باسمه تعالی

تحلیل فنی باج افزار Dbger

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی Satan به نام Dbger خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان، کره‌ای زبان و چینی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES برای رمزگذاری استفاده می‌کند و به جز فایل‌هایی با پسوندهای مشخص و دایرکتوری‌هایی خاص که در ادامه به آن‌ها اشاره خواهیم نمود، بقیه فایل‌ها را رمزگذاری می‌کند، و به این دلیل ممکن است برخی از نرم‌افزارهای نصب شده بر روی سیستم قربانی بعد از حمله‌ی باج‌افزار به درستی اجرا نشوند. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

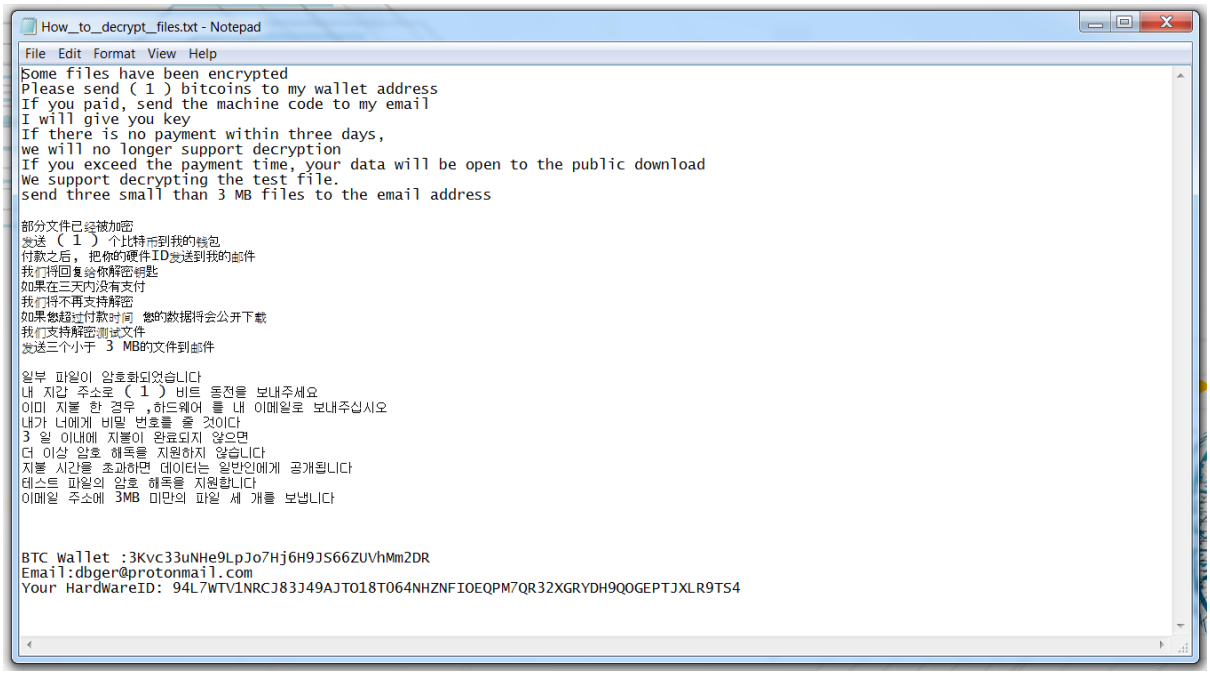
نام فایل	Dbger.exe
MD۵	٤٢١٥bff٤٤fece٨٠٩b٨٥١٦d٣f٠٣٧bc٦٤٥
SHA-١	٤cefe٤٢٦٦٤٢eed٨c٦cec٥f٣fd٩٥٢٠٢٢a٠٧a٠ec١٤
SHA-٢٥٦	٥٠٩٧f١٢d٢٤٢٣c٥٧bb٠e٩f١٠٢٢f٧٧٠٧a٣٢٣١be٥٠bfaf٠b٩dd٤٤c٢٨٤af١bb٣٥٨a٠
اندازه فایل	٤٩٨.٥ KB

فایل اجرایی این باج افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٢٨	٤٠٩٦	٣٥٠٨٦٣	٣٥١٢٣٢
.rdata	٤.٨٤	٣٥٦٣٥٢	١٣٢١٨٦	١٣٢٦٠٨
.data	٣.٣٧	٤٩١٥٢٠	٩٣٧٦	٤٠٩٦
.gfids	٣.٠٢	٥٠٣٨٠٨	٦٩٢	١٠٢٤
.tls	٠.٠٢	٥٠٧٩٠٤	٩	٥١٢
.rsrc	٤.٧٢	٥١٢٠٠٠	٤٨٠	٥١٢
.reloc	٦.٧١	٥١٦٠٩٦	١٩٣٥٢	١٩٤٥٦

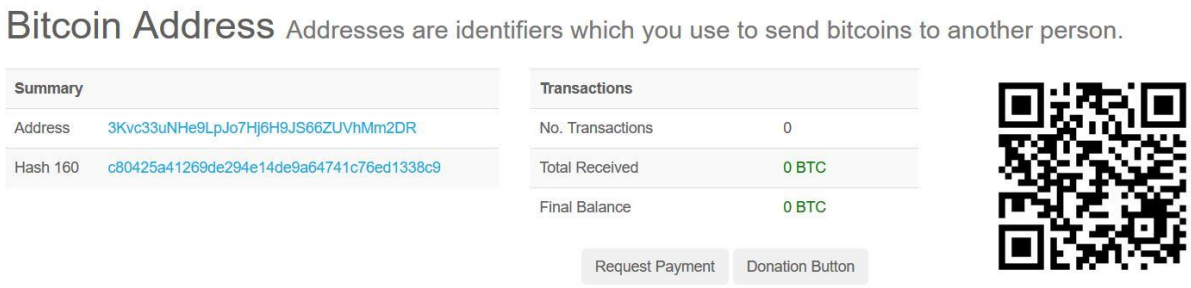
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Dbger، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره فایل‌ها را با استفاده از الگوریتم رمزنگاری AES رمزگذاری کرده و پسوند فایل‌ها را پس از رمزگذاری به dbger. تغییر می‌دهد و همچنین آدرس ایمیل مهاجمین را به ابتدای نام فایل‌های رمزگذاری شده اضافه می‌کند. سپس فرایند مربوط به اجرای باج‌افزار خاتمه پیدا می‌کند و پیغام باج‌خواهی که یک فایل متنی با فرمت TXT تحت عنوان How_to_decrypt_files می‌باشد، بر روی Desktop به نمایش در می‌آید. همچنین یک نسخه از این فایل در کنار فایل‌های رمزگذاری شده قرار می‌گیرد. تصویر زیر پیغام باج‌خواهی باج افزار Dbger را نشان می‌دهد.



بر اساس پیغام باج‌خواهی که به ۳ زبان انگلیسی، کره‌ای و چینی می‌باشد، مهاجمین برای رمزگشایی فایل‌ها، تقاضای پرداخت مبلغ ۱ بیت‌کوین به آدرس ۳Kvc۳۳uNHe۹LpJoVHj٦H۹JS٦٦ZUVhMm۲DR نموده‌اند. پس از پرداخت مبلغ باج، قربانیان باید کد شناسایی خود را که این کد برای هر قربانی منحصربفرد می‌باشد، از طریق آدرس ایمیل dbger@protonmail.com برای مهاجمین ارسال نمایند تا بعد از تایید پرداخت توسط مهاجمین کلید رمزگشایی فایل‌ها در اختیار قربانیان قرار گیرد. مهاجمین برای پرداخت مبلغ باج ۳

روز به قربانیان مهلت داده‌اند. طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افـزار تاکنون تراکنشی نداشته است.

