باسمه تعالی

تحلیل فنی باج افزار Dont_Worry

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار Dont_Worry خبر می‌دهد که پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به <random_ID> -UPS. تغییر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در روز بیستم ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران روسی زبان می‌باشد. والد باج‌افزار Dont_Worry ، باج‌افزار Crypto_Lab می‌باشد، همچنین طبق بررسی‌های انجام شده، برخی از کارشناسان این نسخه از باج‌افزار را نسخه‌ی جدیدی از باج‌افزار Russenger تشخیص داده‌اند، در زیر ریشه‌یابی خانواده‌ی این باج‌افزار قابل مشاهده می‌باشد :

AMBA >> Crypto_Lab > Dont_Worry

این باج‌افزار از الگوریتم‌های رمزنگاری RSA و AES برای رمزگذاری فایل‌ها استفاده می‌کند و فایل‌هایی با پسوندهای خاص را رمزگذاری می‌نماید.

مشخصات فایل اجرایی :

نام فایل	Dont_Worry.exe
MD۵	٤df٨٤٦٠a٤٤٩٦٢٨٠ac١٢٢٢١٥aa٣٩fce٤d
SHA-١	e٣٢٢ee٢٧٤٤٢d١٠c٢٠٧١٢٤eefab٩٤٤٥e٢٩aa٧٧b٩٨
SHA-٢٥٦	٩a٥٢٢b٣b٥a٥١b٥e٠٢١٩٧٧ad٥٥٧٨٠f٥٢٧d٥٨١٩٣d٥٨٧b١c٠١٥٨٨e٠٧cc٤٠a٦٩f٨٨٤
اندازه فایل	٢.٥٢ MB

فایل اجرایی این باج افزار دارای ۹ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.١٨	٤٠٩٦	١٩٢٤٧٥٢	١٩٢٥١٢٠
.data	٢.٢٦	١٩٢٩٢١٦	١٢٣٦٤	١٢٨٠٠
.rdata	٥.٦٨	١٩٤٥٦٠٠	٢٥٣٦٣٢	٢٥٣٩٥٢
.eh_fram	٤.٩	٢١٩٩٥٥٢	٤٣٧٤٠٤	٤٣٧٧٦٠
.bss	٠	٢٦٣٧٨٢٤	٤١٧٦٠	٠
.idata	٥.١٨	٢٦٨٢٨٨٠	٥٧٤٨	٦١٤٤
.CRT	٠.٣٤	٢٦٩١٠٧٢	٥٦	٥١٢

.tls	۰.۲۱	۲۶۹۵۱۶۸	۳۲	۵۱۲
.rsrc	٤.۷	۲۶۹۹۲٦٤	۱۳۲۸	۱۵۳٦

تحلیل پویا :

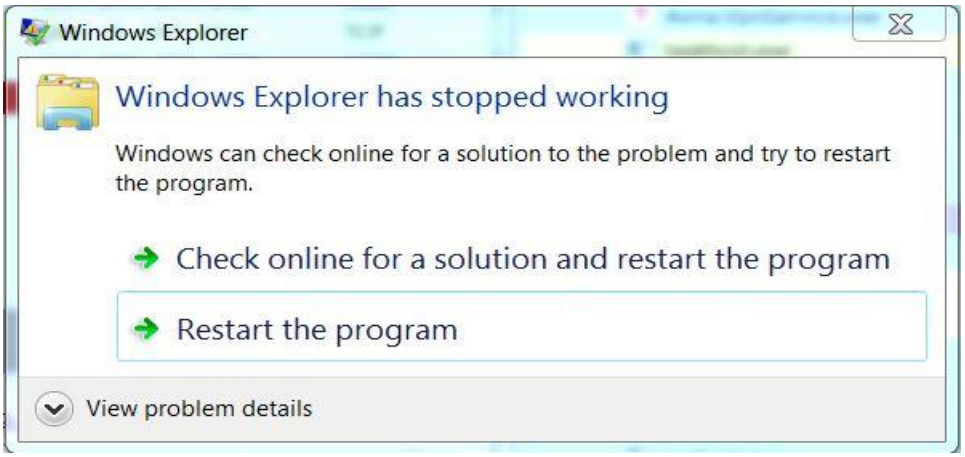
برای بررسی عمیق‌تر باج‌افزار Dont_Worry، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا، شروع به رمزگذاری فایل‌ها می‌کند و پس از اتمام فرایند رمزگذاری، فایلی با نام Dont_Worry.txt در کنار فایل‌های رمزگذاری شده و بر روی Desktop ایجاد می‌کند که شامل پیغام باج‌خواهی می‌باشد و قربانیان جهت رمزگشایی فایل‌ها باید از طریق آدرس ایمیل ups@torbox۳uiot٦wchz.onion با مهاجمین ارتباط برقرار نمایند.

همانطور که اشاره شد این باج‌افزار از الگوریتم‌های رمزنگاری RSA و AES برای رمزگذاری فایل‌ها استفاده می‌کند و فایل‌هایی با پسوندهای زیر را رمزگذاری می‌کند.

