باسمه تعالی

تحلیل فنی باج افزار Armage

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار QNBQW خبر می‌دهد که پس از رمزگذاری فایل‌ها پسوند آن‌ها را به armage. تغییر می‌دهد و به همین دلیل به نام Armage معرفی شده است. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در تاریخ ۲۳ ژوئیه سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم‌های رمزنگاری AES ۲۵۶ بیتی و RSA برای رمزگذاری استفاده می‌کند و طبق بررسی‌های انجام شده به جز فایل‌های موجود در دایرکتوری‌های زیر، تمام فایل‌های موجود بر روی سیستم قربانی را رمزگذاری می‌کند :

Windows, Program Files, Boot

طبق بررسی‌های انجام شده در حال حاضر باج‌افزار Armage آخرین عضو خانواده‌ی QNBQW می‌باشد و ترتیب انتشار آن‌ها به صورت زیر می‌باشد :

QNBQW > zzz۱۲ > Armage

مشخصات فایل اجرایی :

نام فایل	Armage.exe
MD۵	bbacd۷e۵e۷be۹de۰۱۸۱e٤۱۸de۹c۲٦c۵a
SHA-۱	a۰f۷bc۹۱۹۳۷۳۳۰bdec۹bf۳۲bcddc۸dd۲ab۲۹۳ff۱
SHA-۲۵٦	٦۷٦۹۷dcd۸٤۹۳f۲۸۷a۸۸۰cff٦۱٦۵b۹۰۳bfe۱daf۳b۵۵۸۱٤e۹۰de۸۷۹cd۱fb۸df۰۰٤
اندازه فایل	۸۰۹.۵ KB

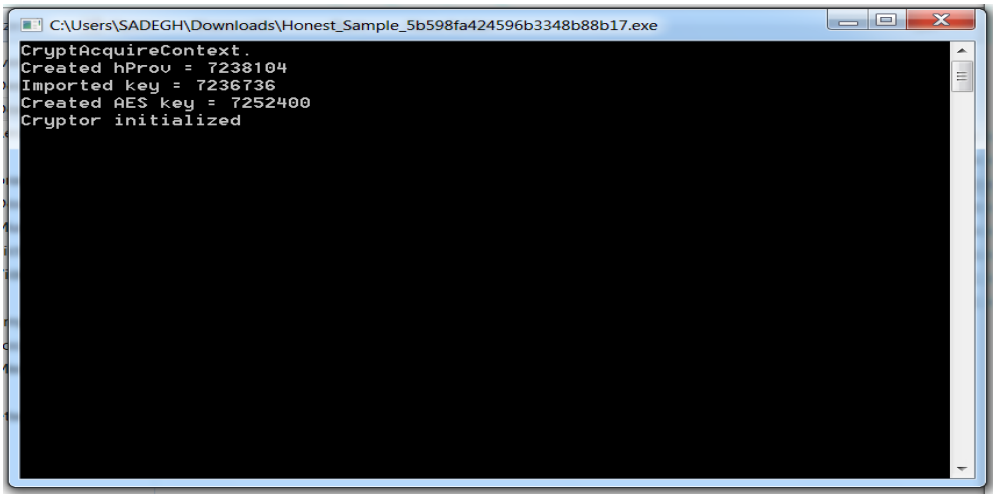
فایل اجرایی این باج افزار دارای هشت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.۱۸	٤۰۹٦	۷۷۱٤٦۰	۷۷۱۵۸٤
.data	۱.۱٤	۷۷۸۲٤۰	۷۸۸	۱۰۲٤
.rdata	۵.۵۹	۷۸۲۳۳٦	٤۳۷۹۲	٤٤۰۳۲
.eh_fram	٤.۷۲	۸۲۷۳۹۲	۵۳۰٤	۵٦۳۲
.bss	۰	۸۳۵۵۸٤	۹۱۸٤	۰
.idata	۵.۲۲	۸٤۷۸۷۲	٤۳۹٦	٤٦۰۸
.CRT	۰.۱۸	۸۵٦۰٦٤	۲۸	۵۱۲

