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 می‌دهد. این باج‌افزار به نام‌های Iron Locker و Iron Unlocker نیز شناخته می‌شود. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در ابتدای ماه آوریل سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. پس از تحلیل و بررسی باج افزار مذکور، آنچه برای ما واضح است، این است که باج‌افزار Iron در طراحی و توسعه، حداقل از سه خانواده باج‌افزارهای مختلف کپی برداری نموده است. این خانواده‌ها به ترتیب زیر می‌باشند :

- باج‌افزار Maktub Locker : در طراحی پورتال پرداخت باج و پیغام باج‌خواهی
- باج‌افزار DMA Locker : در پورتال رمزگشایی فایل‌ها
- باج افزار Satan : در نوع فایل‌های مورد هدف

این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

نام فایل	ado64, Iron.exe, ftp.exe, core.scr
MD۵	۱e٦۰۰۵۰db۵۹e۳d۹۷۷d۲a۹۲۸fff۳d۳٤a٦
SHA-۱	f۵۱bab۸۹b٤e٤۵۱۰b۹۷۳df۸affc۲d۱۱a٤٤۷٦bd۵be
SHA-256	۱۹ee٦d٤a۸۹d۷f۹۵۱٤۵٦٦۰ca٦۸bd۱۳۳edf۹۸۵cc۵b۵c۵۵۹e۷۰٦۲be۸۲٤c۰bb۹e۷۷۰
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	٤۰۹٦	٦۱۳۸۳٤	۰
shared	۰	٦۱۸٤۹٦	۱۷٦۵٦	۰
.rdata	٦.۰۹	٦۳۸۹۷٦	۲٦۳۲۱۲	۲٦۳٦۸۰
.data	۰	۹۰۵۲۱٦	۱۰۱٦۷٦	۰
.vmp۰	۰	۱۰۰۷٦۱٦	۱۳۲۵۵	۰
.vmp۱	۷.۹۵	۱۰۲٤۰۰۰	۳٤۵٦٤٤	۳٤٦۱۱۲
.rsrc	٤.۲۲	۱۳۷۲۱٦۰	۱۵۲۹۹٦	۲۰٤۸

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, .hkx, .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, .mxp, .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, .pwf, .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, .xlk, .xll, .xlm, .xlr, .xlsb, .xltx, .xlv, .xlwx, .xpi, .xpt, .yab, .yps, .z02, .z04, .zap, .zipx, .zoo, .ztmp

با بررسی پسوندهایی که باج‌افزار Iron رمزگذاری می‌کند متوجه شدیم که این باج‌افزار گیمرها را نیز مورد هدف قرار می‌دهد، زیرا پسوندهایی مانند .DayZProfile, .wotreplay, .vdf. مربوط به فایل های بازی‌های کامپیوتری می‌باشد.

نتایج بدست آمده نشان می دهد، دایرکتوری‌های زیر توسط باج‌افزار Iron رمزگذاری نمی‌شوند.

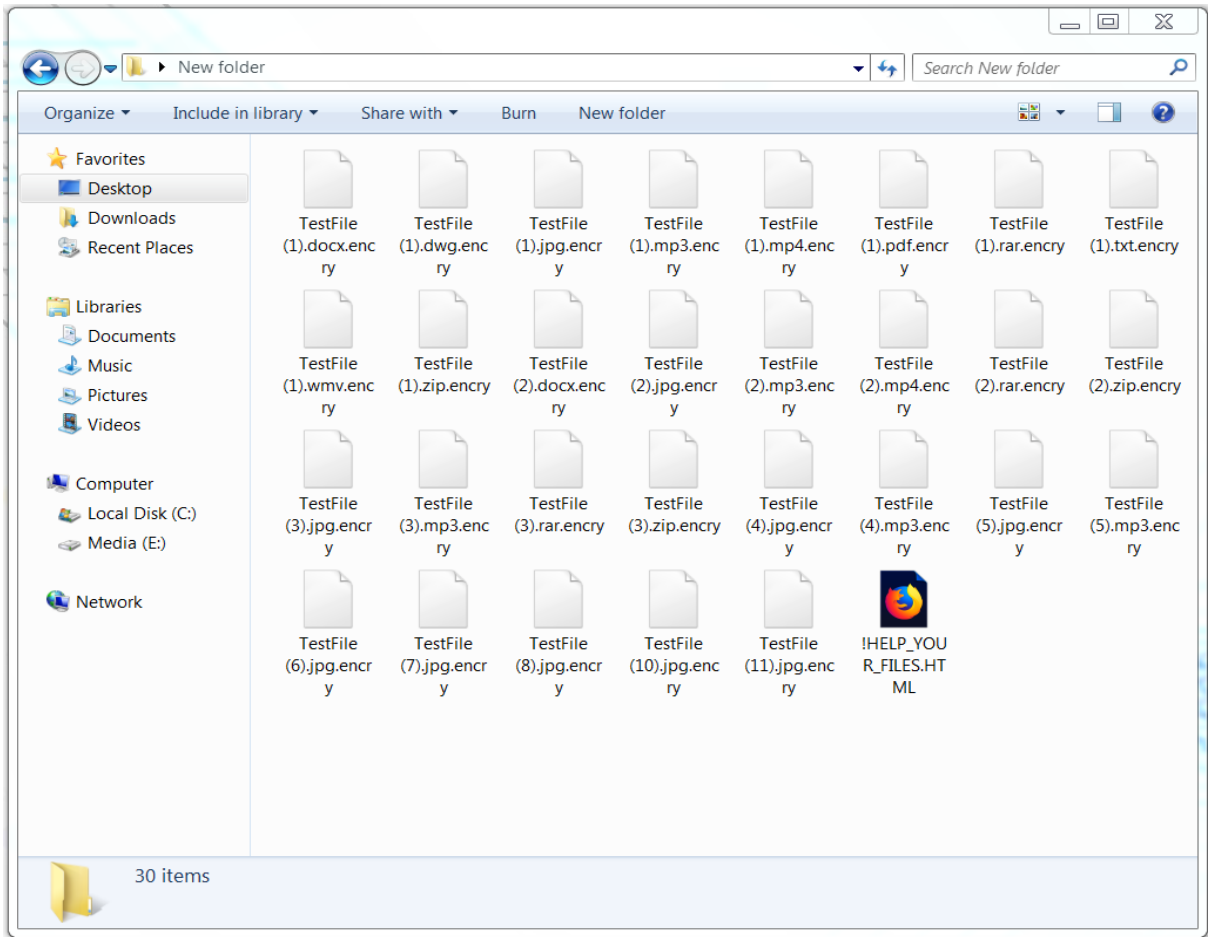
windows, Microsoft, Mozilla Firefox, Opera, Internet Explorer, Temp, Local, LocalLow, $Recycle.bin, boot, i۳۸٦, st_v۲, intel, recycle, ۳٦۰rec, ۳٦۰sec, ۳٦۰sand, internet explorer, msbuild

