Unpacking Ramnit malware

nuha2xmad.github.io/unpacking/ramnit/

January 12, 2022



Muhammad Hasan Ali

Malware Analysis learner

3 minute read

As-salamu Alaykum

Introducton

The Ramnit Trojan is a type of malware able to exfiltrate sensitive data. This kind of data can include anything ranging from banking credentials, FTP passwords, session cookies, and personal data. Leaking this information can easily destroy user trust in a business, and in the process lose customers and ruin reputations. <u>1</u>

MD5: 6B71498D63E05F83648E6D9A9CEDBF0A

Static

Open the sample in **DiE** we see that it's high **Entropy** and it's packed.

Unpacking process

Drag the sample into x32dbg and set BPs at VirtualAlloc, VirtualProtect, CreateProcessInternalW, IsDebuggerPresent, WriteProcessMemory, and NtResumeThread. Then press F9 we to hit the first BP. As we know that Ramnit malware is a dropper, we see that it's dropping a file in the same directory where the sample is being debugged.

| CPU | 📄 Log 📑 Notes | • Breakpoints | 🏧 Memory Map 🗐 | Call Stack | 📽 SEH 🙍 | Script 🏾 👰 | Symbols | Source | References | ≫ Threads | 晶 Handles | ₹ ³ Trace |
|-----|---------------|----------------|----------------|-------------------|------------------|------------|-----------|--------------|------------|----------------|----------------|----------------------|
| EIP | | 74D63C23 68 54 | 060000 | ush 654 | | | CreatePr | ocessInterna | 1w < | | | |
| | | 74D63C28 68 DC | 049D674 p | ush kernel32. | .74D649D0 | | | | | | | |
| | | 74D63C2D E8 B6 | E9FEFF c | all kernel32 | .74D525E8 | | | | | | | |
| | | 74D63C32 8B45 | 08 m | ov eax,dword | ptr_ss:[ebp+ | 8] | | | | | | |
| | | 74D63C35 8985 | AOFCFFFF m | ov dword ptr | ss:[ebp_360] | ,eax | | | | | | |
| | | 74D63C3B 8855 | OC m | ov edx,dword | ptr_ss:Lebp+ | c] | | | | | | |
| | | 74D63C3E 8995 | CCFCFFFF m | ov dword ptr | ss:[ebp-334] | ,edx | | | | | | |
| | | 74D63C44 8B75 | 10 m | ov esi,dword | ptr_ss:[ebp | 10] | [[ebp+10] | :"C:\\Users\ | \De | sktop\\ramn1t\ | \\ramnitmgr.ex | e |
| | | 74D63C47 89B5 | C4FCFFFF m | ov aword ptr | ss:[epp-33C] | ,esi | | | | | | |
| | | 74063C40 8845 | 14 | ov eax,dword | ptr_ss:[eop+ | 14 | | | | | | |
| | | 74003030 8983 | ACFBFFFF III | ov aword per | ss:[eop-454] | 101 | | | | | | |
| | | 74005050 0045 | | ov eax, dword otr | cci lobo 4591 | 10] | | | | | | |
| | | 74003035 8903 | 24 | ov anv dword | ntr cc [ohn | .241 | | | | | | |
| | | 74063662 8985 | SCECEEEE | ov dword ntr | ss · Lebn - 37/1 | 03V | | | | | | |
| | | 74D63C68 8845 | 28 | ov eax dword | ntr ss:[ehn+ | 281 | | | | | | |
| | | 74D63C6B 8985 | 24FCFFFF m | ov dword ptr | ss:[ebn-3DC] | .eax | | | | | | |
| | | 74D63C71 8B45 | 2C | ov eax.dword | ptr ss:[ebp+ | 2C1 | | | | | | |
| | | 74D63C74 8985 | COFBFFFF | ov dword ptr | ss:[ebp-440] | .eax | | | | | | |
| | | 74D63C7A 8B45 | 30 m | ov eax.dword | ptr ss:[ebpi | 301 | | | | | | |
| | | 74D63C7D 8985 | 5CFCFFFF m | ov dword ptr | ss:[ebp-3A4] | ,eax | | | | | | |
| | | 74D63C83 33DB | | or ebx,ebx | | | | | | | | |
| | | 74D63C85 899D | DCFCFFFF m | ov dword ptr | ss:[ebp-324] | ,ebx | | | | | | |
| | | 74D63C8B 899D | A8FCFFFF m | ov dword ptr | ss:[ebp-358] | ,ebx | | | | | | |
| | | 74D63C91 899D | F4FBFFFF m | ov dword ptr | ss:[ebp-40C] | ,ebx | | | | | | |
| | | 74D63C97 899D | 30FCFFFF m | ov dword ptr | ss:[ebp-3D0] | ,ebx | | | | | | |
| | | 74D63C9D 899D | B8FCFFFF m | ov dword ptr | ss:[ebp-348] | ,ebx | | | | | | |
| | | 74D63CA3 899D | 98FCFFFF m | ov dword ptr | | ,epx | | | | | | |
| | | 74D63CA9 899D | 2CFCFFFF m | ov aword ptr | ss:[epp-304] | ,ebx | Lepb-3D4 |]:L"sers\\ | | op\\ramnit\\ra | amnitmgr.exe | |
| | | 74003CAF 8990 | 04FCFFFF M | ov aword ptr | ss:reop-39C | ,eox | | | | | | |
| | | 74003CB5 8990 | OCECEEEE IM | ov dword prr | ss:Tebb-3F41 | ,epx | | | | | | |
| | | 4 | | | | | | | | | | |

