Hunting Layered Malware by Raul Alvarez

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

  What is Vawtrak? • Also known as Neverquest • A banking trojan • Uses layering techniques similar to a Matryoshka doll • Uses mul.ple armoring strategies • Uses DGA • Uses Tor2web

- 7.

  What is Scieron? • Not a popular malware • A regular trojan • Uses layering techniques quite differently than Vawtrak • Uses simple decryp.on

- 8.
- 9.
- 10.
- 11.
- 12.
- 13.
- 14.
- 15.
- 16.
- 17.
- 18.
- 19.
- 20.
- 21.

  Layer 2: Decryp$on+ Garbage Collec$on Layer 2 Layer 3 Self-code Injec.on resource sec8on An.-An.malware hashing for validity decryp.on Layer 4 Layer 2 decryp8on garbage collec.on Layer 3 decrypted + compressed Layer 3 decompressed Decompression RtlDecompressBuffer Layer 1 An.-Emulator An.-Debugger An.-Analysis decryp.on overlay Layer 2 (encrypted) decoy

- 22.

  Layer 2: Decryp$on+ Garbage Collec$on decrypted/compressed executable relevant code decryp.on algorithm garbage code

- 23.
- 24.

  Layer 2: Decompression RtlDecompressBuffer Syntax: NTSTATUS RtlDecompressBuffer(_In_ USHORT CompressionFormat, _Out_ PUCHAR UncompressedBuffer, _In_ ULONG UncompressedBufferSize, _In_ PUCHAR CompressedBuffer, _In_ ULONG CompressedBufferSize, _Out_ PULONG FinalUncompressedSize); compressed decompressed RtlDecompressBuffer(0x102,0x1744e8, 0x30e00, 0x1436d0, 0x2F9AE, 0x12fcc4)

- 25.

  Layer 2: Self-codeInjec$on Layer 2 Layer 3 Self-code Injec.on resource sec8on An.-An.malware hashing for validity decryp.on Layer 4 Layer 2 decryp.on garbage collec.on Layer 3 decrypted + compressed Layer 3 decompressed Decompression RtlDecompressBuffer Layer 1 An.-Emulator An.-Debugger An.-Analysis decryp.on overlay Layer 2 (encrypted) decoy Layer 2 Layer 3 Self-code Injec8on resource sec8on An.-An.malware hashing for validity decryp.on

- 26.

  Layer 2: Self-codeInjec$on Steps: 1. Allocates new memory(0x8a0000) 2. Copies the decompressed Layer 3 to 0x8a0000 3. Zeroes out the original loca.on(0x400000) of Layer 2 4. Copies Layer 3 from 0x8a0000 to 0x400000 5. Fixes IAT of Layer 3 in 0x400000 6. Executes Layer 3

- 27.
- 28.

  Layer 3: An$-an$malware 1. Traverses the following folders: • Program Files • Program Files (x86) • %AppData% 2. Creates hash value for the an.malware pathname 3. Creates registry key • HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosooWindowsSafer CodeIden.fi ers0Paths[hash value] • SaferFlags = 0 • ItemData = pathname

- 29.
- 30.

  Layer 3: Genera$ngLayer 4 Layer 2 Layer 3 Self-code Injec.on resource sec8on An.-An.malware hashing for validity decryp.on Layer 4 Layer 2 decryp.on garbage collec.on Layer 3 decrypted + compressed Layer 3 decompressed Decompression RtlDecompressBuffer Layer 1 An.-Emulator An.-Debugger An.-Analysis decryp.on overlay Layer 2 (encrypted) decoy Layer 2 Layer 3 Self-code Injec.on resource sec8on An8-An8malware hashing for validity decryp.on Layer 2 Layer 3 resource sec8on An.-An.malware hashing for validity decryp.on Layer 4

- 31.

  Layer 3: Genera$ngLayer 4 1. Copies RT_RCDATA from .rscr sec.on to the heap memory 2. Calculates the hash (0x24D2EDEA) of the raw data 3. Decrypts the raw data 4. Calculates the hash(0x52194545) of

the decrypted data(DLL) 5. Creates random filename + ".dat" 6. Copies the decrypted data from heap memory to newly created file (Layer 4) 7. Creates new startup registry key for Layer 4(DLL)

- 32.
- 33.
- 34.

