باسمه تعالی

تحلیل فنی باج‌افزار LockCryptV۲

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام LockCryptV۲ خبر می‌دهد. طبق مشاهدات صورت گرفته، به نظر می‌رسد که این باج‌افزار از خانواده ی باج افزار Satan می‌باشد و پس از رمزگذاری فایل‌ها پسوند BDKR. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند و نام فایل را نیز طبق الگوی خاص تغییر می‌دهد. بررسی‌ها نشان می‌دهد که این باج‌افزار در ۲۳ سپتامبر سال ۲۰۱۸ میلادی به روز رسانی شده است. این باج‌افزار از الگوریتم رمزنگاری RSA-۲۰۴۸ + AES-۲۵۶ استفاده می‌کند.

مشخصات فایل اجرایی :

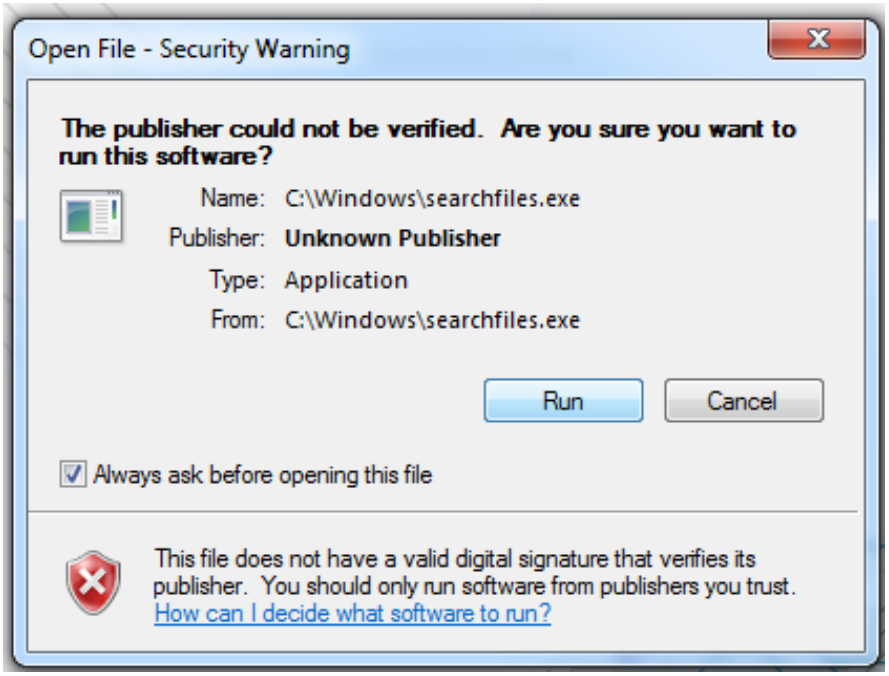
نام فایل	fcr.exe
MD۵	f۱۹۲۷e۷f۹۰۴۱۶bf۳۹fc۷۹۹۱bbc۵۷e۱b۳
SHA-۱	۲۳۶۷۲۴۹۵۶۸ca۴a۳۴f۸۸۲۴a۹۳۱۳b۰۳d۱۶d۱d۷c۰bc
SHA-۲۵۶	۵۳۹b۰b۵d۵۴۷۵۷e۸a۲b۷۵۴ecdc۲۹۳۹eb۷cf۹db۰ed۱۷۲۸e۰eca۴۰۷۵۰۰۲۲۲۶۶۸۵۰۵
اندازه فایل	۱۰ KB
کامپایلر / پکر	

فایل اجرایی این باج‌افزار دارای سه بخش است :

