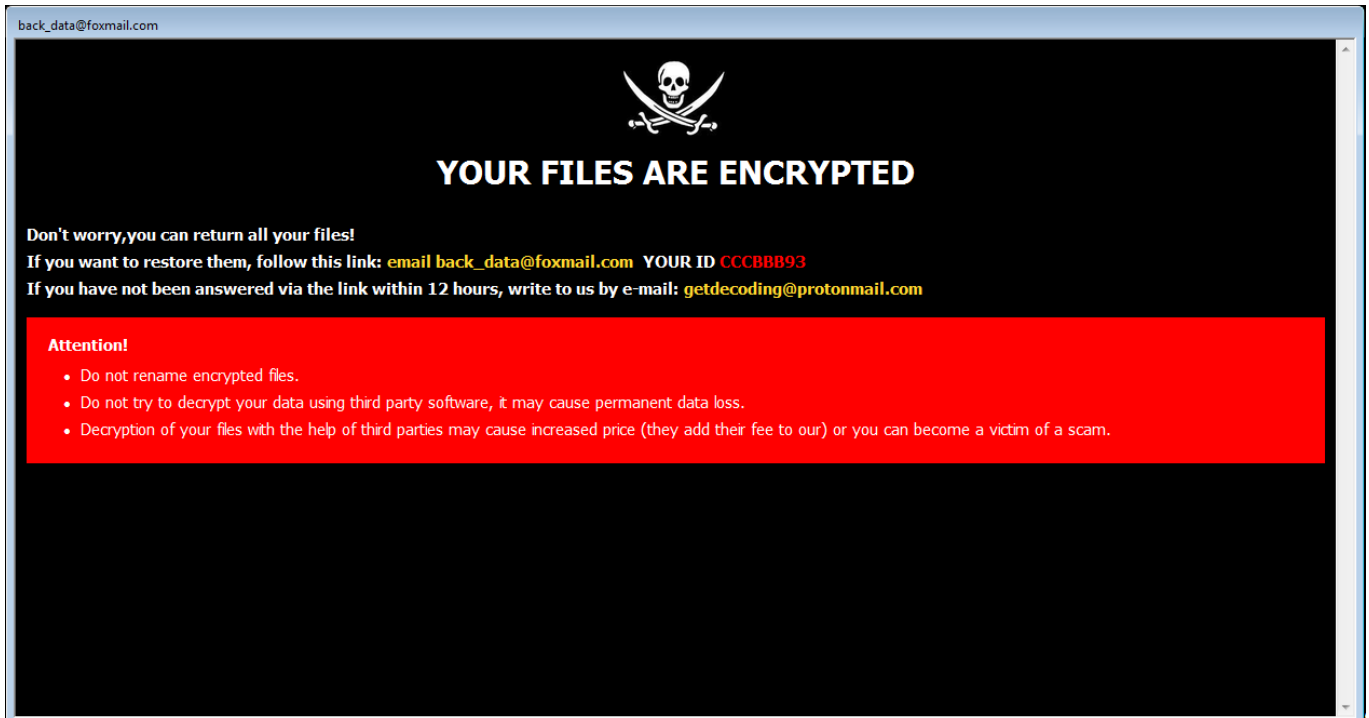


بسمه تعالی

گزارش تحلیلی باج افزار RXX Ransomware



فهرست مطالب

۳	۱ مقدمه
۴	۲ مشخصات و ریزجزئیات فایل باج افزار
۴	۱-۲ مشخصات فایل
۴	۲-۲ بخش های مختلف فایل
۵	۴-۲ وضعیت شناسایی فایل در ویروس توتال
۵	۵-۲ وضعیت شناسایی فایل در ویروس کاو
۵	۳ فرایند آلوده سازی
۷	۴ شرح تحلیل
۷	۱-۴ کتابخانه و توابع مورد استفاده
۸	۲-۴ پروسس های ایجاد شده توسط باج افزار
۹	۳-۴ فایل های ایجاد شده
۹	۴-۴ تغییرات رجیستری
۹	۵-۴ شناسایی کامپایلر
۱۰	۶-۴ ارتباطات شبکه
۱۰	۷-۴ وضعیت منابع سیستم
۱۱	۶ توصیه های امنیتی برای پیشگیری

۱ مقدمه

در چندین سال اخیر که شیوع بدافزارها در دنیای دیجیتال رشد زیادی داشته است باج افزارها رشد زیادی داشته‌اند و روزانه انواع مختلفی از آن ایجاد و انتشار می‌یابد. یکی از این باج افزارها RXX از خانواده Crysis می‌باشد که با رمزگذاری داده‌ها به منظور دریافت وجه برای ارائه ابزار رمزگشایی عمل می‌کند. این باج افزار 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 باج افزار 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 RXX. در انتهای هر فایل. بطور مثال فایلی با نام 1.jpg بصورت 1.jpg.id-@foxmail.com.back_data.1E857D00 تبدیل می‌گردد. همچنین براساس آخرین اطلاعات موجود، این باج افزار نیز همانند باج افزارهای 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 می‌باشند. چنانچه مهاجمان در طول ۱۲ ساعت پاسخی از سمت کاربر دریافت نکنند در این صورت کاربران برای برقراری ارتباط با مهاجمان باید از طریق ایمیل دوم اقدام نمایند.

