

بسمه تعالی



وزارت ارتباطات و فناوری اطلاعات  
سازمان فناوری اطلاعات ایران  
معاونت امنیت فضای تولید و تبادل اطلاعات



مرکز مدیریت امداد و هماهنگی  
عملیات رخدادهای رایانه ای

## تحلیل فنی باج افزار Makop

### گزارش تحلیلی

شناسه سند ..... MaherReportsTemplate\_14010906  
نوع سند ..... گزارش فنی  
شماره نگارش ..... ۰,۱  
تاریخ نگارش ..... ۱۴۰۱/۰۹/۰۶  
طبقه بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی - بین بزرگراه شهید مدرس و خیابان احمد قصیر - پلاک ۲۶۷

cert.ir



(۰۲۱) ۸۸۱۱۵۷۲۴



(۰۲۱) ۸۸۱۱۵۷۲۴





|    |                                     |
|----|-------------------------------------|
| ۳  | ۱. مقدمه: .....                     |
| ۳  | ۲. مشخصات فایل‌های اجرایی: .....    |
| ۴  | ۳. شجره‌نامه .....                  |
| ۴  | ۴. میزان تهدید فایل باج‌افزار ..... |
| ۴  | ۵. تحلیل پویا .....                 |
| ۴  | ۵-۱ آناتومی حمله.....               |
| ۹  | ۵-۲ روش انتشار:.....                |
| ۱۰ | ۵-۳ روش مقابله:.....                |
| ۱۰ | ۶. تحلیل ایستا .....                |
| ۱۰ | ۶-۱ تحلیل کد:.....                  |
| ۱۵ | ۶-۲ تحلیل ترافیک شبکه:.....         |
| ۱۵ | ۶-۳ رمزنگاری و رمزگشایی:.....       |
| ۱۶ | ۷. شناسه‌های تهدید (IOCs) .....     |
| ۱۶ | ۸. شناسایی (Detection) .....        |

## ۱. مقدمه:

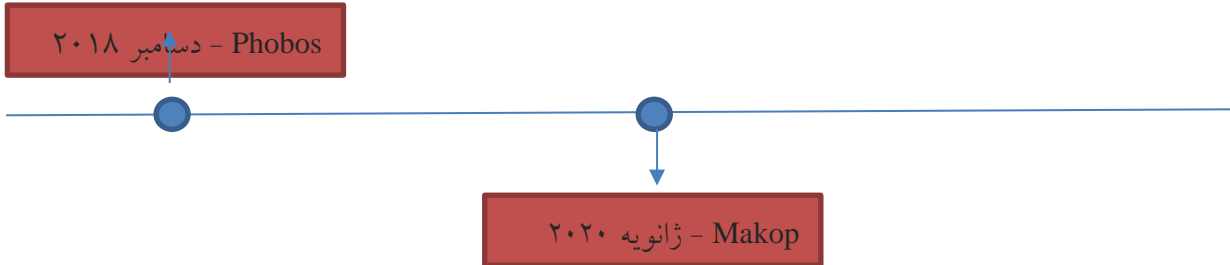
در اوایل سال ۲۰۲۲ حساب کاربری @siri\_urz در توییتر از یک باج‌افزار جدید به نام Makop رونمایی کرد. نسخه اولیه این باج‌افزار پسوند makop را به انتهای فایل‌های رمز شده اضافه می‌کرد. بر اساس تحقیقات صورت گرفته و شواهد موجود، این خانواده باج‌افزاری برای فعالیت خود احتیاجی به اتصال به اینترنت ندارند و بدون دسترسی مدیر سیستم (Administrator) نیز فعالیت خود را به انجام می‌رسانند. باج‌افزار Makop از دو رفتار متفاوت در رمزگذاری فایل‌های سیستم قربانی استفاده می‌کند و بر همین اساس، با دو نوع فایل اجرایی متفاوت نیز مواجه هستیم. یکی از آنها دقیقاً شبیه باج‌افزار Phobos است که ۳ بخش از فایل‌ها را رمز می‌کند و گونه دیگر تنها ابتدای فایل‌ها را رمز می‌کند. مشاهدات حاکی از آن است که باج‌افزارهای خانواده Makop برای توزیع در بین مهاجمین از مدل RaaS استفاده می‌کنند. الگوی پسوندگذاری باج‌افزار در گونه‌های مختلف، به خوبی نمایانگر این موضوع است.

## ۲. مشخصات فایل‌های اجرایی:

|  |             |
|--|-------------|
| d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043.exe | نام فایل    |
| 8D809510A9AE7B8EF6FC6A25E5FEAA22                                     | MD5         |
| EB0888326ADBBBDF1537A965C4D26C71549D43F6                             | SHA-1       |
| D0DD0F7658B938F9A3036CE308F5018AE0CF3BC516AAF3C18B947AFEE136C043     | SHA-256     |
| Win32 EXE  | نوع فایل    |
| 42.00 KB (43008 bytes)   | اندازه فایل |
| ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9.exe | نام فایل    |
| 586d6732d8c8d4045b05276f2a0cbf53                                     | MD5         |
| e58187c1708079e9487310f8c4b34722e4271f35                             | SHA-1       |
| ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9     | SHA-256     |
| Win32 EXE  | نوع فایل    |
| 847.65 KB (867994 bytes)   | اندازه فایل |

