بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

تحلیل بدافزار DOP Ransomware

گزارش تحلیل بدافزار

شناسه سند ..... Maher_13990402-3

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۳/۳۱

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 مقدمه

با توجه به رشد چشمگیر در حوزه‌ی بدافزار در دنیای امروزی متعاقبا باج‌افزار نیز رشد قابل توجهی داشته است. یکی از این باج‌افزارها DOP می‌باشد که یک نسخه دیگر از خانواده و Dharma/Crysis و شبیه به گزارش قبلی (تحلیل باج‌افزار RXX) می‌باشد و برای اولین بار توسط یک محقق مشهور امنیتی به نام dnwls0719 کشف شد. این باج‌افزار مانند سایر نسخه های دیگر، از قربانی می‌خواهد مبلغ مشخصی را به عنوان باج در ازای رمزگشایی بپردازد. این باج‌افزار با توجه به یافته‌ها و بررسی‌های محققین حوزه بدافزار اوایل March سال ۲۰۱۷ میلادی ایجاد شده، ولی اولین مشاهدات آن در سال ۲۰۲۰ می‌باشد. در بررسی‌های صورت گرفته نوع جدیدی از باج‌افزار از خانواده Dharma در حال گسترش هستند که در مقایسه با نسخه‌های قبلی می‌توان به نوع پیام متنی ارائه شده توسط باج‌افزار اشاره کرد.

این باج‌افزار نیز مانند نسخه های موجود دیگر در طی فرآیند رمزگذاری، کلیه فایل‌ها را براساس این الگو تغییر نام می‌دهد: نام اصلی فایل ، شناسه منحصر به فرد، آدرس ایمیل مجرمان سایبری و پسوندdop . در انتهای هر فایل. به عنوان مثال ، فایلی به نام sample.jpg به " sample.jpg.id-1E9800D. [dayonpay@aol.com] .DOP" تغییر می‌یابد. براساس آخرین اطلاعات بدست آمده، این باج‌افزار نیز مانند باج‌افزارهای دیگر از طریق پیوست‌های ایمیل آلوده (ماکرو)، وب سایت‌های تورنت، تبلیغات مخرب انتشار می‌یابد.

مهاجمان بصورت مستقیم مبلغ باج را تعیین نکرده‌اند و کاربران قربانی شده باید با استفاده از آدرس‌های ایمیلی که در فایل راهنما نمایش داده می‌شود با مهاجمان ارتباط برقرار کنند تا مقدار و نحوه پرداخت باج مشخص گردد. آدرس‌های ایمیل بصورت dayonpay@aol.com و dayonpay@goat.si می‌باشند. مهاجمان در فایل متنی خاطر نشان کردن درصورتی که کاربران در طول ۱۲ ساعت از طریق ایمیل اول با آنها ارتباط برقرار نکنند باید برای برقراری ارتباط از طریق ایمیل دومی که مشخص شده برای برقراری ارتباط اقدام نمایند.

۲ مشخصات و ریزجزئیات فایل باج‌افزار

جداول و نمودارهای موجود در این بخش نشان‌دهنده ریزجزئیات فایل اجرایی باج‌افزار می‌باشند که در طول تحلیل‌های استاتیک و پویا توسط ابزارهای مختلف بدست آمده‌اند. این اطلاعات شامل مواردی همچون اندازه فایل، مقادیر هش فایل، وضعیت شناسایی فایل در ویروس‌توتال و ویروس‌کاو و غیره می‌باشد.

۲-۱ مشخصات فایل

همانطور که قبلا اشاره گردید این بدافزار از خانواده باج‌افزار و برای رمزگذاری فایل مورد استفاده قرار می‌گیرد که با استفاده از زبان برنامه‌نویسی C++ طراحی و پیاده‌سازی شده است. جدول زیر مشخصات کلی باج افزار DOP را نشان می‌دهد.

