باسمه تعالی

تحلیل فنی باج‌افزار

DMR

فهرست مطالب

۱. مقدمه :

در تاریخ ۱۲ دسامبر سال ۲۰۱۹ میلادی، اخباری مبنی بر مشاهده باج‌افزاری با عنوان DMR در فضای سایبری منتشر شد. طبق شواهد موجود، باج‌افزار DMR از کتابخانه‌ای متفاوت با نام cryptopp در فرآیند رمزنگاری خود بهره برده است. این باج‌افزار پسوند DMR64. را به انتهای هر فایل رمزشده اضافه می‌کند. با توجه به اینکه مدت زمان زیادی از مشاهده این باج‌افزار نمی‌گذرد، تاکنون اخباری در رابطه با روش انتشار این باج‌افزار و تعداد موارد آلوده شده به آن در سراسر جهان منتشر نشده است. تحلیل پیش رو، مربوط به این باج‌افزار می‌باشد.

۲. مشخصات فایل اجرایی :

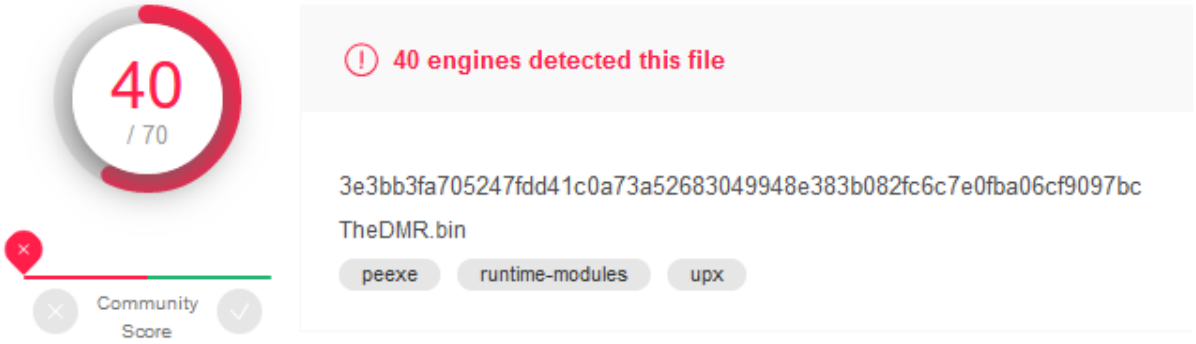
نام فایل	theDMR.exe
MD5	c5d722182c82972a29fd7b67e9755a8a
SHA-1	54c60fd5e05a7856e15d7a8219a063c3c1c92fef
SHA-256	3e3bb3fa705247fdd41c0a73a52683049948e383b082fc6c7e0fba06cf9097bc
نوع فایل	Win32 EXE
اندازه فایل	۱۹۱.۵ کیلوبایت

۳. شجره‌نامه

تاکنون والدی برای این باج‌افزار مشاهده نشده است و به نظر می‌رسد باج‌افزار DMR با هیچ باج‌افزار دیگری ارتباط و یا شباهت ندارد.

٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ٤٠ مورد ۷۰ از ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



۵. تحلیل پویا

۵-۱ آناتومی حمله:

پس از اجرای باج‌افزار در محیط آزمایشگاهی، نتایج زیر مشاهده شد.

باج‌افزار DMR بلافاصله پس از اجرا در سیستم قربانی، ابتدا تمام فایل‌های موجود بر روی صفحه دسکتاپ را رمزگذاری کرده، سپس متحوای موجود در قسمت Recycle Bin سیستم قربانی را حذف کرده و در انتها فایل‌های موجود در دیگر مسیرها و درایوهای سیستم را رمزگذاری می‌نماید. تمامی این فرآیندها در مدت زمان بسیار کوتاهی رخ می‌دهد.

