بسمه تعالی

گزارش فنی و تحلیلی بدافزار

LockCrypt

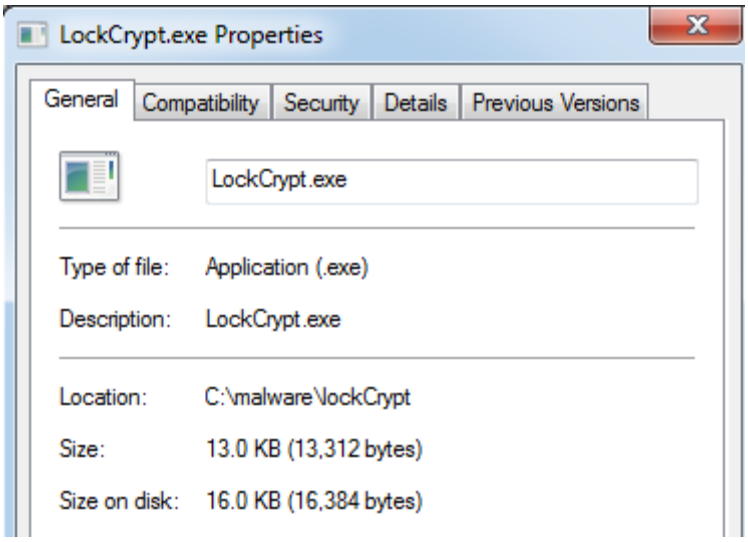
فهرست مطالب

۱ معرفی بدافزار

بدافزار LockCrypt در تاریخ دهم Agu سال ۲۰۱۸ ایجاد شده است. این بدافزار که از الگوریتم رمزگذاری AES-۲۵۶ و RSA-۲۰۴۸ استفاده می‌کند، فایل‌های کاربر را با پسوندی به شکل زیر رمز می‌کند.

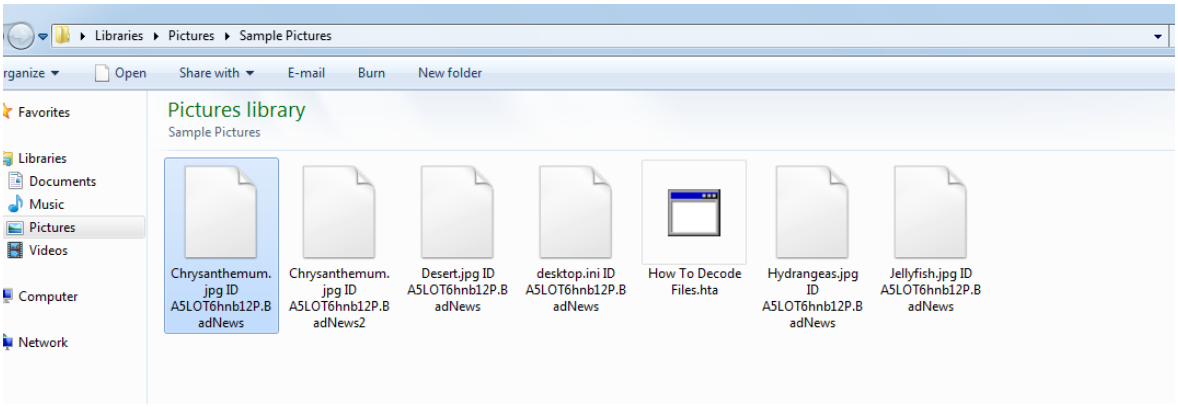
- Filename. Extension ID (user ID).BadNews

شکل ۱ آیکون مربوط به بدافزار را نشان می‌دهد.



شکل ۱- آیکون مربوط به باج‌افزار LockCrypt

باج‌افزار LockCrypt در هر پوشه‌ای که فایل‌های مربوط به آن را رمز نموده است فایلی با عنوان How To Decode File.hta قرار داده است که در فایل ID مربوط به قربانی و آدرس ایمیلی جهت ارتباط با مهاجم ارائه شده است. از قربانی خواسته شده یکی از فایل‌های رمز شده بهمراه ID را به آدرس BM-۲cTAPjtTkqiW۲twtykGm۵mtocFAz۷g۵FZc@bitmessage.ch ایمیل کند تا ضمن دریافت فایل رمزگشایی شده مبلغ باج نیز برای رمزگشایی همه فایل‌ها اعلام گردد. شکل ۲ نمونه فایل‌های رمز شده توسط مهاجم و شکل ۳ پیام باج‌خواهی را نشان می‌دهد.