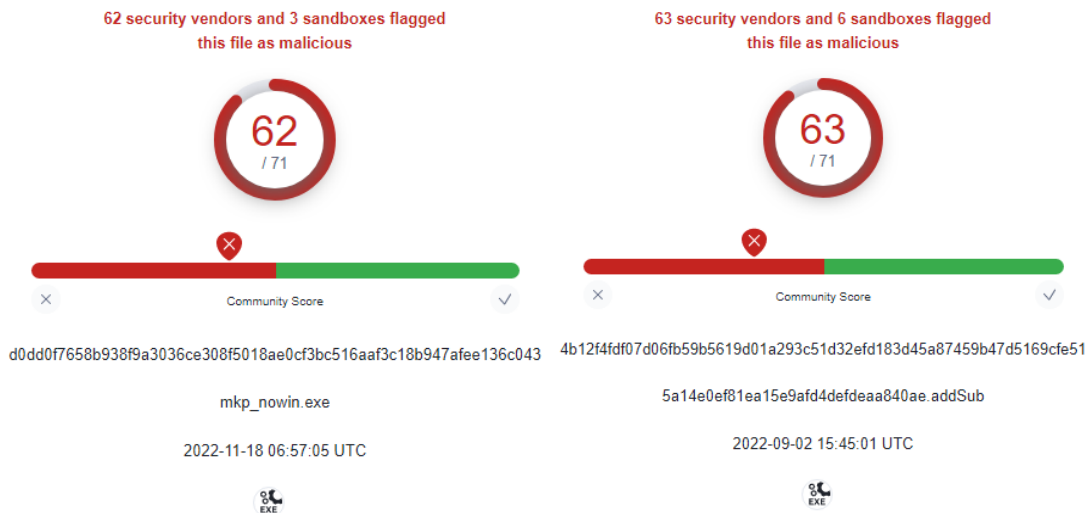
### ۳. شجره نامه

براساس گزارش‌های منتشر شده، ظاهراً باج‌افزار Makop نسخه‌ای توسعه یافته از باج‌افزار Phobos می‌باشد.



### ۴. میزان تهدید فایل باج‌افزار

دو نمونه از خانواده Makop در این تحلیل استفاده شده، که در حال حاضر ضدباج‌افزارهای سامانه VirusTotal بدین گونه آن‌ها را تحلیل می‌کنند:



### ۵. تحلیل پویا

#### ۵-۱ آناتومی حمله

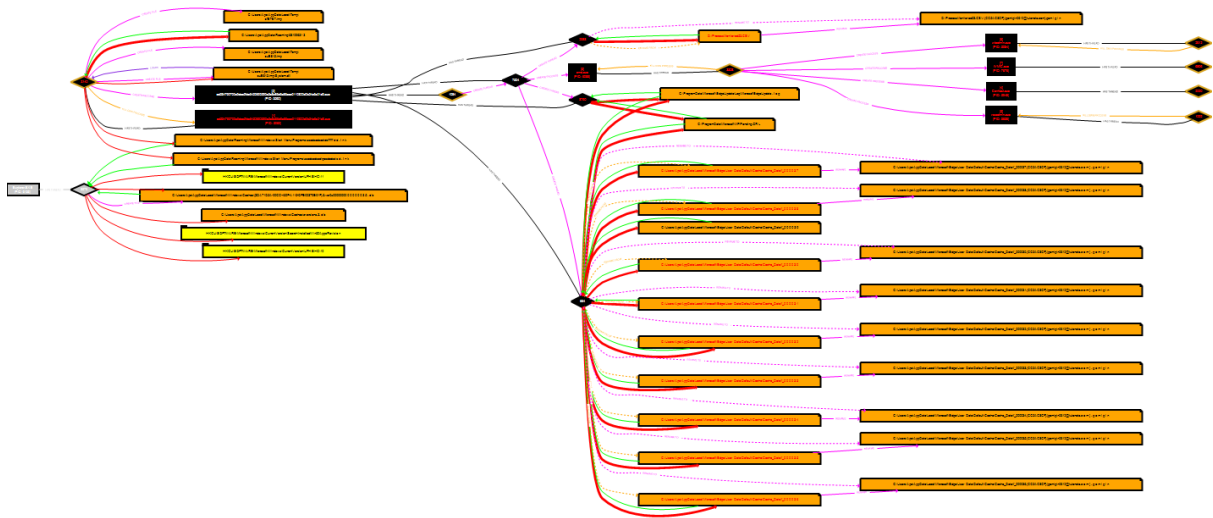
باج‌افزار Makop از آیکن نرم‌افزار اکسل برای فایل اجرایی خود استفاده کرده تا کاربران ناآگاه را فریب دهد.



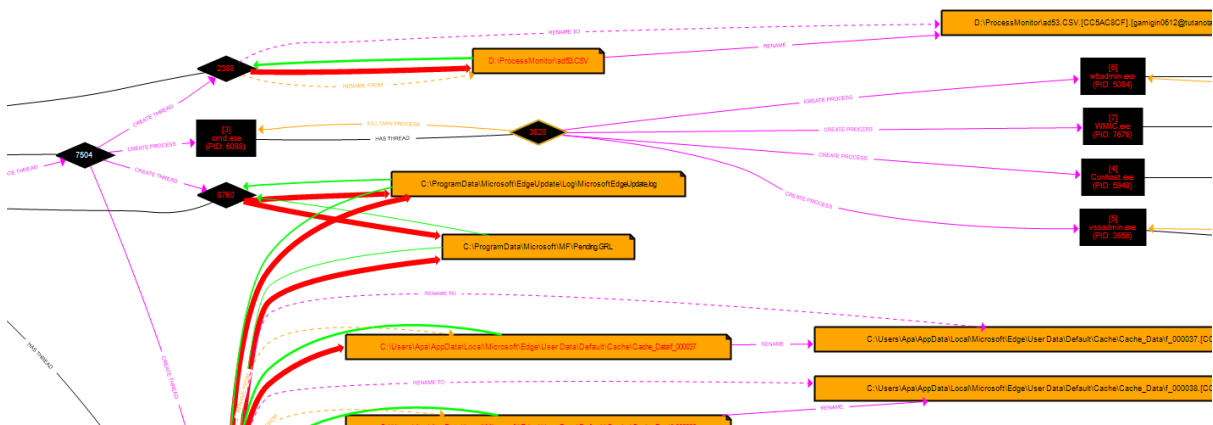
ad534790700a9d  
aa5fda64526925  
90e5e8c86d6a86  
aec0110822d0b...

