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


(۰۲۱) ۴۲۶۵۰۰۰۰


(۰۲۱) ۴۲۶۵۰۰۰۰


cert.ir

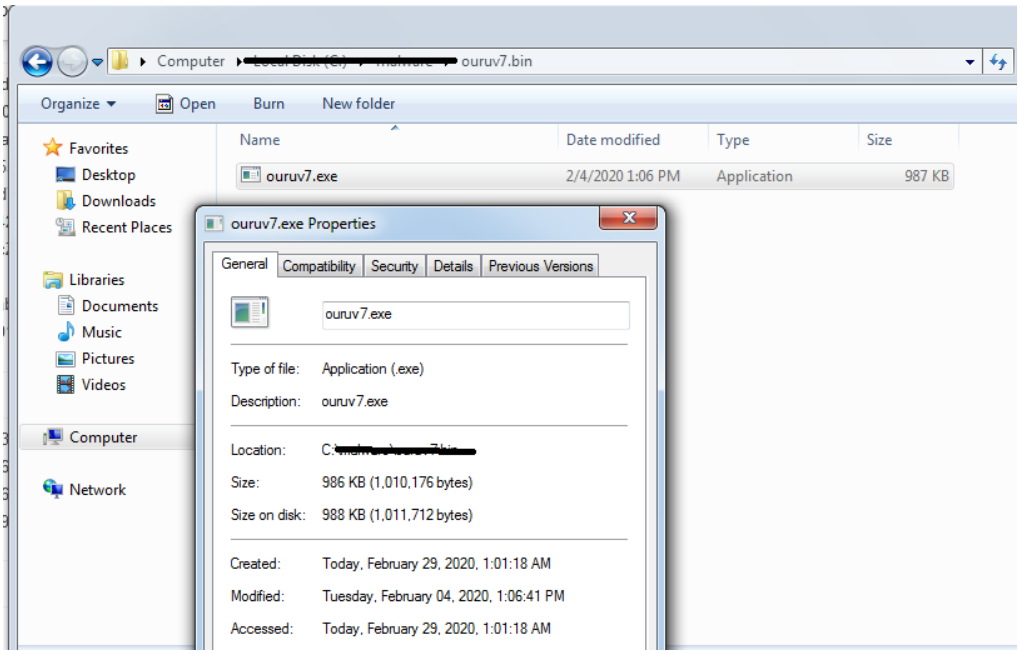
فهرست مطالب

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.

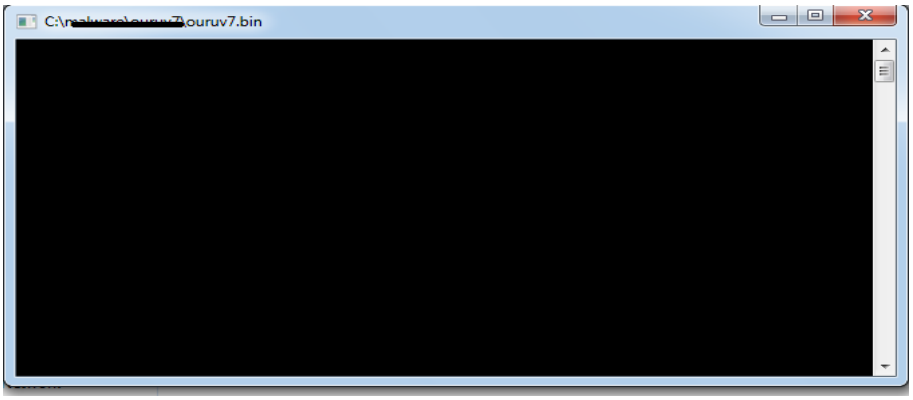
Filename.extension.Email=[Honeylock@protonmail.com]ID=[*id*].odveta

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



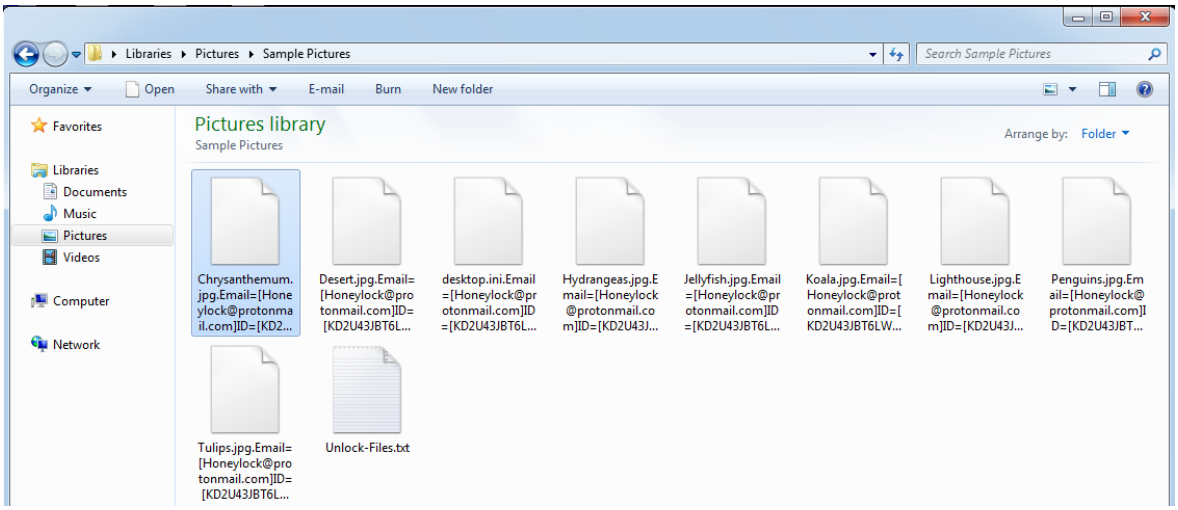
شکل ۱- آیکون فایل ouruv7

شکل ۲ لحظه اجرای باج‌افزار را نشان می‌دهد.