شکل ۲ – نمونه فایل‌های رمز شده

شکل ۳- صفحه باج‌خواهی

شکل ۴ ساختار هگزا دسیمال نمونه ای از فایل رمز شده را در دو زمان مختلف (قبل از رمزگذاری و بعد از آن) نشان می‌دهد.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	60	ÿØÿà..JFIF.....`
00000010	00	60	00	00	FF	EE	00	0E	41	64	6F	62	65	00	64	00	.`..ÿî.Adobe.d.
00000020	00	00	00	01	FF	E1	13	5D	45	78	69	66	00	00	4D	4D	....ÿá.]Exif..MM
00000030	00	2A	00	00	00	08	00	07	01	32	00	02	00	00	00	14	.*.....2.....
00000040	00	00	00	62	01	3B	00	02	00	00	00	07	00	00	00	76	...b.;.....v
00000050	47	46	00	03	00	00	00	01	00	04	00	00	47	49	00	03	GF..........GI..
00000060	00	00	00	01	00	3F	00	00	9C	9D	00	01	00	00	00	0E	.....?.....
00000070	00	00	00	00	EA	1C	00	07	00	00	08	0C	00	00	00	00	....ê.....
00000080	87	69	00	04	00	00	00	01	00	00	00	7D	00	00	00	E7	.i.....}...ç
00000090	32	30	30	39	3A	30	33	3A	31	32	20	31	33	3A	34	36	2009:03:12 13:46
000000A0	3A	34	32	00	43	6F	72	62	69	73	00	00	05	90	03	00	:42.Corbis.....
000000B0	02	00	00	00	14	00	00	00	BF	90	04	00	02	00	00	00	....¿.....
000000C0	14	00	00	00	D3	92	91	00	02	00	00	00	03	35	34	00	....Ó.....54.
000000D0	00	92	92	00	02	00	00	00	03	35	34	00	00	EA	1C	00	.....54..ê..
000000E0	07	00	00	07	B4	00	00	00	00	00	00	00	00	32	30	30	....´.....200
000000F0	38	3A	30	33	3A	31	34	20	31	33	3A	35	39	3A	32	36	8:03:14 13:59:26
00000100	00	32	30	30	38	3A	30	33	3A	31	34	20	31	33	3A	35	.2008:03:14 13:5
00000110	39	3A	32	36	00	00	05	01	03	00	03	00	00	00	01	00	9:26.....
00000120	06	00	00	01	1A	00	05	00	00	00	01	00	00	01	29	01	.....)...
00000130	1B	00	05	00	00	00	01	00	00	01	31	02	01	00	04	00	.....1.....
00000140	00	00	01	00	00	01	39	02	02	00	04	00	00	00	01	00	....9.....
00000150	00	12	1C	00	00	00	00	00	00	00	48	00	00	00	01	00	.....H.....
00000160	00	00	48	00	00	00	01	FF	D8	FF	E0	00	10	4A	46	49	..H.....ÿØÿà..JFI
00000170	46	00	01	01	00	00	01	00	01	00	00	FF	DB	00	43	00	F.....ÿÛ.C.