پس از اجرای باج افزار در محیط آزمایشگاهی، رفتار زیر مشاهده شد:

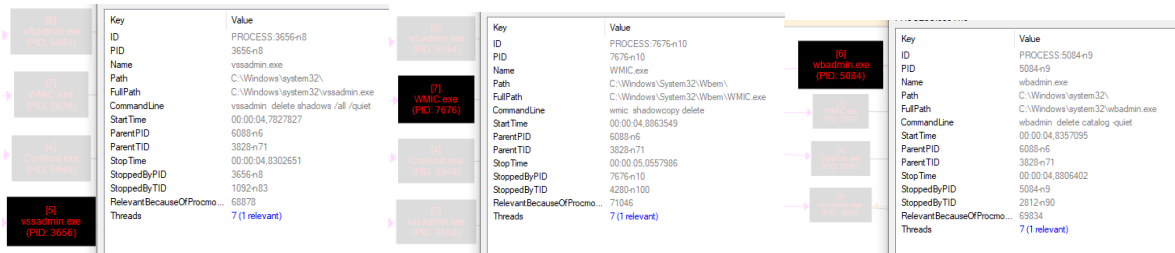
(گرافها مربوط به نمونه ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9 می باشند.)



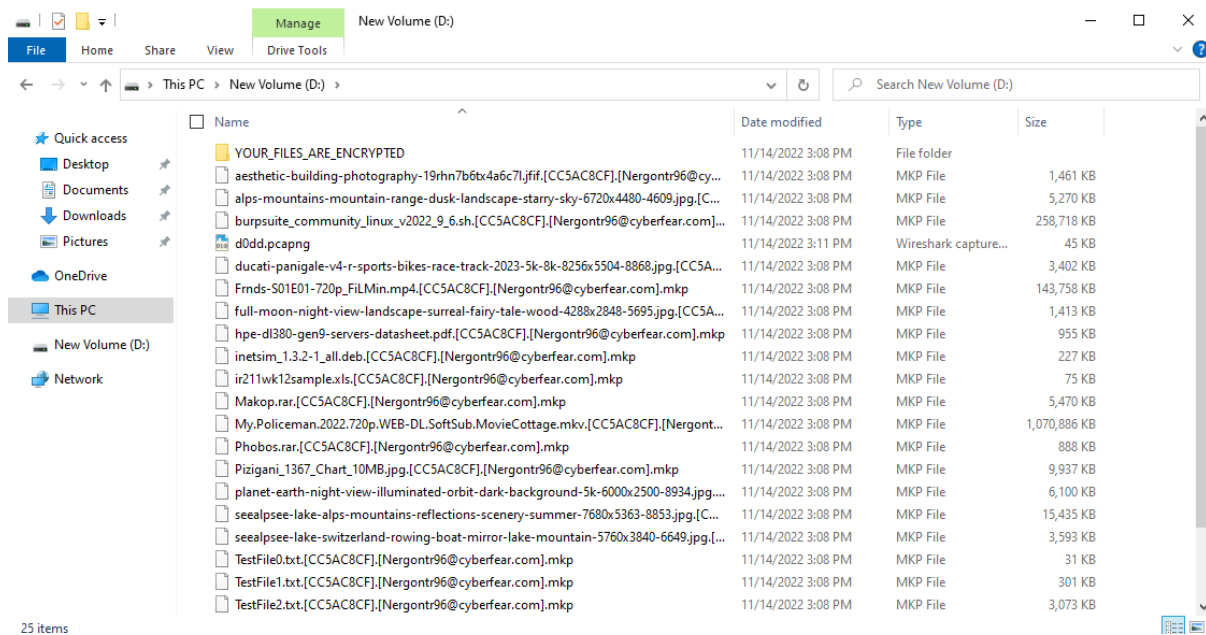
باج افزار در همان ابتدای فعالیت خود با فراخوانی cmd.exe در سیستم قربانی، دستورات زیر را اجرا می کند:



|  |                    |
|--|--------------------|
| <code>cmd.exe vssadmin delete shadows /all /quiet</code> | حذف فضای VSC       |
| <code>cmd.exe wbadm delete catalog -quiet</code>         | حذف اطلاعات بکآپها |
| <code>cmd.exe wmic shadowcopy delete</code>              | حذف فایل های VSC   |



سپس، فرآیند رمزگذاری فایل‌ها در سیستم قربانی شروع می‌شود؛ ابتدا تغییرات روی فایل‌ها صورت می‌گیرد و بعد از آن نام آنها تغییر می‌کند. تصویر زیر، فایل‌های رمزگذاری شده توسط نمونه اول را نشان می‌دهد.



همانطور که در تصویر بالا قابل مشاهده است به انتهای هر فایل رمز شده پسوند زیر اضافه شده است:

`.[CC5AC8CF].[Nergontr96@cyberfear.com].mkp`

الگوی نامگذاری پسوندها به این صورت می‌باشد:

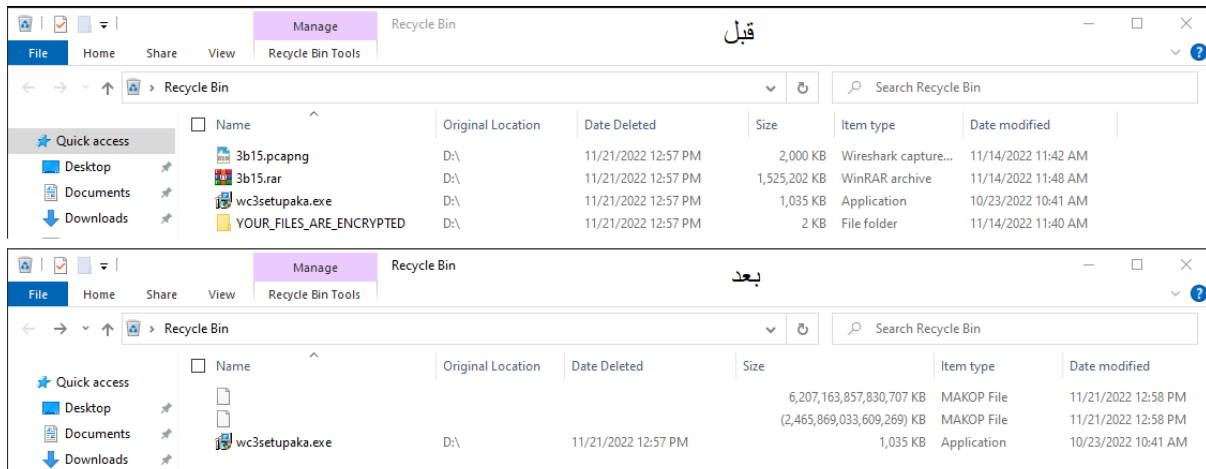
`"original-filename.[unique-ID].[email-address].makop-extension"`