شکل ۲- لحظه اجرای باج‌افزار

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



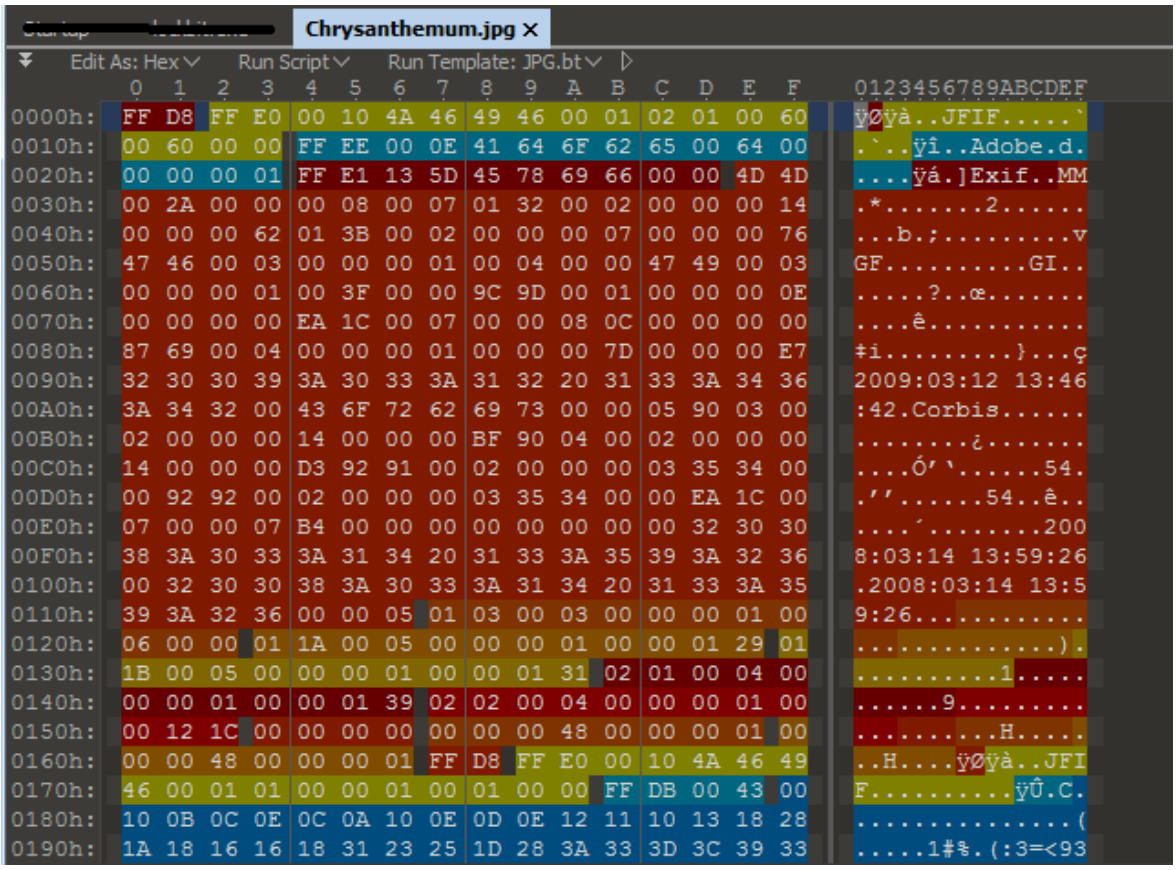
شکل ۳- نمونه فایل‌های رمزگذاری شده

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

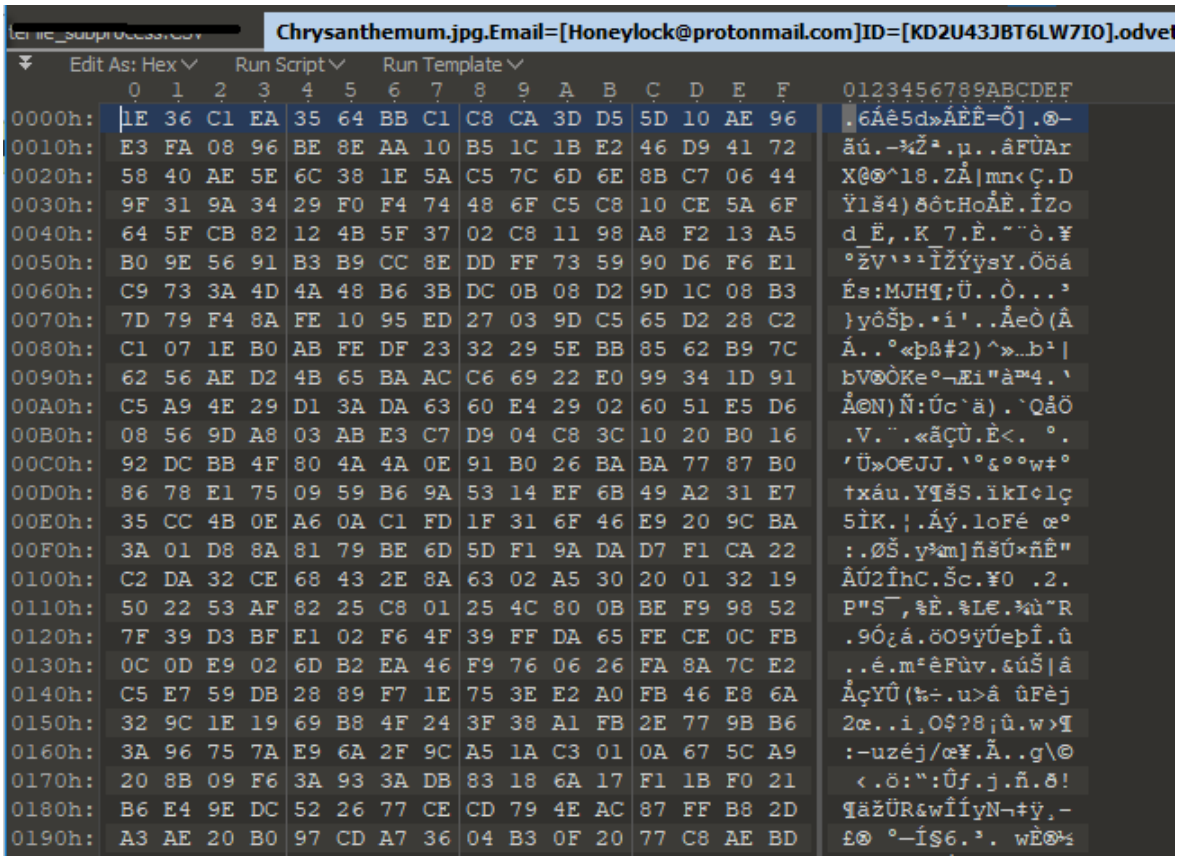
شکل ۴- پیام باج‌افزار خواهی برای قربانی

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 رمزشده (یک فایل تصویری) را در دو زمان مختلف (قبل از اجرای بدافزار و بعد از اجرای بدافزار) را نشان می‌دهد.



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



شکل ۶- محتوای نمونه فایل اجرائی بعد از رمزگذاری

۱ مشخصات فایل

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

۱-۱ کلیات فایل ouruv7

مشخصات اولیه فایل اجرائی مفروض از قبیل درهم‌سازها ، اندازه، زمان کامپایل و سایر مشخصات مربوط به کلیات فایل در جدول ۱ ذکر شده است.

جدول ۱ - مشخصات کلی فایل 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

۱-۲ Sectionهای مختلف فایل ouruv7

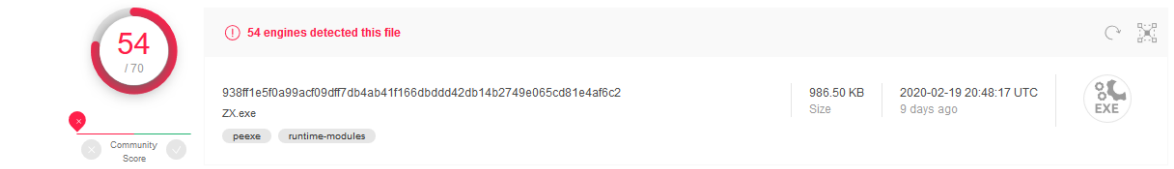
جدول ۲ مشخصات Sectionهای فایل ouruv7 را نشان می‌دهد.

جدول ۲- مشخصات Sectionهای مختلف فایل ouruv7

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	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

۱-۳ بررسی سطح تهدید فایل ouruv7

بررسی‌ها نشان می‌دهد که از تعداد ۷۰ موتور آنتی‌ویروس موجود در سامانه VirusTotal، ۵۴ مورد فایل ouruv7 را بعنوان بدافزار شناسایی کرده‌اند و در این شناسایی نیز برخی از موتورها بدافزارآن باج‌افزاری از خانواده ouroboros دانسته‌اند. شکل ۷ نتیجه ارزیابی فایل ouruv7 با VirusTotal نشان می‌دهد.



