باسمه تعالی

# تحلیل فنی باج‌افزار

# Ouroboros

# فهرست مطالب

## ۱. مقدمه :

براساس اخبار منتشر شده، باج‌افزار Ouroboros از اواخر آوریل ۲۰۱۹ میلادی مشاهده شده است. این باج‌افزار که نسل بعدی باج‌افزار Zeropadypt به شمار می‌آید، به سبب پسوندهایی که به انتهای فایل‌های رمزگذاری شده اضافه می‌کند، به نام‌های Limbo و Lazarus نیز شناخته می‌شود. باج‌افزار Ouroboros از الگوریتم AES جهت رمزگذاری فایل‌های موردنظر خود در سیستم قربانی استفاده می‌کند. نسخه تحلیل شده در این گزارش در تاریخ ۱۸ اوت سال جاری میلادی مشاهده گردیده است.

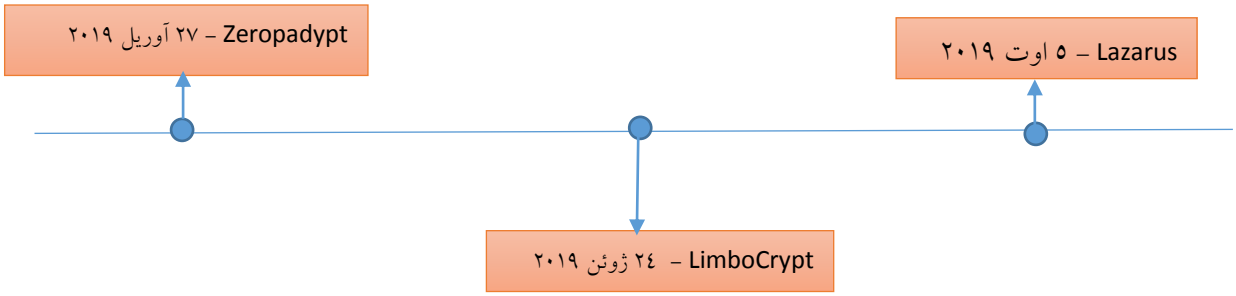
## ۲. مشخصات فایل اجرایی :

| | |
|---|---|
| نام فایل | unlockme123@protonmail.com.exe |
| MD5 | 87283fcc4ac3fce09faccb75e945364c |
| SHA-1 | a0f8ede92af5dd01e6f6fa2c2ef81101196fdbfd |
| SHA-256 | 449271217c8f5d5561f801cfc76d4304c1355fb1025bd1da5cf2705b0840be0f |
| نوع فایل | Win32 EXE |
| اندازه فایل | ٥٤٨.٥ کیلوبایت |

فایل اجرایی این باج‌افزار دارای ۵ بخش است :

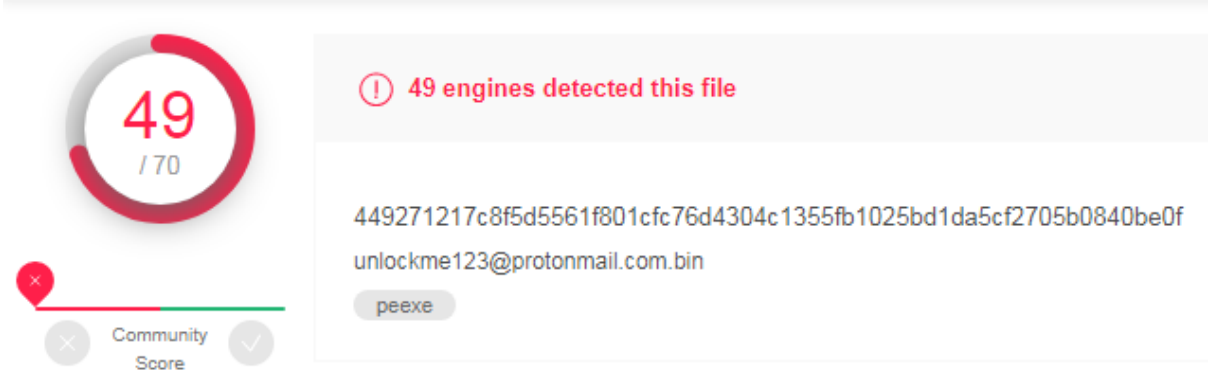
| نام بخش | آنتروپی | آدرس مجازی | اندازه مجازی | اندازه خام |
|---|---|---|---|---|
| .text | ٦.٦٥ | ٤٠٩٦ | ٤١٧٠٦٦ | ٤١٧٢٨٠ |
| .rdata | ٥.٢٧ | ٤٢١٨٨٨ | ١٠٩٤٥٠ | ١٠٩٥٦٨ |
| .data | ٤.٥٥ | ٥٣٢٤٨٠ | ٢٠٠٧٢ | ١٠٧٥٢ |
| .rsrc | ٤.٧٢ | ٥٥٢٩٦٠ | ٤٨٠ | ٥١٢ |
| .reloc | ٦.٥٨ | ٥٥٧٠٥٦ | ٢٢٣٦٤ | ٢٢٥٢٨ |

## ۳. شجره‌نامه




## ٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ٤۹ مورد از ۷۰ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



