

باسمه تعالی

گزارش تحلیل باج افزار Iron

تاریخ نگارش:

۱۳۹۷/۰۲/۱۱

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت باج افزار Iron خبر می دهد. این باج افزار به نام های Iron Locker و Iron Unlocker نیز شناخته می شود. بررسی ها نشان می دهد فعالیت این باج افزار در ابتدای ماه آوریل سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. پس از تحلیل و بررسی باج افزار مذکور، آنچه برای ما واضح است، این است که باج افزار Iron در طراحی و توسعه، حداقل از سه خانواده باج افزارهای مختلف کپی برداری نموده است. این خانواده ها به ترتیب زیر می باشند :

- باج افزار Maktub Locker : در طراحی پورتال پرداخت باج و پیغام باج خواهی
- باج افزار DMA Locker : در پورتال رمزگشایی فایل ها
- باج افزار Satan : در نوع فایل های مورد هدف

این باج افزار همانند اکثر باج افزارها، پس از رمزگذاری فایل ها از قربانیان تقاضای بیت کوین می کند.

مشخصات فایل اجرایی :

| | |
|-------------|--|
| نام فایل | ado64, Iron.exe, ftp.exe, core.scr |
| MD5 | 1e6005db09e3d977d2a928fff3d34a6 |
| SHA-1 | f01bab89b4e4e010b973df8affc2d11a4476bd0be |
| SHA-256 | 19ee6d4a89d7f9014e660ca78bd133edf980cc0b0c009e7062be824c0bb9e770 |
| اندازه فایل | ۵۹۸.۵ KB |

فایل اجرایی این باج افزار دارای هفت بخش است :

| نام بخش | آنتروپی | آدرس مجازی | اندازه مجازی | اندازه خام |
|---------|---------|------------|--------------|------------|
| .text | ۰ | ۴۰۹۶ | ۶۱۳۸۳۴ | ۰ |
| shared | ۰ | ۶۱۸۴۹۶ | ۱۷۶۵۶ | ۰ |
| .rdata | ۶.۰۹ | ۶۳۸۹۷۶ | ۲۶۳۲۱۲ | ۲۶۳۶۸۰ |
| .data | ۰ | ۹۰۵۲۱۶ | ۱۰۱۶۷۶ | ۰ |
| .vmp۰ | ۰ | ۱۰۰۷۶۱۶ | ۱۳۲۵۵ | ۰ |
| .vmp۱ | ۷.۹۵ | ۱۰۲۴۰۰۰ | ۳۴۵۶۴۴ | ۳۴۶۱۱۲ |
| .rsrc | ۴.۲۲ | ۱۳۷۲۱۶۰ | ۱۵۲۹۹۶ | ۲۰۴۸ |

تحلیل پویا :

برای بررسی عمیق‌تر باج افزار Iron، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد آن را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد باج‌افزار مورد اشاره، فایل‌های موجود در دایرکتوری‌هایی خاص و دارای پسوندهای خاص را با استفاده از الگوریتم‌های رمزنگاری AES و RSA رمزگذاری می‌کند، باج‌افزار، پس از اتمام فرآیند رمزگذاری، فایل‌های موجود در Recycle Bin را نیز حذف می‌کند. باج‌افزار Iron نقاط بازیابی یا Shadow Volume Copies را حذف نمی‌کند، بنابراین می‌توان به بازگرداندن فایل‌های از دست رفته امیدوار بود. همچنین این باج‌افزار پس از رمزگذاری موفقیت‌آمیز فایل‌ها، پیغام باج‌خواهی خود را به نمایش می‌گذارد. این باج‌افزار فایل‌هایی با پسوندهای زیر را رمزگذاری می‌کند.

.001, .1cd, .3fr, .8ba, .8bc, .8be, .8bf, .8bi8, .8bl, .8bs, .8bx, .8by, .8li, .DayZProfile, .abk, .ade, .adpb, .adr, .aip, .amxx, .ape, .api, .apk, .arch00, .aro, .arw, .asa, .ascx, .ashx, .asmx, .asp, .asr, .asset, .bar, .bay, .bc6, .bc7, .bi8, .bic, .big, .bin, .bkf, .bkp, .blob, .blp, .bml, .bp2, .bp3, .bpl, .bsa, .bsp, .cab, .cap, .cas, .ccd, .cch, .cer, .cfg, .cfr, .cgf, .chk, .class, .clr, .cms, .cod, .col, .con, .cpp, .cr2, .crt, .crw, .csi, .cso, .css, .csv, .ctt, .cty, .cwf, .d3dbsp, .dal, .dap, .das, .db0, .dbb, .dbf, .dbx, .dcp, .dcr, .dcu, .ddc, .ddcx, .dem, .der, .desc, .dev, .dex, .dic, .dif, .dii, .disk, .dmg, .dmp, .dob, .dox, .dpk, .dpl, .dpr, .dsk, .dsp, .dvd, .dxg, .elf, .epk, .eql, .erf, .esm, .f90, .fcd, .fla, .flp, .for, .forge, .fos, .fpk, .fpp, .fsh, .gam, .gdb, .gho, .grf, .h3m, .h4r, .hkdb, .hxx, .hplg, .htm, .html, .hvpl, .ibank, .icxs, .img, .indd, .ipa, .iso, .isu, .isz, .itdb, .itl, .itm, .iwd, .iwi, .jar, .jav, .java, .jpe, .kdc, .kmz, .layout, .lbf, .lbi, .lcd, .lcf, .ldb, .ldf, .lgp, .litemod, .lng, .lrf, .ltm, .ltx, .lvl, .m3u, .m4a, .map, .mbx, .mcd, .mcgame, .mcmeta, .md0, .md1, .md2, .md3, .mdb, .mdbackup, .mddata, .mdf, .mdl, .mdn, .mds, .mef, .menu, .mm6, .mm7, .mm8, .moz, .mpq, .mpqge, .mrwref, .mxx, .ncf, .nds, .nrg, .nri, .nrw, .ntl, .odb, .odf, .odp, .ods, .odt, .orf, .owl, .oxt, .p12, .p7b, .p7c, .pab, .pbp, .pef, .pem, .pfx, .pkb, .pkh, .pkpass, .plc, .pli, .pot, .potm, .potx, .ppf, .ppsm, .pptm, .prc, .prt, .psa, .pst, .ptx, .pww, .pxp, .qbb, .qdf, .qel, .qic, .qpx, .qtr, .r3d, .raf, .re4, .res, .rgn, .rgss3a, .rim, .rofl, .rrt, .rsrc, .rsw, .rte, .rw2, .rwl, .sad, .sav, .sc2save, .scm, .scx, .sdb, .sdc, .sds, .sdt, .shw, .sid, .sidd, .sidn, .sie, .sis, .slm, .slt, .snp, .snx, .spr, .sql, .sr2, .srf, .srw, .std, .stt, .sud, .sum, .svg, .svr, .swd, .syncdb, .t01, .t03, .t05, .t12, .t13, .tar.gz, .tax, .tcx, .thmx, .tlz, .tor, .torrent, .tpu, .tpx, .ttarch2, .tur, .txd, .txf, .uax, .udf, .umx, .unity3d, .unr, .uop, .upk, .upoi, .url, .usa, .usx, .ut2, .ut3, .utc, .utx, .uvx, .uxx, .vcd, .vdf, .ver, .vfs0, .vhd, .vmf, .vmt, .vpk, .vpp_pc, .vsi, .vtf, .w3g, .w3x, .wad, .war, .wb2, .wdgt, .wks, .wmdb, .wmo, .wotreplay, .wpd, .wpl, .wps, .wtd, .wtf, .x3f, .xla, .xlam, .xlc, .xll, .xlm, .xlr, .xlsb, .xltx, .xlv, .xlwx, .xpi, .xpt, .yab, .yps, .z02, .z04, .zap, .zipx, .zoo, .ztmp