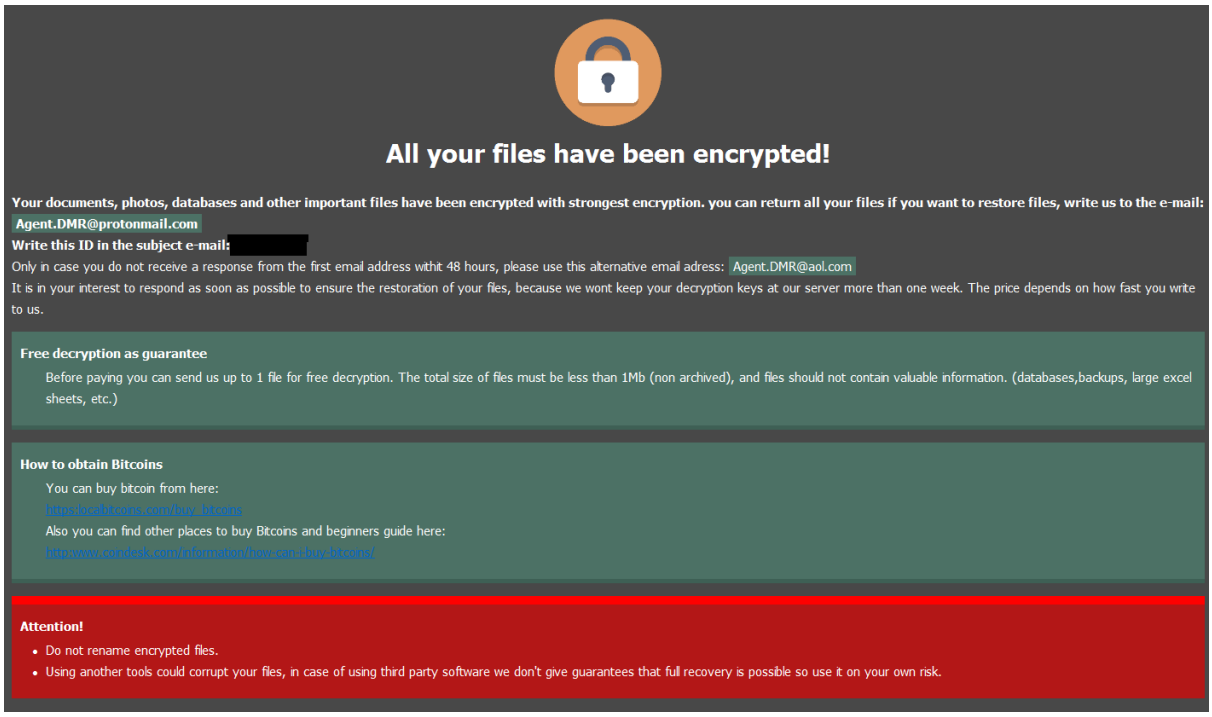
Name	Date modified	Type	Size
[id=[redacted]test (1).apk.DMR64	12/15/2019 5:02 PM	DMR64 File	9,288 KB
[id=[redacted]test (1).avi.DMR64	12/15/2019 5:02 PM	DMR64 File	31,433 KB
[id=[redacted]test (1).bmp.DMR64	12/15/2019 5:02 PM	DMR64 File	737 KB
[id=[redacted]test (1).DAT.DMR64	12/15/2019 5:02 PM	DMR64 File	96,802 KB
[id=[redacted]test (1).docx.DMR64	12/15/2019 5:02 PM	DMR64 File	177 KB
[id=[redacted]test (1).htm.DMR64	12/15/2019 5:02 PM	DMR64 File	90 KB
[id=[redacted]test (1).html.DMR64	12/15/2019 5:02 PM	DMR64 File	3,048 KB
[id=[redacted]test (1).jpg.DMR64	12/15/2019 5:02 PM	DMR64 File	374 KB
[id=[redacted]test (1).mkv.DMR64	12/15/2019 5:02 PM	DMR64 File	864,500 KB
[id=[redacted]test (1).mp3.DMR64	12/15/2019 5:02 PM	DMR64 File	4,485 KB
[id=[redacted]test (1).mpeg.DMR64	12/15/2019 5:02 PM	DMR64 File	45,740 KB
[id=[redacted]test (1).pdf.DMR64	12/15/2019 5:02 PM	DMR64 File	4,256 KB
[id=[redacted]test (1).ppt.DMR64	12/15/2019 5:02 PM	DMR64 File	578 KB
[id=[redacted]test (1).rar.DMR64	12/15/2019 5:02 PM	DMR64 File	1 KB
[id=[redacted]test (1).srt.DMR64	12/15/2019 5:02 PM	DMR64 File	93 KB
[id=[redacted]test (1).ts.DMR64	12/15/2019 5:02 PM	DMR64 File	1,015,200 KB
[id=[redacted]test (2).mp3.DMR64	12/15/2019 5:02 PM	DMR64 File	6,296 KB
[id=[redacted]تست].jpg.DMR64	12/15/2019 5:02 PM	DMR64 File	374 KB
[id=[redacted]تست].mp3.DMR64	12/15/2019 5:02 PM	DMR64 File	4,485 KB
[id=[redacted]تست].mp4.DMR64	12/15/2019 5:02 PM	DMR64 File	111,221 KB
[id=[redacted]تست].mpeg.DMR64	12/15/2019 5:02 PM	DMR64 File	45,740 KB

همانطور که در تصویر بالا قابل مشاهده است، تمامی انواع فایل‌ها رمزگذاری شده‌اند و نام آن‌ها به الگوی زیر تغییر پیدا کرده است.

[id=********]نام.فایل.پسوند DMR64

براساس بررسی‌های صورت گرفته، این باج‌افزار طیف وسیعی از فایل‌ها با پسوندهای مختلف، حتی فایل‌های اجرایی با پسوند exe. را نیز رمزگذاری می‌نماید.