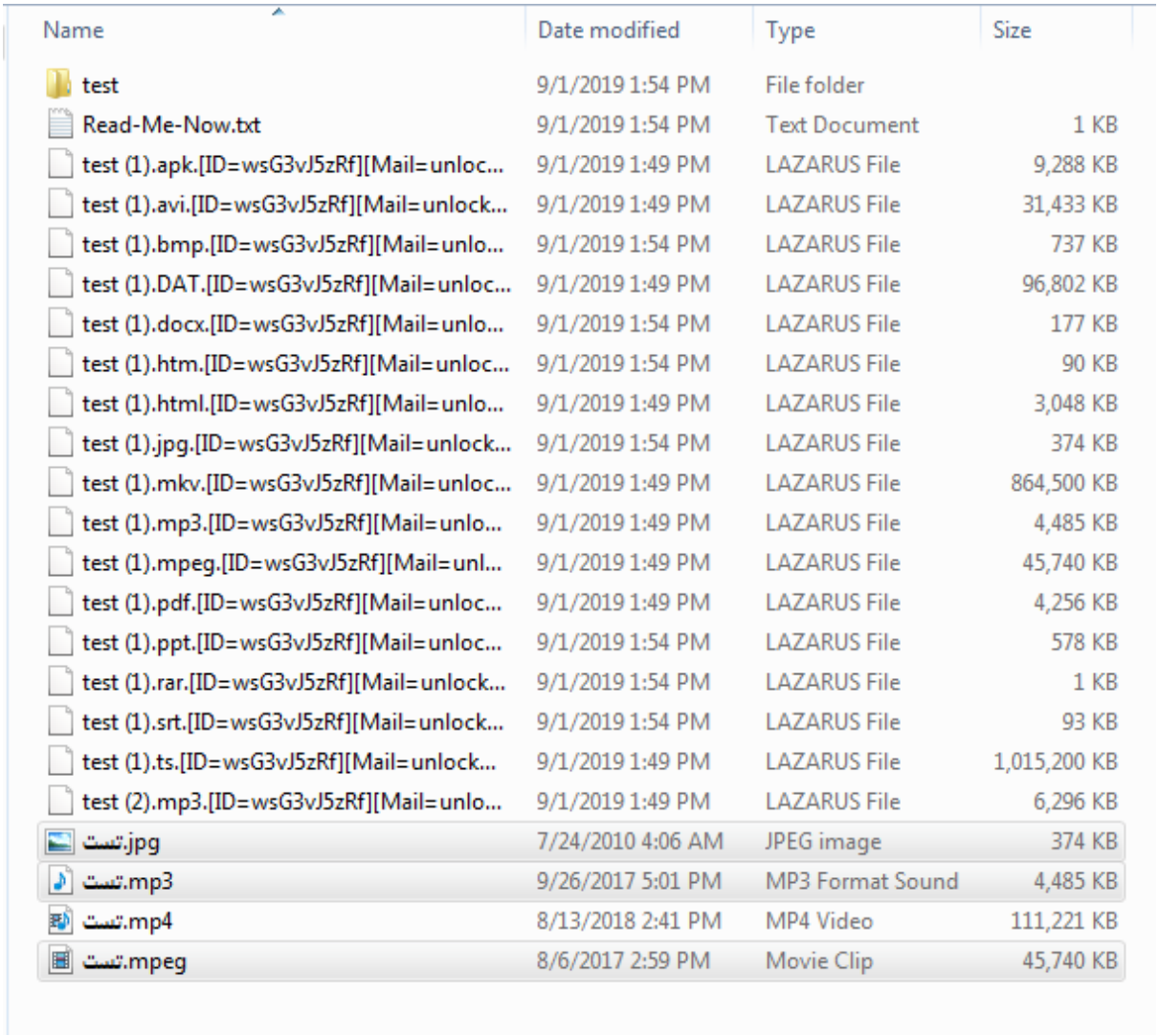

## ۵. تحلیل پویا

### ۵-۱ آناتومی حمله:

باج‌افزار Ouroboros در ابتدای شروع فعالیت خود در سیستم قربانی، توسط دستور زیر اقدام به حذف فضای VSS می‌کند.

| | |
|---|---|
| حذف فضای VSS | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" " vssadmin delete shadows /all /y |

سپس شروع به جست و جو و رمزگذاری فایل‌های مورد نظر خود در سیستم قربانی می‌کند. فایل‌های سیستم قربانی پس از رمزگذاری، به شکل زیر تغییر پیدا می‌کنند.