می‌باشد. از جمله پسوندهای دیگری که این خانواده باج‌افزاری استفاده می‌کند عبارتند از:

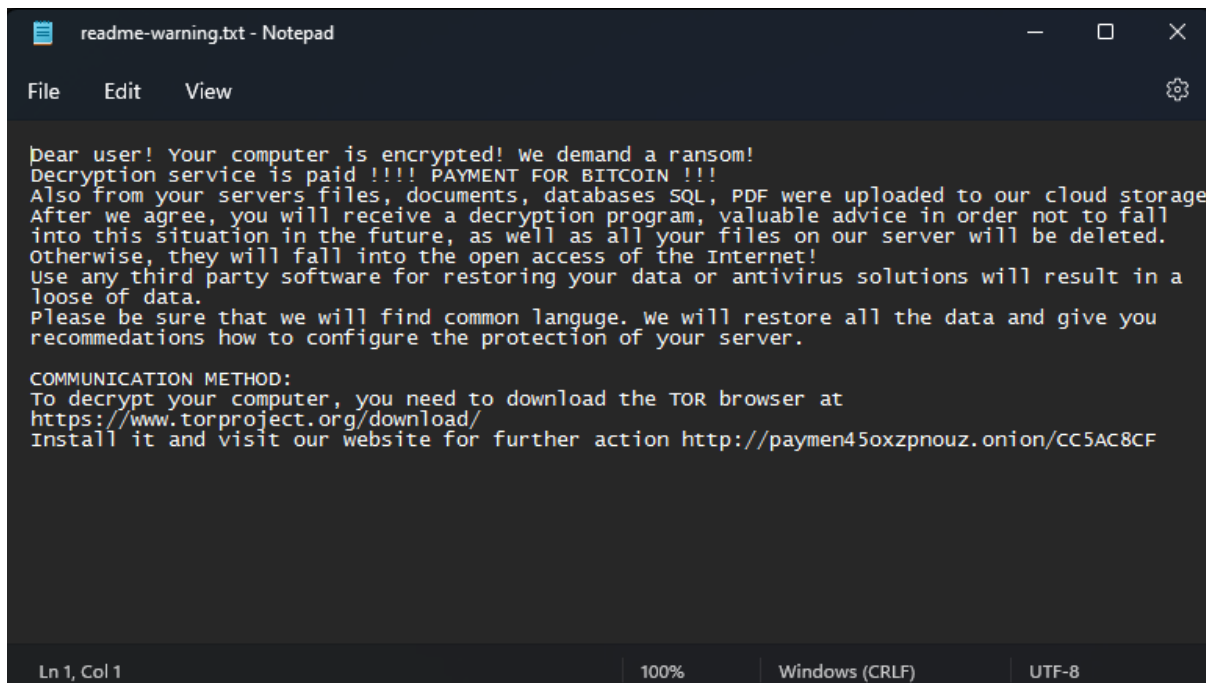
`.makop` ، `.gamigin` ، `.razer` و `.KJHslgkjdfg`

با بررسی دقیق‌تر این باج‌افزار متوجه می‌شویم که فایل‌هایی با پسوندهای `.exe` و `.dll` جزو لیست سفید باج‌افزار هستند و در این فرآیند، رمزگذاری نمی‌شوند. ضمناً دایرکتوری‌های `Windows` یا `Winnt` در درایو سیستم‌عامل (در اینجا C:) دست نخورده باقی می‌مانند.

باج افزار Makop فایل های درون Recycle Bin را نیز رمز می کند و پوشه های درونش را پاک می کند. همچنین میانبرهای برنامه ها روی دسکتاپ یا منوی استارت، پس از اجرای باج افزار حذف می شوند.



در ادامه، فایل پیام باج خواهی این باج افزار با عنوان +README-WARNING+.txt یا readme-warning.txt بر روی Desktop و همینطور در پوشه ای به نام YOUR\_FILES\_ARE\_ENCRYPTED در دایرکتوری هایی که عملیات رمزگذاری صورت گرفته و همچنین در برخی نمونه های باج افزار، بصورت فایلی به اشتراک گذاشته شده در شبکه شده قابل مشاهده است.



(پیغام بالا مربوط به نمونه 4b12f4fdf07d06fb59b5619d01a293c51d32efd183d45a87459b47d5169cfe51 می باشد)

در پیغام باج‌خواهی فوق، پرداخت باج بصورت بیتکوین و بدون ذکر مبلغ درخواست شده و جملاتی برای ترساندن مخاطب مانند "بارگذاری اطلاعات مهم بر روی سرور آن‌ها" و "در صورت همکاری نکردن اطلاعات در اینترنت منتشر می‌شود" استفاده شده است؛ همچنین راه ارتباطی برای تبادل بیان شده است.

```
+README-WARNING+.txt - Notepad
File Edit View
]::: Greetings :::
Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted. The file structure was not damaged, we did everything possible so that this could not happen.
.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay us.
.3.
Q: what about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.
.4.
Q: How to contact with you?
A: You can write us to our mailbox: Nergontr96@cyberfear.com
.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. with this program you will be able to decrypt all your encrypted files.
.6.
Q: If I don't want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause only we have the private key. In practice - time is much more valuable than money.

:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.

Ln 1, Col 1 | 100% | Windows (CRLF) | ANSI
```

