Splunk Insights: Investigating the 3CXDesktopApp Supply Chain Compromise

splunk.com/en_us/blog/security/splunk-insights-investigating-the-3cxdesktopapp-supply-chain-compromise.html

March 31, 2023

SECURITY





CrowdStrike announced on 3/29/2023 that an active intrusion campaign was targeting 3CX customers utilizing a legitimate, signed binary, 3CXDesktopApp (<u>CISA link</u>). As the investigations and public information came out publicly from vendors all across the spectrum, C3X customers of all sizes began investigating their fleet for signs of compromise. These campaigns are often referred to as supply chain compromises, or MITRE ATT&CK <u>T1195</u>. The most notable of these attacks which brought supply chain security to the forefront of most organizations' security posture was <u>SolarWinds</u>. A notable learning of dealing with the Solarwinds vulnerability was the difficulty associated with identifying supply chain compromises at the source. For the 3CXDesktopApp, it all began after a 7 day sleep that the compromised software version began to trigger different anti-virus products and showed suspicious behaviors in EDR products.

Organization defenders must consider attack surface comprising both endpoint and network. Utilizing our defense in depth approach, tracking anti-virus, EDR and other alerts provided can assist with piecing together the puzzle. It's not a simple task when it comes to identifying software supply chain compromises. It may all begin with a post-exploitation event and working backwards allows us to see the source.

In this Splunk blog post, we aim to equip defenders with the necessary tools and strategies to actively hunt down and counteract this campaign. Additionally, we will offer some resilient analytic ideas that can serve as a foundation for future threat detection and response efforts.

Infection Chain Walk Through

The supply chain compromise begins when users download an affected version of the 3CXDesktopApp, which subsequently loads a maliciously crafted or trojanized ffmpeg.dll. This compromised component is responsible for initiating the malicious activities associated with the attack.

Affected 3CX versions:

- 3CXDesktopApp-18.12.407.msi
- 3CXDesktopApp-18.12.416.msi

ffmpeg.dll

The patched ffmpeg.dll is responsible for reading another DLL named "d3dcompiler_47.dll," which contains an encrypted shellcode and additional DLLs that will download several .ico files. Figure 1 presents a code snippet of the maliciously crafted ffmpeg.dll that reads the "d3dcompiler_47.dll" file to search for an embedded encrypted shellcode, starting with an 8-byte sequence "0xFE 0xED 0xFA 0xCE 0xFE 0xED 0xFA 0xCE."

```
GetModuleFileNameW(0i64, Filename, 0x104u);
LOWORD(v3) = 92;
v4 = sub_1800C157C(Filename, v3) + 2;
if ( v4 )
  *(_OWORD *)(v4 + 16) = unk_18023BCCE;
  *( OWORD *)v4 = unk 18023BCBE;
                                               // d3dcompiler 47.dll
  *(_QWORD *)(v4 + 30) = 0x6C006C0064i64;
  *(_DWORD *)sub_1800CDD94() = 22;
  invalid parameter noinfo();
v0 = 0;
fh = CreateFileW(Filename, 0x80000000, 0, 0i64, 3u, 0x80u, 0i64);
if ( fh != (HANDLE)-1i64 )
  fh_1 = fh;
  v6 = 0i64;
  d3d_dll_file_size = GetFileSize(fh, 0i64);
  d3d_read_buff = (int *)mw_allocate_mem(d3d_dll_file_size);
  ReadFile(fh_1, d3d_read_buff, d3d_d1l_file_size, &NumberOfBytesRead, 0i64);
  if ( NumberOfBytesRead )
    if ( *(_WORD *)d3d_read_buff != 0x5A4D )
    sub_1800C0790(v35, (char *)d3d_read_buff + d3d_read_buff[15] + 24, 240i64);
    v9 = 8i64 * (v35[0] != 0x10B);
    v10 = *(unsigned int *)&v35[v9 + 66];
    if ( !*(_DWORD *)&v35[v9 + 66] )
    goto LABEL_29;
v11 = (char *)d3d_read_buff + *(unsigned int *)&v35[v9 + 64];
v12 = v10 - 8;
    v13 = v11 + 3;
    v6 = 0i64;
    v14 = 0i64;
    while ( v11[v14] != (char)0xFE
          || v13[v14 - 2] != (char)0xED
|| v13[v14 - 1] != (char)0xFA
          || v13[v14] != (char)0xCE )
        goto LABEL 30;
```

Figure 1

D3dcompiler_47.dll

The shellcode is encrypted using the RC4 algorithm, with a specific decryption key "3jB(2bsG#c7". Figure 2 illustrates the encrypted code block embedded in d3dcompiler_47.dll before and after the decryption process. Upon examining the decrypted portion of the screenshot, it becomes evident that the shellcode contains instructions to load another DLL.