۲ مشخصات و ریز جزئیات فایل باج افزار

جدول و نمودارهای موجود در این بخش نشان دهنده ریز جزئیات فایل باج افزار می باشند که در طول تحلیل های استاتیک و پویا توسط ابزارهای مختلف بدست آمده اند. این اطلاعات شامل مواردی همچون اندازه فایل، مقادیر هش فایل، آنتروپی، وضعیت شناسایی فایل در ویروس توتال و ویروس کاو و غیره می باشد.

۱-۲ مشخصات فایل

همانطور که قبلا ذکر گردید این بدافزار از خانواده باج افزار و رمزگذار فایل می باشد که با استفاده از زبان برنامه نویسی ++C طراحی و پیاده سازی شده است. جدول زیر مشخصات کلی باج افزار RXX را نشان می دهد.

جدول ۱ - ریز جزئیات مربوط به باج افزار

6172709AD4D6C0A3CD305FC14170C41C	هش md5
8913A24A75090F4A2907680570B1E180F037D1D9	هش SHA1
6985917D29596B66D9BBC745A13D5577110D9B0408719C5559D23DD59A9E4F0B	هش SHA256
Ransomware, Crypto Virus, Files locker	نوع بدافزار
RXX	نام بدافزار
-ld.[back_datafoxmail.com].rxx	پسوند
Infected email attachments (macros), torrent websites, malicious ads.	نحوه انتشار
2017-03-02	زمان کامپایل
Microsoft Visual C++	کامپایلر
94720 bytes	حجم فایل
7.450	آنتروپی کلی فایل
32 bits	معماری فایل
c:\crysis\release\pdb\payload.pdb	آدرس فایل Pdb

۲-۲ بخش های مختلف فایل

جدول موجود در زیر نیز بخش های مختلف تشکیل دهنده فایل باج افزار را با جزئیات کامل مانند مقدار آنتروپی، اندازه خام، اندازه مجازی هر بخش و غیره نشان می دهد. این فایل متشکل از چهار بخش بصورت text، rdata، data بصورت زیر می باشد.

جدول ۲ - بخش های و مشخصات مربوط به آنها

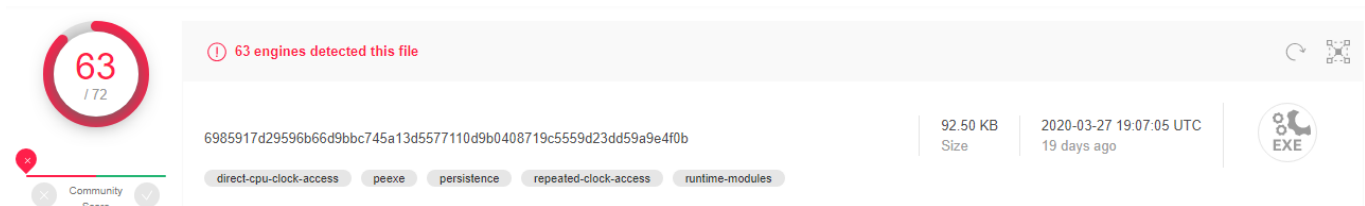
ردیف	نام	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی	بایت های اولیه
1	.text	00001000	00009c25	00009e00	5.965	55 8B EC 83 EC 24 53 56 57
2	.rdata	0000b000	00002636	00002800	7.785	B0 41 00 00 BE 41 00 00 D0

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 نشان‌دهنده مشکوک بودن فایل و بخش‌های ذکر شده می‌باشد. مقادیر بالای هفت و روند صعودی و همچنین مقدار صفر آنتروپی دگرذیسی و چندریختی و مشکوک بودن فایل را نشان می‌دهد.