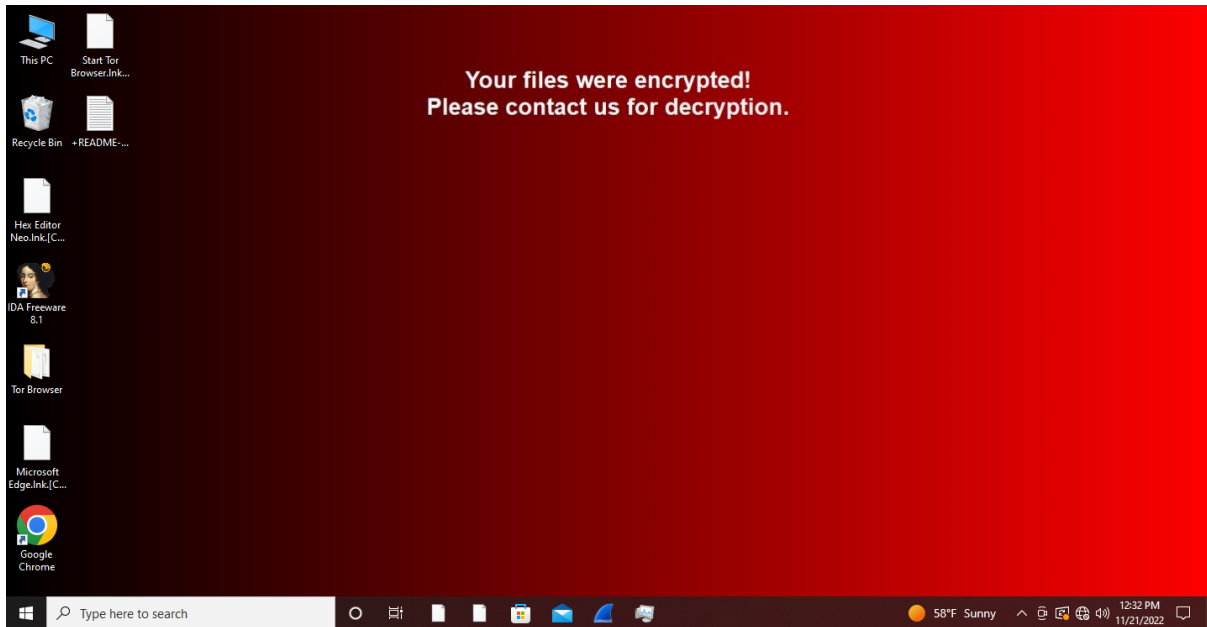
(پیغام بالا مربوط به نمونه d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043 می‌باشد)

اما بر اساس پیغام باج‌خواهی فوق که برای خانواده Makop معمول‌تر است گفته شده که فایل‌ها رمز شده‌اند ولی به ساختار آن‌ها آسیبی نرسیده است و برای بازیابی خواستار پرداخت باج شده است. برای اطمینان هم گفته شده می‌توان دو فایل ساده و کم‌حجم برای مهاجمین فرستاد تا رایگان رمزگشایی کنند. همچنین یک آدرس ایمیل برای برقراری ارتباط با مهاجمین آورده شده است. در ادامه به عباراتی از قبیل اینکه "فایل‌ها برای آن‌ها اهمیتی ندارد"، "اگر سعی در رمزگشایی شود ممکن است خراب شوند" و ... اشاره شده است.

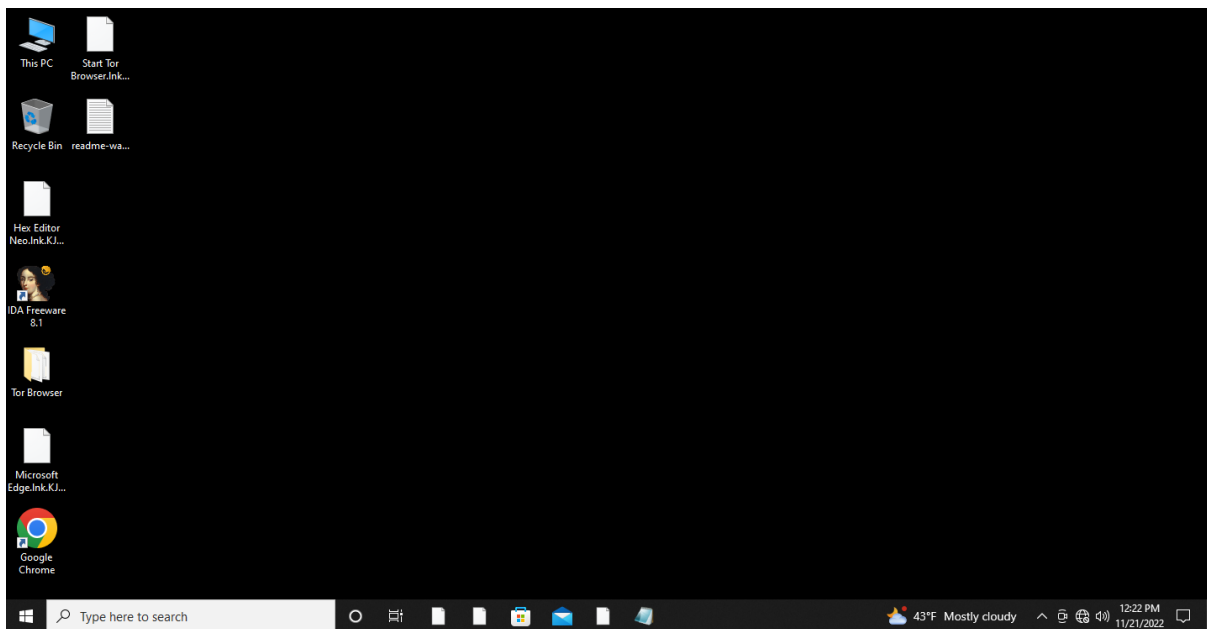


همانطور که در ابتدا اشاره شد، با دو گونه باج افزار Makop با رفتارهای متفاوت مواجه هستیم. هر دو گونه را در محیط آزمایشگاهی اجرا کردیم و نتایج زیر حاصل شد:

گونه اول:



گونه دوم:



فرآیند مربوط به باج افزار Makop پس از انتهای فعالیت خود در سیستم قربانی، متوقف می شود.

۵-۲ روش انتشار:

طبق شواهد موجود و گزارشات بدست آمده، باج افزار Makop معمولاً از طریق ایمیل های فیشینگ به قربانی می رسد و یا بصورت ماکرو در سند های آفیس قرار داده می شود. گزارشاتی نیز مبنی بر انتشار باج افزار از طریق پروتکل دسترسی از راه دور (RDP) به دست رسیده است. هدف این باج افزار بطور کلی سیستم های خانگی و اداری با اطلاعات نسبتاً مهم می باشد.