.tls	۰.۲۳	۸۶۰۱۶۰	۳۲	۵۱۲

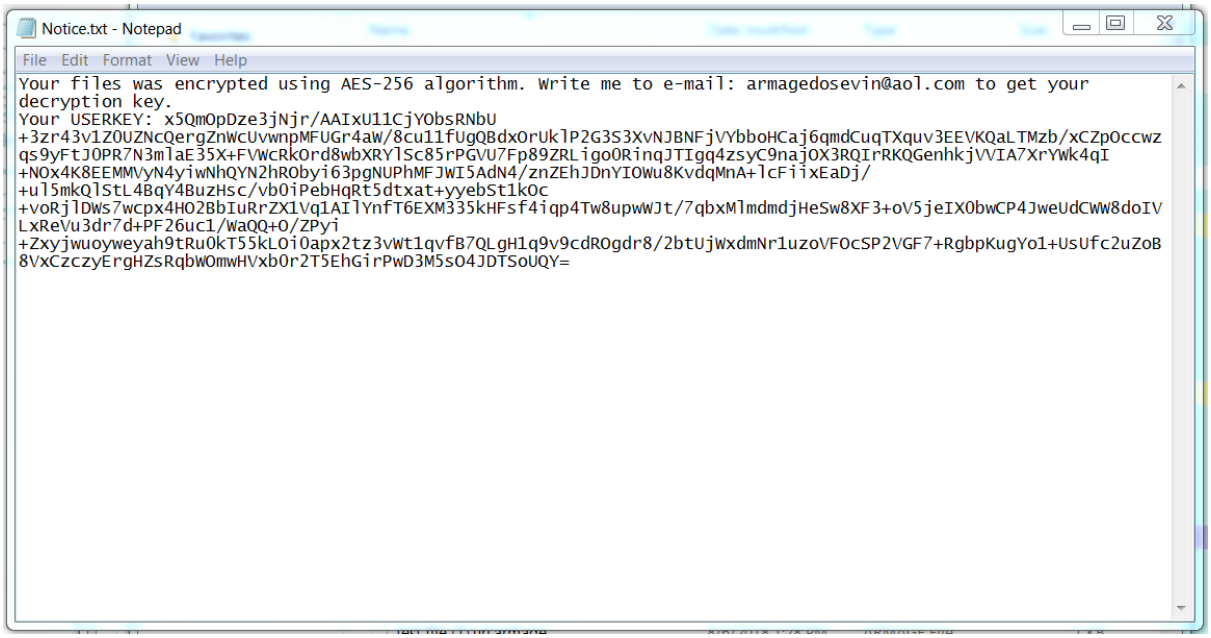
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Armage، 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 در ابتدای اجرا، پنجره‌ی زیر را به نمایش می‌گذارد و با اجرای فرایند vssadmin.exe نسخه‌های shadowcopy را حذف می‌کند :



پس از آن، پنجره‌ی مورد اشاره بسته می‌شود و فرایند رمزگذاری فایل‌ها آغاز می‌گردد و در حین انجام این فرایند، یک فایل متنی تحت عنوان Notice.txt را بر روی Desktop و دایرکتوری‌های مختلف ایجاد می‌کند سپس فایل اجرایی باج‌افزار حذف می‌شود و فرایند مربوط به آن نیز خاتمه پیدا می‌کند.

محتوای فایل متنی که در واقع پیغام باج‌خواهی می‌باشد، در تصویر زیر قابل مشاهده است.



بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌ها را با استفاده از الگوریتم رمزنگاری AES در حالت ۲۵۶ بیتی رمزگذاری نموده‌اند و قربانیان جهت دریافت کلید رمزگشایی بایستی از طریق آدرس ایمیل armagedosevin@aol.com با آن‌ها ارتباط برقرار نمایند. برای کسب اطلاعات بیشتر به صورت ناشناس با مهاجمین ارتباط برقرار نمودیم که پیغام زیر برای ما ارسال شد :

طبق این پیغام مهاجمین اعلام نموده‌اند که مبلغ ۱ بیت‌کوین را تا پایان همان روز برای آن‌ها به کیف پول بیت‌کوین به آدرس ۱FRAsXvRztx۵vSpuCcD۲URZzcwwyC۸۵kAD ارسال نمایید، در غیر این صورت

مبلغ باج به ۲ بیت‌کوین برای روز بعد افزایش می‌یابد. طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تاکنون تعداد ۳۳ تراکنش برابر با ۲.۷۱۶۴۸۹۱ BTC داشته است.

