بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه‌ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

تحلیل بد افزار LockBit Ransomware

گزارش تحلیل بدافزار

شناسه سند	Maher_13990407-1
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۴/۰۵
طبقه‌بندی سند	عادی

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

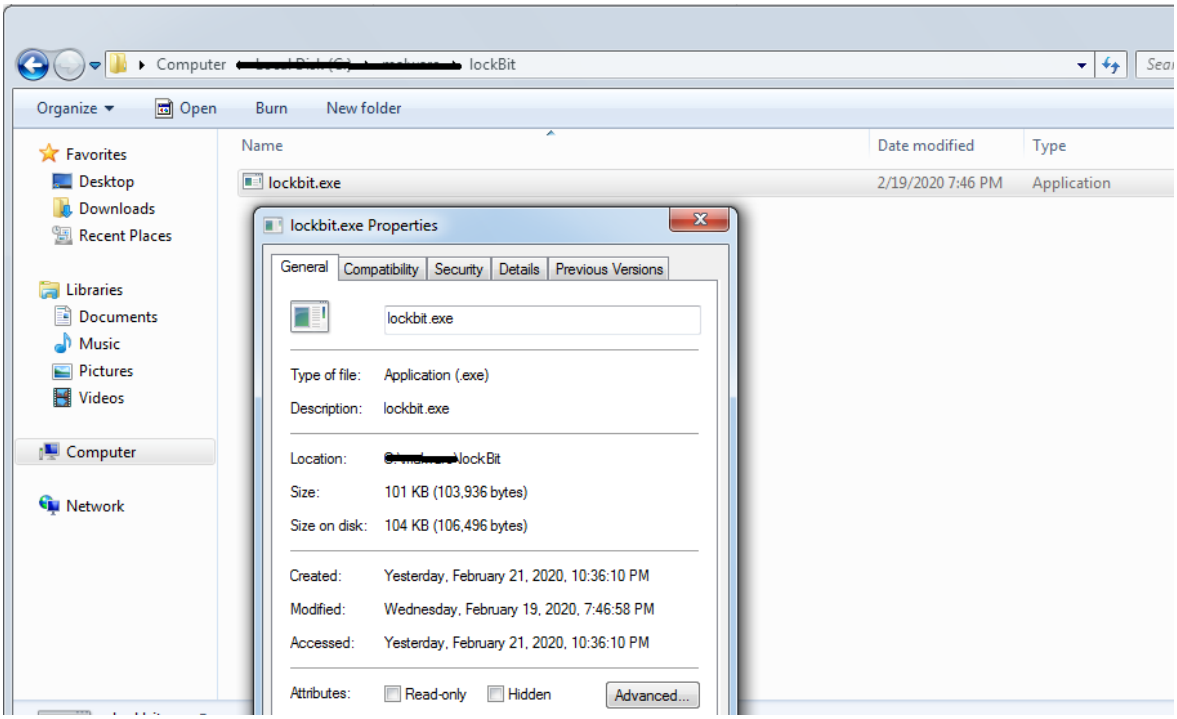
(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ معرفی بدافزار

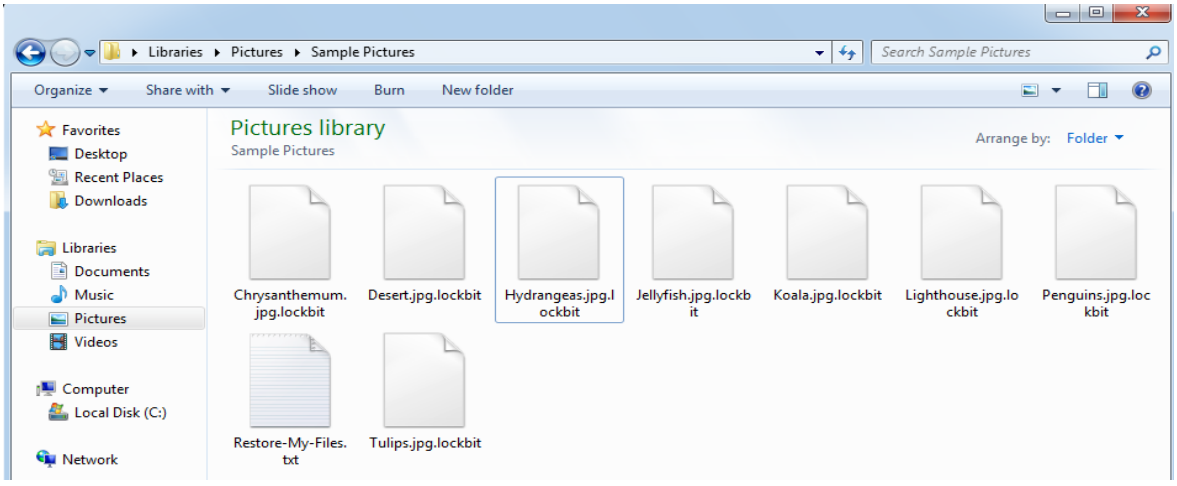
بدافزار LockBit با اندازه ۱۰۲ کیلوبایت در تاریخ ۲۳ Jan سال ۲۰۲۰ ایجاد شده است. این بدافزار فایل‌های کاربر را در ساختاری به صورت زیر رمز می‌کند. شکل ۱ آیکون مربوط به بدافزار را نشان می‌دهد.

Filename.extension.lockbit



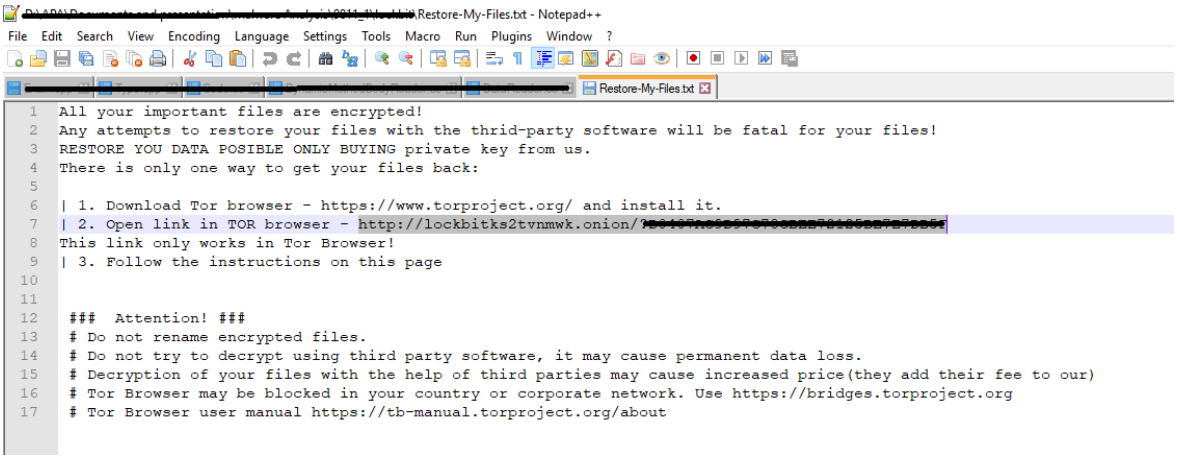
شکل ۱- آیکون فایل lockbit

شکل ۲ نمونه فایل‌های رمزگذاری شده توسط بدافزار را نشان می‌دهد.



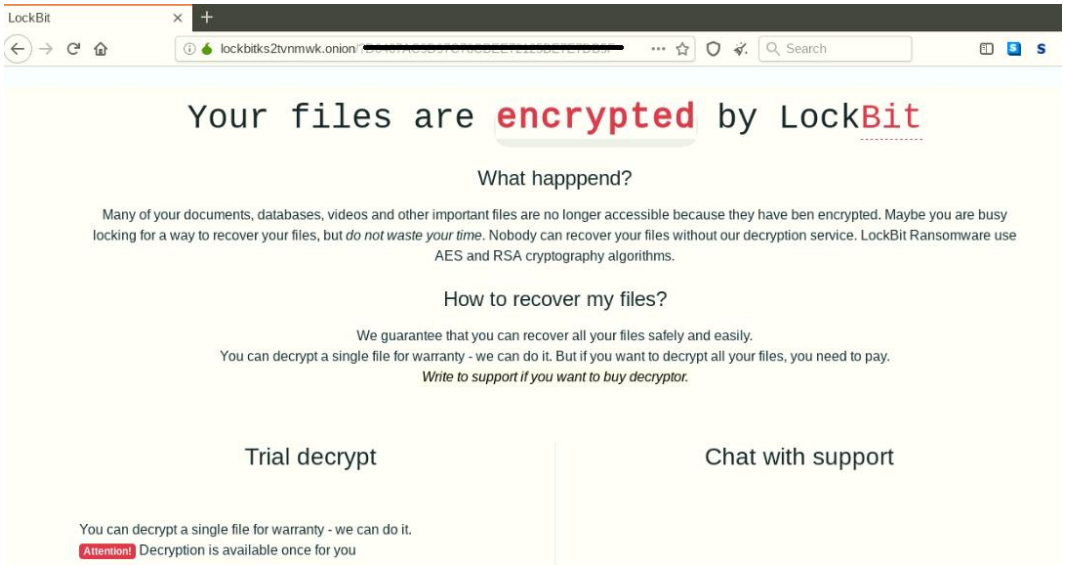
شکل ۲- نمونه فایل‌های رمزگذاری شده

باج‌افزار lockbit با در هر پوشه‌ای که فایل‌های آن را رمز کرد، فایل متنی با نام Restore-My-Files.txt ایجاد می‌کند. شکل ۳ محتوای فایل متنی را نشان می‌دهد.