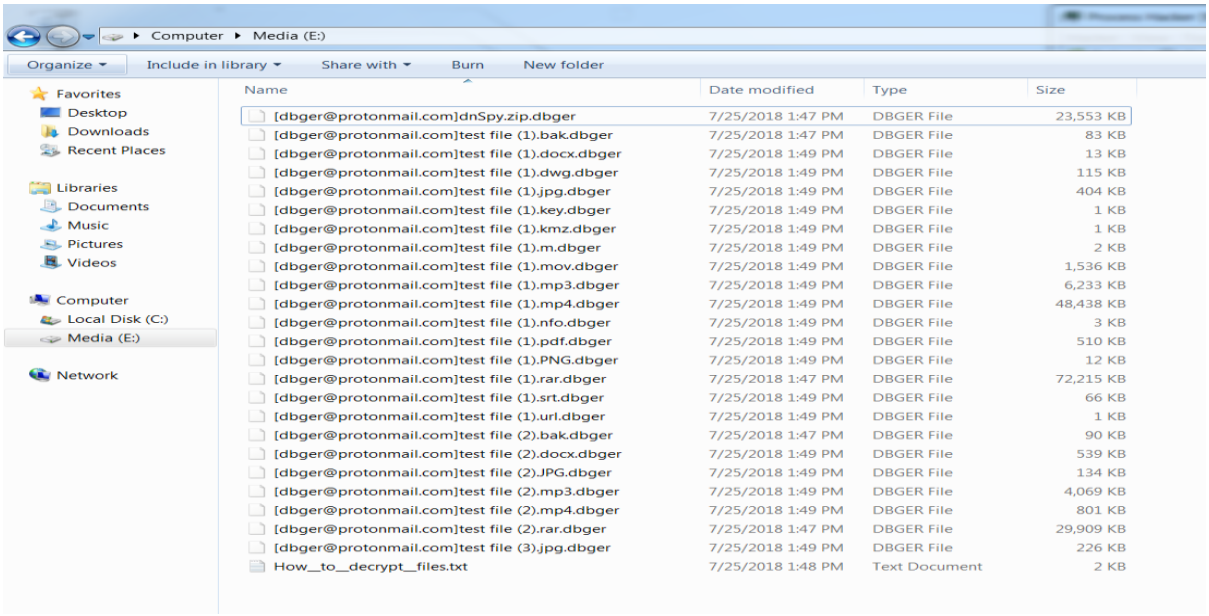

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3Kvc33uNHe9LpJo7Hj6H9JS66ZUVhMm2DR
Hash 160	c80425a41269de294e14de9a64741c76ed1338c9

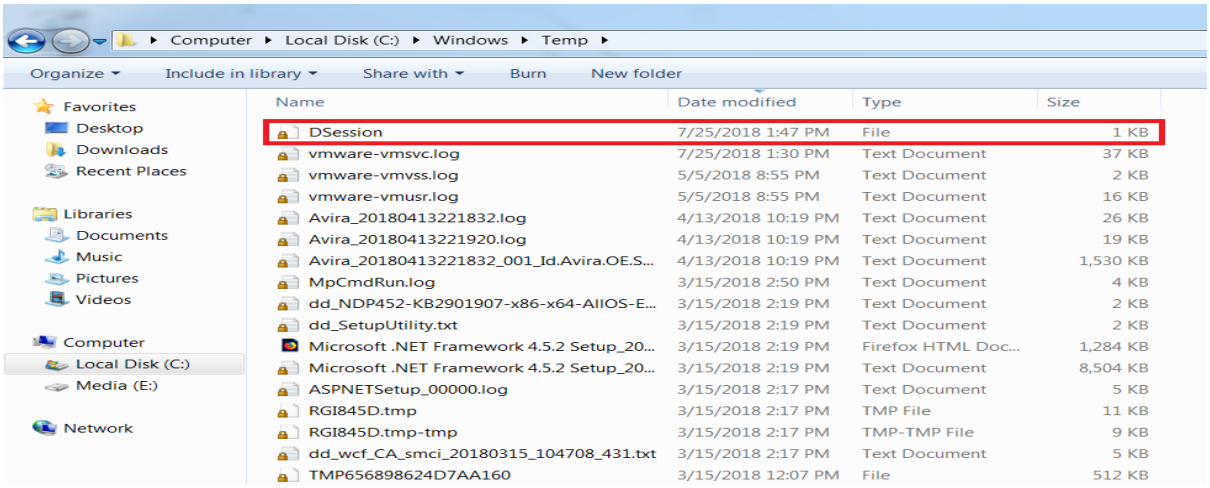
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌هـا، پسـوند آن‌هـا را بـه dbger. تغییـر می‌دهد و آدرس ایمیل مهاجمین را به ابتدای نام فایل‌ها اضافه می‌کند تصـویر زیـر نشـان‌دهنـده فایـل‌هـای رمزگذاری شده توسط این باج افزار می‌باشد :



باج‌افزار Dbger یک فایل با نام DSession در مسیر C:\Windows\Temp ایجاد می‌کند که محتوای آن کـد شناسایی مربوط به قربانی می‌باشد. این فایل در تصویر زیر قابل مشاهده می‌باشد :



همانطور که اشاره شد این باج‌افزار به جز فایل‌هایی با پسوندهای مشخص، باقی فایل‌ها را رمزگذاری می‌نماید. در زیر لیست فایل‌هایی که توسط باج‌افزار رمزگذاری نمی‌شوند، قابل مشاهده می‌باشد :

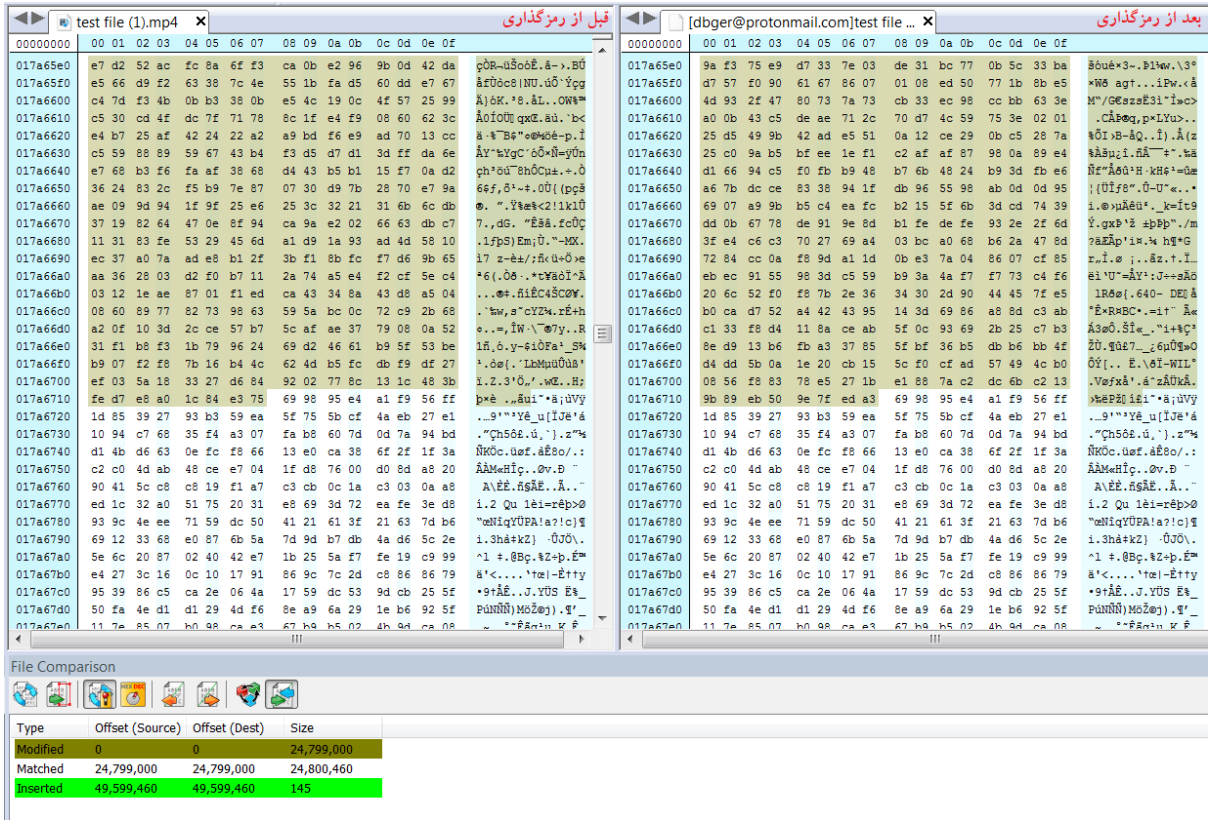
.cab, .pol, .dll, .msi, .exe, .lib, .iso, .bin, .bmp, .tmp, .log, .ocx, .chm, .dat, .sys, .wim, .dic, .mdf, .ldf, .myd, .myi, .frm, .dbf, .sdi, .lnk, .gho, .pbk

بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد. همچنین این باج‌افزار از اکسپلویت‌های EternalBlue و Mimikatz جهت گسترش در شبکه استفاده می‌نماید.