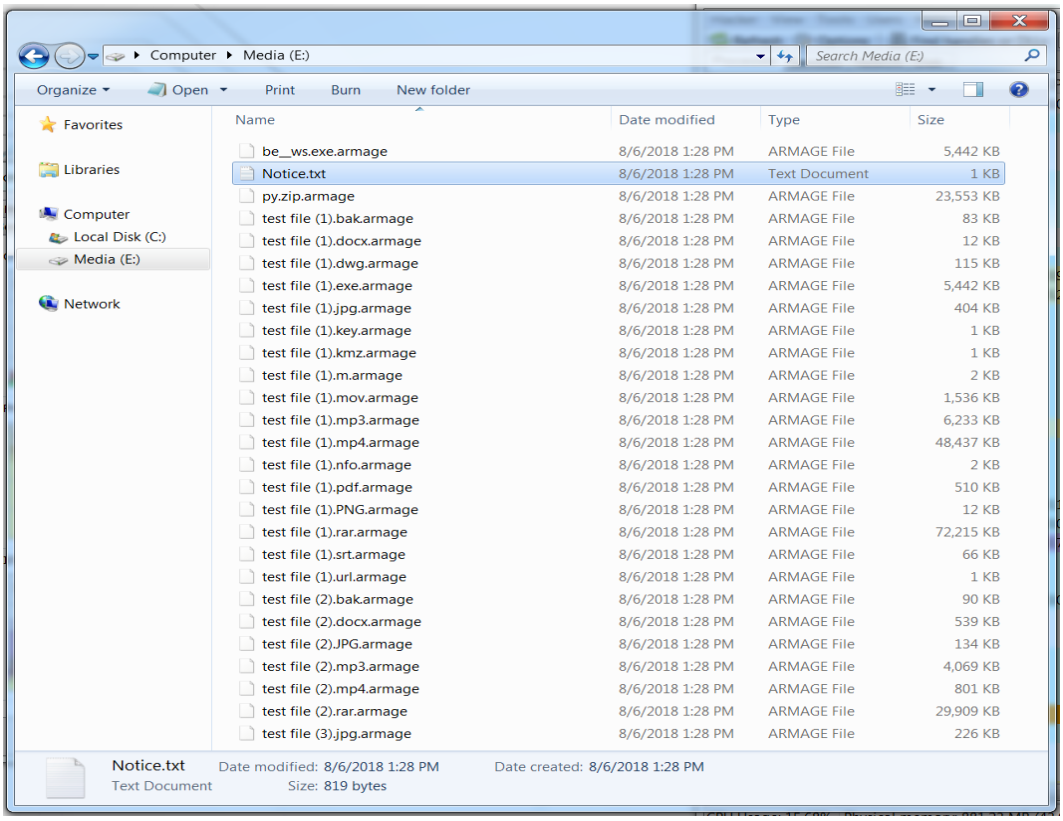

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1FRAsXvRztx5vSpuCcD2URZzcwwyC85kAD
Hash 160	9e23fbf285c0942722ff0b23337310214c7f5417

Transactions	
No. Transactions	33
Total Received	2.7164891 BTC
Final Balance	0 BTC

Request Payment Donation Button

همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به armage. تغییر می‌دهد، تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد :



همانطور که قبلا نیز اشاره شد باج‌افزار Armage به جز فایل‌های موجود در دایرکتوری‌های زیر تمام فایل‌های موجود در سیستم قربانی را رمزگذاری می‌کند :

Windows, Program Files, Boot

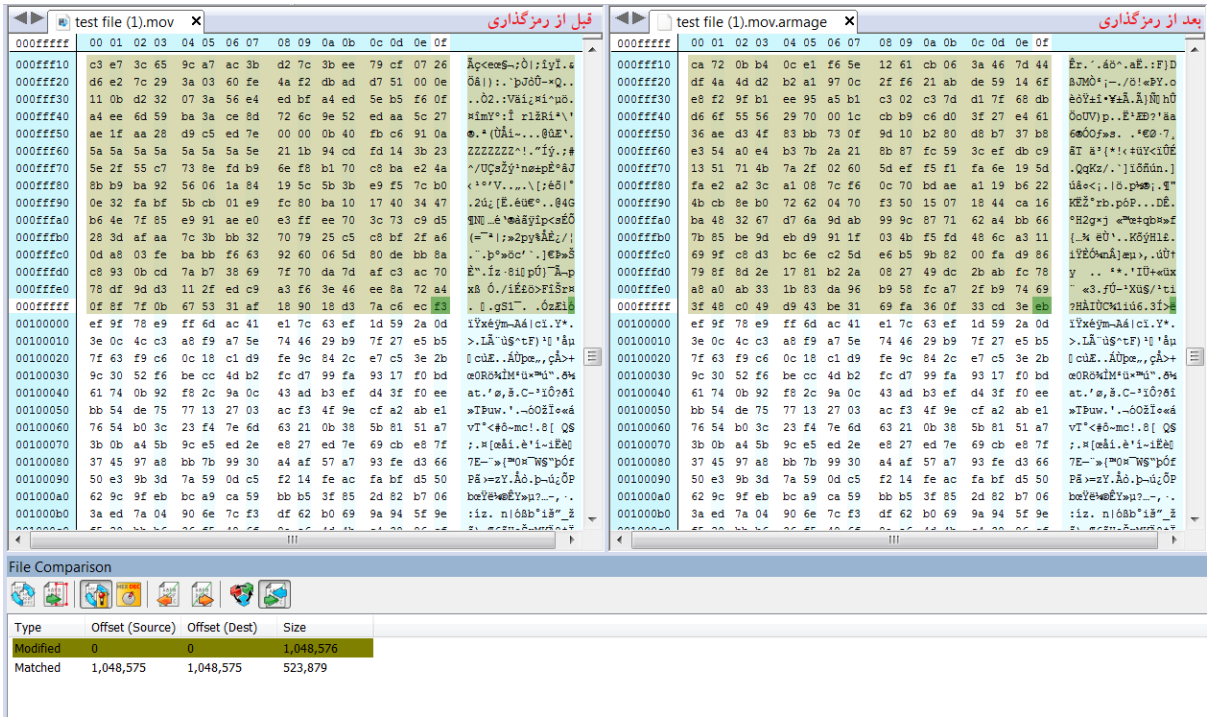
طبق مشاهدات صورت گرفته، هنگام اجرای باج‌افزار Armage به طور میانگین از ۴۰ الی ۵۰ درصد ظرفیت CPU، و ۲۵ الی ۳۵ درصد ظرفیت حافظه (RAM) استفاده می‌گردد.

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.