7D 61 D9 B2 FF 5F		Υ`Ψ=Ψ`Π	Tre-ind ve Illvird vie viebnaz-indeolog of the local contrele sound working
B2 EE 5E	D5 99-70 A9 00 4E-8C 29 43 C5-F6 CB 41 6D	}arÖp- Nî)C+÷πAm	● ΦΣ♦ ╡Ι≈®xLïΦΦ╡♦ ╡XñSσHëD\$(Φ╚♦ ╡►βè┝Hï≡Φ╗♦ ╡»臺\öHëD\$00%♦ ╡3 ₨òHëD\$8Φ¥♦ Hc} <h♥²lïϥ< td=""></h♥²lïϥ<>
	5E 54-37 71 21 26-50 A1 F1 1F-C8 2C 60 B0	ε^T7α!&Pí±Ψ ^L .`∭	
EE AE DA	04 22-44 ED OF E0-07 OC E7 OP 20 7E 9E OF	04-120 10V . 5- 4) X f	
E1 05 04	04 J2-41 JU 3J J3-07 3C L7 3U-23 7L 61 31	TUESAL DUOC T	, Toak S [AITA] 0 DIV [DUCES TIENT PICELKONA[CDUDAU C#[THTFEATCONE[TTT], SUITE I, PVT
54 57 91	91 45-33 04 30 70-07 77 01 47-01 07 49 22	TwæE3 == }• w@G=•1	
CD FC A2	A2 18-6F 84 0A DB-F2 E0 25 31-C2 95 C3 D4	_= ⁿ ó↑oä⊠_≥α%1⊤ò¦⊑	8H╕ (CIà•t)IcD\$ <aoη⊉bïi bid!="" e="">BiL!LIVH∓ îv∉îv dolî îî Ha⊤0HV∥ ≓Ië¢Iâ dIâ dIâ> udi</aoη⊉bïi>
45 47 08	0B 94-9E A2 F3 B0-71 11 CC 9A-88 4D 3F F9	EGðö‰ó≤∭a∢¦ÜêM?•	
36 46 53	57 57-47 6D 58 74-75 69 48 87-68 46 62 64	6aWW9m[zu]:ckEbi	
50 R0 57	70 44 65 54 40 AF 50 DF 40 DF 00 45 60 40		
SE /0 /0	70 11-05 EA 4C AE-FB BF 48 D5-B8 IF 0C 4C	···vp=eur«v] = = vir	11Δ OFA÷€ÇT®D1Δ≽O€E1∞∞A1=A1#A1#A1#A1#A40+40♥a1@aα@uAa⊤ud≈*←∎aπ• FO8≈°∃@ ← #Ŧ♥ŦO)a⊤u⊤aru+12►O
2D F9 F1	F1 58-13 B6 91 79-73 BF 5F 4D-A4 87 99 53	-·±X‼╢æys┐_MñçOS	I≈♠ ♦t♦o∥δoAïNQLìL\$ AïHH♥₦DïHA_rà└oäÇ" _Iâ⊧(Aत@_ Hà¢oà= Eìh⊤ï_(E3└3╥Hâ╔ H♥┃ T\$8E3└Hï₦A
07 AA 72	72 2B-59 99 A6 10-E0 91 47 19-E5 C9 86 86	•¬r+YÖª⊳αæG↓σ _l råå	iê H♥⊮DïZîêà txâz¶ trDïR DïJ\$3 L♥⊮L♥⋕Eà t]Eï⊜L♥⊧3╔┴╔♪Ac┛ I └♥└ACx uфD;βt► ŀIâ⊤♦M♥=A; rਚ5
94 40 26	26 DE-1E 61 72 59-70 40 76 5D-7E 87 55 D6	öá& varYp@vlocUr	
QE A1 01	$\Delta 2 \wedge C_{-} A7 2A \otimes EP_{-} E7 \otimes EQ 1A_{-} AQ AE CE DQ$	ATTYCE T-J-9-CLL	
55 DC C	52 AC-47 24 08 JB-17 BE 10 14-A9 45 C5 D8		
ES 3C 64	DA EE-4C 8D 3F 08-03 31 FD D5-20 DD 78 DE	OKJELIPKCI F& X	FDA±C{ n@vI♦":E_2 +vE1LLLLUL vIB≥AEIA oJ€@vITCα@HAIA.0@RAIA.0@RAIA.0@RAIA*.0@RAUA
7F 7C A1	A1 93-68 40 94 5E-4C 6A 8E 8B-9A F3 0B 34	iôh@ö^LjAïU≤ð4	ම ♬▼ ♬♬ o=!j@L=!This program cannot be run in DOS mode.♪
C3 F7 B2	82 98-5F 🗖 🔪 🎧 🖓 🖓 TS S D3 F3 DA 12	leater the the the the test in t	\$ ►äJvTσ\$*Tσ\$*Tσ\$*cù'+Oσ\$*cù!+#σ\$*cù +Yσ\$*6¥ +[σ\$*6¥'+]σ\$*6¥!+pσ\$*cù%+Yσ\$*Tσ%*#σ\$*5f-
CE 03 84	RA 82-42 BA ES 66-44 30 E6 (C-D8 16 69 CD	±wè≣B∥ fñeul∔=i=	
66 CZ AL		IT WIT ALL WE OVER	
CC 84 E9	E9 65-22 F4 /B EB-25 13 D3 8C-18 C2 5C 50	faΘe" {0%‼"11⊤\P	© ♥Ç♥ .text @ð♥ ► ♀♥ ♦ '.rdata
96 40 C1	C1 19)BF E9 3()VVNI5(30)A4-01-0R48 0A	û@⊥)?σì‼o _I ≻ _Γ ⊑oH⊠	@ @.data ₅▲ ►♦ # •♥ @ ^L .pdata 0! 0♦ " ◘ ♦ @ @ RDATA
14 76 07	07 12-A1 F1 D2 57-D9 AA 79 43-BE 65 6E A3	¶v•\$íß=W ¹ =vC=enú	a a pelociía pa E a a a B
A4 90 PT	P7 00-P1 AE 2E 22-CA 02 0E 04-A7 06 6P 02	81-0=022- 94 490k8	
A4 80 87	57 69-51 41 51 52-64 65 65 64-A7 56 66 55		
DE 7E 40	4E 0A-79 EB 8D 85-07 0B IC 9F-20 0A F5 49	n~NJY01agoLf&J[1	
E3 7E E5	E5 66-CF 5B 4D D0-7F B3 BB 5A-47 A8 98 8F	π~σf≛[M≞Δ ηZG¿ÿA	D╤ Hël\$(Lĭ╬Lĭ╠HЮ\$ Hï╙HïDHâ╔╋00-@à╚┫ oHºHâ~8 ^][[[]]
5F 62 AL	AD B1-F6 4A 92 82-E9 66 97 A9-09 9B C9 0C	b;≣÷JÆéΘfù⊢o⊄r₽	┟┟┟┟┟┟┟┟┟┼┆О┫НÌ┿⋳Ŭ♥ Hà┯HoĔ┯┟┟┟┟┟┟┟┟┟┟┝╹(┛)\/\NUw(ià)A(I→)Ħ♥Rî・Hë@ĭrHâ+Ō0^*@÷Het♪ ↑ Hi≢0Ōo
72 48 54	54 E3-C8 70 E0 D0-91 6B 99 54-65 D4 ED 95	rH7< Ing #akÖTe -do	
AE CA DE	DP 19 EE 76 CC PE 2E 7P A1 EE 0D 67 0C A2		TREAT AN REAL STREAM AND STREAMS AND A TREAT AND REAL AND
05 C4 DE	JB 18-FE 70 CC BE-23 76 AI ES-90 07 9C 05		ul-ultulaos≜ om ultulaosemo (@ ultx::▲ ustuluus. [lkkkk@pusw ul.ultulaos≜ om ultousouru
48 89 Dz	JZ /A-6D /6 5B 1E-E0 C/ 58 95-69 28 9B E3	Heπzmv[▲α∥Xo1(¢π	╒╒╒╔╫┪∞(H1,50♥ 0₽;00 ╔╒╔╔╔╔╔╔╔╔╔╔╔╔╔╔╔╝╝╝╝╝╝╝╝╝╝╝
71 D1 54	54 77-46 6E 40 04-0A 7A A2 91-47 4D 2F BE	q⊤TwFn@ ◆ ≣zóæGM/-	Ì\$▶⊕╓D*⊥AÇ└0Eê⊜Lï⊤Hà╥u╓HÌD\$ELë‼LëS▶H╟C↑◦ Dê‼L;╙t‼LÌD\$EIï〒M+┴Hï╥Фº\$ Hï├HïL\$HH3╟Ф╢♀⊚ Hâ-P[
3F ØB BØ	B6 A4-D6 EE E4 7C-6C BB B1 72-D4 78 9C ED	?ð ñ rεΣ 1╗≣r ⊑x£φ	ŀŀŀŀŀłâ∞(Hâ⊥ Hĭ© PŪÉHâ−(ŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀŀO\\$↑UVWATAUAVAWHÌl\$JHü∞└ Hĭ♣J∩♥ H3−HëE\$Hĭ≿Lĭ±HëM∩E
18 53 3/	34 F7-64 94 48 17-80 90 3C 68-81 AF 48 88	+S:TIUK\$CEChEqui	
EE SD-CO	CA 60 20 D7 AE 40 A2 DP 10 DA 22 AC D4 32	us higher of soll	
55 80 00	CO 05-80 D7 0F A9-02 DB 1D 80-88 0C 84 28		Demonic⊈t, -tjttzunt=iltninowt# Eli∞Phi Ohl+1+ Ha Poet@ Ha~TPNVHIBLeem¢LeemuLem∱nigP
D3 47 58	58 0E-B7 1D 00 C7-ED 9F 45 F0-66 AF 23 98	"GX#¶⇔ ∥ΦქE≡+»#ŷ	²ôŸϡ≕ H;┿HoB┿Hï┳Hà┿@H∥⊦ HoB¤Hù ► r,HiA H;∸oà © Hĭ⊑O2ď© Hà∟oä!© Hìx HàταHëG°ó¢Hà╓t≋
	01 33-C8 10 15 C0-74 B6 EF 36-71 92 C7 06	në@3 ╚►§ Lt n6aÆ ♠	₽û♥ ο⊲∙HìO⊨MïlHï⊯O♠ø@ B⊨♦'A∋@ HìSzû♥ HìMcO⊯# ο► o⊲E≈o►H►o⊲M∙Lëh►H¦M≏o ⊨ LìM»LìE≈HìM≟
6E 89 01			at a transfer the transfer to a transfer to
6E 89 01 71 1D 19	15 82-0D 92 0C 5E-C0 28 81 CB-F <u>9 16 58 1B</u>	q⇔§é♪Æ♀^└(ü च · = X←	Mē,Mēn⊧Mēnîo⊳ Ao⊲¢osH⊳Ao⊲N⊳Lēh⊳H∭@îo ⊨ HiUtHâ•⊳r1H ⊤HiM≟Hi⊣Hü-⊳ <u>rthâ⊤'Hi⊺°H∔-Hât°Ha°⊤o</u>
6E 89 01 71 1D 19 72 0F B4	15 82-0D 92 0C 5E-C0 28 81 CB-F9 16 58 1B 84 D9-CF BE 47 3C-D3 43 CC 14-F9 BE C9 7C	q⇔§é»Æ♀^└(üच+¯X↔	Mē.Mēn⊳Mēnto⊳ Ao∢ao⊳H⊳Ao∢N⊳Lēh⊳H∭@to ¦ HĭUtHā.⊳riH ⊣HĭM≟Hĭ⊥Hū. ⊳ riHā⊤'HĭI°H;∔HāloHā°vo Nokā.⊳riH ⊣HĭMeHi→Hī. ⊳ riHā-'HīTOH,↓HāloHā°vor≛ nomen frīHfHā.⊳riH ⊣HīMcHīJuG. > riHā-'
6E 89 01 71 1D 19 72 0F B4	15 82-0D 92 0C 5E-C0 28 81 CB-F9 16 58 1B 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C 66 63 66 06 06 07 D1 55 14 55 74 63 D8 64 54	q⇔§é)ÆŶ^└(üच·¯X← ro¦┘╬┐G<╙С╠┚α┐╔╎	Мё.Мёп⊳Мёпто⊳ Ао≪о⊳ннАо≪№ Lёрьн∥@1о НІОСНа́ >r1H тнім∔ні́нО· > r0Haт 'HII°н+4halonaðvro UoHa`>r2H тнімні́нП· > riHa⊤'HII°н+4halonaðvro£ Фожд ÉNIOfHa`>r1H тнімскі́нЦі > riHaт Sulfra
6E 89 01 71 1D 19 72 0F B4 0B BD F6	15 82-0D 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C F6 63-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA	q↔§éλ£♀ ^Λ ^L (ü _∓ ·−X _← ro⊣J ₁ G< ^L C⊮9α ₁ _F ð ^{II} ÷cµû+∓^→∩t 9 ∓Ω·	Më.Mën⊁Mënto≽ Ao≪Ao≽H⊭Ao≪N⊭Lën⊭H∥@to ¦ HIUtHâ·≽r1H ⊤HIM≟HI⊥HU· ≽ rHhâ⊤'HII°H+≟Hà ^l o _H â°¥o UoHâ·≽r2H ⊤HIM≈HI≟HU· ≽ rJHâ⊤'HII°H+≟Hà ^l o _H â°¥oç≜ ©o⊠0 ÉHIUfHâ·≽r1H ⊤HIM¢HI≟HU· ≽ rJHâ⊤' mùH∥Ēfo ¦Eç HIU[Hâ·⊧r-H ┭HIM»HI≟HU· ≽ r§Hâ⊤'HII°H+≟Hà ^l oHâ°¥w/Qîc@ II∱HIMIH3∳Q!o© HIES≽©
6E 89 01 71 1D 19 72 0F 84 0B 8D F6 77 11 81	15 82-0D 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C F6 63-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 7B 23 D9-11 0F CF 88	q⇔§éλ£ ^{Ω∧⊥} (ü∓ -X↔ ro ┘⋕₁G <lcŀĵα₁ϝ ϭ^{IJ}÷cµû†╤^→∩t0∓Ω w≪፪Σ₁²±∕Σ{#┘⊲ο±ê</lcŀĵα₁ϝ 	Mē.Mēn⊳Mēnto> Ao≪ooshi>Ao≪osh
6E 89 01 71 1D 19 72 0F 84 0B BD F6 77 11 81 91 4C F4	15 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 4 09-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C F6 63-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 78 23 D9-11 0F CF 88 4 9E-C6 3F FE DD-A8 70 63 92-84 <u>55 3A 08</u>	q⇔§éλÆ ^{Q∧ L} (ü╤·−X↔ ro┥┘⋕┐G< ^{IL} C╠ឭα┐╔│ ϭ ^{IJ} ÷cµû┼╤^→∩t פ ┼Ω· ₩⋖⋚Σ╕ ² ±/Σ{#┘⊲ο≟ê æL[ℝ⊧? Ⅲ %pcÆ <u>]U:</u> □	Мё.Мёл⊳Мёлто⊳ Ао-«ФоннАо-«№ Lёһ»Н∥ёто ¦ HIUthâ·⊳riн тнім∔нічно· > rihâ†'нĭi°н+-hâ ^l «hā°то Uohâ·⊳r2н тнім≈нічно· > rihâ†'нĭi°н+- [⊥] нâ ^l «hā°тос [≟] Фона ÉнïUfhâ·riн тнімсніїню· > rihâ† mùн∥Еfo }Ec ніш[на•⊳r-н тнімэнічно· > r§hâ†'нĭi°н+-há'«hā°ти/Фона) V Édy- Édy-ve Édy-ve Édy-ve konstatistania Hi-HiSOVV нед ĭ thion¥ra/Cose + dvi #kb#kb+hkvsuvkavahils=ню=> ні€°V начеблізмісна нед ĭ се s(LeisenHoSao Dèls(Eiddhi