واضح است که 360rec, 360sec, 360sand توسط ۳٦۰ Qihoo، که یک شرکت امنیتی مستقر در چین است، توسعه یافته‌اند. به طور مثال آنتی ویروس ۳٦۰ Total Security یکی از محصولات این شرکت می‌باشد. بنابراین احتمال اینکه توسعه دهندگان باج افزار، چینی باشند وجود دارد.

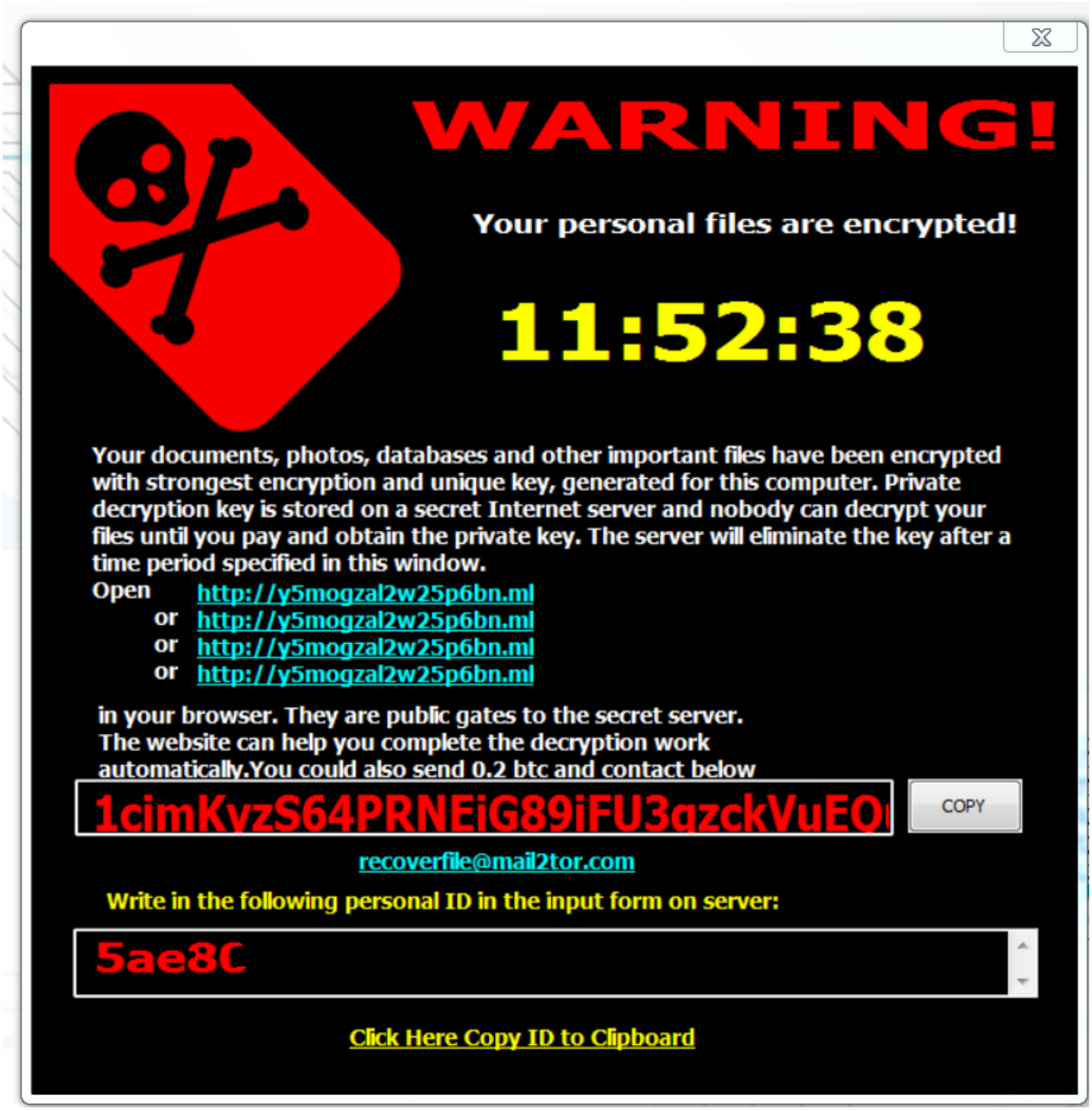
باج‌افزار مورد اشاره یک کلید عمومی RSA را به صورت زیر تعریف می کند.