با بررسی پسوندهایی که باج افزار Iron رمزگذاری می کند متوجه شدیم که این باج افزار گیمرها را نیز مورد هدف قرار می دهد، زیرا پسوندهایی مانند DayZProfile, wotreplay, .vdf, مربوط به فایل های بازی های کامپیوتری می باشد.

نتایج بدست آمده نشان می دهد، دایرکتوری های زیر توسط باج افزار Iron رمزگذاری نمی شوند.

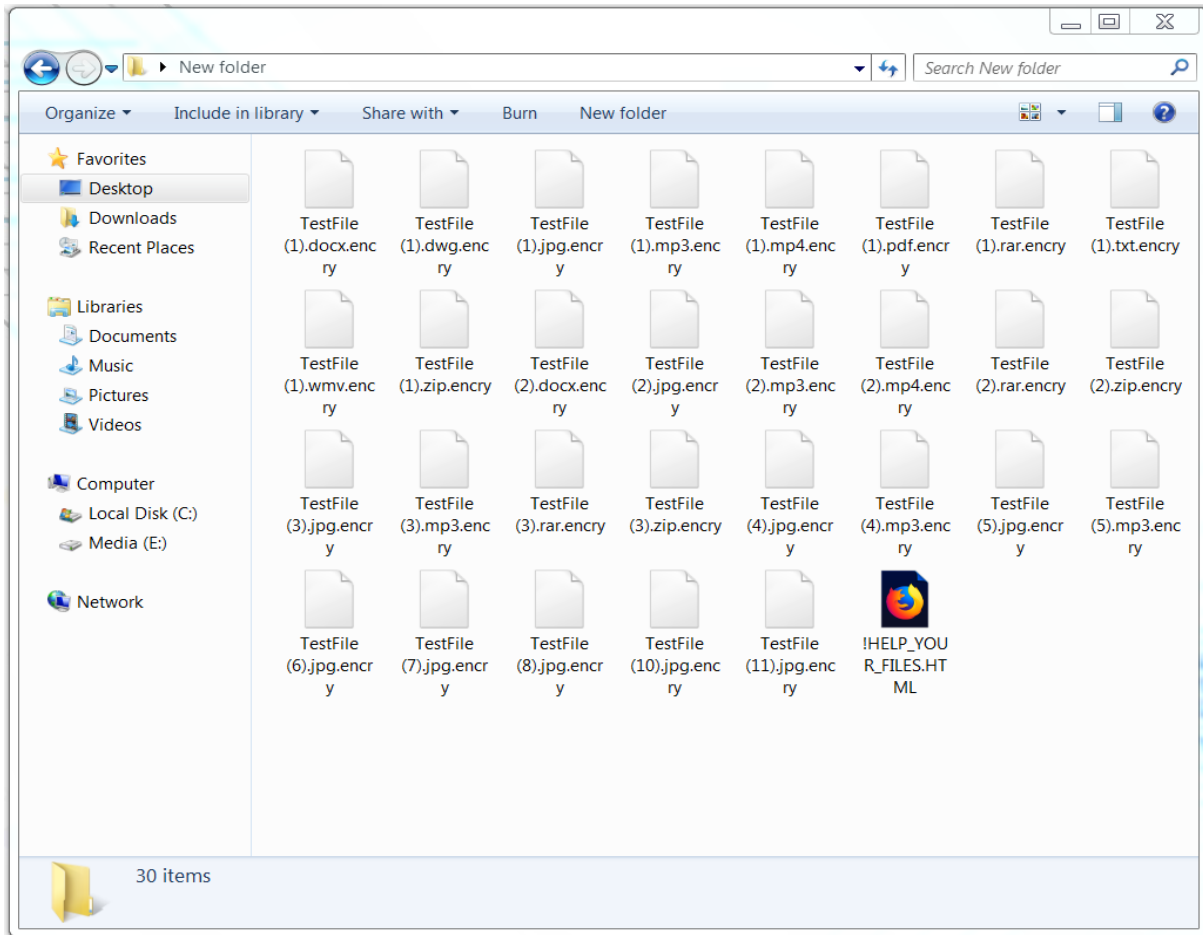
```
windows, Microsoft, Mozilla Firefox, Opera, Internet Explorer, Temp, Local, LocalLow, $Recycle.bin, boot, i۳۸۶, st_v۲, intel, recycle, ۳۶۰rec, ۳۶۰sec, ۳۶۰sand, internet explorer, msbuild
```

واضح است که 360rec, 360sec, 360sand توسط ۳۶۰ Qihoo، که یک شرکت امنیتی مستقر در چین است، توسعه یافته اند. به طور مثال آنتی ویروس Total Security ۳۶۰ یکی از محصولات این شرکت می باشد. بنابراین احتمال اینکه توسعه دهندگان باج افزار، چینی باشند وجود دارد.

باج افزار مورد اشاره یک کلید عمومی RSA را به صورت زیر تعریف می کند.

```
MIGJAoGBAIOyf0KqEOGaxdLmMLypMyZ1q/K+r6DuCdYpwZfs0EPug3ye7UjZa0QMOP5/OySrl/uBJtkmEghEtUEo/zfcBJ7332O1ytJ7/ebiUv+ZcN1Rlswzdv7uZxYRC8u1HvrgBvAz4Atbzx+FbFVqLB0gGixYTqbjqANq21AR6r91+oJtAgMBAAE=
```

تصویر زیر نشان دهنده فایل های رمزگذاری شده توسط این باج افزار می باشد.



همانطور که در تصویر نیز قابل مشاهده است، پسوند تمام فایل‌ها پس از رمزگذاری، به "ency" تغییر پیدا می‌کند و یک فایل به نام !HELP_YOUR_FILES! با فرمت HTML ایجاد می‌شود که شامل پیغام باج‌خواهی می‌باشد. در تصویر زیر پیغام باج‌خواهی باج‌افزار Iron را مشاهده می‌کنید.

WARNING!

Your personal files are encrypted!