Figure(1):



Figure(2):

Then press F9 now we hit NtResumeThread BP now we know that it's injecting unpacking code. If we open Process Hacker we see under the ramnit process there's a ramnitmgr.exe child process which is suspended. The parent process is ramnit.bin and the child process is ramnitmgr.exe.

| 4 🗶 x32dbg.exe | 2948 | 1.52 | 60 B/s 45.89 MB | Second systems. | x64dbg |
|------------------|------|------|-----------------|-------------------------------|----------------|
| 4 💽 ramnit.bin | 2524 | 0.02 | 1.28 MB | and solver, in stationed | |
| 📂 ramnitmgr.exe | 2876 | | 740 kB | and a loss of the loss of the | |
| RocessHacker.exe | 2112 | 2.11 | 11.59 MB | and a loss of the second | Process Hacker |

Figure(3):

Now **Don't close the debugger**. Open a new x32dbg window the press file in the menu then attach the child process. Now we have two x32dbg windows are opened. Now if we try to set BPs in the debugger of the child process it says it's invalid add because the process still suspended. To activate go to the debugger of the parent process and run to user code. Now go to the child debugger and set the first 5 BPs as we did above.

| x32dbg | | _ 🗆 🗙 |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------|
| File View Debug Tracing Plugins Favourites Options Help Jul 1 2021 (TitanE | | |
| 💼 🏷 🔳 🔿 🗏 🍷 🖓 🧇 🦆 🏌 🔩 📓 🥒 🚍 🛷 🥒 | fr. 11 A. R. 🖩 🔍 | |
| 🕅 (1911) 🖬 tan 📫 Matan 🔥 Barahaslata (1931) Managari Man | ell'entre de cell 🖉 entre 🎒 entrete 🛆 entrete 🦄 étande 着 timbre 👌 Tana | |
| 👷 🖓 Log 📑 Notes 🔮 Breakpoints 🚥 Memory Map 📑 | Call stack 🖓 SEH 🖬 Script 🖼 Symbols 🗸 Source 🌾 References 🗨 Inreads 🐂 Handles 🖓 Trace | |
| | Hide | FPU |
| | | i i |
| | | |
| | | |
| | V Attach | |
| | | |
| | 2428 ramit Chiga | |
| | 2056 x32dbg ramnit.bin - PID: 2428 - Module: ntdlC:\Users\ | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Default (stdcall) | 🕶 🔻 5 🛛 🔺 🗌 Unlocked |
| | | |
| | | |
| | | |
| | Search: Type here to filter results | |
| | | · · |
| 🛄 Dump 1 🕮 Dump 2 🕮 Dump 3 🕮 Dump 4 🕮 Dump 5 🧔 | Why is process x not snown/ Kerresh (+5) Hind Willdow Attach Cancel | î |
| Address ASCII | | |
| | | |
| | | 1 |
| | | |
| | | |
| | | |
| | | |
| Command: Commands are comma separated (like assembly instructions): | | Default 🔻 |
| Ready File read thread finished! | | ne Wasted Debugging: 0:07:38:20 |

Figure(4):

Return to Parent debugger, press F9 to hit IsDebuggerPresent BP, beacause the debugger is present so EAX is set to 1 if we continue the debugger will exit and pops up this is a compiled autoit script. So we need to change it to 0. Now Execute till return and double click on EAX and change it to 0. After that run F9 again and IsDebuggerPresent BP hits do the same and change it to 0 and then run F9.

