

باسمه تعالی

تحلیل فنی باج افزار

DMR

فهرست مطالب

۱. مقدمه : ۳
۲. مشخصات فایل اجرایی : ۳
۳. شجره‌نامه ۳
۴. میزان تهدید فایل باج‌افزار: ۳
۵. تحلیل پویا ۴
- ۱-۵ آناتومی حمله: ۴
- ۲-۵ روش انتشار: ۶
- ۳-۵ روش جلوگیری: ۶
- ۶- تحلیل ایستا ۶
- ۱-۶ تحلیل کد: ۶
- ۲-۶ تحلیل ترافیک شبکه: ۱۲
- ۳-۶ رمزگشایی: ۱۴

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 رمز شده 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 :

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

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.

۴. میزان تهدید فایل باج‌افزار

در حال حاضر تعداد ۴۰ مورد ۷۰٪ از ضدبج‌افزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.

40 / 70

40 engines detected this file

3e3bb3fa705247fdd41c0a73a52683049948e383b082fc6c7e0fba06cf9097bc

TheDMR.bin

peexe runtime-modules upx

Community Score

۵. تحلیل پویا

۵-۱ آناتومی حمله:

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

باج افزار DMR بلافاصله پس از اجرا در سیستم قربانی، ابتدا تمام فایل های موجود بر روی صفحه دسکتاپ را رمزگذاری کرده، سپس محتوای موجود در قسمت Recycle Bin سیستم قربانی را حذف کرده و در انتها فایل های موجود در دیگر مسیرها و درایوهای سیستم را رمزگذاری می نماید. تمامی این فرآیندها در مدت زمان بسیار کوتاهی رخ می دهد.

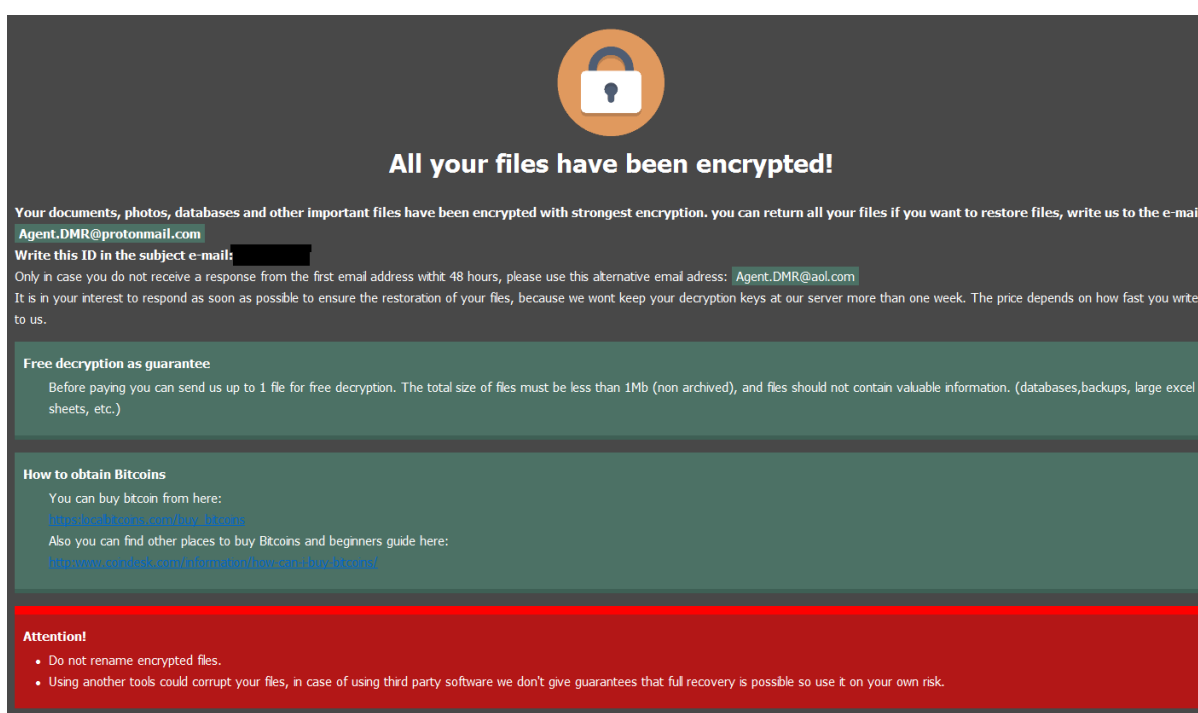
Name	Date modified	Type	Size
[id=██████████]test (1).apk.DMR64	12/15/2019 5:02 PM	DMR64 File	9,288 KB
[id=██████████]test (1).avi.DMR64	12/15/2019 5:02 PM	DMR64 File	31,433 KB
[id=██████████]test (1).bmp.DMR64	12/15/2019 5:02 PM	DMR64 File	737 KB
[id=██████████]test (1).DAT.DMR64	12/15/2019 5:02 PM	DMR64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