6E 89 01 71 1D 19 72 0F 84 08 8D F6 77 11 81 91 4C F4 E8 FD 19	LS 82-0D 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C 66 32-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 7B 23 D9-11 0F CF 88 F4 9E-C6 3F FE DD-AB 70 63 92-E4 55 3A 08 19 8A-A2 96 DF 84-E7 CF 31 09-DD_66 2D 18.	$\begin{array}{l} q \mapsto \underbrace{ \int G M E Q^{-L} \left(\bigcup_{q \to -}^{-1} X_{+} \\ r \circ \downarrow^{-1} \downarrow_{q \to -}^{-1} G \in \underbrace{ I \cap J}_{q \to -} \left[f \cap J \right] \\ d^{-1} + c \mu \widehat{u} \downarrow_{q \to -}^{-1} \circ h \circ f = \underbrace{ \int G M I \cap J}_{q \to -} \left[f \cap J \right] \\ w = \underbrace{ \int G I \cap J}_{q \to -} \left[X_{p \in \mathcal{L}}^{-1} \cup I \cap G \right] \\ a \in \underbrace{ \int G I \cap J}_{q \to -} \left[X_{p \in \mathcal{L}}^{-1} \cup I \cap G \right] \\ g^{-1} \to \widehat{G} \cap G \\ g^{-1} \to \widehat{G} \cap G \right] = \underbrace{ \int G I \cap J}_{q \to -} \left[f \cap G \cap G \right] \\ \end{array}$	Mē.Mēn⊳Mēnto> Ao≪ooshi>Ao≪oshi>Ao <ao≪oshi>Ao≪oshi>Ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao≪oshi>Ao<ao≪oshi>Ao<ao>Ao≪oshi>Ao Ao Ao≪oshi>Ao Ao Ao≪oshi>Ao Ao Ao≪oshi>Ao Ao Ao≪oshi>Ao Ao Ao≪oshi Ao Ao</ao></ao≪oshi></ao≪oshi></ao≪oshi></ao≪oshi></ao≪oshi></ao≪oshi></ao≪oshi>
6E 89 01 71 1D 19 72 0F 84 0B 8D F6 77 11 81 91 4C F4 E8 FD 19 98 91 40	15 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C F6 63-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 78 23 D9-11 0F CF 88 49 5E-C6 3F EF DD-A8 76 63 92-84 55 3A 08 19 8A-A2 96 DF 84-E7 CF 31 09-DD 66 2D 18 18 18-80 06 26 CF1 47 D2 64 20 51 09 C8	q+§€) € 2 · L (U∓ · − X + ro - J + G · L (U∓ · − X + ro - J + G · L (F ga r r) d + c µ u + n t ⊕ + Ω · w = ∑ z + 2 × (H J = o + E at [H + ? =) × p C +] U : 0 ² J è ô û = at - 1 o f - 1 y = - L = - 0 h	Mē.Mēn⊳Mēnto Ao≪oshi Ao≪N⊳LEh⊳H∥@to ¦ HIUtHâ·⊳riH ┬HIM≜HI≟HU·> rēHāŢ HII°H+≟Hā ^L ºHā°vo UoHā·⊳r2H ┬HIM=HIŢHU·> rəHāŢ HII°H+≟Hā ^L ºHā°vocā OsBO ÉHIU∱Hā·RIH ┬HIM€HIŢHU·> rəHāŢ mùH∥Efo ¦Ec HIU Hā·⊳r-H ┬HIM>HI⊐HU·> r§HāŢ HII°H+≟Hā ^L ºHā°w/OiOs II ĦHIMEHI\$[0]co HIE\$⇒ V ÉO! - ĔO/ve ĔO/Ve Eo/Ve Eh¥Heis]¶HEIS]HEIS>NH⤠HI·HIN°H+≟Hā ^L ♡Hā°W/OiOs II ĦHIMEHI\$[0]co HIE\$⇒ V ÉO! - ĔO/ve ĔO/Ve Eo/Ve FHEIS] ↓↓↓↓↓↓ ↓↓↓↓↓↓↓↓ ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
6E 89 01 71 1D 19 72 0F 84 0B 8D F6 77 11 81 91 4C F4 E8 FD 19 98 91 4F	LS 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C 66 33-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-88 FD F1 2F-E4 7E 23 D9-11 0F CF 88 F4 9E-C6 3F FE DD-AB 70 63 92-B4 55 3A 08 98 8A-A2 96 DF 84-E7 CF 31 09-DD 66 2D 18 AF 18-80 D0 03 CB-11 4C 03 FA-2A 51 99 C8	$\begin{array}{l} q + \oint \hat{e}^{\lambda} \hat{E} \hat{O}^{-L} (\ddot{u}_{\overline{q}} \cdot \underline{\neg} X_{+} \\ rol^{-1} \frac{1}{4} + G < \frac{1}{4} C \frac{1}{4} \frac{1}{9} q_{-1} \frac{1}{6} \\ d^{-1} + c_{1} \hat{u}^{+1} \frac{1}{7} + o_{1} + \hat{O} \frac{1}{4} \hat{e} \\ w < \sum_{n} \frac{1}{2} + \sum_{n} \frac{1}{2} \sum_{n} \frac{1}{2} \sum_{n} \frac{1}{2} \frac{1}{2$	Мё.МёльМёлто» Ао «орын» Ао «№ Lёльн∥@то ; НІЦтна » riн тнімніціно: » riнат нітеньна бала « Осна » r2н тнімніціно: » riнат нітеньна бала бала бала бала бала бала парада. Пойщето ; рес ніціна » r:н тнімніци: » riнат нітеньна бала бала бала бала бала бала бала ба
6E 89 02 71 1D 19 72 0F B4 0B BD F6 77 11 B3 91 4C F4 F8 FD 19 98 91 AF 04 90 48	15 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C C2 14 EC 76 72 E6 95 C1 -5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 78 23 D9-11 0F CF 88 84 9E-C6 FE D0-A8 76 39 2-84 53 A0 81 84-82 A0 62 20 18 A1 85 A0 84 A1 46 76 39 2-84 53 A0 84 A1 46 47 47 47 48 47 A1 46 47 47 47 48 47 48 47 47 47 47 47 47 47 47 47 47 47 48 47	q+§63£Q^L(U; -×+ rolign; -x+ discuting; -x+ discut	Mē.MēneMēntos Ao depēheAo delēhetķēto t Hītutā enin turktutu. Mikā turitā vaida turktu vaida tu
6E 89 01 71 1D 19 72 0F B4 0B BD F6 77 11 B1 91 4C F4 E8 FD 19 98 91 AF 04 90 48 27 3B 96	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{l} q+ \S \hat{e} J \hat{k} \hat{O}^{-L} (\ddot{u}_{\overline{T}} \cdot \underline{x} \times n \hat{v}_{\overline{T}}) \\ \pi \hat{v}_{\overline{T}} \hat{o} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{o} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{\sigma}^{J} + c \hat{u} \hat{u}_{\overline{T}} + \hat{\sigma} + \hat{\sigma} \hat{\sigma} \hat{v}_{\overline{T}} \\ \hat{\sigma}^{J} + c \hat{u} \hat{u}_{\overline{T}} + \hat{\sigma} + \hat{\sigma} \hat{v}_{\overline{T}} \\ \hat{\sigma}^{L} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} + \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{\sigma}^{L} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{\sigma}^{J} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{\sigma} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \hat{v}_{\overline{T}} \\ \hat{v}_{\overline{T}} $	Mē.Mēn⊳Mēnto> Ao «bobh»Ao «beh»Ao «beh»H@to ¦ Hīuthā » riн тнімніціни: » rihāţ 'Hītoн∔ Hā ¹ ohā°qo Uohā » r2н тнімніціни: » rihāţ 'Hītoh+uhā'ehā°qočā Oosē Einidfa » rih тнімсніци: » rihāţ Mēlļēfo Ec Hīulhā » r.н тнімніци: » Gihāţ 'Hītoh+uhā'ehā°qožotā Oosē Einidfa » rihāţ thi thistalādo e Hītāse V Edd. Edd.e Edd.e Edwave Hitagrav Hāther vitinistani remtes Ea Lejš(Lejškh [Džāo Dēlš(Eiddh) #######Heiseuvavavahils=huwe Hitagrav Hāther vitinistani remtes Lejš(Lejškh [Džāo Dēlš(Eiddh) #######Heiseuvavavathils=huwe Hitagrav Hāther vitinistani remtes Lejš(Lejškh [Džāo Dēlš(Eiddh) #######Heiseuth@teiseuth@to DēlsHitadi o otaţ remtes Hod Mitagrav H]@to Dēls(Eiddh) Lējaco odEboheodth[Ešveth@to DēlsHitadi oto odţ romtes Hod Mitagrava H]@to Dēls(Eiddh) Hīthu: » rihāţ 'Hītoh+uhā'ehā°vo;?@ Oīto Lej#H[Edo]E Hītāš Hātohar Hītoh+itadi "Hātoharib" Hitashitadi vitinistani vermi Lējšxh [Dš] o Još Hītu Hātohar viti mitatu Hātu vitini vermi Hātohar Vitis Hātohar vitis Hatohar Hitashitadi vermi Hīthu: » rihāţ 'Hītu Hātohar viti mitatu +hītohar Hītashitadi "Hātoharib" (Hātoharib vitis Hatoharib)