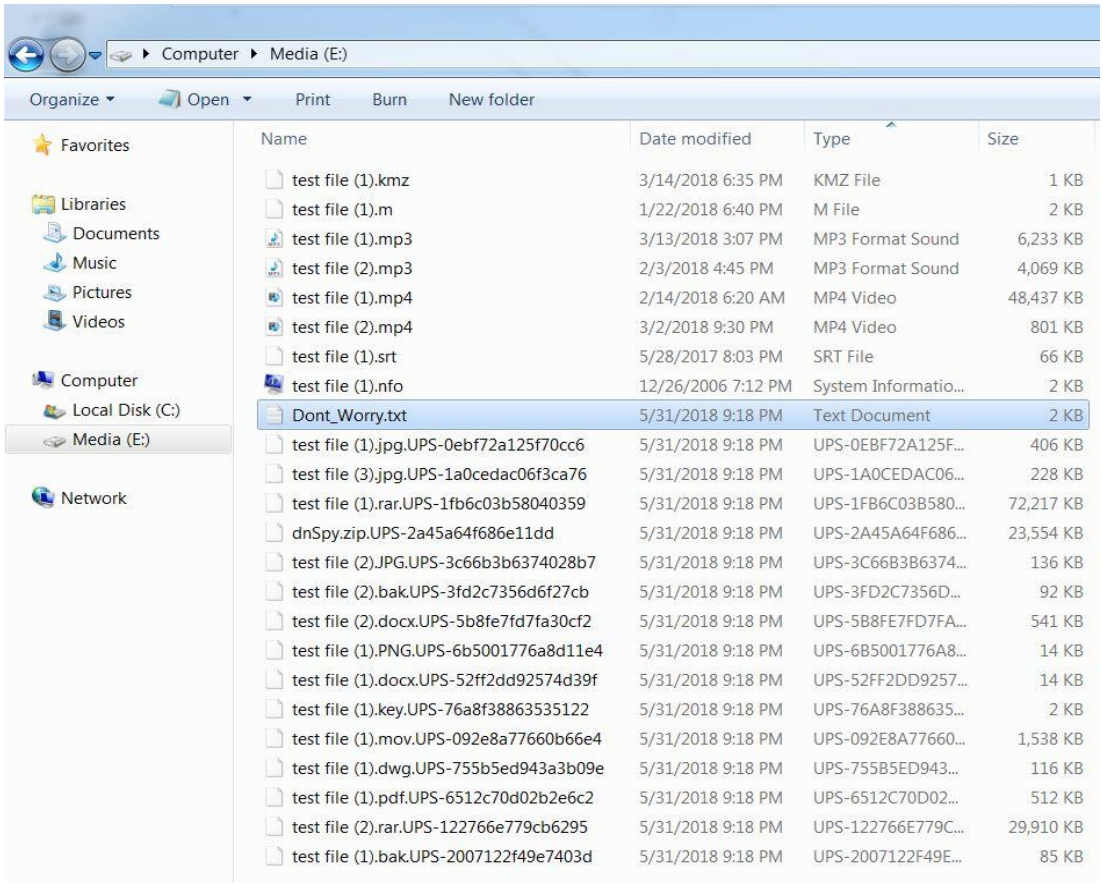
Windows, .tar, .gzip, .tgz, .arj, .jpg, .jpeg, .xls, .xlsx, .rtf, .pdf, .djvu, .efd, .txt, .mdb, .cer, .p۱۲, .pfx, .kwm, .pwm, .md, .dbf, .dd, .cfu, .erf, .epf, .dt, .ifo, .lnk, .cbu, .mov, .m۲v, .dbx, .bln, .dic, .tpl, .a۲u, .mcx, .key, .mkd, .bkc, .wav, .tbh, .tbc, .tbb, .tbn, .rst, .sel, .pas, .ib, .ods, .ppd, .pln, .plan, .gdoc, .px, .abd, .flx, .srx, .tbi, .his, .dfp, .packed, .map, .vmem, .zsp, .bpl, .۱cl, .bac[۰-۹], .tbk, .lzh, .udb, .۷zip, .bls, .rbf, .bdf, .bde, .vbe, .vbk, .dbk, .bks, .frm, .myd, .myi, .php, .vrd, .nbk, .bip, .qib, .cbf, .info, .wbverify, .ldb, .lgd, .edb, .vsv, .avhd, .vmss, .eml, .msf, .ndf, .dcm, .stm, .vdi, .bz۲, .xlsb, .pml, .idx, .lbl, .lvd, .prv, .tmp۰, .cpr, .bf, .svp, .ogd, .rdf, .frx, .dot, .rpt, .pm, .ctl, .gbp, .sfpz, .ddf, .str, .۹tr, .۸tr, .۸t۰, .upd, .ndt, .pbf, .one, .onetoc۲, .rpb, .dgdat, .fkc, .dbt, .eso, .esl, .mac, .sgn, .pbd, .sst, .shd, .bco, .vib, .vbm, .prb, .als, .sqx, .nag, .vpc, .pkr, .skr, .mdx, .prk, .rvs, .iv۲i, .v۲i, .gfo, .gfr, .gfd, .tst, .sdf, .qst, .nef, .gpd, .dsus, .oxps, .ai, .esbak, .mbox, .sbk, .dis, .dcf, .xch, .utf, .sbp, .sqlite, .ans, .twd, .cbm, .rez, .mdt, .mdw, .blk, .vmsn, .vmpl, .sac, .sacx, .ssd, .sln, .tdb, .dbs, .diff, .q۱c, .out, .scx, .tnx, .klt, .~klt~۲, .ctlg, .sem, .hive, .fld, .imm, .vrfs, .req, .pwd, .meb, .laccdb, .bck, .ssf, .jrs, .drs, .dtz, .fob, .pfi, .wrk, .vsd, .sbin, .atc, .atg, .py, .shdb, .sdb, .new, .rk٦, .mak, .v۸i, .۱txt, .irsi, .irss, .snp, .pck, .ips, .xz, .vmrs, .okk, .lic, .lis, .dz, .tid, .a۳d, .custom, .vlx, .lsp, .dcl, .mnc, .mns, .mnr, .lrv, .thm,

.ssp, .spr, .ovf, .repx, .dafile, .n[۰-۹], .nd[۰-۹], .st[۰-۹], .kpm, .trec, .aad, .ipa, .isz, .zup, .data, .wsb, .dct, .etw, .rsz, .rszold, .rse, .stek, .mrimg, .gbr, .webp, .xslt, .p۱۰, .psp, .pslic, .sldprt, .stop, .granit, .wallet, .ytbl, .rr۰d, .doubleoffset, .zip, .rar, .۷z, .gz, .psd, .cdr, .dwg, .max, .bmp, .gif, .png, .doc, .docx, .ppt, .pptx, .htm, .html, .mdf, .iso, .tib, .nrg, .gho, .ghost, .ghs, .bak, .bkp, .bkf, .۱cd, .۲cd, .۱cd۲, .ert, .cf, .cdx, .pfl, .lst, .gdb, .gbk, .fdb, .fbk, .ldf, .sql, .odt, .rn, .zrb, .eif, .pgd, .trn, .nbi, .res, .hbk, .eps, .indd, .bpn, .blf, .ldw, .box, .frw, .pst, .mxl, .xml, .idf, .war, .tab, .nbr, .hdf, .rcf, .lgp, .lgf, .elf, .pgp, .frf, .vhd, .frp, .gsheet, .hbi, .svc, .dmp, .accdb, .csv, .arc, .mb, .xg۰, .yg۰, .db, .backup, .vmdk, .mxlz, .export, .wbcat, .cdb, .ima, .imh, .vbx, .jbc, .sqm, .cfl, .tmp, .mig, .apc, .vhdx, .wim, .cuc, .mft, .tbl, .adb, .car, .ver, .nvram, .vmx, .vmxf, .tmf, .dump, .old, .pf, .pak, .local, .rec, .ifs, .xsd, .dpr, .dproj, .dcu, .fpf, .ps۱, .saved, .save, .bf۳, .rep, .apk, .sct, .fxp, .vct, .fpt, .prg, .vcx, .xxx, .ora, .sfpe, .pl, .scn, .ord, .fil, .ect, .ava, .۱ey, .mde, .wnw, .vvr, .dfb, .dff, .rsu, .gsn, .pdt, .vdb, .ddt, .٦tr, .pkg, .trc, .lg, .sv۲i, .psl, .pfm, .xsc, .xstk, .qrp, .xlsm, .grd, .bcp, .mod, .mdmp, .shs, .viprof, .ost, .vmp, .arch, .vmsd, .kdc, .sob, .sobx, .smf, .smfx, .plb, .vswp, .nsf, .adi, .md٥, .gd, .sdl, .lky, .burn, .ntx, .bz, .ldif, .kmn, .pka, .img, .fbf, .nc, .last, .~ini, .shdl, .mtl, .profile, .amr, .ppsx, .irsf, .fi, .tps, .avhdx, .vmcx, .awr, .unf, .ok, .vvv, .apx, .cmt, .obf, .afd, .pnl, .nif, .cnc, .lay٦, .cui, .cuix, .keg, .ifm, .efm, .btr, .sna, .blb, .amp, .rgt, .bg, .arh, .cr۲, .$$$, .[۰-۹]+, .٦t[۰-۹], .fdb[۰-۹]*, .db[۰-۹]*, .imgc, .axx, .wid, .ci, .pa_*, .nex, .bll, .tzp, .otf, .cut, .aod, .ard, .asd, .dpl, .pcoip, .ova, .mf, .swdsk, .ogg, .opq, .rbk, .sedb, .dbtraffic, .vcf, .xfil, .mrk, .con, .gopaymeb, .lock, .ua_, .enc, .crypt, .cripted, .criptfiles, .vault, .enz*