۲-۴ وضعیت شناسایی فایل در ویروس‌توتال

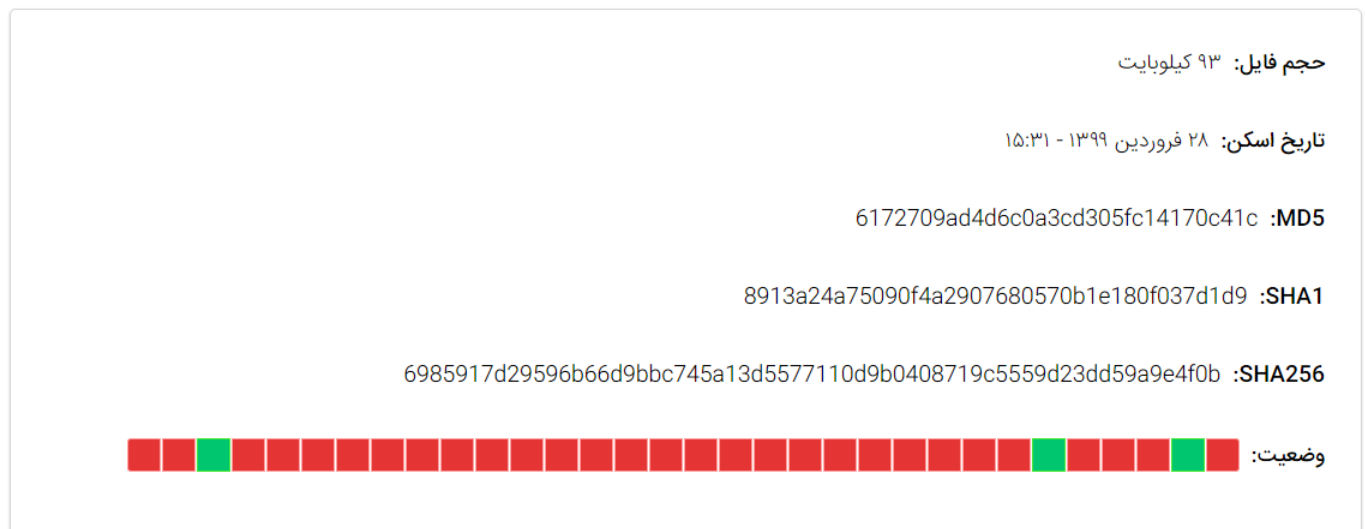
شکل زیر وضعیت شناسایی فایل را در [ویروس‌توتال](#) نشان می‌دهد. در این سامانه از بین ۷۲ موتور تحلیل ۶۳ موتور قادر به شناسایی فایل بعنوان یک فایل بدافزار شده‌اند و در صورت استفاده از نسخه‌های بروز شده این موتورهای آنتی‌ویروس در سیستم می‌توان از انتقال و اجرای آن جلوگیری کرد.



شکل ۱- وضعیت تشخیص فایل در ویروس‌توتال

۲-۵ 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.



