

GandCrab V5.2 变种追踪分析

2019-03-21

1. 前言

最近，安恒威胁情报追踪团队发现在 3 月 11 日传播的勒索软件 GandCrab V5.2 在 3 月 20 日又开始新变种传播，这次攻击者将邮箱投递的文件“03-11-19.rar”直接改成“INFORMATION!你必须在 3 月 21 日_下午 3 点向警察局报到!.zip”，变种 GandCrab 对恶意代码进行了混淆改进，需要引高度重视。

2. 攻击线索

将黑客攻击信息绘制成表格：

攻击时间	投递人	文件名称	文件 Hash	解压后文件名
2019-3-10	Min, Gap Ryong	03-11-19.rar	4e6374b0b3421c739ef90bbf4ffb92d5	你 须 瞋 3 昱 11 祉 珥 3 饒 添 筌 涎 报 羽.exe
2019-3-20	Min, Gap Ryong	INFORMATION!你必须在 3 月 21 日_下午 3 点向警察局报到!.zip”	40b7e2560b168a7882ab0b73377d870a	你必须在 3 月 20 日下午 3 点向警察局报到.doc.exe

平台检测到攻击者使用的邮箱，包括

beom-seyk@amaznsicherheitsdienst.com
beom-seyk@blackmonlabs.com
beom-seyk@idabostian.com
beom-seyk@illwaitforthemovie.com
byung-chal@amaznsicherheitsdienst.com
byung-chal@b4imports.com
jae-bong-police@drowsybear.com
jae-bong-police@idalbostian.com
jae-ho-policesupport@b4imports.com
jae-ho-policesupport@designerbasith.com
jae-ho-policesupport@drowsybear.com
jae-hyuk@amazosicherheitsdienst.com