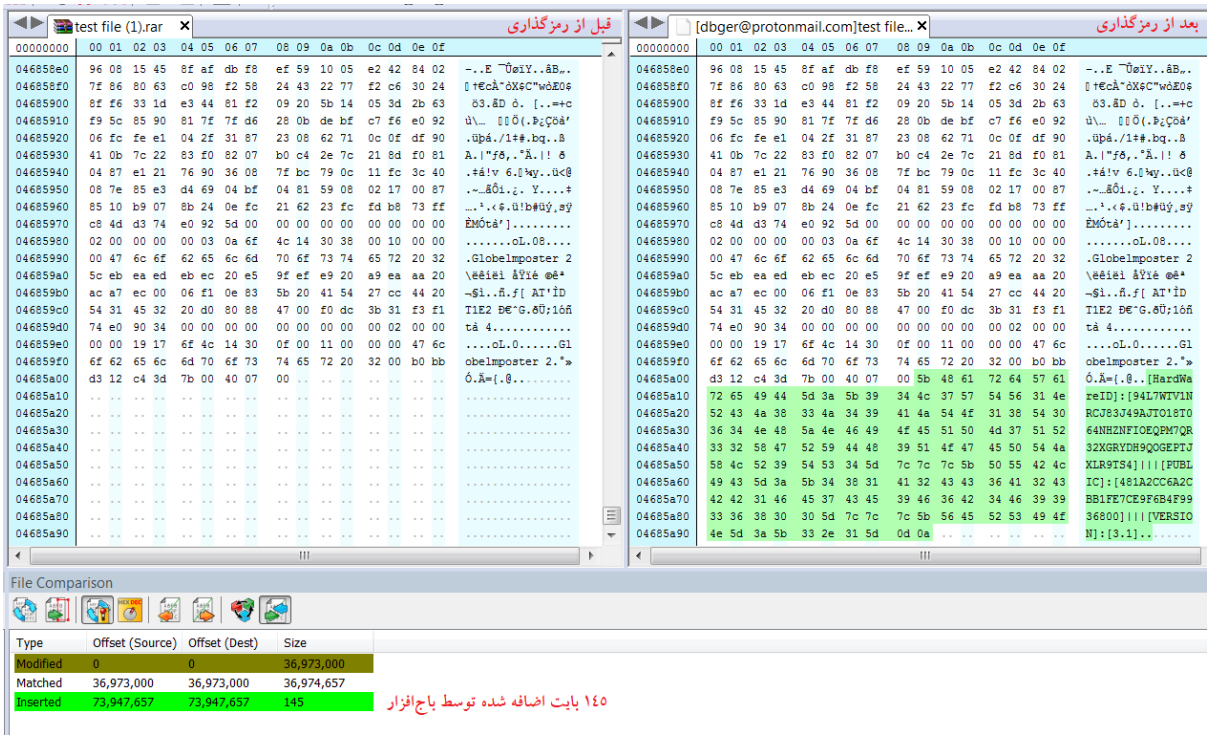
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Dbger به نتایج زیر دست پیدا کردیم.

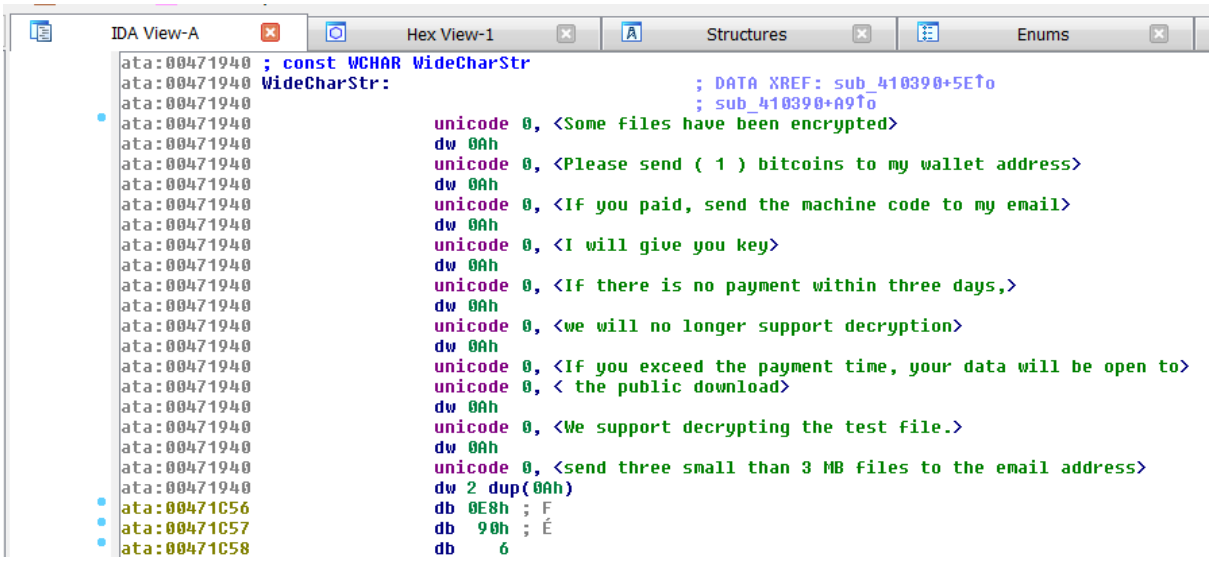
طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار Dbger ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر نمی‌دهد و تنها ۵۰ الی ۶۰ درصد ساختار فایل را تغییر می‌دهد . تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



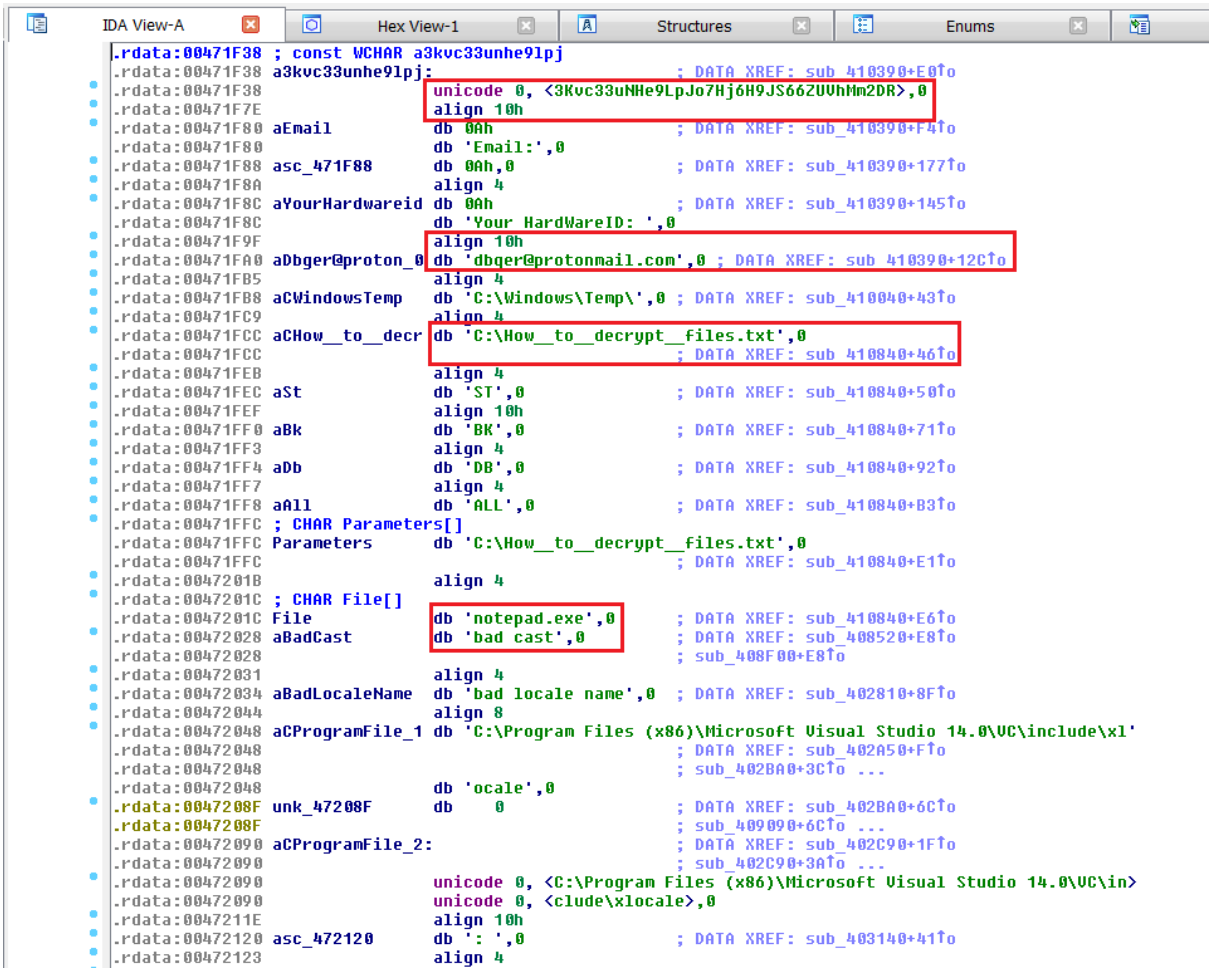
همچنین این باج‌افزار مقدار ۱۴۵ بایت را به انتهای فایل‌های رمزگذاری شده اضافه می‌نماید که طبق بررسی‌های انجام گرفته شامل کد شناسایی قربانی و برخی اطلاعات دیگر می‌باشد. موارد اشاره شده در تصویر زیر قابل مشاهده است :