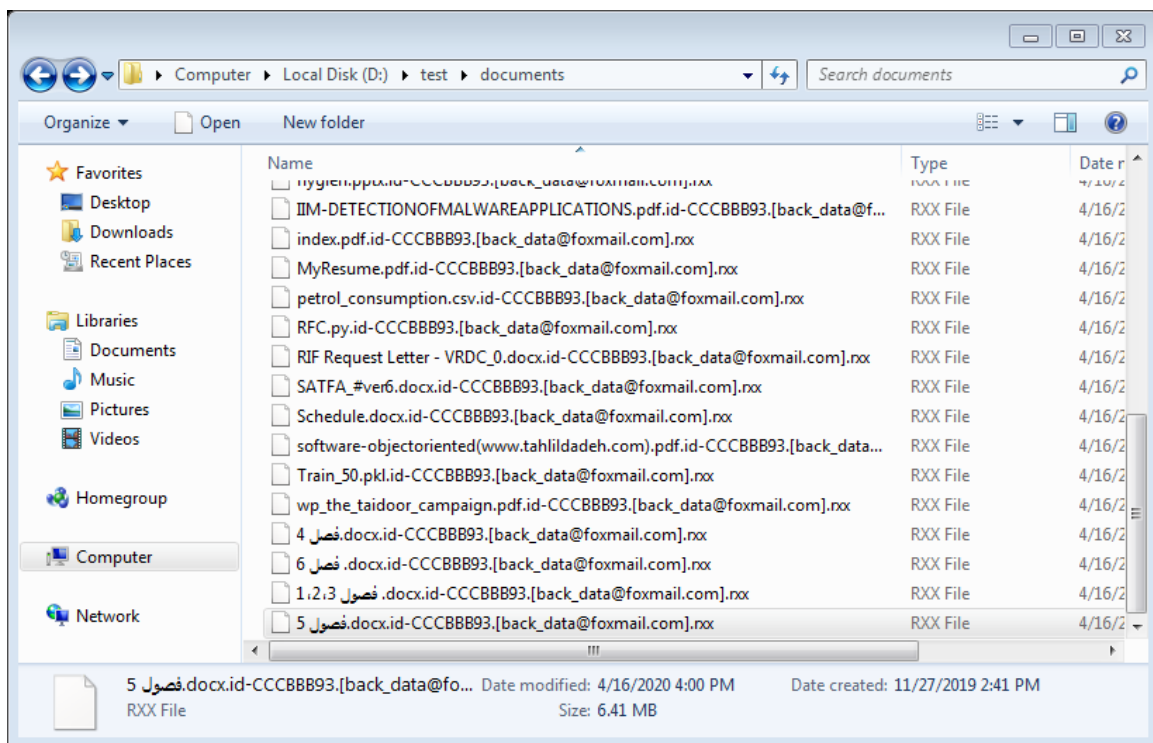
شکل ۲- وضعیت تشخیص فایل در ویروس‌کاو

۳ فرایند آلوده‌سازی

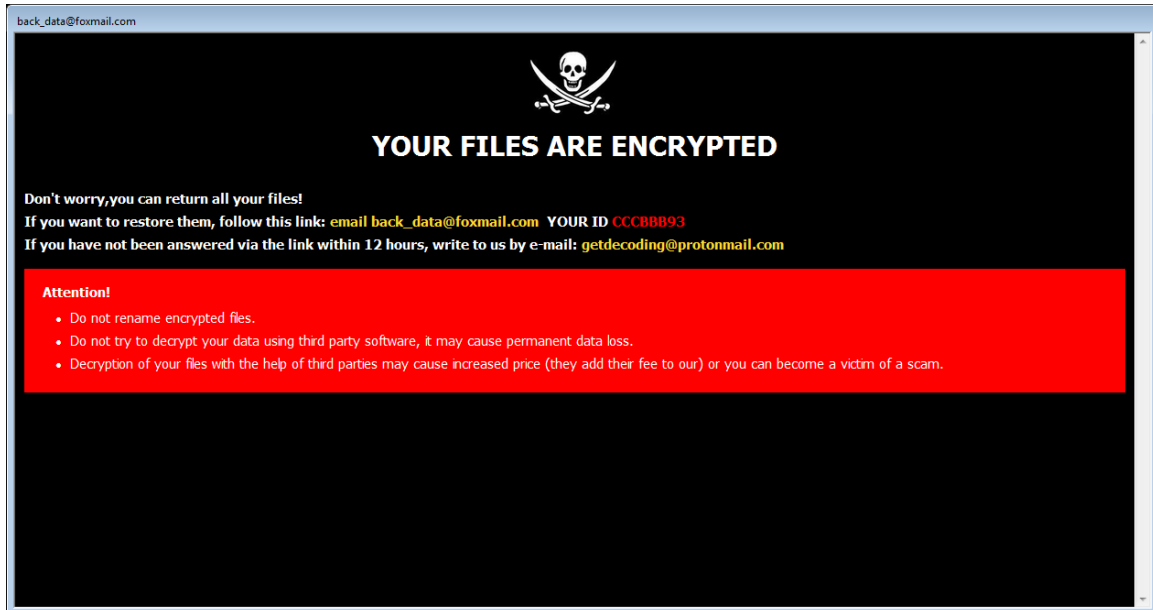
با توجه به یافته‌ها و بررسی‌های محققین حوزه بدافزار این باج‌افزار در اواخر March سال ۲۰۲۰ میلادی انتشار یافته است. این باج‌افزار در طی فرآیند رمزگذاری، کلیه فایل‌ها را براساس این الگو تغییر نام می‌دهد: نام اصلی فایل، شناسه منحصر به فرد، آدرس ایمیل مجرمان سایبری و پسوند .IXX. در طول فرایند رمزگذاری کلیدهای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