DMR64.پسوند فایل.نام[id=*****]

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 **!!!.hta READ THIS !!!** بر روی صفحه نمایش سیستم قربانی نمایان می‌شود.



All your files have been encrypted!

Your documents, photos, databases and other important files have been encrypted with strongest encryption. you can return all your files if you want to restore files, write us to the e-mail: Agent.DMR@protonmail.com

Write this ID in the subject e-mail: [REDACTED]

Only in case you do not receive a response from the first email address within 48 hours, please use this alternative email address: Agent.DMR@aol.com

It is in your interest to respond as soon as possible to ensure the restoration of your files, because we won't keep your decryption keys at our server more than one week. The price depends on how fast you write to us.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

You can buy bitcoin from here:
<https://bitcoindesktop.com/buy-bitcoin/>

Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-to-buy-bitcoin/>

Attention!

- Do not rename encrypted files.
- Using another tools could corrupt your files, in case of using third party software we don't give guarantees that full recovery is possible so use it on your own risk.

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 ۴۸ ساعت، 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.

باچ افزار DMR پس از اتمام فعالیت خود در سیستم قربانی، به صورت غیر فعال درون سیستم باقی می ماند.

۲-۵ روش انتشار:

با توجه به اینکه مدت زمان زیادی از انتشار این باچ افزار نمی گذرد، تاکنون گزارشی از روش یا روش های انتشار آن منتشر نشده است. لذا، احتمال نفوذ باچ افزار DMR از روش های رایج همچون پیوست های مخرب درون هرزنامه ها، فایل های آلوده به کد باچ افزار که در سایت های نامعتبر بارگذاری شده اند، کرک جعلی نرم افزارها، سوء استفاده از آسیب پذیری سیستم عامل یا نرم افزارها و همچنین نفوذ از طریق شکستن رمز عبور RDP وجود دارد.

۳-۵ روش جلوگیری:

با توجه به مشخص نبودن روش انتشار باچ افزار، توصیه می شود اقدامات عمومی همچون به روز رسانی سیستم عامل و مرورگرها، به روز رسانی مداوم آنتی ویروس، باز نکردن پیوست ایمیل های ناشناس و در صورتی که جهت ارتباطات خود از پروتکل RDP استفاده می نمایید، اقدامات مربوط به امن سازی آن حتماً در دستور کار قرار گیرد.

۶. تحلیل ایستا

بررسی های اولیه بر روی فایل اجرایی این باچ افزار نشان می دهد که باچ افزار DMR بر روی تمامی نسخه های سیستم عامل 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	

۱-۶ تحلیل کد:

قسمت های کد و داده فایل، توسط پکر UPX پک شده اند.

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 , 4 Y B *%I(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 بخش های مذکور، موارد زیر در رابطه با کد باچ افزار مشاهده شد.