## ۵-۳ روش مقابله:

هم اکنون خانواده باج افزار Makop توسط اکثر آنتی ویروس های معتبر قابل شناسایی است. توصیه می گردد ضمن بروزرسانی سیستم عامل و نرم افزارها، از نصب و بروزرسانی آنتی ویروس معتبر اطمینان حاصل کنید. در سازمان ها پیشنهاد می گردد علاوه بر موارد فوق، در لایه های مختلف شبکه از مازول آنتی اسپم استفاده گردد و از طریق آموزش کاربران در مواجهه با اسپم ها و ایمیل های فیشینگ، ریسک آلودگی به باج افزار را کاهش دهید. همچنین به عنوان یک اصل، همواره محدودیت های لازم را برای استفاده از سرویس های دسترسی از راه دور رایج از قبیل RDP، Anydesk و ... بکار بگیرید.

## ۶. تحلیل ایستا

بررسی های اولیه بر روی فایل های اجرایی این خانواده باج افزار نشان می دهد که باج افزار Makop بر روی تمامی نسخه های سیستم عامل ویندوز از NT به بعد، اجرا خواهد شد.

|                   |      |                |
|-------------------|------|----------------|
| linker-version    | 80.0 | 80.0           |
| os-version        | 4.0  | Windows NT 4.0 |
| image-version     | 0.0  | 0.0            |
| subsystem-version | 4.0  | 4.0            |

## ۶-۱ تحلیل کد:

کد باج افزارهای خانواده Makop بصورت obfuscate شده می باشد ولی بطور کلی یک رفتار کلی ثابت دارد که به همین دلیل در اینجا تنها بر روی یکی از نمونه بررسی کد را انجام می دهیم.

(نمونه d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043)

```

sub_4014C0 proc near
push    ebx
mov     ebx, [eax+4]
test   ebx, ebx
jz     loc_4015C1

push    ebp
mov     ebp, ds:CryptGenRandom
push    esi
push    edi

loc_4014D5:
mov     eax, php
cmp     dword pt
mov     edi, eax
jnz    short lo_

; Imports from ADVAPI32.dll
;
; Segment type: Externs
; _idata
; BOOL (__stdcall *CryptGenRandom)(HCRYPTPROV hProv, DWORD dwLen, BYTE *pbBuffer)
; extrn CryptGenRandom:dword ; CODE XREF: sub_4014C0+77↑p
; ; sub_4014C0+E6↑p ...

push    0F000000h ; dwFlags
push    18h ; dwProvType
push    0 ; szProvider
push    0 ; szContainer
push    esi ; pHProv
call    ds:CryptAcquireContextW
test   eax, eax
jnz    short loc_402780

mov     [esi], eax
xor    al, al
pop    esi
add    esp, 8
ret    4

; BOOL (__stdcall *CryptAcquireContextH)(HCRYPTPROV *pProv, LPCWSTR szContainer, LPCWSTR szProvider, DWORD dwProvType, DWORD dwFlags)
; extrn CryptAcquireContextH:dword
; ; CODE XREF: sub_4014C0+2D↑p
; ; sub_4014C0+9C↑p ...

; BOOL (__stdcall *CryptSetKeyParam)(HCRYPTKEY hKey, DWORD dwParam, const BYTE *pbData, DWORD dwFlags)
; extrn CryptSetKeyParam:dword
; ; CODE XREF: sub_402AC0+5B↑p
; ; DATA XREF: sub_402AC0+5B↑r

; BOOL (__stdcall *CryptReleaseContext)(HCRYPTPROV hProv, DWORD dwFlags)
; extrn CryptReleaseContext:dword
; ; CODE XREF: sub_4056A0+208↑p
; ; DATA XREF: sub_4056A0+208↑r

; BOOL (__stdcall *CryptImportKey)(HCRYPTPROV hProv, const BYTE *pbData, DWORD dwDataLen, HCRYPTKEY hPubKey, DWORD dwFlags, HCRYPTKEY *pKey)
; extrn CryptImportKey:dword ; CODE XREF: sub_402750+44↑p
; ; sub_402810+10C↑p ...

; BOOL (__stdcall *CryptEncrypt)(HCRYPTKEY hKey, HCRYPTHASH hHash, BOOL Final, DWORD dwFlags, BYTE *pbData, DWORD *pdwDataLen, DWORD dwBufLen)
; extrn CryptEncrypt:dword ; CODE XREF: sub_402750+7F↑p
; ; sub_402B30+13↑p ...

```

تصاویر بالا فرایندهای مربوط به بازخوانی کلید عمومی با الگوریتم رمزنگاری RSA و همچنین ساخت کلیدهای بعدی بر مبنای الگوریتم رمزنگاری متقارن AES256 را در کد باج افزار نشان می دهد.

```

mov     esi, ds:wsprintfW
push   ebp
lea    edx, [esp+48h+var_24]
push   offset aC      ; "\\\\.\\%c:"
push   edx            ; LPWSTR
call   esi ; wsprintfW
push   ebp
lea    eax, [esp+54h+RootPathName]
push   offset aC_0    ; "%c:\\\"
push   eax            ; LPWSTR
call   esi ; wsprintfW
add    esp, 18h
lea    ecx, [esp+44h+RootPathName]
push   ecx            ; lpRootPathName
call   ds:GetDriveTypeW
push   ebx            ; nFileSystemNameSize
push   ebx            ; lpFileSystemNameBuffer
push   ebx            ; lpFileSystemFlags
push   ebx            ; lpMaximumComponentLength
lea    edx, [esp+54h+VolumeSerialNumber]
push   edx            ; lpVolumeSerialNumber
push   ebx            ; nVolumeNameSize
mov    esi, eax
push   ebx            ; lpVolumeNameBuffer
lea    eax, [esp+60h+RootPathName]
push   eax            ; lpRootPathName
call   ds:GetVolumeInformationW
test   eax, eax
jnz    short loc_401362

```

در این بخش از کد باج افزار شروط پسوند فایل و دایرکتوری را برای بررسی لیست سفید و لیست سیاه بررسی می کند.

```

loc_402780:
mov     ecx, [esi+28h]
mov     edx, [esi+24h]
lea    eax, [esp+0Ch+phKey]
push   eax            ; phKey
mov    eax, [esi]
push   0              ; dwFlags
push   0              ; hPubKey
push   ecx            ; dwDataLen
push   edx            ; pbData
push   eax            ; hProv
call   ds:CryptImportKey
test   eax, eax
jnz    short loc_4027AD

```

در اینجا عملیات رمزنگاری فایل ها با import شدن کلید عمومی شروع می شود.

