بسمه تعالی

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

# گزارش تحلیلی بدافزار RXX Ransomware

## گزارش تحلیل بدافزار

| | |
|---|---|
| شناسه سند | Maher_13990424-2 |
| نوع سند | گزارش فنی |
| شماره نگارش | ۱/۰ |
| تاریخ نگارش | ۱۳۹۹/۰۴/۱۸ |
| 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

در چندین سال اخیر که شیوع بدافزارها در دنیای دیجیتال رشد زیادی داشته است باجافزارها رشد زیادی داشته‌اند و روزانه انواع مختلفی از آن ایجاد و انتشار می‌یابد. یکی از این باجافزارها RXX از خانواده Crysis می‌باشد که با رمزگذاری داده‌ها به منظور دریافت وجه برای ارائه ابزار رمزگشایی عمل می‌کند. 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.

این باجافزار در طی فرآیند رمزگذاری، کلیه فایل‌ها را براساس این الگو تغییر نام می‌دهد: نام اصلی فایل ، شناسه منحصر به فرد، آدرس ایمیل مجرمان سایبری وrxx. در انتهای هر فایل. بطور مثال فایلی با نام 1.jpg بصورت **1.**jpg.id-1E857D00.[back_data@foxmail.com].rxx تبدیل می‌گردد. همچنین براساس آخرین اطلاعات موجود، این باجافزار نیز همانند 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 back_data@foxmail.com و getdecoding@protonmail.com می-باشند. چنانچه مهاجمان در طول ۱۲ ساعت پاسخی از سمت کاربر دریافت نکنند دراین صورت کاربران برای برقراری ارتباط با مهاجمان باید از طریق ایمیل دوم 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، آنتروپی، وضعیت شناسایی فایل در ویروس‌توتال و ویروس‌کاو و غیره می‌باشد.

## ۲-۱ مشخصات فایل

همانطور که قبلا ذکر گردید این بدافزار از خانواده باج‌افزار و رمزگذار فایل می‌باشد که با استفاده از زبان برنامه‌نویسی C++ طراحی و پیاده‌سازی شده است. جدول زیر مشخصات کلی باج افزار RXX را نشان می‌دهد.

**جدول ۱ - ریزجزئیات مربوط به باج‌افزار**

| | |
|---|---|
| **هش md5** | 6172709AD4D6C0A3CD305FC14170C41C |
| **هش SHA1** | 8913A24A75090F4A2907680570B1E180F037D1D9 |
| **هش SHA256** | 6985917D29596B66D9BBC745A13D5577110D9B0408719C5559D23DD59A9E4F0B |
| **نوع بدافزار** | Ransomware, Crypto Virus, Files locker |
| **نام بدافزار** | RXX |
| **پسوند** | -Id.[back_datafoxmail.com].rxx |
| **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** | 7.450 |
| **معماری فایل** | 32 bits |
| **آدرس فایل Pdb** | c:\crysis\release\pdb\payload.pdb |

## ۲-۲ بخش‌های مختلف فایل

جدول موجودر در 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 چهار بخش بصورت text، rdata، data بصورت زیر می‌باشد.

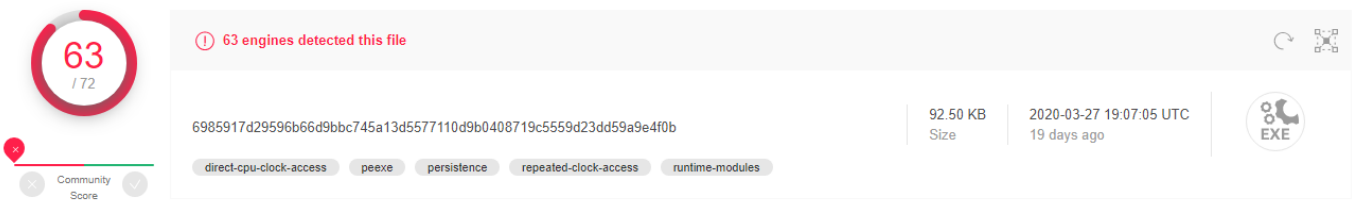
**جدول ۲- بخش‌های و مشخصات مربوط به آن‌ها**