11:52:38

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://y5mogzal2w25p6bn.ml>
or <http://y5mogzal2w25p6bn.ml>
or <http://y5mogzal2w25p6bn.ml>
or <http://y5mogzal2w25p6bn.ml>

in your browser. They are public gates to the secret server.
The website can help you complete the decryption work automatically. You could also send 0.2 btc and contact below

1cimKyzS64PRNEiG89iFU3qzckVuEO

recoverfile@mail2tor.com

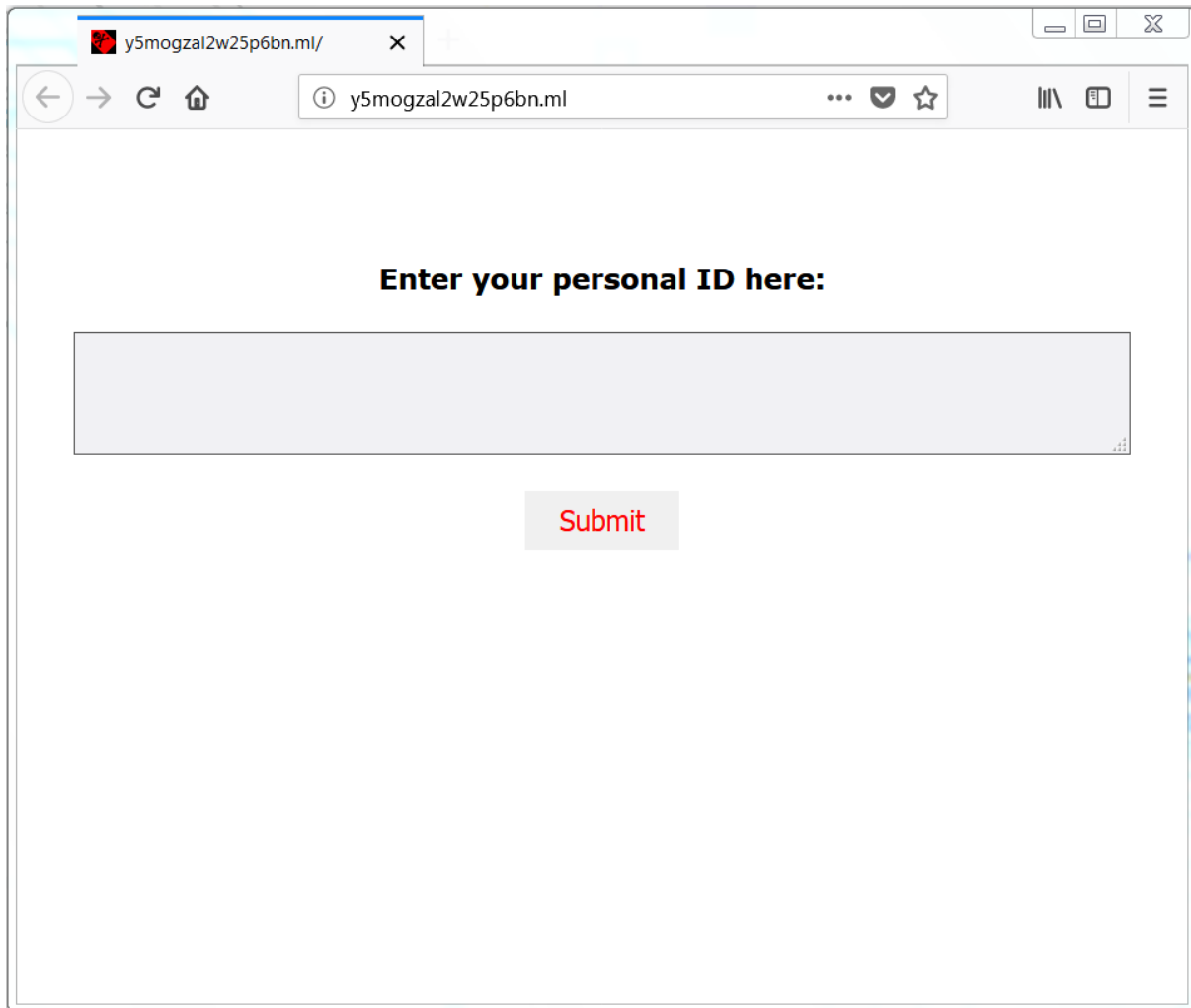
Write in the following personal ID in the input form on server:

5ae8C

[Click Here Copy ID to Clipboard](#)

بر اساس پیغام باج‌خواهی، فایل‌ها با یک کلید قوی و مخصوص که برای سیستم قربانی تولید شده است، رمزگذاری شده و کلید خصوصی جهت رمزگشایی فایل‌ها بر روی یک سرور مخفی به آدرس <http://y5mogzal2w25p6bn.ml> در اینترنت ذخیره شده است، که قربانیان برای دریافت کلید رمزگشایی فایل‌ها باید به آن مراجعه نمایند. قربانی برای ورود به این وب‌سایت باید شناسه مربوط به خود که در انتهای پیغام باج‌خواهی آمده است را وارد نماید. مهاجمین اعلام نموده‌اند که قربانی می‌بایست مبلغ ۰.۲ بیت‌کوین را به کیف پول بیت‌کوین `1cimKyzS64PRNEiG89iFU3qzckVuEQUj` ارسال نمایند، در غیر این صورت پس از پایان مهلت پرداخت باج که ۱۲ ساعت می‌باشد، سرور، کلید رمزگشایی را از بین برده و فایل‌ها دیگر قابل رمزگشایی نیستند. ضمناً مهاجم، ایمیلی به آدرس recoverfile@mail2tor.com را نیز برای ارتباط‌گیری با قربانی، در پیغام باج‌خواهی قرار داده است.