6E 89 01 71 1D 19 72 0F B4 0B BD F6 77 11 B3 91 4C F4 88 FD 19 98 91 4R 04 90 48 27 3B 96 96 0B D7	15 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 09-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C F6 63-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 7B 23 D9-11 0F CF 88 49 9E-C6 3F FE DD-AB 70 63 92-84 55 3A 08 19 8A-A2 96 DF 84-E7 CF 31 09-DD 66 2D 18 AF 18-80 D0 03 CB-11 4C D3 FA-2A 51 99 C8 48 8D-28 7F FE 02-26 5B 00 60-4A 12 57 82 36 5F-75 F3 48 98-56 17 4A 40-03 A1 93 50 70 3-88 FD 35 E4 10 10 1A 2F D-D1 35 2C 4D	$\begin{array}{l} q+\xi \hat{e} + \xi \hat{e} - \chi \hat{e} - \tilde{\chi} \hat{e} \\ rol \frac{1}{4} + (q + \zeta \hat{e} + \eta q - \eta) \\ d^{1} \pm (\mu \hat{e} + \gamma - n + \hat{e} + \hat{e}) \\ d^{1} \pm (\mu \hat{e} + \gamma - n + \hat{e} + \hat{e}) \\ d^{1} \pm (\mu \hat{e} + \gamma - n + \hat{e} + \hat{e}) \\ q^{2} + \hat{e} \hat{o} \hat{d} + \hat{e} + 1 - q \\ d^{2} + \hat{e} \hat{o} \hat{d} + \hat{e} + 1 - q \\ g^{2} + \hat{e} \hat{o} \hat{d} + \hat{e} + 1 - q \\ g^{2} + \hat{e} \hat{e} + \hat{e} + 1 - q \\ g^{2} + \hat{e} \hat{e} + \hat{e} + 1 \\ (z = \eta \hat{e} \hat{e} + 1 - q \\ \hat{e} \hat{e} + \hat{e} + 1 \\ (z = \eta \hat{e} \hat{e} + 2 - \hat{e} + 2 - \hat{e} \\ \hat{e} \hat{e} + \hat{e} + 1 \\ (z = \eta \hat{e} - \hat{e} - \hat{e} + 2 - \hat{e} \\ \hat{e} \hat{e} + \hat{e} + 1 \\ (z = \eta \hat{e} - \hat{e} - \hat{e} - \hat{e} - \hat{e} \\ \hat{e} \hat{e} + 1 \\ \hat{e} - \hat{e} + 1 \\ \hat{e} - \hat{e} - \hat{e} - \hat{e} \\ \hat{e} + 1 \\ \hat{e} - \hat{e} - \hat{e} - \hat{e} \\ $	Mě.Men+Mento- Aosto-H>Aosto-H>Heh+H@to ½ HIUtHà >riH HHHHHHHU. > NHAT HITHL+HA ¹ CHà°to UoHà-r2H HIMHHT+HU. > rHHTHHHHHHHHH MUHEfo EC HIUHA-rFH HIMHHHHHH FNHA V EQI EC HIUHA-rFH HIMHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
6E 89 01 71 1D 19 72 0F B4 0B BD F0 91 4C F4 68 FD 19 94 4C F4 98 91 AF 04 90 48 27 3B 96 06 0B D7 91 3C 70	15 82-00 92 0C 5EC0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C 66 3-E6 96 C5 D1-5E 1A F7 4-20 D8 EA FA 81 E4-B8 FD F1 2F-E4 7B 23 D9-11 0F F8 94 9E-C6 3F FE DD-AB 70 63 92-B4 55 A 88 94 8A-A2 96 DF 84-E7 CF 31 09-D0 66 2D 18 AF 18-80 D0 03 CB-11 40 D3 FA-2A 51 90 68 2D-12 57 82 48 BD-28 7F FE 02-26 58 06 60-4A 12 57 782 <	4+66/λ0 ² · [² (µ ₁ - ×. rol ⁻¹ ⁴ η ₁ G ⁻¹ C ¹ β ⁻¹ σ ⁻¹ δ ⁻¹ w ⁻¹ ² δ ⁻¹ C ¹ β ⁻¹ σ ⁻¹ δ ⁻¹ δ ⁻¹ w ⁻¹ δ ⁻² δ ⁻¹	Mē.Mēn⊳Mēnto> Ao dobeh⊳Ao dobehe Ao dobehe Ao dobe kar hituthā > rih thim hituthu > rihāt 'hitohi ha do dobehe Uohā - r2h thim hitut > rihāt 'hitohi + do dobe kar dobe kiu Ufhā > rih thim hitut > rihāt mullēto te chiu ha - rih thim hitutu > rihāt 'hitohi > rihāt 'hitohi + ha e dobe kiu Ufhā > rihāt thim ha lobe hits V ēdd. Ēd/o Ēd/o Ēd/o Ēd/o Ēd/hē kiesekatseka V ēdd. Ēd/o Ēd/o Ēd/o Ēd/hē kiesekatsekata Hateigati S(hitika) vē Eigdhigov hitohi o oterohio da teken kar dobe beisteli (Eigdhi hiteise o de boeho dod kiesekata (Hateise o teroho da teken kar dobe beisteli (Eigdhi hiteise) vē Eigdhigov die versat thim a sa dobe beisteli teken kar dobe beisteli (Eigdhi hiteise) vē boeho dod kar dobe beisteli teken kar dobe beisteli (Eigdhi hiteise) vē boeho dod kar dobe beisteli teken kar dobe beisteli (Eigdhi hiteise) vē boeho dod kar dobe beisteli (Hateise) teken kar dobe beisteli (Eigdhi hiteise) vē boeho dod kar dobe beisteli (Hateise) teken kar dobe beisteli (Hateise) hiteise ba de boeho dod kar dobe beisteli (Hateise) hiteise ba de ba d
6E 89 01 71 1D 19 72 0F 84 0B BD F0 91 4C F4 88 FD 19 98 91 AB 04 90 48 27 3B 96 06 08 D7 91 36 70	15 82-00 92 0C 5E-C0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 33 CC 14-E0 BF C9 7C 66 3-E6 96 C5 D1-5E 1A EF 74-02 D8 EA FA 81 E4-B8 FD F1 2F-E4 78 23 D9-11 0F F8 84 9E-C6 FE DP-AB 76 32 2-84 55 A0 88 19 8A-A2 96 F8 AE 76 32 2-84 55 A0 84 4F 18-80 06 03 CB-11 4C D3 FA 26 57 78 28 92 68 44 15 77 28 45 76 68-44 12 57 82 46 67 76 78 28 76	α++662,80 ^ L(μ ₁ ×,- σ ¹¹ 4 ₁ G < ¹ C(¹)G α ₁ μ ₁ σ ¹¹ 4 ₁ G < ¹ C(¹)G α ₁ μ ₁ w ≤ Σ ₁ 3 ₂ /Σ(π ¹ + α-bē α ¹ k ₂)Ω(π ¹)G c ² (1) 3 ¹ 0 ² 1b60 ¹ 8π ¹ d0 f f f y ₂ w ₂ -C ¹ V ₂ = (1, - Q)L +6H ¹ (αm⊗2(1) 3 ¹ U(2) ×6H ² (2) (1) 3 ² U(2) ×6	Ma.Man-Manto- Aosto-HeAosto-HeAosto-HeAosto-Léh-H∥@to ¦ HIUtHá-riH HHAHIHHU. > rUHát'HIIHH. > rUHát'HIIHH UoHá-r2H HIMHHIHU. > rUHát HIIPH-HAOsto-Léndrock Goese ÉriufHa-reht HIMHHIHU. > rUHát'HIIPH-HAÍta-Hárock Osto-Léolve Éolve Éolve Éolve Éblen: The Shat'HIIPH-Hát'Hát'HAÍta-Hárok Goese V Éol - Éolve Éolve Éolve Éblen: Hite's HAIHEITHIN HINHEITHIN E Leiste HIGto Distriction (Elevent HIEFS) - Statistic (Elevent) Éblen: The Shat'HIIPH-Hát'Hát'HAÍta-Hárok Goese V Éol - Éolve Éolve Éblen: Hite's HAIHEITHINHEITHIN HANES Leiste (Elesthi HIFEIGHITS(HILShojv ÉElechiste) Hite's HAIHEITHINHEITHINHEITHINHEITE LEISte (Elevent) HIFEIGHITS(HILShojv ÉElechiste) HITE's HAIHEITHINHEITHINHEITHIS HAI+SUS – OSTO-HOSTIN HIFEIGHITS(HILShojv Éblen: Haiheithin Haiheithin HITSHAIHEITHINHEITHINHEITHINHEITHINHEITHINHEITHINHEITHINHEITHIN HIFEIGHITS(HILShojv Éblen: Haiheithin Haiheithin HISHAIHEITHINHEITH
6E 89 01 71 1D 19 72 0F B4 0B BC 11 77 11 83 91 4C F4 E8 FD 19 98 91 AR 04 90 48 27 3B 96 06 0B D2 91 36 70 65 55 89	15 82-00 92 0C 5EC0 28 81 CB-F9 16 58 18 84 D9-CE BF 47 3C-D3 43 CC 14-E0 BF C9 7C 66 3-E6 96 C5 D1-5E 1A F7 4-20 D8 EA FA 81 E4-B8 FD <f1< td=""> 2F-E4 7B 23 D9-11 0F F 88 19 8A-A2 96 DF 84-E7 CF 31 09-D0 66 2D 18 48 B0-28 7F FE 02-C5 58 06 64-4A 12 77 82 96 5F-75 F3 48 98-56 17 4A 04-03 A1 93 50 70 63-88 F7 D3 88-11 11 A2 FD-D1 35 2C 70 63-88 C7 C3</f1<>	α+66/λξ0^L(μ=-X, rol-1 μ= C L(μ=α) μ= α1 ε μμ=η-η-η-τα-μ= w= Σz= 1 ± / Σ (μ= 4 ∞ hē zL [h=γ= X pc.k=(1-1) φ= Σz= 2 ± / Σ (μ= 4 ∞ hē zL [h=γ= X pc.k=(1-2) φ= 2 ± δ c 0 = 2 ± c 0	Mě.Měn⊳Měnto» Ao «bochh Ao «bochh Ad «bochh Higto ; HIUthá • rih thinkhiku v rihát tiru + thiato há ° mo Uoha • r2H thinkhiku • rih thinkhiku • rškát tiru + thiato ka ° mo Billefo ; Ec HiUthá • r.H thinkhiku • rškát tiru + thiato ka ° mo V čel • čel • čel • čel • ve čel • ve čel • ka thiato ka ° mo V čel • čel • čel • ve čel • ve čel • ka thiato ka ° mo Hitei • Mathikato v tiru • ka * mo Hitei • Mathikato v tiru • mo Hitei • mo
6E 89 01 71 1D 19 72 0F B4 0B BD FC 91 4C F4 E8 FD 19 94 90 48 07 3B 96 06 08 07 91 3C 70 91 3C 70 66 68 07 91 3C 70 67 5E 89 06 08 07 67 5E 89 06 06 07	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	α++66+X0^+(jψ-=×. ¬σ+1-β+G< ¹ -C(μ)ση μ α+-C(μ)ση μ α+-C(μ)ση μ α+-C(μ)ση μ σ+2+60-β α+-C(μ)ση μ σ+2+60-βα-1-(μ)ση μ σ+2+0-β α+-C(μ)ση μ σ+2+-C(μ)ση μ σ+2+-C(μ)ση μ σ+2+-C(μ)ση μ σ+2+-C(μ)ση μ σ+2+-C(μ)ση μ σ+2+	Mě.Men+Mento- Aosto-H=Aosto-H=Aosto-Helosto UoHa-r2H +HIMHHI-HU. ► rUHA; HITOH+UHA ^C HA ^O YOC ^A Oose ÉHIUHA: ► rUHA; HITOH+ ^L HA ^L CHA ^O YOC UOHA-r2H +HIMHI ^L HU. ► rUHA; HITOH+ ^L HA ^L CHA ^O YOC ^A Oose ÉHIUHA: ► rUHA; HITOH- ^L HA ^L CHA ^O YOC UOHA-r2H +HIMHI ^L HU. ► rUHA; HITOH+ ^L HA ^L CHA ^O YOC ^A Oose ÉHIUHA: ► rUHA; HITOH- ^L HA ^L CHA ^O YOC V ÉQI. ÉQI. ÉQI. EQI. VE ÉQI. VE ÉQI. EXPERIENTENTION HIEGHITS(HILSNOJV ÉEIGHIS; EN LE HILOH) EN LE CONTRACTURE LE SCHEVENTE HI ^L EIGHITS(HILSNOJV ÉEIGHIS; EN LE CONTRACTURE LE SCHEVENTE, LE SCHEVENTE, EN LUHA + FILH + INTENTI-HILO + FILHA LE SCHEVENTE, EN LE SCHEVENTE, EN LUHA + FILH + INTENTI-HILO + FILHA LE SCHEVENTE, EN LE SCHEVENTE, EN LUHA + FILHA, HITOH-HILO + FILHA LE SCHEVENTE, EN LE SCHEVENTE, EN LUHA + FILHA, HITOH-HILO + FILHA LE SCHEVENTE, EN LE SCHEVENTE, EN LUHA + FILHA, HITOH-HILO + FILHA LE SCHEVENTE, EN LI HIGTH-HITOH-HILOHA E HITOHY HE SCHEVENTE, EN LUHA + FILHA, HITOH-HILO + FILHA E HITOHY HE SCHEVENTE, EN LUHA + FILHA, HITOH-HILOHA, HITOH-HILOHA, HITOH-HILOHA, HITOH-HILOHA, HITOH-HILOHA, HITOH-HILOHA, HITOH-HILOHA, HITOHA-HILOHA, HITOHA-HILOHA, HITOHA-HILOHA, HITOHA-HILOHA, HIT