| 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 جداول ۱ و ۲، مقدار آنتروپی کلی فایل به بخش‌های rdata و data بالاتر از هفت می‌باشد که نشان-دهنده مشکوک بودن فایل و بخش‌های ذکر شده می‌باشد. مقادیر بالای هفت و روند صعودی و همچنین مقدار صفر آنتروپی دگردیسی و چندریختی و مشکوک بودن فایل را نشان می‌دهد.

## ۲-۳ وضعیت شناسایی فایل در ویروس‌توتال

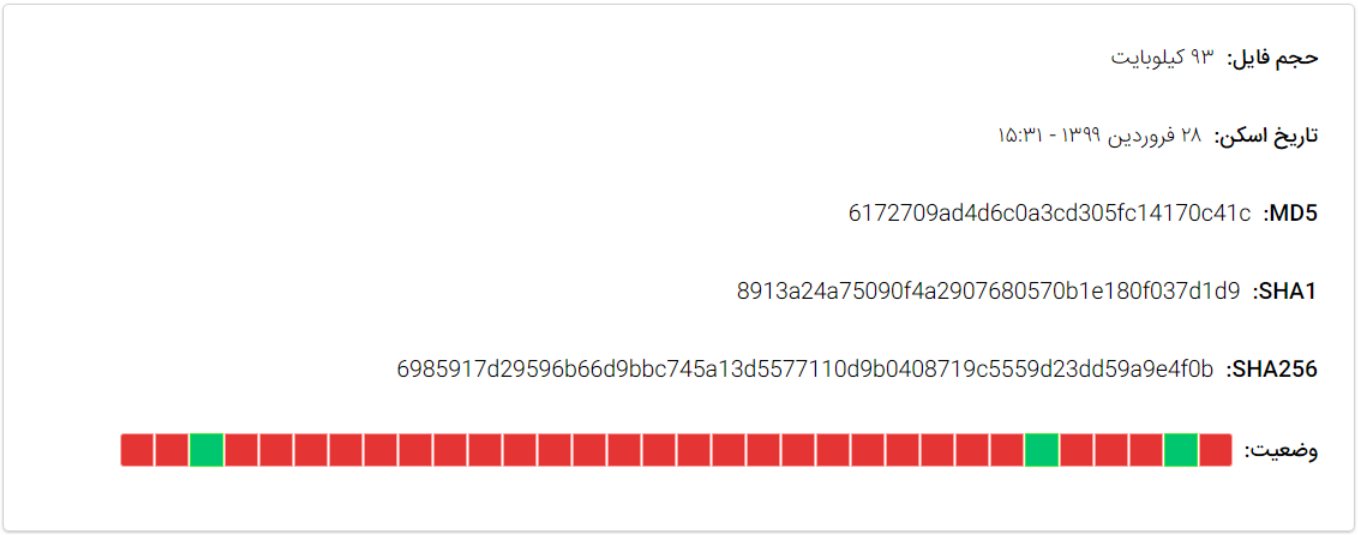
شکل زیر وضعیت شناسایی فایل را در ویروس‌توتال نشان می‌دهد. در این سامانه از بین ۷۲ موتور تحلیل ۶۳ موتور قادر به شناسایی فایل بعنوان یک فایل بدافزار شده‌اند و درصورت استفاده از نسخه‌های بروزشده این موتورهای آنتی‌ویروس در سیستم می‌توان از انتقال و اجرای آن جلوگیری کرد.




**شکل 1- وضعیت تشخیص فایل در ویروس‌توتال**

## ۴-۲ وضعیت شناسایی فایل در ویروس‌کاو

شکل زیر نیز وضعیت شناسایی فایل را در سامانه بومی ویروس‌کاو نشان می‌دهد. از بین ۳۲ موتور موجود تعداد ۲۹ موتور قادر به شناسایی بعنوان فایل مخرب و بدافزار شده‌اند و تنها سه موتور قادر به شناسایی نیست.