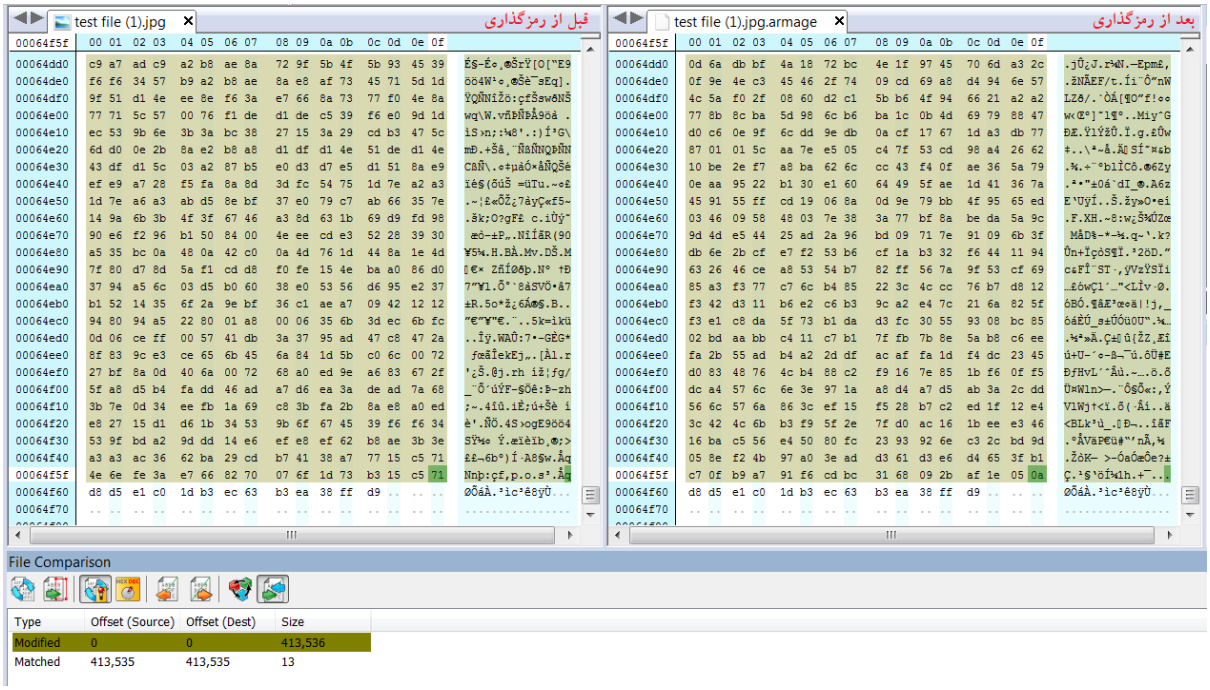
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Armage 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 Armage ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر نمی‌دهد و با توجه به حجم فایل‌ها رفتار متفاوتی از خود نشان می‌دهد، به این صورت که بیش از ۹۹ درصد ساختار فایل‌هایی که حجم آن‌ها کم‌تر از ۱۰۴۸۵۷۶ بایت می‌باشد را تغییر می‌دهد، اما فایل‌هایی که حجم آن‌ها بیشتر از این مقدار است، فقط ۱۰۴۸۵۷۶ بایت ابتدایی آن‌ها را تغییر می‌دهد. تصاویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :

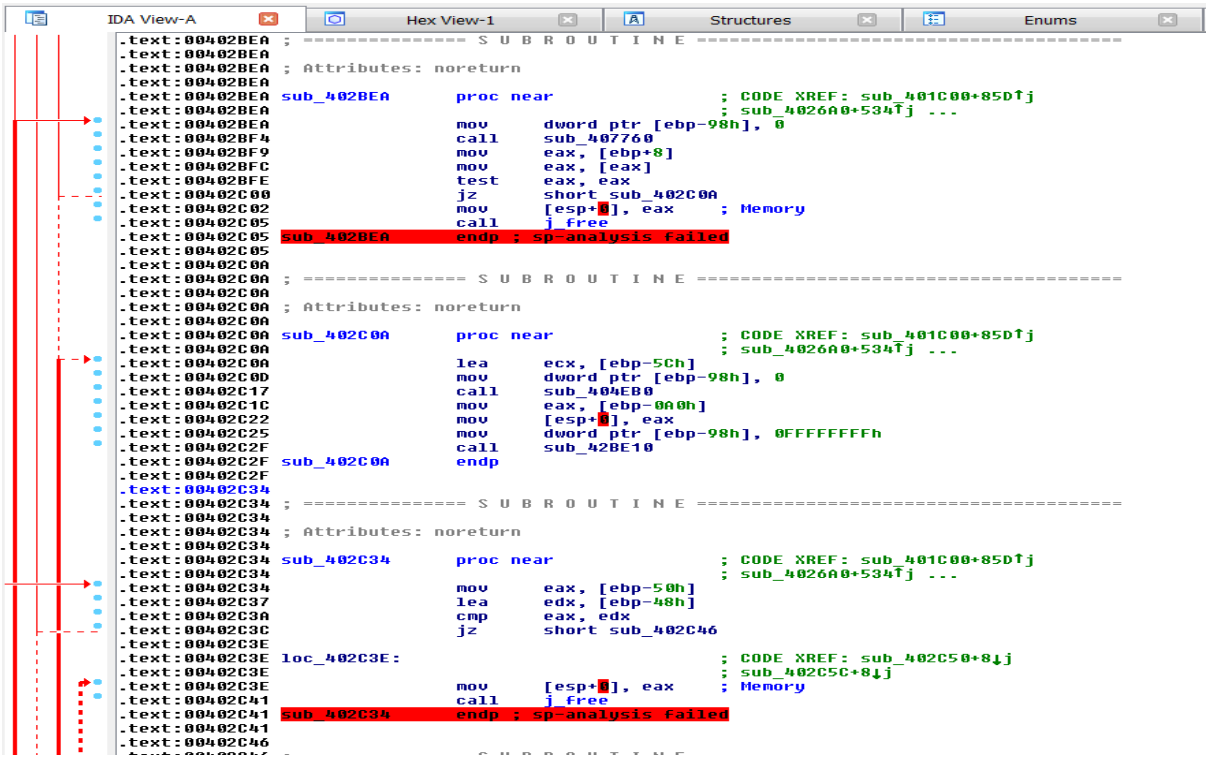


تصویر ۱: فایل با حجم بیشتر از ۱۰۴۸۵۷۶ بایت



تصویر ۲: فایل با حجم کمتر از ۱۰۴۸۵۷۶ بایت که بیش از ۹۹ درصد ساختار آن تغییر کرده است.