MIGJAoGBAIOYf0KqEOGaxdLmMLypMyZ1q/K+r6DuCdYpwZfs0EPug3ye7UjZa0QMOP5/OySrl/uBJtkmEghEtUEo/zfcBJ7332O1ytJ7/ebIUv+ZcN1Rlswzdv7uZxYRC8u1HvrgBvAz4Atbzx+FbFVqLB0gGixYTqbjqANq21AR6r91+oJtAgMBAAE=

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.

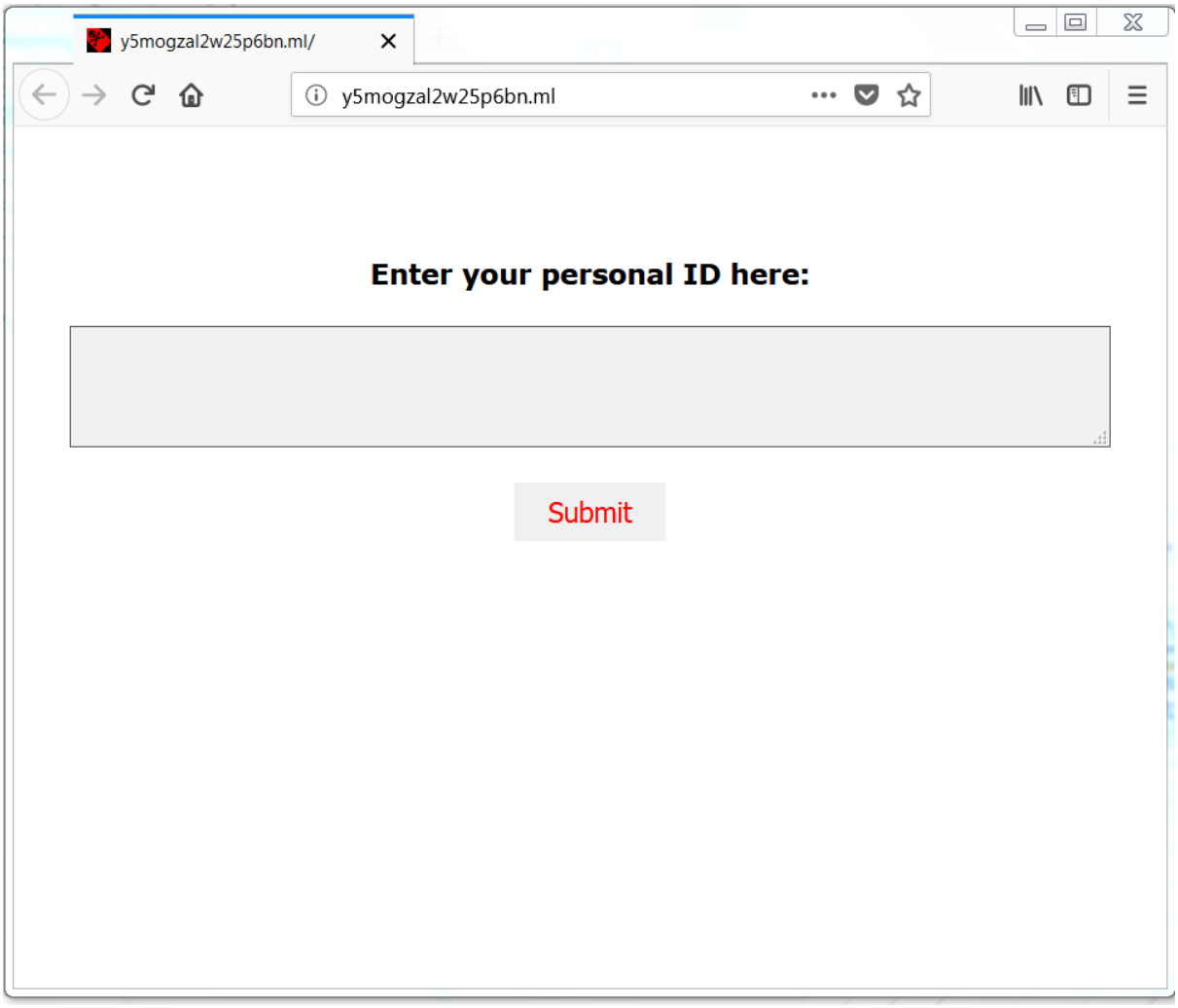


همانطور که در تصویر نیز قابل مشاهده است، پسوند تمام فایل‌ها پس از رمزگذاری، به ".encry" تغییر پیدا می‌کند و یک فایل به نام !HELP_YOUR_FILES با فرمت HTML ایجاد می‌شود که شامل پیغام باج‌خواهی می‌باشد. در تصویر زیر پیغام باج‌خواهی باج‌افزار Iron را مشاهده می‌کنید.



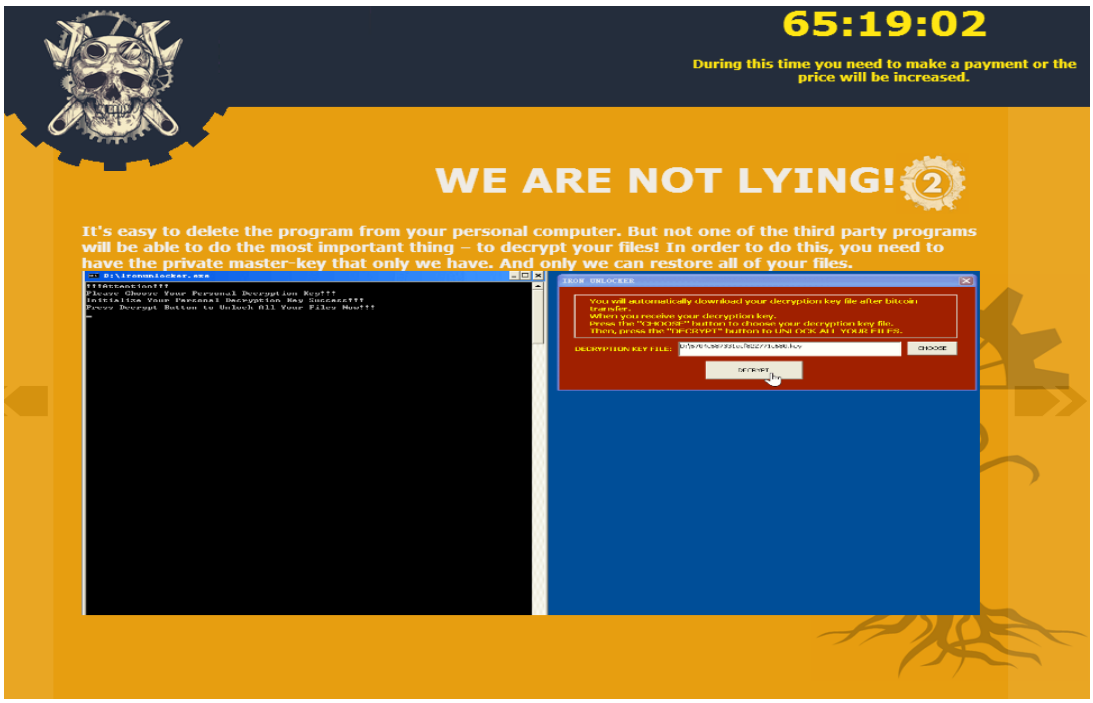
بر اساس پیغام باج‌خواهی، فایل‌ها با یک کلید قوی و مخصوص که برای سیستم قربانی تولید شده است، رمزگذاری شده و کلید خصوصی جهت رمزگشایی فایل‌ها بر روی یک سرور مخفی به آدرس http://y5mogzal2w25p6bn.ml در اینترنت ذخیره شده است، که قربانیان برای دریافت کلید رمزگشایی فایل‌ها باید به آن مراجعه نمایند. قربانی برای ورود به این وب سایت باید شناسه مربوط به خود که در انتهای پیغام باج‌خواهی آمده است را وارد نماید. مهاجمین اعلام نموده‌اند که قربانی می بایست مبلغ ۰.۲ بیت‌کوین را به کیف پول بیت‌کوین 1cimKyzS64PRNEiG89iFU3qzckVuEQuUj 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 باج خواهی قرار داده است.

تصاویر مربوط به درگاه پرداخت باج‌افزار Iron را در زیر مشاهده می‌نمایید.