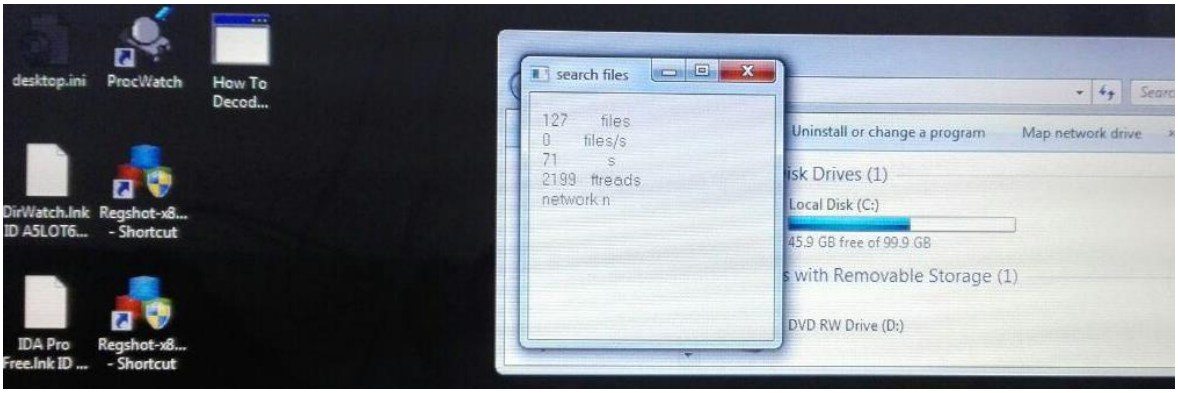
نمونه فایل قبل از اجرای باج افزار

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	EE	2E	97	31	A7	D5	D1	CB	51	EB	3E	2F	5F	9A	07	D5	î.1§ÕÑËQë>/_Õ
00000010	BE	35	01	20	C0	2C	BB	A0	88	A2	2A	44	26	24	92	AF	¾5 .À,» ¢*D&$¯
00000020	97	51	FD	C7	8A	C8	B2	95	91	1A	C8	9C	39	6F	2C	FD	QýÇÈ²´→È9o,ý
00000030	53	39	89	C1	CB	FB	B8	4E	26	A7	CE	90	8B	FE	9A	E7	S9ÁËû¸N&ÎþçÎ
00000040	D0	09	33	7A	ED	E5	C8	16	50	E8	43	87	6E	D1	8B	8E	Ð.3zíåÈPèC‡nÑ‹Ž
00000050	AC	F2	25	6F	18	88	9D	5B	54	0A	80	50	0E	FD	47	A7	¬ò%o[T.€P.ýG§
00000060	FF	39	C7	84	A7	A2	2F	87	48	F3	39	AE	8B	2E	88	36	ÿ9Ç„§¢/‡Hó9®‹.ˆ6
00000070	91	4A	DB	2E	71	60	A2	34	49	E8	F7	12	40	C0	4C	E1	'JÛ.q`¢4Iè÷↕@ÀLá
00000080	9C	A8	85	83	8A	D9	93	33	F0	A6	A1	77	3A	4D	C6	AA	œ¨…ƒŠÙ“3ð¦¡w:MÆª
00000090	83	91	C3	AC	7C	7A	94	A0	DF	60	68	2B	15	73	83	4D	ƒ'Ã¬|z” ß`h+§sƒM
000000A0	F8	76	17	9B	CB	FA	AF	67	B4	42	FA	51	25	72	30	AC	øv›ËúÏg´BúQ%r0¬
000000B0	CE	E7	38	9E	67	24	70	19	E6	3D	98	BE	46	04	DC	73	Îç8žg$p↓æ=˜¾F↵Üs
000000C0	AF	EA	04	E7	B3	89	BB	8F	47	9F	D7	76	F3	1C	97	3F	¯ê↵ç³‰» GŸ×vó—?
000000D0	B2	6B	4A	D3	6F	4A	9A	42	31	B4	9B	5E	2B	50	08	75	²kJÓoJšB1´›^+P◘u
000000E0	E5	31	C4	79	D9	88	50	83	AB	91	FC	E0	B3	4F	4F	20	å1ÄyÙˆPƒ«‘üà³OO
000000F0	73	5D	FB	07	AB	0C	80	B0	15	22	6B	73	DE	E6	12	E2	s]û•«◘€°§"ksÞæ↕â
00000100	AF	F2	C1	57	9F	66	E3	5B	65	2F	33	75	63	31	C8	EE	¯òÁWŸfã[e/3uc1Èî
00000110	F4	84	F2	7A	CD	56	E4	6F	B7	64	BE	B8	EE	08	2E	66	ô„òzÍVäo·d¾¸î◘.f
00000120	42	15	FC	2C	DA	65	C9	63	5D	86	0F	00	97	B2	CE	B1	B§ü,ÚeÉc]†☼.—²Î±
00000130	AF	49	90	50	76	80	34	47	15	54	9E	7E	4D	2A	60	1E	¯I PvG§T~M*`
00000140	BC	23	3E	A4	D0	A7	8B	99	98	5F	99	34	10	DD	C9	50	¼#>¤Ð§‹™˜_™4►ÝÉP
00000150	A1	14	7B	BA	EC	BB	80	88	B2	FF	57	D9	0C	7D	A5	AE	¡¶{ºi»€ˆ²ÿWÙ}¥®
00000160	B6	3B	75	CE	98	DA	AF	24	1A	63	1B	17	20	6F	34	6B	¶;uÎ˜Ú¯$→c←↨ o4k
00000170	5F	EE	72	9F	CE	B0	48	09	6A	A7	F3	21	E3	6B	C2	A5	_îrŸÎ°H.j§ó!ãkÂ¥

نمونه فایل بعد از اجرای باج افزار

شکل ۴- هگزا دسیمال نمونه فایل زمرشده در دو زمان مختلف

این باج‌افزار در شروع اجرا، کلیه فرآیندهای جاری سیستم را kill می نماید. شکل ۵ screenShootای از لحظه اجرای باج‌افزار را نشان می‌دهد.



شکل ۵- لحظه‌ای از اجرای باج‌افزار

۲ مشخصات فایل LockCrypt

مشخصات فایل اجرائی LockCrypt به شرح زیر است:

۲-۱ کلیات فایل LockCrypt

مشخصات اولیه فایل اجرائی مفروض از قبیل درهم‌سازها ، اندازه، زمان کامپایل و سایر مشخصات مربوط به کلیات فایل در جدول ۱ ذکر شده است.