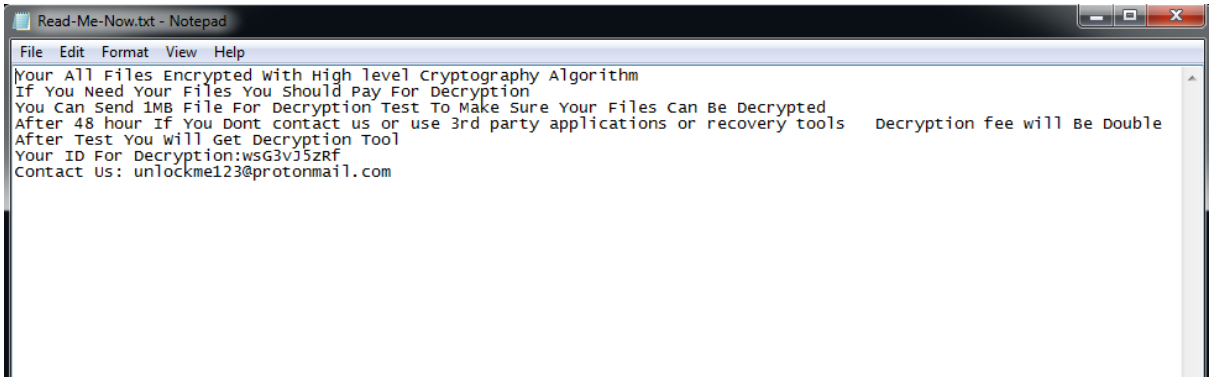
| Name | Date modified | Type | Size |
|---|---|---|---|
| test | 9/1/2019 1:54 PM | File folder | |
| Read-Me-Now.txt | 9/1/2019 1:54 PM | Text Document | 1 KB |
| test (1).apk.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:49 PM | LAZARUS File | 9,288 KB |
| test (1).avi.[ID=wsG3vJ5zRf][Mail=unlock... | 9/1/2019 1:49 PM | LAZARUS File | 31,433 KB |
| test (1).bmp.[ID=wsG3vJ5zRf][Mail=unlo... | 9/1/2019 1:54 PM | LAZARUS File | 737 KB |
| test (1).DAT.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:49 PM | LAZARUS File | 96,802 KB |
| test (1).docx.[ID=wsG3vJ5zRf][Mail=unlo... | 9/1/2019 1:54 PM | LAZARUS File | 177 KB |
| test (1).htm.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:54 PM | LAZARUS File | 90 KB |
| test (1).html.[ID=wsG3vJ5zRf][Mail=unlo... | 9/1/2019 1:49 PM | LAZARUS File | 3,048 KB |
| test (1).jpg.[ID=wsG3vJ5zRf][Mail=unlock... | 9/1/2019 1:54 PM | LAZARUS File | 374 KB |
| test (1).mkv.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:49 PM | LAZARUS File | 864,500 KB |
| test (1).mp3.[ID=wsG3vJ5zRf][Mail=unlo... | 9/1/2019 1:49 PM | LAZARUS File | 4,485 KB |
| test (1).mpeg.[ID=wsG3vJ5zRf][Mail=unl... | 9/1/2019 1:49 PM | LAZARUS File | 45,740 KB |
| test (1).pdf.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:49 PM | LAZARUS File | 4,256 KB |
| test (1).ppt.[ID=wsG3vJ5zRf][Mail=unloc... | 9/1/2019 1:54 PM | LAZARUS File | 578 KB |
| test (1).rar.[ID=wsG3vJ5zRf][Mail=unlock... | 9/1/2019 1:54 PM | LAZARUS File | 1 KB |
| test (1).srt.[ID=wsG3vJ5zRf][Mail=unlock... | 9/1/2019 1:54 PM | LAZARUS File | 93 KB |
| test (1).ts.[ID=wsG3vJ5zRf][Mail=unlock... | 9/1/2019 1:49 PM | LAZARUS File | 1,015,200 KB |
| test (2).mp3.[ID=wsG3vJ5zRf][Mail=unlo... | 9/1/2019 1:49 PM | LAZARUS File | 6,296 KB |
| تست.jpg | 7/24/2010 4:06 AM | JPEG image | 374 KB |
| تست.mp3 | 9/26/2017 5:01 PM | MP3 Format Sound | 4,485 KB |
| تست.mp4 | 8/13/2018 2:41 PM | MP4 Video | 111,221 KB |
| تست.mpeg | 8/6/2017 2:59 PM | Movie Clip | 45,740 KB |

همانطور که در تصویر بالا قابل مشاهده است باج‌افزار Ouroboros از الگوی زیر برای تغییر نام فایل‌های رمزگذاری شده استفاده می‌کند.

[ID=**********][Mail=unlockme123@protonmail.com].Lazarus

طبق آزمایشات صورت گرفته، فایل‌های با اسامی فارسی از رمزگذاری توسط باج‌افزار در امان می‌مانند. با بررسی‌هایی که بر روی مسیرهای مختلف در سیستم‌عامل انجام دادیم، متوجه شدیم باج‌افزار قدرتمند Ouroboros تمامی انواع فایل‌ها حتی فایل‌های اجرایی را نیز رمزگذاری می‌کند. این موضوع سبب می‌شود که نرم‌افزارهای نصب شده در سیستم‌عامل، پس از حمله باج‌افزار قابل اجرا نباشند. فایل پیغام باج‌خواهی با نام Read-Me-Now.txt نیز، درون هر پوشه حاوی فایل‌های رمزشده، قرار می‌گیرد.