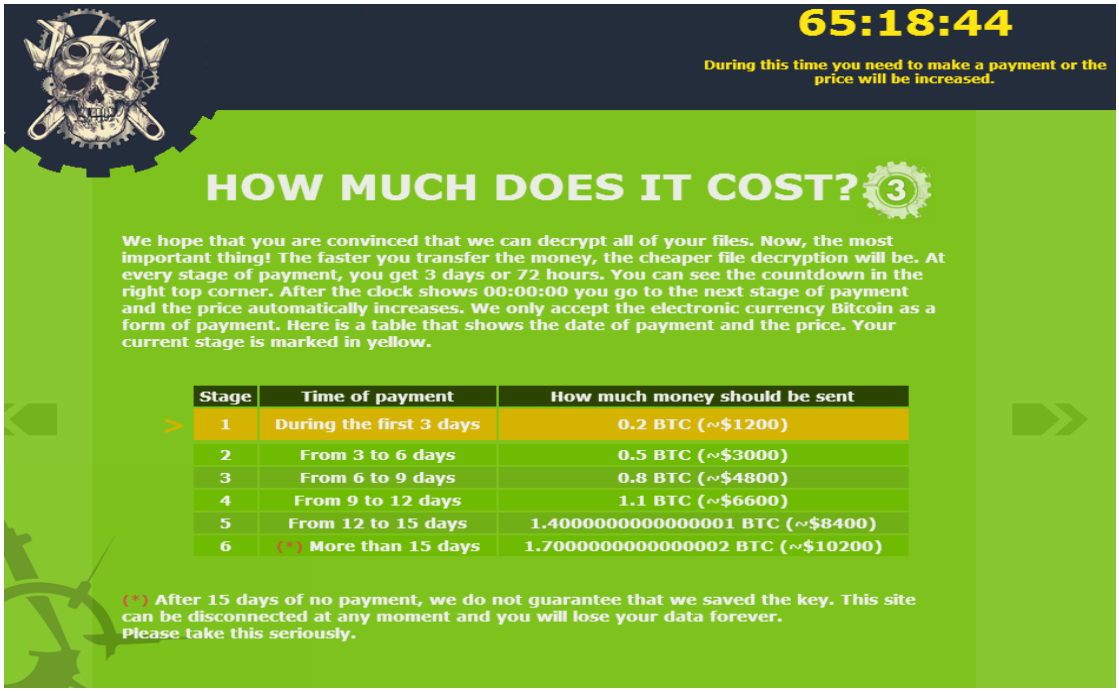


قربانی پس از مراجعه به وب سایتی که اشاره شد باید در کادر مربوطه، شناسه خود را وارد نماید و بر روی دکمه‌ی Submit کلیک نماید. پس از ورود، پیغام‌های زیر به قربانی نمایش داده می‌شود :

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.



در پیغام سوم با این عنوان که "چه مقدار باج باید پرداخت شود؟" مهاجم اعلام می‌کند که طبق جدول موجود، مهلت پرداخت شامل چند مرحله می‌باشد که در صورت پایان مهلت پرداخت، وارد مرحله‌ی بعدی شده و مبلغ باج نیز افزایش خواهد یافت. طبق این جدول قربانی هر چه سریعتر مبلغ باج را پرداخت نماید کمتر ضرر می‌کند. 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 فایل‌های رمزگذاری شده برای همیشه از بین بروند.

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 می‌کشد تا ابزارهای لازم برای رمزگشایی فایل‌ها در اختیار قربانی قرار گیرد. در ادامه، مبلغ باج، آدرس کیف پول بیت‌کوین و ابزارهای رمزگشایی فایل‌ها که پس از پرداخت فعال می‌شوند، قرار گرفته‌اند. نکته‌ای که در این‌جا می‌توان به آن اشاره نمود آدرس کیف پول بیت‌کوین می‌باشد که با آدرسی که در پیغام باج‌خواهی وجود دارد متفاوت است.

اما در پیغام پنجم، آدرس وب سایت‌هایی جهت تهیه بیت‌کوین قرار داده شده است.

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا:

پس از بررسی کدمنبع باج‌افزار نتایج زیر حاصل گردید :

همانطور که پیش‌تر نیز اشاره شد، کدمنبع این باج‌افزار شباهاتی با کدمنبع باج‌افزار Satan دارد. طبق بررسی‌های انجام شده نحوه‌ی رمزگذاری فایل‌ها توسط دو باج‌افزار با یکدیگر متفاوت است، اما تشابهاتی در لیست فایل‌هایی که مورد هدف قرار می‌دهند بین دو باج‌افزار مشاهده شده است که در تصویر زیر قابل مشاهده می‌باشد.

Iron ransomware

```
lea     eax, [esp+18h+arg_28]
push    offset aBoot    ; "boot"
push    eax
call    sub_48677A
pop     ecx
pop     ecx
test    eax, eax
jz      loc_40AAB7
```

```
lea     eax, [esp+18h+arg_28]
push    offset aI386    ; "i386"
push    eax
call    sub_48677A
pop     ecx
pop     ecx
test    eax, eax
jz      loc_40AAB7
```

```
lea     eax, [esp+18h+arg_28]
push    offset aStV2    ; "st_v2"
push    eax
call    sub_48677A
pop     ecx
pop     ecx
test    eax, eax
jz      loc_40AAB7
```

```
lea     eax, [esp+18h+arg_28]
push    offset aIntel   ; "intel"
push    eax
call    sub_48677A
pop     ecx
pop     ecx
test    eax, eax
jz      loc_40AAB7
```