جدول ۱-مشخصات کلی فایل LockCrypt

نام فایل	LockCrypt
نوع فایل	۳۲ بیتی
درهم ساز MD۵	eafaa۴۲۶۷۳af۸۹۸۲۱d۵۶bd۷fc۸۴۸a۸۸f
درهم ساز SHA۲۵۶	۱c۲bdfa۵e۳۰cbf۸eb۹۲c۳۷۶۴de۹b۱۰۶aa۷۲۲a۸۱b۵۰۶۴۱۶۹۸d۲۶۲۰a۴۹b۵۳۰b۰b۴
درهم ساز SHA۱	۸۶a۷d۰۳e۷۱۰d۵۴۶۵۱۷۵۲e۹۹۰۴۶۶۶۹۰۸۸۶۹۶e۶۸b۸
حجم فایل	۰.۰۱۲۶۹۵۳۱۲۵مگا بایت
تعداد Section ها	۴
زمان کامپایل	Fri Aug ۱۰ ۱۰:۴۰:۲۷ ۲۰۱۸

۲-۲ Section های مختلف فایل LockCrypt

جدول ۲ مشخصات Sectionهای فایل LockCrypt را نشان می‌دهد

جدول ۲- Sectionهای فایل LockCrypt

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD٥	Characteristics
.text	٤٠٩٦	٤٩٩٦	٥١٢٠	٥.٦٦	٥٤٤٥e٥٧٩٦e٤٥٦df٦٨٠٦٨٩ed٤٢bffdd٤٣	CNT_CODE, MEM_EXECUTE, MEM_READ,
.rdata	١٢٢٨٨	٢١٥٦	٢٥٦٠	٤.٥١	c٩٢c٠٨٤٨٣٩٣١٤٩٣٩٥٣e٤٠cc١٥db٥٥e٥c	CNT_INITIALIZED_DATA, MEM_READ
.data	١٦٣٨٤	٤٦٢٤	٢٥٦٠	٧.٥١	b٤ad٩b٦٩e٩b٧fb٠٨c٤efc٢٥٠٥٤١ef٢b٦	CNT_INITIALIZED_DATA, MEM_READ, MEM_WRITE
.rsrc	٢٤٥٧٦	١٥٦٨	٢٠٤٨	٦.١٠	٨ddafd٨٨e٦ad٣d٣٥٧b٩eab٩٢eab٧c٤de	CNT_INITIALIZED_DATA, MEM_READ,

۲-۳ بررسی سطح تهدید فایل LockCrypt

شکل ۶ بررسی سطح تهدید فایل اجرائی LockCrypt در سامانه virusTotal.com نشان می‌دهد که از تعداد ۶۸ موتور آنتی‌ویروس ۵۰ مورد فایل مذکور را بعنوان بدافزار شناسایی کرده‌اند.

Ad-Aware	Trojan.GenericKD.31178078	ALYac	Trojan.Ransom.LockCrypt
Antiy-AVL	Trojan/Win32.AntiAV	Arcabit	Trojan.Generic.D1DBBD5E
Avast	FileRepMalware	AVG	FileRepMalware
Avira	TR/ATRAPS.Gen	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.31178078
CAT-QuickHeal	Trojan.Fuerboos	Comodo	.UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.e710d5
Cylance	Unsafe	Cyren	W32/Trojan.EMYO-1230
DrWeb	Trojan.KillProc.56506	Emsisoft	Trojan.GenericKD.31178078 (B)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.31178078
ESET-NOD32	Win32/Filecoder.NPA	F-Secure	Trojan.GenericKD.31178078
Fortinet	W32/AntiAV.NPA!tr	GData	Trojan.GenericKD.31178078
Ikarus	Trojan-Ransom.FileCoder	Jiangmin	Trojan.AntiAV.ang
K7AntiVirus	Trojan (005235101)	K7GW	Trojan (005235101)
Kaspersky	HEUR:Trojan.Win32.AntiAV	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=99)	McAfee	RDN/Generic.dx
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.AntiAV.fgwaxm
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	HEUR/QVM20.1.5621.Malware.Gen	Rising	Trojan.GenKryptik!8.AA55 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan Horse
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	Ransom_LOCKCRYPT.THHBIAH
TrendMicro-HouseCall	Ransom_LOCKCRYPT.THHBIAH	VBA32	BScope.Trojan.AntiAV
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Highconfidence.13312.F
Webroot	W32.Trojan.GenKD	ZoneAlarm	HEUR:Trojan.Win32.AntiAV
AegisLab	Clean	AhnLab-V3	Clean
Avast Mobile Security	Clean	Babable	Clean
Bkav	Clean	ClamAV	Clean
CMC	Clean	eGambit	Clean
F-Prot	Clean	Kingsoft	Clean
McAfee-GW-Edition	Clean	SUPERAntiSpyware	Clean
TACHYON	Clean	TheHacker	Clean
TotalDefense	Clean	Yandex	Clean
Zillya	Clean	Zoner	Clean