Layer 1: SimpleDecryp$on Layer 1 Normal-looking Code decryp.on explorer.exe process Layer 2 shellcode TRF#.tmp Layer 3 dropped file Code Injec.on Layer 3 Code Injec.on .rsrc sec8on Layer 4 (mshVps.dll) rundll32.exe process

- 35.
- 36.

Layer 1: CodeInjec$on - Shellcode Layer 1 Normal-looking Code decryp.on explorer.exe process Layer 2 shellcode TRF#.tmp Layer 3 dropped file Code Injec.on Layer 3 Code Injec.on .rsrc sec8on Layer 4 (mshVps.dll) rundll32.exe process

- 37.

Layer 1: CodeInjec$on - Shellcode shellcode explorer.exe process scieron.exe process

- 38.

Layer 1: CodeInjec$on - Shellcode shellcode (code view) shellcode (hex view)

- 39.
- 40.

Layer 2: CodeInjec$on – TRF file Layer 1 Normal-looking Code decryp.on explorer.exe process Layer 2 shellcode TRF#.tmp Layer 3 dropped file Code Injec.on Layer 3 Code Injec.on .rsrc sec8on Layer 4 (mshVps.dll) rundll32.exe process

- 41.

Layer 2: CodeInjec$on – TRF file explorer.exe Loads TRF file into explorer.exe process.

- 42.
- 44.

Layer 3: Genera$ngLayer 4 Layer 1 Normal-looking Code decryp.on explorer.exe process Layer 2 shellcode TRF#.tmp Layer 3 dropped file Code Injec.on Layer 3 Code Injec.on .rsrc sec8on Layer 4 (mshVps.dll) rundll32.exe process

- 45.

Layer 3: Genera$ngLayer 4 1. Locates resource named "ID101" of type RT_RCDATA 2. Creates a new file "mshUps.dll" 3. Writes the the content of resource "ID101" to the newly created file

- 46.
- 47.
- 48.
- 49.

  psxview c:v24 --profile=WinXPSP2x86 -fvawtrak.vmem psxview Volatility Foundation Volatility Framework 2.4 Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskth ---------- -------------- ------ ------ ------ ------ -------- ------ ----- ------- ------ 0x01b8db28 mainOUT-crypted 224 True True True True True True True 0x019d4c90 cmd.exe 1420 True True True True True True True 0x01aa01d8 lsass.exe 680 True True True True True True True 0x01704218 wscntfy.exe 1672 True True True True True True True 0x0193c8d8 jusched.exe 1832 True True True True True True True 0x018ebda0 winlogon.exe 624 True True True True True True True 0x01aa4a28 svchost.exe 1208 True True True True True True True 0x01aaada0 svchost.exe 1044 True True True True True True True 0x018deac0 explorer.exe 1692 True True True True True True True <<cut>>

- 50.

  malfind c:v24 --profile=WinXPSP2x86 -fvawtrak.vmem malfind -p 224 Volatility Foundation Volatility Framework 2.4 Process: mainOUT-crypted Pid: 224 Address: 0x890000 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6 0x00890000 55 53 57 56 81 ec 98 01 00 00 8b 84 24 ac 01 00 USWV.....$... 0x00890010 00 c7 84 24 d4 00 00 00 00 00 00 00 c7 84 24 fc ...$.....$. 0x00890020 00 00 00 00 00 00 00 66 c7 84 24 9e 00 00 00 0f .....f..$..... 0x00890030 6e c7 84 24 38 01 00 00 01 00 00 00 8b 8c 24 38 n..$8.....$8 0x890000 55 PUSH EBP 0x890001 53 PUSH EBX 0x890002 57 PUSH EDI 0x890003 56 PUSH ESI 0x890004 81ec98010000 SUB ESP, 0x198 0x89000a 8b8424ac010000 MOV EAX, [ESP+0x1ac] 0x890011 c78424d400000000000000 MOV DWORD [ESP+0xd4], 0x0 0x89001c c78424fc00000000000000 MOV DWORD [ESP+0xfc], 0x0 0x890027 66c784249e0000000f6e MOV WORD [ESP+0x9e], 0x6e0f 0x890031 c784243801000001000000 MOV DWORD [ESP+0x138], 0x1 0x89003c 8b DB 0x8b 0x89003d 8c2438 MOV [EAX+EDI], FS