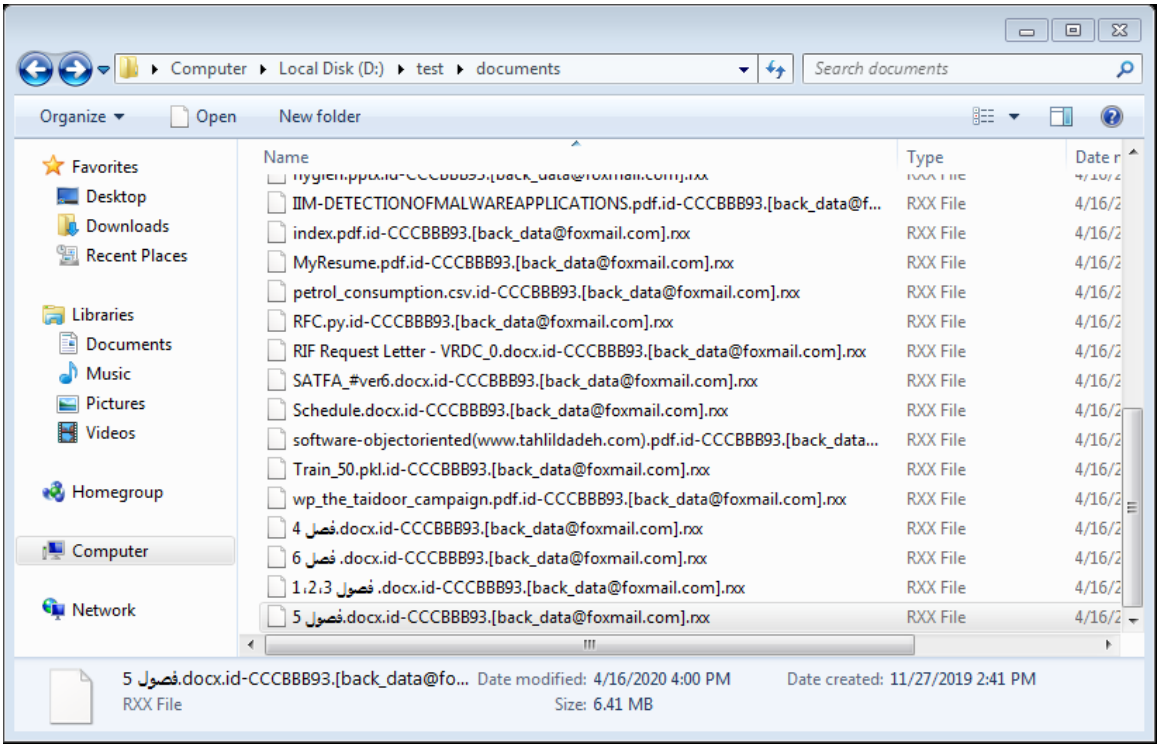



**شکل 2 – وضعیت تشخیص فایل در ویروس‌کاو**

# ۳ فرایند آلوده‌سازی

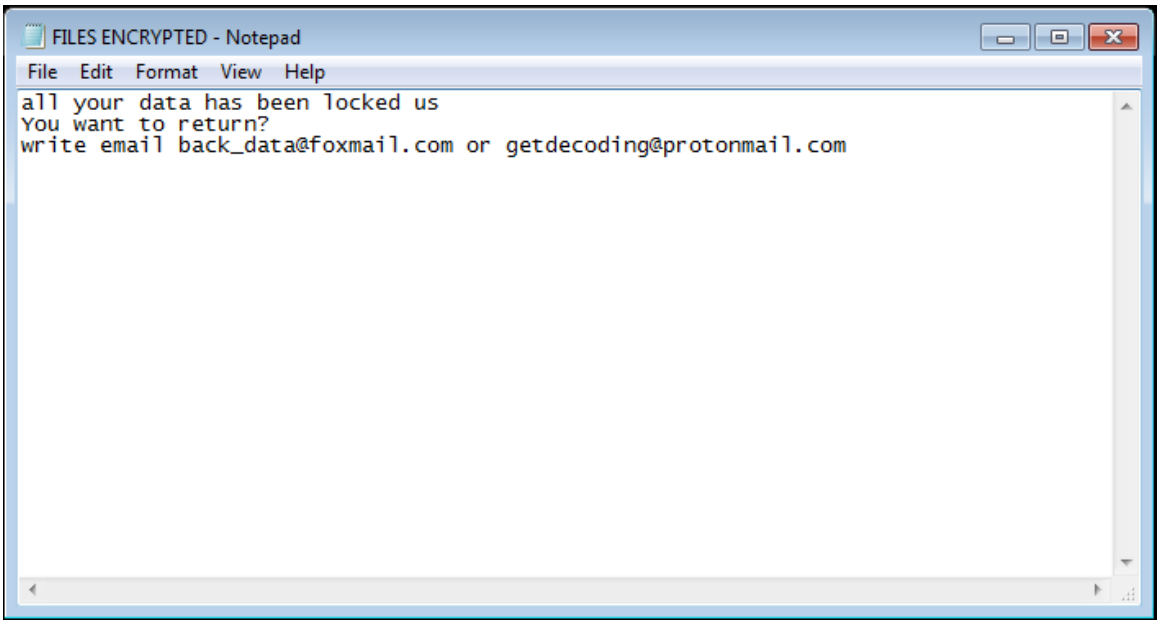
با توجه به یافته‌ها و بررسی‌های محققین حوزه بدافزار این باج‌افزار در اواخر March سال ۲۰۲۰ میلادی انتشار یافته است. این باج‌افزار در طی فرآیند رمزگذاری، کلیه فایل ها را براساس این الگو تغییر نام می‌دهد: نام اصلی فایل، شناسه منحصر به فرد، آدرس ایمیل مجرمان سایبری و پسوندrxx. در طول فرایند رمزگذاری کلیدهای 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.

مهاجمان بصورت مستقیم مبلغ باج را تعیین نکرده‌اند و کاربران قربانی شده باید با استفاده از آدرس‌های ایمیلی که در پنجره بازشو نمایش داده می‌شود با مهاجمان ارتباط برقرار کنند تا مقدار و نحوه پرداخت باج مشخص گردد. آدرس‌های ایمیل بصورت back_data@foxmail.com و getdecoding@protonmail.com می‌باشند. چنانچه مهاجمان در طول ۱۲ ساعت پاسخی از سمت کاربر دریافت نکنند دراین صورت کاربران برای برقراری