پس از اتمام فرآیند رمزگذاری، تصویر پیغام باج‌خواهی باج‌افزار با عنوان READ THIS !!!.hta !!! بر روی صفحه نمایش سیستم قربانی نمایان می‌شود.



براساس پیغام باج‌خواهی این باج‌افزار، قربانی جهت برقراری ارتباط با مهاجم یا مهاجمین، باید شناسه اشاره شده را در قسمت عنوان ایمیل خود قرار داده و آن را به آدرس Agent.DMR@protonmail.com ارسال نماید. در صورت عدم دریافت پاسخ تا مدت زمان ۴۸ساعت، می‌تواند ایمیل دیگری را مجدداً به آدرس دیگری با عنوان Agent.DMR@aol.com ارسال کند. همچنین، در قسمتی از پیغام باج‌خواهی عنوان شده است که قربانی قبل از پرداخت مبلغ باج می‌تواند یک فایل غیر فشرده با حجم ۱ مگابایت که حاوی اطلاعات ارزشمند نظیر پایگاه داده، فایل پشتیبان (بکاپ)، فایل‌های اکسل و ... نباشد را از طریق ایمیل جهت رمزگشایی رایگان ارسال کند. مبلغ باج درون پیغام ذکر نشده است و قربانی جهت اطلاع از آن باید با مهاجم یا مهاجمین ارتباط برقرار کند.

باج‌افزار DMR پس از اتمام فعالیت خود در سیستم قربانی، به صورت غیرفعال درون سیستم باقی می‌ماند.

۵-۲ روش انتشار:

با توجه به اینکه مدت زمان زیادی از انتشار این باج‌افزار نمی‌گذرد، تاکنون گزارشی از روش یا روش‌های انتشار آن منتشر نشده است. لذا، احتمال نفوذ باج‌افزار DMR از روش‌های رایج همچون پیوست‌های مخرب درون هرزنامه‌ها، فایل‌های آلوده به کد باج‌افزار که در سایت‌های نامعتبر بارگذاری شده‌اند، کرک جعلی نرم‌افزارها، سوء استفاده از آسیب‌پذیری سیستم‌عامل یا نرم‌افزارها و همچنین نفوذ از طریق شکستن رمزعبور RDP وجود دارد.

۵-۳ روش جلوگیری:

با توجه به مشخص نبودن روش انتشار باج‌افزار، توصیه می‌شود اقدامات عمومی همچون به روز رسانی سیستم‌عامل و مرورگرها، به روز رسانی مداوم آنتی‌ویروس، باز نکردن پیوست ایمیل‌های ناشناس و در صورتی که جهت ارتباطات خود از پروتکل RDP استفاده می‌نمایید، اقدامات مربوط به امن‌سازی آن حتماً در دستور کار قرار گیرد.

٦. تحلیل ایستا

بررسی‌های اولیه بر روی فایل اجرایی این باج‌افزار نشان می‌دهد که باج‌افزار DMR بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ویندوز ویستا به بعد، اجرا خواهد شد.

OS version (major)	0006	Windows Vista
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	
Sub system version (major)	0006	
Sub system version (minor)	0000	

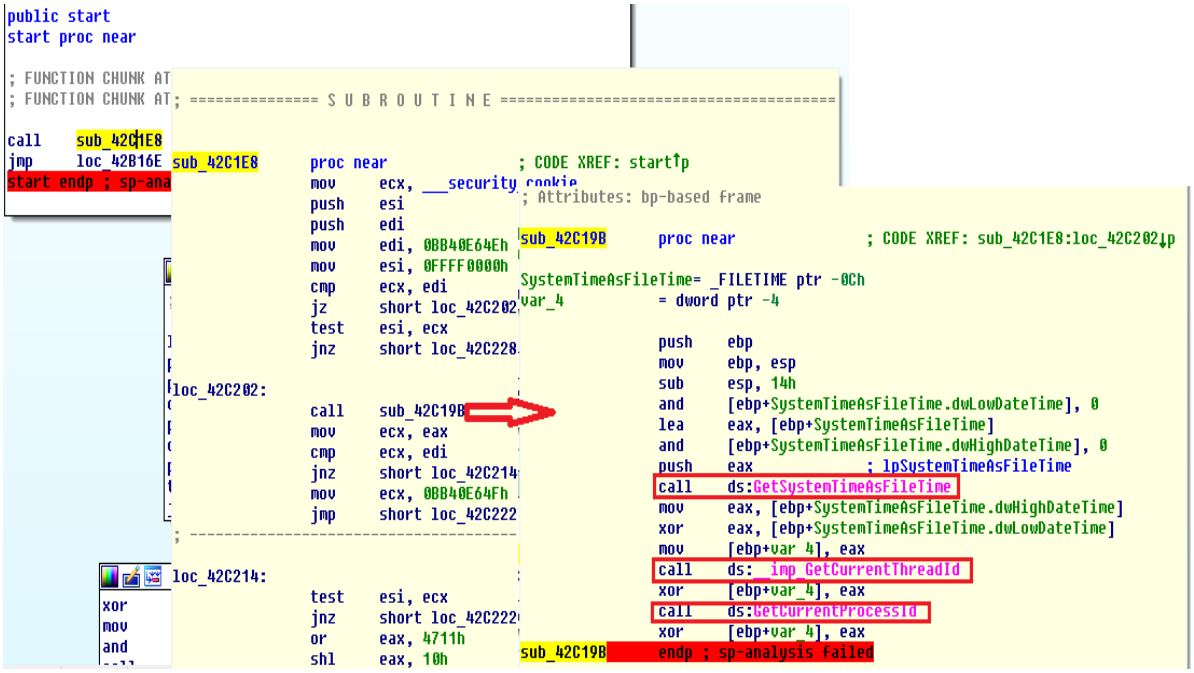
٦-١ تحلیل کد:

قسمت‌های کد و داده فایل، توسط پکر UPX پک شده‌اند.

01	00001000	0004F000	00000400	00000000	E0000080	UPX0	!ZERO SIZE!	?	
02 ep	00050000	00030000	00000400	0002F600	E0000040	UPX1	FB DF F9 FF 68 00 05 ...	h |, ↰ Y B •%↑(oIw	Strong Packed - 0.8457 % ZERO
03 i...	00080000	00001000	0002FA00	00000400	C0000040	.rsrc	00 00 00 00 00 00 00 0...	↑ ↑	Very not packed - 42.7734 % ZERO

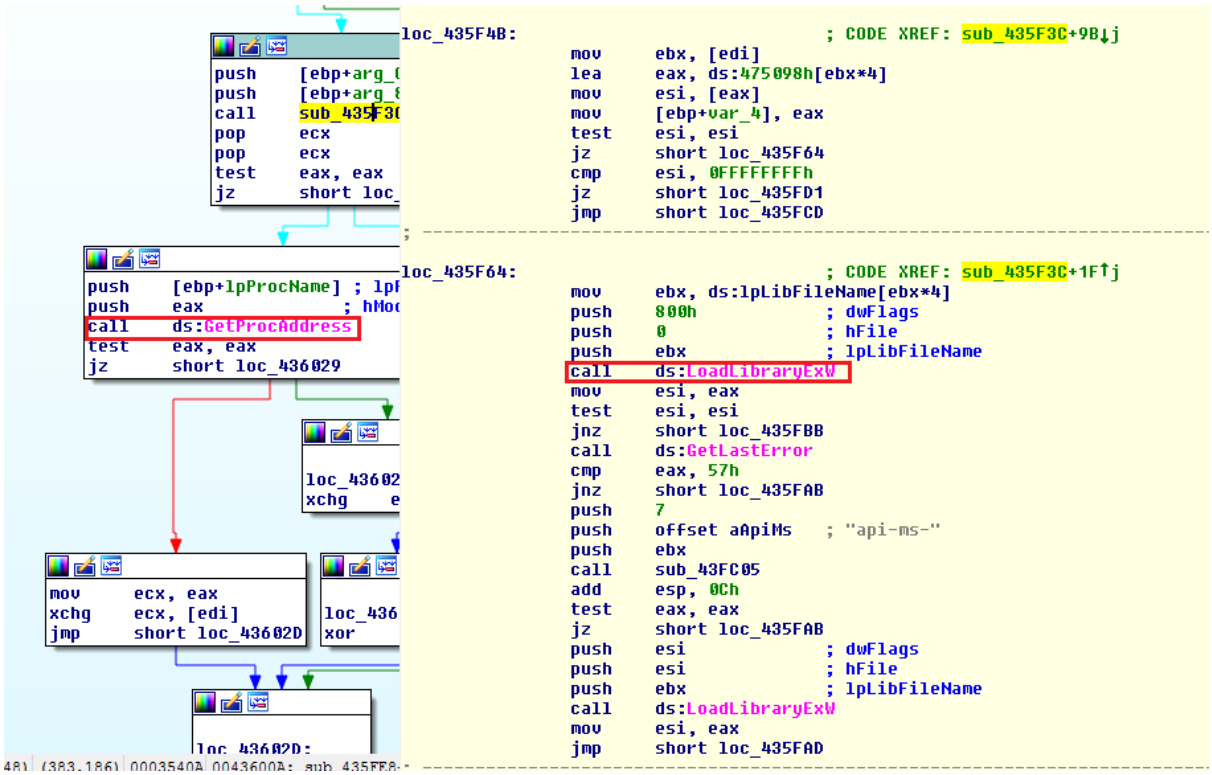
پس از آنپک کردن بخش‌های مذکور، موارد زیر در رابطه با کد باج‌افزار مشاهده شد.

این باج‌افزار از تابع Start شروع شده و در ابتدای فعالیت خود، زمان سیستم قربانی را دریافت می‌کند.



توابع آماده سازی فایل جهت اجرا در سیستم قربانی نیز، در تصویر بالا مشخص شده‌اند.