این باچ افزار از تابع Start شروع شده و در ابتدای فعالیت خود، زمان سیستم قربانی را دریافت می کند.

```

public start
start proc near
; FUNCTION CHUNK AT
; FUNCTION CHUNK AT; ----- SUBROUTINE -----
call sub_42C1E8
jmp loc_42B16F sub_42C1E8
start endp ; sp-ana

proc near ; CODE XREF: start↑p
; Attributes: bp-based frame
mov ecx, __security_cookie
push esi
push edi
mov edi, 0BB40E64Eh sub_42C19B proc near ; CODE XREF: sub_42C1E8:loc_42C202↓p
mov esi, 0FFFFFF0000h
cmp ecx, edi
jz short loc_42C202
test esi, ecx
jnz short loc_42C228

loc_42C202:
call sub_42C19B
mov ecx, eax
cmp ecx, edi
jnz short loc_42C214
mov ecx, 0BB40E64Fh
jmp short loc_42C222

loc_42C214:
xor
mov
and
shl
test esi, ecx
jnz short loc_42C222
or eax, 4711h
shl eax, 10h sub_42C19B endp ; sp-analysis failed

proc near ; CODE XREF: sub_42C19B:loc_42C202↓p
push ebp
mov ebp, esp
sub esp, 14h
and [ebp+SystemTimeAsFileTime.dwLowDateTime], 0
lea eax, [ebp+SystemTimeAsFileTime]
and [ebp+SystemTimeAsFileTime.dwHighDateTime], 0
push eax ; lpSystemTimeAsFileTime
call ds:GetSystemTimeAsFileTime
mov eax, [ebp+SystemTimeAsFileTime.dwHighDateTime]
xor eax, [ebp+SystemTimeAsFileTime.dwLowDateTime]
mov [ebp+var_4], eax
call ds:imp_GetCurrentThreadId
xor [ebp+var_4], eax
call ds:GetCurrentProcessId
xor [ebp+var_4], eax
sub_42C19B endp ; sp-analysis failed

```

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.

```

loc_435F4B:
mov ebx, [edi]
lea eax, ds:4750980h[ebx*4]
mov esi, [eax]
mov [ebp+var_4], eax
test esi, esi
jz short loc_435F64
cmp esi, 0FFFFFFFh
jz short loc_435FD1
jmp short loc_435FCD

loc_435F64:
push [ebp+lpProcName] ; lpProcName
push eax ; hMod
call ds:GetProcAddress
test eax, eax
jz short loc_436029

loc_436029:
mov ecx, eax
xchg ecx, [edi]
jmp short loc_43602D

loc_435F4B:
; CODE XREF: sub_435F3C+9B↓j
mov ebx, [edi]
lea eax, ds:4750980h[ebx*4]
mov esi, [eax]
mov [ebp+var_4], eax
test esi, esi
jz short loc_435F64
cmp esi, 0FFFFFFFh
jz short loc_435FD1
jmp short loc_435FCD

loc_435F64:
; CODE XREF: sub_435F3C+1F↑j
mov ebx, ds:lpLibFileName[ebx*4]
push 800h ; dwFlags
push 0 ; hFile
push ebx ; lpLibFileName
call ds:LoadLibraryExW
mov esi, eax
test esi, esi
jnz short loc_435FBB
call ds:GetLastError
cmp eax, 57h
jnz short loc_435FAB
push 7
push offset aApiMs ; "api-ms-"
push ebx
call sub_43FC05
add esp, 0Ch
test eax, eax
jz short loc_435FAB
push esi ; dwFlags
push esi ; hFile
push ebx ; lpLibFileName
call ds:LoadLibraryExW
mov esi, eax
jmp short loc_435FAD

```

این باج افزار، از یک فرآیند ویندوزی به نام mshta.exe جهت نمایش پیغام باج خواهی خود استفاده می کند که در بخش قبل به آن اشاره شد.