شکل ۶- وضعیت بدافزار در سامانه virusTotal

۳ فرآیند آلوده‌سازی

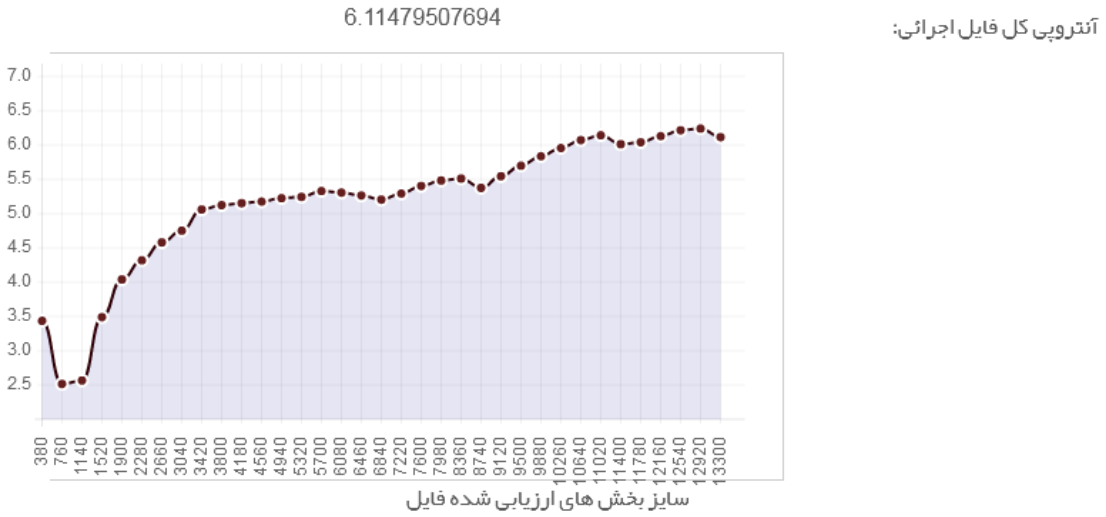
تحقیقات و بررسی ها نشان می‌دهد نحوه گسترش باج‌افزار از طریق ایمیل‌های spam می باشد

۴ ویژگی های فایل LockCrypt براساس تحلیل ایستا

ویژگی‌های فایل LockCrypt براساس تحلیل ایستا به شرح زیر است:

۴-۱ آنتروپی

روند صعودی و مقدار بیش از ۷ آنتروپی، احتمال رفتار بدافزاری فایل را افزایش می‌دهد. آنتروپی فایل LockCrypt در شکل ۹ نشان داده است.



شکل ۷- آنتروپی فایل LockCrypt

۴-۲ تحلیل مقاومتی

EnrtyPoint فایل LockCrypt برابر با ۰۰۰۰۱e۴a است که در شکل ۱۰ هگزادیسمال و Disassembly نقطه شروع نشان داده شده است.

```
00401e4a  6A00          push 00000000h
00401e4c  E80D040000    call 0040225Eh
00401e51  A3EC484000    mov dword ptr [004048ECh], eax
00401e56  68E0080000    push 000008E0h
00401e5b  6800404000    push 00404000h
00401e60  E89BF1FFFF    call 00401000h
00401e65  E8FAFAFFFF    call 00401964h
00401e6a  50            push eax
00401e6b  E8B2030000    call 00402222h
00401e70  55            push ebp
00401e71  8BEC          mov ebp, esp
00401e73  8B450C        mov eax, dword ptr [ebp+0Ch]
00401e76  3D10010000    cmp eax, 00000110h
00401e7b  7541          jne 00401EBEh
00401e7d  8B4508        mov eax, dword ptr [ebp+08h]
00401e80  A3E8484000    mov dword ptr [004048E8h], eax
```

شکل ۸- هگزادسیمال و Disassembly نقطه شروع

بررسی Signature فایل LockCrypt با پایگاه‌داده‌ای از Signatureهای سامانه ستفا نشان می‌دهد که در زبان TASM / MASM کامپایل شده است.

۳-۴ کتابخانه ها و توابع استفاده شده

جدول ۳ براساس تحلیل ایستا کتابخانه‌ها و توابع استفاده شده در ساختار فایل LockCrypt را نشان می‌دهد.

جدول ۳- کتابخانه‌ها و توابع استفاده شده از هر کتابخانه

نام کتابخانه	توابع استفاده شده
user۳۲.dll	UpdateWindow, TranslateMessage, ShowWindow, SetTimer, SendMessageA, GetMessageA, GetDlgItem, DispatchMessageA, CreateDialogParamA,
kernel۳۲.dll	FindClose, FindFirstFileW, FindNextFileW, FindResourceA, GetCurrentProcessId, GetEnvironmentVariableA, GetFileAttributesW, GetLogicalDrives, GetModuleFileNameA, GetModuleHandleA, GlobalAlloc, GlobalFree, GlobalMemoryStatus, LoadResource, CreateThread, MoveFileW, MultiByteToWideChar, OpenProcess, Process۳۲FirstW, Process۳۲NextW, RtlMoveMemory, ExitProcess, CreateFileW, SetFileAttributesW, SetFilePointer, SetThreadPriority, SizeofResource, Sleep, TerminateProcess, UnmapViewOfFile, WriteFile, lstrcatW, lstrcmpW, lstrcmpiA, lstrcmpiW, lstrcpyW, lstrlenA, lstrlenW, CreateFileMappingA, CreateFileA, CopyFileA, CloseHandle, RtlZeroMemory, CreateToolhelp۳۲Snapshot, MapViewOfFile, SetErrorMode,
shell۳۲.dll	ShellExecuteA,
advapi۳۲.dll	LookupPrivilegeValueA, CryptReleaseContext, CryptImportKey, CryptGenKey, CryptDestroyKey, CryptDecrypt, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, CryptAcquireContextA, AdjustTokenPrivileges, OpenProcessToken, RegCloseKey, CryptExportKey, CryptEncrypt,
comctl۳۲.dll	InitCommonControls,
mpr.dll	WNetEnumResourceA, WNetOpenEnumA, WNetCloseEnum,