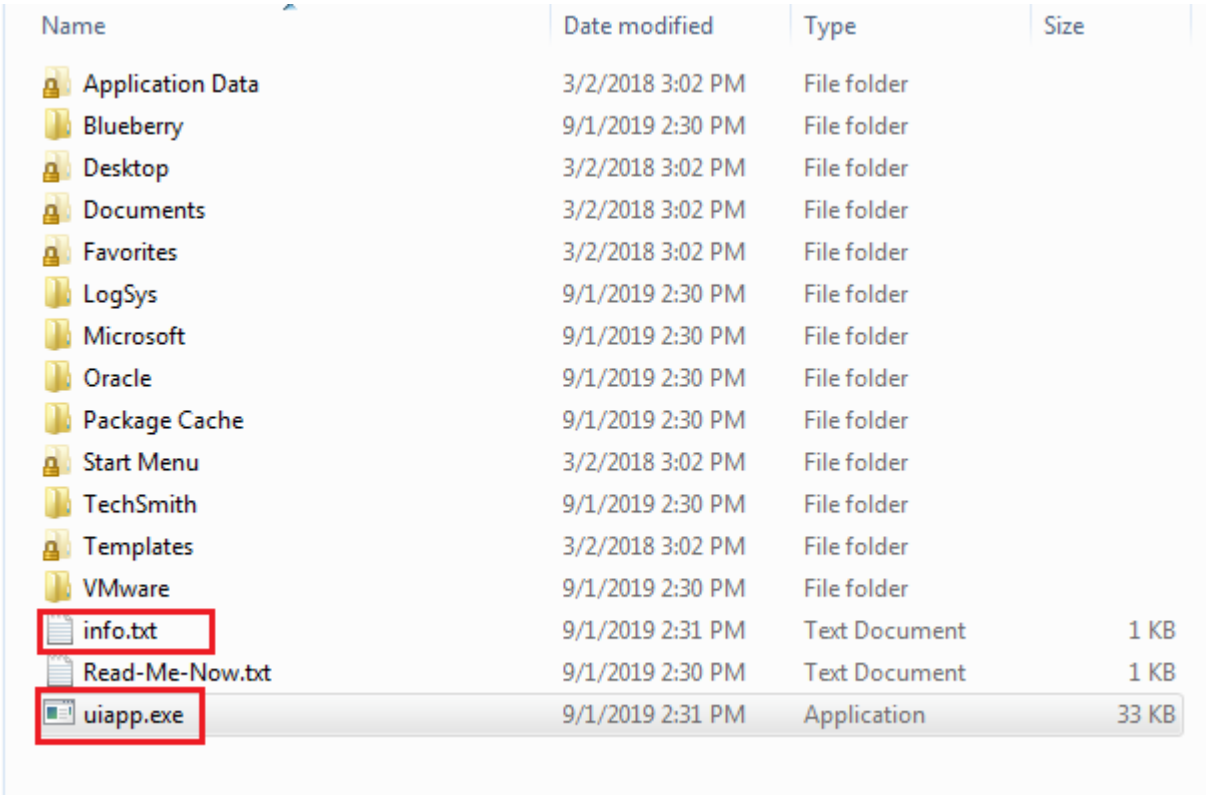
تصویر زیر پیغام باج‌خواهی این باج‌افزار را نشان می‌دهد.



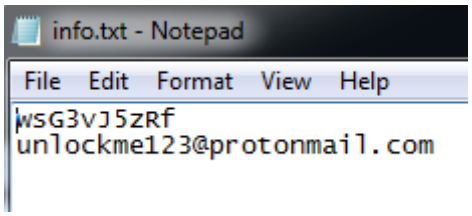

همانطور که در پیغام باج‌خواهی این باج‌افزار مشخص شده است قربانی می‌تواند فایلی با حجم حداکثر یک مگابایت را برای مهاجمین ارسال کند تا به صورت رایگان رمزگشایی شود. مهاجمین این کار را جهت جلب اعتماد قربانی انجام می‌دهند. در ادامه عنوان شده است که در صورت عدم ارتباط با مهاجمین و پرداخت باج در مدت زمان ۴۸ساعت و همچنین استفاده از ابزار دیگر جهت رمزگشایی فایل‌ها، مبلغ باج دوبرابر خواهد شد. قربانی برای ارتباط با مهاجمین، باید شناسه خود را به ایمیل قرارداده شده در انتهای پیغام باج‌خواهی ارسال کند.

باج‌افزار Ouroboros پس از اتمام کار خود در سیستم قربانی متوقف می‌شود. همزمان، پنجره‌ی پیغام باج‌خواهی با اجرای برنامه‌ای با عنوان uiapp.exe نیز بر روی صفحه نمایش قربانی ظاهر می‌شود.

با بررسی مسیر قرارگیری این فایل اجرایی متوجه ایجاد فایل دیگری با عنوان info.txt توسط باج‌افزار شدیم.




هر دوی این فایلها در مسیر C:\ProgramData درون سیستم قربانی قرار می‌گیرند. محتوای فایل info.txt حاوی شناسه قربانی و ایمیل مهاجم است.




تغییرات رجیستری ایجاد شده توسط باج‌افزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر می‌باشد:

مقادیر اضافه شده:

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-304: "Public Recorded TV"

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-312: "Sample Media"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HO-PREG\Qrfxgbc\haybpxzr123@cebgbaznvy.pbz.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 7D 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 30 C7 B0 0B A6 60 D5 01 00 00 00 00

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\UB-CERT\Desktop\unlockme123@protonmail.com.exe: "unlockme123@protonmail.com.exe"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\UB-CERT\Desktop\unlockme123@protonmail.com.exe: "unlockme123@protonmail.com.exe"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-304: "Public Recorded TV"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-312: "Sample Media"

کلیدهایی که مقادیر آن‌ها تغییر پیدا کرده است:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter

HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff02

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKLM\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff02

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx

### ۵-۲ روش انتشار:

روش انتشار خاصی برای این باج‌افزار در منابع معتبر گزارش نشده است. لذا ممکن است از طریق هر یک از روش‌های معمول و رایج همچون ایمیل‌های مخرب که در قالب اسپم دریافت می‌شوند، فعال‌سازهای جعلی مجموعه آفیس مایکروسافت، وب‌سایت‌های هک شده، شکستن رمزعبور RDP و ... که اکثر باج‌افزارها از آن‌ها برای نفوذ و انتشار در سیستم قربانیان بهره می‌برند، منتشر گردد.