- 51.

  yarascan c:v24 --profile=WinXPSP2x86 -fvawtrak.vmem yarascan -p 224 --yara-rules="MZ“ Rule: r1 Owner: Process mainOUT-crypted Pid 224 0x77dd0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.............. 0x77dd0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@....... 0x77dd0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 0x77dd0030 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 .... 0x77dd0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x77dd0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x77dd0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x77dd0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$....... 0x77dd0080 a8 6a e2 68 ec 0b 8c 3b ec 0b 8c 3b ec 0b 8c 3b .j.h...;...;...; 0x77dd0090 2f 04 d1 3b eb 0b 8c 3b 2f 04 83 3b e1 0b 8c 3b /..;...;/..;...; 0x77dd00a0 3d 07 d3 3b ee 0b 8c 3b ec 0b 8d 3b 54 0a 8c 3b =..;...;...;T..; 0x77dd00b0 2f 04 d0 3b ed 0b 8c 3b 2f 04 d2 3b ed 0b 8c 3b /..;...;/..;...; 0x77dd00c0 2f 04 ec 3b f1 0b 8c 3b 2f 04 d3 3b 7e 0b 8c 3b /..;...;/..;~..; 0x77dd00d0 2f 04 d6 3b ed 0b 8c 3b 52 69 63 68 ec 0b 8c 3b /..;...;Rich...; 0x77dd00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 ..... 0x77dd00f0 50 45 00 00 4c 01 04 00 71 03 90 49 00 00 00 00 PE..L...q..I.... Rule: r1 Owner: Process mainOUT-crypted Pid 224 0x77de8218 4d 5a 75 1d 8b 48 3c 8d 51 40 3b da 72 13 33 d2 MZu..H<.Q@;.r.3. 0x77de8228 81 3c 01 50 45 00 00 0f 94 c2 8b c2 5b 5d c2 04 .<.PE.....[].. 0x77de8238 00 33 c0 eb f7 90 90 90 4d 5a 00 90 90 90 90 90 .3.....MZ..... <<next slide>>

- 52.

  yarascan <<continuation>> 0x77de8248 8b ff55 8b ec 51 8b 45 08 53 56 33 f6 48 57 8b ..U..Q.E.SV3.HW. 0x77de8258 7d 10 89 75 fc 74 67 48 0f 85 59 03 02 00 8d 45 }..u.tgH..Y....E 0x77de8268 10 50 ff 75 0c 89 75 10 ff 15 a8 11 dd 77 83 f8 .P.u..u.....w.. 0x77de8278 ff 89 45 08 74 7f 39 75 10 0f 85 59 03 02 00 56 ..E.t.9u...Y...V 0x77de8288 56 56 6a 02 56 ff 75 0c ff 15 0c 12 dd 77 8b d8 VVj.V.u.....w.. 0x77de8298 3b de 74 61 56 56 56 6a 04 53 ff 15 10 12 dd 77 ;.taVVVj.S.....w 0x77de82a8 53 89 47 04 ff 15 34 10 dd 77 39 77 04 74 46 8b S.G...4..w9w.tF. 0x77de82b8 45 08 89 07 8b 45 fc 5f 5e 5b c9 c2 0c 00 56 68 E....E._^[....Vh 0x77de82c8 80 00 00 00 6a 03 56 6a 01 68 00 00 00 80 ff 75 ....j.Vj.h.....u 0x77de82d8 0c ff 15 08 12 dd 77 8b d8 83 fb ff 74 17 ff 75 ......w.....t..u 0x77de82e8 10 53 6a 02 e8 57 ff ff ff 53 89 45 fc ff 15 34 .Sj..W...S.E...4 0x77de82f8 10 dd 77 eb bf ff 15 54 10 dd 77 e9 e1 02 02 00 ..w....T..w..... 0x77de8308 90 90 90 90 90 8b ff 55 8b ec 81 ec 50 02 00 00 .......U....P... Rule: r1 Owner: Process mainOUT-crypted Pid 224 0x77de8240 4d 5a 00 90 90 90 90 90 8b ff 55 8b ec 51 8b 45 MZ.....U..Q.E 0x77de8250 08 53 56 33 f6 48 57 8b 7d 10 89 75 fc 74 67 48 .SV3.HW.}..u.tgH 0x77de8260 0f 85 59 03 02 00 8d 45 10 50 ff 75 0c 89 75 10 ..Y....E.P.u..u. 0x77de8270 ff 15 a8 11 dd 77 83 f8 ff 89 45 08 74 7f 39 75 .....w....E.t.9u 0x77de8280 10 0f 85 59 03 02 00 56 56 56 6a 02 56 ff 75 0c ...Y...VVVj.V.u. 0x77de8290 ff 15 0c 12 dd 77 8b d8 3b de 74 61 56 56 56 6a .....w..;.taVVVj 0x77de82a0 04 53 ff 15 10 12 dd 77 53 89 47 04 ff 15 34 10 .S.....wS.G...4. 0x77de82b0 dd 77 39 77 04 74 46 8b 45 08 89 07 8b 45 fc 5f .w9w.tF.E....E._ 0x77de82c0 5e 5b c9 c2 0c 00 56 68 80 00 00 00 6a 03 56 6a ^[....Vh....j.Vj