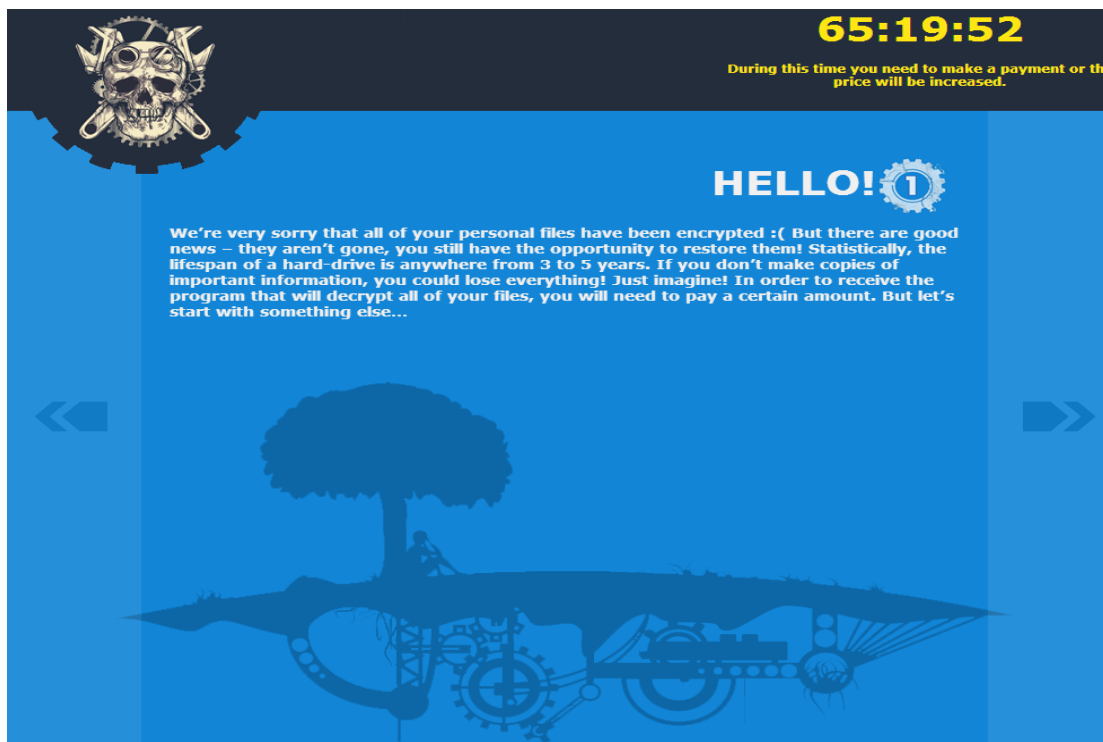
تصاویر مربوط به درگاه پرداخت باج افزار Iron را در زیر مشاهده می نمایید.



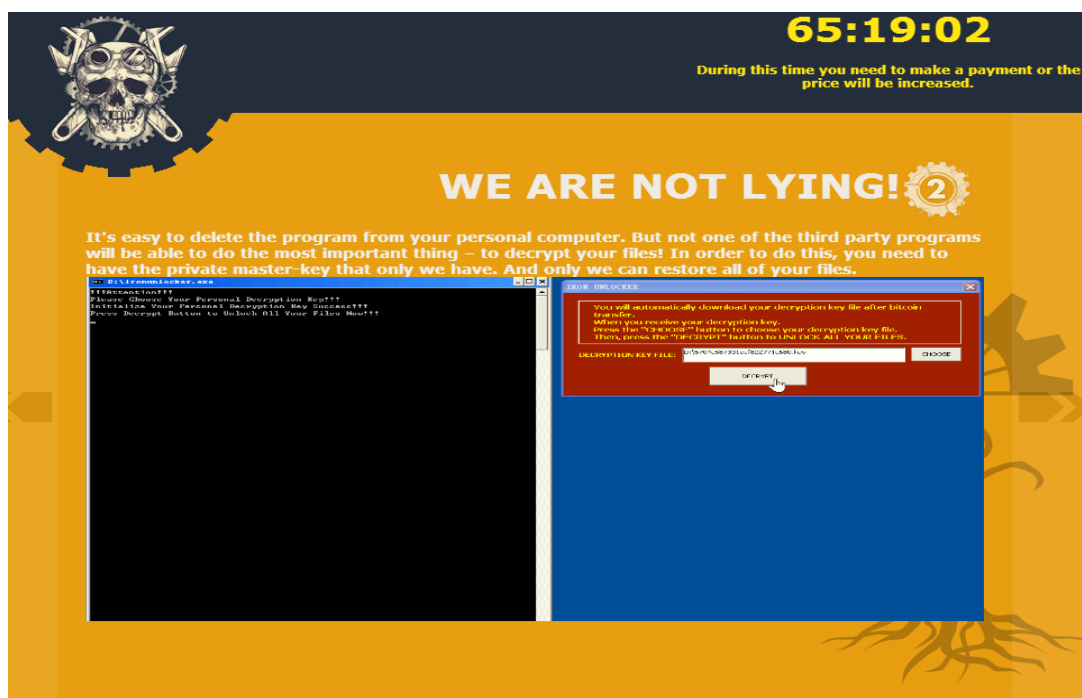
The screenshot shows a web browser window with the address bar displaying 'y5mogzal2w25p6bn.ml/'. The main content of the page is a form with the following elements:

- A heading: **Enter your personal ID here:**
- A large, empty rectangular input field for entering the ID.
- A button labeled **Submit** in red text, centered below the input field.


قربانی پس از مراجعه به وب سایتی که اشاره شد باید در کادر مربوطه، شناسه خود را وارد نماید و بر روی دکمه ی Submit کلیک نماید. پس از ورود، پیغام های زیر به قربانی نمایش داده می شود :



پیغام اول با عنوان "سلام!" ، پس از وارد کردن شناسه شخصی به قربانی نمایش داده می‌شود و در آن مهاجم ابراز شرمساری خود را از اینکه فایل‌ها رمزگذاری شده‌اند، اعلام کرده است و در ادامه اعلام نموده در صورت این که فایل‌های خود را می‌خواهید هر چه سریع‌تر مبلغ باج را پرداخت نمایید.



پیغام دوم نحوه‌ی رمزگشایی فایل‌ها پس از پرداخت مبلغ باج را نشان می‌دهد. در اینجا مهاجم سعی در جلب اعتماد قربانی برای پرداخت باج دارد.



65:18:44
During this time you need to make a payment or the price will be increased.


HOW MUCH DOES IT COST? 3

We hope that you are convinced that we can decrypt all of your files. Now, the most important thing! The faster you transfer the money, the cheaper file decryption will be. At every stage of payment, you get 3 days or 72 hours. You can see the countdown in the right top corner. After the clock shows 00:00:00 you go to the next stage of payment and the price automatically increases. We only accept the electronic currency Bitcoin as a form of payment. Here is a table that shows the date of payment and the price. Your current stage is marked in yellow.

| Stage | Time of payment | How much money should be sent |
|-------|-------------------------|-----------------------------------|
| 1 | During the first 3 days | 0.2 BTC (~\$1200) |
| 2 | From 3 to 6 days | 0.5 BTC (~\$3000) |
| 3 | From 6 to 9 days | 0.8 BTC (~\$4800) |
| 4 | From 9 to 12 days | 1.1 BTC (~\$6600) |
| 5 | From 12 to 15 days | 1.4000000000000001 BTC (~\$8400) |
| 6 | More than 15 days | 1.7000000000000002 BTC (~\$10200) |

! After 15 days of no payment, we do not guarantee that we saved the key. This site can be disconnected at any moment and you will lose your data forever. Please take this seriously.

در پیغام سوم با این عنوان که "چه مقدار باج باید پرداخت شود؟" مهاجم اعلام می کند که طبق جدول موجود، مهلت پرداخت شامل چند مرحله می باشد که در صورت پایان مهلت پرداخت، وارد مرحله ی بعدی شده و مبلغ باج نیز افزایش خواهد یافت. طبق این جدول قربانی هر چه سریعتر مبلغ باج را پرداخت نماید کمتر ضرر می کند. در صورتی که بعد از ۱۵ روز مبلغ باج پرداخت نشود هیچ گونه ضمانتی برای ذخیره کلید رمزگشایی وجود ندارد و هر لحظه ممکن است ارتباط با سایت برای قربانی قطع شود و دسترسی به فایل های رمزگذاری شده برای همیشه از بین بروند.