شکل ۷ – سطح تهدید فایل ouruv7 از دیدگاه ویروس توتال

شکل ۸ نیز بررسی سطح تهدید باج‌افزار ouruv7 را در سامانه ویروس‌کاو در مورخ ۹۸/۱۲/۱۰نشان می‌دهد.

آنتی ویروس	نتیجه اسکن	
Norton	✓	Clean
Max		undetected
Symantec	✓	Clean
Drweb	✓	Clean
Zillya	✓	Clean
Immunet	✓	Clean
Vba32	ii	Dangerous BScope.Trojan.DelShad
Kaspersky	ii	Dangerous
Nanoav	✓	Clean
Avast	✓	Clean
Fprot	ii	Dangerous W32/Ransom.MQ.gen!Eldorado
Trustport	ii	Dangerous Generic.Ransom.Ouroboros.B486E52D
Windefender	ii	Dangerous RansomWin32/Ouroboros.PA!MTB
Fsecure	ii	Dangerous DeepScan:Generic.Ransom.AmnesiaE.B486E52D DeepScan:Generic.Ransom.AmnesiaE.B486E52D
Emsisoft	ii	Dangerous Generic.Ransom.Ouroboros.B486E52D
Comodo	✓	Clean
Atlantis	ii	Dangerous Trojan-Ransom.Ouroboros
Clamav	✓	Clean
Clamwin	✓	Clean
Mcafee	ii	Dangerous RDN/Ransom trojan
Satfaa	ii	Dangerous
Ikarus	ii	Dangerous Trojan-Ransom.Ouroboros
Eset	ii	Dangerous Win32/Filecoder.Ouroboros.D trojan
Adaware	ii	Dangerous Generic.Ransom.Ouroboros.B486E52D
Escan	ii	Dangerous Generic.Ransom.Ouroboros.B486E52D
Gridinsoft	✓	Clean
Avira	ii	Dangerous HEUR/AGEN.1044416
Bitdefender	ii	Dangerous
Sophos	✓	Clean
ZonerAndroid	✓	Clean
TrendMicro	✓	Clean
Gdata	ii	Dangerous Generic.Ransom.Ouroboros.B486E52D
BitdefenderAndroid	✓	Clean
AvgAndroid	✓	Clean
AvastAndroid	✓	Clean