- 53.

  yarascan <<continuation>> Rule: r1 Owner: ProcessmainOUT-crypted Pid 224 0x00400000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x00400010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x00400020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x00400030 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 ..... 0x00400040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x00400050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x00400060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x00400070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x00400080 52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 Ro..... 0x00400090 1f 76 2c c9 17 0e b9 c9 16 0e b9 c9 15 0e b9 c9 .v,..... 0x004000a0 1f 76 2a c9 1b 0e b9 c9 16 0e b8 c9 4a 0e b9 c9 .v*.....J... 0x004000b0 79 78 17 c9 1b 0e b9 c9 79 78 23 c9 17 0e b9 c9 yx.....yx#..... 0x004000c0 79 78 24 c9 17 0e b9 c9 52 69 63 68 16 0e b9 c9 yx$.....Rich.... 0x004000d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x004000e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ........PE..L... 0x004000f0 6e 22 2c 52 00 00 00 00 00 00 00 00 e0 00 03 01 n",R..... Layer 1

- 54.

yarascan <<continuation>> Rule: r1 Owner: ProcessmainOUT-crypted Pid 224 0x001436d3 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 MZ.....0.... 0x001436e3 b8 00 38 2d 01 00 40 04 38 19 00 e8 00 0c 0e 1f ..8-..@.8..... 0x001436f3 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 .....!...L.!Th 0x00143703 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e is..program..can 0x00143713 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 not..be.run.i.n. 0x00143723 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 86 DOS.mo.de....$.. 0x00143733 00 52 6f d7 9a 16 0e b9 c9 41 05 03 1f 76 2c c9 .Ro.....A...v,. 0x00143743 17 04 0b 15 11 02 0f 2a c9 1b 02 0f b8 c9 4a 11 .....*.....J. 0x00143753 00 07 79 78 17 02 0f 79 78 23 11 02 27 79 78 24 ..yx...yx#..'yx$ 0x00143763 02 07 52 69 63 06 68 01 33 15 ab 50 45 00 00 4c ..Ric.h.3..PE..L 0x00143773 80 01 05 00 6e 22 2c 52 05 13 00 e0 00 03 01 0b ....n",R..... 0x00143783 01 0a 00 42 00 01 46 e6 02 00 00 00 01 96 7e 10 ...B..F.....~. 0x00143793 80 05 81 01 02 80 00 02 81 05 80 0b 05 cc 00 01 ..... 0x001437a3 82 19 85 03 00 60 80 9a 00 9a f4 5f c7 02 0f 81 .....`....._.... 0x001437b3 02 14 81 15 86 03 06 03 41 02 00 68 5c 00 00 8c ....A..h... 0x001437c3 01 04 80 30 00 00 1c d0 80 18 45 00 50 00 04 00 ...0.....E.P... Compressed Layer 3