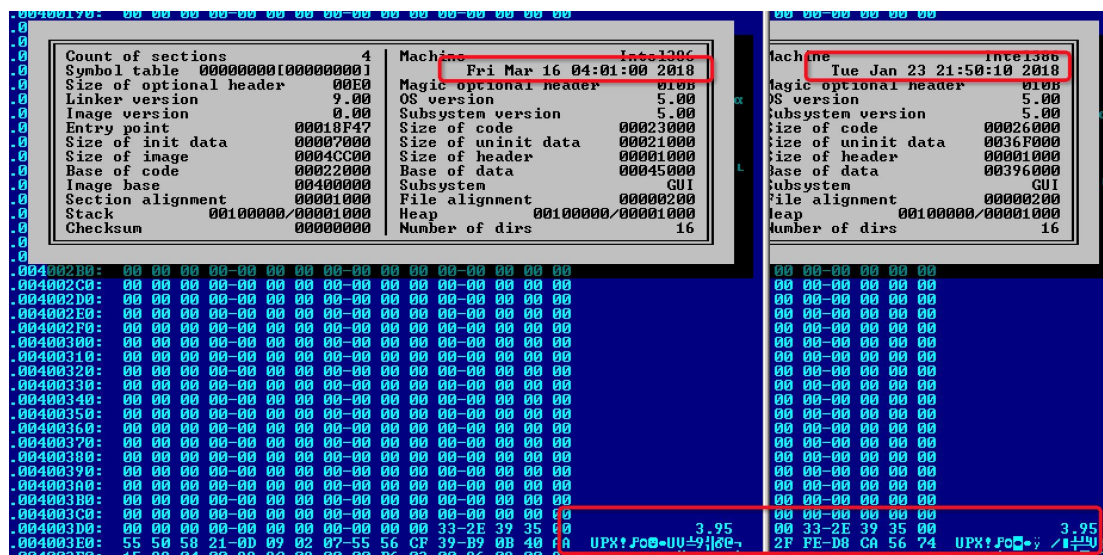
3. 样本分析

通过观察发现变种样本由原来的伪装 Word 图标成一个闹钟图案，

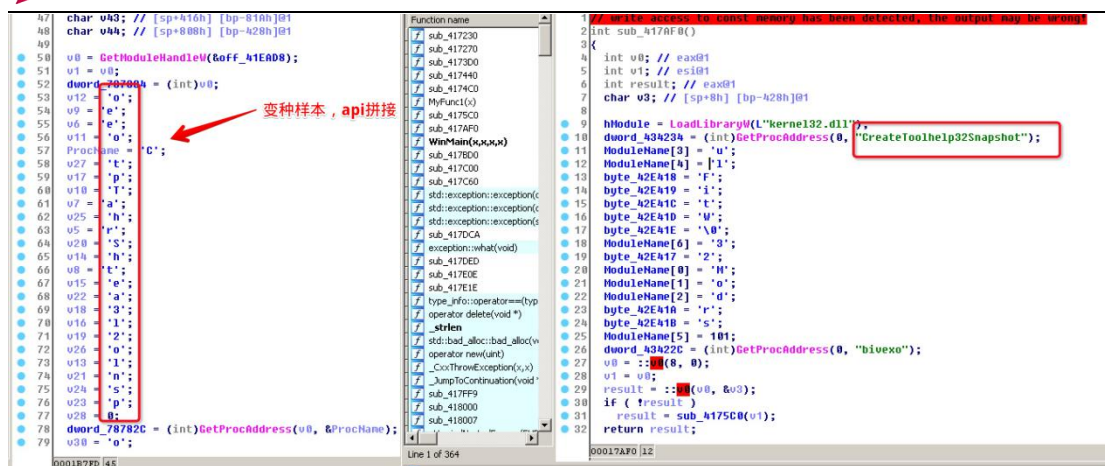


两个文件都是使用 Upx 进行加壳，编译时间都是 2018 年，且变种样本的编译时间比首次发现的样本时间要早，推出攻击者故意修改了编译时间。

- 2018-03-16 04:01:00 首次样本
- 2018-01-23 21:50:10 变种样本



对比原始样本，变种样本对字符串采用了拼接技术



使用填充垃圾指令绕过杀毒检测

0041B495	50	push	eax	Class
0041B496	53	push	ebx	hKey
0041B497	FF15 04C0410	call	dword ptr [<ADVAPI32.RegQueryInfoKeyA	RegQueryInfoKeyA
0041B49D	53	push	ebx	BackupName
0041B49E	53	push	ebx	NewFileName
0041B49F	53	push	ebx	Subkey
0041B4A0	53	push	ebx	hKey
0041B4A1	FF15 0CC0410	call	dword ptr [<ADVAPI32.RegReplaceKeyW	RegReplaceKeyW
0041B4A7	53	push	ebx	Count
0041B4A8	53	push	ebx	pPoints
0041B4A9	53	push	ebx	hDC
0041B4AA	FF15 2CC0410	call	dword ptr [<GDI32.PolyBezier>	PolyBezier
0041B4B0	53	push	ebx	CombineMode
0041B4B1	53	push	ebx	hSrcRegion2
0041B4B2	53	push	ebx	hSrcRegion1
0041B4B3	53	push	ebx	hDestRegion
0041B4B4	FF15 20C0410	call	dword ptr [<GDI32.CombineRgn>	CombineRgn
0041B4BA	53	push	ebx	pStyle
0041B4BB	53	push	ebx	StyleSize
0041B4BC	8D45 A0	lea	eax, dword ptr [ebp-60]	
0041B4BF	50	push	eax	pLogbrush
0041B4C0	53	push	ebx	Width
0041B4C1	53	push	ebx	PenStyle
0041B4C2	FF15 34C0410	call	dword ptr [<GDI32.ExtCreatePen	ExtCreatePen