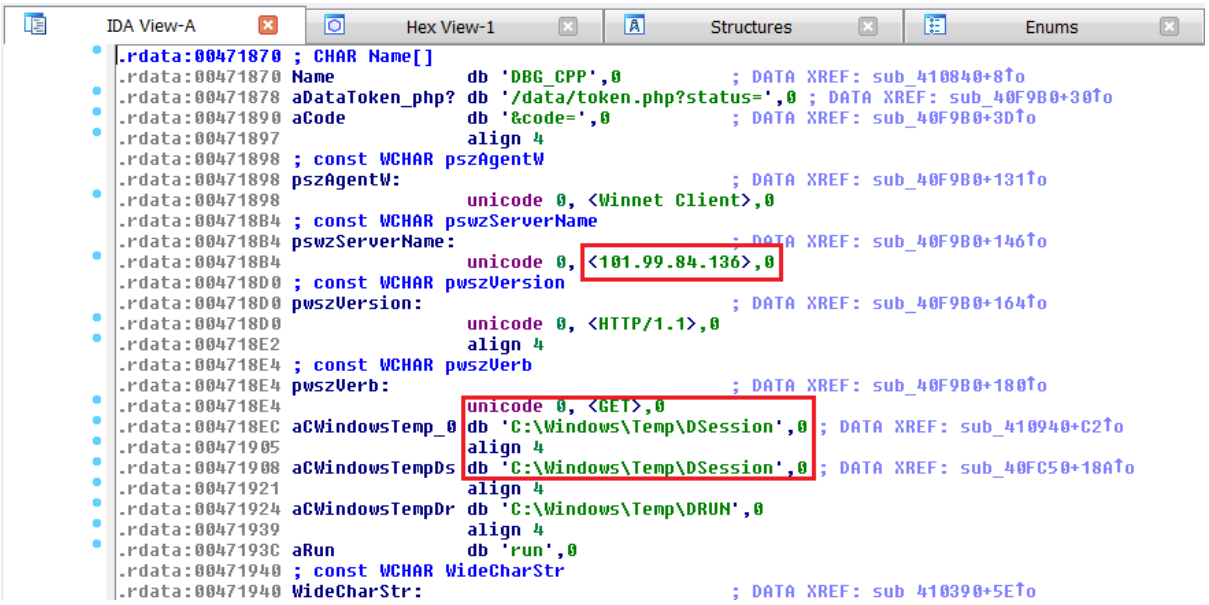
قطعه کد زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.



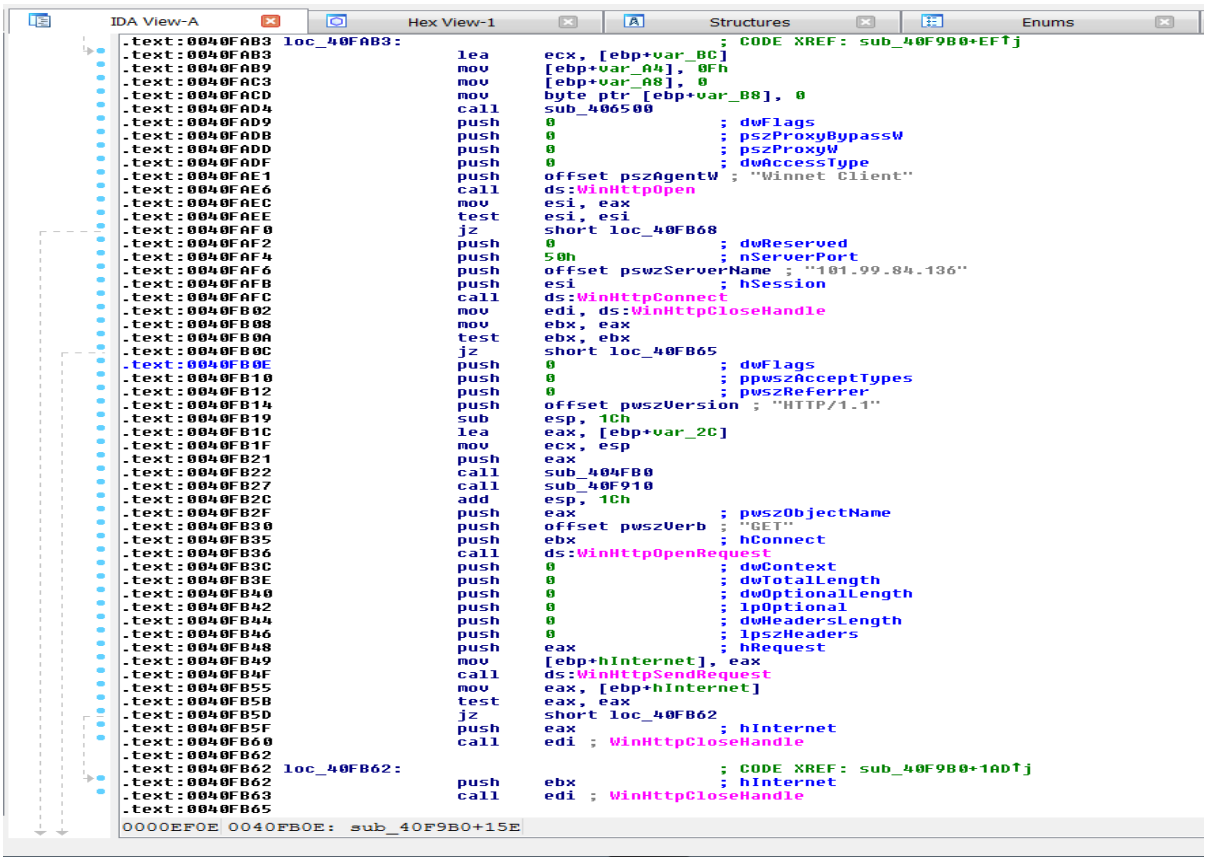
تصویر زیر نشان دهنده ایمیل مهاجم، فرایند notepad.exe برای نمایش پیغام باج‌خواهی، آدرس کیف پول بیت‌کوین و ... می‌باشد.



باج‌افزار پس از حمله به سیستم قربانی، با سرور کنترل و فرماندهی (C&C) خود ارتباط برقرار کرده و از این طریق کد شناسایی مربوط به قربانی دریافت می‌شود. تصاویر نشان‌دهنده‌ی این فرایند می‌باشد.

