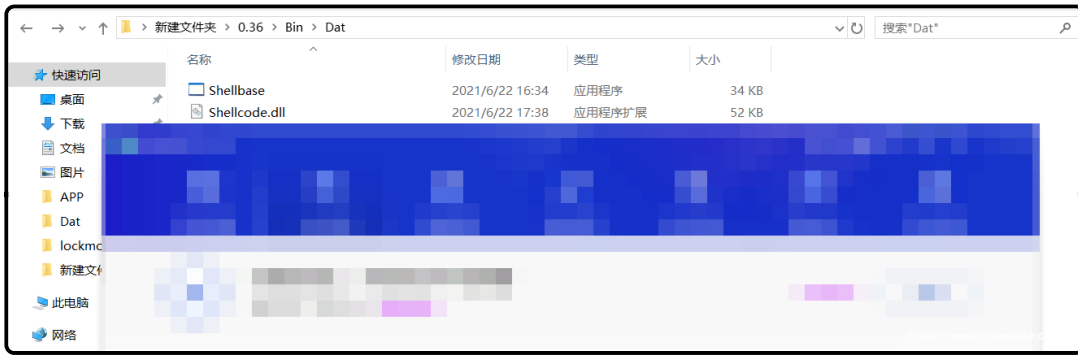
Shellcode是更改对Server.dll的16进制加密器



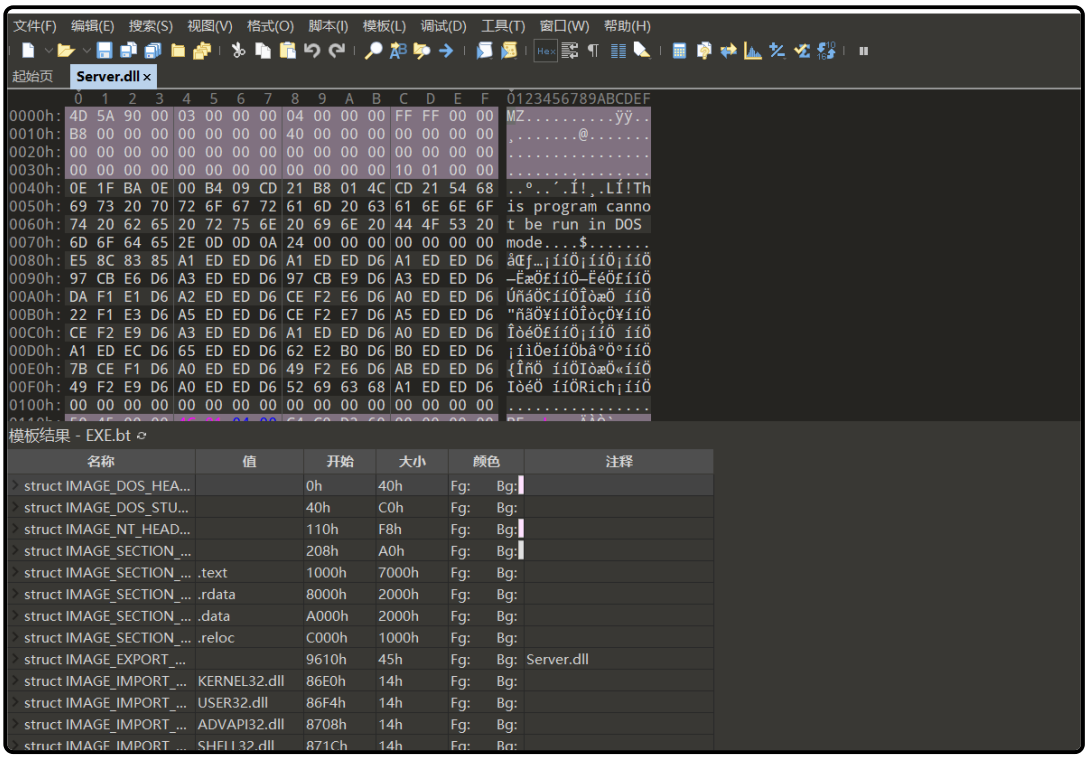
首先生成一个Server.dll 然后生成加密器和Url加密器。

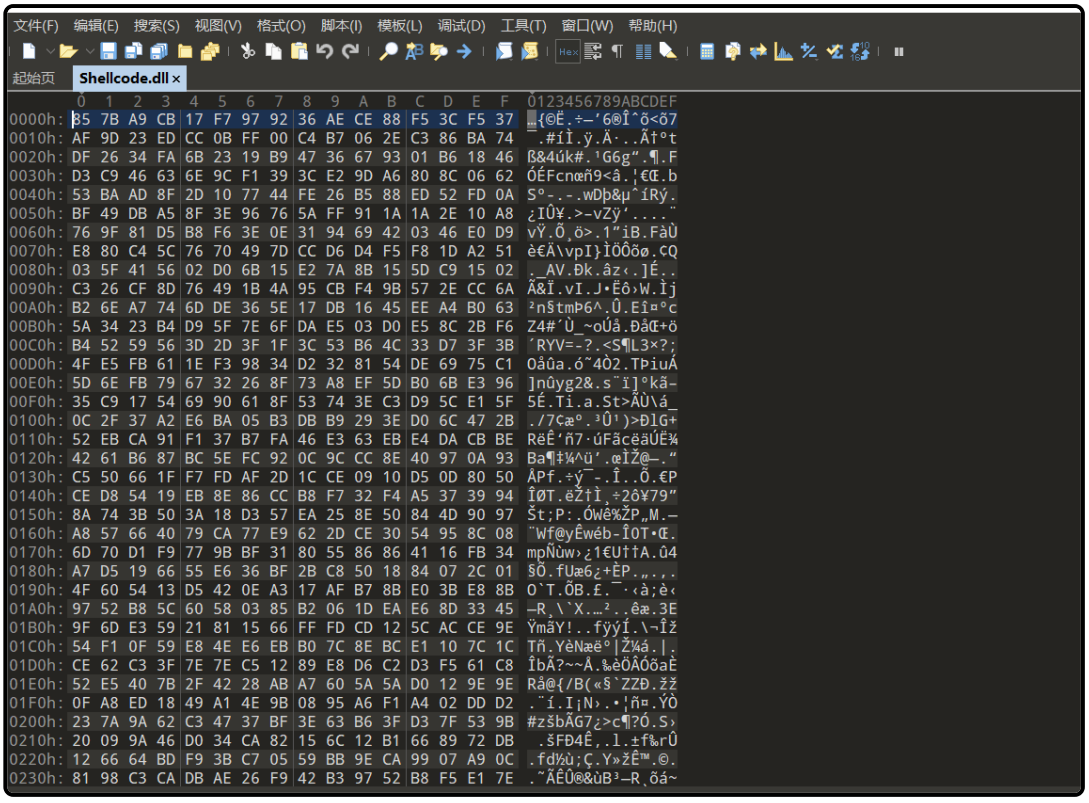
通过查杀发现被杀

运行ShellCode加密Server.dll后查杀可发现已经不杀了



笔者来对比一下ShellCode加密前后的Server.dll


文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)
起始页
Server.dll ×
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
0010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0030h: 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 ....