- 55.

  yarascan <<continuation>> Rule: r1 Owner: ProcessmainOUT-crypted Pid 224 0x001744e8 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x001744f8 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x00174508 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x00174518 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 ..... 0x00174528 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x00174538 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x00174548 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x00174558 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x00174568 52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 Ro..... 0x00174578 1f 76 2c c9 17 0e b9 c9 16 0e b9 c9 15 0e b9 c9 .v,..... 0x00174588 1f 76 2a c9 1b 0e b9 c9 16 0e b8 c9 4a 0e b9 c9 .v*.....J... 0x00174598 79 78 17 c9 1b 0e b9 c9 79 78 23 c9 17 0e b9 c9 yx.....yx#..... 0x001745a8 79 78 24 c9 17 0e b9 c9 52 69 63 68 16 0e b9 c9 yx$.....Rich.... 0x001745b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x001745c8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ........PE..L... 0x001745d8 6e 22 2c 52 00 00 00 00 00 00 00 e0 00 03 01 n",R..... Decompressed Layer 3

- 56.

  yarascan <<continuation>> Rule: r1 Owner: ProcessmainOUT-crypted Pid 224 0x008a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x008a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x008a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x008a0030 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 ..... 0x008a0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x008a0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x008a0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x008a0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x008a0080 52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 Ro..... 0x008a0090 1f 76 2c c9 17 0e b9 c9 16 0e b9 c9 15 0e b9 c9 .v,..... 0x008a00a0 1f 76 2a c9 1b 0e b9 c9 16 0e b8 c9 4a 0e b9 c9 .v*.....J... 0x008a00b0 79 78 17 c9 1b 0e b9 c9 79 78 23 c9 17 0e b9 c9 yx.....yx#..... 0x008a00c0 79 78 24 c9 17 0e b9 c9 52 69 63 68 16 0e b9 c9 yx$.....Rich.... 0x008a00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x008a00e0 00 00 00 00 00 00 00

00 00 50 45 00 00 4c 01 05 00 .....PE..L... 0x008a00f0 6e 22 2c 52 00 00 00 00 00 00 00 00 e0 00 03 01 n",R..... Layer 3 for self-code injec.on

- 57.

  yarascan <<continuation>> Rule: r1 Owner: Processmain OUT-crypted Pid 224 0x00aaa668 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x00aaa678 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x00aaa688 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x00aaa698 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 ..... 0x00aaa6a8 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 .....!..L.!Th 0x00aaa6b8 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x00aaa6c8 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x00aaa6d8 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x00aaa6e8 8b 95 09 e6 cf f4 67 b5 cf f4 67 b5 cf f4 67 b5 .....g...g...g. 0x00aaa6f8 3e 32 a8 b5 d6 f4 67 b5 3e 32 aa b5 c4 f4 67 b5 >2....g.>2....g. 0x00aaa708 3e 32 a9 b5 95 f4 67 b5 c6 8c f4 b5 ca f4 67 b5 >2....g.....g. 0x00aaa718 cf f4 66 b5 9c f4 67 b5 54 1f a8 b5 cd f4 67 b5 ..f...g.T.....g. 0x00aaa728 54 1f ae b5 ce f4 67 b5 54 1f ab b5 ce f4 67 b5 T.....g.T.....g. 0x00aaa738 52 69 63 68 cf f4 67 b5 50 45 00 00 4c 01 05 00 Rich..g.PE..L... 0x00aaa748 42 e1 2d 52 00 00 00 00 00 00 00 00 e0 00 02 21 B.-R.....! 0x00aaa758 0b 01 08 00 00 30 02 00 00 00 02 00 00 00 00 00 .....0..... Layer 4

- 58.
- 59.
- 60.
- 61.