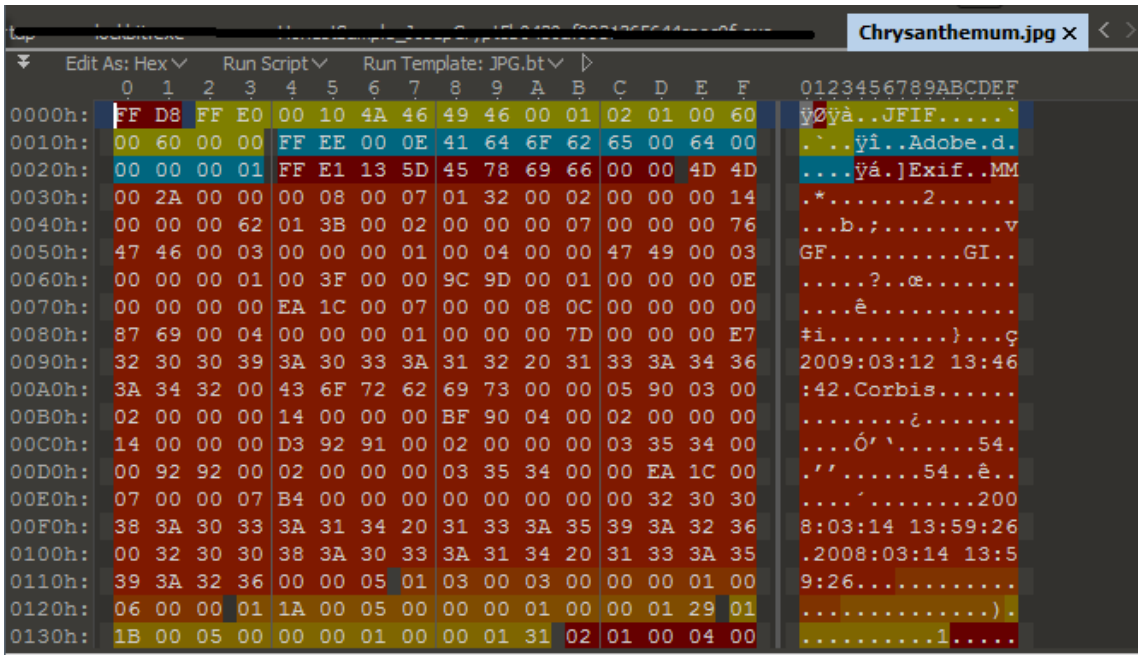
شکل ۳- محتوای فایل متنی باج‌افزار برای قربانی

با مراجعه به لینکی که فایل متنی در اختیار قربانی قرار داده است صفحه‌ای همانند شکل ۴ مشاهده می‌شود. در این صفحه اشاره شده است که فایل‌های قربانی با الگوریتم AES و RSA رمزشده است. مجرم جهت اطمینان‌بخشی به قربانی یکی از فایل‌ها lockbit. با اندازه دقیقا ۲۵۶ کیلوبایت را رمزگشایی می‌کند.

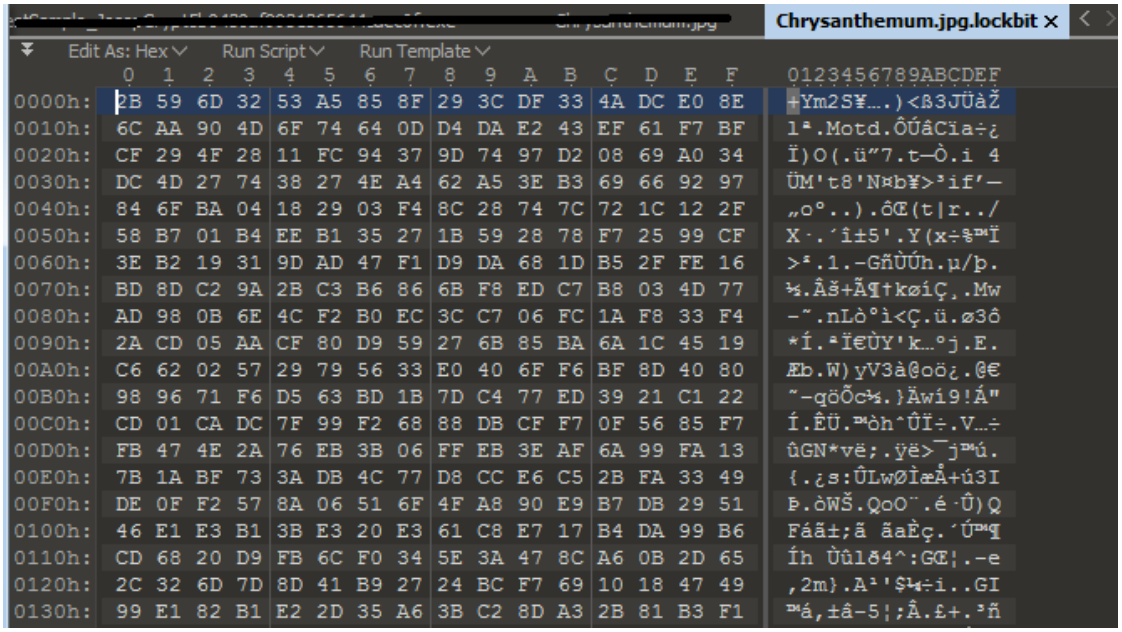


شکل ۴- صفحه لینک موجود در فایل متنی

شکل ۵ و ۶ ساختار هگزادسیمال نمونه‌ای از فایل رمزشده (یک فایل تصویری) را در دو زمان مختلف (قبل از اجرای بدافزار و بعد از اجرای بدافزار) را نشان می‌دهد.



شکل ۵- هگزا دسیمال فایل اجرائی دلخواه قبل از رمزگذاری بدافزار



شکل ۶- محتوای نمونه فایل اجرائی بعد از رمزگذاری

۲ مشخصات فایل

مشخصات کلی و بخش‌های مختلف باج‌افزار lockbit به شرح زیر است:

۲-۱ کلیات فایل lockbit

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 lockbit

نام فایل	lockbit
MD5	889328e2cf5f5d74531b9b0a25c1871c
SHA-256	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f
SHA-1	d14a6e699a1f0805bd1248c80c2dc9dfccf0f403
حجم فایل	102کیلو بایت
زمان کامپایل	Thu Jan 23 16:27:42 2020
تعداد بخش ها	3

۲-۲ Sectionهای مختلف فایل lockbit

جدول ۲ مشخصات Sectionهای فایل lockbit را نشان می‌دهد.

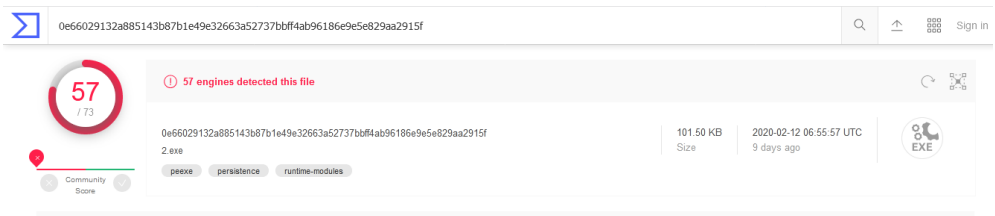
جدول ۲- مشخصات Sectionهای مختلف فایل lockbit

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Characteristic
.text	4096	77955	78336	6.46	6876089ea17286e0700bd2559add683d	CNT_CODE, MEM_EXECUTE, MEM_READ
.rdata	86016	24016	24064	7.08	1e76f111ca7f9984186428b770be19ff	CNT_INITIALIZED_DATA, MEM_READ
.data	110592	9028	512	4.60	60f58202fbbe2ba4ab8dd79524fd3230	CNT_INITIALIZED_DATA, MEM_READ, MEM_WRITE

اختلاف بین اندازه دخیره شده بر روی دیسک و اندازه در نظر گرفته شده در حافظه برای section سوم (.data) و همچنین عدم وجود section ریسورس‌ها احتمال رفتار بدافزاری فایل را افزایش می‌دهد.