Figure 2

Decrypted-DLL

The shellcode proceeds to load the decrypted DLL export "DIIGetClassObject," which initiates a thread to examine the manifest file. It then sleeps for a duration based on a randomly generated value relative to the system date and time. Following this, it reads the machine GUID from the registry. Figure 3 demonstrates how the shellcode accesses the <u>Cryptography</u> registry to parse the MachineGUID of the targeted or compromised host.



Figure 3

Upon retrieving the Machine GUID, the shellcode calls a function that attempts to download several .ico files from the GitHub repository. At the time of writing, the URL link was no longer accessible, but the <u>cybersecurity community</u> shared the files, enabling us to examine the next stage.

Figure 4 presents a code snippet of the decrypted DLL that attempts to download multiple .ico files for decoding and decryption. The code highlights an intriguing approach employed by the attacker, using .ico files as configuration files. After downloading the .ico files, the shellcode reads them byte by byte, searching for the character "\$". This character serves as a marker for the encoded and encrypted <u>C2</u> URL link.



Figure 4

Figure 5 presents a basic hex view snippet of two malicious .ico files that the decrypted DLL attempts to download. The hex bytes highlighted in the yellow box represent the base64-encoded and encrypted C2 URL link, which begins with the "\$" character. We recommend using the <u>decrypt-ico.py</u> script created by the Volexity team to automatically decrypt this string. The decrypted C2 server can be found in the IOC section of this blog.