65:18:06
During this time you need to make a payment or the price will be increased.

WHERE DO I PAY? 4

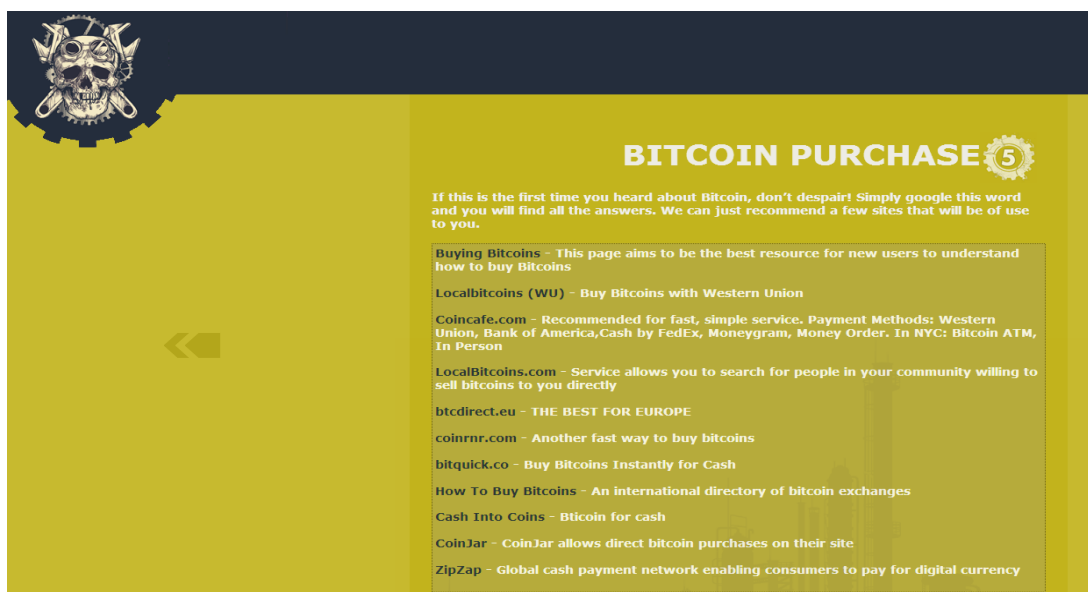
The whole process of payment confirmation is automated! As soon as you send the money, it will only take 1 minutes for the system to automatically count them and create the program that will decode your files. After sending your payment just refresh this site after 1 minutes(or go to homepage input your personal ID).

You must transfer **0.2 BTC** to the following address:

1tD2ofc9Yw2J4AWtjvxo46BV3w3YdomS9

| Number | File Name | Size | Link |
|--------|-----------------------------|---------|----------|
| 0 | IronUnlocker.exe | unknown | Download |
| 1 | 5accb7cb4addc05c7577b71.key | unknown | Download |

پیغام چهارم با عنوان "از چه طریقی پرداخت را انجام دهم؟" می باشد بر طبق آن، پس از پرداخت مبلغ مورد نظر، یک دقیقه طول می کشد تا ابزارهای لازم برای رمزگشایی فایل ها در اختیار قربانی قرار گیرد. در ادامه، مبلغ باج، آدرس کیف پول بیت کوین و ابزارهای رمزگشایی فایل ها که پس از پرداخت فعال می شوند، قرار گرفته اند. نکته ای که در این جا می توان به آن اشاره نمود آدرس کیف پول بیت کوین می باشد که با آدرسی که در پیغام باج خواهی وجود دارد متفاوت است.



اما در پیغام پنجم، آدرس وب سایت هایی جهت تهیه بیت کوین قرار داده شده است.

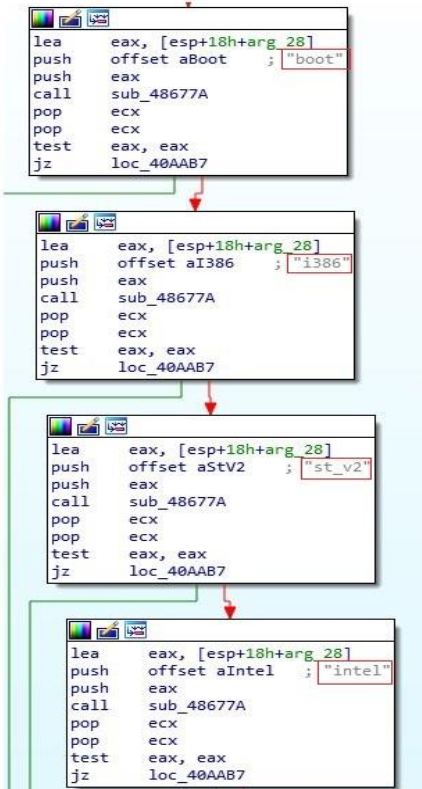
طبق بررسی های انجام شده اکثر آنتی ویروس های معتبر، این باج افزار را به عنوان یک تروجان شناسایی نموده اند. لذا احتمال نفوذ باج افزار به سیستم از راه های متداول از جمله هرزنامه ها وجود دارد.

تحلیل ایستا:

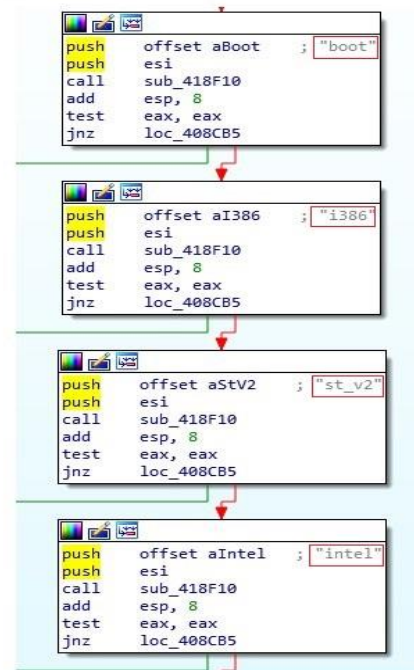
پس از بررسی کد منبع باج افزار نتایج زیر حاصل گردید :

همانطور که پیش تر نیز اشاره شد، کد منبع این باج افزار شباهاتی با کد منبع باج افزار Satan دارد. طبق بررسی های انجام شده نحوه رمزگذاری فایل ها توسط دو باج افزار با یکدیگر متفاوت است، اما تشابهاتی در لیست فایل هایی که مورد هدف قرار می دهند بین دو باج افزار مشاهده شده است که در تصویر زیر قابل مشاهده می باشد.