  psxview c:v24 --profile=WinXPSP2x86 -fscieron.vmem psxview Volatility Foundation Volatility Framework 2.4 Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskth ---------- -------------- ------ ------ ------ ------ -------- ------ ----- ------- ------ 0x02317c10 scieron.exe 1692 True True False True True False 0x0215f020 winlogon.exe 628 True True True True True True True 0x02421020 lsass.exe 684 True True True True True True True 0x02160778 alg.exe 1972 True True True True True True True 0x024135e8 svchost.exe 972 True True True True True True True 0x02339868 services.exe 672 True True True True True True True 0x02443648 svchost.exe 1088 True True True True True True True 0x0236dda0 explorer.exe 1872 True True True True True True True <<cut>>

- 62.

  malfind c:v24 --profile=WinXPSP2x86 -fscieron.vmem malfind –p 1872 Volatility Foundation Volatility Framework 2.4 Process: explorer.exe Pid: 1872 Address: 0x23e0000 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6 0x023e0000 cc 9c 8b 44 24 24 83 e8 05 89 44 24 24 c7 00 b8 ...D$$....D$$... 0x023e0010 19 00 00 c6 40 04 b8 e8 04 01 00 00 43 3a 5c 44 ....@.....C:D 0x023e0020 4f 43 55 4d 45 7e 31 5c xx xx xx xx xx 5c 4c 4f OCUME~1userXLO 0x023e0030 43 41 4c 53 7e 31 5c 54 65 6d 70 5c 54 52 46 32 CALS~1TempTRF2 0x23e0000 cc INT 3 0x23e0001 9c PUSHF 0x23e0002 8b442424 MOV EAX, [ESP+0x24] 0x23e0006 83e805 SUB EAX, 0x5 0x23e0009 89442424 MOV [ESP+0x24], EAX 0x23e000d c700b8190000 MOV DWORD [EAX], 0x19b8 0x23e0013 c64004b8 MOV BYTE

[EAX+0x4], 0xb8 0x23e0017 e804010000 CALL 0x23e0120 0x23e001c 43 INC EBX 0x23e001d 3a5c444f CMP BL, [ESP+EAX*2+0x4f] 0x23e0021 43 INC EBX 0x23e0022 55 PUSH EBP 0x23e0023 4d DEC EBP ----continued---- Layer 2 injected shell code

- 63.

  malfind ----continuation---- 0x23e0024 45 INCEBP 0x23e0025 7e31 JLE 0x23e0058 0x23e0027 5c POP ESP 0x23e0028 7769 JA 0x23e0093 0x23e002a 6e OUTS DX, BYTE [ESI] 0x23e002b 58 POP EAX 0x23e002c 50 PUSH EAX 0x23e002d 5c POP ESP 0x23e002e 4c DEC ESP 0x23e002f 4f DEC EDI 0x23e0030 43 INC EBX 0x23e0031 41 INC ECX 0x23e0032 4c DEC ESP 0x23e0033 53 PUSH EBX 0x23e0034 7e31 JLE 0x23e0067 0x23e0036 5c POP ESP 0x23e0037 54 PUSH ESP 0x23e0038 656d INS DWORD [ES:EDI], DX 0x23e003a 705c JO 0x23e0098 0x23e003c 54 PUSH ESP 0x23e003d 52 PUSH EDX 0x23e003e 46 INC ESI 0x23e003f 32 DB 0x32

- 64.

  yarascan c:v24 --profile=WinXPSP2x86 -fscieron.vmem yarascan -p 1872 --yara-rules="MZ" Rule: r1 Owner: Process explorer.exe Pid 1872 0x023f0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x023f0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x023f0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x023f0030 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 ..... 0x023f0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x023f0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x023f0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x023f0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x023f0080 57 dd d9 19 13 bc b7 4a 13 bc b7 4a 13 bc b7 4a W......J...J...J 0x023f0090 34 7a cc 4a 14 bc b7 4a 13 bc b6 4a 1c bc b7 4a 4z.J...J...J...J 0x023f00a0 1a c4 3d 4a 12 bc b7 4a 1a c4 25 4a 12 bc b7 4a ..=J...J..%J...J 0x023f00b0 0d ee 23 4a 12 bc b7 4a 1a c4 26 4a 12 bc b7 4a ..#J...J..&J...J 0x023f00c0 52 69 63 68 13 bc b7 4a 00 00 00 00 00 00 00 00 Rich...J..... 0x023f00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x023f00e0 50 45 00 00 4c 01 04 00 00 00 00 00 00 00 00 00 PE..L..... 0x023f00f0 00 00 00 00 e0 00 02 21 0b 01 09 00 00 02 00 00 .....!..... Layer 3