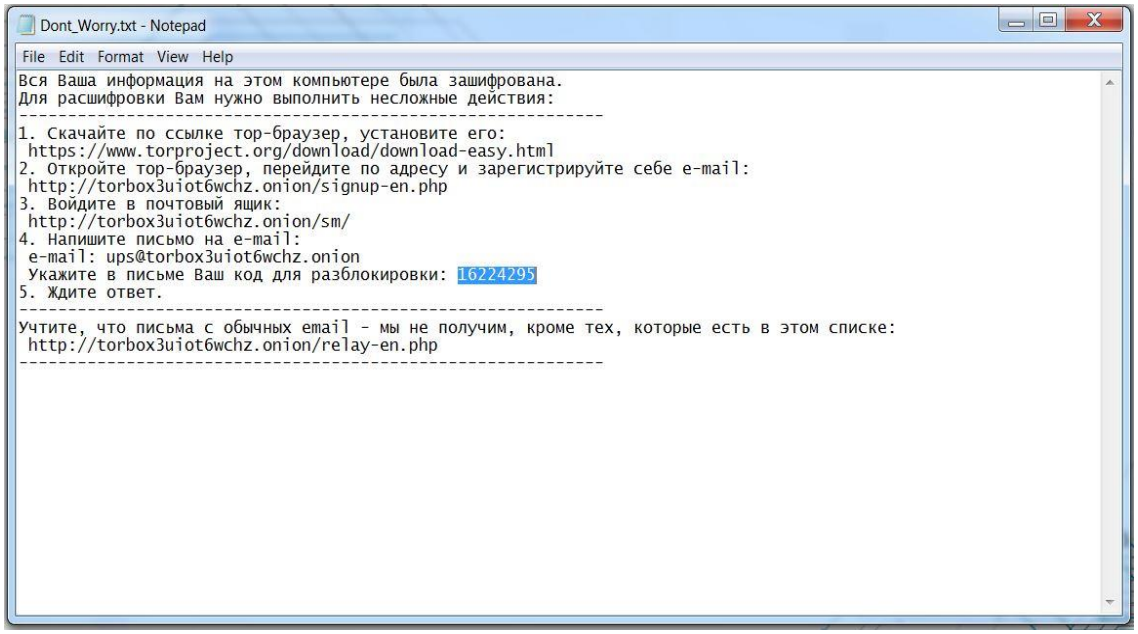
باج افزار در حین اجرا، فعالیت Windows Explorer را متوقف کرده و پیغام زیر به نمایش در می‌آید:



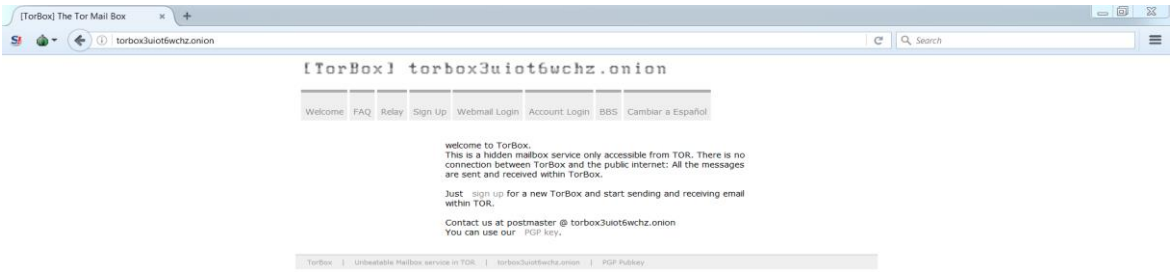
تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.



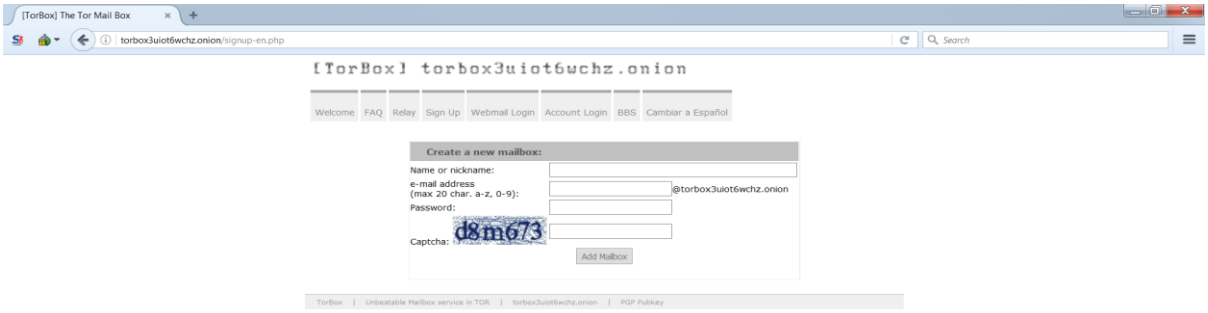
همانطور که در تصویر نیز مشخص است، این باج‌افزار فایل‌هایی با پسوندهای خاص را رمزگذاری می‌کند و یک فایل تحت عنوان Dont_Worry.txt را در دایرکتوری‌های مختلف ایجاد می‌کند که شامل پیغام باج‌خواهی به زبان روسی می‌باشد. همچنین به دلیل رمزگذاری برخی از فایل‌های مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی، ممکن است برخی از آن‌ها قابل استفاده نباشند. تصویر زیر پیغام باج‌خواهی باج افزار Dont_Worry را نشان می‌دهد.



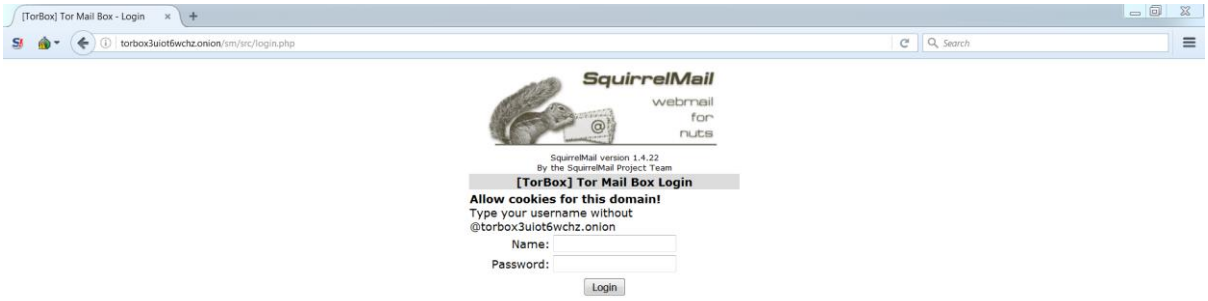
بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید به آدرس http://torbox۳uiot٦wchz.onion در دارک‌وب مراجعه نمایند و یک ایمیل برای خود ایجاد نموده و از طریق ایمیل ایجاد شده با مهاجمین ارتباط برقرار نمایند. آدرس ایمیل مهاجمین جهت برقراری ارتباط با آن‌ها ups@torbox۳uiot٦wchz.onion می‌باشد. تصاویر زیر مربوط به موارد اشاره شده می‌باشد :