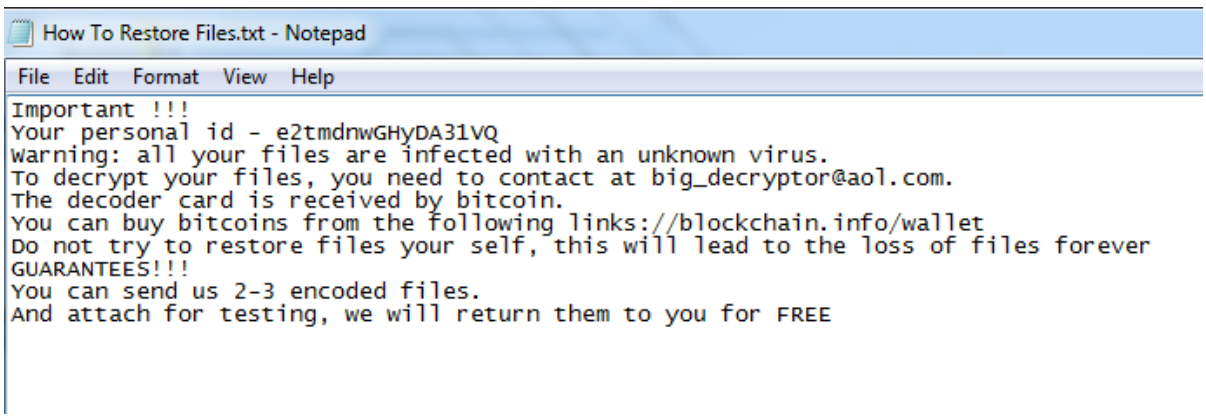
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۵.۵۸۲۸۱۸۳۰۲۸۳	۰x۱۰۰۰	۰x۱۰d۴	۰x۱۲۰۰
.rdata	۴.۳۲۵۶۰۳۵۰۷۹۹	۰x۳۰۰۰	۰x۴cc	۰x۶۰۰
.data	۷.۹۳۳۳۱۳۳۶۰۴۶	۰x۴۰۰۰	۰x۱۳۹۰	۰xc۰۰

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار LockCryptV۲ فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. طبق بررسی‌های صورت گرفته، باج‌افزار LockCryptV۲ پس از اجرا از شروع فعالیت برخی فرآیندها جلوگیری می کند. تمام فایل های موجود در سیستم، رمزگذاری شده و فعالیت تمام نرم افزارهای گشوده شده را به پایان می‌رساند. حین اجرا فرآیند searchfiles.exe شروع به فعالیت می کند :



سپس پیغام باج‌خواهی گشوده می‌شود که این پیغام در تمامی فولدرهای رمزگذاری شده و رمزگذاری نشده نیز وجود دارد. تصویر زیر پیغام باج‌خواهی باج‌افزار را که به نام How To Restore Files.txt !!! می باشد را نشان می‌دهد.



بر اساس پیغام باج‌خواهی، در ابتدای آن شناسه ۱۶ کارکتری قربانی را مشخص کرده که در نام

تمام فایل های رمزگذاری شده نیز تکرار شده است. در ادامه اشاره شده که تمام فایل های سیستم قربانی توسط ویروسی ناشناخته آلوده شده است. سپس مهاجم برای برقراری ارتباط آدرس ایمیل big_decryptor@aol.com را نیز تعیین نموده است. در تصویر زیر پاسخ مهاجم به ایمیل ارسال شده را مشاهده می‌کنید که در آن تقاضای پرداخت ۲ بیت‌کوین را دارد.

Hi! to restore the files you need to pay a ransom of 2 bitcoins
Our bitcoin address 12bz7q9GYJRGxLQAneVU3baXCv4fdhDBua
Encrypt a screenshot of the transaction confirmation
After receiving the foreclosure, we will send you a utility decoder
Here are our recommendations:
If you have no Bitcoin address register https://blockchain.info/wallet
fill up your wallet some of the ways
Btcdirect.eu - Good service for Europe
Bittylicious.com - Bitcoins through Visa / MC or through SEPA (EC) transfer
Localbitcoins.com - Here you can find people who want to sell Bitcoins
directly (WU, in cash, SEPA, Paypal u.s.).
Cex.io - buy bitcoins with Visa / Mastercard or Wire Transfer.
Coincafe.com - Designed for quick and easy service. Payment methods:
Western Union, Bank of America, cash by FedEx, Moneygram, as money
transfer
Bitstamp.net - well known and established Bitcoins seller
Coinmama.com - Visa / Mastercard
Btc-e.com - Bitcoins vendor (Visa / Mastercard, etc.)
If you have not found any bitcoins in your region, try to find them here:
Buybitcoinworldwide.com - International Bicoins Exchange Directory
Bitcoin-net.com - Another directory of Bitcoins sellers
Howtobuybitcoins.info - International Bicoins Exchange Directory
Bittybot.co/eu - Directory for countries of the European Union
write to Google how to buy Bitcoin in your country?

big decryptor
big_decryptor@aol.com

همچنین آدرس کیف پول زیر را در پیغام باج خواهی به قربانی معرفی می‌کند:

۱۲bz۷q۹GYJRGxLQAneVU۳baXCv٤fdhDBua

طبق بررسی های صورت گرفته این کیف پول تاکنون حال هیچ تراکنشی نداشته است.