جدول ۱ - ریزجزئیات مربوط به باج‌افزار

هش md5	BA0693CEDEBCF9714553728B1785A0F1
هش SHA1	AB5673CEF6B74FB8B3CA4A2213081DF7C66D3B4D
هش SHA256	1919EC3094BB0297CFCCA7716658336202FFE43629301AC0F368EB16A4554CAB
نوع بدافزار	Ransomware, Crypto Virus, Files locker
نام بدافزار	DOP (Dharam Family)
پسوند	-Id.[back_datafoxmail.com].dop
نحوه انتشار	Infected email attachments (macros), torrent websites, malicious ads.
زمان کامپایل	2017-03-02
کامپایلر	Microsoft Visual C++
حجم فایل	94720 bytes
آنتروپی کلی فایل	7.454
معماری فایل	32 bits
آدرس فایل Pdb	C:\crysis\Release\PDB\payload.pdb

۲-۲ بخش‌های مختلف فایل

جدول زیر نیز بخش‌های مختلف تشکیل‌دهنده فایل باج‌افزار را با جزئیات کامل مانند مقدار آنتروپی، اندازه خام، اندازه مجازی هر بخش و غیره نشان می‌دهد. این فایل متشکل از سه بخش text، rdata، data است.

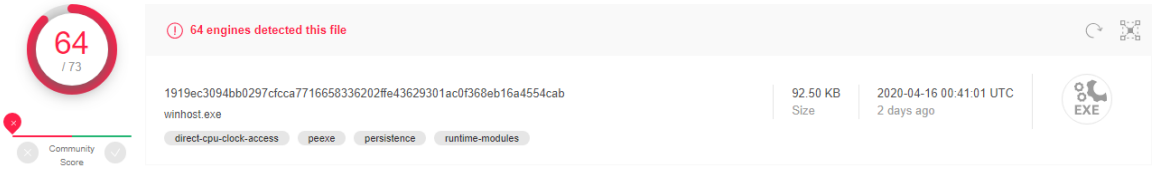
جدول ۲- بخش‌های و مشخصات مربوط به آن‌ها

ردیف	نام	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی	بایت‌های اولیه
1	.text	00001000	00009c25	00009e00	5.965	55 8B EC 83 EC 24 53 56 57
2	.rdata	0000b000	00002636	00002800	7.785	B0 41 00 00 BE 41 00 00 D0
3	.data	0000e000	0000aad5	0000a800	7.982	98 3F 40 00 88 3F 40 00 60

با توجه به مقادیر نشان داده شده در جدول ۱ و ۲، مقدار آنتروپی کلی فایل به بخش‌های rdata و data مقداری بالاتر از هفت می‌باشد که نشان‌دهنده مشکوک بودن فایل و بخش‌های ذکر شده می‌باشد. مقادیر بالای هفت و روند صعودی و همچنین مقدار صفر آنتروپی دگردیسی و چندریختی و رفتار غیر عادی، بدافزار بودن فایل را نشان می‌دهد.

۳-۲ وضعیت شناسایی فایل در ویروس‌توتال

شکل زیر وضعیت تشخیص فایل مورد بررسی را در ویروس‌توتال نشان می‌دهد. در این سامانه از بین ۷۳ موتور تحلیل ۶۴ موتور قادر به شناسایی فایل بعنوان یک فایل بدافزار شده‌اند و درصورت استفاده از نسخه‌های بروزشده این موتورهای آنتی‌ویروس در سیستم می‌توان از انتقال و اجرای آن جلوگیری کرد.