قطعه کد زیر مربوط به استفاده از روش‌های مختلف ضد دیس‌اسمبل جهت جلوگیری از بررسی و تحلیل‌های بیشتر توسط محققین می‌باشد :

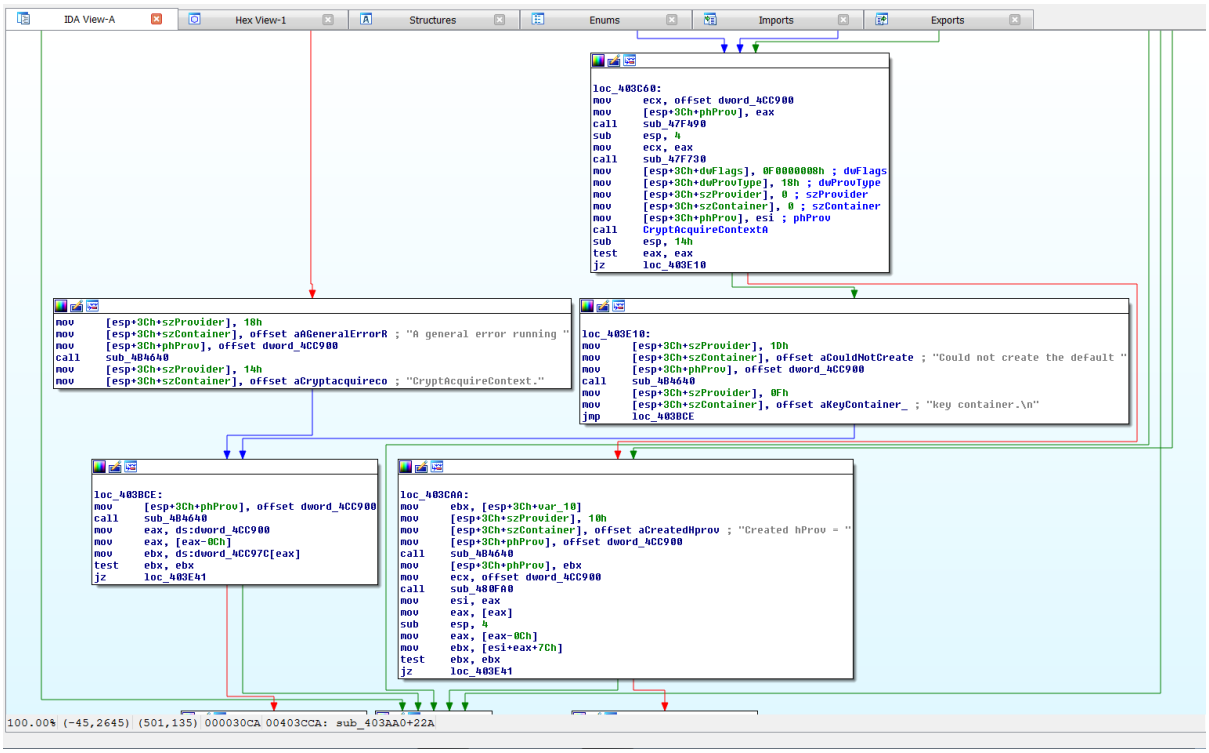


قطعه کد زیر مربوط به قرار دادن فایل متنی مربوط به پیغام باج‌خواهی در دایرکتوری‌های مختلف و متن پیغام باج‌خواهی می‌باشد:

Honest_Sample_5b598fa424596b3348b88b17.c

```
3809    LPCSTR v16; // [sp+68h] [bp-30h]@1
3810    int v17; // [sp+6Ch] [bp-2Ch]@1
3811    char v18; // [sp+70h] [bp-28h]@1
3812    char v19; // [sp+80h] [bp-18h]@1
3813
3814    v13 = &v19;
3815    v11 = sub_405670;
3816    v12 = (int)dword_4BB460;
3817    v7 = (int *)&v9;
3818    v14 = sub_40157D;
3819    v15 = &lpFileName;
3820    sub_42B7B0((int)&v9);
3821    v16 = &v18;
3822    v2 = *(_DWORD *)a1 + *(_DWORD *)(a1 + 4);
3823    lpFileName = *(LPCSTR *)a1;
3824    v10 = 1;
3825    sub_401360(&v16, (void *)lpFileName, v2);
3826    if ( (unsigned int)(0x7FFFFFFF - v17) <= 0xA )
3827    {
3828      v10 = 3;
3829      sub_406DB0("basic_string::append");
3830    }
3831    v10 = 3;
3832    sub_4A8BA0((int)&v16, "\\Notice.txt", 0xBu);
3833    v10 = 2;
3834    hFile = CreateFileA(v16, 0xC0000000, 0, 0, 2u, 0x80u, 0);
3835    if ( v16 != &v18 )
3836      j_free((void *)v16);
3837    if ( hFile != (HANDLE)-1 )
3838    {
3839      v10 = 1;
3840      WriteFile(
3841        hFile,
3842        "Your files was encrypted using AES-256 algorithm. Write me to e-mail: armagedosevin@aol.com to get your decryption key.\r\nYour USERKEY: ",
3843        0x87u,
3844        (LPDWORD)&v16,
3845        0);
3846      dwCreationDisposition = 0;
3847      lpSecurityAttributes = (LPSECURITY_ATTRIBUTES)&v16;
3848      WriteFile(hFile, *(LPCVOID *)a2, *(_DWORD *)(a2 + 4), (LPDWORD)&v16, 0);
3849      CloseHandle(hFile);
3850    }
3851    return sub_42B910(v7);
3852  }
```