00002800:	D5 5	F 03	6D-D2	FE	2C 5	SC-FD	ED 9	8 07	-BC	CE 0)F	09	Ē ♥Μ┰∎,∖²	¢ÿ∙⊒⋕₀o					
00002810:	7C F	2 D8	24-A5	5A	C4 F	-4-5E	40 0	2 9F	-1D	6C E	8	02	≥+\$Ñz-[^	@⊖f⇔l _∃ ⊖					
00002820:	09 6	C 2C	FE-3F	13	CA 6	55-48	81 E	1 ED)-6A	00 e	0	00	ol,∎?‼ [⊥] eH	üßφj					
00002830:	00 4	9 45	4E-44	AE	42 6	50-82	24 4	B 51	-41	41 4	1	4D	IEND«B é	\$KQAAAM					
00002840:	43 5	A 55	37-36		45 4	19-44	7A 5	2 59	-69	45 4		2B	CZU76iEID	zRYiEO+					
00002850:	64 3	7 71	75-2B	6B	77 5	51-57	7A 6	8 61	-36	73 7	8	51	d7qu+kwQW	lzha6sxQ					
00002860:	72 7	4 7A	46-6F	33	6F 5	50-53	65 6	B 4D)-34	71 3	0	57	rtzFo3oPS	ekM4q0W					
00002870:	75 3	4 36	73-4B	71	76 3	31-71	2B 4	7 63	-68	6D 6	iΑ ·	47	u46sKqv1q	+GchmjG					
00002880:	30 4	8 47	2F-66	6C	34 3	31-4F	69 6	7 61	-61	6C 3	6	38	0HG/fl410	igaal68					
00002890:	41 4	8 72	4B-38	31	36 6	5C-2F		A 76	5-5A	2F 7	'3	78	AHrK8161/	izvZ/sx					
000028A0:	52 <u>3</u>	<u>3</u> 6E	68-42	51	61 6	54-52	4A 7	9 68	3-48	6E 3	2	51	R <u>3</u> nhBQadR	JyhHn2Q					
000028B0:	BD 3	D																	
1Help 2Pu	itBlk	3Edi	t <mark>4</mark> M	ode	5 G	ioto	6 <mark>Da</mark>	tRef	7 Se	arch	8	Head	der <mark>9</mark> Files	10Quit	11Hem	12Name	s 📕		
00006CF1:	ØF B	8 DF	F1-9D	78	BF 7	7B-8F	69 E	E 30)-27	BB F	F	C1	os∎±¥xa{Â	iε='π ⊥					
00006D01:	FF 9	A EØ	FE-2F	D7	E0 3	3B-74	74 C	0 35	5-8E	74 C)7	7D	Üα∎/-la:t	t ^L 5Ät+}					
00006D11:	AF 1	B 87	EF-E0	C1	4E F	-6-1D	FD 4	E CE	E-FE	50 3	3A	FD	»←c∩α [⊥] N÷€	² N=P 2					
00006D21:	77 7	9 0D	D5-4A	1E	0C 9	90-C1	40 F	1 C1	-12	68 8	31	C0	wyĴ≓J≰QÉ	-@± [⊥] ≎hü∟					
00006D31:	F1 C	D 07	DØ-BD	83	6C 4	44-80	8D 1	.c c2	2-FC	9F 6)D	FE	±≟•∭âlDQ	ĭ∟⊤"f⊅∎					
00006D41:	3B D	F 81	83-9D	18	68 F	E-F5	04 5	E 68	3-E0	18 8	36	0D	;■üâ¥↑h∎	♦^kaîå♪					
00006D51:	61 7	F DØ	0E-FE	7D	BF 8	36-8A	8A (1 93	3-39	D4 2	24	BF	ao [⊥] /∎}⊤åè	è [⊥] ô9 ⊑\$⊤					
00006D61:	13 A	8 7E	9B-FD	A6	F7 1	IA-FC	FF F	F CF	-44	ED F		BF	ll ¿~¢²ª≈→r	±Dφ η					
00006D71:	EE C	0 5E	.EE-03	87	RF 3	39-A1	60 B	7 EA	-30	<u>66 (</u>	90	00	_∎L^ ♥c¬9i		-				
00006D81:	00 4	9 45	4E-44	AE	42 6	50-82	24 4	B 51	-41	41 4	11	4B	IEND«B`é	\$KQAAAK					
00006D91:	57 2	B 64	54-6A	63	44 3	31-44	4C 7	0 65	5-64	33 6	51	41	g+dTjcD1D	Lped3aA					
00006DA1:	55 3	8 43	6F-4F		77 5	51-57	7A 6	8 61	L-36	73 7	78	51	e8CoOkwQk	lzha6sxQ					
00006DB1:	72 7	4 7A	46-6F	33		50-53		9 73	3-34	75 3	30	57	rtzFo3oPS	eis4u0W					
00006DC1:	2B 3	4 73	4D-4C	32	76 3	30-75	2B 4	1 40)-67	76 6	5A	47	+4sML2v0u	ı+AMgvjG					
00006DD1:	73 4	8 46	66-66	79	34 7	77-6D		B 61	L-61	73 3	36	34	sHFffy4wn	ikaas64					
00006DE1:	45 4	8 71	4B-39	31	36 6	5C-66		iC 2F	- 5A	74 7	73	78	EHqK916lf	il/Ztsx					
00006DF1:	4E 3	3 68	42-41	5A	61 6	53-39	4A 7	A 78	3-47	47 3	32	64	N3hBAZac9	JzxGG2d					
00006E01:	74 7	9 50	57-4D	6D	53 5	56-78		7 6E	3-67	37 4	18	67	tyPWMmSV>	iWkg7Hg					
00006E11:	56 6	6 70	43-55	ЗD		-			-				VfpCU=						
1Help 2Pu	ıtBlk	BEdi	t <mark>4</mark> M	ode	50	Goto	6Da	tRef	7Se	arch	8	Hea	der <mark>9</mark> Files	10Quit	11Hem	12Name	s 📕		

Figure 5

The aforementioned C2 server proceeds to download an additional configuration JSON file, ultimately leading to the final payload binary, which is a browser stealer malware. This malware is designed to extract sensitive information from the victim's web browsers.

Browser Stealer Payload

The browser stealer is a separate x64-bit DLL that executes its malicious code through the "DIIGetClassObject" export function. This malware aims to extract information such as domain name, computer name, and OS version using the NetWkstaGetInfo() and RtIGetVersion() APIs. Figure 6.1 and 6.2 display code snippets illustrating how the malware retrieves the specified information using these two Windows APIs and formats it before transmitting the data to its C2 server.







Finally, the malware targets several well-known browsers, including "Chrome," "Firefox," "MSEdge," and "Brave," in order to steal information. It achieves this by accessing browser history and the places.sqlite database, copying it, and then querying the discovered SQLite browser databases to parse the URL and title, limited to the first 500 entries. Figure 7 displays a code snippet illustrating how the stealer executes the SQL command once it locates the browser SQLite database it needs to parse and subsequently sends the information to its C2 server.

			10	int64 v15+ // rbx
Segment type:	Pure data		11	
Segment nermi	ssions: Read/Write		12	int v17: // edi
data	segment para public 'DA'	Tå' use64	13	chan % ville // nav
uucu	accume ce: data	14 43004	14	int for y20; // [rsn+30h] [rhn_D0h] BVPFF
	topg 199113999h		15	inter v20, // [rept30] [rbp c0] BVPE
fo browcon fil	o path de officet aAppdat	alocalGo , "AppData\\Local\\Googlo\\Chromo\\Ulco	16	
13_01 003C1_111	da officat aligndatal ocali	Mi : "AppData\\Local\\Microsoft\\Edge\\User D"	17	m128 Nave 1 Jahren 231 // (Seri Politic Laboration 1 Jahren 1 Jahren 1 Jahren 1 Jahren 1 Jahren 231 // (Seri Politic Laboration 1 Jahren 231 Ja
	dq offset papedatalocal	Pr : "AppData\\Local\\ProvoSoftware\\ProvoSoftware\\Provo	10	
	dq offset aAppdataLocali	<pre>br ; AppData(\Local(bravesortware(brave-br ;</pre>	10	mizer v2+[35]; // [rsp+zcen] [rop+icen] biker
FF 100112020	dq offset ampuatakoami	ng ; Appbala(\koaming(\nozilia(\Firelox(\Pro .	- 20	
11_100112020	ad offset anistory	; History	20	$v_2 = dz_2$
	dd offset ahistory	; History	21	V21 = 0154;
	ad offset anistory	; history	22	v20 = 0104;
	dd ottset aplacessdiite	; piaces.squite	23	
Ts_targeted_br	owser dq ottset achrome	; DATA XREF: mw_steal_browser_into+24to	24	mw memset(V24, 0, 0x208u164);
		; "Chrome"	25	*(_QWORD *)&UriComponents.dwExtrainfoLength = 0164;
	dq offset aEdge	; "Edge"	26	"(_OWORD ")&UrlComponents.dwStructSize = 0164;
	dq offset aBrave	; "Brave"	27	*(_OWORD *)&UrlComponents.dwSchemeLength = 0164;
	dq offset afirefox	; "Firefox"	28	"(_OWORD ")&UrlComponents.dwHostNameLength = 0164;
fs_select_url_	title dq offset aSelectU	rlTitle	0 29	*(_OWORD *)&UrlComponents.dwUserNameLength = 0i64;
			9 30	*(_OWORD *)&UrlComponents.dwPasswordLength = 0164;
		; "SELECT url, title FROM urls ORDER BY id"	0 31	*(_OWORD *)&UrlComponents.dwUrlPathLength = 0i64;
	dq offset aSelectUrlTit	le ; "SELECT url, title FROM urls ORDER BY id".	0 32	<pre>mw_memset(NewFileName, 0, 0x208ui64);</pre>
	dq offset aSelectUrlTit	le ; "SELECT url, title FROM urls ORDER BY id".	• 33	<pre>mw_str_format_0((int)NewFileName, (int)L"%s.old", lpExistingFileName);</pre>
	dq offset aSelectUrlTit	<pre>le_0 ; "SELECT url, title FROM moz_places ORDER</pre>	0 34	CopyFileW(lpExistingFileName, (LPCWSTR)NewFileName, 0);
<pre>uintptr_t _se</pre>			0 35	if (!(unsigned int)sub_1800CB440(NewFileName, &v21))
security cook				
			0 37	v9 = -1i64;
word 180113088	dg 0FFFFD466D2205DCDh		0 38	<pre>mw select url title sql cmd = ofs select url title[v5];</pre>
-			0 39	while (mw select url title sal cmd[++v9] != 0)
	db 0FFh ; ÿ		0 40	
	db ØFFh : ÿ		• 41	if (!(unsigned int)sub 180088990(v21, (int)mw select url title sql cmd, 2 * (int)v9, (int64)&v20, 0i64)
	db ØFFh : ÿ			&& (unsigned int)sub 180037030(v20) == 100)
	db ØFFh : ÿ			
			44	
			 46 	memset(&ur)(omponents @ sizeof(Ur)(omponents));
			40	liniformonets horzhorthama - (196STB)/24-
word 180113098	dd 1	• DATA XREE: sub 1800D43D8+loc 1800D44C6tw	48	UnComponents destructive = 104
"or u_100115050		sub 180004308+1001w	0 /0	UnComponents duriostilame langth - 360.
word 190112000		, DATA YREE, cub 190004309+6954	50	UnComponents during characteristic = 200,
word_18011309C	. uu 2	, oub 19000420911154	50	location = (const MCMD # North 18022020(020 _ 0)64);
		, SUD_100004500T1151W	51	1952011 - (CONST WINK)SUD_100030220(V20, 0104);
	uq bobbii	, DATA ARCT: SUD_10000450010	52	do
and 100112010		, INV_INCHISECTUSTIC	53	
woru_1801130A8	uq 20000000	; DATA ARCF: SUD_1000D43D8+59TW	54	++uwuritengen;
		; mw_memset+DCTP	55	While (ipszoralaworitengenj); Zatarstate (ipszoralaworitengen);
DWORD GWIISIN	uex		56	internettratkuriw(ipszuri, dwuritength, 0, &uritemponents);
Eigure 7				
i igule /				