0040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
0060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
0070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
0080h: E5 8C 83 85 A1 ED ED D6 A1 ED ED D6 A1 ED ED D6 åŒƒ…¡ííÖ¡ííÖ¡ííÖ
0090h: 97 CB E6 D6 A3 ED ED D6 97 CB E9 D6 A3 ED ED D6 —ËæÖ£ííÖ—ËéÖ£ííÖ
00A0h: DA F1 E1 D6 A2 ED ED D6 CE F2 E6 D6 A0 ED ED D6 ÚñáÖ¢ííÖÎòæÖ ííÖ
00B0h: 22 F1 E3 D6 A5 ED ED D6 CE F2 E7 D6 A5 ED ED D6 "ñãÖ¥ííÖÎòçÖ¥ííÖ
00C0h: CE F2 E9 D6 A3 ED ED D6 A1 ED ED D6 A0 ED ED D6 Îòé֣ííÖ¡ííÖ ííÖ
00D0h: A1 ED EC D6 65 ED ED D6 62 E2 B0 D6 B0 ED ED D6 ¡ífÖeííÖbâ°Ö°ííÖ
00E0h: 7B CE F1 D6 A0 ED ED D6 49 F2 E6 D6 AB ED ED D6 {ÎñÖ ííÖIòæÖ«ííÖ
00F0h: 49 F2 E9 D6 A0 ED ED D6 52 69 63 68 A1 ED ED D6 Ióé֠ííÖRich¡ííÖ
0100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
模板结果 - EXE.bt
名称 值 开始 大小 颜色 注释
struct IMAGE_DOS_HEA... 0h 40h Fg: Bg:
struct IMAGE_DOS_STU... 40h C0h Fg: Bg:
struct IMAGE_NT_HEAD... 110h F8h Fg: Bg:
struct IMAGE_SECTION_... 208h A0h Fg: Bg:
struct IMAGE_SECTION_... .text 1000h 7000h Fg: Bg:
struct IMAGE_SECTION_... .rdata 8000h 2000h Fg: Bg:
struct IMAGE_SECTION_... .data A000h 2000h Fg: Bg:
struct IMAGE_SECTION_... .reloc C000h 1000h Fg: Bg:
struct IMAGE_EXPORT_... 9610h 45h Fg: Bg: Server.dll
struct IMAGE_IMPORT_... KERNEL32.dll 86E0h 14h Fg: Bg:
struct IMAGE_IMPORT_... USER32.dll 86F4h 14h Fg: Bg:
struct IMAGE_IMPORT_... ADVAPI32.dll 8708h 14h Fg: Bg:
struct IMAGE_IMPORT_... SHELL32.dll 871Ch 14h Fg: Bg:


文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)
起始页
Shellcode.dll ×
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: B5 7B A9 CB 17 F7 97 92 36 AE CE 88 F5 3C F5 37 µ{©Ë.÷—'6®Î^õ<õ7
0010h: AF 9D 23 ED CC 0B FF 00 C4 B7 06 2E C3 86 BA 74 ¯.#íÌ.ÿ.Ä·..Ã†ºt
0020h: DF 26 34 FA 6B 23 19 B9 47 36 67 93 01 B6 18 46 ß&4úk#.¹G6g“.¶.F
0030h: D3 C9 46 63 6E 9C F1 39 3C E2 9D A6 80 8C 06 62 ÓÉFcnœñ9<â.¦€Œ.b
0040h: 53 BA AD 8F 2D 10 77 44 FE 26 B5 88 ED 52 FD 0A Sº-.-.wDþ&µ^íRý.
0050h: BF 49 DB A5 8F 3E 96 76 5A FF 91 1A 1A 2E 10 A8 ¿IÛ¥.>–vZÿ'....¨
0060h: 76 9F 81 D5 B8 F6 3E 0E 31 94 69 42 03 46 E0 D9 vŸ.Õ¸ö>.1”iB.FàÙ
0070h: E8 80 C4 5C 76 70 49 7D CC D6 D4 F5 F8 1D A2 51 è€Ä\vpI}ÌÖÔõø.¢Q
0080h: 03 5F 41 56 02 D0 6B 15 E2 7A 8B 15 5D C9 15 02 ._AV.Ðk.âz‹.]É..