تصویر ۱: صفحه وب‌سایت http://torbox۳uiot٦wchz.onion

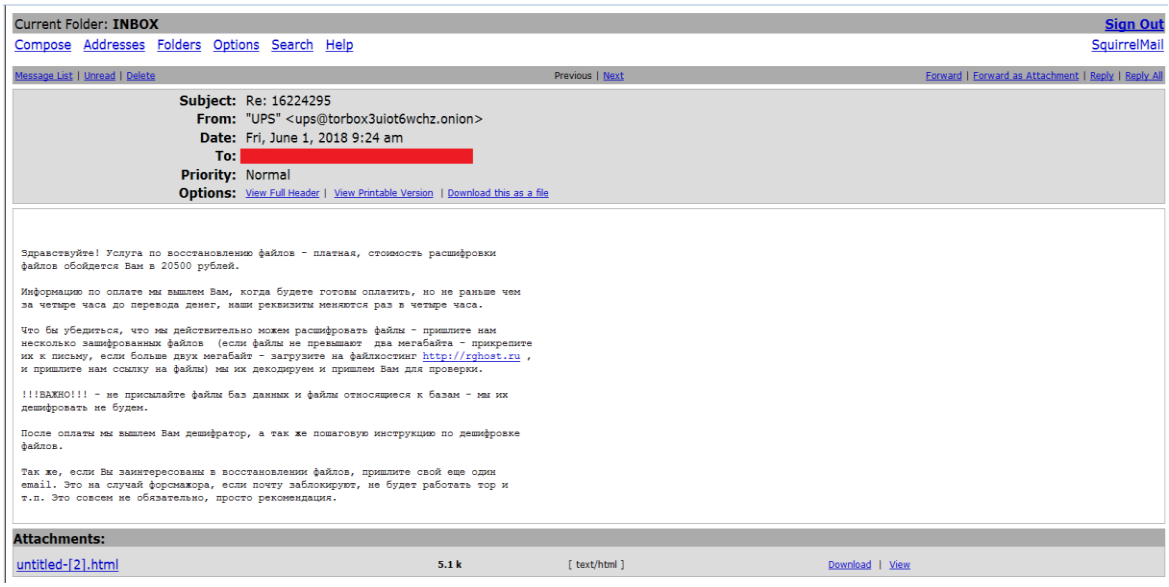


تصویر ۲: صفحه مربوط به ایجاد ایمیل به آدرس http://torbox۳uiotٶwchz.onion/signup-en.php



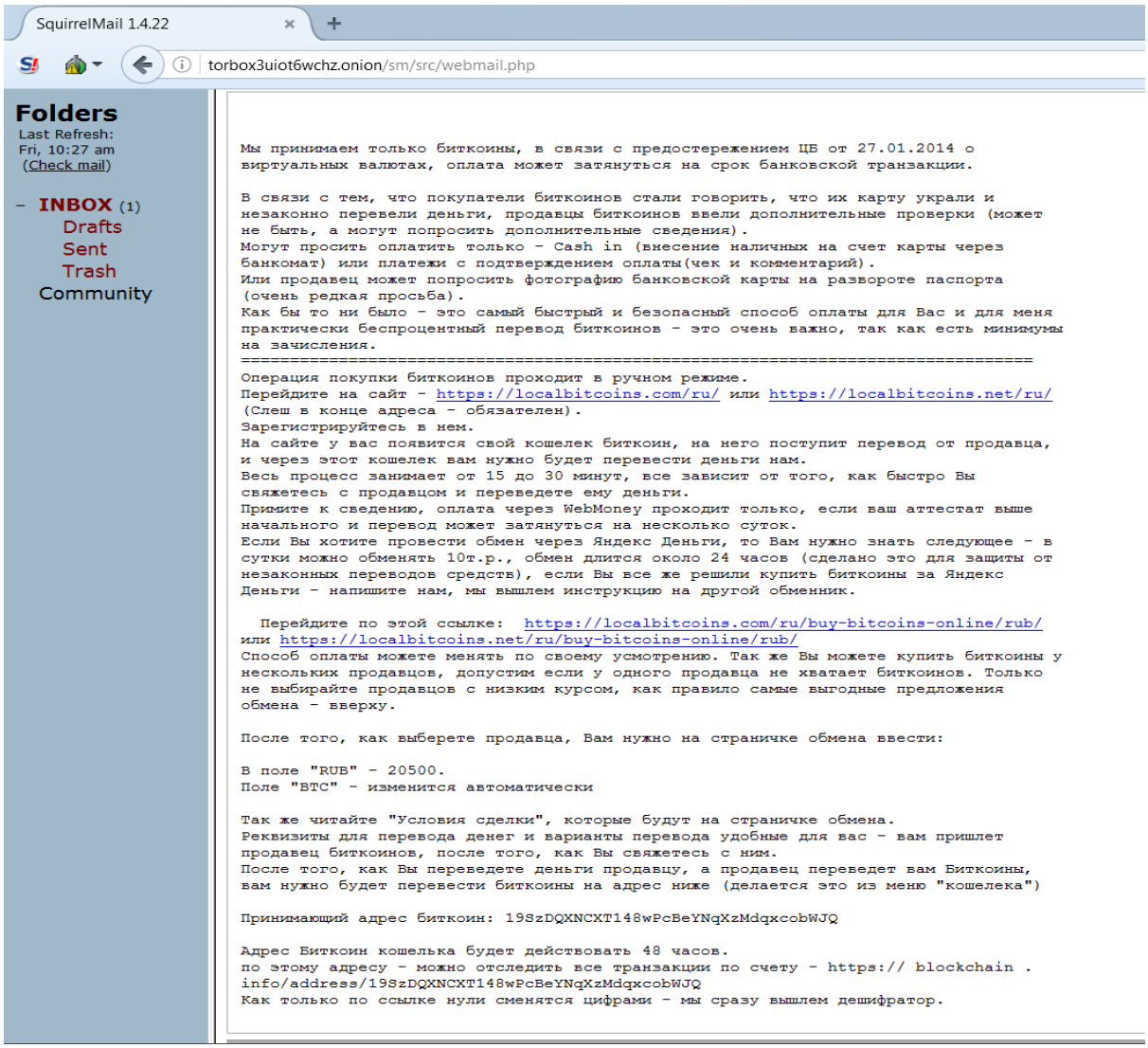
تصویر ۳: صفحه ورود به ایمیل

قربانیان جهت برقراری ارتباط با مهاجمین می بایست کد شناسایی سیستم خود را در قسمت Subject ایمیل وارد نمایند. پس از برقراری ارتباط با مهاجمین به صورت ناشناس، ابتدا از تعداد سیستم‌های رمزگذاری شده توسط باج‌افزار سوال گردید و سپس پیغام زیر را برای ما ارسال شد.