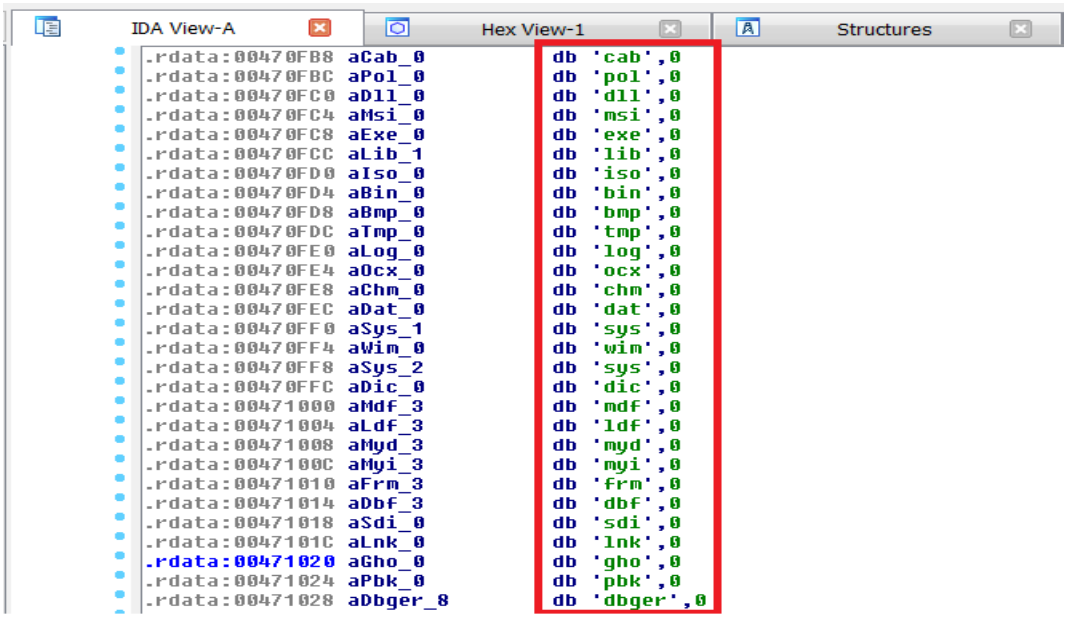


تصویر ۱

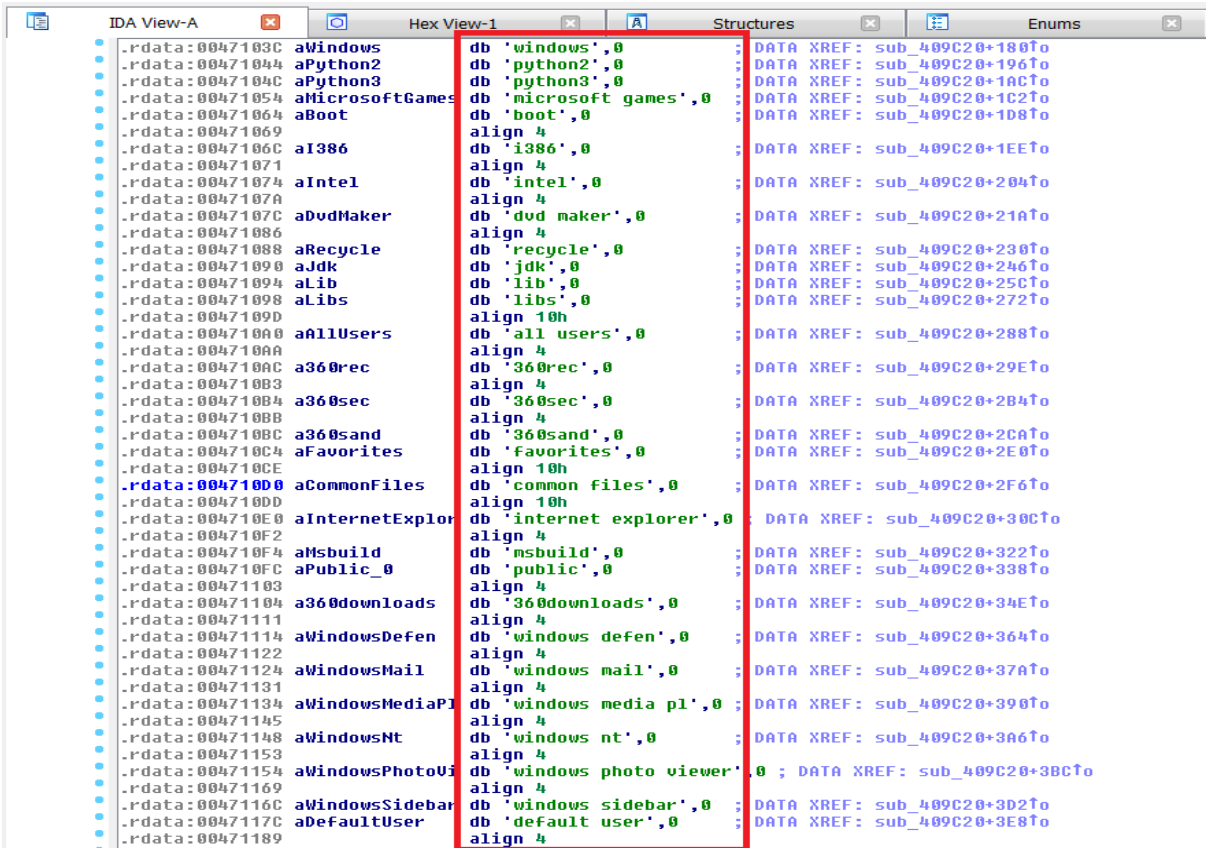


تصویر ۲

طبق بررسی‌های انجام شده، فایل‌های موجود در پوشه‌های زیر با پسوندهای اشاره شده، توسط این باج‌افزار رمزگذاری نمی‌شوند.

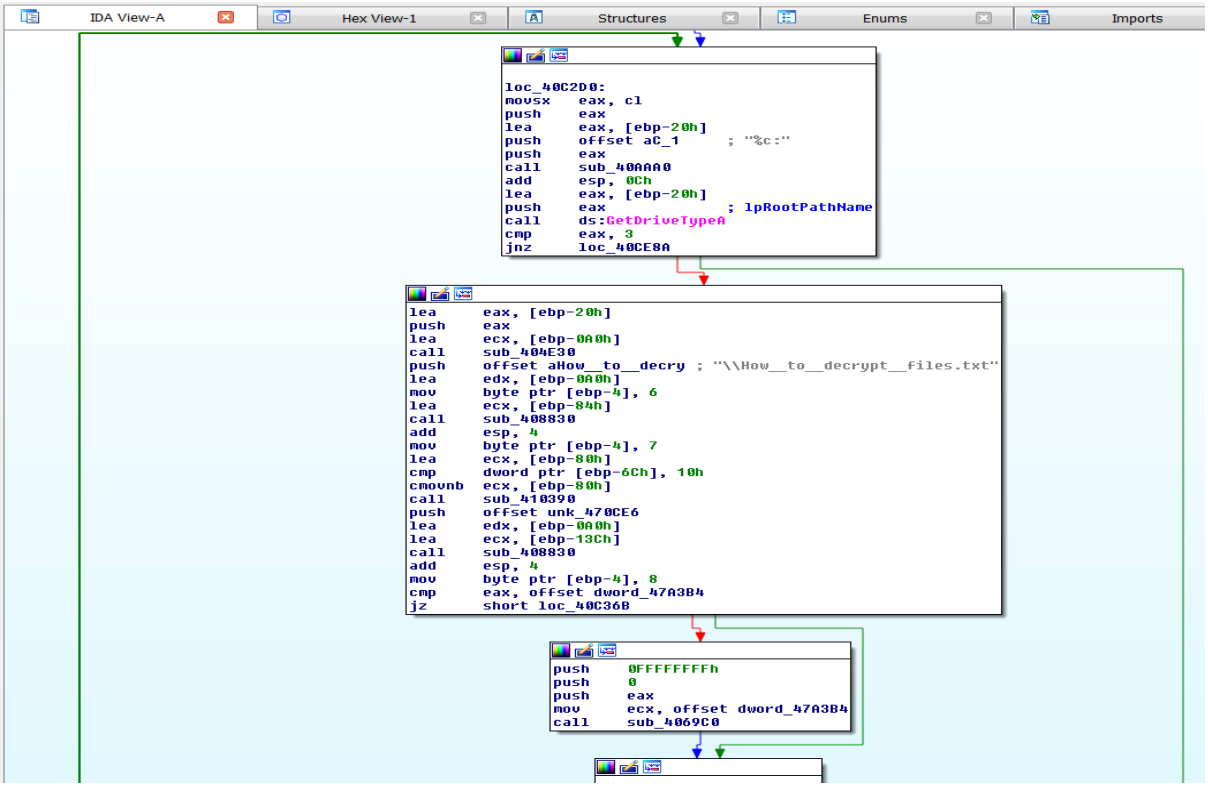


تصویر ۱: فایل‌ها با پسوندهای مشخص شده در تصویر بالا توسط باج‌افزار رمزگذاری نمی‌شوند.

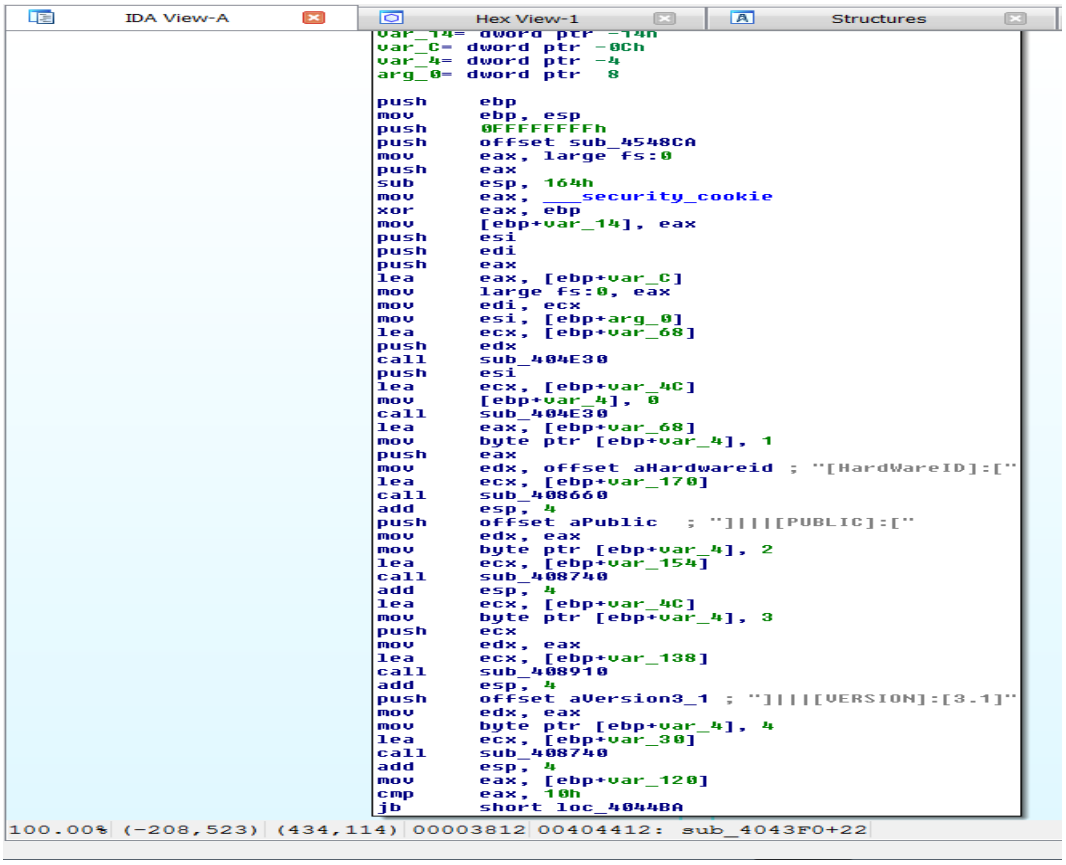


تصویر ۲: فایل‌های موجود در پوشه‌های مشخص شده در تصویر بالا توسط باج‌افزار رمزگذاری نمی‌شوند.