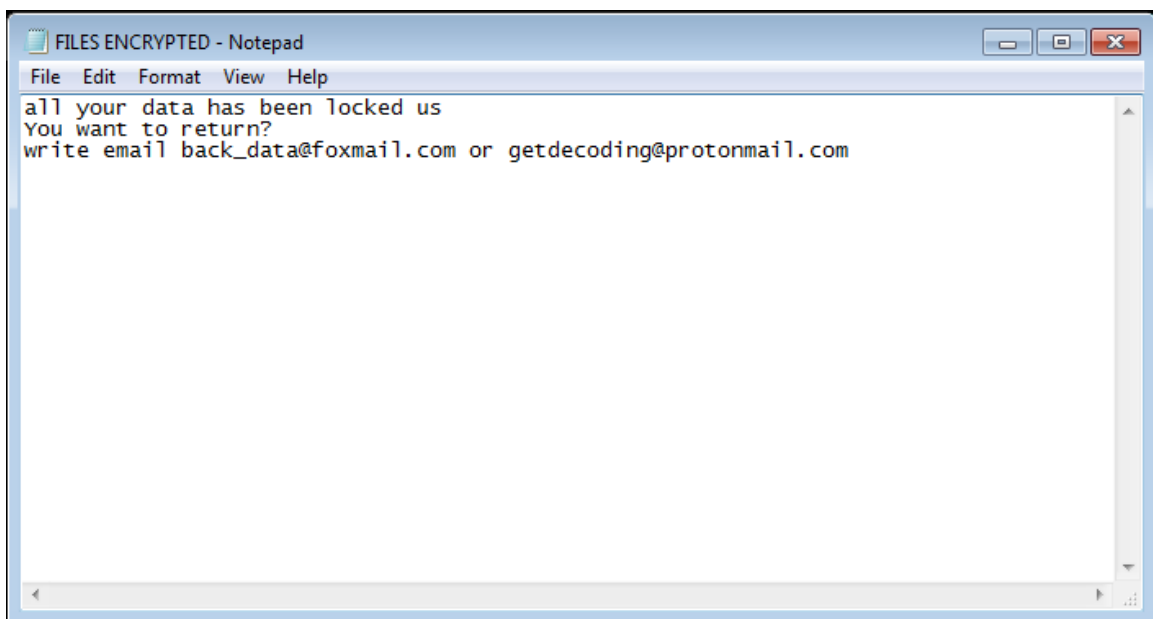
مهاجمان بصورت مستقیم مبلغ باج را تعیین نکرده‌اند و کاربران قربانی شده باید با استفاده از آدرس‌های ایمیلی که در پنجره بازشو نمایش داده می‌شود با مهاجمان ارتباط برقرار کنند تا مقدار و نحوه پرداخت باج مشخص گردد. آدرس‌های ایمیل بصورت back_data@foxmail.com و getdecoding@protonmail.com می‌باشند. چنانچه مهاجمان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



شکل 3 - نمونه فایل‌های رمز شده 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 باج افزار را توسط ابزارهای تحلیل در قسمت های مختلف نشان می دهد و شامل مواردی مانند کتابخانه و توابع، رشته ها، فعالیت های شبکه و غیره می باشند.

۴-۱ کتابخانه و توابع مورد استفاده

فایل اجرایی باج افزار با استفاده از تکنیک های مبهم سازی، توابع و رشته های آن را تغییر داده که هنگام دیس اسمبل کردن فایل، تعداد کتابخانه و توابع را محدود نشان داده و رشته ها را بصورت کاراکترهای ناخوانا نشان می دهد. لذا هنگام فرایند دیس اسمبل کتابخانه و توابع موجود در جدول زیر بدست می آید.

جدول ۳ - کتابخانه و توابع مورد استفاده از باج افزار

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

از بین این توابع می توان به توابعی همانند GetProcAddress و LoadLibrary اشاره کرد. همچنین رشته های موجود و قابل دسترس هنگام دیس اسمبل نیز در جدول زیر قابل مشاهده می باشد که در برخی موارد با استفاده از عملیات مبهم سازی^۱ به رشته های ناخوانا که معنی و مفهوم خاصی ندارد، تبدیل شده اند.

جدول ۴ - رشته های قابل استخراج از فایل باج افزار

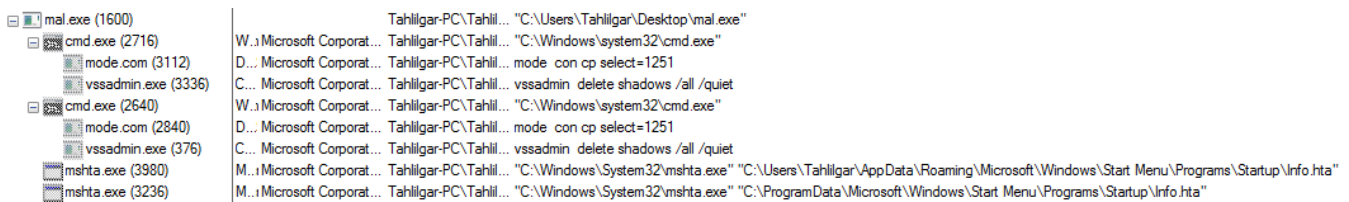
```
C:\crisis\Release\PDB\payload.pdb
!This program cannot be run in DOS mode.
KERNEL32.dll
%sh(
ssbss
ComSpec=C:\Windows\system32\cmd.exe
TEMP=C:\Users\TAHLIL~1\AppData\Local\Temp
C:\Windows\system32\KERNELBASE.dll
C:\Windows\system32\RPCRT4.dll
FILES ENCRYPTED.txt
outlook.exe
mysqld.exe
mysqld.exe
mssqlserver
bootfont.bin
mysqld-nt.exe
sqlservr.exe
ntdetect.com
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
.[back_data@foxmail.com]
.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;
.xlam;.xlk;.xlm;.xls;.xlsb;.xslm;.xlsx;.xlt;.xltm;.xlt;.xlw;.xml;.xps;.xsd;.xsf;.xsl;.xslt;.xsn;.xtp;.xtp2;.xyze;.xz;.zip;%USERTrust RSA
```

رشته های قابل دریافت

از بین رشته ها می توان به مواردی همانند آدرس سایت های مختلف، پسوند اضافه شده به فایل ها، پسوند های قابل رمزگذاری، نام فایل تصویر ایجاد شده، کتابخانه های سیستمی مختلف، آدرس مسیریابی از سیستم و غیره اشاره کرد.