قطعه کد زیر مربوط به اطلاعات موجود در پنجره‌ای است که ابتدای اجرای باج‌افزار به نمایش در می‌آید :



همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به armage. تغییر می‌دهد، قطعه کد زیر مربوط به انجام این فرایند می‌باشد :

Honest_Sample_5b598fa424596b3348b88b17.c

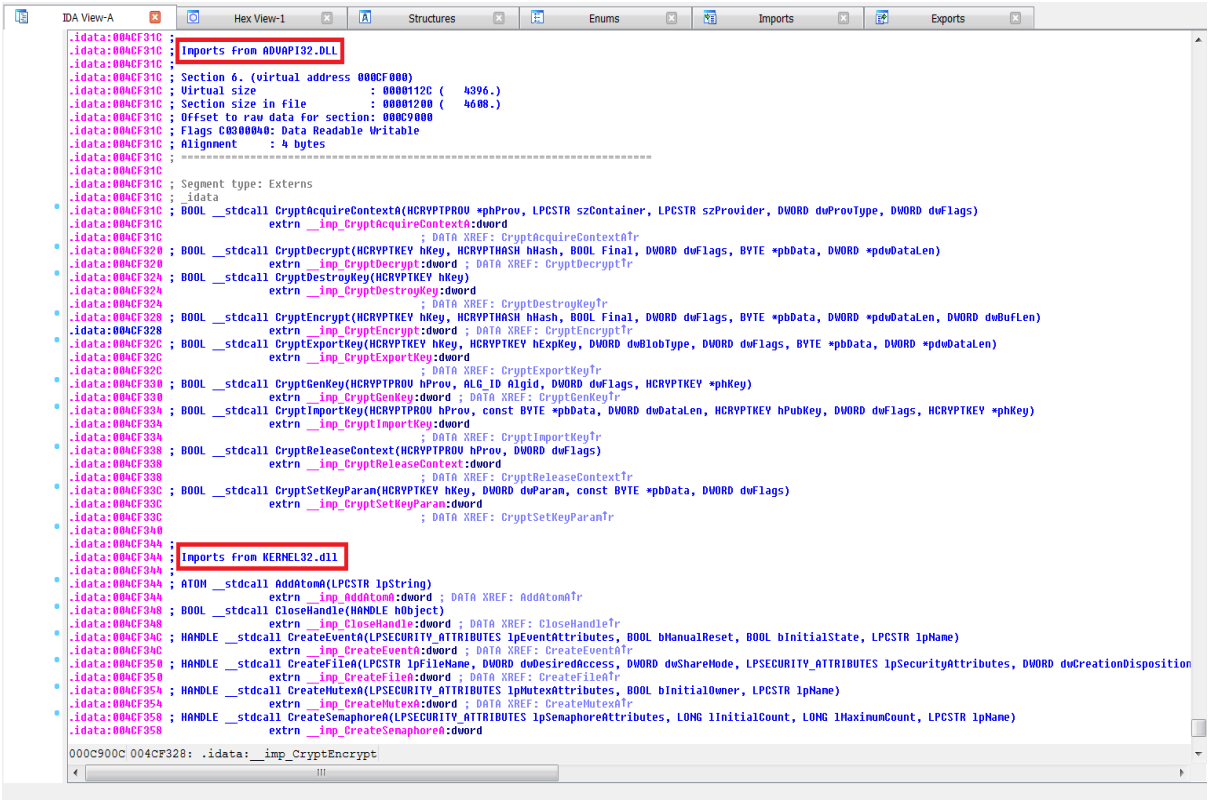
```
3987        j_free(Memory);
3988      if ( v24 != &v25 )
3989        j_free(v24);
3990      if ( !(_BYTE)lpNumberOfBytesWritten )
3991      {
3992        hTemplateFile = 0;
3993        dwFlagsAndAttributes = 128;
3994        dwCreationDisposition = 4;
3995        lpSecurityAttributes = 0;
3996        dwShareMode = 0;
3997        dwDesiredAccess = -1073741824;
3998        Size = *(_DWORD *)a1;
3999        v18 = 2;
4000        v4 = CreateFileA((LPCSTR)Size, 0xC0000000, 0, 0, 4u, 0x80u, 0);
4001        if ( v4 != (HANDLE)-1 )
4002        {
4003          NumberOfBytesRead = 0;
4004          lpNumberOfBytesWritten = &NumberOfBytesRead;
4005          hFile = v4;
4006          ReadFile(v4, lpBuffer, 0x100000u, &NumberOfBytesRead, 0);
4007          NumberOfBytesRead &= 0xFFFFFFF0;
4008          sub_404AC0((int)&unk_4CC020, (BYTE *)lpBuffer, NumberOfBytesRead);
4009          SetFilePointer(hFile, 0, 0, 0);
4010          WriteFile(hFile, lpBuffer, NumberOfBytesRead, lpNumberOfBytesWritten, 0);
4011          CloseHandle(hFile);
4012          lpNewFileName = &v34;
4013          sub_401360(&lpNewFileName, *(void **)a1, *(_DWORD *)a1 + *(_DWORD *)(a1 + 4));
4014          if ( (unsigned int)(0x7FFFFFFF - v33) <= 6 )
4015          {
4016            v18 = 4;
4017            sub_406DB0("basic_string::append");
4018          }
4019          v18 = 4;
4020          sub_4A8BA0((int)&lpNewFileName, ".armage", 7u);
4021          dwDesiredAccess = (DWORD)lpNewFileName;
4022          Size = *(_DWORD *)a1;
4023          v18 = 3;
4024          MoveFileA((LPCSTR)Size, lpNewFileName);
4025          if ( lpNewFileName != &v34 )
4026            j_free((void *)lpNewFileName);
4027        }
4028        free(lpBuffer);
4029      }
4030      return sub_42B910(v14);
4031    }
```