### ۵-۳ روش جلوگیری:

از آنجا که تاکنون روش مشخصی برای نفوذ این باج‌افزار منتشر نشده است، در گام اول، به‌روزرسانی سیستم‌عامل و نرم‌افزارهای امنیتی نصب شده بر روی آن همچون آنتی‌ویروس، می‌تواند بسیار مفید باشد. در گام بعد، اگر به صورت فعال از پروتکل RDP استفاده می‌کنید حتماً باید اقدامات مربوط به امن‌سازی این پروتکل همچون تنظیم رمزعبور پیچیده، تنظیم احراز هویت دوعاملی و ... را انجام دهید و در گام آخر، توجه بیشتر در بازدید از وبسایت‌ها، عدم استفاده از کرک‌های جعلی جهت به شکستن قفل نرم‌افزارها و بازنکردن پیوست ایمیل‌های دریافتی ناشناس و مشکوک، می‌تواند در جلوگیری از نفوذ این باج‌افزار، بسیار مؤثر باشد.

## ۶. تحلیل ایستا

### ۶-۱ تحلیل کد:

پس از تحلیل کد باج‌افزار، نتایج زیر حاصل گردید. نتایج بررسی اولیه فایل باج‌افزار نشان می‌دهد باج‌افزار Ouroboros بر روی نسخه سیستم‌عامل ویستا به بعد اجرا می‌شود.

| | |
|---|---|
| size-of-heap-commit | 4096 (bytes) |
| section-alignment | 0x00001000 (4096 bytes) |
| file-alignment | 0x00000200 (512 bytes) |
| os-version | 6.0 |
| image-version | 0.0 |

باج‌افزار در همان ابتدای شروع فعالیت خود، فضای VSS سیستم‌عامل را پاک می‌کند تا بازگردانی فایل‌ها را برای قربانی مشکل‌تر کند.

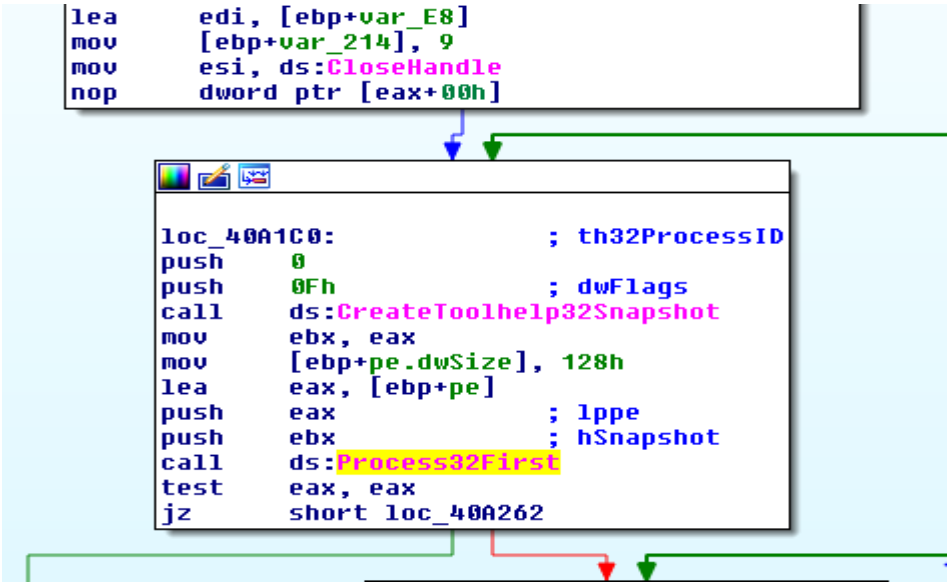
```
push    offset Parameters ; "vssadmin delete shadows /all /y"
push    offset File       ; "powershell.exe"
push    offset Operation  ; "runas"
push    0                 ; hwnd
call    ds:ShellExecuteA
```

سپس فرآیندهای زیر را متوقف می‌کند.

```
aSqlserver_exe  db 'sqlserver.exe',0
                align 4
aMsftesql_exe   db 'msftesql.exe',0
                align 4
aSqlagent_exe   db 'sqlagent.exe',0
                align 4
aSqlbrowser_exe db 'sqlbrowser.exe',0
                align 4
aSqlwriter_exe  db 'sqlwriter.exe',0
                align 4
aMysqld_exe     db 'mysqld.exe',0
                align 4
aMysqldNt_exe   db 'mysqld-nt.exe',0
                align 4
aMysqldOpt_exe  db 'mysqld-opt.exe',0
                align 4
```

همانطور که قابل مشاهده است فرآیندهای بالا مربوط به پایگاه‌های داده هستند. فایل‌های پایگاه داده از اهداف اصلی باج‌افزارها هستند و باج‌افزار Ouroboros نیز، تمامی فرآیندهای مربوط به پایگاه‌های داده را در صورت فعال بودن در سیستم قربانی متوقف می‌کند تا ضمن جلوگیری از به‌روزرسانی فایل‌های خروجی پایگاه داده، مشکلی در رمزگذاری این فایل‌ها که معمولا با پسوندهای mdf. و sql. در سیستم قربانی ذخیره می‌شوند، نداشته باشد.