۲-۴ پروسیس های ایجاد شده توسط باج افزار

شکل زیر پروسیس ها و فرایندهای ایجاد شده در سیستم را در طول اجرا و فعالیت باج افزار را نشان می دهد که در آن باج-افزار اقدام به اجرای CMD کرده و توسط آن دستورات مختلفی را در سیستم اجرا می کند. از این دستورات به دلیل پاکسازی Shadowها استفاده شده است.



```
Tahlilgar-PC\Tahlil... "C:\Users\Tahlilgar\Desktop\mal.exe"
W. Microsoft Corporat... Tahlilgar-PC\Tahlil... "C:\Windows\system32\cmd.exe"
D... Microsoft Corporat... Tahlilgar-PC\Tahlil... mode con cp select=1251
C... Microsoft Corporat... Tahlilgar-PC\Tahlil... vssadmin delete shadows /all /quiet
W. Microsoft Corporat... Tahlilgar-PC\Tahlil... "C:\Windows\system32\cmd.exe"
D... Microsoft Corporat... Tahlilgar-PC\Tahlil... mode con cp select=1251
C... Microsoft Corporat... Tahlilgar-PC\Tahlil... vssadmin delete shadows /all /quiet
M... Microsoft Corporat... "C:\Windows\System32\mshta.exe" "C:\Users\Tahlilgar\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"
M... Microsoft Corporat... Tahlilgar-PC\Tahlil... "C:\Windows\System32\mshta.exe" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"
```

شکل 7- ساختار درختی پروسیس های اجرای در طول فعالیت باج افزار

۳-۴ فایل های ایجاد شده

همانطور که قبلا نیز ذکر گردید باج افزار در طول فعالیت خود فایل هایی را در مسیرهایی از سیستم ایجاد می کند. این فایل های ایجاد شده همان فایل اصلی باج افزار و فایل های راهنما می باشد که در مسیر Startup برای ماندگاری و اجرای همیشگی آنها ایجاد شده اند.

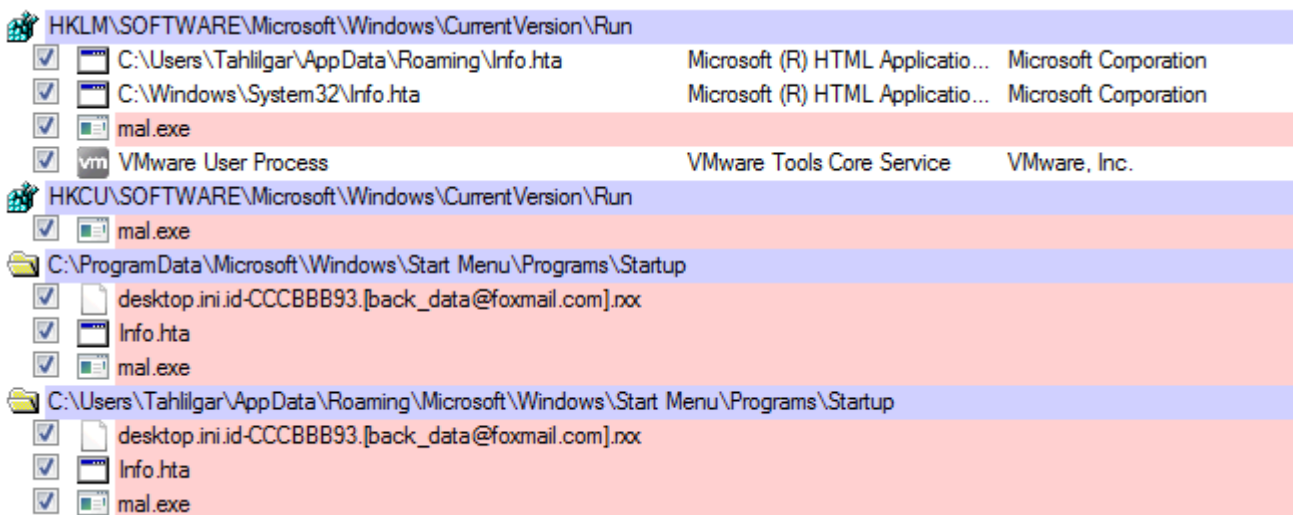
1. C:\Users\...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mal.exe
2. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\mal.exe
3. C:\FILES ENCRYPTED.txt
4. C:\Users\...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
5. C:\Users\...\AppData\Roaming\Info.hta

۴-۴ تغییرات رجیستری

باج افزار بعد از اجرا و رمز کردن فایل های سیستم باعث ایجاد تغییراتی در رجیستری سیستم شده و کلیدهایی را ثبت می کند. همانند ایجاد فایل، از این ویژگی هم برای ماندگاری باج افزار استفاده شده است. این مسیر و کلیدهایی ثبت شده به صورت زیر می باشند.