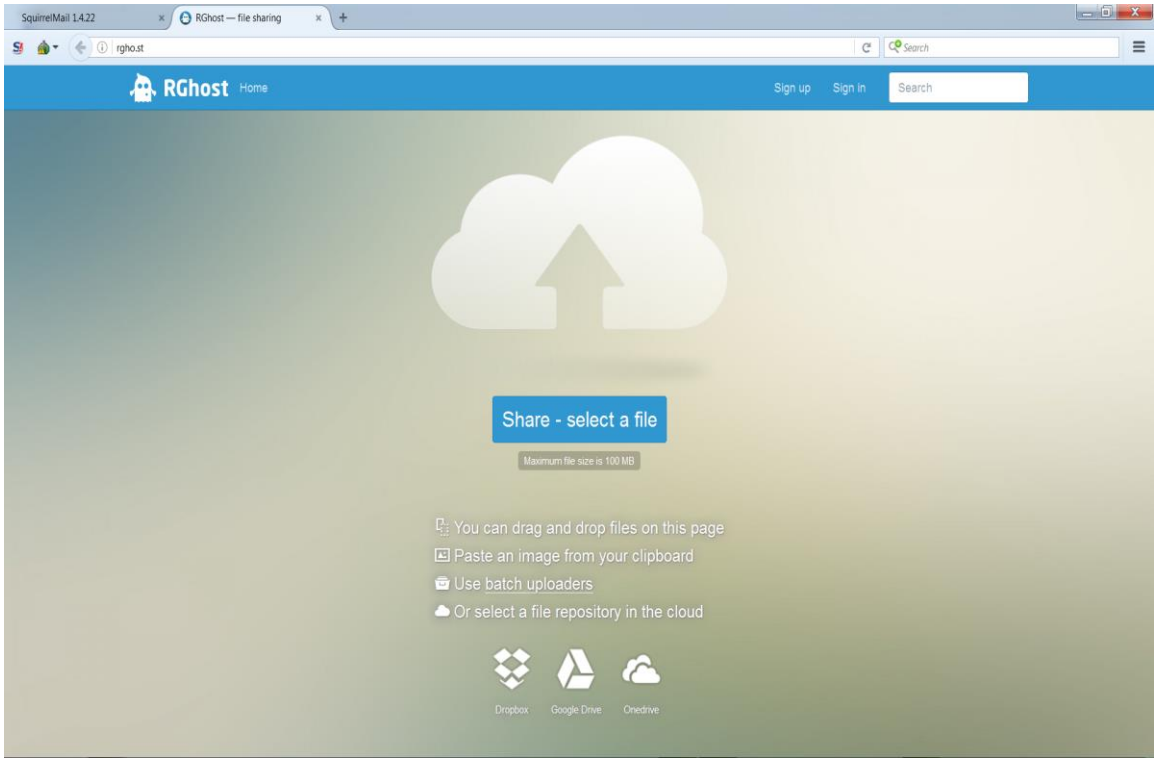


طبق این پیام مبلغ باج، ۲۰۵۰۰ روبل روسیه تعیین شده است و در صورت تمایل، اطلاعات مربوط به نحوه‌ی پرداخت برای قربانیان ارسال خواهد شد. همچنین به منظور جلب اعتماد قربانیان امکان رمزگشایی تعدادی از فایل‌ها قبل از پرداخت مبلغ باج نیز فراهم شده است که قربانیان در صورت تمایل، می‌توانند چند فایل با حداکثر حجم ۲ مگابایت را برای رمزگشایی از طریق وب‌سایت به آدرس http://rghost.ru ارسال نمایند. در ادامه، مهاجمین اطلاعات مربوط به نحوه‌ی پرداخت را برای ما ارسال نمودند. در این پیغام اعلام شده است که مبلغ باج فقط از طریق کیف پول بیت‌کوین به آدرس

۱۹SzDQXNCXT۱٤۸wPcBeYNqXzMdqxcobWJQ برای مهاجمین ارسال گردد. ضمناً ایـن آدرس پـس از مدت زمان ٤۸ ساعت از بین می‌رود. تصاویر زیر مربوط به موارد اشاره شده می‌باشد :

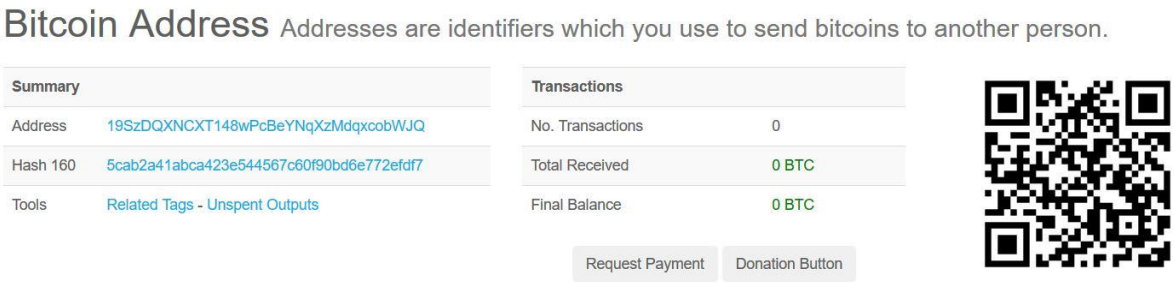


تصویر ۱: اطلاعات مربوط به نحوه‌ی پرداخت

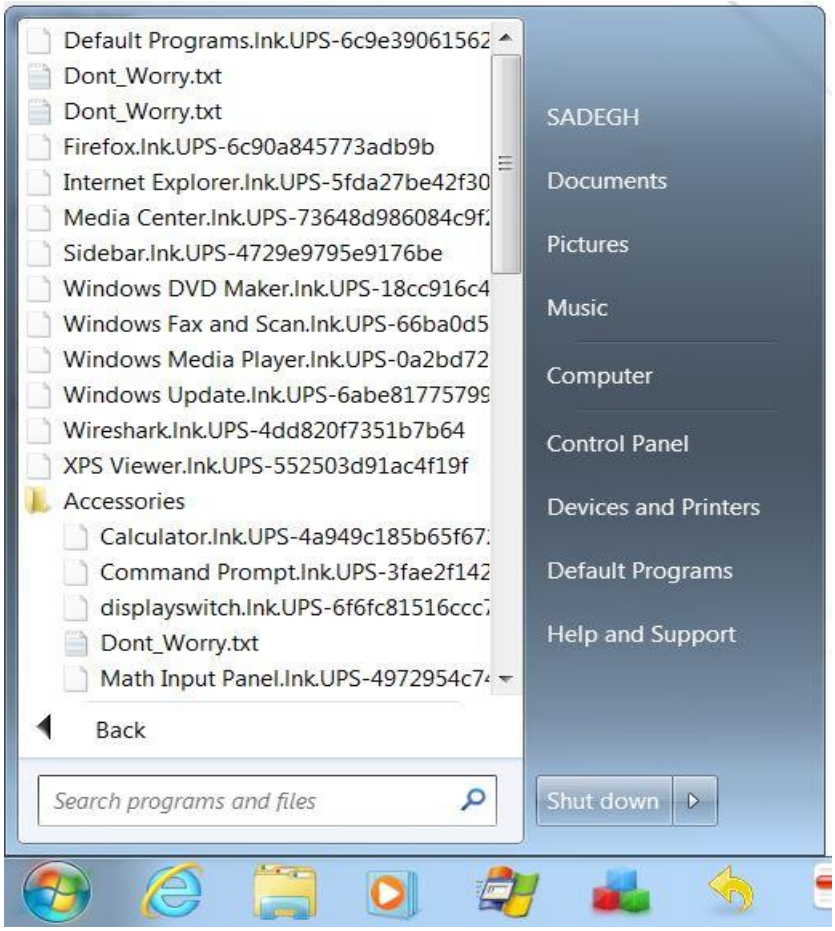


تصویر ۲: صفحه وب‌سایت http://rghost.ru جهت ارسال فایل‌ها

طبق بررسی‌های انجام شده، کیف پول مربوط به این باج‌افزار تاکنون هیچ تراکنشی نداشته است :