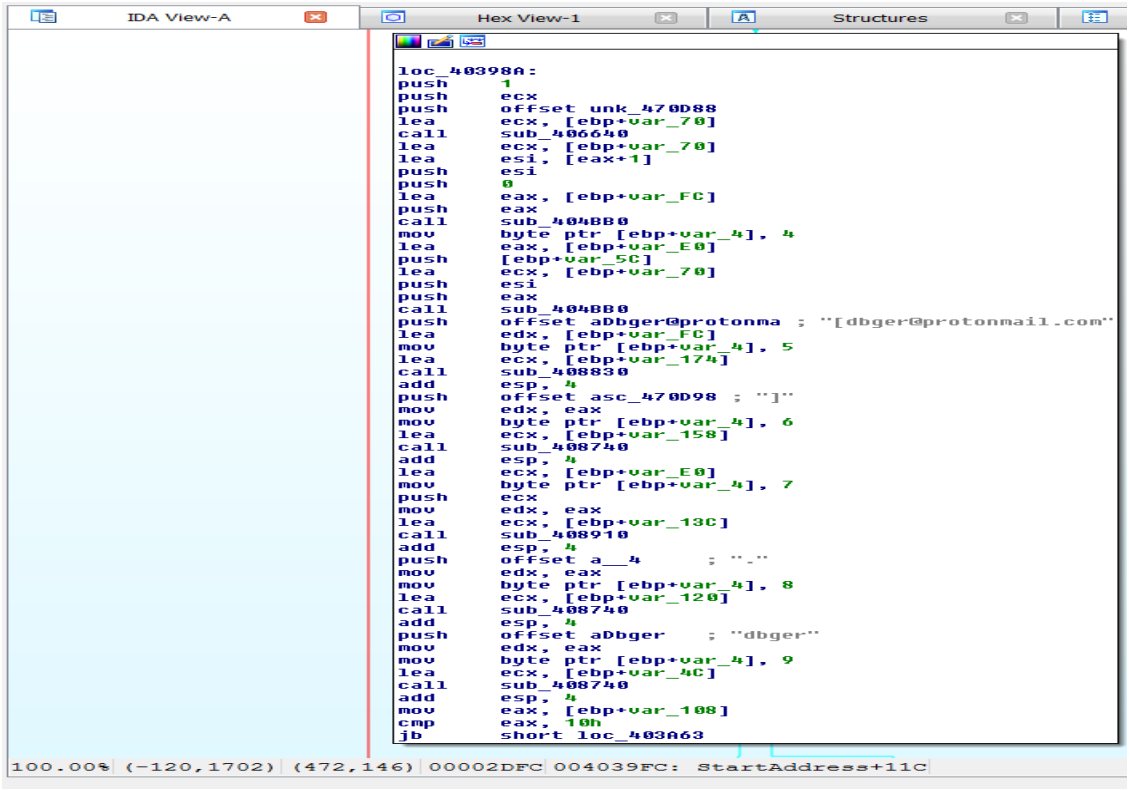
قطعه کد زیر مربوط به ایجاد فایل مربوط به پیغام باج‌خواهی در دایرکتوری‌های مختلف می‌باشد :



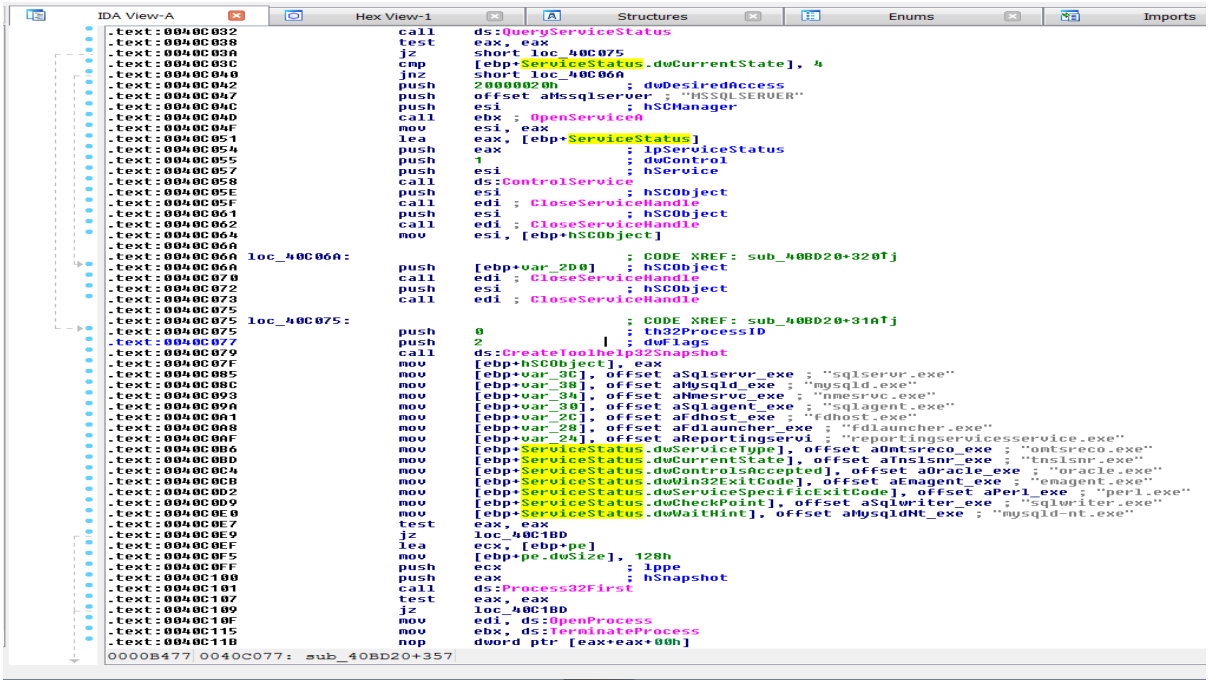
قطعه کد زیر مربوط به ۱۴۵ بایتی می‌باشد که به انتهای فایل‌ها اضافه می‌شود :