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

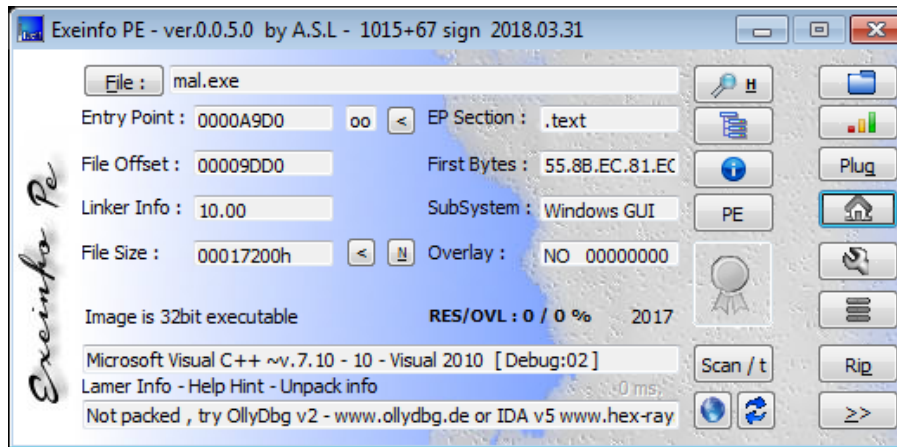
شکل زیر نیز این کلیدها را نشان می دهد که در سیستم ثبت شده اند.



شکل 8- ساختار رجیستری های باز و خوانده شده

۴-۵ شناسایی کامپایلر

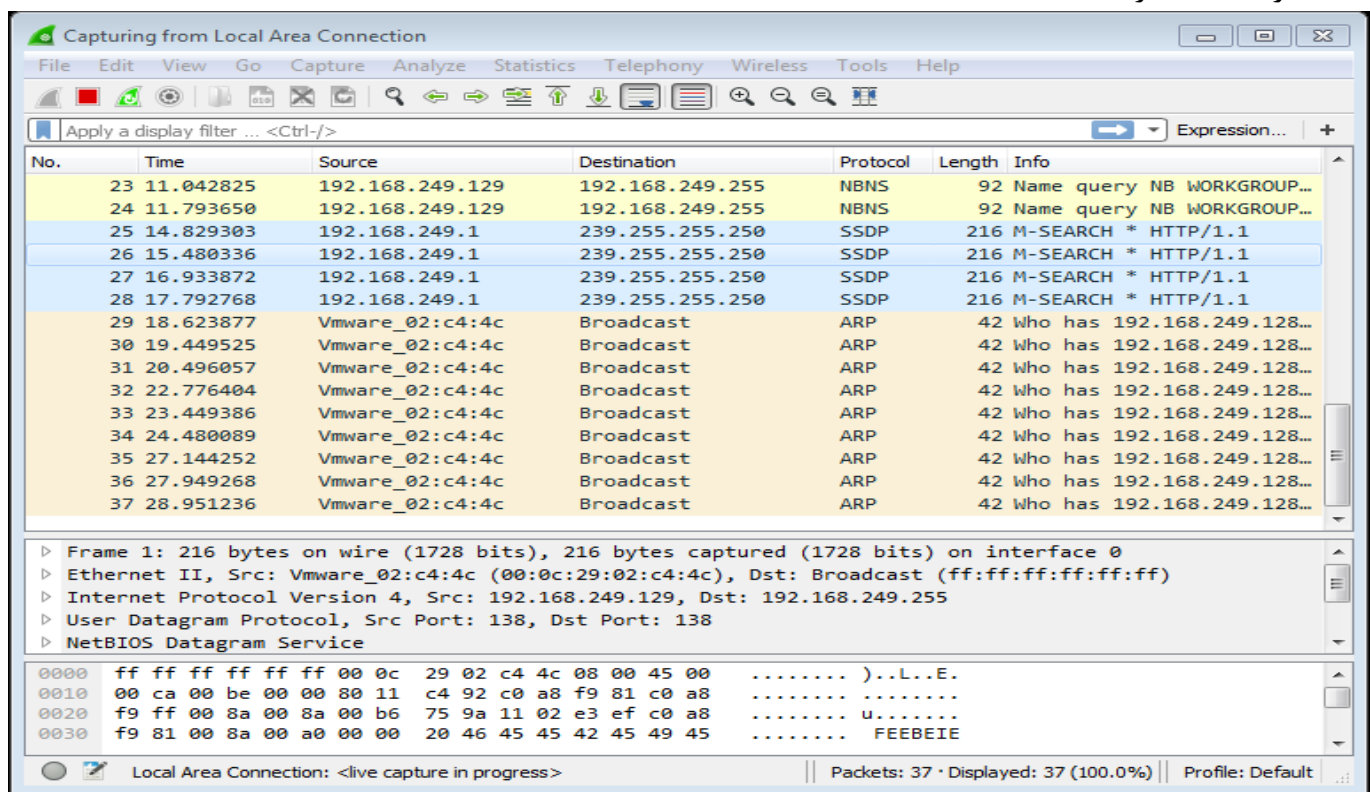
همانطور که قبلا نیز ذکر گردید کامپایلر و زبان برنامه نویسی فایل باج افزار C++ می باشد. شکل زیر این نتیجه را توسط ابزار تشخیص کامپایلر نشان می دهد.