شکل ۱ وضعیت تشخیص فایل در ویروس توتال

۴-۲ وضعیت شناسایی فایل در ویروس‌کاو

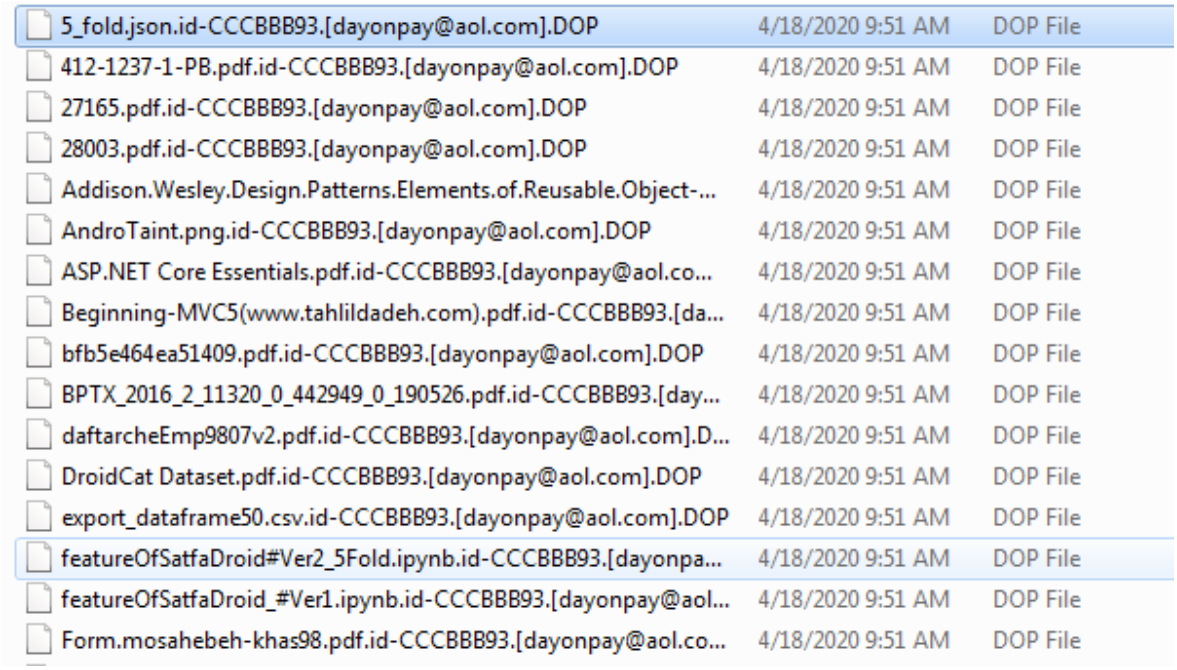
شکل زیر نشان دهنده وضعیت تشخیص فایل را در سامانه بومی ویروس‌کاو نشان می‌دهد. در این سامانه از بین ۳۹ موتور موجود تعداد ۳۰ موتور قادر به تشخیص فایل به عنوان فایل مخرب و بدافزار می‌باشند و تنها ۹ موتور قادر به شناسایی نبوده و یک موتور جوابی برای فایل ارسال نکرده است.