۲-۳ بررسی سطح تهدید فایل lockbit

بررسی‌ها نشان می‌دهد که از تعداد ۷۳ موتور آنتی‌ویروس موجود در سامانه VirusTotal، ۵۷ مورد فایل lockbit را بعنوان بدافزار شناسایی کرده‌اند و در این شناسایی نیز برخی از موتورها بدافزار را از خانواده Trojan، Ransomware دانسته‌اند. شکل ۷ نتیجه ارزیابی فایل lockbit با VirusTotal نشان می‌دهد.



شکل ۷ – سطح تهدید فایل lockbit از دیدگاه ویروس توتال

شکل ۸ نیز بررسی سطح تهدید باج‌افزار lockbit را در سامانه ویروس‌کاو در مورخ ۹۸/۱۲/۰۳نشان می‌دهد.

آنتی ویروس	نتیجه اسکن
Avast	Dangerous
Immunet	Clean
Clamwin	Clean
Clamav	Clean
Symantec	Clean
پادویش	Clean
Zillya	Clean
Windefender	Dangerous RansomWin32/LokiBot!MSR
Nanoav	Clean
Kaspersky	Dangerous
Vba32	Clean
Satfaa	Dangerous
Fprot	Clean
Drweb	Clean
Fsecure	Dangerous Gen:Heur.Ransom.Imps.1 Gen:Heur.Ransom.Imps.1
Emsisoft	Dangerous Generic.Ransom.LockBit.91CBD888
Comodo	Clean
Atlantis	Clean
Mcafee	Dangerous RDN/Generic.rp trojan
Escan	undetected
Ikarus	Clean
Adaware	Dangerous Gen:Heur.Ransom.Imps.1
Trustport	Dangerous Generic.Ransom.LockBit.91CBD888
Eset	Dangerous a variant of Win32/Filecoder.NXQ trojan
Gridinsoft	Clean
Avira	Dangerous TR/Crypt.ZPACK.Gen
Sophos	Clean
Bitdefender	Dangerous
ZonerAndroid	Clean
Gdata	Dangerous Generic.Ransom.LockBit.91CBD888 , Win32.Trojan-Ransom.Lockibit.A
TrendMicro	Clean
AviraAndroid	Clean
Cyberbyte	Clean
BitdefenderAndroid	Clean
AvastAndroid	Clean
AvgAndroid	Clean
Winessentials	Clean
FsecureAndroid	Clean
GdataAndroid	Clean
AhnlabAndroid	Clean

شکل ۸- سطح تهدید فایل lockbit از دیدگاه ویروس‌کاو (در تاریخ ۹۸/۱۲/۰۳)

۳ شرح تحلیل

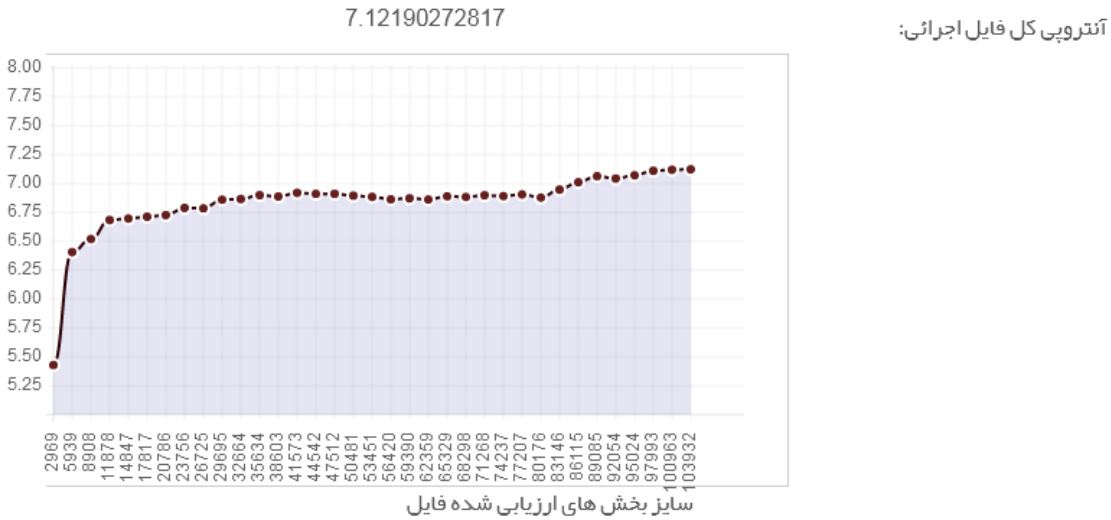
شرح تحلیل باجافزارLockBit در سه قسمت ارائه می‌شود:

۳-۱ بررسی ساختار فایل lockbit بر اساس تحلیل ایستا

در تحلیل استاتیک فایل LockBit ، به بررسی نکاتی در ارتباط با ساختار فایل پرداخته می‌شود:

۳-۱-۱ آنتروپی

روند صعودی و مقدار بیش از ۷ مقدار آنتروپی احتمال رفتار بدافزاری فایل اجرائی را افزایش می‌دهد. شکل ۷ آنتروپی فایل lockbit را نشان می‌دهد که برابر با 7.12 است.



شکل ۹- آنتروپی فایل lockbit

۳-۱-۲ کتابخانه‌ها و توابع استفاده شده

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

جدول ۳- کتابخانه‌ها و توابع استفاده شده

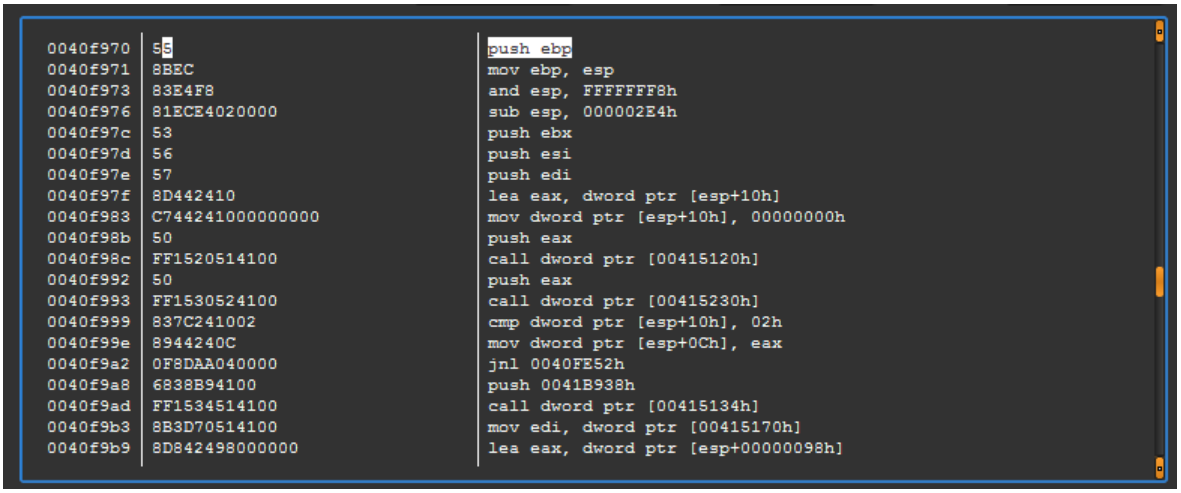
نام کتابخانه	نوابع استفاده شده از آن
NETAPI32.dll	NetShareEnum, NetApiBufferFree,
IPHLPAPI.DLL	GetAdaptersInfo,
WS2_32.dll	htons, ioctlsocket, WSAGetLastError, connect, inet_addr, __WSAFDIsSet, closesocket, select, WSACleanup, WSAStartup, socket,
CRYPT32.dll	CryptBinaryToStringA,
gdiplus.dll	GdipDrawString, GdipCreateStringFormat, GdipDeleteFontFamily, GdipGetImageEncoders, GdipCreateFontFamilyFromName, GdipDeleteBrush, GdipDisposeImage, GdipCreateFont, GdipCreateSolidFill, GdipFillRectangle, GdipG