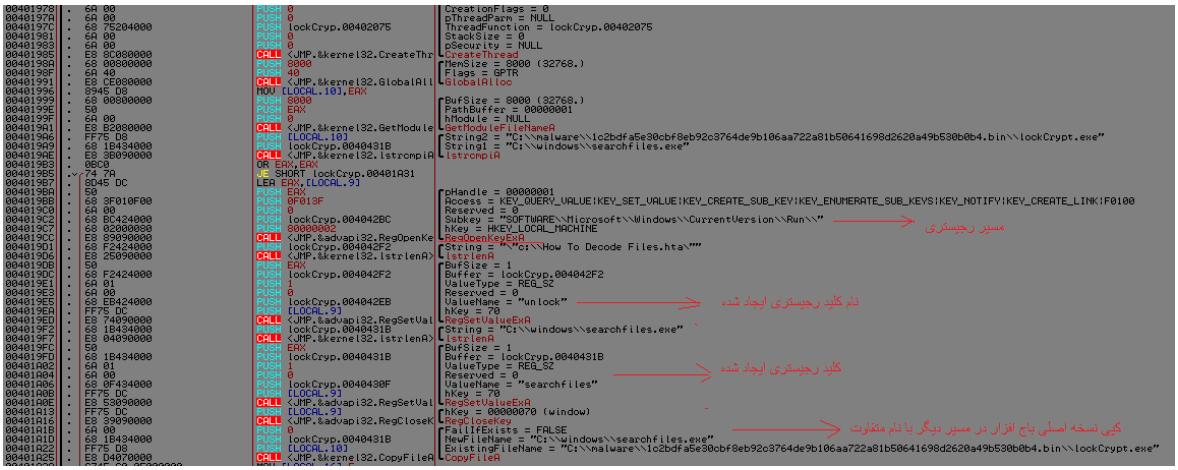
توابع استفاده شده درساختار ایستا فایل LockCrypt احتمال فعالیت‌های مشکوک Dropper و IATHook را نشان می‌دهد.

۵ تحلیل کد فایل LockCrypt

بررسی دستورات LockCrypt در محیط دیباگ نتایج زیر را نشان می‌دهد:

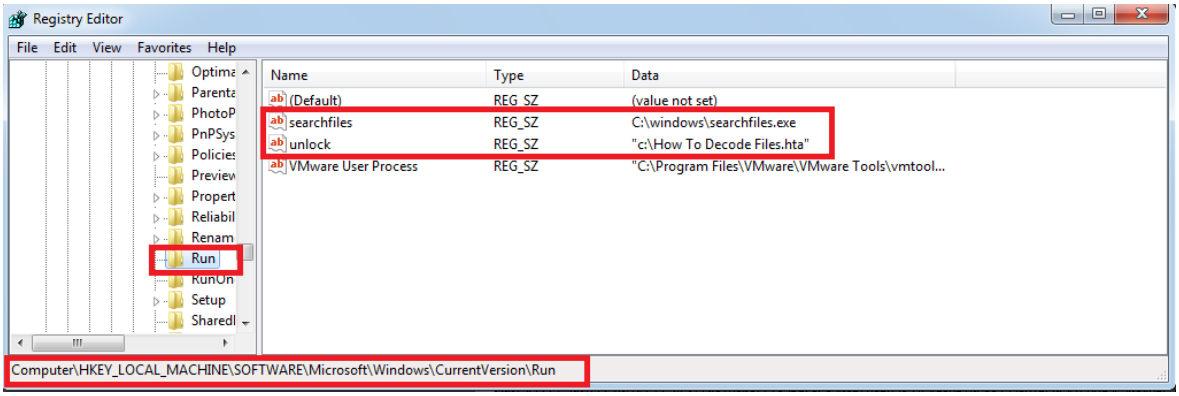
۵–۱ Set نمودن کلیدهای جدید در رجیستری

قطعه کد ۱ بخشی از دستورات اجرای lockCrypt است که نشان می‌دهد این باج‌افزار در مسیر رجیستری HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\Run ، دو کلید جدید با نام های serchfile و unlock ایجاد می‌کند. مقادیر این کلیدها فایل‌هایی به ترتیب با نام searchfile که کپی از نسخه اصلی باج‌افزار است و How to Decode Files.hta است. در مواقع هدف باج‌افزار اجرا مجدد فایل بدافزاری و پیام باج خواهی بعد در هنگام شروع مجدد سیستم است.