شکل 9- شناسایی کامپایلر

۴-۶ ارتباطات شبکه

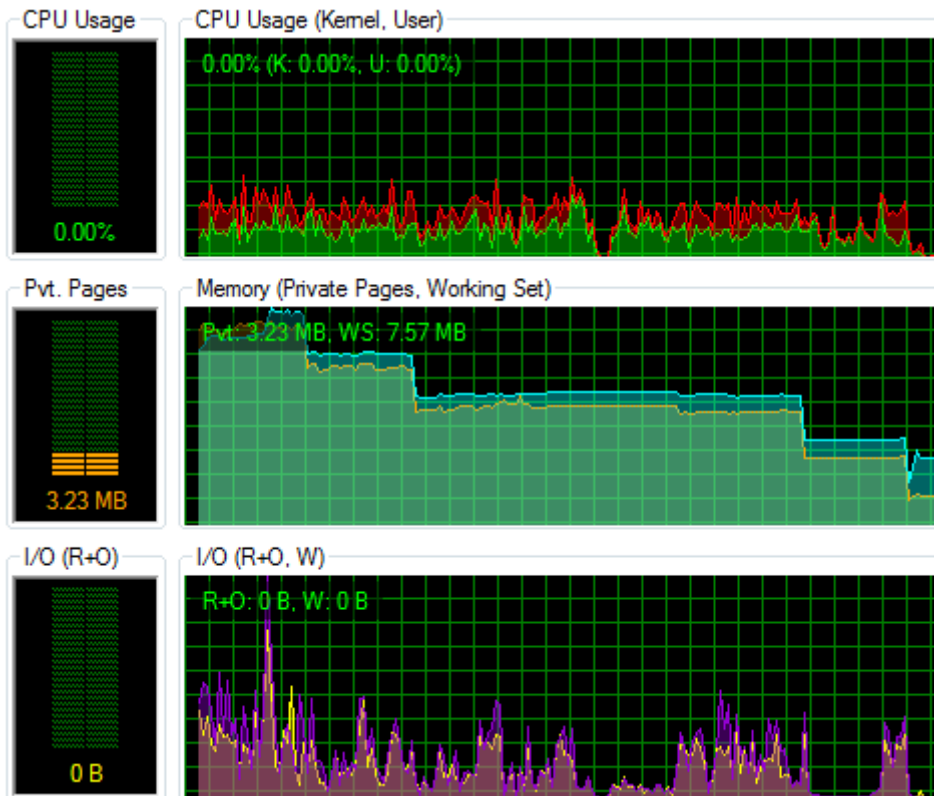
در طول اجرای باج افزار در سیستم هیچ نوع فعالیتی مبنی بر ارتباط شبکه مشاهده نگردید، که در شکل زیر می توان این فعالیت را مشاهده کرد.



شکل 10 - بررسی فعالیت شبکه در طول اجرای باج افزار

۴-۷ وضعیت منابع سیستم

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



شکل 11- وضعیت منابع سیستم در طول اجرای باج افزار

۶ توصیه های امنیتی برای پیشگیری

- ۱) گرفتن فایل پشتیبان بصورت دوره ای از فایل های سیستم و ذخیره آن در محل دیگر
- ۲) استفاده از آنتی ویروس قوی و بروزرسانی مداوم آن
- ۳) خودداری از باز کردن و اجرا فایل های مشکوک و ناشناس
- ۴) خودداری از باز کردن ایمیل های مشکوک و ناشناس
- ۵) اطمینان از سالم بودن دستگاه های جانبی مانند فلش
- ۶) استفاده از رمز عبور قوی بر روی درایوهای سیستم
- ۷) استفاده از سیستم عامل جدید و بروزرسانی شده
- ۸) بروزرسانی مداوم سیستم عامل
- ۹) پیکربندی مناسب پروتکل های مورد استفاده در شبکه متناسب با محیط کار