DescriptionValuesTargeted browserChrome, msedge, firefox and braveTargeted browser file pathAppData\Local\Google\Chrome\User Data
AppData\Local\BraveSoftware\Brave-Browser\User Data
AppData\Local\BraveSoftware\Brave-Browser\User Data
AppData\Roaming\Mozilla\Firefox\ProfilesTargeted browser databaseHistory, places.sqliteSQL commandSELECT url, title FROM urls ORDER BY id DESC LIMIT 500
SELECT url, title FROM moz_places ORDER BY id DESC LIMIT 500IOCs

Decrypted C2 in .ico	hxxps://www[.]3cx[.]com/blog/event-trainings/ hxxps://msstorageazure[.]com/window hxxps://akamaitechcloudservices[.]com/v2/storage hxxps://akamaitechcloudservices[.]com/v2/storage hxxps://azureonlinestorage[.]com/azure/storage hxxps://msedgepackageinfo[.]com/microsoft-edge hxxps://glcloudservice[.]com/v1/console hxxps://glcloudservice[.]com/v1/console hxxps://officestoragebox[.]com/exchange hxxps://officestoragebox[.]com/api/session hxxps://visualstudiofactory[.]com/workload hxxps://azuredeploystore[.]com/cloud/services hxxps://msstorageboxes[.]com/office hxxps://officeaddons[.]com/technologies hxxps://sourceslabs[.]com/downloads hxxps://zacharryblogs[.]com/feedhxxps://pbxcloudeservices[.]com/phonesystem
Github repo URL link	hxxps[:]//raw[.]githubusercontent[.]com/IconStorages/images/main/icon%d[.]ico
.ico zip archive	5c54932fdbb077d73c58ac41a1ad3f6ea5576b3e1f719c8b714b637c9ceb361b
ffmpeg.dll	7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
ffmpeg.dll	c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02
d3dcompiler_47.dll	11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03

We identified several key factors during our analysis that aid in guiding Splunk content creation. Now, let's delve into the content and examine the various ways in which Splunk can be of assistance.

Security Content

There are numerous methods for generating content in Splunk, as well as a wide variety of data sources. Based on the indicators provided and our analysis above, we can present the following content. Some of these examples may serve as Splunk inspiration, while others may be suitable for notables. Throughout our discussion, we will offer insights on building resilient analytics for each example.

Hunting 3CXDesktopApp Software

Initially, like many, we want to identify endpoints across our fleet that have C3XdesktopApp running and what version. We decided to use the Endpoint.Processes datamodel so the results would be back fast. If data is not normalized in the datamodel, that's ok! Modify the analytic for your environment by looking for the process names. Note here that the datamodel does not provide file version, we are specifically just looking for where this process is running across the fleet. | tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where Processes.process_name=3CXDesktopApp.exe OR Processes.process_name="3CX Desktop App" by Processes.dest Processes.user Processes.parent_process_name Processes.process_name Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id

- | `drop_dm_object_name(Processes)`
- | `security_content_ctime(firstTime)`
- | `security_content_ctime(lastTime)`

dest \$	user 🗘 🖌	parent_process_name \$	process_name ≠	original_file_name \$	process \$
mswin- dc01.attackrange.local	Administrator	3CXDesktopApp.exe	3CXDesktopApp.exe	3CXDesktopApp.exe	$\label{eq:c:Users} \label{eq:C:Users} eq:C$
mswin- dc01.attackrange.local	Administrator	3CXDesktopApp.exe	3CXDesktopApp.exe	3CXDesktopApp.exe	$\label{eq:constraint} C: Users \ Administrator \ AppData \ Local \ Programs \ 3CXDesktop \ App\ 3CXDesktop \ App, exe^{*}$
mswin- dc01.attackrange.local	Administrator	3CXDesktopApp.exe	3CXDesktopApp.exe	3CXDesktopApp.exe	*C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" revision=0gpu-driver-version=10.0.14393.2608user-data-dir="C:\Users\Administrato preferences=UAAAAAAADDAAAYAAAAAAAAAAAAAAAAAAAAAAAAA
mswin- dc01.attackrange.local	Administrator	3CXDesktopApp.exe	3CXDesktopApp.exe	3CXDesktopApp.exe	*C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" preferences=UAAAAAAADgAAAYAAAAAAAAAAAAAAAAAAAAAAAAAA
mswin- dc01.attackrange.local	Administrator	3CXDesktopApp.exe	3CXDesktopApp.exe	3CXDesktopApp.exe	*C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe* preferences=UAAAAAAADgAAAYAAAAAAAAAAAAAAAAAAAAAAAAAA

Two aspects we recommend examining closely at this time are the file path and the command line. These elements may vary across different environments, so it's important to identify the default location of the binary for your organization and determine if the command line follows a consistent pattern.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as
lastTime from datamodel=Endpoint.Processes where Processes.process_name=3CXDesktopApp.exe OR
Processes.process_name="3CX Desktop App" by Processes.process_path Processes.process_name
```

| `drop_dm_object_name(Processes)`

- | `security_content_ctime(firstTime)`
- | `security_content_ctime(lastTime)`

process_path \$	/	process_name \$	/	count 🗢 🖌
C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe		3CXDesktopApp.exe		29
C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe		3CXDesktopApp.exe		23049

Windows Vulnerable 3CX Software

Switching to Sysmon, we wrote a query to look for 3CXDesktopApp by file version. Depending on the EDR product in use, many provide signature information, VirusTotal enrichment, prevalence and so forth.

The <u>Splunk Attack Range</u> uses a broad configuration <u>file</u> meant to capture every artifact provided. Each EDR product today provides similar or more, so it is very important to understand the product and how it can assist your organization in an event like this.

```
`sysmon` (process_name=3CXDesktopApp.exe OR OriginalFileName=3CXDesktopApp.exe)
FileVersion=18.12.*
| rename Computer as dest
| stats count min(_time) as firstTime max(_time) as lastTime by dest,
parent_process_name, process_name, OriginalFileName, CommandLine
```

dest 🗢	1	process_name \$	1	FileVersion \$	/	count 🗘 🖌	1
mswin-dc01.attackrange.local		3CXDesktopApp.exe		18.12.407		28	3
mswin-dc01.attackrange.local		3CXDesktopApp.exe		18.12.407.0		4	

According to <u>3CX</u>, the security issue affects version numbers 18.12.407 and 18.12.416 on Windows. We adopt a slightly broader approach by searching for any 18.12.* version, primarily to monitor for any instances that may have gone unnoticed. Furthermore, you can modify this analytic to examine any version or simply extract the version information for an inventory overview.

Another take on this query showing just the process and version number by host.

```
`sysmon` (process_name=3CXDesktopApp.exe OR OriginalFileName=3CXDesktopApp.exe)
| rename Computer as dest
| stats count min(_time) as firstTime max(_time) as lastTime by dest process_name FileVersion
```

dest \$	<pre>process_name \$</pre>	✓ FileVersion \$	/	count 🗘 🖌
mswin-dc01.attackrange.local	3CXDesktopApp.exe	18.12.407		6
mswin-dc01.attackrange.local	3CXDesktopApp.exe	18.12.407.0		2
mswin-exch01.attackrange.local	3CXDesktopApp.exe	18.12.422		22
mswin-exch01.attackrange.local	3CXDesktopApp.exe	18.12.422.0		2

18.12.422 is the latest version as of 3/31/2023.

<u>3CX Supply Chain Attack Network Indicators</u>

We would like to thank CrowdStrike and numerous other organizations for providing indicators. The method for detecting the domains used will depend on an organization's security stack. Some products reveal the URI, while others do not. In our case, we utilize DNS queries from Sysmon, which populates the Network_Resolution data model.

Hunting with these domains may provide false positives and filtering / tuning is definitely recommended. Note here that a hit on the domain is not 100% true positive. Some of these are legitimate and will require further review. In addition to looking for the domains, it may provide value in doing two additional tasks based on product support:

- 1. Restrict the network indicators to 3CXDesktopApp, or broadly any process
- 2. Add URIs to the lookup, or a new query, and hunt for beaconing activity.