شکل ۲ وضعیت تشخیص فایل در ویروس‌کاو

۳ فرایند آلوده‌سازی

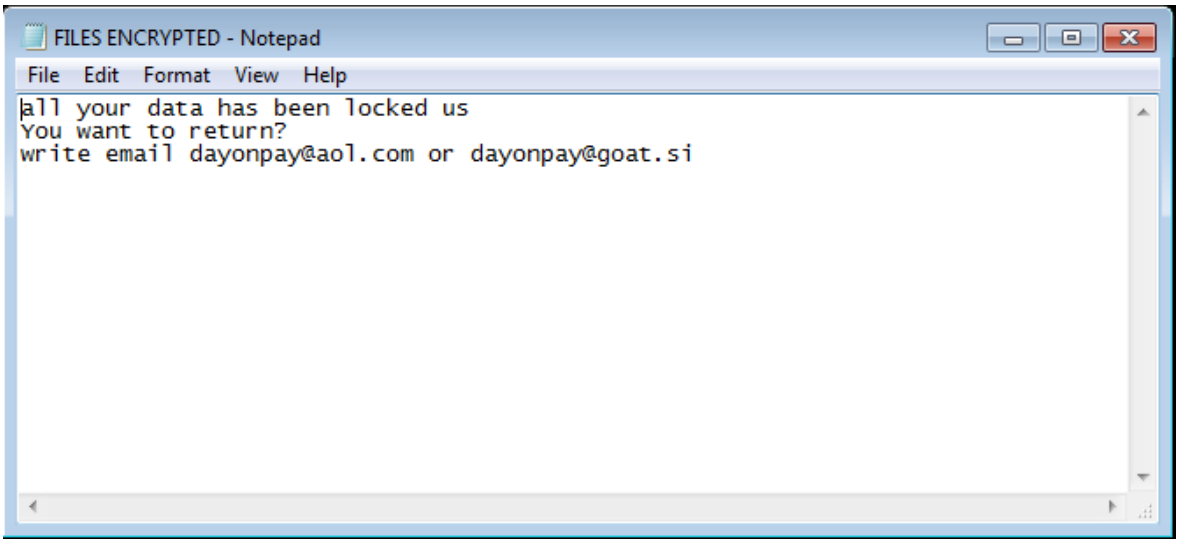
باج‌افزار DOP یکی از باج¬افزارهای انتشار یافته در اواخر March سال ۲۰۲۰ میلادی می‌باشد که یک نسخه دیگر از خانواده باج‌افزار Dharma/Crysis می‌باشد که با استفاده از فایل‌های ضمیمه ایمیل‌های جعلی، تبلیغات آلوده و وب سایت‌های تورنت به سیستم کاربران قربانی شده انتقال می‌یابد. این باج افزار فایلها را با کلید رمزنگاری AES رمزگذاری می‌کند. باج‌افزار DOP می‌تواند وحشتناک باشد زیرا ممکن است مجدداً دوباره خود را فعال کند، زیرا فایل‌های خود را روی رایانه‌ها مخفی نگه می‌دارد. این باج‌افزار در طی فرآیند رمزگذاری، کلیه فایل‌ها را براساس این الگو تغییر نام می¬دهد: نام اصلی فایل، شناسه منحصر به فرد، آدرس ایمیل مجرمان سایبری و پسوند.dop .باج‌افزار در طول فرآیند اجرا رمزگذاری کلیدهای رجیستری مختلف را ثبت کرده و فایل‌هایی را در سیستم ایجاد می‌کند. این عملیات ثبت و ایجاد، به این دلیل می‌باشد که بدافزار در سیستم، هر زمان درحال فعالیت باشد. پس از اتمام این فرآیند، یک پنجره بازشو نمایش داده می‌شود، و یک فایل متنی بصورت FILES ENCRYPTED ایجاد می‌شود، که در این فایل متنی یک شناسه به کاربر اختصاص داده شده است که این فایل متنی در دسک تاپ کاربر نمایش داده می‌شود.

آدرس‌های ایمیل بصورت dayonpay@aol.com و dayonpay@goat.si می‌باشند. مهاجمان در فایل متنی خاطر نشان کردن درصورتی که کاربران در طول ۱۲ ساعت از طریق ایمیل اول با آنها ارتباط برقرار نکنند باید برای برقراری ارتباط از طریق ایمیل دومی که مشخص شده برای برقراری ارتباط اقدام نمایند.



شکل ۳ نمونه فایل‌های رمزشده توسط باج‌افزار

شکل ۴ فایل راهنما ایجاد شده توسط باج افزار



شکل ۵ فایل متنی ایجاد شده در داخل هر پوشه

۴ شرح تحلیل

در این بخش نتیجه تحلیل و بررسی فایل باج‌افزار توسط ابزارهای تحلیل استاتیک و پویا در قسمت‌های مختلف نشان داده می‌شود و شامل مواردی مانند کتابخانه و توابع، رشته‌ها، فعالیت‌های شبکه و غیره می‌باشند.