فرآیندهای مذکور، طی پروسه‌ای با کمک توابع زیر متوقف می‌شوند.




همانطور که در بخش قبلی اشاره شد، این باج‌افزار فایل‌های زیر را در سیستم قربانی ایجاد می‌کند.

```
aCProgramdataIn db 'C:\ProgramData\info.txt',0 ; DATA XREF: sub_40A2B0+469↑o
aCProgramdataUi:                               ; DATA XREF: sub_40A2B0+534↑o
                unicode 0, <C:\ProgramData\uiapp.exe>,0
                align 10h
asc_478990:                                    ; DATA XREF: sub_40DC80+83↑o
                                               ; .text:0041A94A↑o ...
```

فایل info.txt حاوی شناسه قربانی و ایمیل مهاجم جهت برقراری ارتباط است و فایل uiapp.exe پس از اجرا، پنجره‌ی پیغام باج‌خواهی را بر روی صفحه نمایش سیستم قربانی قرار می‌دهد. این فایل، شناسه قربانی و ایمیل قرارداده شده را از فایل info.txt می‌خواند.

```
19          public MainWindow()
20          {
21              this.InitializeComponent();
22              Thread.Sleep(1000);
23              try
24              {
25                  IEnumerable<string> enumerable = File.ReadLines("C:\\ProgramData\\info.txt");
26                  int num = 0;
27                  foreach (string text in enumerable)
28                  {
29                      if (num == 0)
30                      {
31                          this.lblid.Content = text.ToString();
32                      }
33                      if (num == 1)
34                      {
35                          this.lblmail.Content = text.ToString();
36                          num++;
37                      }
38                      num++;
39                  }
40              }
41              catch
42              {
43                  this.lblmail.Content = "You Can See Our Email in Read-Me-Now.txt";
44                  this.lblid.Content = "You Can See Your id in Read-Me-Now.txt files";
45              }
```

در صورتی که به هر دلیلی فایل info.txt در سیستم قربانی ایجاد نشود، محتوای مشخص شده درون کادر آبی رنگ به جای شناسه قربانی و ایمیل درون پنجره باج‌خواهی قرار می‌گیرد. این باج‌افزار تمام اطلاعات مربوط به ارایه دهنده سرویس اینترنت به قربانی را نیز، دریافت می‌کند.

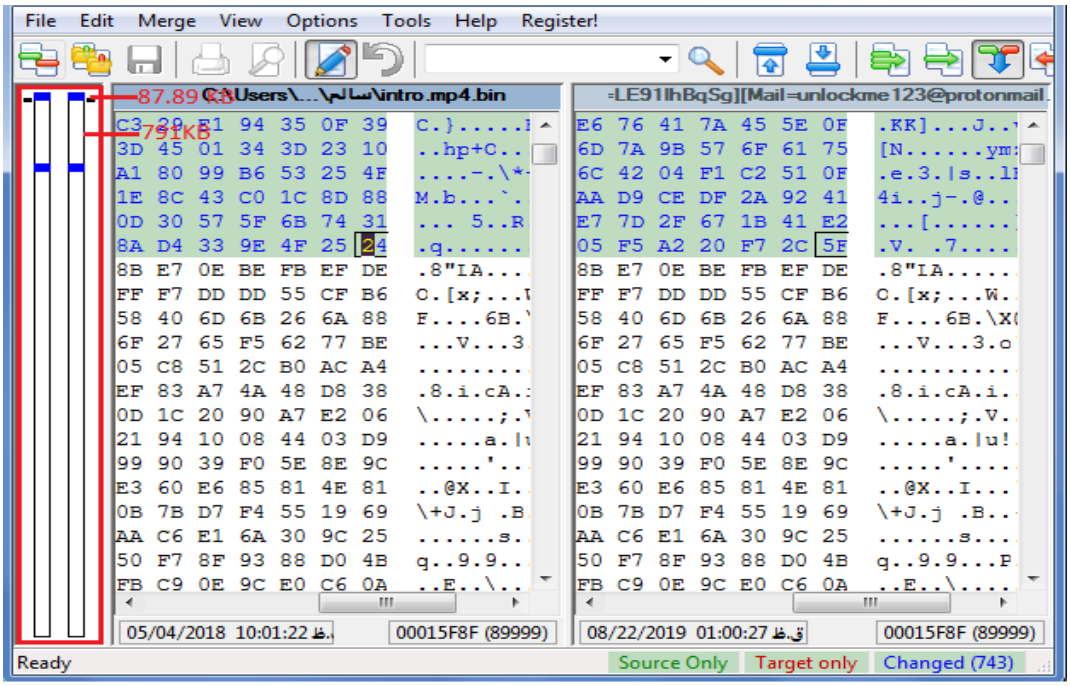
```
push    offset aIpProvider_php ; "/ip-provider.php"
lea     ecx, [ebp+var_B0]
mov     byte ptr [ebp+var_4], 3
mov     [ebp+var_A0], 0
mov     [ebp+var_9C], 0Fh
mov     byte ptr [ebp+var_B0], 0
call    sub_40F420
lea     eax, [ebp+var_C8]
mov     byte ptr [ebp+var_4], 4
```

این اطلاعات شامل دریافت نام کشور، نام شرکت ارایه دهنده سرویس اینترنت، آدرس و مواردی دیگر از این قبیل می‌باشد. الگوریتم استفاده شده در فرآیند رمزگذاری فایل‌ها الگوریتم متقارن AES در حالت CBC است.