| ramnit.bin - PID: 1312 - Module: kernelbase.dll - Thread: Main Thread 1368 - x32dbg | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| File Yaw Debug Tracing Plugins Favourites Options Help Jul 1 2021 (TitanEngine) | | |
| 📫 10 🔳 → 11 † 14 14 3 † -4 3 🖉 🖋 🥔 🎋 | - # A - B, B - 9 | |
| 🖾 CPU 📑 Log 👔 Notes 🔸 Breakpoints 🚥 Memory Map 💣 Call S | si Stack 💁 SELL 🗴 Script 🗿 Symbols 🔗 Source 🔎 References 🛸 Threads 🐴 Handles 🤄 Trace | |
| Image: Construction Image: Construction | Block Statu Source Network Intests Nanoes Intests edi acti esp so esp so esp so est act, down d ptr ss:[ebp+8] eax, down d ptr ss:[ebp-8] eax, down d ptr ss:[ebp-10] eax, down d | Î |
| 76693927 8045 F0 16a ea 76693912 8045 F0 16a ea 76693932 8045 F8 16a ea 76693932 8045 F8 15 00106876 public 7669336 80F0 mov e5 | bax_choword ptr ss:[ebp-10] Unsgned: 0 eax_choword ptr ss:[ebp-8] ASCII: dword ptr ds:[-skrt]Unicodestring OK Cancel OK Cancel 1: [ssp+4] 00000000 1: [ssp+4] 00000000 2: [ssp+4] 00000000 | icked |

Figure(5):

Now we go back to the child process debugger to get the unpacked file. Then run F9 hits VirtualProtect BP then Execute till return we see the 2nd parameter points to a location 400000 and change the permission to RWC which an indicator of unpacking. Then we dump it we see MZ magic byte. Run F9 again we see the same location but changes the permission to R which an indicator to finish unpacking. We go and Follow in Memory map and save it. Analyze it then come back it's not our goal.

| 🕅 CPU 📑 Log 👔 Notes 🔹 Breakpoints 🚥 Memory Map 🧊 Call Stack 😪 SEH 🖬 Script 💁 Symbols | 🗢 Source 🔎 References 👒 Threads 👍 Handles 🧳 Trace |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EIP 7668F0FE C2 1000 ret 10 ret of 2nd VirtualProte | A Hide FPU |
| 7668100 CC 1113 1113 7668101 CC 1113 1113 7668101 CC 1113 1113 7668101 CC 1113 1113 7668101 SEF mov edit edit virtu 7668101 FF7 SO push dword ptr 551 (ebp+1)0 roberter 7668101 Edit FFF FF CC 111 (ebr=1) virtu 7668101 CC 111 (ebr=1) virtu virtu 7668101 CC 111 (ebr=1) virtu virtu 7668102 CC 1113 virtu virtu 7668102 CC 1113 virtu virtu 7668102 CC 1113 virtu virtu 7668102 CC | alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuery alQuer |
| /668F12A FF/5 10 push dword ptr 55: [ebp+14] 7668F12D FF75 10 push dword ptr 55: [ebp+10] 7668F120 FF75 0r push dword ptr 55: [ebp+10] | C5 0028 D5 0028 |
| 7668F136 F75 08 push dword ptr 5s.[ebp+8] | |
| 7658F138 E8 4BFFFFFF call <kernelbase.virtualallocex> 7668F13D 5D pop ebp</kernelbase.virtualallocex> | Unicked T : [esp+4] 00400000 "MZ" |
| .tox::7668PDFE kernelbase.dll:SFDFF #sfFF | → ?: (csp.s) 00001002 2: (csp.s) 0000002 4: (csp.s) 0000002 5: (csp.s) 0000004 |
| 11 Duran 1 11 Duran 2 11 Duran 4 11 Duran 5 14 Match 1 Jacob 2 Charact | 0018FF54 p00440384 return to ramnitmgr.00440384 from ??? |
| Construct Construct <t< td=""><td>013#F\$8 00400000 ramitegr.04400000 013#F\$8 0000000 013#F\$8 0003000 013#F\$8 0000000 013#F\$8 0000000 0000000 0000000 0000000 0000000</td></t<> | 013#F\$8 00400000 ramitegr.04400000 013#F\$8 0000000 013#F\$8 0003000 013#F\$8 0000000 013#F\$8 0000000 0000000 0000000 0000000 0000000 |
| Command: Commands are comma separated (like assembly instructions): mov eax, ebx | Default 🔻 |

Figure(6):

Now we are back and press F9 hits VirtualAlloc BP and Execute till return we see it's allocating memory then dump EAX in dump 2 then press F9 we see it's unpacking some strange strings in the dump 2. Then Execute till return and dump EAX in dump 3 then press F9 we see dump 3 is empty. Then Execute till return and dump EAX to dump 4. Then run F9 and chech dump 4 we see our unpacked file.