باج‌افزار DMR همانند اکثر باج‌افزارها از تابع LoadLibraryExW جهت استفاده از کتابخانه‌های موردنیاز خود بهره برده است. برای دسترسی به هر تابع درون کتابخانه‌ها نیز از تابع GetProcAddress استفاده شده است.



این باج‌افزار، از یک فرآیند ویندوزی به نام mshta.exe جهت نمایش پیغام باج‌خواهی خود استفاده می‌کند که در بخش قبل به آن اشاره شد.

تصویر زیر بخشی از این پیغام را نشان می‌دهد.

```
'ZNbVAAAAAElFTkSuQmCC',27h,'><div class=',27h,'header',27h,'><div>All your '
'files have been encrypted!</div></div><div class=',27h,'bold',27h,'>You'
'r documents, photos, databases and other important files have bee'
'n encrypted with strongest encryption. you can return all your fi'
'les if you want to restore files, write us to the e-mail: <span c'
'lass=',27h,'mark',27h,'>Agent.DMR@protonmail.com</span></div> <div clas'
's=',27h,'bold',27h,'>Write this ID in the subject e-mail:<span class=',27h
'mark',27h,'>',0
```

باج‌افزار DMR تمام برچسب‌های ممکن برای درایوهای سیستم‌عامل را جهت فرآیند رمزگذاری، جست‌وجو می‌کند.

```
db 'M:\',0
db 'N:\',0
db 'A:\',0      db 'O:\',0
db 'B:\',0      db 'P:\',0
db 'C:\',0      db 'Q:\',0
db 'D:\',0      db 'R:\',0
db 'E:\',0      db 'S:\',0
db 'F:\',0      db 'T:\',0
db 'G:\',0      db 'U:\',0
db 'H:\',0      db 'V:\',0
db 'I:\',0      db 'W:\',0
db 'J:\',0      db 'X:\',0
db 'K:\',0      db 'Y:\',0
db 'L:\',0      db 'Z:\',0
```

تمام اطلاعات موردنیاز در مورد درایو یافت شده، توسط تابع GetVolumeInformationA استخراج می‌شود.

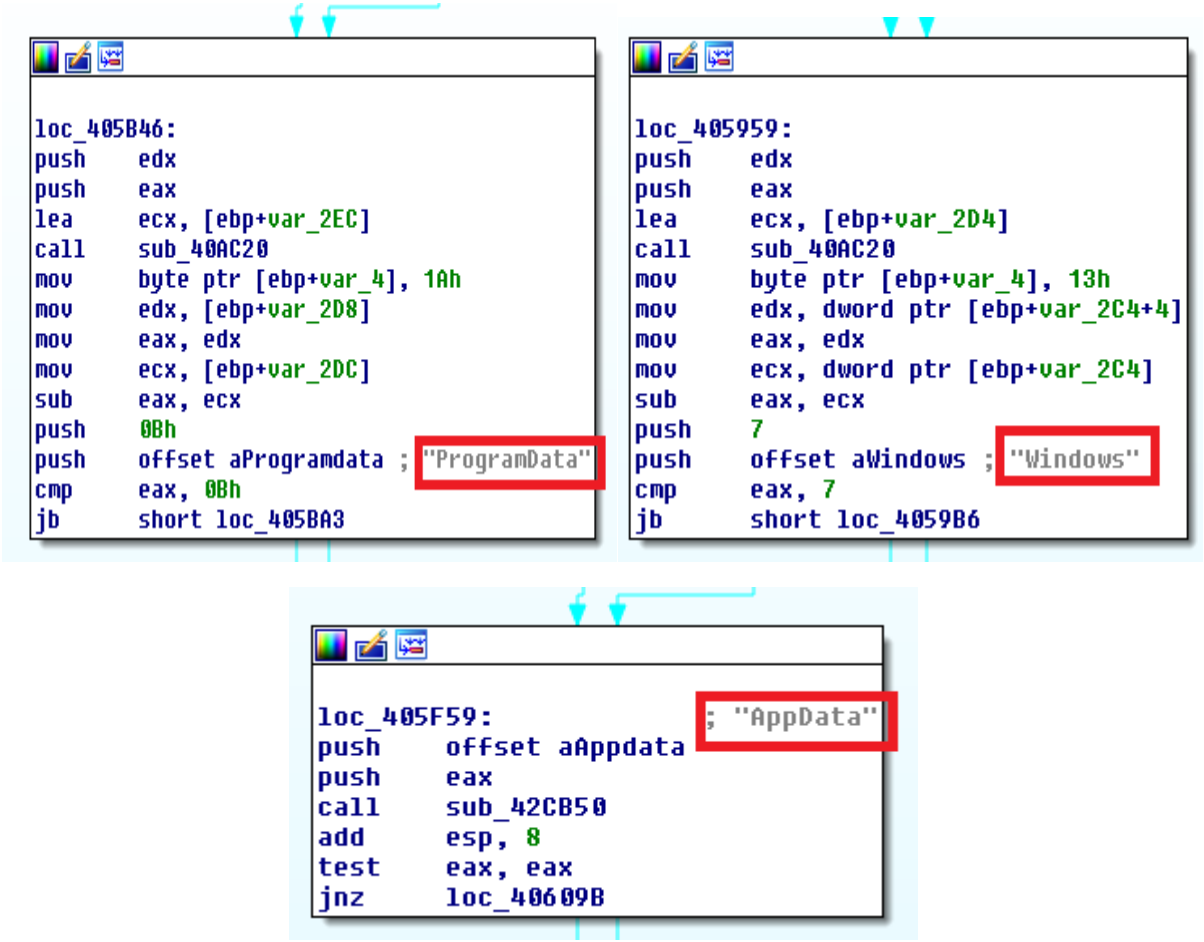
```
push    0               ; nFileSystemNameSize
push    0               ; lpFileSystemNameBuffer
push    0               ; lpFileSystemFlags
push    0               ; lpMaximumComponentLength
push    ecx             ; lpVolumeSerialNumber
push    0               ; nVolumeNameSize
lea     eax, [ebp+lpRootPathName]
mov     [ebp+var_278], 24h
cmovnb  eax, [ebp+lpRootPathName]
push    0               ; lpVolumeNameBuffer
push    eax             ; lpRootPathName
call    ds:GetVolumeInformationA
mov     edx, [ebp+var_180]
cmp     edx, 10h
jb      short loc_40DBAD
```