Iron ransomware



Satan ransomware



این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هر کدام از کتابخانه ها استفاده می کند. در تصویر زیر که مربوط به کد منبع باج افزار Iron می باشد کاربرد این کتابخانه ها به خوبی قابل مشاهده است. همچنین لیست کامل این کتابخانه ها به همراه توابع مورد استفاده نیز در ادامه متن آمده است.

```

IDA View-A | Hex View-1 | Structures | Enums | Imports
.vmp1:00505A60 ; Import names for USER32.dll
.vmp1:00505A60 off_505A60 dd rva word_5050A7 ; DATA XREF: .vmp1: __IMPORT_DESCRIPTOR_USER32fo
.vmp1:00505A64 dd rva word_4FA8C3
.vmp1:00505A68 dd rva word_5068FF
.vmp1:00505A6C dd rva word_504E29
.vmp1:00505A70 dd rva word_4FD535
.vmp1:00505A74 dd rva word_503E1A
.vmp1:00505A78 dd rva word_4FA12C
.vmp1:00505A7C dd rva word_4FA7F4
.vmp1:00505A80 dd rva word_4FA805
.vmp1:00505A84 dd rva word_505506
.vmp1:00505A88 dd rva word_5494C3
.vmp1:00505A8C dd rva word_4FA854
.vmp1:00505A90 dd rva word_4FA714
.vmp1:00505A94 dd rva word_4FC98B
.vmp1:00505A98 dd rva word_4FC45F
.vmp1:00505A9C dd rva word_4FD4B6
.vmp1:00505AA0 dd 0
.vmp1:00505AA4 ; Import names for GDI32.dll
.vmp1:00505AA4 off_505AA4 dd rva word_506962 ; DATA XREF: .vmp1: __IMPORT_DESCRIPTOR_GDI32fo
.vmp1:00505AA8 dd rva word_506C10
.vmp1:00505AAC dd rva word_506A31
.vmp1:00505AB0 dd rva word_50511D
.vmp1:00505AB4 dd rva word_4FD880
.vmp1:00505AB8 dd rva word_502944
.vmp1:00505ABC dd 0
.vmp1:00505AC0 ; Import names for ADVAPI32.dll
.vmp1:00505AC0 off_505AC0 dd rva word_507081 ; DATA XREF: .vmp1: __IMPORT_DESCRIPTOR_ADVAPI32fo
.vmp1:00505AC4 dd rva word_4FFF2D
.vmp1:00505AC8 dd rva word_4FA998
.vmp1:00505ACC dd 0
.vmp1:00505AD0 ; Import names for SHELL32.dll
.vmp1:00505AD0 off_505AD0 dd rva word_4FFFB8 ; DATA XREF: .vmp1: __IMPORT_DESCRIPTOR_SHELL32fo
.vmp1:00505AD4 dd rva word_503FCF
.vmp1:00505AD8 dd rva word_50448A
.vmp1:00505ADC dd 0
.vmp1:00505AE0 ; Import names for ole32.dll
.vmp1:00505AE0 off_505AE0 dd rva word_4FA8B4 ; DATA XREF: .vmp1: __IMPORT_DESCRIPTOR_ole32fo
.vmp1:00505AE4 dd rva word_5036E1
.vmp1:00505AE8 dd rva word_505E7F
.vmp1:00505AEC dd rva word_5067DE
.vmp1:00505AF0 dd rva word_4FD4FC
.vmp1:00505AF4 dd 0
.vmp1:00505AF8 ;

```

| WINHTTP.dll | USER32.dll | USER32.dll | USER32.dll |
|---|--|---|--|
| WinHttpCloseHandle WinHttpQueryHeaders | SendMessageA SetClipboardData SetDlgItemTextA SetWindowLongA SetWindowPos wsprintfA | CloseClipboard DialogBoxParam W EmptyClipboard GetDlgItemID GetDlgItem | GetProcessWindowStation GetSysColorBrush GetObjectInformation W MessageBoxA OpenClipboard |

| ADVAPI32.dll | GDI32.dll | ole32.dll | SHELL32.dll | WS2_32.dll |
|---|---|---|---|---|
| DeregisterEventSource RegisterEventSourceA ReportEventA | CreateFontIndirectA CreateSolidBrush GetObjectA GetStockObject SetBkColor SetTextColor | CoCreateGuid CoCreateInstance CoInitialize CoTaskMemFree CoUninitialize | ShellExecuteA SHEmptyRecycl eBinA SHGetFolderPat hW | gethostbyname inet_addr inet_ntoa WSACleanup WSAStartup |

| KERNEL۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll |
|---------------------------------------|-------------------------|-----------------------------|-------------------------|---------------------|
| GetSystemTimeAsFileTime | CloseHandle | RaiseException | GetCurrentThreadId | UnhandledException |
| GetTickCount | CompareStringW | ReadConsoleInputA | GetEnvironmentString | Filter |
| GlobalAlloc | CreateEventW | ReadConsoleW | sW | VirtualFree |
| GlobalLock | CreateFileW | ReadFile | GetFileAttributesExW | VirtualQuery |
| GlobalMemoryStatus | CreateMutexA | ReleaseMutex | GetFileType | WaitForSingleObject |
| GlobalUnlock | DecodePointer | ResetEvent | GetLastError | Ex |
| HeapAlloc | DeleteCriticalSection | RtlUnwind | GetModuleFileNameA | WideCharToMultiByte |
| HeapFree | EncodePointer | SetConsoleCtrlHandler | GetModuleFileNameW | WriteConsoleW |
| HeapReAlloc | EnterCriticalSection | er | W | WriteFile |
| HeapSize | ExitProcess | SetConsoleMode | GetModuleHandleA | TlsFree |
| InitializeCriticalSectionAndSpinCount | FindClose | SetEndOfFile | GetModuleHandleEx | TlsGetValue |
| InitializeSListHead | FindFirstFileExA | SetEnvironmentVariableA | W | TlsSetValue |
| IsDebuggerPresent | FindNextFileA | SetEvent | GetModuleHandleW | GetCPIInfo |
| IsProcessorFeaturePresent | FlushConsoleInputBuffer | SetFilePointerEx | GetOEMCP | GetCurrentProcess |
| IsValidCodePage | FlushFileBuffers | SetLastError | GetProcAddress | GetCurrentProcessId |
| LCMapStringW | FreeEnvironmentStringsW | SetStdHandle | GetProcessHeap | MoveFileExW |
| LeaveCriticalSection | FreeLibrary | SetUnhandledExceptionFilter | GetStartupInfoW | MultiByteToWideChar |
| LoadLibraryA | GetACP | ionFilter | GetStdHandle | MultiByteToWideChar |
| LoadLibraryExW | GetCommandLineA | Sleep | GetStringTypeW | TlsAlloc |
| LocalAlloc | GetCommandLineW | TerminateProcess | QueryPerformanceCounter | GetConsoleMode |
| LocalFree | GetConsoleCP | | | |

نتایج حاصل از تحلیل ها نشان می دهد، کد باج افزار Iron کاملاً منحصر به فرد است و مانند یک باج افزار کاملاً جدید به نظر می رسد و این امکان نیز وجود دارد که یک پروژه جانبی توسط توسعه دهندگان باج افزار Satan باشد. با این حال، به طور قطع نمی توان گفت که چه کسی یا گروهی توسعه دهنده این باج افزار است.