ارتباط با مهاجمان باید از طریق ایمیل دوم اقدام نمایند. شکل‌های زیر نمونه فایل‌های رمزشده، توسط این باج‌افزار را نشان می‌دهد که فایل‌هایی با نام‌های فارسی نیز قابل رمزگذاری می‌باشند.




شکل 3 – نمونه فایل‌های رمزشده توسط باج‌افزار


شکل 5- فایل راهنما و با نام info.hta




**شکل 6 -فایل متنی ایجاد شده در داخل هر پوشه**

# ۴ شرح تحلیل

این بخش از گزارش نتیجه تحلیل و بررسی فایل باج‌افزار را توسط ابزارهای تحلیل در قسمت‌های مختلف نشان می‌دهد 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، توابع و رشته‌های آن را تغییر داده که هنگام دیس-اسمبل 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 |

از بین این توابع می‌توان به توابعی همانند GetProcAddress و LoadLibrary اشاره کرد. همچنین رشته‌های موجود و قابل دسترس هنگام دیس‌اسمبل نیز در جدول زیر قابل مشاهده می‌باشد که در برخی موارد با استفاده از عملیات مبهم‌سازی[۱] به رشته‌های ناخوانا که معنی و مفهوم خاصی ندارد، تبدیل شده‌اند.