	etGenericFontFamilySansSerif, GdiplusStartup, GdipGetImageGraphicsContext, GdipGetImageEncodersSize, GdipDeleteGraphics, GdipDeleteStringFormat, GdipDeleteFont, GdipCreateBitmapFromScan0, GdipSaveImageToFile,
SHLWAPI.dll	PathRemoveExtensionA, PathRemoveBackslashW, PathAddBackslashW, StrFormatByteSize64A, PathRemoveFileSpecW, PathFindExtensionW,
MPR.dll	WNetAddConnection2W, WNetOpenEnumW, WNetEnumResourceW, WNetGetConnectionW, WNetCloseEnum,
ntdll.dll	RtlAdjustPrivilege, RtlInitUnicodeString, NtAllocateVirtualMemory, LdrEnumerateLoadedModules, RtlAcquirePebLock, RtlReleasePebLock, memcpy, memset,
msvcrt.dll	malloc, calloc, free,
KERNEL32.dll	QueryDosDeviceW, FindFirstVolumeW, GetModuleFileNameW, lstrcpyW, GetWindowsDirectoryW, lstrcatW, InterlockedPopEntrySList, AllocConsole, GetCurrentProcessId, InitializeSListHead, InterlockedPushEntrySList, lstrcpyA, InterlockedFlushSList, MoveFileW, CreateIoCompletionPort, SystemTimeToFileTime, GetQueuedCompletionStatus, SetFileTime, WriteFile, GetFileSizeEx, ReadFile, SetThreadAffinityMask, FindNextVolumeW, GetVolumePathNamesForVolumeNameW, FindVolumeClose, SetVolumeMountPointW, GetLogicalDrives, FindFirstFileExW, EnterCriticalSection, GetCommandLineW, FindNextFileW, lstrlenW, WaitForMultipleObjects, LeaveCriticalSection, InitializeCriticalSection, FindClose, GetFileAttributesW, ExitThread, OpenProcess, SetFileAttributesW, CreateToolhelp32Snapshot, Sleep, GetLastError, Process32NextW, GetDiskFreeSpaceExW, GlobalAlloc, Process32FirstW, GlobalFree, CloseHandle, CreateThread, DeleteCriticalSection, ExitProcess, GetConsoleWindow, lstrcmpiW, GetDriveTypeW, GetTempPathW, MultiByteToWideChar, GetTempFileNameW, CreateMutexA, OpenMutexA, LoadLibraryA, GetProcAddress, GetTickCount, GetSystemInfo, GetLocalTime, Process32First, TerminateProcess, GetUserDefaultLangID, GetConsoleMode, WaitForSingleObject, GetModuleHandleA, Process32Next, lstrcmpiA, CreateProcessA, lstrcmpW, SetConsoleCtrlHandler, SetConsoleTextAttribute, SetConsoleTitleA, GetStdHandle, WriteConsoleA, SetConsoleMode, SetProcessShutdownParameters, SetErrorMode, CreateFileW,
USER32.dll	PeekMessageW, GetWindowLongA, wvsprintfA, SetWindowLongA, ShowWindow, GetMessageW, CharLowerBuffW, CharUpperA, DeleteMenu, wsprintfW, FlashWindow, wsprintfA, IsWindowVisible, SystemParametersInfoW, GetSystemMetrics, EnableMenuItem, SetLayeredWindowAttributes, RegisterHotKey, ShutdownBlockReasonCreate, GetSystemMenu,
ADVAPI32.dll	RegCreateKeyExA, DuplicateToken, SetThreadToken, OpenProcessToken, RegSetValueExA, RegOpenKeyA, RegCloseKey, RegQueryValueExA, GetAclInformation, GetAce, AllocateAndInitializeSid, AddAce, AddAccessDeniedAce, FreeSid, InitializeAcl, SetSecurityInfo, GetLengthSid, GetSecurityInfo, EnumDependentServicesA, CryptReleaseContext, InitializeSecurityDescriptor, CloseServiceHandle, OpenSCManagerA, GetTokenInformation, ControlService, RegSetValueExW, RegDeleteValueW, QueryServiceStatusEx, RegQueryValueExW, OpenServiceA, AdjustTokenPrivileges, SetFileSecurityW, CryptAcquireContextW, SetSecurityDescriptorOwner, CryptGenRandom, LookupPrivilegeValueA, CreateWellKnownSid, CheckTokenMembership,
SHELL32.dll	SHEmptyRecycleBinW, ShellExecuteExA, ShellExecuteExW, CommandLineToArgvW,
ole32.dll	CoGetObject, CoUninitialize, CoInitializeEx,

بررسی استاتیک توابع استفاده شده در فایل اجرائی مفروض، احتمال فعالیت‌های مخرب RegAPI، Execution، IATHooking ، Downloader را نشان می‌دهد.

۳-۱-۳ تحلیل مقاومتی

بررسی‌ها نشان می‌دهد نقطه شروع فایل اجرائی lockbit برابر با 0x0000f970 است که شکل ۱۰ هگزادسیمال و Disassembly را در نقطه شروع فایل نشان می‌دهد.



شکل ۱۰- هگزادسیمال و Disassembly فایل در نقطه شروع

بررسی امضا نقطه شروع فایل اجرایی lockbit با پایگاه داده‌ای از امضاها، نشان می‌دهد که این بدافزار در زبان C++ نوشته شده است.

۴-۱-۳ بررسی رشته‌ها

جدول ۴ برخی از رشته‌های بکاررفته در باج‌افزار lockbit را نشان می‌دهد.

جدول ۴- رشته‌های بکاررفته در باج‌افزار lockbit

برخی از رشته‌های بکاررفته در lockbit
!This program cannot be run in DOS mode.
Restore-My-Files.txt
Control Panel\Desktop
Global\{02B49784-1CA2-436C-BC08-72FA3956507D}
Global\{BEF590BE-11A6-442A-A85B-656C1081E04C}
SeDebugPrivilege
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
cmd.exe
runas
SOFTWARE\LockBit
\Restore-My-Files.txt
gdiplus.dll
ntdll.dll
$recycle.bin
tor browser
Windows nt
Msbuild
ntuser.dat.log
bootsect.bak
autorun.inf

.386
.cmd, .ani, .msi , msp, .com , .nls, .ocx, .cpl, .hta, .prf, .rdp, .bin, .hlp, .shs , .drv, .wpx, .bat, .msc, .spl, .key, .exe ,.dll, .lnk, .ico, .hlp, .sys, .drv, .cur, .ini, .reg, .mp3,
Boot, system volume information, appdata, Rich, .text, `.rdata, @.data, %S %s total / %s free
. Found FIXED drive %S, . Found REMOTE drive %S [%S]
%ld files encrypted, 19:27:24, WallpaperStyle, TileWallpaper
All your files are encrypted by LockBit, for more information see Restore-My-Files.txt that is located in every encrypted folder
Debug Privilege: OK
OS: Win 10 SRV, OS: Win 10, OS: Win SRV 2012 R2, OS: Win 8.1, OS: Win SRV 2012
OS: Win 8, OS: Win SRV 2008 R2, OS: Win 7, OS: Win SRV 2008, OS: Win Vista, OS: Win XP x64
OS: Win SRV 2003, OS: Win XP, OS: Win 2000, OS: Unknown
Local time: %d.%d %d:%d
PC: %s, Removed autorun key
Service %s stopped
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
supervise
360se
360doctor
Killed process: %s [pid: %ld]
kernel32
/c vssadmin Delete Shadows /All /Quiet, /c bcdedit /set {default} recoveryenabled No
/c bcdedit /set {default} bootstatuspolicy ignoreallfailures, /c wbadmin DELETE SYSTEMSTATEBACKUP, /c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
/c wmic SHADOWCOPY /nointeractive, /c wevtutil cl security
/c wevtutil cl system, /c wevtutil cl application
Volume Shadow Copy & Event log clean
LockBit Ransom
Process created with limited rights

۳-۲ بررسی رفتار lockbit بر اساس تحلیل پویا

فایل اجرائی Lockbit تحت شرایط آزمایشگاهی و بر روی سیستم عامل 7 ، ۳۲ بیتی اجرا گردید و در مدت زمان اجرا نتایج زیر برای تحلیل پویا حاصل شد.

۳-۲-۱ فرآیندهای ایجاد شده

جدول ۵ نشان می‌دهد بدافزار Lockbit در مدت زمان اجرای خود در محیط آزمایشگاهی کدام فرایندها فراخوانی نموده است.