این باج‌افزار فایل‌های موجود در Recycle Bin را نیز حذف می‌نماید و تمام ابزارهـای کـاربردی ویـنـدوز را نیز رمزگذاری می‌کند. تصویر زیر مربوط به رمزگذاری ابزارهای کاربردی ویندوز توسط باج‌افزار می‌باشد :

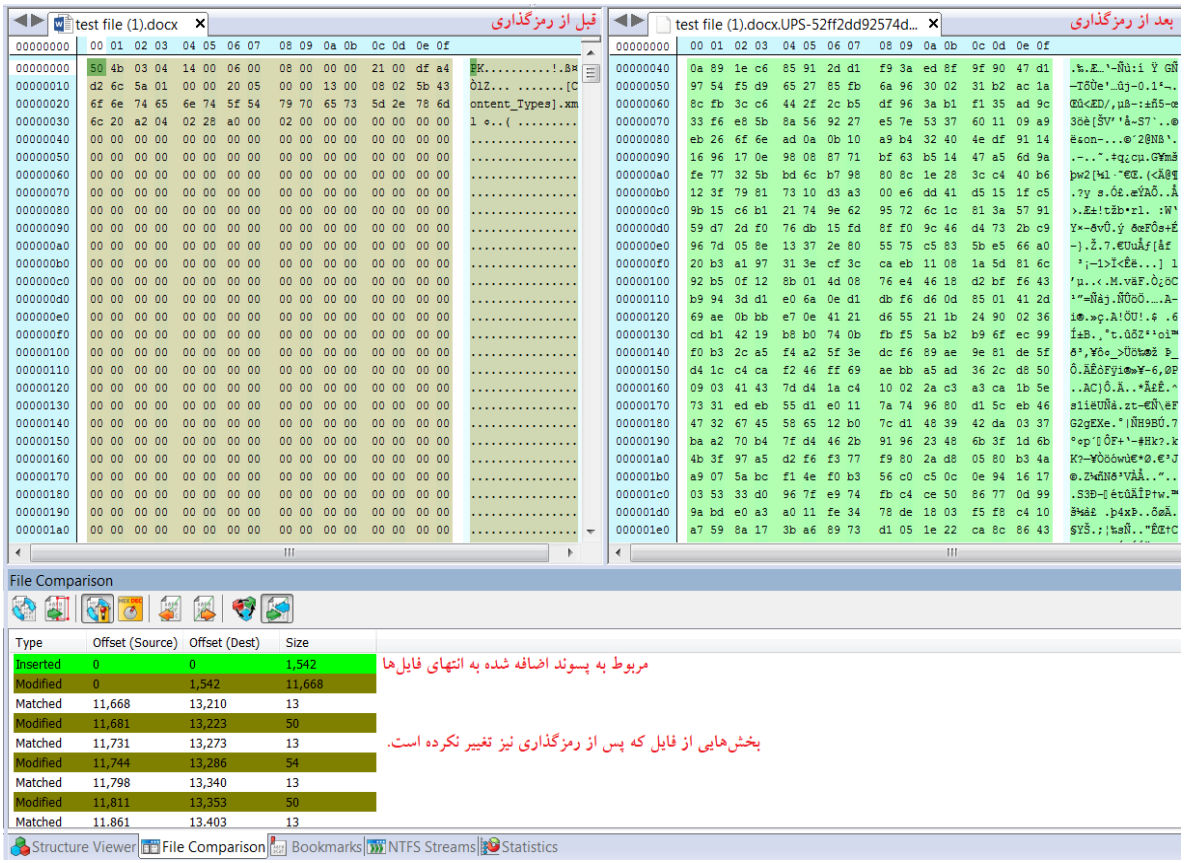


طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا:

پس از تحلیل کد باج‌افزار Dont_Worry به نتایج زیر دست پیدا کردیم.

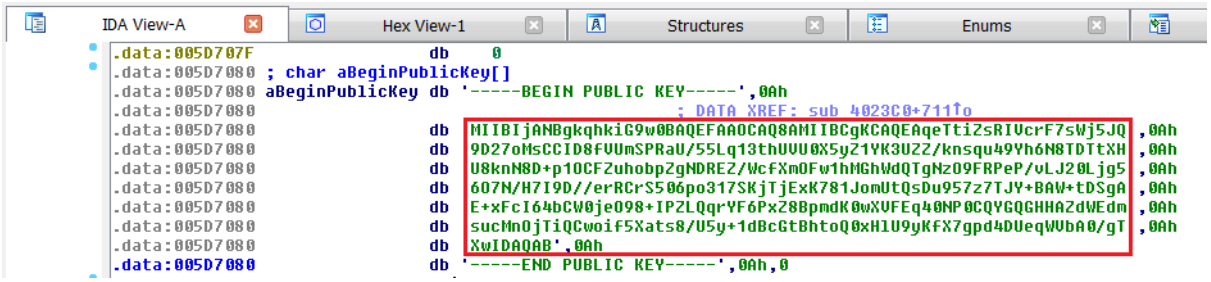
طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری توسط باج‌افزار، انجام دادیم شاهد این بودیم که باج‌افزارDont_Worry ساختار فایل‌ها را پس از رمزگذاری به کلی تغییر نمی‌دهد. نتایج این بررسی‌ها در تصویر زیر قابل مشاهده است.



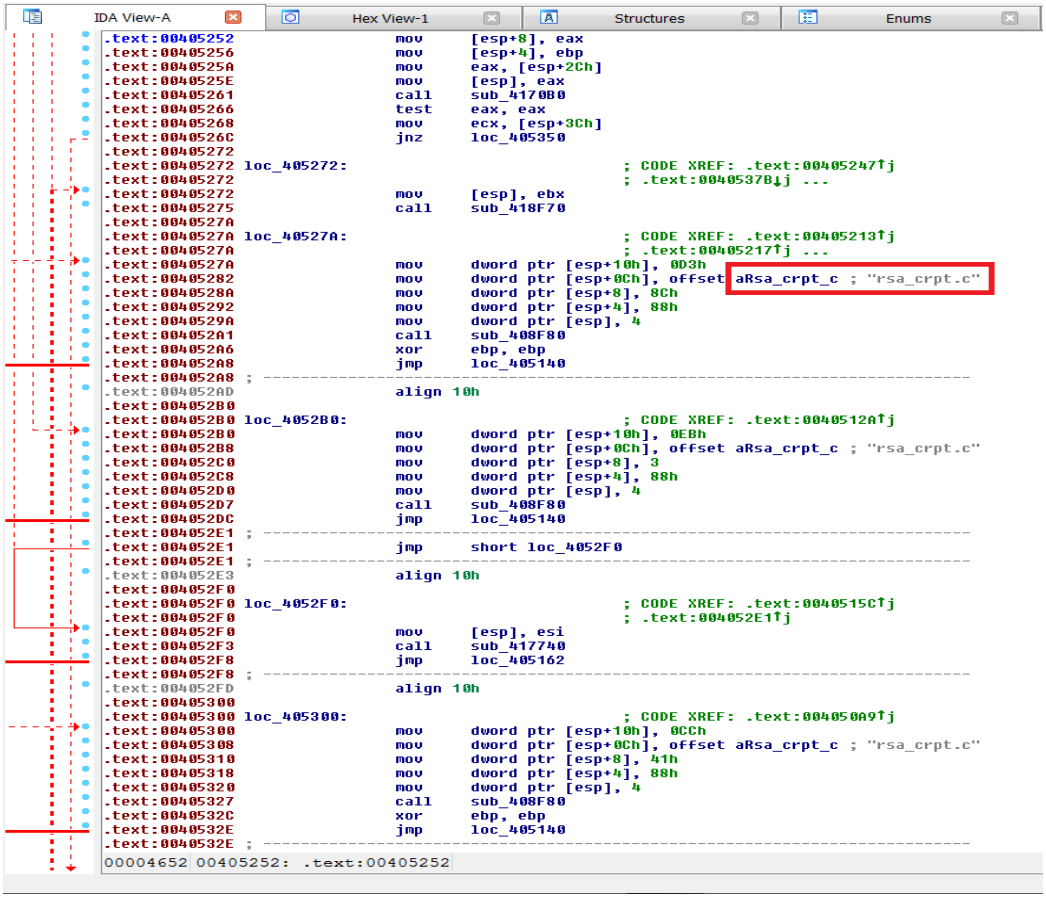
مقدار کلید عمومی باج‌افزار جهت رمزگذاری فایل‌ها در زیر قابل مشاهده می‌باشد.