**جدول ۴ - رشته‌های قابل استخراج از فایل باج‌افزار**

| | |
|---|---|
| C:\crysis\Release\PDB\payload.pdb<br>!This program cannot be run in DOS mode.<br>KERNEL32.dll<br>%sh(<br>ssbss<br>ComSpec=C:\Windows\system32\cmd.exe<br>TEMP=C:\Users\TAHLIL~1\AppData\Local\Temp<br>C:\Windows\system32\KERNELBASE.dll<br>C:\Windows\system32\RPCRT4.dll<br>FILES ENCRYPTED.txt<br>outlook.exe<br>mysqld.exe<br>mssqlserver<br>bootfont.bin<br>mysqld-nt.exe<br>sqlservr.exe<br>ntdetect.com<br>.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC<br>.[back_data@foxmail.com]<br>.vda;.vdr;.vdw;.vdx;.vrp;.vsd;.vss;.vst;.vsw;.vsx;.vtm;.vtml;.vtx;.wb2;.wav;.wbm;.wbmp;.wim;.wmf;.wml;.wmv;.wpd;.wps;.x3f;.xl; | رشته‌های قابل دریافت |

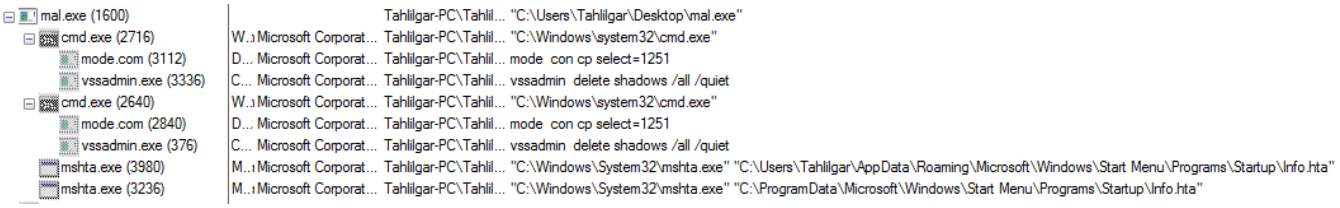
[۱] Obfuscation

| |
|---|
| .xlam;.xlk;.xlm;.xls;.xlsb;.xlsm;.xlsx;.xlt;.xltm;.xltx;.xlw;.xml;.xps;.xsd;.xsf;.xsl;.xslt;.xsn;.xtp;.xtp2;.xyze;.xz;.zip;%USERTr ust RSA |

از بین رشته‌ها می‌توان به مواردی همانند آدرس سایت‌های مختلف، پسوند اضافه شده به فایل‌ها، پسوندهای قابل رمزگذاری، نام فایل تصویر ایجاد شده، کتابخانه‌های سیستمی مختلف، آدرس مسیرهایی از سیستم و غیره اشاره کرد.

## ۴-۲ پروسس‌های ایجاد شده توسط باج‌افزار

شکل زیر پروسس‌ها و فرایندهای ایجاد شده در سیستم را در طول اجرا و فعالیت باج‌افزار را نشان می‌دهد که در آن باج‌افزار اقدام به اجرای CMD کرده و توسط آن دستورات مختلفی را در سیستم اجرا می‌کند. از این دستورات به دلیل پاکسازی Shadowها استفاده شده است.




**شکل 7- ساختار درختی پروسس‌های اجرای در طول فعالیت باج‌افزار**

## ۴-۳ فایل‌های ایجاد شده

همانطور که قبلا نیز ذکر گردید باج‌افزار در طول فعالیت 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 ماندگاری و اجرای همیشگی آن‌ها ایجاد شده‌اند.