درون کد باج‌افزار به پوشه‌ها و مسیرهای خاصی از سیستم‌عامل اشاره شده است که پس از اجرای باج‌افزار و بررسی رفتار آن در هر یک از این مسیرها و پوشه‌های اشاره شده، موارد زیر مشاهده شد.

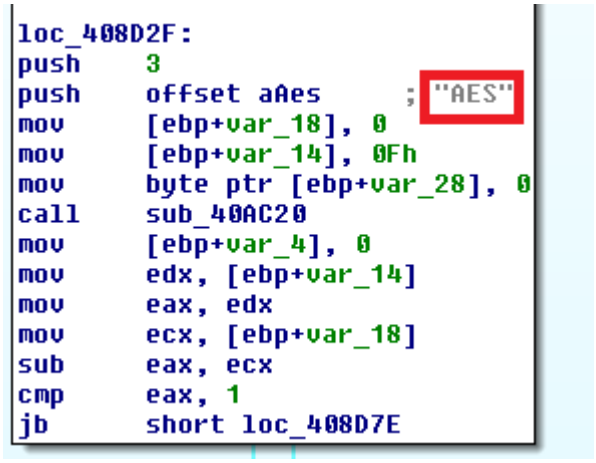
محتوای قسمت Recycle Bin توسط باج‌افزار حذف می‌شود.

```
loc_40F62F:
push    edi
push    eax
lea     ecx, [ebp+var_2D4]
call    sub_40AC20
mov     byte ptr [ebp+var_4], 19h
mov     edx, dword ptr [ebp+var_2C4+4]
mov     eax, edx
mov     ecx, dword ptr [ebp+var_2C4]
sub     eax, ecx
push    0Ch
push    offset aRecycle_bin ; "$Recycle.Bin"
cmp     eax, 0Ch
jb      short loc_40F68C
```