قطعه کد زیر مربوط به اجرای فرایند vssadmin.exe و حذف نسخه‌های shadowcopy می‌باشد :

Honest_Sample_5b598fa424596b3348b88b17.c

```
103822    size_t v130; // [sp+30Ch] [bp-8h]@144
103823    int v131; // [sp+310h] [bp-4h]@62
103824
103825    Command = &a1;
103826    v80 = &v128;
103827    v82 = &dwMilliseconds;
103828    v78 = sub_405670;
103829    v79 = (int)dword_4BB4FC;
103830    v81 = (int)&loc_4BACCB;
103831    sub_42B7B0((int)&v76);
103832    sub_42AF40();
103833    v77 = -1;
103834    Sleep(0x4E20u);
103835    v1 = GetConsoleWindow();
103836    ShowWindow(v1, 0);
103837    setlocale(0, 0);
103838    sub_4026A0((int)&v83);
103839    system("vssadmin delete shadows /all");
103840  LABEL_2:
103841    v2 = (int)v84;
103842    if ( v83 != v84 )
103843    {
103844      while ( 1 )
103845      {
103846        v3 = *(_DWORD *)(v2 - 20);
103847        Str = &v88;
103848        v4 = *(_DWORD *)(v2 - 24) + v3;
103849        Command = *(char **)(v2 - 24);
103850        v77 = 1;
103851        sub_401360(&Str, Command, v4);
103852        v5 = (int)(v84 - 16);
103853        v84 -= 24;
103854        if ( *(_DWORD *)(v5 - 8) != v5 )
103855        {
103856          Command = *(char **)(v5 - 8);
103857          j_free(Command);
103858        }
103859        v75 = Str;
103860        Memory = &v90;
103861        v6 = -1;
103862        if ( Str )
103863        {
103864          v7 = strlen(Str);
103865          v6 = (int)((char *)v75 + v7);
103866        }
```

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	MPR.DLL	SHELL۳۲.DLL	USER۳۲.dll	KERNEL۳۲.dll
CryptAcquireContextA	WNetEnumResourceA	ShellExecuteA	ShowWindow	AddAtomA
CryptDecrypt	WNetOpenEnumA			CloseHandle
CryptDestroyKey				CreateEventA
CryptEncrypt				CreateFileA
CryptExportKey				CreateMutexA
CryptGenKey				CreateSemaphoreA
CryptImportKey				DeleteCriticalSection
CryptReleaseContext				DuplicateHandle
CryptSetKeyParam				EnterCriticalSection

KERNEL۳۲.dll	KERNEL۳۲.dll	msvcrt.dll	msvcrt.dll	msvcrt.dll
ExitProcess	InitializeCriticalSection	memcmp	__getmainargs	fprintf
FindAtomA	InterlockedDecrement	memcpy	__mb_cur_max	fputc
FindClose	InterlockedExchange	memmove	__p__environ	fputs
FindFirstFileA	InterlockedExchangeAdd	memset	__p__fmode	fread
FindNextFileA	InterlockedIncrement	printf	__set_app_type	free
GetAtomNameA	IsDBCSLeadByteEx	putc	_beginthreadex	fsetpos
GetConsoleWindow	LeaveCriticalSection	putwc	_cexit	fwrite
GetCurrentDirectoryA	MoveFileA	realloc	_endthreadex	getc
GetCurrentProcess	MultiByteToWideChar	setlocale	_errno	getenv
GetCurrentThread	ReadFile	setvbuf	_fdopen	getwc
GetCurrentThreadId	ReleaseMutex	signal	_filelengthi٦٤	iswctype
GetDriveTypeA	ReleaseSemaphore	sprintf	_fstati٦٤	localeconv
GetHandleInformation	ResetEvent	strchr	_iob	longjmp
GetLastError	ResumeThread	strcmp	_lseeki٦٤	malloc
GetLogicalDriveStringsA	SetCriticalSectionSpinCount	strcoll	_onexit	memchr
GetModuleFileNameA	SetEvent	strerror	_read	wcsftime
GetModuleHandleA	SetFilePointer	strftime	_setjmp	wcslen
GetProcAddress	SetLastError	strlen	_setmode	wcsxfrm