Satan ransomware

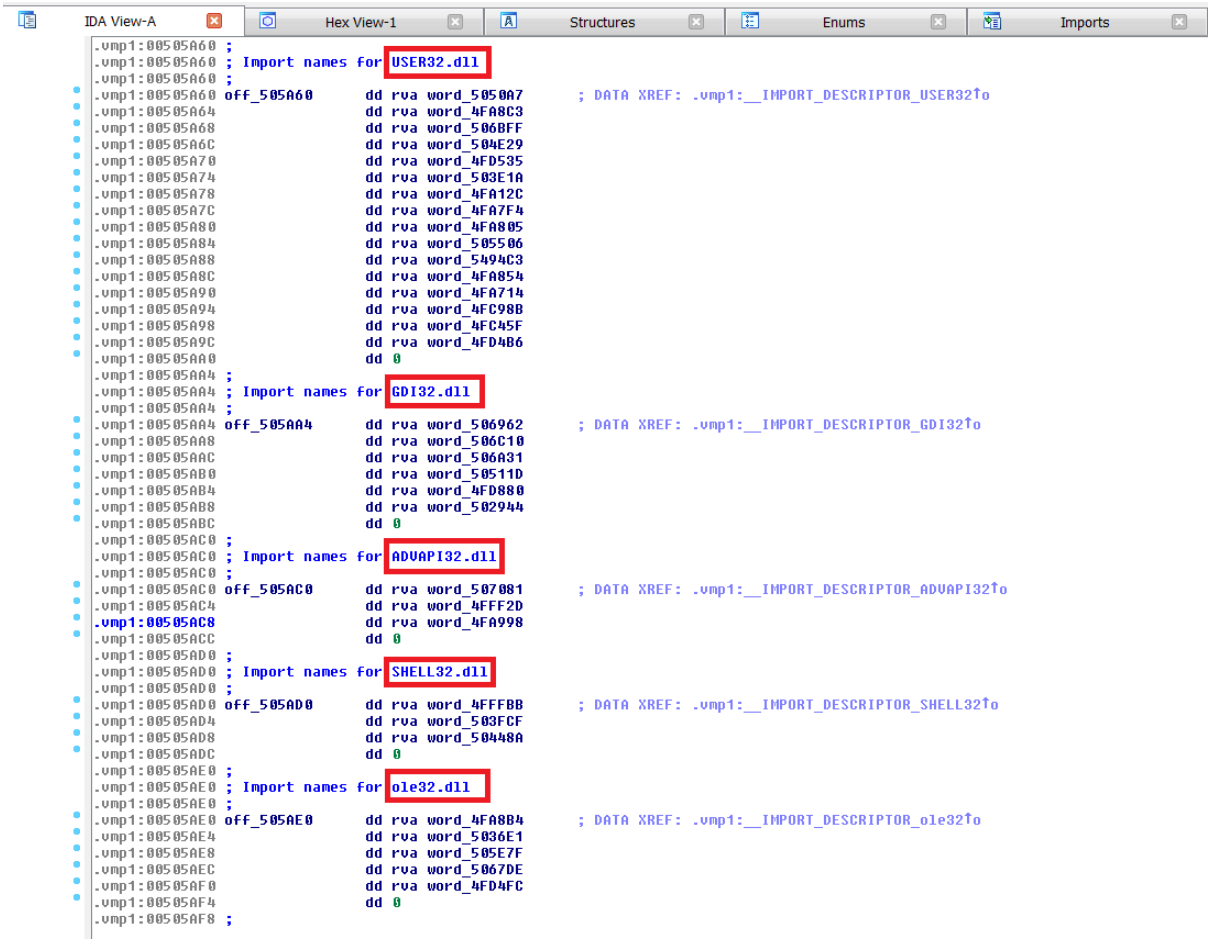
```
push    offset aBoot    ; "boot"
push    esi
call    sub_418F10
add     esp, 8
test    eax, eax
jnz     loc_408CB5
```

```
push    offset aI386    ; "i386"
push    esi
call    sub_418F10
add     esp, 8
test    eax, eax
jnz     loc_408CB5
```

```
push    offset aStV2    ; "st_v2"
push    esi
call    sub_418F10
add     esp, 8
test    eax, eax
jnz     loc_408CB5
```

```
push    offset aIntel   ; "intel"
push    esi
call    sub_418F10
add     esp, 8
test    eax, eax
jnz     loc_408CB5
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند. در تصویر زیر که مربوط به کدمنبع باج‌افزار Iron می‌باشد کاربرد این کتابخانه‌ها به خوبی قابل مشاهده است. همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه متن آمده است.



WINHTTP.dll	USER۳۲.dll	USER۳۲.dll	USER۳۲.dll
WinHttpCloseHandle WinHttpQueryHeaders	SendMessageA SetClipboardData SetDlgItemTextA SetWindowLongA SetWindowPos wsprintfA	CloseClipboard DialogBoxParam W EmptyClipboard GetDlgCtrlID GetDlgItem	GetProcessWindowStation GetSysColorBrush GetUserObjectInformation W MessageBoxA OpenClipboard

ADVAPI۳۲.dll	GDI۳۲.dll	ole۳۲.dll	SHELL۳۲.dll	WS۲_۳۲.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 GetTickCount GlobalAlloc GlobalLock GlobalMemoryStatus GlobalUnlock HeapAlloc HeapFree HeapReAlloc HeapSize InitializeCriticalSectionAndSpinCount InitializeSListHead IsDebuggerPresent IsProcessorFeaturePresent IsValidCodePage LCMapStringW