۴-۱ کتابخانه و توابع مورد استفاده

فایل اجرایی باج‌افزار با استفاده از تکنیک‌های مبهم‌سازی[۱]، توابع و رشته‌های آن را تغییر داده که هنگام دیس‌اسمبل کردن فایل، تعداد کتابخانه و توابع را محدود نشان داده و رشته‌ها را بصورت کاراکترهای ناخوانا نشان می‌دهد. لذا هنگام فرایند دیس‌اسمبل کتابخانه و توابع موجود در جدول زیر بدست می‌آید.

جدول ۳ کتابخانه و توابع مورد استفاده از باج‌افزار

کتابخانه و توابع	Kernel32.dll
	WaitForSingleObject، InitializeCriticalSectionAndSpinCount، LeaveCriticalSection، EnterCriticalSection، ReleaseMutex، GetProcAddress، LoadLibraryA، GetLastError،CloseHandle

درمیان این توابع، توابعی همانند GetProcAddress و LoadLibrary قابل توجه می باشد. همچنین رشته‌های موجود و قابل دسترس هنگام دیس‌اسمبل نیز در جدول زیر قابل مشاهده می‌باشد که در برخی موارد با استفاده از عملیات مبهم‌سازی به رشته‌های ناخوانا که معنی و مفهوم خاصی ندارد، تبدیل شده‌اند.

جدول ۴ رشته‌های قابل استخراج از فایل باج‌افزار

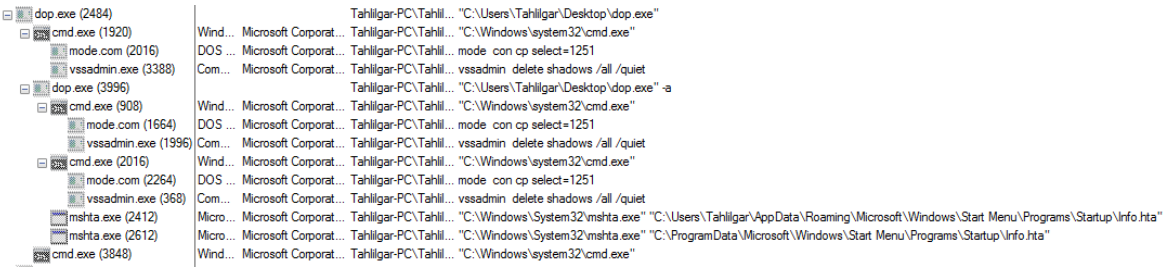
رشته‌های قابل دریافت
C:\crysis\Release\PDB\payload.pdb
!This program cannot be run in DOS mode.
GetProcAddress
LoadLibraryA
GetLastError
WaitForSingleObject
InitializeCriticalSectionAndSpinCount
LeaveCriticalSection
EnterCriticalSection
ReleaseMutex

۴-۲ پروسس‌های ایجاد شده توسط باج‌افزار

در شکل زیر پروسس‌ها و فرایندهای که در حین اجرای باج‌افزار ایجاد شده نشان داده شده است که در آن باج‌افزار با اجرای CMD در سیستم دستورات مختلفی را اجرا می‌کند. از این دستورات به دلیل پاکسازی Shadowها استفاده شده است.

---

[۱] Obfuscator



شکل ۶ ساختار درختی پروسس‌های اجرای در طول فعالیت باج‌افزار

۳-۴ فایل‌های ایجاد شده

همانطور که در قسمت‌های بالا نیز اشاره شد باج‌افزار درطول اجرای خود فایل‌هایی را در مسیرهایی از سیستم ایجاد می‌کند. این فایل‌های ایجاد شده همان فایل اصلی باج‌افزار و فایل‌های راهنما می‌باشد که در مسیر Startup برای اجرای آن در هربار اجرای سیستم عامل ایجاد شده‌اند.