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqeTtiZsRIVcrF7sWj5JQ9D27oMsCCI
D8fVUmSPRaU/55Lq13thUVU0X5yZ1YK3UZZ/knsqu49Yh6N8TDTtXHU8knN8D+p10CFZuhob
pZgNDREZ/WcfXmOFw1hMGhWdQTgNzO9FRPeP/vLJ20Ljg5670N/H7I9D//erRCrS506po317SK
KjTjExK781JomUtQsDu957z7TJY+BAW+tDSgAE+xFcI64bCW0je098+IPZLQqrYF6PxZ8BpmdK0
wXVFEq40NP0CQYGQGHHAZdWEdmsucMnOjTiQCwoif5Xats8/U5y+1dBcGtBhtoQ0xHlU9yKfX7
gpd4DUeqWVbA0/gTXwIDAQAB
```

قطعه کد زیر این موضوع را نشان می دهد :



همانطور که اشاره نمودیم باج‌افزار Dont_Worry از الگوریتم‌های رمزنگاری RSA و AES برای رمزگذاری فایل‌ها استفاده می‌کند در قطعه کد زیر استفاده از الگوریتم رمزنگاری RSA توسط این باج‌افزار مشهود است:



در بخش تحلیل پویا به پسوند فایل‌هایی که مورد هدف باج‌افزار قرار می‌گیرند، اشاره شد. پس از بررسی کدمنبع باج‌افزار این موضوع اثبات شد، که در قطعه کد زیر می‌توان آن را مشاهده نمود :

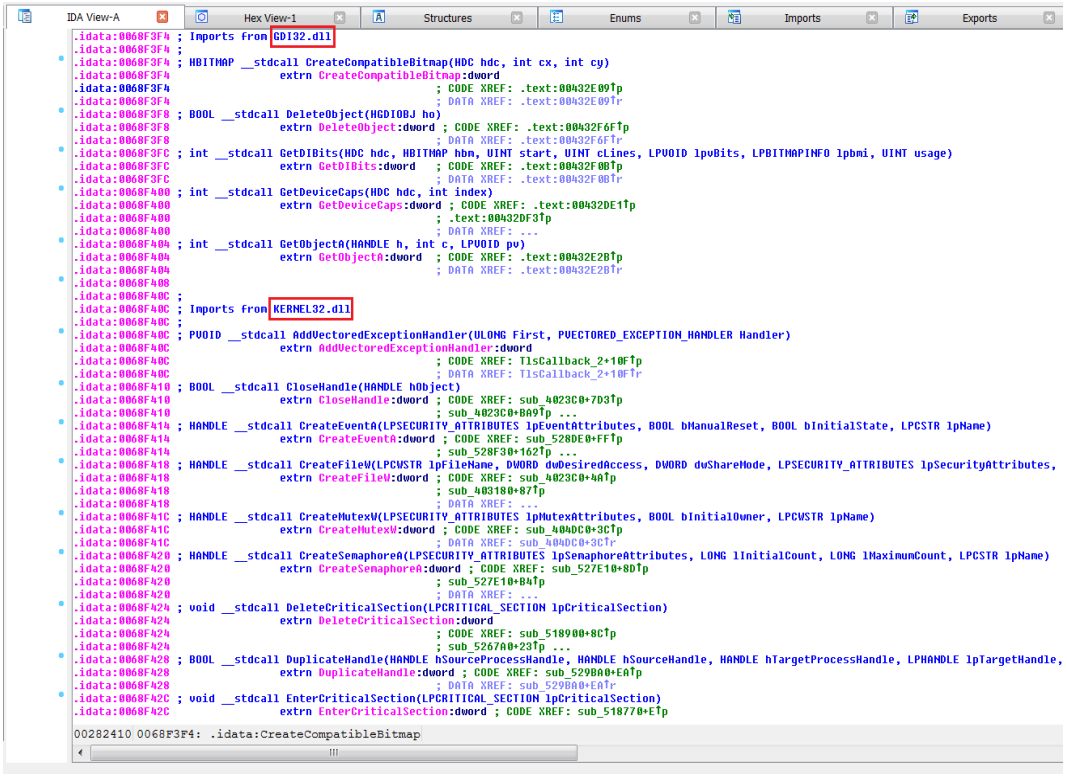
```
.text:005CA010
.text:005CA010 ; =============== S U B R O U T I N E =======================================
.text:005CA010
.text:005CA010 ; Attributes: bp-based frame
.text:005CA010
.text:005CA010 sub_5CA010       proc near               ; DATA XREF: .text:005CED58↓o
.text:005CA010
.text:005CA010 var_28           = dword ptr -28h
.text:005CA010 var_4            = dword ptr -4
.text:005CA010
.text:005CA010                  push    ebp
.text:005CA011                  mov     ecx, offset unk_68B408
.text:005CA016                  mov     ebp, esp
.text:005CA018                  push    ebx
.text:005CA019                  sub     esp, 24h
.text:005CA01C                  call    sub_5B9BB0
.text:005CA021                  mov     [esp+28h+var_28], offset sub_404BD0 ; _onexit_t
.text:005CA028                  call    sub_517DF0
.text:005CA02D                  mov     [esp+28h+var_28], offset a__zip ; ".*\\.zip"
.text:005CA034                  mov     ecx, offset unk_687DC0
.text:005CA039                  call    sub_5C9FD0
.text:005CA03E                  sub     esp, 4
.text:005CA041                  mov     ecx, offset unk_687DD8
.text:005CA046                  mov     [esp+28h+var_28], offset a__rar ; ".*\\.rar"
.text:005CA04D                  call    sub_5C9FD0
.text:005CA052                  sub     esp, 4
.text:005CA055                  mov     ecx, offset unk_687DF0
.text:005CA05A                  mov     [esp+28h+var_28], offset a__7z ; ".*\\.7z"
.text:005CA061                  call    sub_5C9FD0
.text:005CA066                  sub     esp, 4
.text:005CA069                  mov     ecx, offset unk_687E08
.text:005CA06E                  mov     [esp+28h+var_28], offset a__68 ; ".-"
.text:005CA075                  call    sub_5C9FD0
.text:005CA07A                  sub     esp, 4
.text:005CA07D                  mov     ecx, offset unk_687E20
.text:005CA082                  mov     [esp+28h+var_28], offset asc_5DE342 ; ".-"
.text:005CA089                  call    sub_5C9FD0
.text:005CA08E                  sub     esp, 4
.text:005CA091                  mov     ecx, offset unk_687E38
.text:005CA096                  mov     [esp+28h+var_28], offset a__gz ; ".*\\.gz"
.text:005CA09D                  call    sub_5C9FD0
.text:005CA0A2                  sub     esp, 4
.text:005CA0A5                  mov     ecx, offset unk_687E50
.text:005CA0AA                  mov     [esp+28h+var_28], offset a__69 ; ".-"
.text:005CA0B1                  call    sub_5C9FD0
.text:005CA0B6                  sub     esp, 4
.text:005CA0B9                  mov     ecx, offset unk_687E68
.text:005CA0BE                  mov     [esp+28h+var_28], offset asc_5DE372 ; ".-"
.text:005CA0C5                  call    sub_5C9FD0
.text:005CA0CA                  sub     esp, 4
.text:005CA0CD                  mov     ecx, offset unk_687E80
.text:005CA0D2                  mov     [esp+28h+var_28], offset asc_5DE382 ; ".-"
.text:005CA0D9                  call    sub_5C9FD0
.text:005CA0DE                  sub     esp, 4
.text:005CA0E1                  mov     ecx, offset unk_687E98
.text:005CA0E6                  mov     [esp+28h+var_28], offset asc_5DE392 ; ".-"
.text:005CA0ED                  call    sub_5C9FD0
.text:005CA0F2                  sub     esp, 4
.text:005CA0F5                  mov     ecx, offset unk_687EB0
.text:005CA0FA                  mov     [esp+28h+var_28], offset a__psd ; ".*\\.psd"
.text:005CA101                  call    sub_5C9FD0
.text:005CA106                  sub     esp, 4
.text:005CA109                  mov     ecx, offset unk_687EC8
.text:005CA10E                  mov     [esp+28h+var_28], offset a__cdr ; ".*\\.cdr"
.text:005CA115                  call    sub_5C9FD0
.text:005CA11A                  sub     esp, 4
.text:005CA11D                  mov     ecx, offset unk_687EE0
.text:005CA122                  mov     [esp+28h+var_28], offset a__dwg ; ".*\\.dwg"
.text:005CA129                  call    sub_5C9FD0
.text:005CA12E                  sub     esp, 4
001C9410 005CA010: sub_5CA010
```

بررسی ها نشان میدهد باج‌افزار Dont_Worry از OPENSSL (یک مجموعه نرم‌افزار و کتابخانه از توابع رمزنگاری است) برای رمزگذاری فایل ها استفاده می‌کند :

HonestSample_Dont_Worry5b07c80a4b24264120bc64fe.c