通过对内存进行加解密操作, 从内存中解密出 PE 文件

00159850	50	push	eax
00159851	E8 E3070000	call	0015A039
00159856	83C4 14	add	esp, 14
00159859	EB 43	jmp	short 0015989E
0015985B	83A5 48FFFFFF	and	dword ptr [ebp-B8], 0
00159862	EB 0D	jmp	short 00159871
00159864	8B85 48FFFFFF	mov	eax, dword ptr [ebp-B8]
0015986A	40	inc	eax
0015986B	8985 48FFFFFF	mov	dword ptr [ebp-B8], eax
00159871	8B85 58FFFFFF	mov	eax, dword ptr [ebp-A8]
00159877	8B8D 48FFFFFF	mov	ecx, dword ptr [ebp-B8]
0015987D	3B48 02	cmp	ecx, dword ptr [eax+2]
00159880	73 1C	jnb	short 0015989E
00159882	8B45 E0	mov	eax, dword ptr [ebp-10]

003D0000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	MZ? ... }...üü..
003D0010	B8 00 00 00	00 00 00 00	40 00 00 00	00 00 00 00	?.....@.....
003D0020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
003D0030	00 00 00 00	00 00 00 00	00 00 00 00	E8 00 00 00?..
003D0040	0E 1F BA 0E	00 B4 09 CD	21 B8 01 4C	CD 21 54 68	■??.???L?Th
003D0050	69 73 20 70	72 6F 67 72	61 6D 20 63	61 6E 6E 6F	is program canno
003D0060	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F 53 20	t be run in DOS
003D0070	6D 6F 64 65	2E 0D 0D 0A	24 00 00 00	00 00 00 00	mode....\$......
003D0080	1D 75 60 44	59 14 0E 17	59 14 0E 17	59 14 0E 17	■u`DY■■■■Y■■■■Y■■■
003D0090	50 6C 9B 17	5A 14 0E 17	59 14 0F 17	39 14 0E 17	P1?Z■■■■Y■■■■9■■■
003D00A0	50 6C 9D 17	52 14 0E 17	CE 4A 0A 16	5B 14 0E 17	P1?R■■■■■.■[■■■
003D00B0	CE 4A 0B 16	44 14 0E 17	CB 4A 0D 16	5A 14 0E 17	■■■D■■■■■.■Z■■■
003D00C0	CE 4A 0C 16	58 14 0E 17	52 69 63 68	59 14 0E 17	■.■X■■■■RichY■■■
003D00D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
003D00E0	00 00 00 00	00 00 00 00	50 45 00 00	4C 01 04 00PE..L.!
003D00F0	C8 94 8A 5C	00 00 00 00	00 00 00 00	E0 00 02 01	章獎.....? 爻
003D0100	0B 01 0E 00	00 00 01 00	00 82 00 00	00 00 00 00	■.■.....爻. ?.....

其 MD5:D1960357F97D64FB1339E44D90D09D47, 对比第一次攻击样本文件在内存解密出来的文件 MD5: 7AA1751726B3F25E695E40786187E451 的编译时间