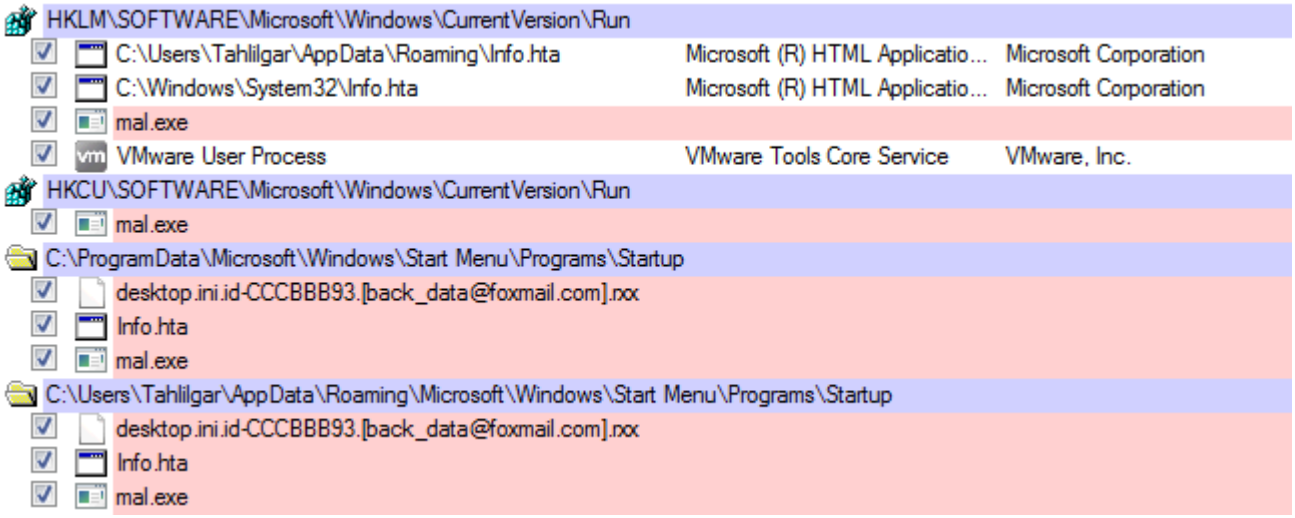
1. C:\Users\...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mal.exe
2. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\mal.exe
3. C:\FILES ENCRYPTED.txt
4. C:\Users\...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
5. C:\Users\...\AppData\Roaming\Info.hta

## ۴-۴ تغییرات رجیستری

باج‌افزار بعد از اجرا و رمزکردن فایل‌های سیستم باعث ایجاد تغییراتی در رجیستری سیستم شده و کلیدهایی را ثبت می‌کند. همانند ایجاد فایل، از این ویژگی هم برای ماندگاری باج‌افزار استفاده شده است. این مسیر و کلیدهای ثبت شده به صورت زیر می‌باشند.

1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mal.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

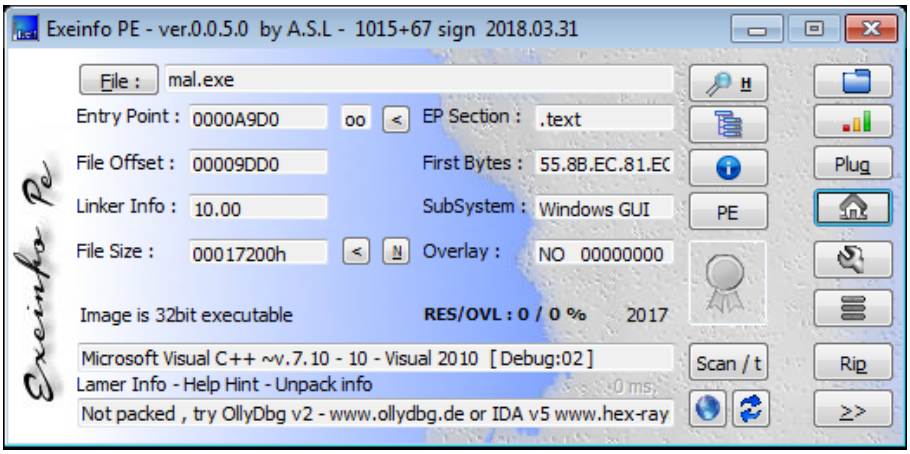
شکل زیر نیز این کلیدها را نشان می‌دهد که در سیستم ثبت شده‌اند.