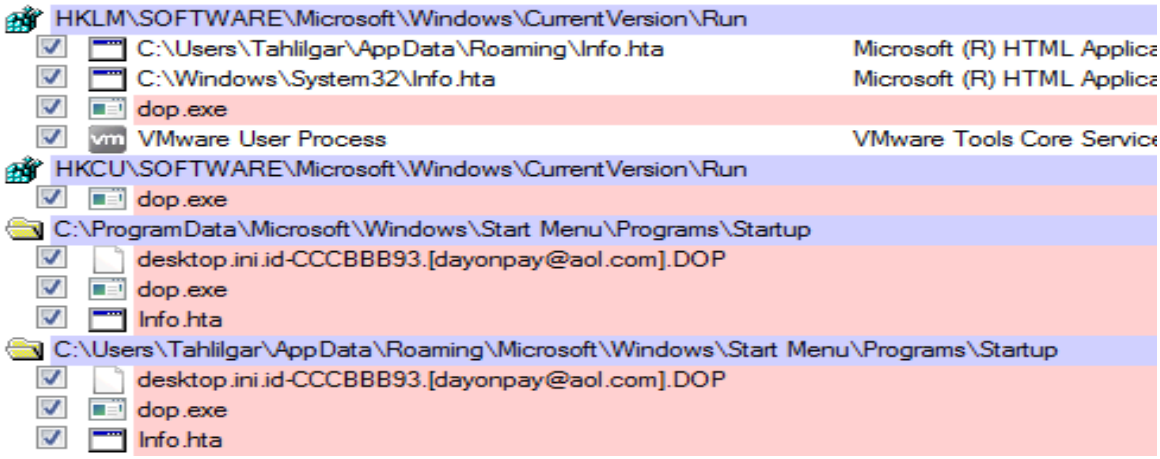
1. C:\Users\Tahlilgar\AppData\Roaming\dop.exe
2. C:\Users\Tahlilgar\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\dop.exe
3. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\dop.exe
4. C:\FILES ENCRYPTED.txt
5. C:\Users\Tahlilgar\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
6. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta

۴-۴ تغییرات رجیستری

عبارت و شکل زیر آدرس رجیسترهای ثبت شده توسط باج‌افزار درسیستم را نشان می‌دهد.

1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\dop.exe
2. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\C:\Windows\System32\Info.hta
3. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\C:\Users\Tahlilgar\AppData\Roaming\Info.hta

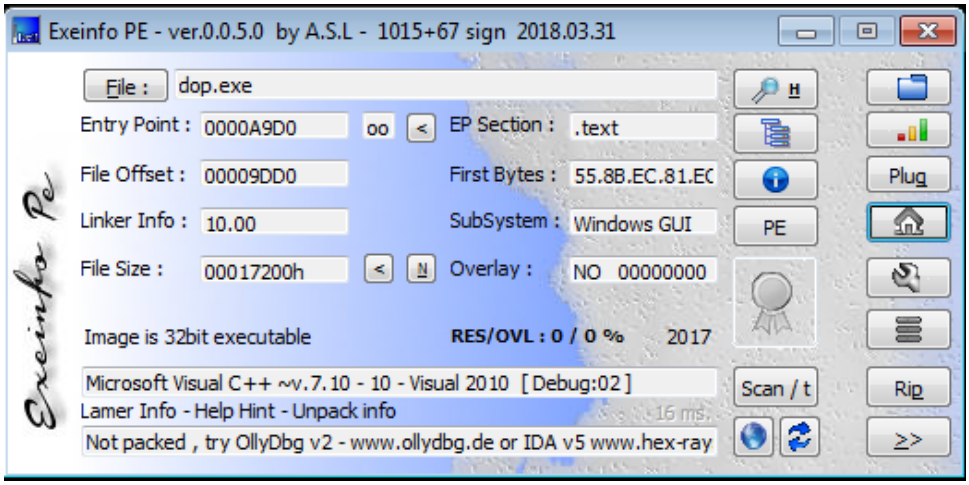
شکل زیر نیز این کلیدها را نشان می‌دهد که در سیستم ثبت شده‌اند.