قطعه کد ۱- کدهای مربوط به ایجاد کلیدهای رجیستری جدید در سیستم قربانی

همان‌طور که در شکل ۱۱ مشاهده می‌شود پیگیری مسیر رجیستری وجود کلیدها با مقادیر ذکر شده را نیز نشان می‌دهد.



شکل ۹- کلیدهای ایجاد شده در مسیر رجیستری

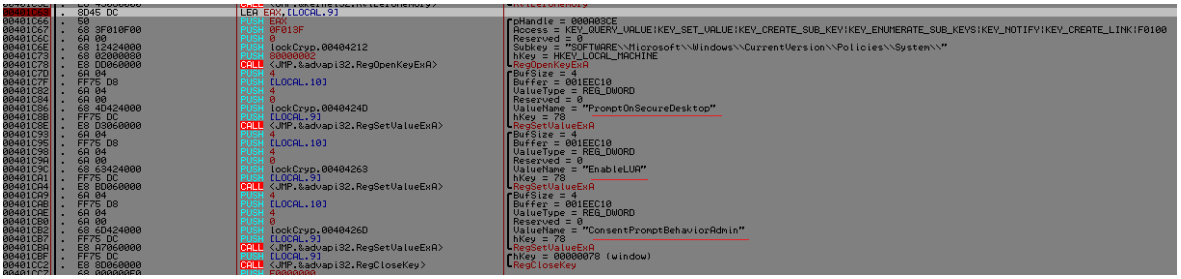
شکل ۱۲ بررسی درهم‌ساز MD۵ فایل searchfile.exe را نشان می‌دهد که مشخص می‌سازد فایل مذکور کپی ار نسخه اصلی فایل باج‌افزار است.

شکل ۱۰- مشخصات فایل Searchfile.exe

۵-۲ اعمال تغییرات در User Account Contorl

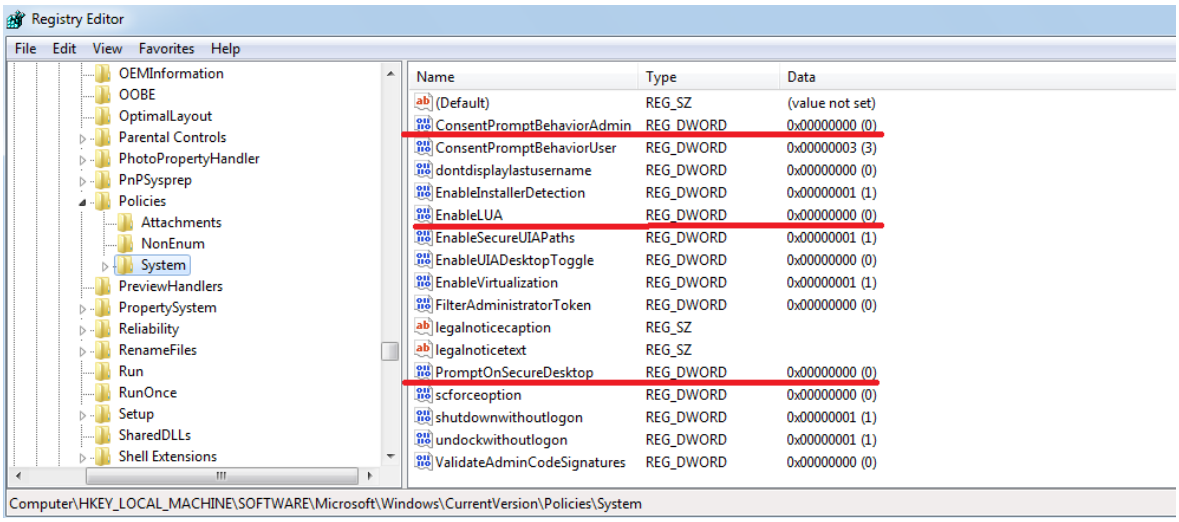
قطعه کد ۲ نشان می‌دهدکه مهاجم تلاش می‌کند تغییراتی را UAC سیستم قربانی از طریق رجیستری زیر ایجاد کند.

- HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\Policies\system



قطعه کد ۲- ایجاد تغییرات در UAC سیستم قربانی

در قطعه کد فوق تغغیرات در سه کلید رجیستری PromptOnSecureDesktop، EnableLUA ، ConsentPromptBehaviorAdmin دیده می‌شود. شکل ۱۳ مقادیر این کلیدهای رجیستری را نشان می‌دهد.