تصویر زیر بخشی از این پیغام را نشان می دهد.

```

'ZNbVAAAAAE1FTkSuQmCC',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
    
```

باج افزار DMR تمام برچسب های ممکن برای درایوهای سیستم عامل را جهت فرآیند رمز گذاری، جست و جو می کند.


```

db 'M:\',0
db 'N:\',0
db 'O:\',0
db 'P:\',0
db 'Q:\',0
db 'R:\',0
db 'S:\',0
db 'T:\',0
db 'U:\',0
db 'V:\',0
db 'W:\',0
db 'X:\',0
db 'Y:\',0
db 'Z:\',0

```

تمام اطلاعات مورد نیاز در مورد درایو یافت شده، توسط تابع GetVolumeInformationA استخراج می شود.

```

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
jnb short loc_40DBAD

```

درون کد باج افزار به پوشه ها و مسیرهای خاصی از سیستم عامل اشاره شده است که پس از اجرای باج افزار و بررسی رفتار آن در هر یک از این مسیرها و پوشه های اشاره شده، موارد زیر مشاهده شد. محتوای قسمت Recycle Bin توسط باج افزار حذف می شود.

```

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
jnb short loc_40F68C

```

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

```

loc_405B46:
push     edx
push     eax
lea     ecx, [ebp+var_2EC]
call    sub_40AC20
mov     byte ptr [ebp+var_4], 1Ah
mov     edx, [ebp+var_2D8]
mov     eax, edx
mov     ecx, [ebp+var_2DC]
sub     eax, ecx
push    0Bh
push    offset aProgramdata ; "ProgramData"
cmp     eax, 0Bh
jb     short loc_405BA3

loc_405959:
push     edx
push     eax
lea     ecx, [ebp+var_2D4]
call    sub_40AC20
mov     byte ptr [ebp+var_4], 13h
mov     edx, dword ptr [ebp+var_2C4+4]
mov     eax, edx
mov     ecx, dword ptr [ebp+var_2C4]
sub     eax, ecx
push    7
push    offset aWindows ; "Windows"
cmp     eax, 7
jb     short loc_4059B6

loc_405F59:
push    offset aAppdata ; "AppData"
push    eax
call    sub_42CB50
add     esp, 8
test    eax, eax
jnz    loc_40609B
    
```

باج افزار DMR از الگوریتم AES جهت رمز گذاری فایل‌های مورد نظر خود در سیستم قربانی بهره برده است.

```

loc_408D2F:
push    3
push    offset aAes ; "AES"
mov     [ebp+var_18], 0
mov     [ebp+var_14], 0Fh
mov     byte ptr [ebp+var_28], 0
call    sub_40AC20
mov     [ebp+var_4], 0
mov     edx, [ebp+var_14]
mov     eax, edx
mov     ecx, [ebp+var_18]
sub     eax, ecx
cmp     eax, 1
jb     short loc_408D7E
    
```