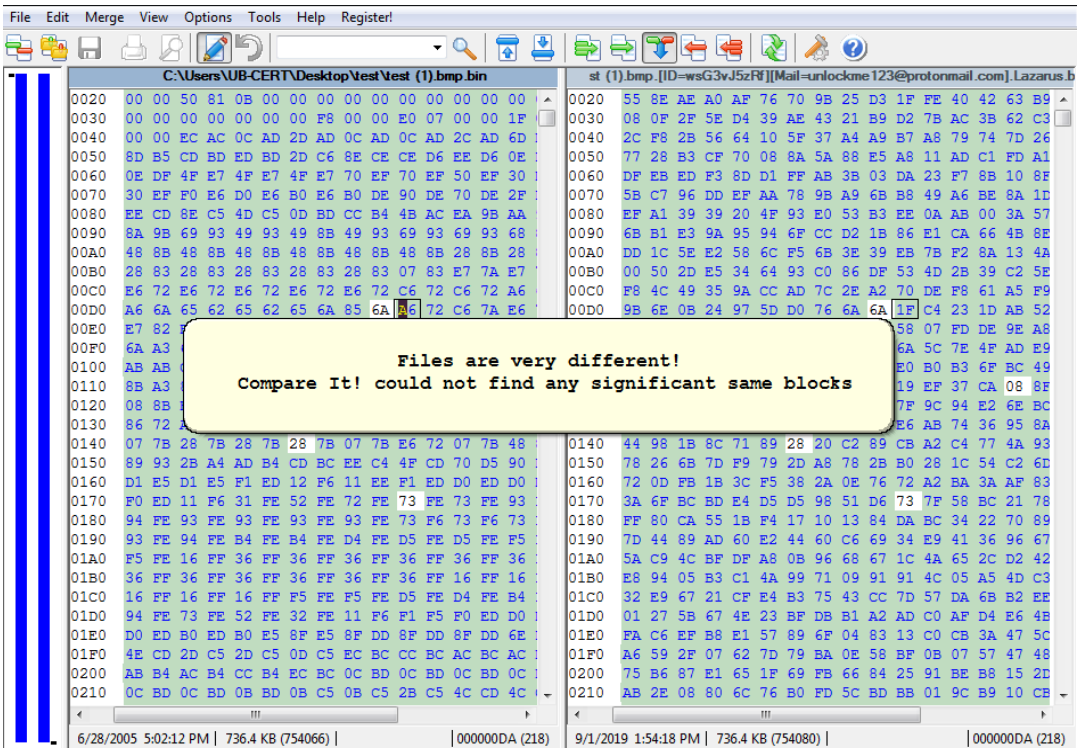
```
push    offset aCbc     ; "CBC"
cmp     eax, 3
jb      short loc_40DD87
cmp     edx, 10h
lea     esi, [ebp+var_28]
lea     eax, [ecx+3]
cmovnb  esi, dword ptr [ebp+var_28]
add     esi, ecx
mov     dword ptr [ebp+var_18], eax
push    esi
call    sub_43D190
```

```
push    offset aAes     ; "AES"
mov     [ebp+var_4], esi
mov     dword ptr [esi+10h], 0
mov     dword ptr [esi+14h], 0Fh
mov     byte ptr [esi], 0
call    sub_40F420
mov     eax, esi
pop     esi
mov     esp, ebp
pop     ebp
retn    4
endp
```

پس از بررسی چند نمونه فایل سالم و رمزشده متوجه شدیم که الگوی رمزگذاری باج‌افزار به این شکل است که حدود ۸۸ کیلوبایت از ابتدای هر فایل رمزگذاری می‌شود، سپس ۷۹۱ کیلوبایت بعدی فایل سالم باقی می‌ماند. مجدداً ۸۸ کیلوبایت از فایل رمزگذاری شده و بقیه محتوای فایل بدون تغییر باقی می‌ماند.




رفتار باج‌افزار در مورد فایل‌های با حجم کمتر از ۱کیلوبایت متفاوت است و تمامی محتوای فایل رمزگذاری می‌شود.



### ۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ایجادشده حین اجرای باج‌افزار، موارد زیر مشاهده گردید.

| کشور | پروتکل | شماره پورت | آدرس آی‌پی |
|---|---|---|---|
| آلمان | http,TCP | ۸۰ | ۱۴۸.۲۵۱.۲۴۷.۱۷۴ |
| فرانسه | TCP | ۸۰۸۰ | ۱۷۶.۳۱.۶۸.۳۰ |