**شکل 8- ساختار رجسترهای باز و خوانده شده**

# ۵ شناسایی کامپایلر

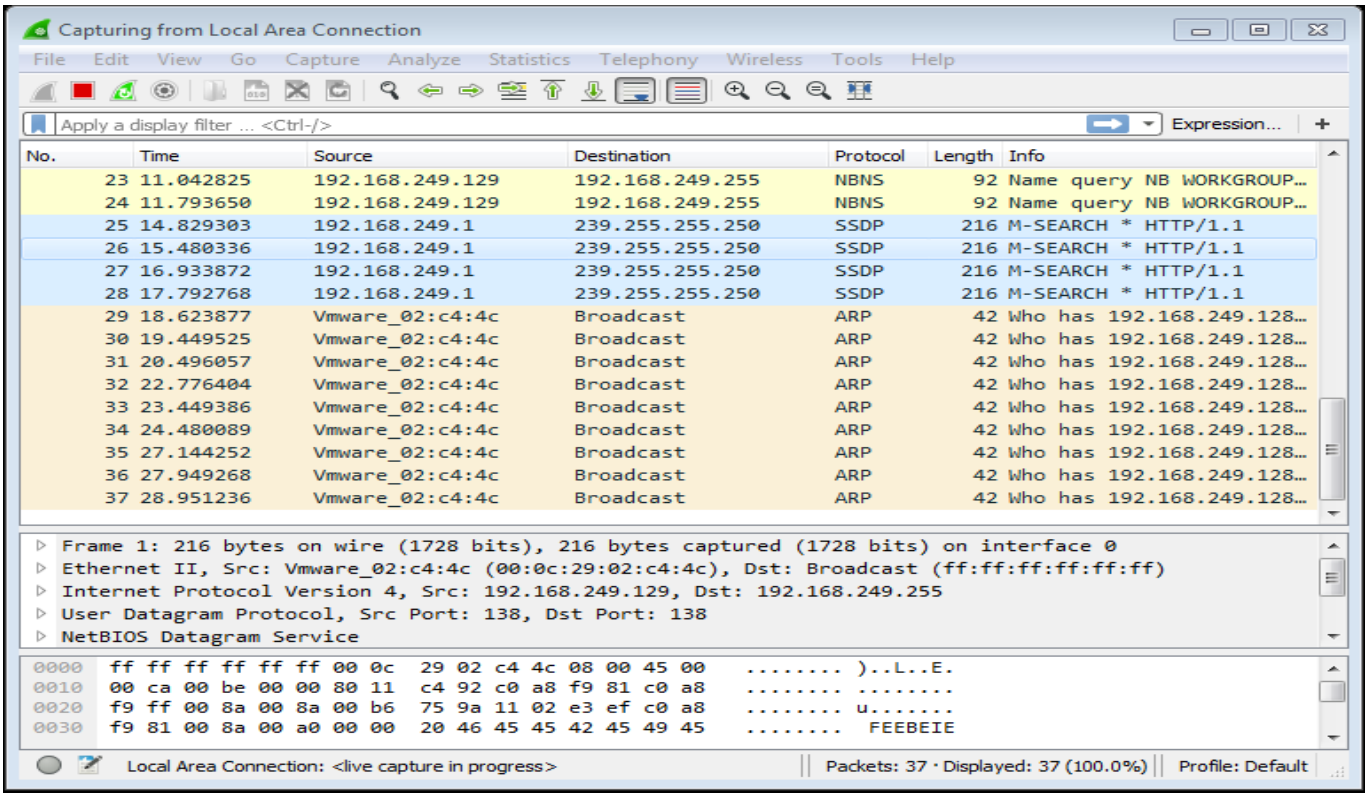
همانطور که قبلا نیز ذکر گردید کامپایلر و زبان برنامه نویسی فایل باج‌افزار C++ می‌باشد. شکل زیر این نتیجه را توسط ابزار تشخیص کامپایلر نشان می‌دهد.