بر اساس بررسی های صورت گرفته، باج افزار Iron پس از اجرا، ۱۳ فرایند را ایجاد می کند، که این فرایندها طبق لیست زیر می باشند :

Iron.exe

```
iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/
iexplore.exe SCODEF:۲۵۲۸ CREDAT:۲۷۵۴۵۷ /prefetch:۲
iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/
iexplore.exe SCODEF:۲۱۲۸ CREDAT:۲۷۵۴۵۷ /prefetch:۲
iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/
iexplore.exe SCODEF:۴۵۶۰ CREDAT:۲۷۵۴۵۷ /prefetch:۲
iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/
```

iexplore.exe SCODEF:۱۳۹۶ CREDAT:۲۷۵۴۵۷ /prefetch:۲

iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/

iexplore.exe SCODEF:۲۸۳۶ CREDAT:۲۷۵۴۵۷ /prefetch:۲

iexplore.exe http://y۵mogzal۲w۲۵p۶bn.ml/

iexplore.exe SCODEF:۴۴۵۶ CREDAT:۲۷۵۴۵۷ /prefetch:۲

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج افزار Iron را نشان می دهد.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 22 | 1.365090 | 104.31.69.125 | 192.168.1.37 | HTTP | 781 | [TCP Previous segment not captured] Continuation |
| 23 | 1.365090 | 104.31.69.125 | 192.168.1.37 | HTTP | 60 | Continuation |
| 24 | 1.365117 | 192.168.1.37 | 104.31.69.125 | TCP | 66 | 49178 → 80 [ACK] Seq=960 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=3536 |
| 25 | 1.365210 | 192.168.1.37 | 104.31.69.125 | TCP | 66 | [TCP Dup ACK 24#1] 49178 → 80 [ACK] Seq=960 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=3541 |
| 26 | 1.372292 | 104.31.69.125 | 192.168.1.37 | TCP | 1458 | [TCP Out-Of-Order] 80 → 49178 [ACK] Seq=1405 Ack=232 Win=30720 Len=1404 |
| 27 | 1.372293 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49178 [RST, ACK] Seq=3541 Ack=960 Win=31744 Len=0 |
| 28 | 1.372330 | 192.168.1.37 | 104.31.69.125 | TCP | 54 | 49178 → 80 [ACK] Seq=960 Ack=3541 Win=65792 Len=0 |
| 29 | 1.472140 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49178 [RST] Seq=1405 Win=0 Len=0 |
| 30 | 1.473026 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49178 [RST] Seq=1405 Win=0 Len=0 |
| 31 | 1.478435 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49178 [RST] Seq=3541 Win=0 Len=0 |
| 32 | 2.399565 | 192.168.1.37 | 104.31.69.125 | TCP | 66 | 49179 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 33 | 2.505962 | 104.31.69.125 | 192.168.1.37 | TCP | 66 | 80 → 49179 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1404 SACK_PERM=1 WS=1024 |
| 34 | 2.506011 | 192.168.1.37 | 104.31.69.125 | TCP | 54 | 49179 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0 |
| 35 | 2.506195 | 192.168.1.37 | 104.31.69.125 | TCP | 347 | 49179 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=293 [TCP segment of a reassembled PDU] |
| 36 | 2.506289 | 192.168.1.37 | 104.31.69.125 | HTTP | 782 | POST /receive HTTP/1.1 (application/json) |
| 37 | 2.621091 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [ACK] Seq=1 Ack=294 Win=30720 Len=0 |
| 38 | 2.628284 | 104.31.69.125 | 192.168.1.37 | HTTP | 60 | [TCP Previous segment not captured] Continuation |
| 39 | 2.628316 | 192.168.1.37 | 104.31.69.125 | TCP | 66 | [TCP Dup ACK 34#1] 49179 → 80 [ACK] Seq=1022 Ack=1 Win=65792 Len=0 SLE=3386 SRE=3391 |
| 40 | 2.632807 | 104.31.69.125 | 192.168.1.37 | TCP | 1458 | [TCP Out-Of-Order] 80 → 49179 [ACK] Seq=1405 Ack=294 Win=30720 Len=1404 [TCP segment of a reassembled PDU] |
| 41 | 2.632828 | 192.168.1.37 | 104.31.69.125 | TCP | 74 | [TCP Dup ACK 34#2] 49179 → 80 [ACK] Seq=1022 Ack=1 Win=65792 Len=0 SLE=1405 SRE=2809 SLE=3386 SRE=3391 |
| 42 | 2.635469 | 104.31.69.125 | 192.168.1.37 | TCP | 631 | [TCP Out-Of-Order] 80 → 49179 [PSH, ACK] Seq=2809 Ack=294 Win=30720 Len=577 |
| 43 | 2.635581 | 192.168.1.37 | 104.31.69.125 | TCP | 60 | [TCP Dup ACK 34#3] 49179 → 80 [ACK] Seq=1022 Ack=1 Win=65792 Len=0 SLE=1405 SRE=3391 |
| 44 | 2.641859 | 104.31.69.125 | 192.168.1.37 | TCP | 1458 | [TCP Fast Retransmission] 80 → 49179 [ACK] Seq=1 Ack=294 Win=30720 Len=1404 [TCP segment of a reassembled PDU] |
| 45 | 2.641903 | 192.168.1.37 | 104.31.69.125 | TCP | 54 | 49179 → 80 [ACK] Seq=1022 Ack=3391 Win=65792 Len=0 |
| 46 | 2.642060 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [RST, ACK] Seq=3391 Ack=1022 Win=31744 Len=0 |
| 47 | 2.733666 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [RST] Seq=1 Win=0 Len=0 |
| 48 | 2.740401 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [RST] Seq=1 Win=0 Len=0 |
| 49 | 2.741776 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [RST] Seq=1 Win=0 Len=0 |
| 50 | 2.747971 | 104.31.69.125 | 192.168.1.37 | TCP | 60 | 80 → 49179 [RST] Seq=3391 Win=0 Len=0 |

درخواست های DNS، پس از اجرای باج افزار به شرح جدول زیر می باشد.

| کشور | آدرس آی پی | دامنه |
|---------------------|---------------|---------------------|
| ایالات متحده امریکا | ۱۰۴.۳۱.۶۹.۱۲۵ | y۵mogzal۲w۲۵p۶bn.ml |
| ایالات متحده امریکا | ۶۷.۲۱۵.۹۲.۲۱۵ | myip.dnsomatic.com |

از بین موارد فوق، آی پی ۱۰۴.۳۱.۶۹.۱۲۵، مربوط به سرور C&C باج افزار می باشد.