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

۲ شرح تحلیل

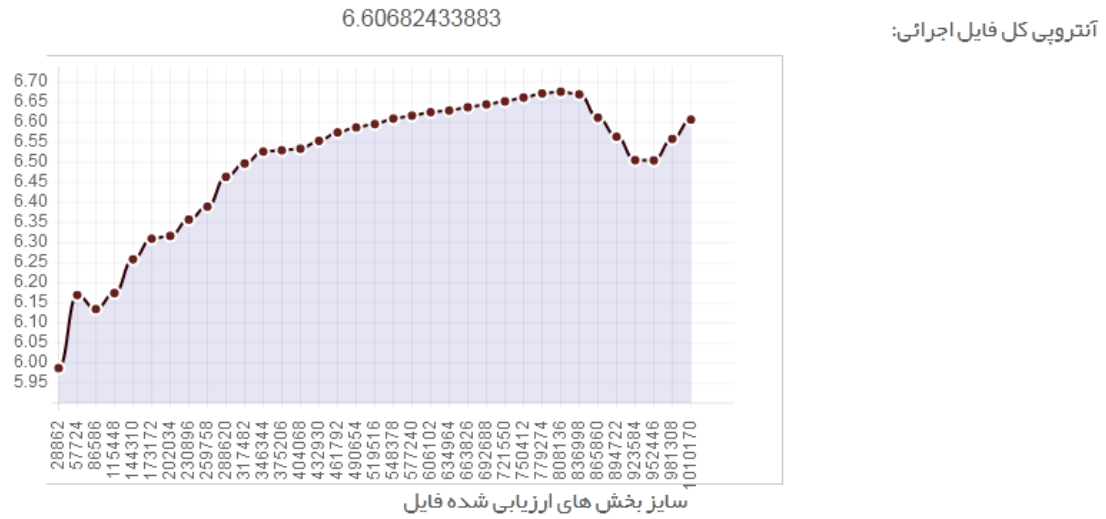
شرح تحلیل باج‌افزارouruv7 در سه قسمت ارائه می‌شود:

۲-۱ بررسی ساختار فایل ouruv7 براساس تحلیل ایستا

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

۲-۱-۱ آنتروپی

روند صعودی و مقدار بیش از ۷ مقدار آنتروپی احتمال رفتار بدافزاری فایل اجرائی را افزایش می‌دهد. شکل ۹ آنتروپی فایل ouruv7 را نشان می‌دهد که برابر با 6.60 است.



شکل ۹- آنتروپی فایل ouruv7

۲-۱-۲ کتابخانه‌ها و توابع استفاده شده

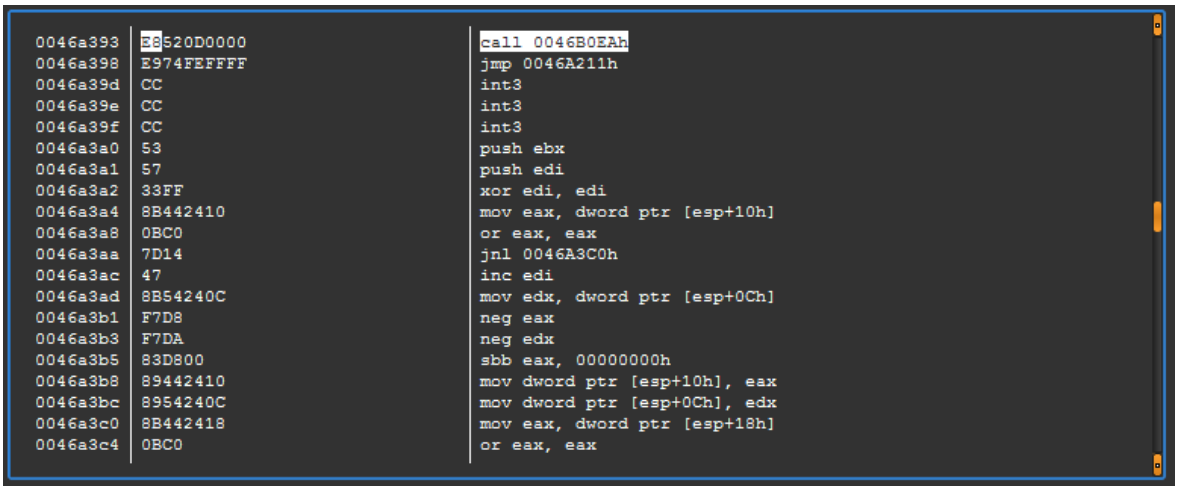
جدول ۳ براساس تحلیل ایستا کتابخانه‌ها و توابع استفاده شده در ساختار فایل ouruv7 را نشان می‌دهد. بررسی استاتیک توابع استفاده شده در فایل اجرائی مفروض، احتمال فعالیت‌های مخرب Information Gathering، IATHooking را نشان می‌دهد.

جدول ۳- کتابخانه‌ها و توابع استفاده شده

کتابخانه	توابع استفاده شده
KERNEL32.dll	FindClose, CloseHandle, lstrcmpW, 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, WSAStartup, htons, ioctlsocket, closesocket, freeaddrinfo, getaddrinfo, inet_ntoa, inet_addr, WSAGetLastError, select, recv, ntohl, htonl, getpeername, connect, socket, setsockopt, send,

۳-۱-۲ تحلیل مقاومتی

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



شکل ۱۰- هگزادسیمال و Disassembly فایل در نقطه شروع

بررسی امضا نقطه شروع فایل اجرایی 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 اجرائی 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.