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	12bz7q9GYJRGxLQAneVU3baXCv4fdhDBua
Hash 160	1195f2af688a97953ff480a46daa653f4dcc53a0

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment | Donation Button

پس از رمزگذاری، باج افزار پسوند فایل های رمزگذاری شده را به .BDKR تغییر می‌دهد و انتهای نام فایل‌ها را نیز طبق الگوی زیر تغییر می‌دهد :

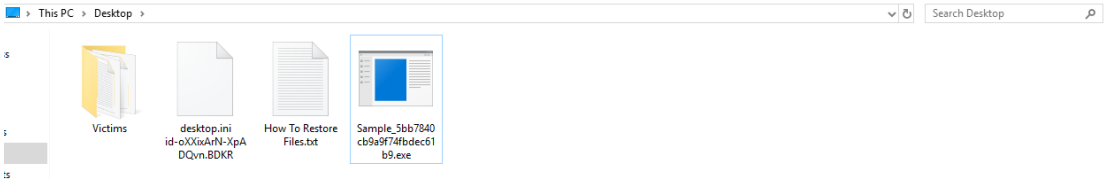
.BDKR + (آی دی قربانی) + (-)+ id + (فاصله) + (نام فایل و پسوند فایل)

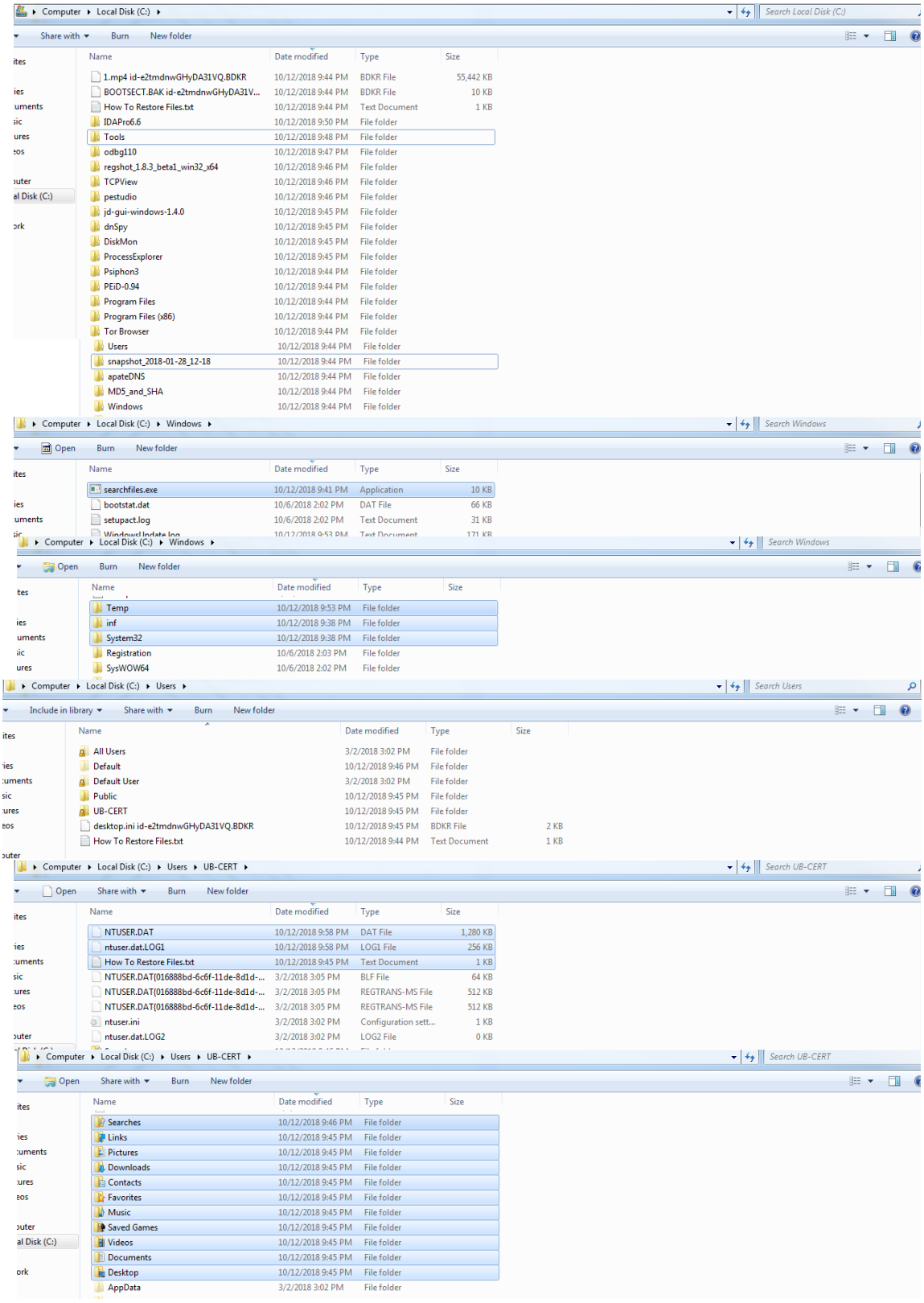
1 (4).png id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:47 PM	BDKR File	200 KB
1 (46).jpg id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:47 PM	BDKR File	329 KB
1.pot id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:47 PM	BDKR File	243 KB
2 O'clock Spotlight.ple id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:48 PM	BDKR File	23 KB
03_01_layout.mov id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:46 PM	BDKR File	10,075 KB
4_5854862790426099907.mp4 id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:48 PM	BDKR File	1,421 KB
73 - www.farsbooks.mihanblog.com.rar id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:48 PM	BDKR File	985 KB
adlink_7582.html id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:48 PM	BDKR File	2 KB
adsutil.vbs id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	16 KB
analytics.js id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	28 KB
AppLocker.psd1 id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	3 KB
AppxBlockMap.xml id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	2 KB
ar-SA_BitLockerToGo.exe.mui id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	10 KB
bb.jpeg id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	1,542 KB
BEH AARAMI.PPt id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	536 KB
berme.doc id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	130 KB
bg-BG_BitLockerToGo.exe.mui id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	10 KB
Block.bat id-e2tmdnwGHyDA31VQ.BDKR	10/12/2018 9:49 PM	BDKR File	3 KB