شکل 9- شناسایی کامپایلر

## ۵-۱ ارتباطات شبکه

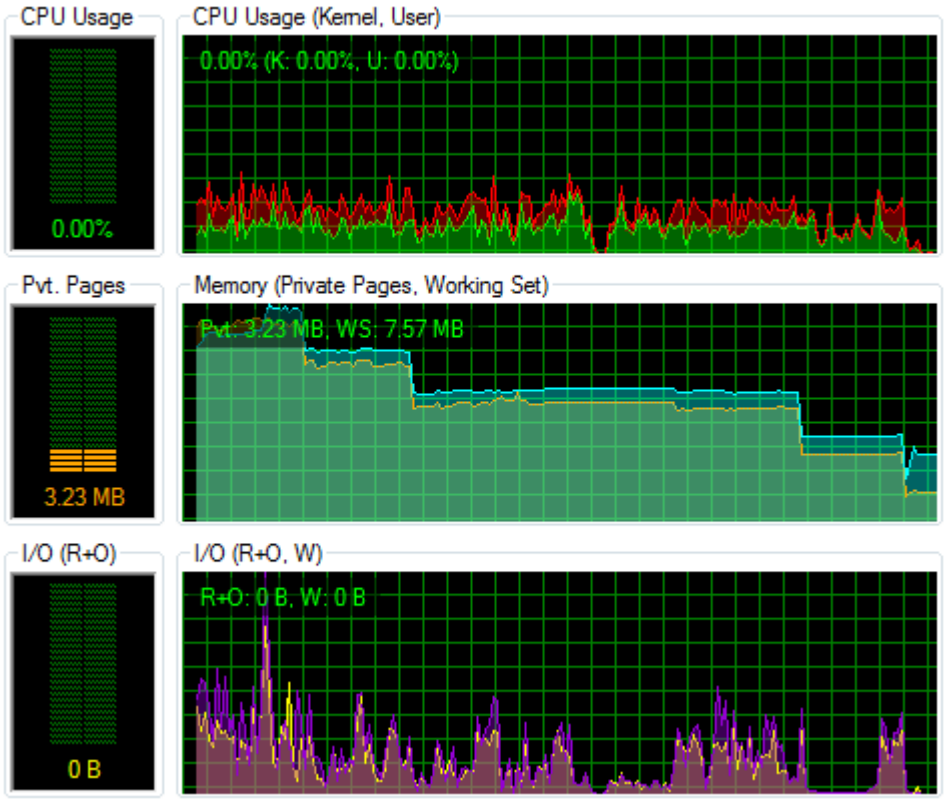
در طول اجرای باج‌افزار در سیستم هیچ نوع فعالیتی مبنی بر ارتباط شبکه مشاهده نگردید، که در شکل زیر می‌توان این فعالیت را مشاهده کرد.




شکل 10 – بررسی فعالیت شبکه در طول اجرای باج‌افزار

## ۵-۲ وضعیت منابع سیستم

شکل زیر وضعیت منابع سیستم را فقط برای فایل اجرایی باجافزار نشان می‌دهد که در حال مصرف است. با توجه به شکل مشاهده می‌گردد که میزان استفاده از CPU و MEMORY بیشتر بوده و در طول فعالیت باجافزار میزان بیشتری از آن‌ها را درگیر کرده است. همچنین مقدار I/O نیز مصرف بیشتری داشته و نسبت به قبل و بعد از فعالیت باجافزار مصرف زیادی دارد.




**شکل 11- وضعیت منابع سیستم در طول اجرای باجافزار**

# ۶ 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