- 2019-02-24 00:51:29 首次样本核心模块
- 2019-03-15 01:52:08 变种样本核心模块

很明显这里的时间才是真正的攻击者开发时间, 确定了外壳部分可能是人为修改或工具自动完成

00400000:	23 0D 23 BD-67 EC 4D EE-67 EC 4D EE-67 EC 4D EE	#i\$4gMECgMECgMEC	24 00 00 00-00 00 00 00	Mode.JJCS
00400090:	6E 94 D0 EE-64 EC 4D EE-67 EC 4D EE-0D EC 4D EE	nä+deMEgoleJwME	59 14 0E 17-59 14 0E 17	mi DYWYVWYVWYVW
004000A0:	6E 94 DE EE-6A EC 4D EE-F0 B2 49 EF-65 EC 4D EE	nä JEjMEJInewME	59 14 0F 17-39 14 0E 17	PlEzWYVWYVWYVW
004000B0:	F0 B2 48 EF-7A EC 4D EE-F5 B2 4E EF-64 EC 4D EE	≡InzMEJNndwME	CE 40 00 16-5B 14 0E 17	PlEzWYVWYVWYVW
004000C0:	F0 B2 4F EF-66 EC 4D EE-52 69 63 68-67 EC 4D EE	≡OnfMECRichwME	CB 40 0D 16-5A 14 0E 17	WYVWYVWYVWYVW
004000D0:	00 00 00 00-00 00 00 00 00 00 00 00 00 00 00		52 69 63 68-59 14 0E 17	WYVWYVWYVWYVW
004000E0:	50 45 00 00-4C 01 04 00-11 7A 71 5C-00 00 00 00	PE L0* 4g\	00 00 00 00-00 00 00 00	
004000F0:	00 00 00 00-E0 00 02 01-0B 01 0E-00 00 00 01	α 000E\	00 00 00 00-00 00 02 01	Us2\
				α 000E\

在内存中明显发“GandCrab V5”字符串信息

```

00407FD2 50 PUSH EAX
00407FD3 FF15 7C104100 CALL DWORD PTR DS:[<@KERNEL32.CreateFileW
00407FD9 8BD8 MOV EBX,EAX
00407FDB 83FB FF CMP EBX,-1
00407FDE 74 34 JE SHORT 1123.00408014
00407FE0 56 PUSH ESI
00407FE1 8D45 FC LEA EAX,WORD PTR SS:[EBP-4]
00407FE4 50 PUSH EAX
00407FE5 FF35 84984100 PUSH DWORD PTR DS:[419884]
00407FE6 FF15 E8104100 CALL DWORD PTR DS:[<@KERNEL32.lstrlenW>]
00407FE7 03C0 ADD EAX,EAX
00407FE8 50 PUSH EAX
00407FE9 FF35 84984100 PUSH DWORD PTR DS:[419884]
00407FFA 53 PUSH EBX
00407FFB FF15 70104100 CALL DWORD PTR DS:[<@KERNEL32.WriteFile
00408001 53 PUSH EBX
00408002 8BF0 MOV ESI,EAX
00408004 FF15 4C104100 CALL DWORD PTR DS:[<@KERNEL32.CloseHand
0040800A 57 PUSH EDI
0040800B E9 C1460000 CALL 1123.0040C6D1
00408010 8BC6 MOV EAX,ESI
00408012 EB 21 JMP SHORT 1123.00408035

```

针对各种后缀文件进行加密，涉及对后缀名非常多。

```

00403B6A FF75 F4 PUSH DWORD PTR SS:[EBP-C]
00403B6D FF15 E0104100 CALL DWORD PTR DS:[<@KERNEL32.VirtualFree
00403B73 58 PUSH ESI
00403B74 E8 ED040000 CALL 1123.00404066
00403B79 59 POP ECX
00403B7A 85C0 TEST EAX,EAX
00403B7C 74 2D JE SHORT 1123.00403BAB
00403B7E E8 9A090000 CALL 1123.0040451D
00403B83 8D45 F0 LEA EAX,WORD PTR SS:[EBP-10]
00403B86 C705 78984100 MOV DWORD PTR DS:[419878],1123.00413C70
00403B90 50 PUSH EAX
00403B91 C705 7C984100 MOV DWORD PTR DS:[41987C],1123.00413EA8
00403B9B C705 80984100 MOV DWORD PTR DS:[419880],1123.00413F78
00403BA5 E8 D3020000 CALL 1123.00403E7D
00403BAA 59 POP ECX
00403BAB 53 PUSH EBX

```

00413F78=1123.00413F78 (UNICODE "? .1st .602 .docb .xlm .xlsx .xslm .xltx .xltm .xlsb .xla .xlam .s
DS:[00419880]=00413F78 (1123.00413F78), UNICODE "? .1st .602 .docb .xlm .xlsx .xslm .xltx .xltm .x