GetProcessAffinityMask	SetProcessAffinityMask	strtod	_write	
GetSystemTimeAsFileTime	SetThreadContext	strtoul	abort	
GetThreadContext	SetThreadPriority	strxfrm	atexit	
GetThreadPriority	SetUnhandledExceptionFilter	system	atoi	
TryEnterCriticalSection	Sleep	towlower	calloc	
VirtualProtect	SuspendThread	towupper	exit	
VirtualQuery	TlsAlloc	ungetc	fclose	
WaitForMultipleObjects	TlsGetValue	ungetwc	fflush	
WaitForSingleObject	TlsSetValue	vfprintf	fgetpos	
WideCharToMultiByte	WriteFile	wcscoll	fopen	

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

Armage.exe

- cmd.exe
  - vssadmin.exe vssadmin Delete Shadows /All /Quiet

با اجرای فرایند vssadmin.exe و انجام دستور Delete Shadows /All /Quiet نسخه‌های shadowcopy حذف می‌شوند.

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم باز می‌شوند که به کاربرد برخی از آن‌ها اشاره شده است:

<HKLM>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	اطلاعات راجع به بسته‌های Winlogon توسط این کلید ذخیره می‌شود.
<HKLM>\System\CurrentControlSet\Control\Terminal Server	جهت فعالسازی سرویس ریموت دسکتاپ (RDP)
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	جهت تغییر مسیر فولدرها در سیستم

<HKCU>\SessionInformation
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics
<HKLM>\System\CurrentControlSet\Control\Error Message Instrument
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Windows
<HKLM>\system\CurrentControlSet\control\NetworkProvider\HwOrder
<HKLM>\Software\Microsoft\Windows\CurrentVersion\Explorer\Performance
<HKLM>\SYSTEM\Setup
<HKLM>\System\CurrentControlSet\Control\Session Manager
<HKLM>\System\CurrentControlSet\Control\SafeBoot\Option
<HKCU>\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
<HKLM>\Software\Microsoft\Windows NT\CurrentVersion\LanguagePack
<HKLM>\SOFTWARE\Microsoft\CTF\SystemShared
<HKLM>\SOFTWARE\Microsoft\CTF
<HKLM>\system\CurrentControlSet\services\RDPNP\NetworkProvider
<HKLM>\system\CurrentControlSet\services\LanmanWorkstation\NetworkProvider

<HKLM>\system\CurrentControlSet\services\WebClient\NetworkProvider

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 Armage نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٧ مورد از ٦٦ 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.31115680	AegisLab	Troj.Ransom.W32.Cryptor!c
AhnLab-V3	Trojan/Win32.Davidran.C2596698	ALYac	Trojan.Ransom.Armage
Antiy-AVL	Trojan[Ransom]/Win32.Cryptor	Arcabit	Trojan.Generic.D1DAC9A0
Avast	FileRepMalware	AVG	FileRepMalware
Avira	TR/Genasom.bimth	BitDefender	Trojan.GenericKD.31115680
CAT-QuickHeal	Trojan.Sigmal.S3206508	Comodo	.UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/Trojan.VDHY-8107	DrWeb	Trojan.Encoder.25725
Emsisoft	Trojan.Ransom.Armage (A)	eScan	Trojan.GenericKD.31115680
ESET-NOD32	Win32/Filecoder.NRL	F-Secure	Trojan.GenericKD.31115680
Fortinet	W32/Cryptor.BTX!tr	GData	Trojan.GenericKD.31115680
Ikarus	Trojan-Ransom.Rokku	Jiangmin	Trojan.Cryptor.hs
K7AntiVirus	Trojan (0001140e1)	K7GW	Trojan (0001140e1)
Kaspersky	Trojan-Ransom.Win32.Cryptor.btx	Malwarebytes	Ransom.Armage
MAX	malware (ai score=88)	McAfee	Artemis!BBACD7E5E7BE
McAfee-GW-Edition	BehavesLike.Win32.Dropper.ch	Microsoft	Ransom:Win32/Genasom
NANO-Antivirus	Trojan.Win32.Cryptor.ffqxui	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.8ea
Rising	Ransom.Genasom!8.293 (CLOUD)	Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen.2	TACHYON	Ransom/W32.Cryptor.828928
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	Ransom_ARMAGE.THGBDAH
TrendMicro-HouseCall	Ransom_ARMAGE.THGBDAH	VBA32	TrojanRansom.Cryptor
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Cryptor.828928
ZoneAlarm	Trojan-Ransom.Win32.Cryptor.btx	Avast Mobile Security	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۱ 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 Honest_Sample_5b598fa424596b3348b88b17.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	نتیجه‌ای یافت نشد.		
f_secure	نتیجه‌ای یافت نشد.		
kaspersky	نتیجه‌ای یافت نشد.		
eset	نتیجه‌ای یافت نشد.		
drweb	نتیجه‌ای یافت نشد.		
clam_av	نتیجه‌ای یافت نشد.		
comodo	نتیجه‌ای یافت نشد.		
bitdefender	نتیجه‌ای یافت نشد.		
avast	نتیجه‌ای یافت نشد.		
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2