جدول ۵- فرایندهای ایجاد شده

فرایندها و دستورات command line
▪ C:\Windows\System32\cmd.exe ○ C:\Windows\system32\vssadmin.exe ▪ Command line: delete shadows /all /quiet ○ C:\Windows\System32\Wbem\WMIC.exe ▪ Command line: shadowcopy delete ○ C:\Windows\system32\bcdedit.exe

- Command line: /set {default} bootstatuspolicy ignoreallfailures
- C:\Windows\system32\bcdedit.exe
  - Command line: /set {default} recoveryenabled no
- C:\Windows\system32\wbadmin.exe
  - Commad line: delete catalog -quiet

در واقع بدافزار Lockbit با خدفShadow سیستم و فایل‌های Shadowcopy و غیرفعال نمودن تنظیمات پیش‌فرض امکان بازیابی را از قربانی می‌گیرد.

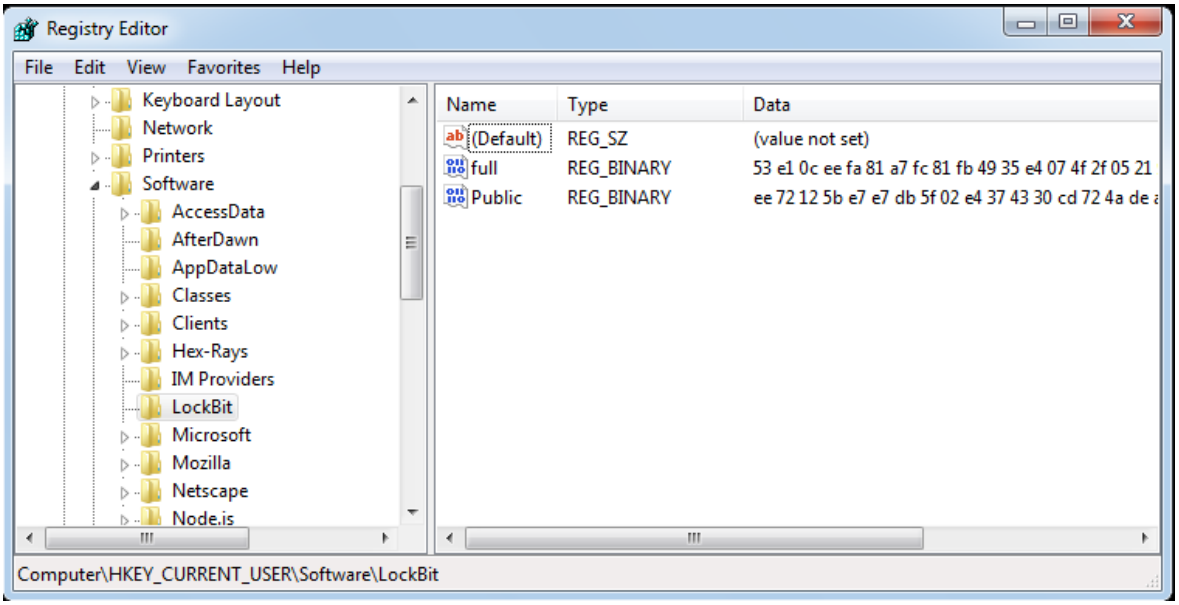
۳-۲-۲ بررسی‌های سطح رجیستری

جدول ۶ بررسی‌های سطح رجیستری فایل اجرائی Lockbit را نشان می‌دهد.

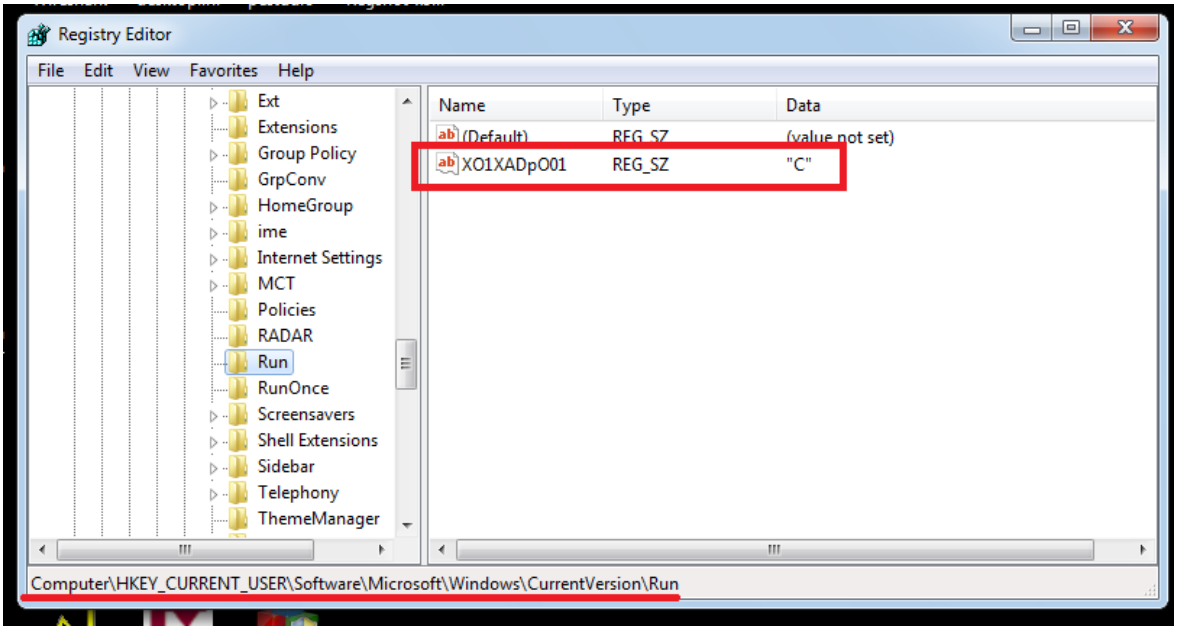
جدول ۶- بررسی سطح رجیستری

Operation	path
RegCreateKey	▪ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ▪ HKCU\SOFTWARE\LockBit ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{7666fdb8-0aa9-11e8-a917-806e6f6e6963} ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket ▪ HKLM\Software\Microsoft\WBEM\CIMOM ▪ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings ▪ HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0 ▪ HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\16000009
RegSetValue	▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Run\XO1XADpO01 ▪ HKCU\Software\LockBit\full ▪ HKCU\Software\LockBit\Public ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\DefaultIcon\(Default) ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet ▪ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ ▪ ZoneMap\AutoDetect ▪ HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0\Element

شکل‌های ۱۱ و ۱۲ قرار گرفتن کلید LockBit در بخش Current User و Set نمودن مقادیر برای کلید رجیستری run را در سیستم قربانی نشان می‌دهد.



شکل ۱۱- ایجاد کلید lockbit در رجیستری سیستم قربانی



شکل ۱۲- قرار گرفتن در بخش run رجیستری

۳-۲-۳ بررسی‌های کتابخانه‌های بارگذاری شده

جدول ۷ کتابخانه‌های بارگذاری شده در زمان اجرا را نشان می‌دهند.