地址	UNICODE 数据	00C1FCF0	00C50000	UNICODE
00414178	.bad .bbs .bdp .bdr .bean .bib .bib .bibtex .bml .bna .boc .brx	00C1FCF4	009A0000	UNICODE
00414178	.btd .brabw .calca .charset .chart .chord .cnm .cod .cowl .cws	00C1FCF8	00000000	UNICODE
00414278	.cyi .dca .dfti .dgs .diz .dne .dot .doc .docm .dotx .docx .docxm	00C1FCFC	00C1FF88	UNICODE
00414278	.l .docz .dox .dropbox .dsc .dvi .dwd .dx .dxb .dyp .eio .eit .em	00C1FD00	00C1FF8C	UNICODE
00414378	.f .enl .emlx .emulecollection .epp .err .err .etf .etx .euc .fac	00C1FD04	00408ACF	返回
00414378	.ein .template .faq .fbl .fcf .fdf .fdr .fds .fdt .fdx .fdxt .fft	00C1FD08	00C50000	UNICODE
00414478	.fgs .flr .fodt .fountain .fpt .ftr .fwd .fwdn .gmd .gpd .gpn .g	00C1FD0C	00C50000	UNICODE
00414478	.sd .gthr .gv .hbk .hht .hs .hwp .hwp .hz .idx .iil .ipf .ipspot	00C1FD10	00B10000	UNICODE
00414578	.jarvis .jis .jnp .joe .jpl .jrtf .jtd .kes .klg .knt .kon	00C1FD14	00B10000	UNICODE
00414578	.kwd .latex .lbt .lis .lnt .log .lp2 .lst .lst .ltr .ltx .lue .l	00C1FD18	FFFFFFFF	UNICODE
00414678	.uf .lwp .lxfml .lyt .lyx .man .mbox .mcw .md5 .me .mell .mellel	00C1FD1C	7C93B00A	返回
00414678	.min .mnt .msg .mw .mwd .mwp .nb .ndoc .nfo .ngloss .njx .note	00C1FD20	7C92D04C	返回
00414778	.notes .now .nwctxt .nwm .nwp .ocr .odif .odm .odo .odt .ofl .ope	00C1FD24	7C92E43F	返回
00414778	.ico .openbsd .ort .ott .p7s .pages .pages-tef .pdpcmd .pfx .pjt	00C1FD28	00C1FD30	UNICODE
00414878	.plain .plantuml .pmo .prt .prt .psw .pu .pvj .pvm .pwd .pwdp .p	00C1FD2C	00000001	UNICODE
00414878	.wdpl .pwi .pwr .qdl .qpf .rad .readme .rft .ris .rpt .rst .rtd	00C1FD30	00010017	UNICODE
00414978	.rtf .rtfd .rtx .run .rvf .rzlk .rzn .saf .safetext .sam .sam .sav	00C1FD34	00000000	UNICODE
00414978	.e .scc .scm .scriv .scrivx .set .scw .sdm .sdoc .sdw .se .sessio	00C1FD38	00000000	UNICODE
00414A78	.n .sgn .sig .skcard .sla .sla .gz .smf .sms .ssa .story .strings	00C1FD3C	00000020	UNICODE
00414A78	.stw .sty .sublime-project .sublime-workspace .sxg .sxw .tab .te	00C1FD40	00159F10	UNICODE
00414B78	.b .tdf .tdf .template .tex .text .textclipping .thp .tlb .tm .tm	00C1FD44	00150000	UNICODE
00414B78	.d .tmdx .tmv .tmvx .tpe .trelby .tvj .txt .u3i .unauth .unx .uof	00C1FD48	00000000	UNICODE
00414C78	.uot .upd .utf8 .utxt .vct .vnt .vw .wbk .webdoc .wn .wp .wp4	00C1FD4C	00000000	UNICODE
00414CF8	.wp5 .wp6 .wp7 .wpa .wpd .wpd .wpd .wpl .wps .wps .wpt .wpt .wpw	00C1FD50	01015678	vmh;
00414D78	.wri .wsd .wtt .wtx .xbdoc .xbplate .xdl .xdl .xwp .xwp .xwp .xy	00C1FD54	00C1FD0C	UNICODE