۲-۲-۱ فرآیندهای ایجاد شده

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

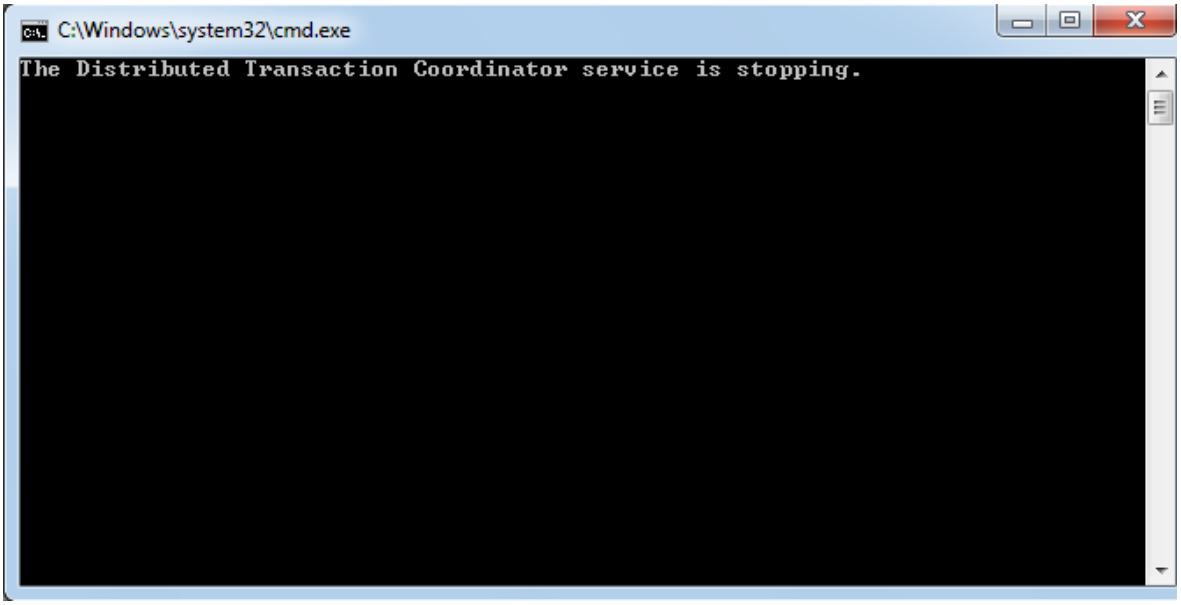
جدول ۵- فرایندهای ایجاد شده

فرایندها و دستورات command line

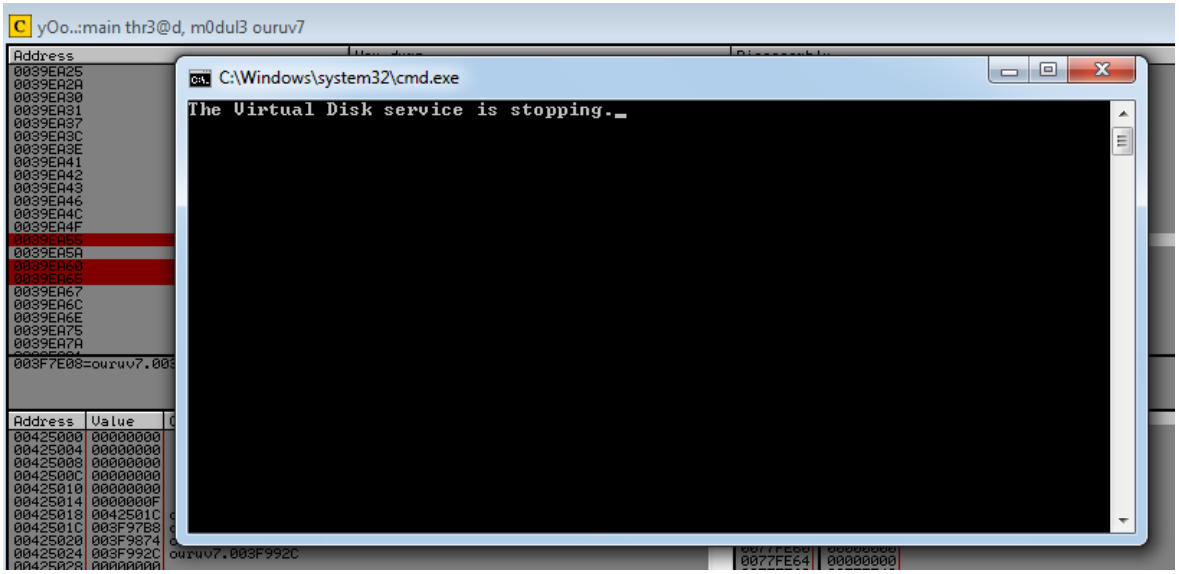
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop SQLWriter
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop SQLBrowser
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop MSSQLSERVER
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop MSSQL$CONTOSO1
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop MSDTC
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c bcdedit /set {default} recoveryenabled no
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c wbadmin delete catalog –quiet
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop SQLSERVERAGENT
• C:\Windows\System32\cmd.exe
  • **Command line**: C:\Windows\system32\cmd.exe /c net stop MSSQLSERVER
• C:\Windows\System32\cmd.exe
  ○ **Command line**: C:\Windows\system32\cmd.exe /c net stop vds
• C:\Windows\System32\cmd.exe
  ○ Command line: C:\Windows\system32\cmd.exe /c netsh advfirewall set currentprofile state off
• C:\Windows\System32\cmd.exe
  • **Command line**: C:\Windows\system32\cmd.exe /c netsh firewall set opmode mode=disable

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 اجرائی ouruv7 را نشان می‌دهد.