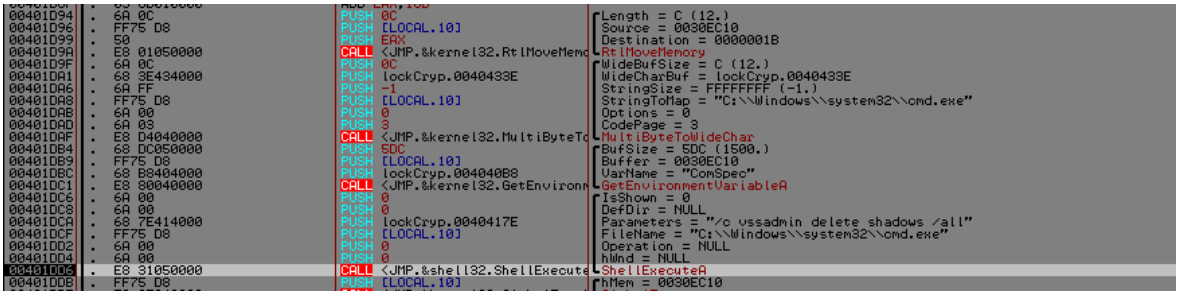


شکل ۱۱- مقادیر کلیدهای رجیستری

شکل فوق نشان می‌دهد هشدارهای مربوط به اجرا با اختیارات Admin فرآیندی در سیستم غیرفعال گردیده است.

۳-۵ حذف فایل های Volume Shadow Copy

همانطور که در قطعه کد ۳ نشان داده شده است فایل مورد تحلیل، تلاش می‌کند با فراخوانی فرآیند vssadmin با دستور delete shadows /all ، کلیه فایل‌های volume shadow copy را پاک نماید به این ترتیب قربانی قادر نخواهد بود از قابلیت perviosu version ویندوز برای بازیابی فایل‌های خود استفاده نماید.



قطعه کد ۳- استفاده از vssadmin جهت پاک کردن volume Shadow Copy

۶ ویژگی های فایل LockCrypt براساس تحلیل پویا

برخی از ویژگی‌های مربوط به تحلیل پویا مانند رجیستری ها و با بررسی ابزارهای تحلیل فایل‌اجرایی در محیط آزمایشگاه این نتایج از رفتار بدافزار از زمان اجرا تا اتمام فرایند رمزگذاری بدست‌آمده است.

۶-۱ کتابخانه های بارگذاری شده

جدول ۴ لیست کتابخانه‌هایی که در زمان اجرای باج‌افزار بارگذاری می‌شود، را نشان می‌دهد.

جدول ۴- لیست کتابخانه‌های بارگذاری شده

لیست کتابخانه‌های بارگذاری شده
• C:\Windows\System۳۲\ntdll.dll • C:\Windows\System۳۲\kernel۳۲.dll • C:\Windows\System۳۲\KERNELBASE.dll • C:\Windows\System۳۲\user۳۲.dll • C:\Windows\System۳۲\gdi۳۲.dll • C:\Windows\System۳۲\lpk.dll • C:\Windows\System۳۲\usp۱۰.dll • C:\Windows\System۳۲\msvcrt.dll • C:\Windows\System۳۲\shell۳۲.dll • C:\Windows\System۳۲\shlwapi.dll • C:\Windows\System۳۲\advapi۳۲.dll • C:\Windows\System۳۲\sechost.dll • C:\Windows\System۳۲\rpcrt۴.dll • C:\Windows\winsxs\x۸۶_microsoft.windows.common-controls_۶۵۹۵b۶۴۱۴۴ccf۱df_۵.۸۲.۷۶۰۱.۱۷۵۱۴_none_ec۸۳dffa۸۵۹۱۴۹af\comctl۳۲.dll • C:\Windows\System۳۲\mpr.dll

- C:\Windows\System۳۲\imm۳۲.dll
- C:\Windows\System۳۲\msctf.dll

۶-۲ اطلاعات شبکه

در بررسی ها ارتباطات شبکه‌ای خاصی یافت نشد.

۷ روند پاک سازی

برای پاک‌سازی سیستم ابتدا بایستی اجرای را متوقف نمود می‌توان از طریق Task Manager اقدام کرد و سپس با یک آنتی‌ویروس قانونی سیستم را پویش نمود.

در مرحله دوم برای بازیابی فایل‌های قربانی در صورتی که قبلا از سیستم نسخه پشتیبانی‌ای در cloud تهیه شده باشد، می‌توان از طریق Safe Mode With Networking یا بازیابی از طریق System Restore اقدام کرد.

۸ روش های پیشگیری

- اطمینان از تهیه نسخه پشتیبان
- استفاده از آنتی‌ویروسی که دارای تشخیص رفتار است
- نصب به‌روزرسانی‌های سیستم‌عامل
- بروز نگه داشتن برنامه‌ها
- اعمال فیلترهای SPAM
- فعال کردن مشاهده پسوند برنامه‌ها
- تغییر نام Vssadmin در ویندوز
- غیر فعال کردن اسکریپت ویندوز
- غیرفعال کردن Windows PowerShell
- استفاده از کلمات عبور قوی

- غیرفعال کردن Remote Desktop یا تغییر پورت آن
- راه اندازی سیاست های محدودیت نرم افزار در ویندوز