LeaveCriticalSection LoadLibraryA LoadLibraryExW LocalAlloc LocalFree	CloseHandle CompareStringW CreateEventW CreateFileW CreateMutexA DecodePointer DeleteCriticalSection EncodePointer EnterCriticalSection ExitProcess FindClose FindFirstFileExA FindNextFileA FlushConsoleInputBuffer FlushFileBuffers FreeEnvironmentStringsW FreeLibrary GetACP GetCommandLineA GetCommandLineW GetConsoleCP	RaiseException ReadConsoleInputA ReadConsoleW ReadFile ReleaseMutex ResetEvent RtlUnwind SetConsoleCtrlHandler SetConsoleMode SetEndOfFile SetEnvironmentVariableA SetEvent SetFilePointerEx SetLastError SetStdHandle SetUnhandledExceptionFilter Sleep TerminateProcess	GetCurrentThreadId GetEnvironmentStringsW GetFileAttributesExW GetFileType GetLastError GetModuleFileNameA GetModuleFileNameW GetModuleHandleA GetModuleHandleExW GetModuleHandleW GetOEMCP GetProcAddress GetProcessHeap GetStartupInfoW GetStdHandle GetStringTypeW QueryPerformanceCounter	UnhandledExceptionFilter VirtualFree VirtualQuery WaitForSingleObjectEx WideCharToMultiByte WriteConsoleW WriteFile TlsFree TlsGetValue TlsSetValue GetCPInfo GetCurrentProcess GetCurrentProcessId MoveFileExW MultiByteToWideChar TlsAlloc GetConsoleMode

نتایج حاصل از تحلیل ها نشان می دهد، کد باج‌افزار Iron کاملا منحصر به فرد است و مانند یک باج‌افزار کاملا جدید به نظر می‌رسد و این امکان نیز وجود دارد که یک پروژه جانبی توسط توسعه‌دهندگان باج‌افزار Satan باشد. با این حال، به طور قطع نمی‌توان گفت که چه کسی یا گروهی توسعه دهنده این باج‌افزار است.