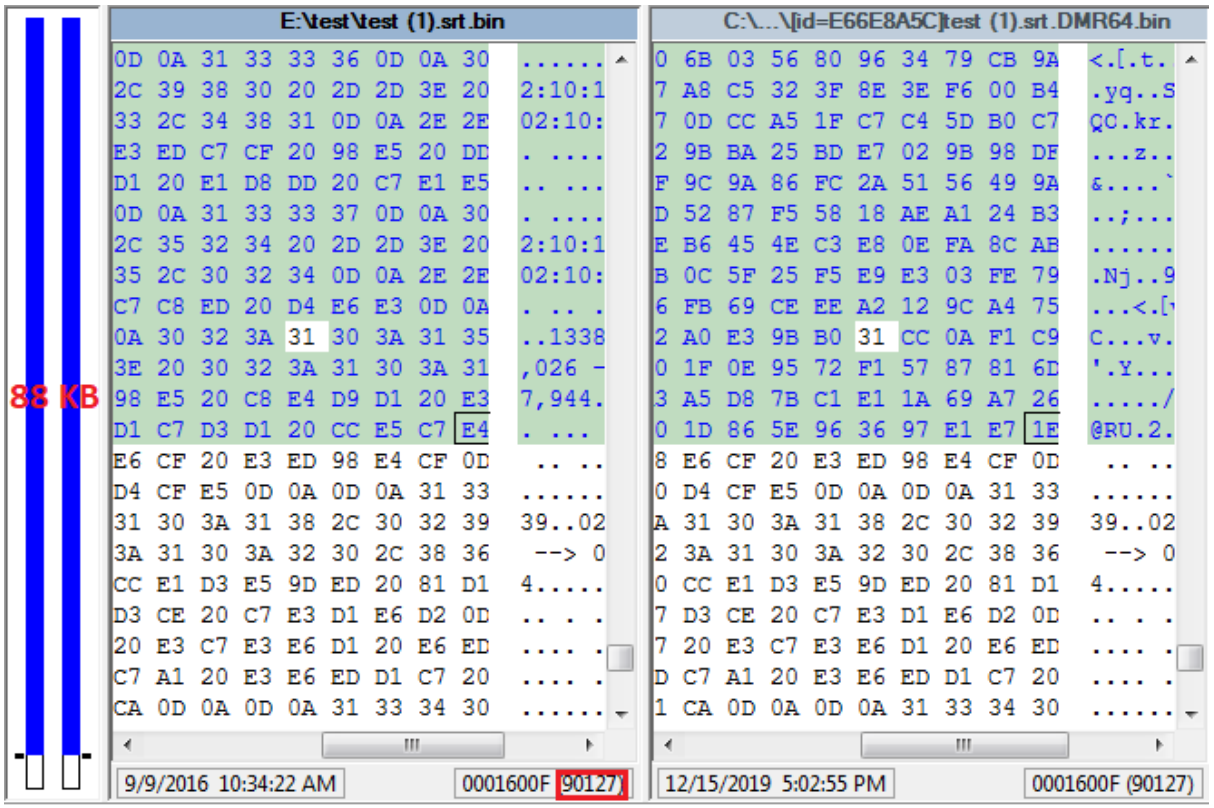
پوشه‌های ProgramData، Windows و AppData سیستم‌عامل در لیست سفید قرار داشته و هیچ فایلی در این پوشه‌ها رمز گذاری نخواهد شد.