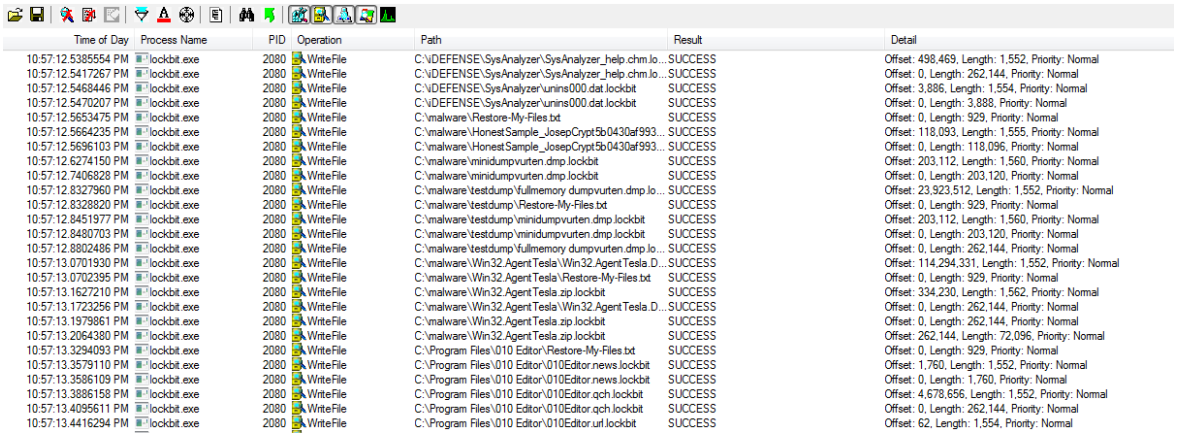
جدول ۷- کتابخانه‌های بارگذاری شده

کتابخانه‌های بارگذاری شده
• C:\Windows\System32\ntdll.dll • C:\Windows\System32\kernel32.dll • C:\Windows\System32\KernelBase.dll • C:\Windows\System32\netapi32.dll • C:\Windows\System32\netutils.dll • C:\Windows\System32\msvcrt.dll • C:\Windows\System32\srvcli.dll • C:\Windows\System32\rpcrt4.dll • C:\Windows\System32\wkscli.dll • C:\Windows\System32\IPHLPAPI.DLL • C:\Windows\System32\nsi.dll • C:\Windows\System32\winnsi.dll • C:\Windows\System32\ws2_32.dll • C:\Windows\System32\crypt32.dll • C:\Windows\System32\msasn1.dll • C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll • C:\Windows\System32\user32.dll • C:\Windows\System32\gdi32.dll • C:\Windows\System32\lpk.dll • C:\Windows\System32\usp10.dll • C:\Windows\System32\ole32.dll • C:\Windows\System32\shlwapi.dll • C:\Windows\System32\mpr.dll • C:\Windows\System32\advapi32.dll • C:\Windows\System32\sechost.dll • C:\Windows\System32\shell32.dll • C:\Windows\System32\blb_ps.dll • C:\Windows\System32\RpcRtRemote.dll • C:\Windows\System32\rsaenh.dll • C:\Windows\System32\cryptsp.dll • C:\Windows\System32\clbcatq.dll • C:\Windows\System32\cryptbase.dll • C:\Windows\System32\Wldap32.dll • C:\Windows\System32\ntmarta.dll • C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll • C:\Windows\System32\msctf.dll • C:\Windows\System32\imm32.dll • C:\Windows\System32\credui.dll • C:\Windows\System32\slc.dll • C:\Windows\System32\devobj.dll • C:\Windows\System32\cfgmgr32.dll • C:\Windows\System32\setupapi.dll • C:\Windows\System32\oleaut32.dll • C:\Windows\System32\ntdsapi.dll • C:\Windows\System32\wbem\fastprox.dll

- C:\Windows\System32\wbem\wbemsvc.dll
- C:\Windows\System32\msvcr100.dll
- C:\Program Files\Common Files\microsoft shared\OFFICE15\MSOXMLMF.DLL
- C:\Windows\System32\dwmapi.
- C:\Windows\System32\uxtheme.dll
- C:\Windows\System32\dnsapi.dll
- C:\Windows\System32\mpr.dll
- C:\Windows\System32\vmhgfs.dll
- C:\Windows\System32\version.dll
- C:\Windows\System32\drprov.dll
- C:\Windows\System32\winsta.dll
- C:\Windows\System32\ntlanman.dll
- C:\Windows\System32\davclnt.dll
- C:\Windows\System32\propsys.dll
- C:\Windows\System32\cscapi.dll
- C:\Windows\System32\browcli.dll
- C:\Windows\System32\actxprxy.dll
- C:\Windows\System32\profapi.dll
- C:\Windows\System32\apphelp.dll
- C:\Windows\System32\ieframe.dll
- C:\Windows\System32\psapi.dll
- C:\Windows\System32\oleacc.dll
- C:\Windows\System32\iertutil.dll
- C:\Windows\System32\urlmon.dll
- C:\Windows\System32\wininet.dll
- C:\Windows\System32\sspicli.dll
- C:\Windows\System32\sfc.dll
- C:\Windows\System32\sfc_os.dll
- C:\Windows\System32\vss_ps.dll
- C:\Windows\System32\winbrand.dll
- C:\Windows\System32\atl.dll
- C:\Windows\System32\vsstrace.dll
- C:\Windows\System32\vssapi.dll
- C:\Windows\System32\framedynos.dll
- C:\Windows\System32\wtsapi32.dll
- C:\Windows\System32\secur32.
- C:\Windows\System32\wbem\wbemprox.dll
- C:\Windows\System32\wbemcomn.dll
- C:\Windows\System32\msxml3.dll
- C:\Windows\System32\urlmon.dll

۳-۲-۴ بررسی‌های سطح فایل

شکل ۱۳ نمونه فایل‌های رمزگذاری شده توسط باجافزار Lockbit را نشان می‌دهد.



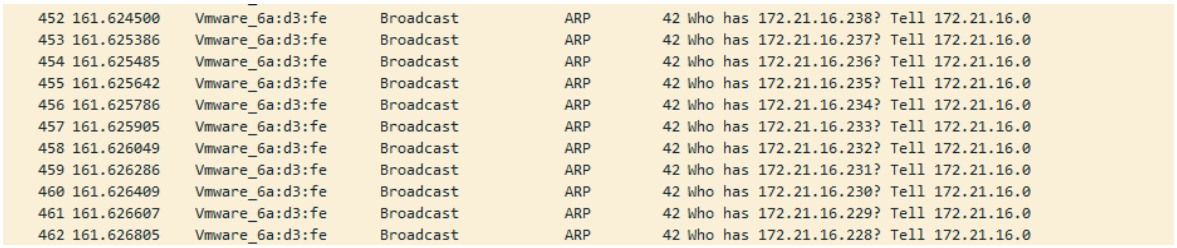
Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:57:12.5385554 PM	lockbit.exe	2080	WriteFile	C:\DEFENSE\SysAnalyzer\SysAnalyzer_help.chm.lo...	SUCCESS	Offset: 498,469, Length: 1,552, Priority: Normal
10:57:12.5417267 PM	lockbit.exe	2080	WriteFile	C:\DEFENSE\SysAnalyzer\SysAnalyzer_help.chm.lo...	SUCCESS	Offset: 0, Length: 262,144, Priority: Normal
10:57:12.5468446 PM	lockbit.exe	2080	WriteFile	C:\DEFENSE\SysAnalyzer\unins000.dat.lockbit	SUCCESS	Offset: 3,886, Length: 1,554, Priority: Normal
10:57:12.5470207 PM	lockbit.exe	2080	WriteFile	C:\DEFENSE\SysAnalyzer\unins000.dat.lockbit	SUCCESS	Offset: 0, Length: 3,888, Priority: Normal
10:57:12.5653475 PM	lockbit.exe	2080	WriteFile	C:\malware\Restore-My-Files.txt	SUCCESS	Offset: 0, Length: 929, Priority: Normal
10:57:12.5664235 PM	lockbit.exe	2080	WriteFile	C:\malware\HonestSample_JosepCrypt5b0430af993...	SUCCESS	Offset: 118,093, Length: 1,555, Priority: Normal
10:57:12.5696103 PM	lockbit.exe	2080	WriteFile	C:\malware\HonestSample_JosepCrypt5b0430af993...	SUCCESS	Offset: 0, Length: 118,096, Priority: Normal
10:57:12.6274150 PM	lockbit.exe	2080	WriteFile	C:\malware\minidumpvurten.dmp.lockbit	SUCCESS	Offset: 203,112, Length: 1,560, Priority: Normal
10:57:12.7406828 PM	lockbit.exe	2080	WriteFile	C:\malware\minidumpvurten.dmp.lockbit	SUCCESS	Offset: 0, Length: 203,120, Priority: Normal
10:57:12.8327960 PM	lockbit.exe	2080	WriteFile	C:\malware\testdump\fullmemory dumpvurten.dmp.lo...	SUCCESS	Offset: 23,923,512, Length: 1,552, Priority: Normal
10:57:12.8328820 PM	lockbit.exe	2080	WriteFile	C:\malware\testdump\Restore-My-Files.txt	SUCCESS	Offset: 0, Length: 929, Priority: Normal
10:57:12.8451977 PM	lockbit.exe	2080	WriteFile	C:\malware\testdump\minidumpvurten.dmp.lockbit	SUCCESS	Offset: 203,112, Length: 1,560, Priority: Normal
10:57:12.8480703 PM	lockbit.exe	2080	WriteFile	C:\malware\testdump\minidumpvurten.dmp.lockbit	SUCCESS	Offset: 0, Length: 203,120, Priority: Normal
10:57:12.8802486 PM	lockbit.exe	2080	WriteFile	C:\malware\testdump\fullmemory dumpvurten.dmp.lo...	SUCCESS	Offset: 0, Length: 262,144, Priority: Normal
10:57:13.0701930 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla\Win32.AgentTesla.D...	SUCCESS	Offset: 114,294,331, Length: 1,552, Priority: Normal
10:57:13.0702395 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla\Restore-My-Files.txt	SUCCESS	Offset: 0, Length: 929, Priority: Normal
10:57:13.1627210 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla.zip.lockbit	SUCCESS	Offset: 334,230, Length: 1,562, Priority: Normal
10:57:13.1723256 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla\Win32.AgentTesla.D...	SUCCESS	Offset: 0, Length: 262,144, Priority: Normal
10:57:13.1979861 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla.zip.lockbit	SUCCESS	Offset: 0, Length: 262,144, Priority: Normal
10:57:13.2064380 PM	lockbit.exe	2080	WriteFile	C:\malware\Win32.AgentTesla.zip.lockbit	SUCCESS	Offset: 262,144, Length: 72,096, Priority: Normal
10:57:13.3294093 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\Restore-My-Files.txt	SUCCESS	Offset: 0, Length: 929, Priority: Normal
10:57:13.3579110 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\010Editor.news.lockbit	SUCCESS	Offset: 1,760, Length: 1,552, Priority: Normal
10:57:13.3586109 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\010Editor.news.lockbit	SUCCESS	Offset: 0, Length: 1,760, Priority: Normal
10:57:13.3886158 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\010Editor.qch.lockbit	SUCCESS	Offset: 4,678,656, Length: 1,552, Priority: Normal
10:57:13.4095611 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\010Editor.qch.lockbit	SUCCESS	Offset: 0, Length: 262,144, Priority: Normal
10:57:13.4416294 PM	lockbit.exe	2080	WriteFile	C:\Program Files\010 Editor\010Editor.url.lockbit	SUCCESS	Offset: 62, Length: 1,554, Priority: Normal