- 65.

  yarascan <<continuation>> Rule: r1 Owner: Processexplorer.exe Pid 1872 0x023f3060 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x023f3070 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x023f3080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x023f3090 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 ..... 0x023f30a0 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x023f30b0 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x023f30c0 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x023f30d0 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x023f30e0 2c c8 cb 2b 68 a9 a5 78 68 a9 a5 78 68 a9 a5 78 ,..+h..xh..xh..x 0x023f30f0 61 d1 30 78 69 a9 a5 78 4f 6f de 78 67 a9 a5 78 a.0xi..xOo.xg..x 0x023f3100 68 a9 a4 78 5b a9 a5 78 61 d1 2f 78 6c a9 a5 78 h..x[..xa./xl..x 0x023f3110 61 d1 37 78 69 a9 a5 78 76 fb 31 78 69 a9 a5 78 a.7xi..xv.1xi..x 0x023f3120 61 d1 34 78 69 a9 a5 78 52 69 63 68 68 a9 a5 78 a.4xi..xRichh..x 0x023f3130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x023f3140 00

00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 .....PE..L... 0x023f3150 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 .....! Layer 4 mshUps,dll

- 66.
- 67.

psxview c:v24 --profile=WinXPSP2x86 -fscieron.vmem psxview Volatility Foundation Volatility Framework 2.4 Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskth ---------- ---------- ------ ------ ------ ------ -------- ------ ----- ------- ------ 0x0215f020 winlogon.exe 628 True True True True True True 0x02421020 lsass.exe 684 True True True True True True 0x02160778 alg.exe 1972 True True True True True True True 0x024135e8 svchost.exe 972 True True True True True True 0x02339868 services.exe 672 True True True True True True 0x021565f0 svchost.exe 864 True True True True True True 0x0236dda0 explorer.exe 1872 True True True True True True 0x023001f8 rundll32.exe 1768 True True True True True True <<cut>>

- 68.

malfind c:v24 --profile=WinXPSP2x86 -fscieron.vmem malfind –p 1872 Volatility Foundation Volatility Framework 2.4 Process: explorer.exe Pid: 1872 Address: 0x1490000 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6 0x01490000 60 9c 8b 44 24 24 83 e8 05 89 44 24 24 c7 00 b8 `..D$$....D$$... 0x01490010 19 00 00 c6 40 04 b8 e8 04 01 00 00 43 3a 5c 44 ....@.....C:D 0x01490020 4f 43 55 4d 45 7e 31 5c xx xx xx xx xx 5c 4c 4f OCUME~1userXLO 0x01490030 43 41 4c 53 7e 31 5c 54 65 6d 70 5c 54 52 46 32 CALS~1TempTRF2 0x1490000 60 PUSHA 0x1490001 9c PUSHF 0x1490002 8b442424 MOV EAX, [ESP+0x24] 0x1490006 83e805 SUB EAX, 0x5 0x1490009 89442424 MOV [ESP+0x24], EAX 0x149000d c700b8190000 MOV DWORD [EAX], 0x19b8 0x1490013 c64004b8 MOV BYTE [EAX+0x4], 0xb8 0x1490017 e804010000 CALL 0x1490120 0x149001c 43 INC EBX 0x149001d 3a5c444f CMP BL, [ESP+EAX*2+0x4f] 0x1490021 43 INC EBX 0x1490022 55 PUSH EBP 0x1490023 4d DEC EBP ----continued---- Layer 2 same shellcode

- 69.