جدول ۶- بررسی سطح رجیستری

Operation	path
RegCreateKey	▪ HKLM\System\CurrentControlSet\Services\NapAgent\Qecs ▪ HKLM\System\CurrentControlSet\Services\NapAgent\Shas ▪ HKLM\System\CurrentControlSet\Services\Tcpip\Parameters ▪ HKLM\System\CurrentControlSet\Services\NapAgent\LocalConfig ▪ HKCU\SYSTEM\CurrentControlSet\Control\NetTrace ▪ HKCU\System\CurrentControlSet\Control\NetTrace\Session ▪ HKLM\System\CurrentControlSet\services\napagent\LocalConfig\Enroll\HcsGroups ▪ HKLM\System\CurrentControlSet\services\napagent\LocalConfig\UI ▪ HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0
RegSetValue	• HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\LanguageList • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-100 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-101 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-102 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-103 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-100 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-101 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-102 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-103 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-1 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-2 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-3 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-4 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-100 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-101 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-102 • HKCU\Software\Classes\Local Settings\MuiCache\112\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-103 • HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\16000009\Element • HKLM\BCD00000000\Objects\{64e91fe3-0aa9-11e8-b0e9-83753d9bc567}\Elements\250000e0\Element

۲-۲-۳ کتابخانه‌های بارگذاری شده

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

جدول ۷- کتابخانه‌های بارگذاری شده

کتابخانه‌های بارگذاری شده
• C:\Windows\System32\cryptsp.dll • C:\Windows\System32\rsaenh.dll • C:\Windows\System32\mswsock.dll • C:\Windows\System32\user32.dll • C:\Windows\System32\gdi32.dll • C:\Windows\System32\lpk.dll • C:\Windows\System32\usp10.dll • C:\Windows\System32\imm32.dll • C:\Windows\System32\msctf.dll • C:\Windows\System32\WSHTCPIP.DLL

۲-۲-۴ بررسی‌های سطح فایل

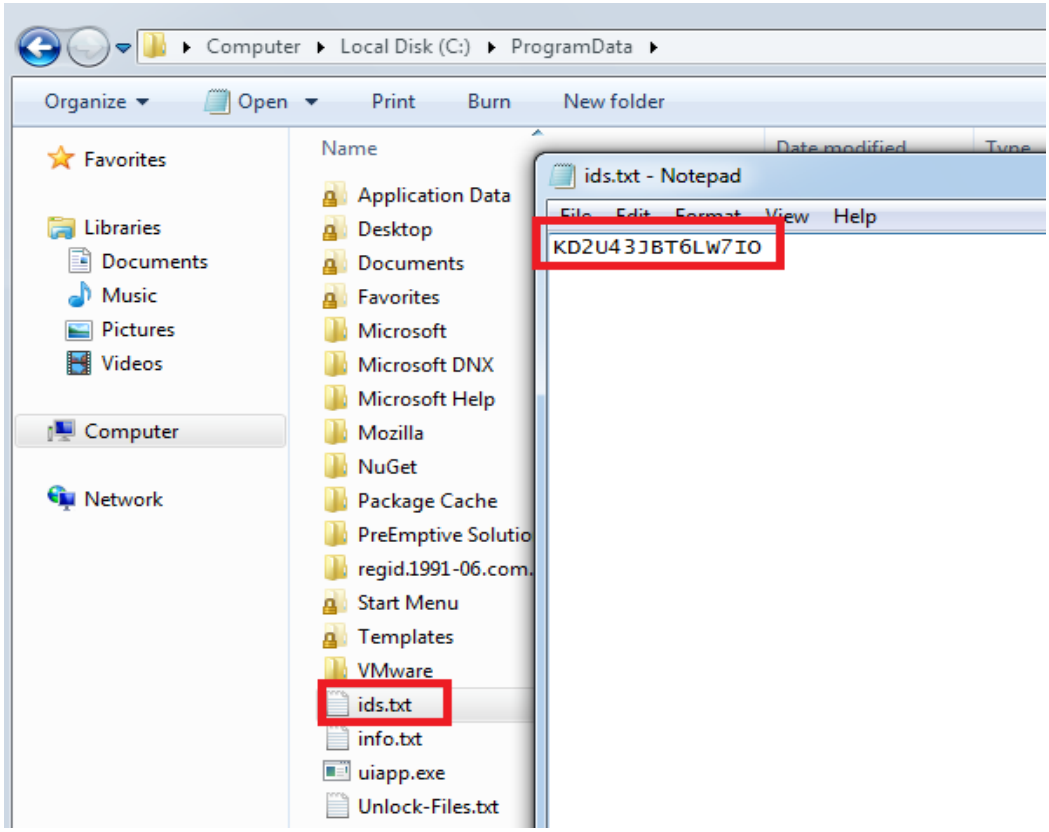
جدول ۸ نمونه فایل‌های رمزگذاری شده توسط باج‌افزار ouruv7 را نشان می‌دهد.

جدول ۸- بخشی از فایل‌های رمزگذاری شده

نمونه‌ای از فایل‌های رمزگذاری شده
• C:\Program Files\Microsoft Analysis Services\AS OLEDB\110\msmdlocal.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Microsoft Office\Office15\EXCEL.EXE.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\OllyDBG2I\WIN32.HLP.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\R4ndoms_OllyDBG\Win32Help Files\WIN32.HLP.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\malware\testdump\fullmemory dumpvurten.dmp.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Microsoft Office\Templates\1033\IntroducingPowerPoint2010.potx.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Graphviz2.38\share\graphviz\examples\world.gv.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Cracker Tools 2.3 By yildo\unpacker\InstallShield Unpacker\Unpack Smart Install Maker.swf.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Common Files\VMware\Drivers\video_wddm\vm3dgl.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Cracker Tools 2.3 By yildo\Disassembler\ida61\QtWebKit4.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta" • C:\Program Files\Microsoft Office\Office15\1033\PSRCHSRN.DAT.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta"