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

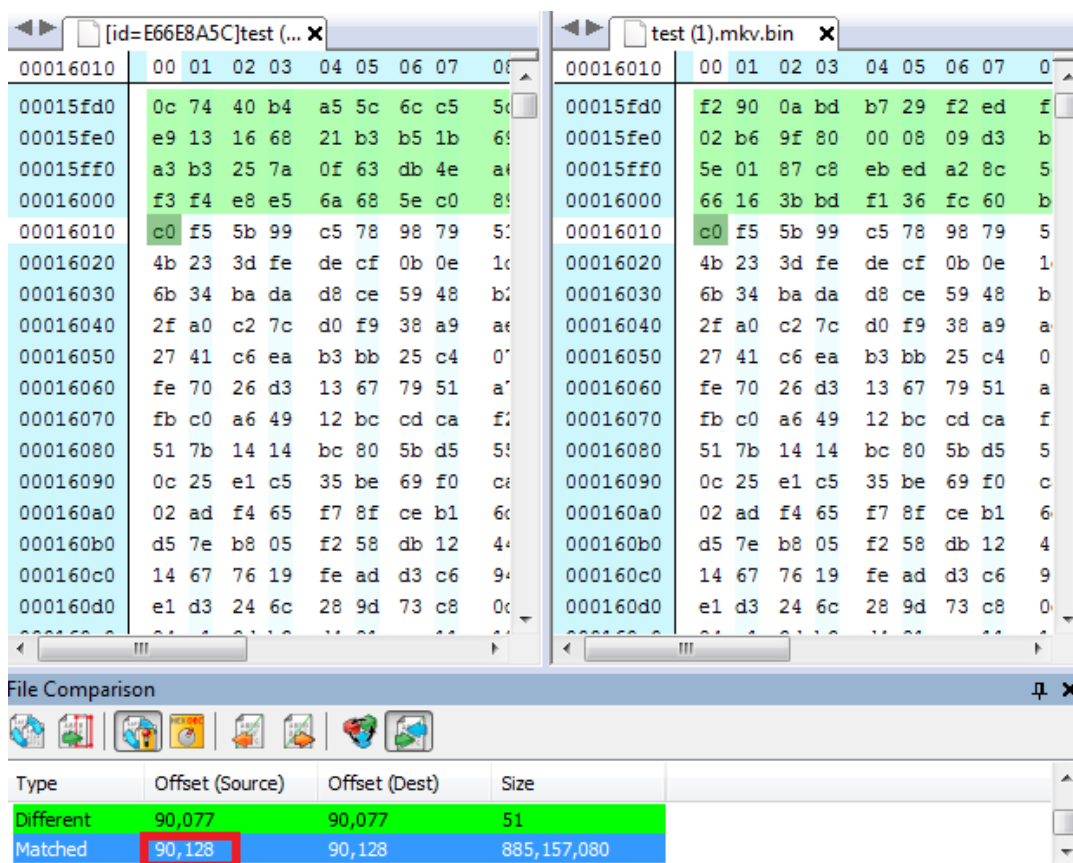
E:\test\test (1).srt.bin	C:\...\[id=E66E8A5C]test (1).srt.DMR64.bin
0D 0A 31 33 33 36 0D 0A 30	0 6B 03 56 80 96 34 79 CB 9A
2C 39 38 30 20 2D 2D 3E 20	7 A8 C5 32 3F 8E 3E F6 00 B4
33 2C 34 38 31 0D 0A 2E 2E	7 0D CC A5 1F C7 C4 5D B0 C7
E3 ED C7 CF 20 98 E5 20 DD	2 9B BA 25 BD E7 02 9B 98 DF
D1 20 E1 D8 DD 20 C7 E1 E5	F 9C 9A 86 FC 2A 51 56 49 9A
0D 0A 31 33 33 37 0D 0A 30	D 52 87 F5 58 18 AE A1 24 B3
2C 35 32 34 20 2D 2D 3E 20	E B6 45 4E C3 E8 0E FA 8C AB
35 2C 30 32 34 0D 0A 2E 2E	B 0C 5F 25 F5 E9 E3 03 FE 79
C7 C8 ED 20 D4 E6 E3 0D 0A	6 FB 69 CE EE A2 12 9C A4 75
0A 30 32 3A 31 30 3A 31 35	2 A0 E3 9B B0 31 CC 0A F1 C9
3E 20 30 32 3A 31 30 3A 31	0 1F 0E 95 72 F1 57 87 81 6D
98 E5 20 C8 E4 D9 D1 20 E3	3 A5 D8 7B C1 E1 1A 69 A7 26
D1 C7 D3 D1 20 CC E5 C7 E4	0 1D 86 5E 96 36 97 E1 E7 1E
E6 CF 20 E3 ED 98 E4 CF 0D	8 E6 CF 20 E3 ED 98 E4 CF 0D
D4 CF E5 0D 0A 0D 0A 31 33	0 D4 CF E5 0D 0A 0D 0A 31 33
31 30 3A 31 38 2C 30 32 39	A 31 30 3A 31 38 2C 30 32 39
3A 31 30 3A 32 30 2C 38 36	2 3A 31 30 3A 32 30 2C 38 36
CC E1 D3 E5 9D ED 20 81 D1	0 CC E1 D3 E5 9D ED 20 81 D1
D3 CE 20 C7 E3 D1 E6 D2 0D	7 D3 CE 20 C7 E3 D1 E6 D2 0D
20 E3 C7 E3 E6 D1 20 E6 ED	7 20 E3 C7 E3 E6 D1 20 E6 ED
C7 A1 20 E3 E6 ED D1 C7 20	D C7 A1 20 E3 E6 ED D1 C7 20
CA 0D 0A 0D 0A 31 33 34 30	1 CA 0D 0A 0D 0A 31 33 34 30