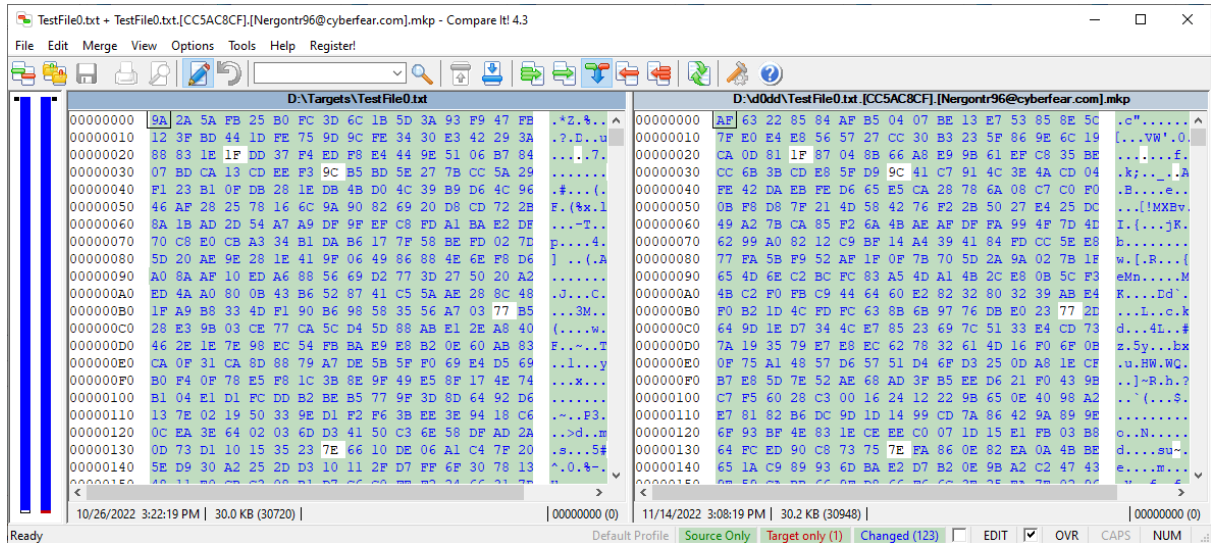


و بدین گونه بخشی از رمزگذاری انجام و کلیدها از حافظه پاک می شوند.

```

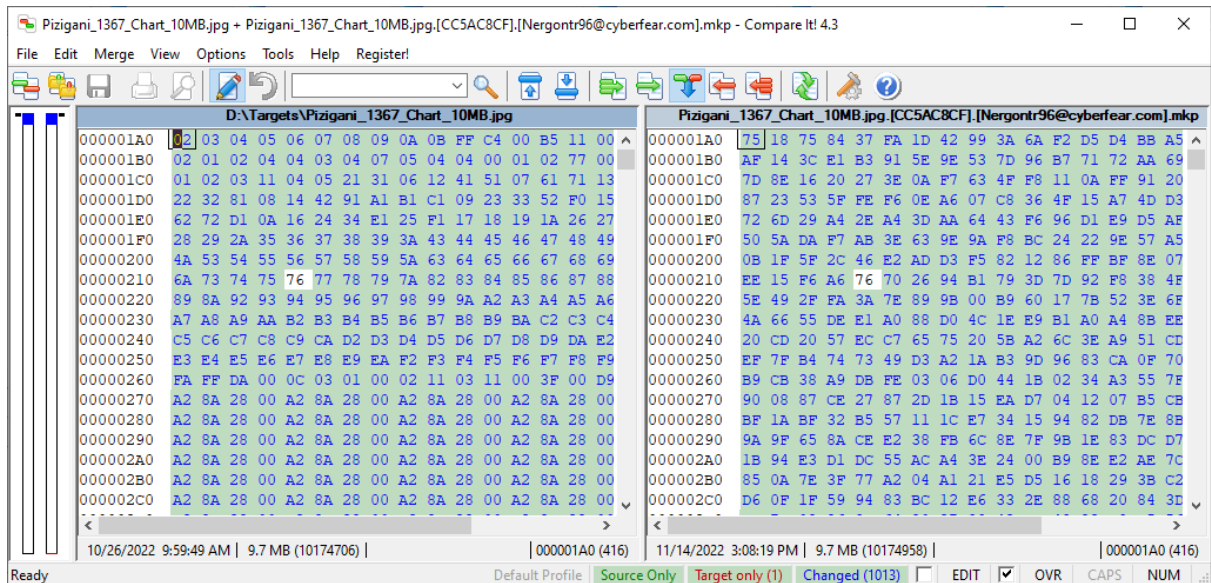
LABEL_9:
wsprintf(PathName, L"%s\\%s", a2, a5);
DirectoryW = CreateDirectoryW(PathName, 0);
if ( DirectoryW )
{
a2 = PathName;
LABEL_11:
LOBYTE(DirectoryW) = sub_4075F0(a3, (int)a2, a1, a4);
}
return DirectoryW;
    
```

پس از بررسی چند نمونه فایل سالم با نمونه رمز شده آن‌ها در خانواده باج‌افزار Makop مشخص گردید که باج‌افزار همیشه دو کلید جدید تولید می‌کند که بردار مقدار اولیه آن در انتهای فایل اضافه می‌شود؛ همچنین فایل‌های با حجم زیر 1.5MB را بطور کامل رمزگذاری می‌کند.