```
| tstats `summariesonly` values(DNS.answer) as IPs min(_time) as firstTime from
datamodel=Network_Resolution by DNS.src, DNS.query
| `drop_dm_object_name(DNS)`
> `security content ctime(firstTime)`
`security_content_ctime(lastTime)`
| lookup 3cx_ioc_domains domain as query OUTPUT Description isIOC
| search isIOC=true
src $
                  🖌 query 🌣 🖌 IPs 🌣
                                        🖌 firstTime 🗘 🖌 Description 🗘
                                                                                                                                       ✓ islOC $
                               104.18.14.54
104.18.15.54
2606:4700::6812:e36
2606:4700::6812:f36
::ffff:104.18.14.54
::ffff:104.18.15.54
  win-server.attackrange.local
                                             2023-03-30T13:05:13
                                                           https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/
                      www.3cx.com
```

Utilizing the <u>Splunk</u> App for Lookup File Editing, we can easily add/remove indicators or new columns.

	domain	IsIOC	Description
1	akamaicontainer.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
2	akamaitechcloudservices.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
3	azuredeploystore.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
4	azureonlinecloud.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
5	azureonlinestorage.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
6	dunamistrd.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
7	glcloudservice.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
8	journalide.org	TRUE	https://www.reddit.com/r/crowdstrike/cor
9	msedgepackageinfo.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
10	msstorageazure.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
11	msstorageboxes.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
12	officeaddons.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
13	officestoragebox.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
14	pbxcloudeservices.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
15	pbxphonenetwork.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
16	pbxsources.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
17	qwepoi123098.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
18	sbmsa.wiki	TRUE	https://www.reddit.com/r/crowdstrike/cor
19	sourceslabs.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
20	visualstudiofactory.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
21	zacharryblogs.com	TRUE	https://www.reddit.com/r/crowdstrike/cor
22	www.3cx.com	TRUE	https://www.sentinelone.com/blog/smoot
23	akamaitechcloudservices.com	TRUE	https://www.sentinelone.com/blog/smoot
24	azureonlinestorage.com	TRUE	https://www.sentinelone.com/blog/smoot
25	msedgepackageinfo.com	TRUE	https://www.sentinelone.com/blog/smoot
26	glcloudservice.com	TRUE	https://www.sentinelone.com/blog/smoot
27	pbxsources.com	TRUE	https://www.sentinelone.com/blog/smoot
28	msstorageazure.com	TRUE	https://www.sentinelone.com/blog/smoot

DLLs on Disk

As mentioned earlier, it is important to pay attention to the process path. In this specific campaign, we aim to identify any additional files that were dropped on the disk, collect their hashes, and explore potential leads that may offer further insights. Using Sysmon, we have narrowed our focus to the \Appdata\local\ path and sorted the data by the ImageLoaded (DLL) and various metadata points that Sysmon offers. It's important to note that different EDR products will provide varying levels of visibility, so as you analyze this telemetry, start identifying alternative ways to pivot. Be sure to check for prevalence within your organization. For example, if the ffmpeg.dll with this specific hash is found on only 5 out of 5,000 endpoints, it is certainly worth investigating further.

`sysmon` 3cxdesktopapp.exe

```
ImageLoaded="C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\*" | stats
values(ImageLoaded) by loaded_file MD5 FileVersion Company Description
service_dll_signature_verified
```

loaded_file ≎ ✓	MD5 \$	FileVersion 🗘 🖌 🖌	Company \$	Description ₽ ≑	service_dll_signature_verified \$	values(ImageLoaded) *
3CXDesktopApp.exe	08D79E1FFFA244CC0DC61F7D2036ACA9	18.12.407.0	3CX Ltd.	3CX Desktop App	true	$\label{eq:c:Users} C: \label{eq:c:Users} C$
3CXDesktopApp.exe	BB915073385DD16A846DFA318AFA3C19	18.12.407	3CX Ltd.	3CX Desktop App	true	$\label{eq:c:Users} C: \label{eq:c:Users} C$
d3dcompiler_47.dll	82187AD3F0C6C225E2FBA0C867280CC9	10.0.20348.1 (WinBuild.160101.0800)	Microsoft Corporation	Direct3D HLSL Compiler for Redistribution	false	$\label{eq:c:Users} C: Users \ \ dministrator \ \ pp at \ \ conditions \ \ \ conditions \ \ \ conditions \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
ffmpeg.dl1	748C2D086680FAA1A5A76B27E5479CBC	-	-	-	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dll
libEGL.dll	5DE7E395632AF0D31D8165EE5E5267DD	2.1.18365 git hash: 9405b9ea9935	-	ANGLE libEGL Dynamic Link Library	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\libEGL.dll
libGLESv2.dll	F96FC251BAE55A5FC0F1DDAED8706015	2.1.18365 git hash: 9405b9ea9935	-	ANGLE libGLESv2 Dynamic Link Library	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\libGLESv2.dll
notifications_bindings.node	8A3E8B48A5A5E4475C9F1E0478A86BAB	-	-	-	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\resources\app.asar.unp
robotjs.node	4DB8C1BEE7025D7F9B6FADE2EDDB636C	-	-	-	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\resources\app.asar.unp
vk_swiftshader.dll	11308456ED9D5A9EBFDBC0F86160E797	5.0.0	-	SwiftShader Vulkan 32-bit Dynamic Link Library	false	C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\vk_swiftshader.dll
vulkan-1.dll	ACC5484AE9CFFF351FFC0341FAE483DC	1.0.1111.2222.Dev Build	-	Vulkan Loader - Dev Build	false	$\label{eq:c:Users} \label{eq:c:Users} C: \label{eq:c:Users} u$

#ToolTips

Image loads are a voluminous datasource and can be cumbersome to hunt through. Here are some tips to narrow down interesting image loads.

- 1. Focus on non-standard paths. Native Windows DLLs will not run out of the user profile
- 2. Identify signing information and use it to your advantage to look for Unsigned or revoked based on file paths
- 3. If possible, look for processes loading DLLs from non-standard paths. Filter by signing status.

Registry

Revisiting the initial installation process involving MsiExec.exe, it's important to note that several registry modifications occur to ensure the persistence of this version of 3CXDesktopApp.

`sysmon` EventID IN (12,13,14) process_name="msiexec.exe" *\\appdata*
| stats values(registry_value_data) by registry_path

registry_path ≎	/	values(registry_value_data) *	1
HKU\S-1-5-21-2126937381-3842905989-1636914737-500_Classes\3CXDesktopApp.callto\shell\open\command\(Default)		<pre>"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe" "X</pre>	a* -
HKU\S-1-5-21-2126937381-3842905989-1636914737-500_Classes\3CXDesktopApp.tcx+app\shell\open\command\(Default)		"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe" "%	a*
HKU\S-1-5-21-2126937381-3842905989-1636914737-500_Classes\3CXDesktopApp.tel\shell\open\command\(Default)		"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe" "%	a*
HKU\S-1-5-21-2126937381-3842905989-1636914737-500_Classes\callto\shell\open\command\(Default)		"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe" "%	a*
HKU\S-1-5-21-2126937381-3842905989-1636914737-500_Classes\tcx+app\shell\open\command\(Default)		<pre>"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe" "%"</pre>	a*
HKU\S-1-5-21-2126937381-3842905909-1636914737-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\3CXDesktopApp		"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe"	

Now the registry modifications from the 3CXDesktopApp. This is an abbreviated version as there are a lot of standard modifications in the output.

`sysmon` EventID IN (12,13,14) process_name="3cxdesktopapp.exe"
| stats values(registry_value_data) by registry_path

registry_path \$	/	values(registry_value_data) 🗸
HKU\S-1-5-21-2126937381-3842905909-1636914737-500_Classes\tcx+nav\(Default)		URL:tcx+nav
HKU\S-1-5-21-2126937381-3842905909-1636914737-500_Classes\CLSID\(520AA812-3968-40DE-8ED1-0EDC70630DBE)\LocalServer32\(Default)		C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe
HKU\S-1-5-21-2126937381-3842905909-1636914737-500\SOFTWARE\Microsoft\ActiveMovie\devenum 64-bit\Version		8x00000807
HKU\S-1-5-21-2126937381-3842905909-1636914737-500\SOFTWARE\Microsoft\CTF\RemoteSession\KeyboardLayout		0x0000000
HKU\S-1-5-21-2126937381-3842905909-1636914737-500\SOFTWARE\Microsoft\CTF\RemoteSession\CLSID		(Empty)
HKU\S-1-5-21-2126937381-3842905909-1636914737-500\SOFTWARE\Microsoft\CTF\RemoteSession\Profile		(Empty)
HKU\S-1-5-21-2126937381-3842905909-1636914737-500_Classes\tcx+nav\URL Protocol		(Empty)
HKU\S-1-5-21-2126937381-3842905909-1636914737-500_Classes\tcx+nav\shell\open\command\(Default)		"C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" "%%1"

Learn More

You can find the latest content and security <u>analytic stories</u> on <u>GitHub</u> and in <u>Splunkbase</u>. <u>Splunk</u> <u>Security Essentials</u> also has all these detections available via push update.

For a full list of security content, check out the release notes on Splunk Docs.

Feedback

Any feedback or requests? Feel free to put in an issue on GitHub and we'll follow up. Alternatively, join us on the <u>Slack</u> channel #security-research. Follow <u>these instructions</u> If you need an invitation to our Splunk user groups on Slack.

Contributors

We would like to thank <u>Michael Haag</u> and <u>Teoderick Contreras</u> for authoring this post and the entire Splunk Threat Research Team (<u>Rod Soto</u>, <u>Mauricio Velazco</u>, <u>Lou Stella</u>, <u>Bhavin Patel</u>, <u>Eric McGinnis</u>, and <u>Patrick Bareiss</u>) for their contribution to this release.

References:



Posted by

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the <u>Attack Data repository</u>.

Our goal is to provide security teams with research they can leverage in their day to day operations

and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more Splunk Security Content.