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 85 | 57.793288 | PcsCompu_0a:7d:76 | RealtekU_12:35:02 | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.15 |
| 86 | 57.793449 | RealtekU_12:35:02 | PcsCompu_0a:7d:76 | ARP | 60 | 10.0.2.2 is at 52:54:00:12:35:02 |
| 87 | 64.809059 | 10.0.2.15 | 176.31.68.30 | TCP | 54 | 49193 → 8080 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 88 | 65.798464 | fe80::1818:f6ad:dfa… | ff02::1:2 | DHCPv6 | 151 | Solicit XID: 0x29b4aa CID: 0001000124ce7eb40800270a7d76 |
| 89 | 177.546780 | PcsCompu_0a:7d:76 | Broadcast | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.15 |
| 90 | 177.546945 | RealtekU_12:35:02 | PcsCompu_0a:7d:76 | ARP | 60 | 10.0.2.2 is at 52:54:00:12:35:02 |
| 91 | 177.546953 | 10.0.2.15 | 148.251.247.174 | TCP | 66 | 49195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 92 | 177.768582 | 148.251.247.174 | 10.0.2.15 | TCP | 60 | 80 → 49195 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 93 | 177.768646 | 10.0.2.15 | 148.251.247.174 | TCP | 54 | 49195 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 94 | 177.768931 | 10.0.2.15 | 148.251.247.174 | HTTP | 188 | GET /ip-provider.php HTTP/1.0 |
| 95 | 177.769321 | 148.251.247.174 | 10.0.2.15 | TCP | 60 | 80 → 49195 [ACK] Seq=1 Ack=135 Win=65535 Len=0 |
| 96 | 177.973618 | 148.251.247.174 | 10.0.2.15 | TCP | 269 | 80 → 49195 [PSH, ACK] Seq=1 Ack=135 Win=65535 Len=215 [TCP segment of a reassembled PDU] |
| 97 | 177.973619 | 148.251.247.174 | 10.0.2.15 | HTTP | 60 | HTTP/1.1 200 OK (text/html) |
| 98 | 177.973653 | 10.0.2.15 | 148.251.247.174 | TCP | 54 | 49195 → 80 [ACK] Seq=135 Ack=217 Win=64025 Len=0 |
| 99 | 177.973813 | 10.0.2.15 | 148.251.247.174 | TCP | 54 | 49195 → 80 [FIN, ACK] Seq=135 Ack=217 Win=64025 Len=0 |
| 100 | 177.973947 | 148.251.247.174 | 10.0.2.15 | TCP | 60 | 80 → 49195 [ACK] Seq=217 Ack=136 Win=65535 Len=0 |
| 101 | 177.974102 | 10.0.2.15 | 176.31.68.30 | TCP | 66 | 49196 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 102 | 178.178810 | 176.31.68.30 | 10.0.2.15 | TCP | 60 | 8080 → 49196 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 103 | 178.178850 | 10.0.2.15 | 176.31.68.30 | TCP | 54 | 49196 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 104 | 178.178973 | 10.0.2.15 | 176.31.68.30 | TCP | 168 | 49196 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=114 [TCP segment of a reassembled PDU] |
| 105 | 178.179177 | 176.31.68.30 | 10.0.2.15 | TCP | 60 | 8080 → 49196 [ACK] Seq=1 Ack=115 Win=65535 Len=0 |
| 106 | 178.383771 | 176.31.68.30 | 10.0.2.15 | TCP | 61 | 8080 → 49196 [PSH, ACK] Seq=1 Ack=115 Win=65535 Len=7 [TCP segment of a reassembled PDU] |
| 107 | 178.383958 | 10.0.2.15 | 176.31.68.30 | TCP | 54 | 49196 → 8080 [FIN, ACK] Seq=115 Ack=8 Win=64233 Len=0 |

بررسی محتوای بسته‌های جابه‌جا شده توسط آی‌پی‌های مربوط به باج‌افزار موارد دیگری را نمایان کرد. همانطور که در بخش قبل اشاره شد، این باج‌افزار اطلاعاتی از جمله نام ارایه دهنده سرویس اینترنت به قربانی و موقعیت جغرافیایی وی را دریافت می‌کند. ضمناً شناسه قربانی و ایمیل مهاجم نیز، از طریق آدرس آی‌پی ۱۷۶.۳۱.۶۸.۳۰ دریافت می‌شود.

```
▲ Hypertext Transfer Protocol
  ▷ GET /ip-provider.php HTTP/1.0\r\n
  ▷ content-length: 0\r\n
    from: user@sfml-dev.org\r\n
    host: www.sfml-dev.org\r\n
    user-agent: libsfml-network/2.x\r\n
    \r\n
    [Full request URI: http://www.sfml-dev.org/ip-provider.php]
    [HTTP request 1/1]
    [Response in frame: 97]
```

```
0000  52 54 00 12 35 02 08 00  27 0a 7d 76 08 00 45 00   RT··5··· '·}v··E·
0010  00 ae 02 17 40 00 80 06  00 00 0a 00 02 0f 94 fb   ····@··· ········
0020  f7 ae c0 2b 00 50 87 8f  c8 86 02 44 14 02 50 18   ···+·P·· ···D··P·
0030  fa f0 99 59 00 00 47 45  54 20 2f 69 70 2d 70 72   ···Y··GE T /ip-pr
0040  6f 76 69 64 65 72 2e 70  68 70 20 48 54 54 50 2f   ovider.p hp HTTP/
0050  31 2e 30 0d 0a 63 6f 6e  74 65 6e 74 2d 6c 65 6e   1.0··con tent-len
0060  67 74 68 3a 20 30 0d 0a  66 72 6f 6d 3a 20 75 73   gth: 0·· from: us
0070  65 72 40 73 66 6d 6c 2d  64 65 76 2e 6f 72 67 0d   er@sfml- dev.org·
0080  0a 68 6f 73 74 3a 20 77  77 77 2e 73 66 6d 6c 2d   ·host: w ww.sfml-
0090  64 65 76 2e 6f 72 67 0d  0a 75 73 65 72 2d 61 67   dev.org· ·user-ag
```

### ۶-۳ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارایه نشده است.