شکل ۷ ساختار رجسترهای باز و خوانده شده

۴-۵ شناسایی کامپایلر

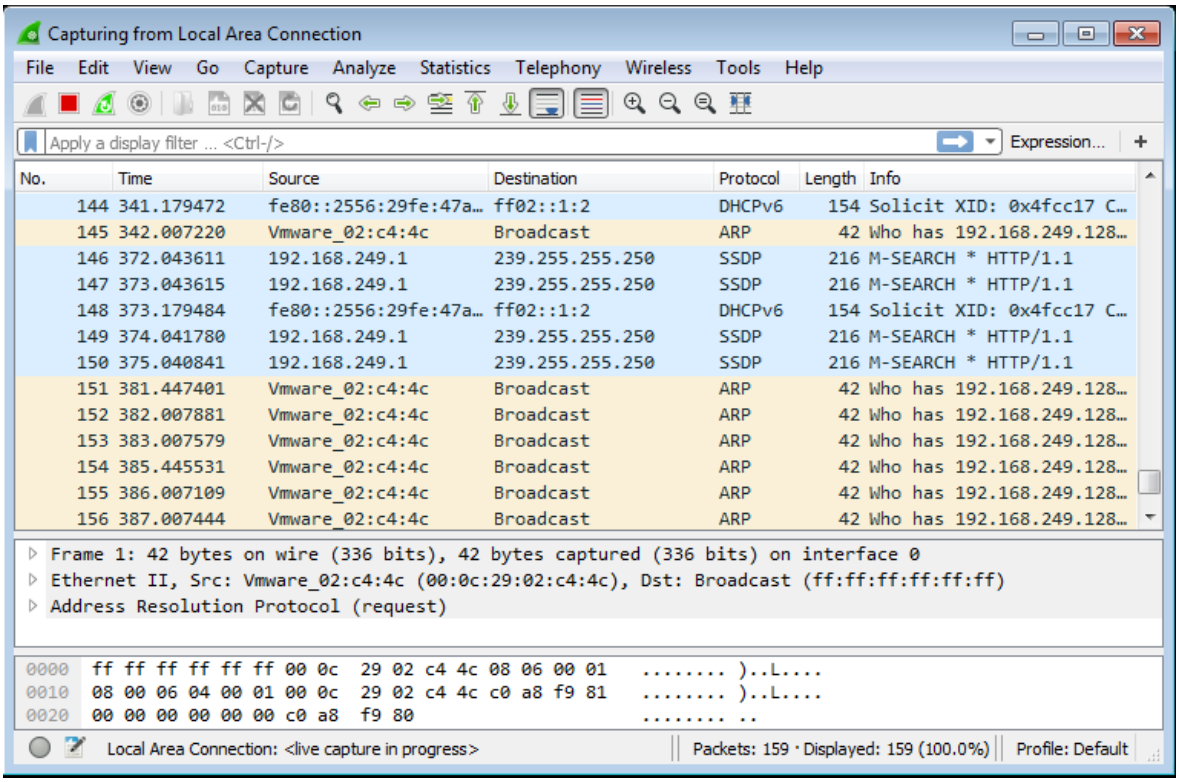
کامپایلر و زبان برنامه نویسی فایل باجافزار C++ می‌باشد. شکل زیر این نتیجه را توسط ابزار تشخیص کامپایلر نشان می‌دهد.