| 100 | Dump | i 🕨 | Į | | Dum | p 2 | | . | Dun | np 3 | | i 11 | Du | mp 4 | 1 | , , | D | ump 5 | 60 | Wa | tch 1 | | - Lo | ocals | 2 | Struct | |
|--------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------|-------|------|-------|---|--------|--|
| Addr | ess | Hex | ĸ | | | | | | | | | | | | | | | ASCII | | | | | | | | | |
| 001E 001E 001E 001E 001E 001E 001E 001E | 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 | 55 45 54 F4 FF 8B 74 FF 41 | 8B FC 89 FF 3C 0B 40 03 FF C6 | EC 89 85 FF 75 C0 04 5B 44 85 | 81 45 50 50 75 8B C9 C6 A8 | C4 C8 F6 68 E8 0B 40 C3 85 FD | 48 64 FF C3 5F 8B 04 C6 A6 FF | F4 A1 FF C1 08 85 0D 85 FD FF | FF 18 6A BE 00 4C 20 A4 FF 50 | FF 00 04 36 00 F6 00 FD FF C6 | 53 00 8D E8 FF 20 FF 56 85 | E8 00 40 0D D0 FF 00 FF C6 A9 | E3 8B 04 8B 8B 3D 41 85 FD | 06 40 50 85 40 7 <u>C</u> 6 A7 FF | 00 30 8D 00 48 38 00 85 FD FF | 00 8B 85 68 F4 EB 77 A5 FF 49 | 8B 40 48 A1 FF 03 00 FD FF C6 | U.ì.ÄH EÜ.EÈC TLÖŸ ÔŸŸPh Ô <upè_ Ÿ.Au .@@ t.[ÉĂ, ŸŸDÆ. AÆ. ÝÝ</upè_ | HÔÿÿS J; ÿÿj ¼Å¾6è LÖÿ LÖÿ VÿŸV ÿŸPÆ. | 5èã. @ @.P /Ð /Ÿ.@ /Ÿ.@ /Ÿ.@ /¥.§ ©ÝŸ | 0.@ н .h; Hôÿ 8ë. .w. .¥ý ýÿÿ ŸIÆ | | | | | | |
| Comm | and: | Com | | ds (| are | cor | | | par | ated | д (| lik | | | nbl | y in | | ructio | ns): | mov | eax | , ebx | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure(7):

Now we open **Process Hacker** to save our unpacked file which is packed with **UPX**. The OEP might be different to yours. Then unpack **UPX** using **CFF Explorer** tool.

| 🍽 Dun | np 1 | 1 | Du | ump | 2 | 100 | Dur | n <mark>p 3</mark> | | 1 00 | Dun | np 4 | | (0) | D | ump 5 | 60 | Watch 1 | l | [<i>x</i> =] L | ocals | 2 | Struct | |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|----------------------------------------------------|---------------------------------------------------|--------|-------------------------------------------------|---|-----------------|-------|---|--------|--|
| Address | Hex | | | | | | | | | | | | | | | ASCII | | | | | | | | |
| 0026000 0026001 0026002 0026003 0026004 0026005 0026006 0026007 0026008 0026009 | 0 4D 0 88 0 00 0 00 0 0E 0 69 0 74 0 6D 0 87 0 7D | 5A 00 00 1F 73 20 6F E2 9C | 90 00 00 BA 20 62 62 64 D9 A4 | 00 00 00 00 00 00 00 00 00 00 70 70 65 22 65 25 55 F | 03 0 00 0 00 0 00 0 00 8 72 6 20 7 22 0 73 8 53 8 | 00 00 00 | 0 00 0 00 0 00 0 00 0 00 0 00 7 72 5 6E 0 0A 7 06 7 06 | 04 40 00 21 61 20 24 F3 0F | 00 00 00 88 6D 69 00 83 A3 | 00 00 00 01 20 6E 00 B7 A5 | 00 00 00 4C 63 20 00 06 06 | FF 00 C8 CD 61 44 00 F3 F2 | FF 00 00 21 6E 4F 00 83 83 | 00 00 00 54 6E 53 00 87 87 | 00 00 00 68 6F 20 00 06 06 | MZ is pro t be r mode âùUó. }.¤.Á. | @. | ÿÿ È .Lf!Th canno n DOS ó ¥.ò | | | | | | |
| Command | Comm | land | | re (| com | | epar | | d (1 | like | e as | | ubly | y in | | ruction | ເຮ): | mov eax | | ebx | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | |

Figure(8):

Article quote

لن يدومَ الهمُّ يا حلوَ المُحيّا، لن يظلّ الحزنُ في عينيكَ يحيا

REF

1- https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan

2- https://www.youtube.com/watch?v=l6ZunH6YG0A&ab_channel=GuidedHacking