بر اساس بررسی‌های صورت گرفته، باج‌افزار Iron پس از اجرا، ۱۳ فرایند را ایجاد می‌کند، کـه ایـن فراینـدها طبق لیست زیر می‌باشند :

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/

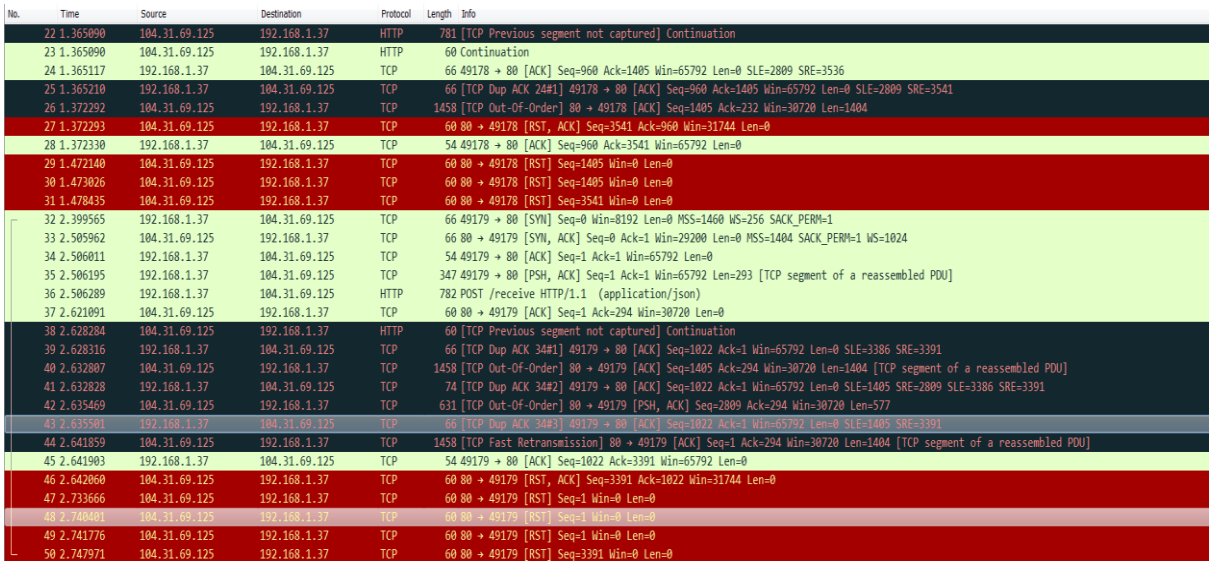
iexplore.exe SCODEF:۴۵۶۰ CREDAT:۲۷۵۴۵۷ /prefetch:۲

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	2.635501	192.168.1.37	104.31.69.125	TCP	66	[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.

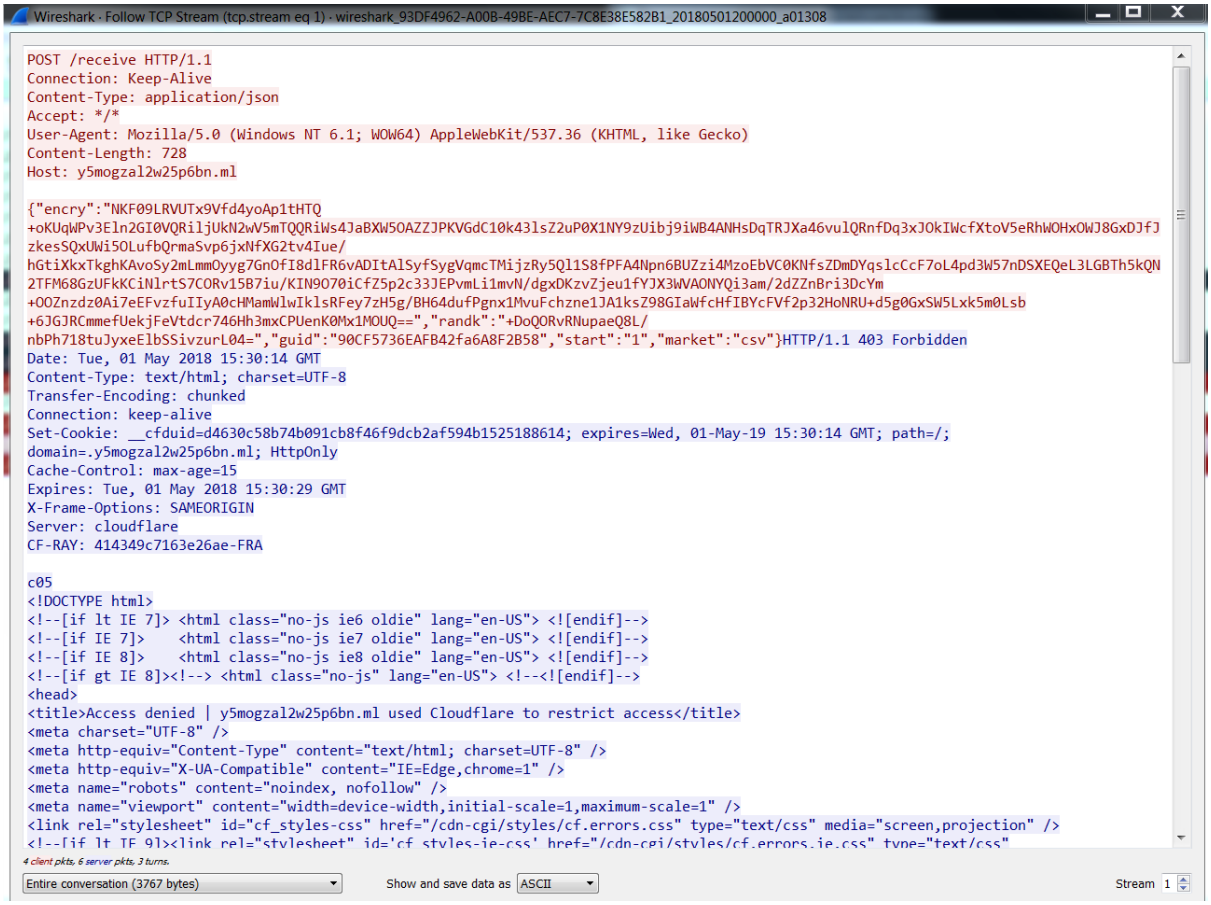
کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۱۰٤.۳۱.٦۹.۱۲۵	y۵mogzal۲w۲۵p٦bn.ml
ایالات متحده امریکا	٦۷.۲۱۵.۹۲.۲۱۵	myip.dnsomatic.com

از بین موارد فوق، آی پی ۱۰٤.۳۱.٦۹.۱۲۵ ، 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 باج‌افزار Iron پس از حمله، آی‌پی سیستم قربانی را مشخص کرده و یک درخواست ارسال بسته را به سرور C&C ارسال می‌نماید.



به نظر می‌رسد باج‌افزار Iron برای هر سیستمی که رمزگذاری می‌کند، یک کد شناسایی اختصاص می‌دهد تا دوباره آن سیستم را مورد حمله قرار ندهد. این باج‌افزار مقادیر زیر را به سرور C&C ارسال می نماید.

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

- Randk (seed)
- Market (unknown)

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش، تعداد ۴۷ مورد از ٦٦ آنتی‌ویروس معتبر دنیا قادر به تشخیص آلودگی این باج‌افزار در سامانه VirusTotal شده‌اند.

Ad-Aware	Trojan.GenericKD.40187953	AegisLab	Troj.Ransom.W32.Gen!c
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
Bkav	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