malfind ----continuation---- 0x1490024 45 INCEBP 0x1490025 7e31 JLE 0x1490058 0x1490027 5c POP ESP 0x1490028 7769 JA 0x1490093 0x149002a 6e OUTS DX, BYTE [ESI] 0x149002b 58 POP EAX 0x149002c 50 PUSH EAX 0x149002d 5c POP ESP 0x149002e 4c DEC ESP 0x149002f 4f DEC EDI 0x1490030 43 INC EBX 0x1490031 41 INC ECX 0x1490032 4c DEC ESP 0x1490033 53 PUSH EBX 0x1490034 7e31 JLE 0x1490067 0x1490036 5c POP ESP 0x1490037 54 PUSH ESP 0x1490038 656d INS DWORD [ES:EDI], DX 0x149003a 705c JO 0x1490098 0x149003c 54 PUSH ESP 0x149003d 52 PUSH EDX 0x149003e 46 INC ESI 0x149003f 32 DB 0x32

- 70.

filescan c:v24 --profile=WinXPSP2x86 -fscieron.vmem filescan Volatility Foundation Volatility Framework 2.4 Offset(P) #Ptr #Hnd Access Name ------------------ ------ ------ ------ ---- <<cut>>

0x000000000245c818 1 0 R--r-d DeviceHarddiskVolume1Documents and Settings userXApplication Datamshttps.dll <<cut>> Layer 4 mshUps.dll (already deleted)

- 71.

  yarascan c:v24 --profile=WinXPSP2x86 -fscieron.vmem yarascan -p 1768 --yara-rules="MZ“ Volatility Foundation Volatility Framework 2.4 Rule: r1 Owner: Process rundll32.exe Pid 1768 0x01000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x01000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x01000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x01000030 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 ..... 0x01000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x01000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x01000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x01000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x01000080 31 fa 71 f9 75 9b 1f aa 75 9b 1f aa 75 9b 1f aa 1.q.u...u...u... 0x01000090 b6 94 10 aa 74 9b 1f aa 75 9b 1e aa 58 9b 1f aa ....t...u...X... 0x010000a0 b6 94 42 aa 7e 9b 1f aa b6 94 41 aa 74 9b 1f aa ..B.~.....A.t... 0x010000b0 b6 94 40 aa 73 9b 1f aa b6 94 45 aa 74 9b 1f aa ..@.s.....E.t... 0x010000c0 52 69 63 68 75 9b 1f aa 00 00 00 00 00 00 00 00 Richu..... 0x010000d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ........PE..L... 0x010000e0 bc 7d 10 41 00 00 00 00 00 00 00 00 e0 00 0f 01 .}.A..... 0x010000f0 0b 01 07 0a 00 14 00 00 00 6a 00 00 00 00 00 00 .....j..... rundll32.exe process

- 72.

  yarascan <<continuation>> Rule: r1 Owner: Processrundll32.exe Pid 1768 0x10000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... 0x10000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@..... 0x10000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x10000030 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 ..... 0x10000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th 0x10000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno 0x10000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS. 0x10000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... 0x10000080 2c c8 cb 2b 68 a9 a5 78 68 a9 a5 78 68 a9 a5 78 ,..+h..xh..xh..x 0x10000090 61 d1 30 78 69 a9 a5 78 4f 6f de 78 67 a9 a5 78 a.0xi..xOo.xg..x 0x100000a0 68 a9 a4 78 5b a9 a5 78 61 d1 2f 78 6c a9 a5 78 h..x[..xa./xl..x 0x100000b0 61 d1 37 78 69 a9 a5 78 76 fb 31 78 69 a9 a5 78 a.7xi..xv.1xi..x 0x100000c0 61 d1 34 78 69 a9 a5 78 52 69 63 68 68 a9 a5 78 a.4xi..xRichh..x 0x100000d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0x100000e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ........PE..L... 0x100000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 .....! Layer 4 mshUps.dll

- 73.
- 74.

  Malware As APlaWorm mainOUT- crypted-5.exe Diana-23.jpg vawtrak encrypted overlay vawtrak decrypted overlay mainOUT- crypted-5.exe compressed exe decompressed executable decompressed executable decompressed executable .rsrc sec.on payload executable (exe,dll) rundll32 process TRF#.tmp scieron explorer process shellcode TRF# .rsrc sec.on payload executable (dll) malware process scieron A B

- 75.

- 76.
- 77.
- 78.