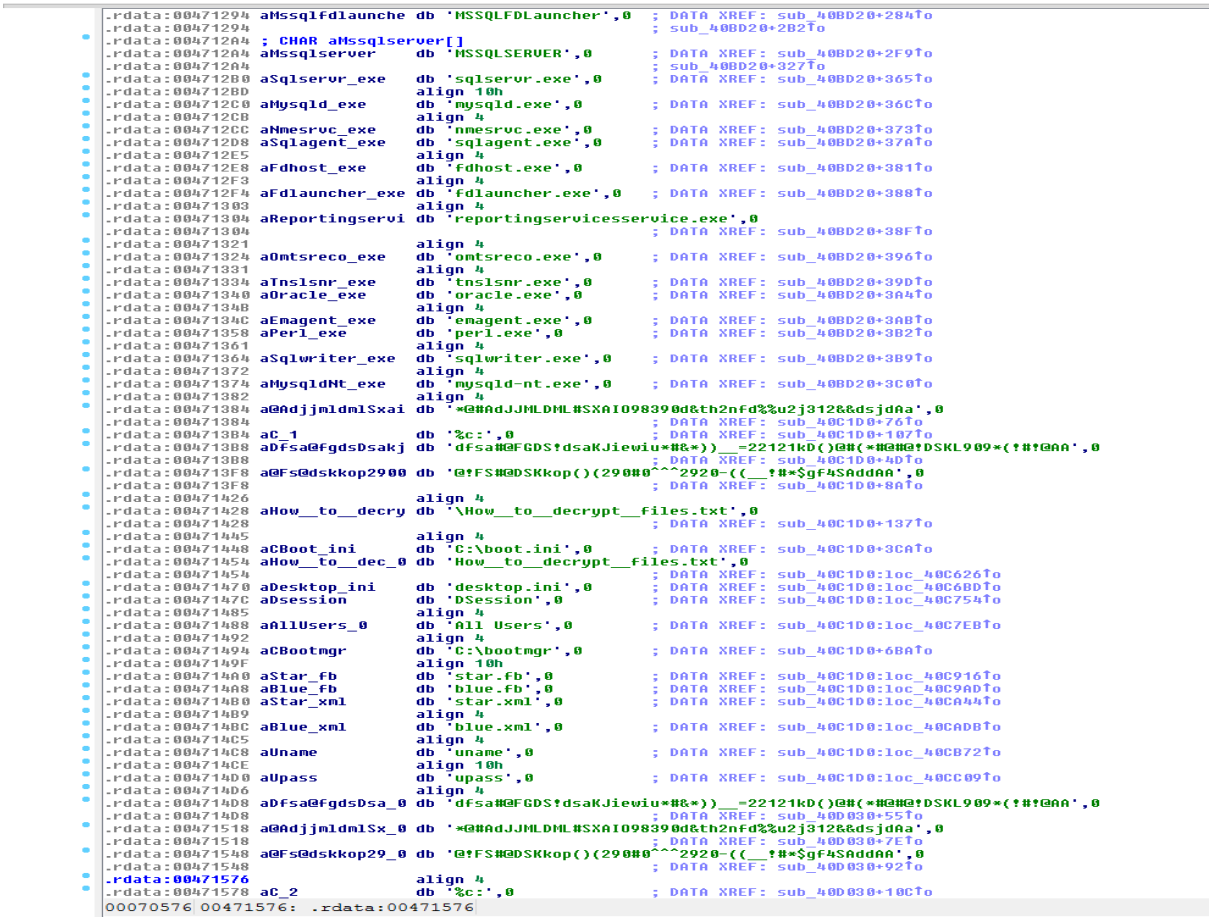
قطعه کد زیر مربوط به تغییر نام فایل‌ها و اضافه نمودن پسوند dbger. به انتهای فایل‌ها می‌باشد :



قطعه کدهای زیر مربوط به برخی از فرایندها و فایل‌های مرتبط با باج‌افزار می‌باشد :

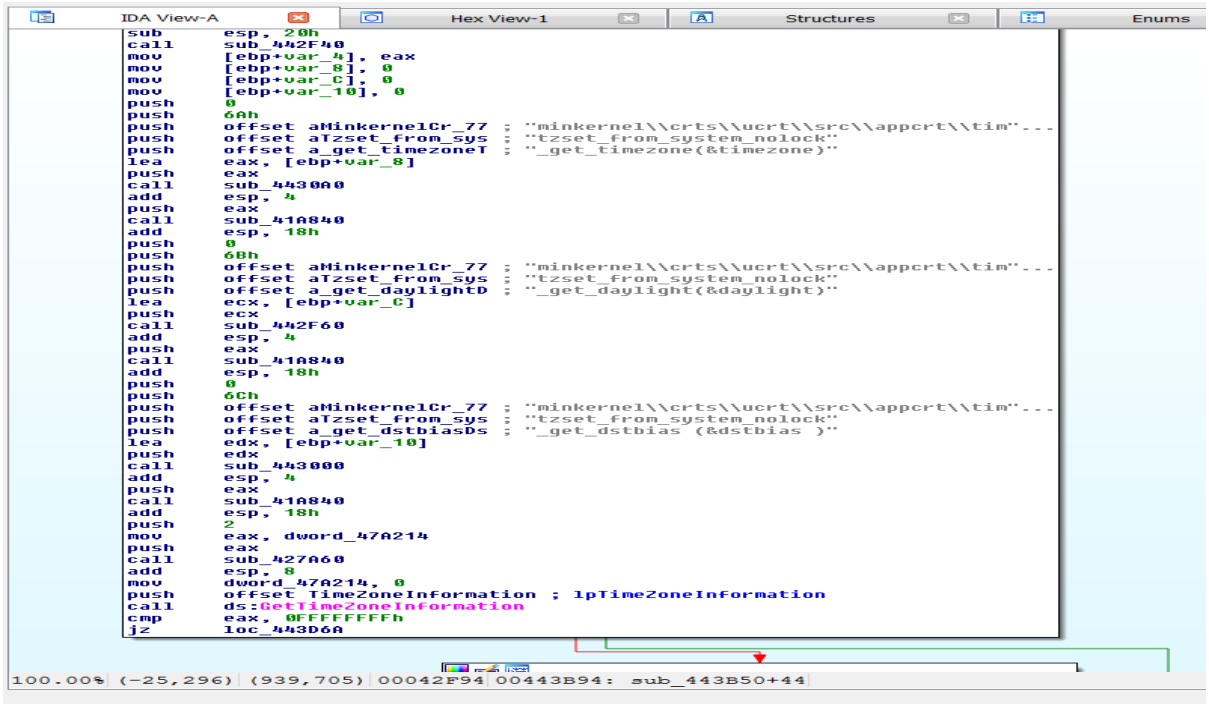


تصویر ۱

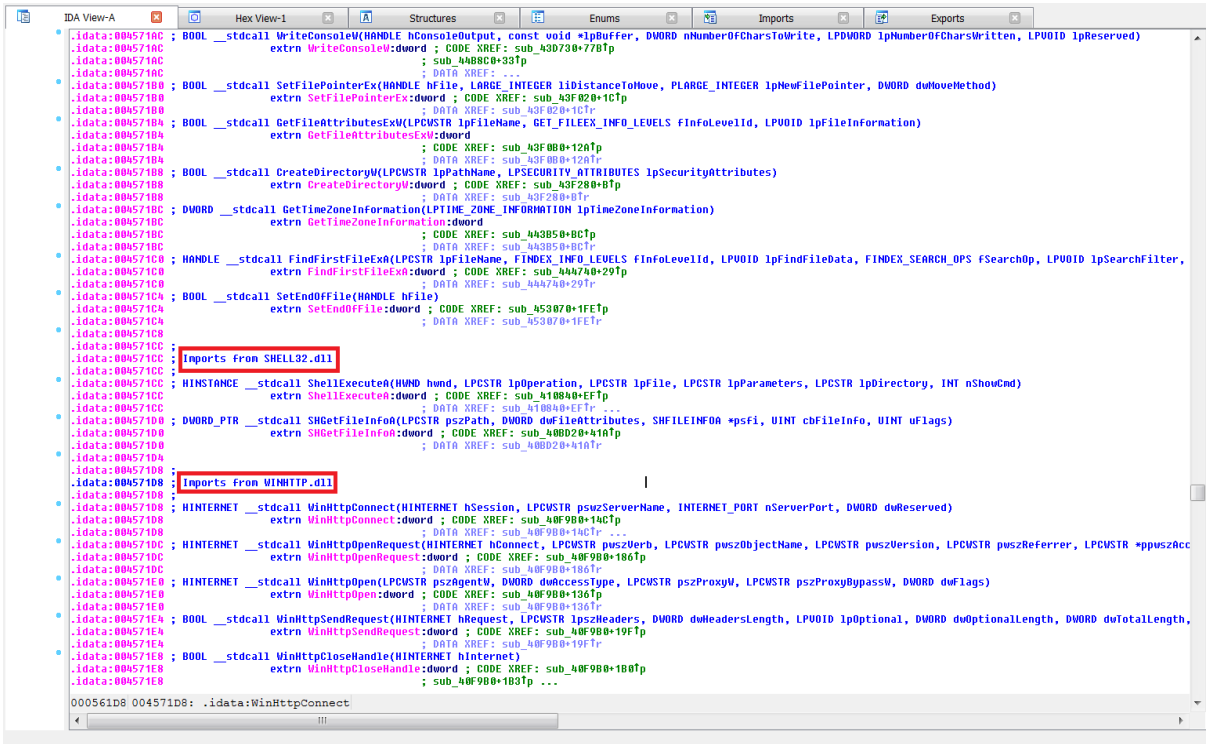


تصویر ۲

قطعه کد زیر مربوط به بررسی منطقه زمانی کاربران می‌باشد و به نظر می‌رسد باج‌افزار از آن برای هدف قرار دادن کاربرانی خاص استفاده می‌کند :



این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر 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.