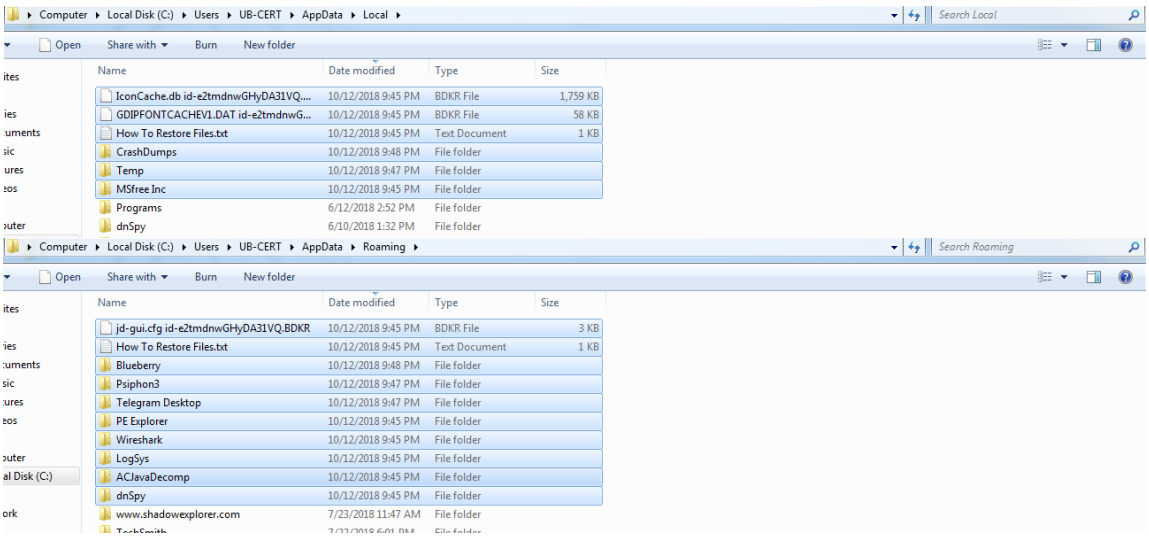
طبق آزمایش‌های صورت گرفته، تمام فایل های قربانی حتی فایل های سیستمی مانند ntdetect.com, ntldr, boot.ini و ... رمزگذاری می شوند:

PNG .PSD .PSPIMAGE .TGA .THM .TIF .TIFF .YUV .AI .EPS .PS .SVG .INDD .PCT .PDF .XLR .XLS .XLSX .ACCDB .DB .DBF .MDB .PDB .SQL .APK .APP .BAT .CGI .COM .EXE .GADGET .JAR .PIF .WSF .DEM .GAM .NES .ROM .SAV CAD Files .DWG .DXF GIS Files .GPX .KML .KMZ .ASP .ASPX .CER .CFM .CSR .CSS .HTM .HTML .JS .JSP .PHP .RSS .XHTML. DOC .DOCX .LOG .MSG .ODT .PAGES .RTF .TEX .TXT .WPD .WPS .CSV .DAT .GED .KEY .KEYCHAIN .PPS .PPT .PPTX ..INI .PRF Encoded Files .HQX .MIM .UUE . ٧Z .CBR .DEB .GZ .PKG .RAR .RPM .SITX .TAR.GZ .ZIP .ZIPX .BIN .CUE .DMG .ISO .MDF .TOAST .VCD SDF .TAR .TAX ٢٠١٤.TAX ٢٠١٥.VCF .XML Audio Files .AIF .IFF .M ٣U .M ٤A .MID .MP ٣.MPA .WAV .WMA Video Files . ٣G ٢. ٣GP .ASF .AVI .FLV .M ٤V .MOV .MP ٤.MPG .RM .SRT .SWF .VOB .WMV ٣D . ٣DM . ٣DS .MAX .OBJ R.BMP .DDS .GIF .JPG ..CRX .PLUGIN .FNT .FON .OTF .TTF .CAB .CPL .CUR .DESKTHEMEPACK .DLL .DMP .DRV .ICNS .ICO .LNK .SYS .CFG ,...

این باج افزار، فایل اجرایی خود را در انتها پاک کرده و همچنین فایل های موجود در recycle bin را حذف می‌کند. در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows پس از اجرای باج‌افزار را مشاهده می‌کنید :