0090h: C3 26 CF 8D 76 49 1B 4A 95 CB F4 9B 57 2E CC 6A Ã&Ï.vI.J•Ëô›W.Ìj
00A0h: B2 6E A7 74 6D DE 36 5E 17 DB 16 45 EE A4 B0 63 ²n§tmÞ6^.Û.Eî¤°c
00B0h: 5A 34 23 B4 D9 5F 7E 6F DA E5 03 D0 E5 8C 2B F6 Z4#´Ù_~oÚå.Ðå+ö
00C0h: B4 52 59 56 3D 2D 3F 1F 3C 53 B6 4C 33 D7 3F 3B ´RYV=-?.<S¶L3×?;
00D0h: 4F E5 FB 61 1E F3 98 34 D2 32 81 54 DE 69 75 C1 Oåûa.ó˜4Ò2.TÞiuÁ
00E0h: 5D 6E FB 79 67 32 26 8F 73 A8 EF 5D B0 6B E3 96]nûyg2&.s¨ï]°kã–
00F0h: 35 C9 17 54 69 90 61 8F 53 74 3E C3 D9 5C E1 5F 5É.Ti.a.St>ÃÙ\á_
0100h: 0C 2F 37 A2 E6 BA 05 B3 DB B9 29 3E D0 6C 47 2B ./7¢æº.³Û¹)>ÐlG+
0110h: 52 EB CA 91 F1 37 B7 FA 46 E3 63 EB E4 DA CB BE RëÊ‘ñ7·úFãcëäÚË¾
0120h: 42 61 B6 87 BC 5E FC 92 0C 9C CC 8E 40 97 0A 93 Ba¶‡¼^ü’.œÌŽ@—.“
0130h: C5 50 66 1F F7 FD AF 2D 1C CE 09 10 D5 0D 80 50 ÅPf.÷ý¯-.Î..Õ.€P
0140h: CE D8 54 19 EB 8E 86 CC B8 F7 32 F4 A5 37 39 94 ÎØT.ëŽ†Ì¸÷2ô¥79”
0150h: 8A 74 3B 50 3A 18 D3 57 EA 25 8E 50 84 4D 90 97 Št;P:.ÓWê%ŽP„M.—
0160h: A8 57 66 40 79 CA 77 E9 62 2D CE 30 54 95 8C 08 ¨Wf@yÊwéb-Î0T•Œ.
0170h: 6D 70 D1 F9 77 9B BF 31 80 55 86 86 41 16 FB 34 mpÑùw›¿1€U††A.û4
0180h: A7 D5 19 66 55 E6 36 BF 2B C8 50 18 84 07 2C 01 §Õ.fUæ6¿+ÈP.„.,.
0190h: 4F 60 54 13 D5 42 0E A3 17 AF B7 8B E0 3B E8 8B O`T.ÕB.£.¯·‹à;è‹
01A0h: 97 52 B8 5C 60 58 03 85 B2 06 1D EA E6 8D 33 45 —R¸\`X.…²..êæ.3E
01B0h: 9F 6D E3 59 21 81 15 66 FF FD CD 12 5C AC CE 9E Ÿmãy!..fÿýÍ.\¬Îž
01C0h: 54 F1 0F 59 E8 4E E6 EB B0 7C 8E BC E1 10 7C 1C Tñ.YèNæë°|Ž¼á.|.
01D0h: CE 62 C3 3F 7E 7E C5 12 89 E8 D6 C2 D3 F5 61 C8 ÎbÃ?~~Å.‰èÖÂÓõaÈ
01E0h: 52 E5 40 7B 2F 42 28 AB A7 60 5A 5A D0 12 9E 9E Rå@{/B(«§`ZZÐ.žž
01F0h: 0F A8 ED 18 49 A1 4E 9B 08 95 A6 F1 A4 02 DD D2 .¨í.I¡N›.•¦ñ¤.ÝÒ
0200h: 23 7A 9A 62 C3 47 37 BF 3E 63 B6 3F D3 7F 53 9B #zšbÃG7¿>c¶?Ó.S›
0210h: 20 09 9A 46 D0 34 CA 82 15 6C 12 B1 66 89 72 DB .šFÐ4Ê‚.l.±f‰rÛ
0220h: 12 66 64 BD F9 3B C7 05 59 BB 9E CA 99 07 A9 0C .fd½ù;Ç.Y»žÊ™.©.
0230h: 81 98 C3 CA DB AE 26 F9 42 B3 97 52 B8 F5 E1 7E .˜ÃÊÛ®&ùB³—R¸õá~