لیست میزبان هایی که باج افزار با آن ها ارتباط برقرار کرده است.

| نام کشور | شماره پورت | آدرس آی پی |
|---------------------|------------|---------------|
| ایالات متحده امریکا | ۸۰ TCP | ۱۰۴.۳۱.۶۹.۱۲۵ |
| ایالات متحده امریکا | ۸۰ TCP | ۶۷.۲۱۵.۹۲.۲۱۵ |

نتایج حاصل از تحلیل ها نشان می دهد که باج افزار Iron پس از حمله، آی پی سیستم قربانی را مشخص کرده و یک درخواست ارسال بسته را به سرور C&C ارسال می نماید.

```

Wireshark - Follow TCP Stream (tcp.stream eq 1) - wireshark_93DF4962-A00B-49BE-AEC7-7C8E38E582B1_20180501200000_a01308

POST /receive HTTP/1.1
Connection: Keep-Alive
Content-Type: application/json
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Content-Length: 728
Host: y5mogzal2w25p6bn.ml

{"ency": "NKF09LRVUTx9Vfd4yoAp1tHTQ
+oKUqWpV3Eln2GI0VQRiljUkN2wV5mTQQRiws4JaBxW50AZZJPKVGdc10k43lsZ2uP0X1N9y9zUibj9iWB4ANHsDqTRJXa46vu1QRnFdq3xJ0kIwcfXtoV5eRhW0Hx0WJ8GxDJfJ
zkesSQxUwi50LufBQrmaSvp6jxNFXG2tv4Iue/
hGtiXkxTkghKAvoS2mLmmOyyg7GnOfI8d1FR6vADItA1SyfSygVqmcTmiJzRy5Q11S8fPFA4Npn6BUZzi4MzoEbVC0KNfsZDmDYqs1cCcF7oL4pd3W57nDSXEQeL3LGBTh5kQN
2TFM68GzUfkkCinlrT57CORv15B7iu/KIN9070iCFZ5p2c33JEPvml1mVl/dgxDKzvZjeu1fYJX3WVAONYQi3am/zdZznBri3DcYm
+00Znzdz0A17eEFvzfuiIYA0cHmAmMlwIk1sRfey7zH5g/BH64dufPgnx1MvuFchzne1JA1ksZ98GIaWfchFIBYcFVfz32HoNRU+d5g0GxSW5Lxk5m0Lsb
+6JGJRCmmeFuekjFeVtdcr746Hh3mxCPuenK0Mx1MOUQ==", "randk": "+DoQORvRNupaeQ8L/
nbPh718tuJyxeE1bS5ivzurl04=", "guid": "90CF5736EAFB42fa6A8F2B58", "start": "1", "market": "csv"}HTTP/1.1 403 Forbidden
Date: Tue, 01 May 2018 15:30:14 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d4630c58b74b091cb8f46f9dcb2af594b1525188614; expires=Wed, 01-May-19 15:30:14 GMT; path=/;
domain=.y5mogzal2w25p6bn.ml; HttpOnly
Cache-Control: max-age=15
Expires: Tue, 01 May 2018 15:30:29 GMT
X-Frame-Options: SAMEORIGIN
Server: cloudflare
CF-RAY: 414349c7163e26ae-FRA

c05
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif-->
<head>
<title>Access denied | y5mogzal2w25p6bn.ml used Cloudflare to restrict access</title>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id="cf_styles-ie-css" href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css"
4 client ptkts, 6 server ptkts, 3 turns.
Entire conversation (3767 bytes) Show and save data as ASCII Stream 1

```

به نظر می رسد باج افزار Iron برای هر سیستمی که رمزگذاری می کند، یک کد شناسایی اختصاص می دهد تا دوباره آن سیستم را مورد حمله قرار ندهد. این باج افزار مقادیر زیر را به سرور C&C ارسال می نماید.

- کلید رمزگذاری
- کد شناسایی
- شروع (آیا باج افزار با موفقیت اجرا شده است)

- Rank (seed)
- Market (unknown)

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش، تعداد ۴۷ مورد از ۶۶ آنتی ویروس معتبر دنیا قادر به تشخیص آلودگی این باج افزار در سامانه VirusTotal شده اند.

| | | | |
|--------------------|---|----------------------|---------------------------|
| Ad-Aware | Trojan.GenericKD.40187953 | AegisLab | Troj.Ransom.W32.GenIc |
| AhnLab-V3 | Trojan/Win32.FileCoder.C2456998 | ALYac | Trojan.Ransom.Iron |
| Arcabit | Trojan.Generic.D2653831 | Avast | Win32:Malware-gen |
| AVG | Win32:Malware-gen | Avira | TR/FileCoder.zceqb |
| AVware | Trojan.Win32.Generic!BT | BitDefender | Trojan.GenericKD.40187953 |
| Blkav | HW32.Packed.9987 | CAT-QuickHeal | Trojan.IGENERIC |
| CrowdStrike Falcon | malicious_confidence_100% (W) | Cylance | Unsafe |
| Cyren | W32/Trojan.EEXN-5257 | DrWeb | Trojan.Encoder.25083 |
| Emsisoft | Trojan-Ransom.Iron (A) | eScan | Trojan.GenericKD.40187953 |
| ESET-NOD32 | a variant of Win32/Filecoder.NHS | Fortinet | W32/Gen.HSR!tr |
| GData | Trojan.GenericKD.40187953 | Ikarus | Trojan-Ransom.Maktub |
| K7AntiVirus | Trojan (004f8e121) | K7GW | Trojan (004f8e121) |
| Kaspersky | Trojan-Ransom.Win32.Gen.hsr | Malwarebytes | Ransom.FileCryptor |
| MAX | malware (ai score=99) | McAfee | Ransom-Iron!1E60050DB59E |
| McAfee-GW-Edition | BehavesLike.Win32.DownloadAdmin.hc | Microsoft | Trojan:Win32/Tiggre!rfn |
| NANO-Antivirus | Trojan.Win32.Encoder.faddjn | Palo Alto Networks | generic.ml |
| Panda | Trj/CI.A | Qihoo-360 | Win32/Trojan.5a2 |
| Rising | Trojan.Azden!8.F0E3 (TFE:5:He2A7ob9XzP) | SentinelOne | static engine - malicious |
| Sophos AV | Troj/Maktub-E | Sophos ML | heuristic |
| Symantec | Trojan Horse | Tencent | Win32.Trojan.Raas.Auto |
| TrendMicro | Ransom_MAKTUB.THDAAAH | TrendMicro-HouseCall | Ransom_MAKTUB.THDAAAH |
| VBA32 | suspected of Trojan.Downloader.gen.h | VIPRE | Trojan.Win32.Generic!BT |
| ViRobot | Trojan.Win32.Z.Agent.612864.DA | Webroot | W32.Ransomware.Gen |
| ZoneAlarm | Trojan-Ransom.Win32.Gen.hsr | Antiy-AVL | Clean |