该勒索软件加密的文本名称和后缀均为随机生成，勒索信息文本为固定格式{随机字符串}-MANUAL.txt

其中 Tor 节点如下

- hxxp://gandcrabmfe6mnef.onion/2e71d83f64fbef51

```
LXHOJH-MANUAL.txt - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)

-----  GANDCRAB U5.2  -----

*****UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED*****

****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .LXHOJH

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover y

The server with your key is in a closed network TOR. You can get there by the following ways:

-----

| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:  http://gandcrabmfe6nnf.onion/2e71d83f64fbef51
| 4. Follow the instructions on this page

-----

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
1AQAAI+i06JP6623cGMsoxP2bKRpnrhSUCPFQzJUT9t1GN7Lp+jLFw4Yu2GXFPiJd10qzULjEj0RomP1U4kZ4b/0uRKs+uK6+uFq70Ts4dDn1Pt1n+uEbLkcFD1q1HIU
TcrMsAEhPL1U1NYCCcHvBNP0F/kaepFSKGYxTEg8rv6cH2FXGjtbHMcZewiUc60uThHDD0UuH4FeQ5u22SupKyeE9aLhrH6C56U21wCH0JumVQi8p131QqFrr3UC+YQb
AU2bHkrAH0Kd8d+thR20pfHI76xS0e+CwXahIJz7FRDT1HxDPRkb96xLp+/W/KSPH3osS/0htAzB/1m2ISzJH43eW6nUHD/HP9jsDG2pkIHqQ6wz6tU33KVJ1F5/cc36Q
5+n1uaJ090FuSuP3uvW08RNGdgennPX/v8ed9nE7UokQ0ev5T/uQLuSF3LyUAsm0thHTc2pHkxXH0tF8k0WmZX1pnDL54baBrS0bt1Pr0LRrMhAgC9sF11ydG0m3y2KdL
tBAa2dFs4FLQZ6L9NU0tH/FYA7/0X8CNz22rmGdqHxvKPTjyHm/PFuU4+5Y31sCUSPaWj/aarZ1z07FpZAR88KQHT4WqRz1cFX0K0EG+U1UwUXfbIBHJJ1PNg6vsLW16G/
aK2FCeHhwkz+zKdZ2hQrWfMsznsH5XGt1Fz8tjKjQ1k2JQFw85zN2+6mXH8UFwT37U0FahI9EmU23k4F0b7Djng7wL5nJK0Du2FjARxk0p/YKT10Y1eGNZ3uFe24HJsk
U92+yprrYVBBJCSf3LcGB5RtXEWasFg0HUSeooQM1UPWFH2oSf1KB4Seta9d1CwJREG0uqR7SQW94gWhUvqCBA0/UyUo2Fn0LE4Swc0NU0qno8oHAMBPTTLwFcPpmfuC6
1P8ePtJst2jS8KPTbJDPULM5HJiu6UFfr/mAVLdvhnyPiXxeXcLIpio0M9Rz10WV8fYhF29XqpmEbvBhWt9hj31cst9c/nXsxy/KFuAFk10FBKKXjwA055RnzpYX+
```

4. 建议

勒索病毒一旦感染主机会对珍贵数据进行加密并要求受害者支付赎金, 在受害者支付赎金后仍有可能存在不可解密的风险, 建议在关键信息基础设施所在单位部署网络安全态势感知系统, 实时感知存在的网络安全威胁, 加强网络防控能力; 建议在关键信息基础设施服务器部署终端防护软件 (EDR)、APT 预警平台等, 都可有效防止勒索病毒感染与传播。