88 KB

9/9/2016 10:34:22 AM 0001600F 90127 12/15/2019 5:02:55 PM 0001600F (90127)

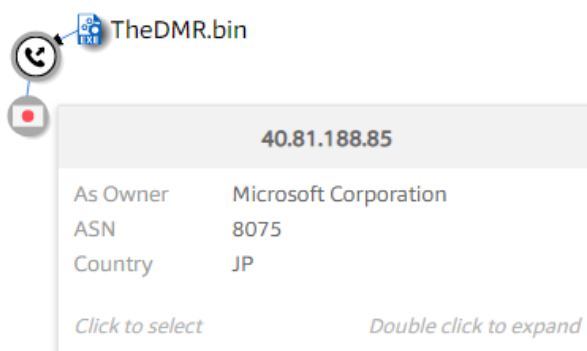
E:\test\test (1).DAT.bin	C:\...\[id=E66E8A5C]test (1).DAT.DMR64.bin
04 30 8A 00 A0	7 08 EC 24 CA 4F
00 D0 03 40 54	2 D2 EA 85 F6 9A
33 00 1D 02 47	F 29 40 F4 A5 77
A2 C1 02 00 A0	C F9 D6 E0 FB 1A
75 01 8D FA 04	5 10 DC 61 9C 1C
1E 80 C4 11 7D	0 1E 80 C4 11 7D
82 09 18 0C 40	0 82 09 18 0C 40
40 D3 00 50 03	0 40 D3 00 50 03
10 4B F7 98 06	3 10 4B F7 98 06
02 80 07 60 88	8 02 80 07 60 88
04 2F 91 E0 1C	2 04 2F 91 E0 1C
81 37 2C 06 00	8 81 37 2C 06 00
03 10 40 B8 00	C 03 10 40 B8 00
8C 12 08 41 20	0 8C 12 08 41 20
48 20 8D 80 1E	1 48 20 8D 80 1E
02 40 60 03 00	1 02 40 60 03 00
7A 00 A0 01 D8	0 7A 00 A0 01 D8
60 02 10 1D 02	7 60 02 10 1D 02
0F C0 74 08 42	0 0F C0 74 08 42
00 3B 04 5F 7A	4 00 3B 04 5F 7A
00 62 08 19 40	B 00 62 08 19 40
BD C1 48 26 EA	0 BD C1 48 26 EA

10/31/2015 12:27:26 AM 0001600F 90127 12/15/2019 5:02:54 PM 0001600F (90127)



۲-۶ تحلیل ترافیک شبکه:

مطابق بررسی ترافیک شبکه بعد از اجرای باج افزار و همینطور نتایج سندباکس های آنلاین، مورد خاصی در رابطه با ارتباط باج افزار مشاهده نشد. اما، خروجی سامانه virustotal ارتباط این باج افزار با یک آی پی در کشور ژاپن را نشان می دهد.



۳-۶ رمزگشایی:

در حال حاضر، هیچ گونه ابزاری جهت رمزگشایی فایل های رمز شده توسط این باج افزار، ارایه نشده است.