شکل ۸ شناسایی کامپایلر

۴-۶ ارتباطات شبکه

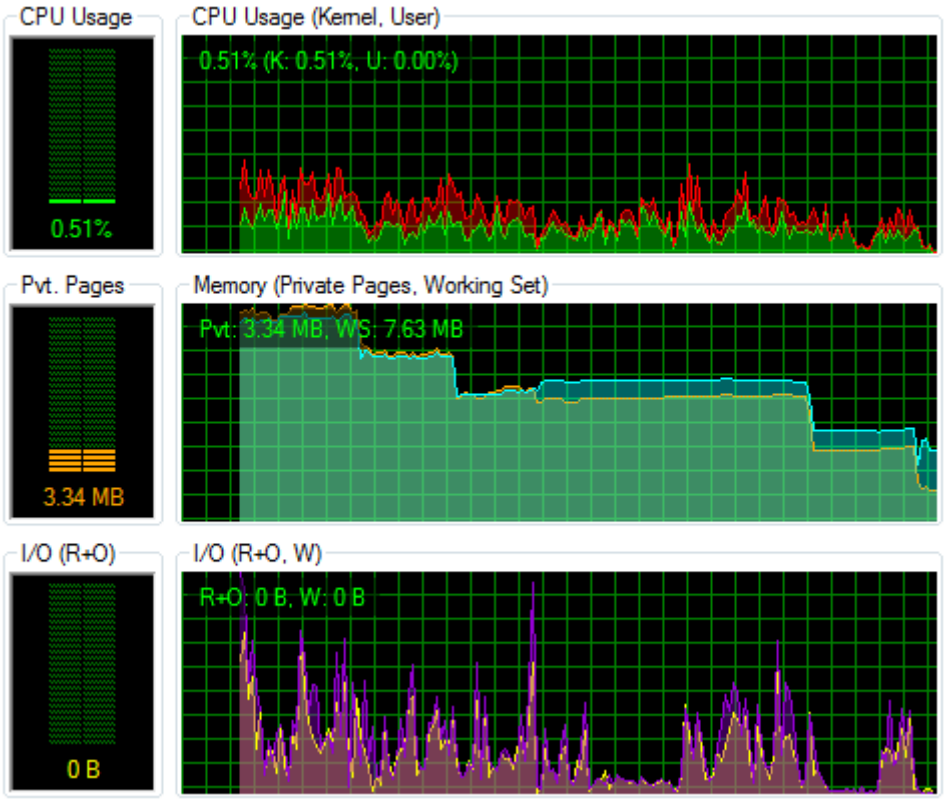
باتوجه به بررسی های صورت گرفته در طول اجرای باجافزار در سیستم هیچ نوع فعالیتی مبنی بر ارتباط شبکه مشاهده نگردید، که در شکل زیر می‌توان این فعالیت را مشاهده کرد.



شکل ۹ بررسی فعالیت شبکه در طول اجرای باجافزار

۷-۴ وضعیت منابع سیستم

شکل زیر وضعیت مصرف منابع سیستم را در زمانی که باجافزار در حال فعالیت است را نشان می‌دهد. با توجه به شکل مشاهده می‌گردد که میزان استفاده از CPU پایین بوده ولی میزان استفاده از MEMORY و I/O بیشتر بوده و در طول فعالیت باجافزار میزان بیشتری از آن‌ها را درگیر کرده است.



شکل ۱۰ وضعیت منابع سیستم در طول اجرای باج‌افزار

۵ توصیه‌های امنیتی برای پیشگیری

۱. گرفتن فایل پشتیبان بصورت دوره‌ای از فایل‌های سیستم و ذخیره آن در محل دیگر
۲. استفاده از آنتی‌ویروس قوی و بروزرسانی مداوم آن
۳. خودداری از بازکردن و اجرا فایل‌های مشکوک و ناشناس
۴. خودداری از بازکردن ایمیل‌های مشکوک و ناشناس
۵. اطمینان از سالم بودن دستگاه‌های جانبی مانند فلش
۶. استفاده از رمزعبور قوی بر روی درایوهای سیستم
۷. استفاده از سیستم‌عامل جدید و بروزرسانی شده
۸. بروزرسانی مداوم سیستم عامل
۹. پیکربندی مناسب پروتکل‌های مورد استفاده در شبکه متناسب با محیط کار