ADVAPI۳۲.dll	WINHTTP.dll	SHELL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
CryptDeriveKey CloseServiceHandle	WinHttpOpen WinHttpConnect	SHGetFileInfoA ShellExecuteA	GetStdHandle FileTimeToSystemTime	GetTimeZoneInformation OutputDebugStringW

CryptReleaseContext OpenServiceA CryptAcquireContextA QueryServiceStatus ControlService CryptEncrypt CryptHashData OpenSCManagerA CryptCreateHash	WinHttpOpenRequest WinHttpSendRequest WinHttpCloseHandle		GetDriveTypeA SetEndOfFile EncodePointer SystemTimeToTzSpecificLocalTime DeleteCriticalSection	FindClose TlsGetValue OutputDebugStringA SetLastError GetModuleFileNameW IsDebuggerPresent

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
HeapFree	GetProcAddress	ReadFile	SetFilePointerEx
EnterCriticalSection	CreateEventW	CloseHandle	CreateMutexA
Process۳۲First	CreateFileW	GetACP	CreateThread
SetEvent	GetFileType	GetModuleHandleW	SetUnhandledExceptionFilter
QueryPerformanceCounter	TlsSetValue	GetFileAttributesExW	IsProcessorFeaturePresent
TlsAlloc	CreateFileA	IsValidCodePage	DecodePointer
FlushFileBuffers	ExitProcess	Sleep	SetEnvironmentVariableA
RtlUnwind	LeaveCriticalSection	GetOEMCP	TerminateProcess
Process۳۲Next	GetLastError	GetLocaleInfoW	GetModuleHandleExW
OpenProcess	LCMapStringW	SetStdHandle	ReadConsoleW
GetStartupInfoW	GetSystemInfo	WideCharToMultiByte	GetCurrentThreadId
CreateDirectoryW	lstrlenA	WriteFile	WriteConsoleW
GetUserDefaultLCID	GetConsoleCP	GetSystemTimeAsFileTime	CreateToolhelp۳۲Snapshot
GetProcessHeap	GetEnvironmentStringsW	HeapReAlloc	InitializeCriticalSectionAndSpinCount
CompareStringW	WaitForSingleObjectEx	GetStringTypeW	
FindFirstFileExA	GetCurrentProcessId	SetFileAttributesA	GetCurrentProcess
FindFirstFileA	GetCommandLineW	FreeLibrary	GetConsoleMode
HeapValidate	HeapQueryInformation	MoveFileA	UnhandledExceptionFilter
ResetEvent	GetCPInfo	HeapAlloc	FreeEnvironmentStringsW
FindNextFileA	HeapSize	GetModuleFileNameA	InitializeSListHead
IsValidLocale	GetCommandLineA	EnumSystemLocalesW	MultiByteToWideChar
FindFirstFileExW	RaiseException	LoadLibraryExW	TlsFree

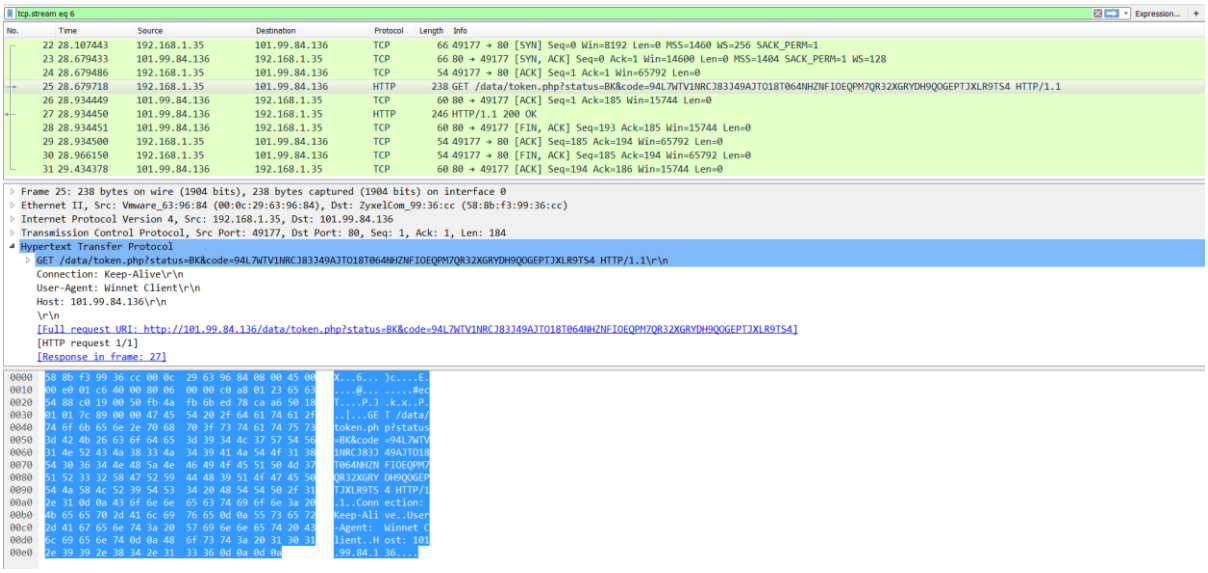
بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند :

- Dbger.exe

پس از خاتمه فرایند مربوط به باج‌افزار فرایند notepad.exe ایجاد می‌شود و پیغام باج‌خواهی به نمایش در می‌آید.

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج‌افزار Dbger را نشان می‌دهد.



طبق بررسی های صورت گرفته، درخواست‌های HTTP، پس از اجرای باج افزار به شرح زیر می‌باشد.

http://۱۰۱.۹۹.۸٤.۱۳٦/data/token.php?status=ST&code=HZJCJKJ۰۲۲QZNAXNI۷٤TRM۳M۱S٤۱۳٥A۷۹XW۸ZEYO۹M۰۲RPGR٥٤G۷D۳٥SN٤UFQTWF

http://۱۰۱.۹۹.۸٤.۱۳٦/data/token.php?status=BK&code=HZJCJKJ۰۲۲QZNAXNI۷٤TRM۳M۱S٤۱۳٥A۷۹XW۸ZEYO۹M۰۲RPGR٥٤G۷D۳٥SN٤UFQTWF

http://۱۰۱.۹۹.۸٤.۱۳٦/data/token.php?status=DB&code=HZJCJKJ۰۲۲QZNAXNI۷٤TRM۳M۱S٤۱۳٥A۷۹XW۸ZEYO۹M۰۲RPGR٥٤G۷D۳٥SN٤UFQTWF

میزبانی که باج افزار با آن ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
مالزی	۸۰ TCP	۱۰۱.۹۹.۸٤.۱۳٦

جزئیات بیشتر مربوط به ترافیک شبکه در تصاویر زیر قابل مشاهده است :

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٥ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.31084440	ALYac	Trojan.Ransom.Satan
Antiy-AVL	Trojan[Ransom]/Win32.Natas	Arcabit	Trojan.Generic.D1DA4F98
Avast	Win32:Adware-gen [Adw]	AVG	Win32:Adware-gen [Adw]
Avira	TR/FileCoder.dhtfi	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.31084440	CAT-QuickHeal	Trojan.Emelent
CrowdStrike Falcon	malicious_confidence_70% (W)	Cybereason	malicious.6642ee
Cylance	Unsafe	Cyren	W32/Trojan.IAOB-0215
Emsisoft	Trojan.Ransom.Dbger (A)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.31084440	ESET-NOD32	a variant of Win32/Filecoder.Natas.C
F-Secure	Trojan.GenericKD.31084440	Fortinet	W32/Filecoder_Natas.C!tr
GData	Trojan.GenericKD.31084440	Ikarus	Trojan-Ransom.Natas
K7AntiVirus	Trojan (0053785b1)	K7GW	Trojan (0053785b1)
Kaspersky	not-a-virus:HEUR:AdWare.Win32.Generic	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=95)	McAfee	RDN/Generic.RP
McAfee-GW-Edition	BehavesLike.Win32.Trojan.gh	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.FileCoder.ffjxty	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Virus.Adware.b51
Rising	Ransom.FileCryptor!8.1A7 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Generic PUA EM (PUA)	Sophos ML	heuristic
Symantec	Ransom.Cryptolocker	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_DBGER.THGAFAH	TrendMicro-HouseCall	Ransom_DBGER.THGAFAH
VBA32	BScope.Trojan.CoinMiner	VIPRE	Trojan.Win32.Generic!BT
ZoneAlarm	not-a-virus:HEUR:AdWare.Win32.Generic	AegisLab	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۶ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Sample_5b4c40cc7c404b5672aeb902.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	Clean
sophos	9.14.2	Clean
f_secure	11.00	Dangerous: Trojan.GenericKD.31084440
kaspersky	5.5	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.38183	Dangerous: Win32/Filecoder.Natas.C
drweb	11.0.1.1607061217	Clean
clam_av	0.99.2	Clean
comodo	1.1.268025.1	Dangerous: ApplicUnwnt
bitdefender	11.0.1.18	Dangerous: Trojan.GenericKD.31084440
avast	2.1.2	Clean
symantec	7.9.0.30	Dangerous: Ransom.Cryptolocker