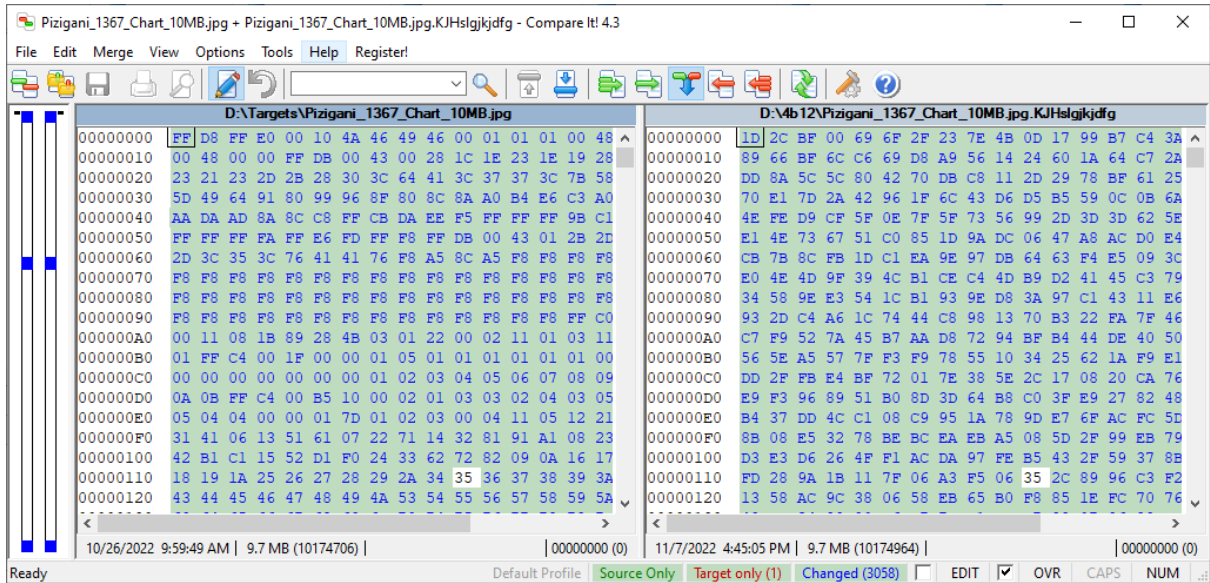


این باج افزار برای فایل های با حجم بیشتر از 1.5MB دو رفتار متفاوت نشان می دهد.

در برخی گونه ها تنها ابتدای هر فایل را به اندازه 256KB رمز می کند و در انتهای فایل نیز بین ۲۵۲ تا ۳۳۲ بایت به انتهای هر فایل رمز شده اضافه می نماید:



و در برخی دیگر سه بخش از فایل به مکان های ابتدا، یک سوم بعد از ابتدای فایل و انتهای فایل را رمز گذاری می کند و در انتهای فایل نیز بین ۲۴۴ تا ۳۴۰ بایت به انتهای هر فایل رمز شده اضافه می نماید:



## ۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ضبط شده حین اجرای باج افزار و همچنین بررسی نتایج سندباکس های آنلاین، هیچ گونه ارتباط شبکه ای مرتبط با باج افزار مشاهده نشد و نتایج نشان داد که باج افزار Makop کاملاً آفلاین فعالیت می کند.

## ۶-۳ رمزنگاری و رمزگشایی:

خانواده باج افزار Makop با الگوریتم رمزنگاری متقارن AES256 فایل ها را رمزگذاری می کند. بدین گونه که باج افزار از یک کلید با طول ۲۵۶ بیت برای رمزگشایی کلید عمومی RSA استفاده می کند، در ادامه دو کلید جدید با استفاده از الگوریتم AES256 می سازد که با استفاده از آن ها اطلاعات فایل ها رمز می شوند، که برای هر کلید یک بردار مقدار اولیه جدید (IV) ۱۶ بیتی نیز ساخته و در انتهای فایل ذخیره می شود. در انتها نیز هر دو کلید AES که برای رمزگذاری استفاده می شوند توسط کلید عمومی RSA رمزگذاری می شوند. در نهایت باتوجه به رمزگذاری صورت گرفته توسط این خانواده در حال حاضر هیچ گونه ابزاری جهت رمزگشایی فایل های رمز شده توسط این باج افزار، ارایه نشده است.

## ۷. شناسه‌های تهدید (IOCs)

نمونه‌ها (Samples):

```
4b12f4fdf07d06fb59b5619d01a293c51d32efd183d45a87459b47d5169cfe51
3b15b66bf6a7d7ebab6437906686037f23a797d15e0fbff3d6741d3f58db8f1e
fe52d906fa596e7ae16633074ff7178b3ac40e26a93f0009f1b33d5cbf219e91
a6566bc4c76a36a0e880d2151e0a86a59c3af57082b7c83a669dba3f28afb959
7b367f4c26ea8c16697cd8b2d41e568a1fa3a6a7909475b7e0850dc38f374dce
50b0c7858bc2bb2d1fa3d441bd2c4e3930b88b77c6cef11a51af5705727d6639
```

## ۸. شناسایی (Detection)

با توجه به اینکه باج‌افزار Makop بلافاصله پس از اجرا، فضای VSS را حذف می‌کند، با استفاده از رول زیر در اسپلانک می‌توان گسترش باج‌افزار در شبکه را شناسایی کرد:

```
((EventCode="4688" OR EventCode="1") (CommandLine="*vssadmin* *delete* *shadows*"
OR CommandLine="*wmic* *shadowcopy* *delete*" OR CommandLine="*vssadmin* *resize*
*shadowstorage*")) OR (EventCode="5857" ProviderName="MSVSS__PROVIDER") OR
(EventCode="5858" Operation="*Win32_ShadowCopy*")
```

| host            | ParentImage                 | Image                              | CommandLine                         |
|-----------------|-----------------------------|------------------------------------|-------------------------------------|
| DESKTOP-01V6302 | C:\Windows\System32\cmd.exe | C:\Windows\System32\wbem\WMIIC.exe | wmic shadowcopy delete              |
| DESKTOP-01V6302 | C:\Windows\System32\cmd.exe | C:\Windows\System32\vssadmin.exe   | vssadmin delete shadows /all /quiet |