شکل ۱۳- نمونه فایل‌های رمزگذاری شده توسط Lockbit

۳-۲-۵ بررسی سطح شبکه

فعالیت‌های سطح شبکه ای Lockbit در مدت زمانی که در شرایط آزمایشگاهی اجرا گردید به شرح زیر است.

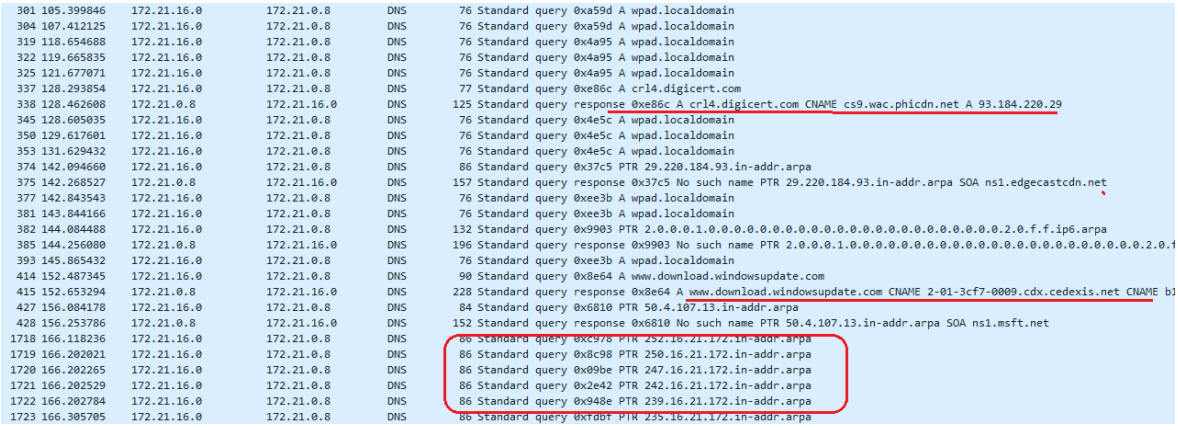
- پروتکل ARP :



```
452 161.624500   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.238? Tell 172.21.16.0
453 161.625386   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.237? Tell 172.21.16.0
454 161.625485   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.236? Tell 172.21.16.0
455 161.625642   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.235? Tell 172.21.16.0
456 161.625786   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.234? Tell 172.21.16.0
457 161.625905   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.233? Tell 172.21.16.0
458 161.626049   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.232? Tell 172.21.16.0
459 161.626286   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.231? Tell 172.21.16.0
460 161.626409   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.230? Tell 172.21.16.0
461 161.626607   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.229? Tell 172.21.16.0
462 161.626805   Vmware_6a:d3:fe   Broadcast   ARP   42 Who has 172.21.16.228? Tell 172.21.16.0
```

شکل ۱۴- پروتکل ARP

- پروتکل DNS :



```
301 105.399846   172.21.16.0   172.21.0.8    DNS    76 Standard query 0xa59d A wpad.localdomain
304 107.412125   172.21.16.0   172.21.0.8    DNS    76 Standard query 0xa59d A wpad.localdomain
319 118.654688   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4a95 A wpad.localdomain
322 119.665835   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4a95 A wpad.localdomain
325 121.677071   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4a95 A wpad.localdomain
337 128.293854   172.21.16.0   172.21.0.8    DNS    77 Standard query 0xe86c A crl4.digicert.com
338 128.462608   172.21.0.8    172.21.16.0   DNS   125 Standard query response 0xe86c A crl4.digicert.com CNAME cs9.wac.phicdn.net A 93.184.220.29
345 128.605035   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4e5c A wpad.localdomain
350 129.617601   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4e5c A wpad.localdomain
353 131.629432   172.21.16.0   172.21.0.8    DNS    76 Standard query 0x4e5c A wpad.localdomain
374 142.094660   172.21.16.0   172.21.0.8    DNS    86 Standard query 0x37c5 PTR 29.220.184.93.in-addr.arpa
375 142.268527   172.21.0.8    172.21.16.0   DNS   157 Standard query response 0x37c5 No such name PTR 29.220.184.93.in-addr.arpa SOA ns1.edgecastcdn.net
377 142.843543   172.21.16.0   172.21.0.8    DNS    76 Standard query 0xee3b A wpad.localdomain
381 143.844166   172.21.16.0   172.21.0.8    DNS    76 Standard query 0xee3b A wpad.localdomain
382 144.084488   172.21.16.0   172.21.0.8    DNS   132 Standard query 0x9903 PTR 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa
385 144.256080   172.21.0.8    172.21.16.0   DNS   196 Standard query response 0x9903 No such name PTR 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f
393 145.865432   172.21.16.0   172.21.0.8    DNS    76 Standard query 0xee3b A wpad.localdomain
414 152.487345   172.21.16.0   172.21.0.8    DNS    90 Standard query 0x8e64 A www.download.windowsupdate.com
415 152.653294   172.21.0.8    172.21.16.0   DNS   228 Standard query response 0x8e64 A www.download.windowsupdate.com CNAME 2-01-3cf7-0009.cdx.cedexis.net CNAME b1
427 156.084178   172.21.16.0   172.21.0.8    DNS    84 Standard query 0x6810 PTR 50.4.107.13.in-addr.arpa
428 156.253786   172.21.0.8    172.21.16.0   DNS   152 Standard query response 0x6810 No such name PTR 50.4.107.13.in-addr.arpa SOA ns1.msft.net
1718 166.118236  172.21.16.0   172.21.0.8    DNS    86 Standard query 0xc978 PTR 252.16.21.172.in-addr.arpa
1719 166.202021  172.21.16.0   172.21.0.8    DNS    86 Standard query 0x8c98 PTR 250.16.21.172.in-addr.arpa
1720 166.202265  172.21.16.0   172.21.0.8    DNS    86 Standard query 0x09be PTR 247.16.21.172.in-addr.arpa
1721 166.202529  172.21.16.0   172.21.0.8    DNS    86 Standard query 0x2e42 PTR 242.16.21.172.in-addr.arpa
1722 166.202784  172.21.16.0   172.21.0.8    DNS    86 Standard query 0x948e PTR 239.16.21.172.in-addr.arpa
1723 166.305705  172.21.16.0   172.21.0.8    DNS    86 Standard query 0xfdbf PTR 235.16.21.172.in-addr.arpa
```

شکل ۱۵- پروتکل DNS

- پروتکل HTTP

).	Time	Source	Destination	Protocol	Length	Info
	126 34.923750	172.21.16.0	93.184.220.29	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAYN1sHQZ5AbVHX8%2
	129 34.973761	93.184.220.29	172.21.16.0	OCSP	529	Response
	154 44.520261	172.21.16.0	93.184.220.29	HTTP	187	GET /Omniroot2025.crl HTTP/1.1
	162 44.575399	93.184.220.29	172.21.16.0	HTTP	269	HTTP/1.1 200 OK (application/x-pkcs7-crl)
	212 79.971186	172.21.16.0	93.184.220.29	HTTP	305	GET /sha2-assured-cs-g1.crl HTTP/1.1
	241 80.129762	93.184.220.29	172.21.16.0	HTTP	78	HTTP/1.1 200 OK (application/x-pkcs7-crl)
	289 104.245269	172.21.16.0	93.184.220.29	HTTP	403	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1DlgCEAxTltyylJxw%2BsSKs1
	291 104.369070	93.184.220.29	172.21.16.0	OCSP	853	Response
	342 128.516066	172.21.16.0	93.184.220.29	HTTP	309	GET /DigiCertAssuredIDRootCA.crl HTTP/1.1
	344 128.568861	93.184.220.29	172.21.16.0	HTTP	970	HTTP/1.1 200 OK (application/x-pkcs7-crl)
	419 152.701726	172.21.16.0	13.107.4.50	HTTP	357	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
	421 152.746695	13.107.4.50	172.21.16.0	HTTP	184	HTTP/1.1 304 Not Modified