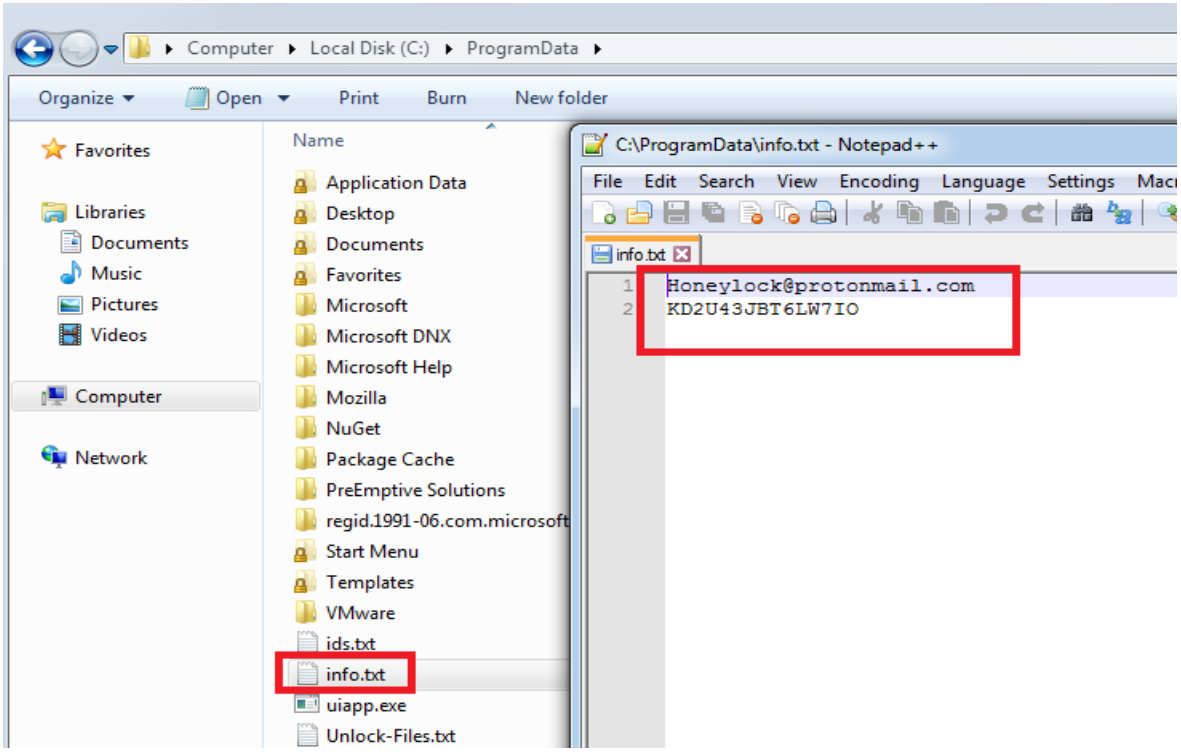
- C:\Program Files\Common Files\microsoft shared\TRANSLAT\ESEN\MSB1ESEN.ITS.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta"
- C:\Program Files\Cracker Tools 2.3 By yildo\Debuggers\JangOLLy\dbghelp.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta"
- C:\Program Files\Cracker 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_Decompiler\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\OllyDgb 4fr33\dllhelp.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\ipcsecproc.dll.Email=[Honeylock@protonmail.com]ID=[QDKM24ABWZP9CHU].odveta"
- C:\Program Files\Cracker Tools 2.3 By yildo\Web-Tool\CharlesV3.9.2\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\OllyDBG2I\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\AutoDiagramer.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 فایلی متنی با عنوان ids.txt ایجاد نموده که محتوای آن id مربوط به قربانی است.



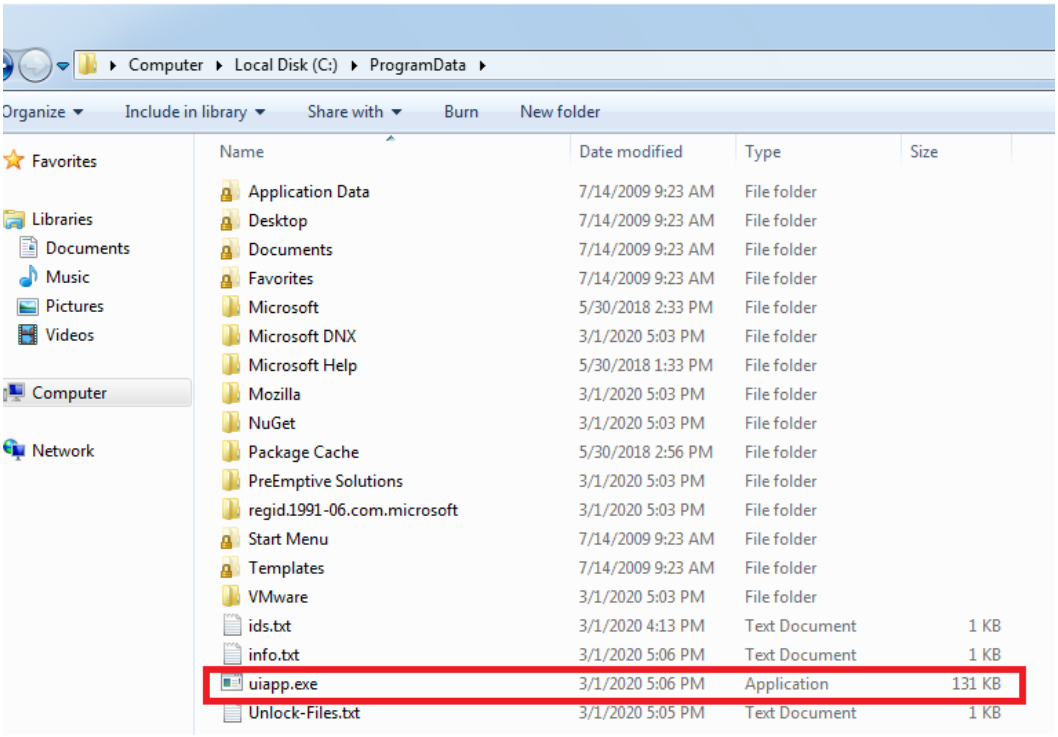
شکل ۱۳- فایل متنی ids.txt

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 ، اجرائی است. در سامانه ویروس توتال ۴۳ آنتی ویروس از ۷۳ آنتی ویروس آن را بعنوان بدافزار شناسایی کرده است.