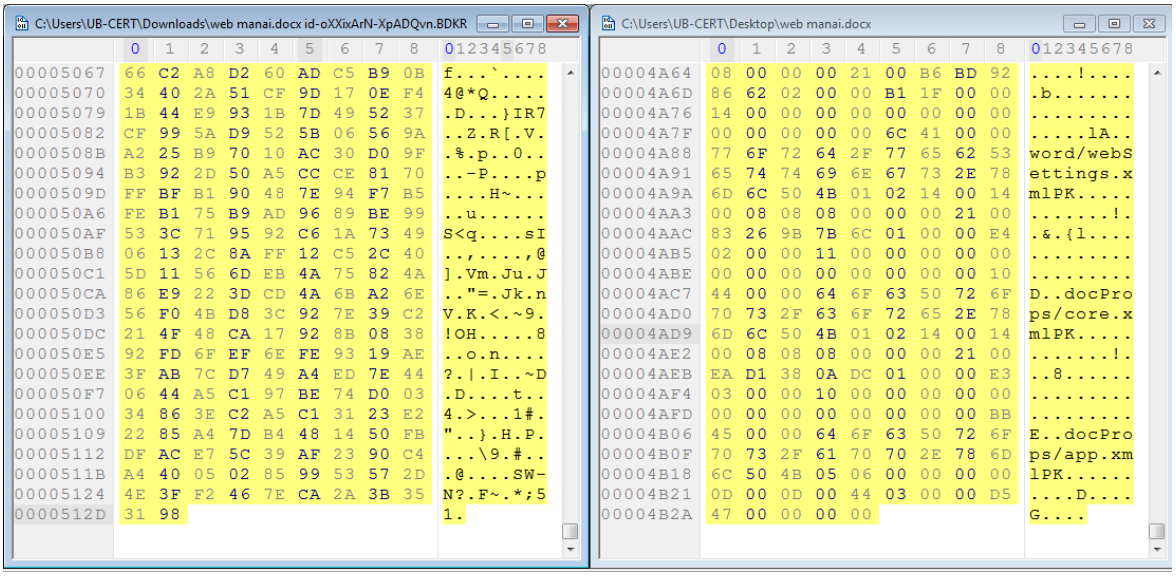



Computer ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Share with ▾ Burn New folder
Name Date modified Type Size
1.mp4 id-e2tmdnwGHyDA31VQ.BDKR 10/12/2018 9:44 PM BDKR File 55,442 KB
BOOTSECT.BAK id-e2tmdnwGHyDA31V... 10/12/2018 9:44 PM BDKR File 10 KB
How To Restore Files.txt 10/12/2018 9:44 PM Text Document 1 KB
IDAPro6.6 10/12/2018 9:50 PM File folder
Tools 10/12/2018 9:48 PM File folder
odbg110 10/12/2018 9:47 PM File folder
regshot_1.8.3_beta1_win32_x64 10/12/2018 9:46 PM File folder
TCPView 10/12/2018 9:46 PM File folder
pestudio 10/12/2018 9:46 PM File folder
jd-gui-windows-1.4.0 10/12/2018 9:45 PM File folder
dnSpy 10/12/2018 9:45 PM File folder
DiskMon 10/12/2018 9:45 PM File folder
ProcessExplorer 10/12/2018 9:45 PM File folder
Psiphon3 10/12/2018 9:44 PM File folder
PEiD-0.94 10/12/2018 9:44 PM File folder
Program Files 10/12/2018 9:44 PM File folder
Program Files (x86) 10/12/2018 9:44 PM File folder
Tor Browser 10/12/2018 9:44 PM File folder
Users 10/12/2018 9:44 PM File folder
snapshot_2018-01-28_12-18 10/12/2018 9:44 PM File folder
apateDNS 10/12/2018 9:44 PM File folder
MD5_and_SHA 10/12/2018 9:44 PM File folder
Windows 10/12/2018 9:44 PM File folder
Computer ▸ Local Disk (C:) ▸ Windows ▸
Search Windows
Open Burn New folder
searchfiles.exe 10/12/2018 9:41 PM Application 10 KB
bootstat.dat 10/6/2018 2:02 PM DAT File 66 KB
setupact.log 10/6/2018 2:02 PM Text Document 31 KB
Temp 10/12/2018 9:53 PM File folder
inf 10/12/2018 9:38 PM File folder
System32 10/12/2018 9:38 PM File folder
Registration 10/6/2018 2:03 PM File folder
SysWOW64 10/6/2018 2:02 PM File folder
Computer ▸ Local Disk (C:) ▸ Users ▸
Search Users
Include in library ▾ Share with ▾ Burn New folder
All Users 3/2/2018 3:02 PM File folder
Default 10/12/2018 9:46 PM File folder
Default User 3/2/2018 3:02 PM File folder
Public 10/12/2018 9:45 PM File folder
UB-CERT 10/12/2018 9:45 PM File folder
desktop.ini id-e2tmdnwGHyDA31VQ.BDKR 10/12/2018 9:45 PM BDKR File 2 KB
How To Restore Files.txt 10/12/2018 9:44 PM Text Document 1 KB
Computer ▸ Local Disk (C:) ▸ Users ▸ UB-CERT ▸
Search UB-CERT
Open Share with ▾ Burn New folder
NTUSER.DAT 10/12/2018 9:58 PM DAT File 1,280 KB
ntuser.dat.LOG1 10/12/2018 9:58 PM LOG1 File 256 KB
How To Restore Files.txt 10/12/2018 9:45 PM Text Document 1 KB
NTUSER.DAT{016888bd-6c6f-11de-8d1d-... 3/2/2018 3:05 PM BLF File 64 KB
NTUSER.DAT{016888bd-6c6f-11de-8d1d-... 3/2/2018 3:05 PM REGTRANS-MS File 512 KB
NTUSER.DAT{016888bd-6c6f-11de-8d1d-... 3/2/2018 3:05 PM REGTRANS-MS File 512 KB
ntuser.ini 3/2/2018 3:02 PM Configuration sett... 1 KB
ntuser.dat.LOG2 3/2/2018 3:02 PM LOG2 File 0 KB
Computer ▸ Local Disk (C:) ▸ Users ▸ UB-CERT ▸
Search UB-CERT
Open Share with ▾ Burn New folder
Searches 10/12/2018 9:46 PM File folder
Links 10/12/2018 9:45 PM File folder
Pictures 10/12/2018 9:45 PM File folder
Downloads 10/12/2018 9:45 PM File folder
Contacts 10/12/2018 9:45 PM File folder
Favorites 10/12/2018 9:45 PM File folder
Music 10/12/2018 9:45 PM File folder
Saved Games 10/12/2018 9:45 PM File folder
Videos 10/12/2018 9:45 PM File folder
Documents 10/12/2018 9:45 PM File folder
Desktop 10/12/2018 9:45 PM File folder
AppData 3/2/2018 3:02 PM File folder