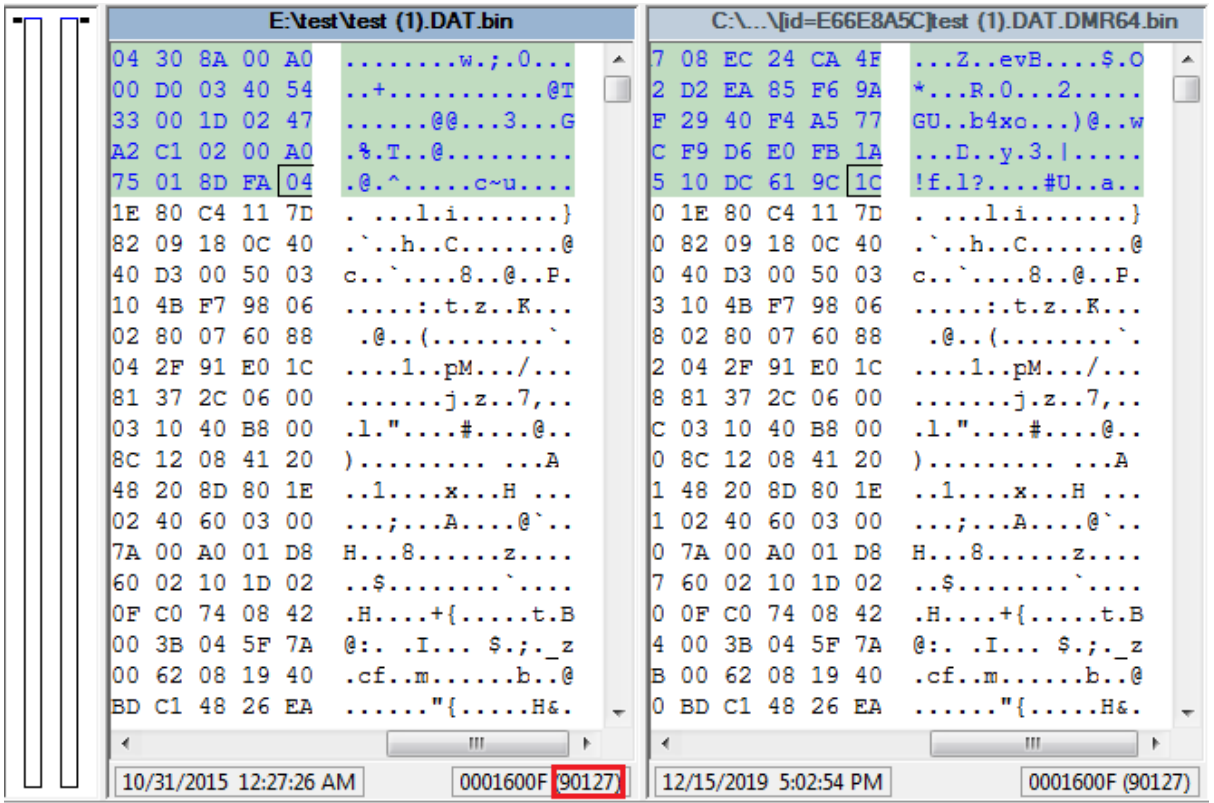


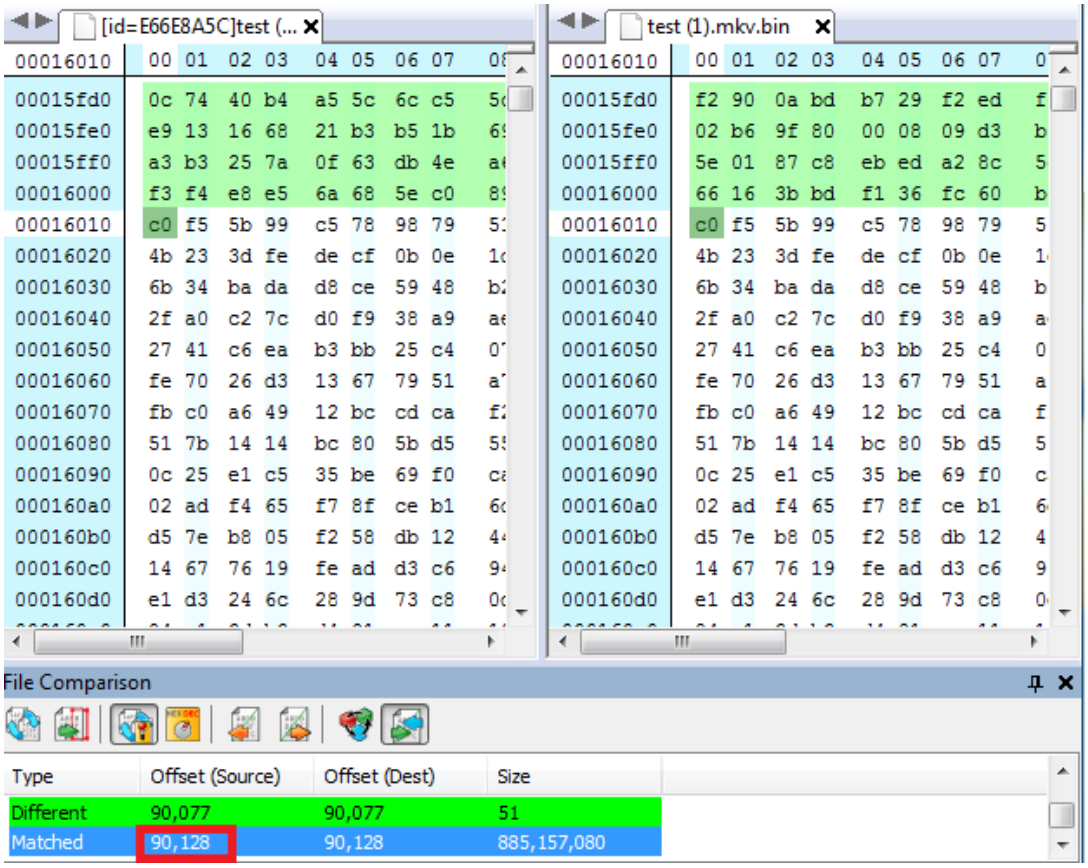
باج‌افزار DMR از الگوریتم AES جهت رمزگذاری فایل‌های موردنظر خود در سیستم قربانی بهره برده است.



بررسی نمونه فایل‌های رمزشده با نمونه سالم آن‌ها نشان می‌دهد این باج‌افزار، فقط ۸۸کیلوبایت اول از هر فایل را رمزگذاری می‌کند.

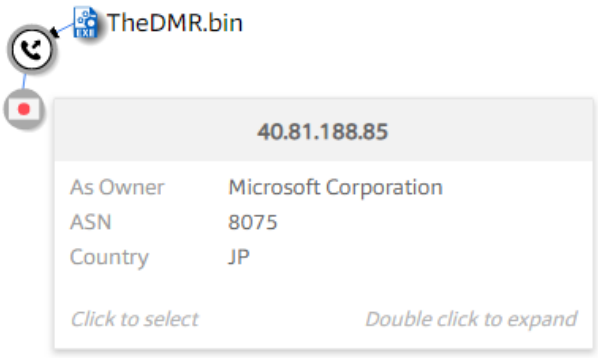






۶-۲ تحلیل ترافیک شبکه:

مطابق بررسی ترافیک شبکه بعد از اجرای باج‌افزار و همینطور نتایج سندباکس‌های آنلاین، مورد خاصی در رابطه با ارتباط باج‌افزار مشاهده نشد. اما، خروجی سامانه virustotal ارتباط این باج‌افزار با یک آی‌پی در کشور ژاپن را نشان می‌دهد.



۶-۳ رمزگشایی:

در حال حاضر، هیچ‌گونه ابزاری جهت رمزگشایی فایل‌های رمزشده توسط این باج‌افزار، ارایه نشده است.