شکل ۱۵- فایل اجرائی uiapp.exe

۵-۲-۲ 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 /1614CEEEC50A9336EBF690886CAA747D6811C45D37086A3FA7B11C9E83926C6C 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

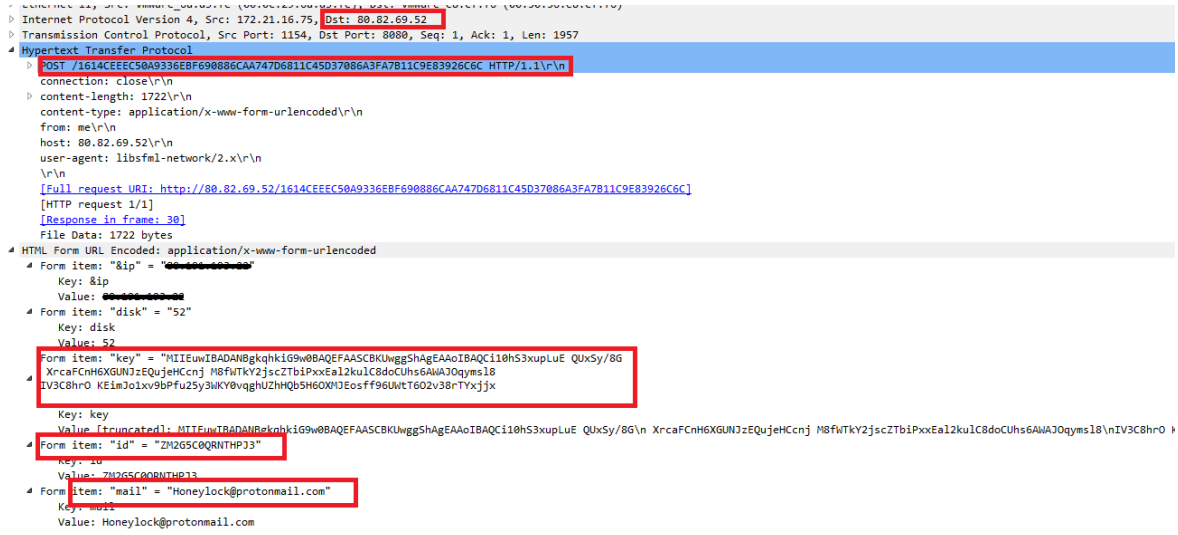
شکل ۱۷- پروتکل DNS

- 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

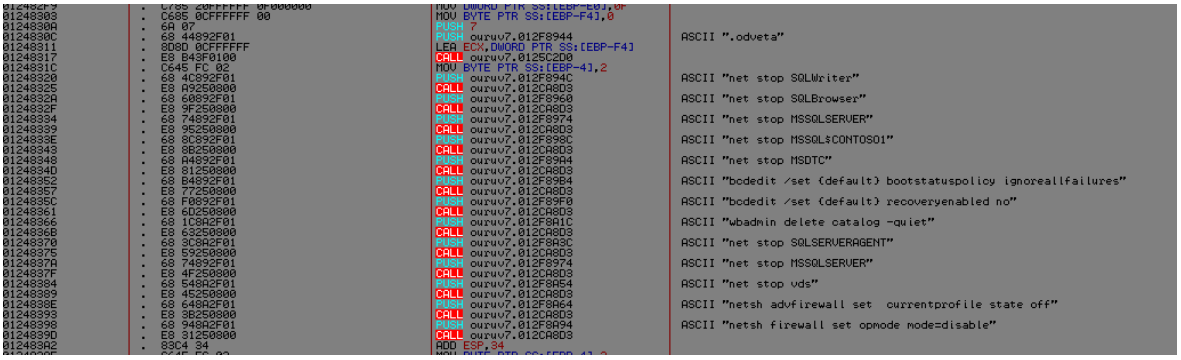
شکل ۱۹- url مربوط به درخواست GET



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

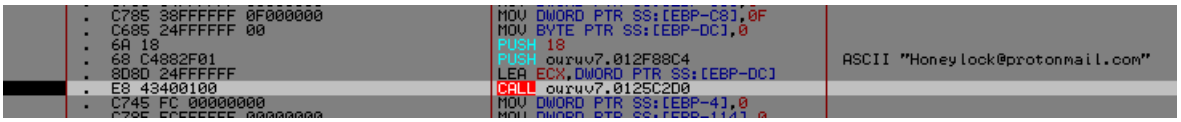
۳-۲ بررسی کد

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.



شکل ۲۱- غیرفعال کردن سرویس‌ها در سیستم قربانی

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



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 باج افزار اشاره می‌شود:

- اطمینان از تهیه نسخه پشتیبان
- استفاده از آنتی‌ویروسی که دارای تشخیص رفتار است
- نصب به‌روزرسانی‌های سیستم‌عامل
- بروز نگه داشتن برنامه‌ها
- اعمال فیلترهای SPAM
- فعال کردن مشاهده پسوند برنامه‌ها

- پیوست‌ها را باز نکنید مگر با تأیید شخصی که آنرا به شما ارسال کرده است
- مراقبت در اینترنت دانلود
- تغییر نام Vssadmin در ویندوز
- غیر فعال کردن اسکریپت ویندوز
- غیرفعال کردن Windows PowerShell
- استفاده از کلمات عبور قوی
- غیرفعال کردن Remote Desktop یا تغییر پورت آن
- راه اندازی سیاست های محدودیت نرم افزار در ویندوز