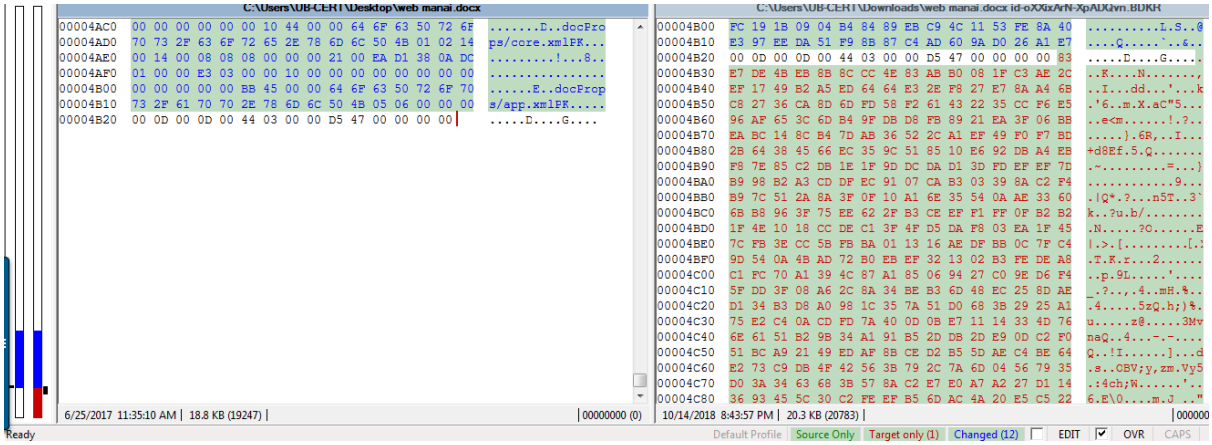


تحلیل ایستا:

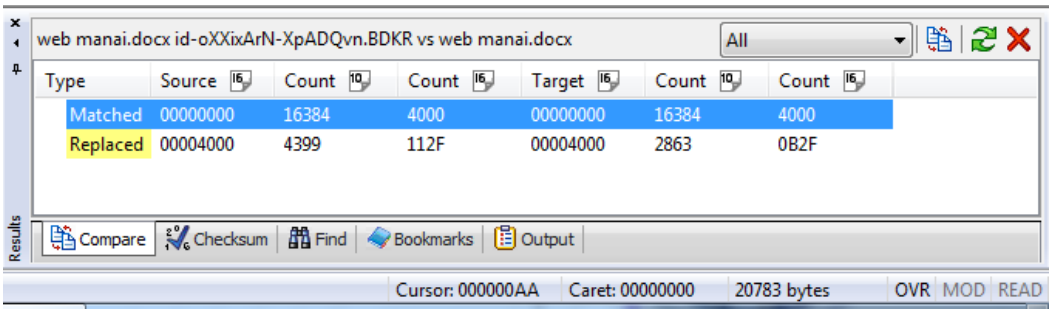
پس از تحلیل کد باج‌افزار LockCryptV۲ به نتایج زیر دست پیدا کردیم. این باج افزار بدون اتصال اینترنت نیز رمزگذاری را انجام می‌دهد. مقایسه نمونه فایل، قبل و بعد از رمزگذاری :



مقایسه نمونه فایل سالم و رمزگذاری شده همسان، نشان می‌دهد که پس از رمزگذاری بیش از دو برابر محتوای اولیه حجم افزوده شده است.



تعداد بایت های جایگزین شده ی نمونه فایل بعد از رمزگذاری:



این باج افزار قادر به رمزگذاری فایل های ویندوزهای چندکاربره می باشد.توانایی رمزگذاری بدون اتصال به اینترنت را دارد.فرآیند sqlbrowser.exe را نیز در حافظه متوقف می کند.

از ویژگی های دیگری که در این نسخه از باج افزار دیده می شود ایجاد فایل های زیر درون حافظه های جانبی مانند CD , DVD ، فلش و... می باشد:

how to restore files.txt - elvisimp.rdf - middaugh_keynote.pptx - stoc ۱۳_ml_quoc_le.pptx
indogerman ۲۰۱۰.pptx - gruenspecht_ ۰۲۱۷۲۰۱۶.pptx - waterresourcesag.pptx - proposaltemplates.ppt - sim_gametheory_to_finance.ppt - writingcompletesarnarrative_ ۱۱۰۳.ppt - metac.ppt

حذف فایل های shadow با اجرای ستورات زیر در خط فرمان سیستم :

```
sc stop VVS
sc stop wscsvc
sc stop WinDefend
sc stop wuauserv
sc stop BITS
sc stop ERSvc
sc stop WerSvc
cmd.exe /C bcdedit /set {default} recoveryenabled No
cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures
C:\Windows\System ۳۲\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet
```

کلید رجیستری اضافه شده:

HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\orsa
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\rsa
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\ConsentPromptBehaviorAdmin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\EnableLUA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\PromptOnSecureDesktop
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\searchfiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\unlock
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند که در جدول زیر قابل مشاهده است :

advapi۳۲.dll	kernel۳۲.dll	kernel۳۲.dll
AdjustTokenPrivileges	CloseHandle	lstrcmpW
CryptAcquireContextA	CopyFileA	lstrcpyW
CryptDecrypt	CreateFileA	lstrlenA
CryptDestroyKey	CreateFileMappingA	lstrlenW
CryptEncrypt	CreateFileW	MapViewOfFile
CryptExportKey	CreateThread	MoveFileW
CryptGenKey	GetEnvironmentVariableA	MultiByteToWideChar
CryptImportKey	GetFileAttributesW	RtlMoveMemory
CryptReleaseContext	GetModuleFileNameA	RtlZeroMemory
LookupPrivilegeValueA	GlobalAlloc	SetFileAttributesW
OpenProcessToken	GlobalFree	SetFilePointerEx
RegCloseKey	GlobalMemoryStatus	SetThreadPriority
RegOpenKeyExA	lstrcatW	Sleep
RegQueryValueExA	lstrcmpiA	UnmapViewOfFile

RegSetValueExA	lstrcmpiW	WriteFile

بر اساس بررسی‌های صورت گرفته، باج‌افزار LockCryptV۲ پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

- *Input Sample* (PID: ۳۵۰۰)
  - cmd.exe /c vssadmin delete shadows /all (PID: ۲۲۶۰)
    - vssadmin.exe vssadmin delete shadows /all (PID: ۲۷۲۸)

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار LockCryptV۲ نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۲ مورد از ۶۸ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Ransom.LockCrypt.7	ALYac	Trojan.Ransom.LockCrypt
Arcabit	Trojan.Ransom.LockCrypt.7	Avast	Win32:Dh-A [Heur]
AVG	Win32:Dh-A [Heur]	Avira	TR/Crypt.ZPACK.Gen
BitDefender	Gen:Variant.Ransom.LockCrypt.7	CAT-QuickHeal	Trojan.IGENERIC
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.f90416
Cylance	Unsafe	Cyren	W32/Trojan.GFBI-5179
DrWeb	Trojan.KillProc.56620	Emsisoft	Gen:Variant.Ransom.LockCrypt.7 (B)
Endgame	malicious (high confidence)	eScan	Gen:Variant.Ransom.LockCrypt.7
ESET-NOD32	a variant of Win32/Filecoder.NPA	F-Secure	Gen:Variant.Ransom.LockCrypt.7
Fortinet	W32/Encoder.NPA!tr.ransom	GData	Gen:Variant.Ransom.LockCrypt.7
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan-Ransom.Win32.Encoder.tr
McAfee	RDN/Generic.hra	McAfee-GW-Edition	RDN/Generic.hra
Microsoft	Ransom:Win32/LockCrypt	NANO-Antivirus	Trojan.Win32.Encoder.fihfeq
Palo Alto Networks	generic.ml	Panda	Generic Malware
Qihoo-360	Win32/Trojan.872	Rising	Ransom.Encoder!8.FFD4 (CLOUD)
Sophos AV	Mal/EncPk-ZC	Sophos ML	heuristic
Symantec	Trojan.Zbot	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_LOCKCRYPT.THOIBDAH	TrendMicro-HouseCall	Ransom_LOCKCRYPT.THOIBDAH
VBA32	TrojanRansom.Encoder	ViRobot	Trojan.Win32.LockCrypt.10240
Webroot	W32.Malware.Gen	ZoneAlarm	Trojan-Ransom.Win32.Encoder.tr

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو مرکز ماهر قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.


پرینت

نام فایل: fcr.bin

حجم فایل: ۱۰ کیلوبایت

تاریخ اسکن: ۲۰ مهر ۱۳۹۷ - ۲۲:۳۵

MD5: f1927e7f90416bf39fc7991bbc57e1b3

SHA1: 2367249568ca4a34f8824a9313b03d16d1d7c0bc

SHA256: 539b0b5d54757e8a2b754ecdc2939eb7cf9db0ed1728e0eca407500222668505

وضعیت:

نتیجه اسکن fcr.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	ii	Dangerous: Mal/EncPk-ZC
f_secure	11.00	ii	Dangerous: Gen:Variant.Ransom.LockCrypt.3
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.Win32.Encoder.Tr
eset	4.5.3.38914	ii	Dangerous: Win32/Filecoder.NPA
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.KillProc.56620
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Gen:Variant.Ransom.LockCrypt.3
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan.Zbot