شکل ۱۶- پروتکل HTTP

۳-۳ بررسی کد

شکل‌های ۱۷ و ۱۸ و ۱۹ ایجاد و استفاده از مقادیرکلید رجیستری LockBit توسط باجافزار را نمایش می‌دهد.

```
004117B9  .  0F1145 CA        MOVUPS DQWORD PTR SS:[EBP-36],XMM0
004117BD  .  66:C745 DA 6F00  MOV WORD PTR SS:[EBP-26],6F
004117C3  >  884D C8          MOV CL,BYTE PTR SS:[EBP-36]
004117C6  .  304C05 CB        XOR BYTE PTR SS:[EBP+EAX-35],CL
004117CA  .  40               INC EAX
004117CB  .  83F8 10          CMP EAX,10
004117CE  .^ 72 F3            JB SHORT lockbit.004117C3
004117D0  .  8D45 AC          LEA EAX,DWORD PTR SS:[EBP-54]
004117D3  .  C645 DB 00       MOV BYTE PTR SS:[EBP-25],0
004117D7  .  50               PUSH EAX                                 ; pDisposition = 0012FBEB
004117D8  .  8D45 E8          LEA EAX,DWORD PTR SS:[EBP-18]
004117DB  .  50               PUSH EAX                                 ; pHandle = 0012FBEB
004117DC  .  6A 00            PUSH 0                                   ; pSecurity = NULL
004117DE  .  68 3F000F00      PUSH 0F003F                              ; Access = KEY_ALL_ACCESS
004117E3  .  6A 00            PUSH 0                                   ; Options = REG_OPTION_NON_VOLATILE
004117E5  .  6A 00            PUSH 0                                   ; Class = NULL
004117E7  .  6A 00            PUSH 0                                   ; Reserved = 0
004117E9  .  8D45 CB          LEA EAX,DWORD PTR SS:[EBP-35]
004117EC  .  50               PUSH EAX                                 ; Subkey = "SOFTWARE\\LockBit"
004117ED  .  68 01000080      PUSH 80000001                            ; hKey = HKEY_CURRENT_USER
004117F2  .  FF15 00504100    CALL DWORD PTR DS:[<&ADVAPI32.RegCreateKeyExA>]  ; RegCreateKeyExA
004117F8  .  85C0             TEST EAX,EAX
004117FA  .v 0F85 E9010000    JNZ lockbit.004119E9
00411800  .  B4 3D            MOV AH,3D
```

شکل ۱۷- ایجادکلید رجیستری LockBit

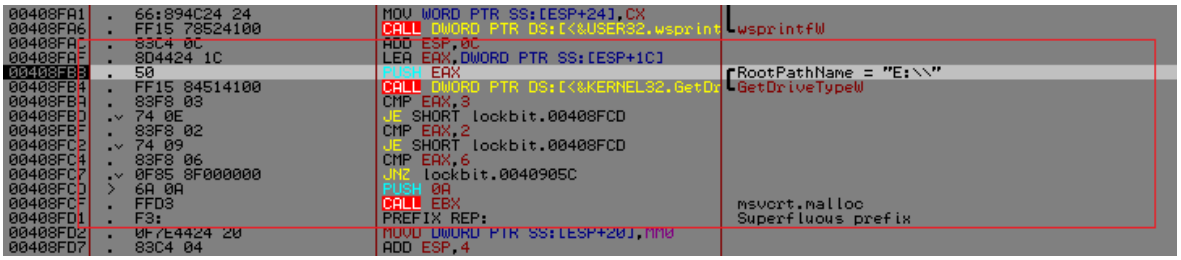
```
00411828  .  32DC             XOR BL,AH
0041182A  .  8855 F9          MOV BYTE PTR SS:[EBP-7],DL
0041182D  .  B1 48            MOV CL,48
0041182F  .  885D FA          MOV BYTE PTR SS:[EBP-6],BL
00411832  .  32CC             XOR CL,AH
00411834  .  8D45 E4          LEA EAX,DWORD PTR SS:[EBP-1C]
00411837  .  50               PUSH EAX                                 ; pBufSize = 0012FC17
00411838  .  68 90CA4100      PUSH lockbit.0041CA90                    ; Buffer = lockbit.0041CA90
0041183D  .  8D45 B0          LEA EAX,DWORD PTR SS:[EBP-50]
00411840  .  884D F8          MOV BYTE PTR SS:[EBP-8],CL
00411843  .  50               PUSH EAX                                 ; pValueType = 0012FC17
00411844  .  6A 00            PUSH 0                                   ; Reserved = NULL
00411846  .  8D45 F7          LEA EAX,DWORD PTR SS:[EBP-9]
00411849  .  50               PUSH EAX                                 ; ValueName = "full"
0041184A  .  FF75 E8          PUSH DWORD PTR SS:[EBP-18]               ; hKey = 154
0041184D  .  FF15 1C504100    CALL DWORD PTR DS:[<&ADVAPI32.RegQueryValueExA>]  ; RegQueryValueExA
00411853  .  8BF0             MOV ESI,EAX
00411855  .  C645 F5 00       MOV BYTE PTR SS:[EBP-B],0
00411859  .  B6 35            MOV DH,35
```

شکل ۱۸- استفاده از مقدار کلید رجیستری

```
00411874  .  B1 40            MOV CL,40
00411876  .  8865 F3          MOV BYTE PTR SS:[EBP-D],AH
00411879  .  B2 57            MOV DL,57
0041187B  .  8D45 E4          LEA EAX,DWORD PTR SS:[EBP-1C]
0041187E  .  B5 56            MOV CH,56
00411880  .  50               PUSH EAX                                 ; pBufSize = 0012FC0F
00411881  .  FF75 FC          PUSH DWORD PTR SS:[EBP-4]                ; Buffer = 00392CC8
00411884  .  8D45 B0          LEA EAX,DWORD PTR SS:[EBP-50]
00411887  .  B3 59            MOV BL,59
00411889  .  50               PUSH EAX                                 ; pValueType = 0012FC0F
0041188A  .  6A 00            PUSH 0                                   ; Reserved = NULL
0041188C  .  8D45 EF          LEA EAX,DWORD PTR SS:[EBP-11]
0041188F  .  32CE             XOR CL,DH
00411891  .  50               PUSH EAX                                 ; ValueName = "Public"
00411892  .  FF75 E8          PUSH DWORD PTR SS:[EBP-18]               ; hKey = 154
00411895  .  32D6             XOR DL,DH
00411897  .  884D F0          MOV BYTE PTR SS:[EBP-10],CL
0041189A  .  32DE             XOR BL,DH
0041189C  .  8855 F1          MOV BYTE PTR SS:[EBP-F],DL
0041189F  .  32EE             XOR CH,DH
004118A1  .  885D F2          MOV BYTE PTR SS:[EBP-E],BL
004118B4  .  886D F4          MOV BYTE PTR SS:[EBP-C],CH
004118B7  .  FF15 1C504100    CALL DWORD PTR DS:[<&ADVAPI32.RegQueryValueExA>]  ; RegQueryValueExA
004118BD  .  85F6             TEST ESI,ESI
004118BF  .v 75 04            JNZ SHORT lockbit.004118B5
004118B1  .  85C0             TEST EAX,EAX
004118B3  .v 74 1F            JE SHORT lockbit.004118D4
```

شکل ۱۹ – استفاده از مقدار کلید رجیستری

شکل ۲۰ نشان می‌دهد بدافزار lockbit درایوهای فعال سیستم را جتسجو می‌کند.



شکل ۲۰- جستجوی درایوهای فعال در سیستم

۴ روش‌های پیشگیری

واقعیت این است که باج‌افزارها وجود دارند روزبه روز هم در حال گسترش هستند. حداقل کاری که یک کاربر می‌تواند انجام دهد این است روش‌های پیشگیرانه‌ای در نظر گیرد تا روند باج‌گیری برای مهاجم سخت گردد. در ادامه این مطلب به روش‌های مقابله در برابر باج افزار اشاره می‌شود:

- 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
- پیوست‌ها را باز نکنید مگر با تأیید شخصی که آنرا به شما ارسال کرده است
- مراقبت در اینترنت دانلود
- 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