```
21136   //----- (00412020) --------------------------------------------------------
21137   int sub_412020()
21138   {
21139     int v0; // eax@1
21140     int result; // eax@3
21141     HMODULE v2; // eax@5
21142     const CHAR *v3; // edx@5
21143     HWINSTA v4; // eax@9
21144     void *v5; // ebx@9
21145     DWORD v6; // edx@13
21146     unsigned int v7; // eax@13
21147     void *v8; // esp@13
21148     DWORD v9; // eax@14
21149     wchar_t *v10; // ecx@14
21150     LPCSTR lpModuleName; // [sp+0h] [bp-58h]@0
21151     char lpModuleNamea; // [sp+0h] [bp-58h]@10
21152     char v13; // [sp+23h] [bp-35h]@13
21153     wchar_t *Str; // [sp+2Ch] [bp-2Ch]@13
21154     DWORD nLengthNeeded; // [sp+3Ch] [bp-1Ch]@10
21155
21156     v0 = dword_68C944;
21157     if ( dword_68C944
21158       || ((v2 = GetModuleHandleA(0), lpModuleName = v3, !v2) ? (v0 = dword_68C944) : (v0 = (int)GetProcAddress(
21159                                                                                          v2,
21160                                                                                          "_OPENSSL_isservice"),
21161                                                                                  dword_68C944 = v0),
21162           v0) )
21163     {
21164       if ( v0 != -1 )
21165         return ((int (__cdecl *)(LPCSTR))v0)(lpModuleName);
21166     }
21167     else
21168     {
21169       dword_68C944 = -1;
21170     }
21171     v4 = GetProcessWindowStation();
21172     v5 = v4;
21173     if ( v4
21174       && !GetUserObjectInformationW(v4, 2, 0, 0, &nLengthNeeded)
21175       && GetLastError() == 122
21176       && nLengthNeeded <= 0x200
21177       && (v6 = (nLengthNeeded + 1) & 0xFFFFFFFE,
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر استفاده از این کتابخانه‌ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است.



ADVAPI۳۲.dll	GDI۳۲.dll	USER۳۲.dll	SHELL۳۲.dll
DeregisterEventSource RegisterEventSourceA ReportEventA	CreateCompatibleBitmap DeleteObject GetDeviceCaps GetDIBits GetObjectA	GetDC GetProcessWin dowStation GetUserObjectI nformationW MessageBoxA ReleaseDC	ShellExecuteW

msvcrt.dll	msvcrt.dll	msvcrt.dll	msvcrt.dll
__dllonexit	fopen	strcmp	_lock
__doserrno	fprintf	strcoll	_lseeki٦٤
__getmainargs	fputc	strcpy	_onexit
__initenv	fputs	strerror	_read
__lconv_init	fread	strftime	_setjmp۳
__mb_cur_max	free	strlen	_setmode
__pioinfo	fseek	strncmp	_strdup
__set_app_type	fsetpos	strncpy	_strnicmp
__setusermatherr	ftell	strrchr	_ultoa
_acmdln	fwrite	strtol	_unlock
_amsg_exit	getc	strtoul	_vsnprintf
_beginthreadex	getenv	strxfrm	_wfopen
_cexit	getwc	time	_write
_endthreadex	gmtime	tolower	abort
_errno	isalnum	towlower	atoi
_exit	isspace	towupper	calloc
_fdopen	isupper	ungetc	exit
_filelengthi٦٤	iswctype	ungetwc	fclose
_fileno	isxdigit	vfprintf	feof

_fmode	localeconv	wcscmp	ferror
_fstat٦٤	localtime	wcscoll	fflush
_getch	longjmp	wcscpy	fgetpos
_initterm	malloc	wcsftime	fgets
_iob	memchr	wcslen	putc
realloc	memcmp	wcsstr	putwc
setlocale	memcpy	wcsxfrm	qsort
setvbuf	memmove	sprintf	raise
signal	memset	sscanf	strchr
	printf	strcat	

KERNEL٣٢.dll	KERNEL٣٢.dll	KERNEL٣٢.dll	KERNEL٣٢.dll
AddVectoredExceptionHandler	GetCurrentThread	RaiseException	GetProcessAffinityMask
CloseHandle	GetCurrentThreadId	ReadFile	GetShortPathNameW
CreateEventA	GetFileSizeEx	ReleaseMutex	GetStartupInfoA
CreateFileW	GetEnvironmentVariableW	ReleaseSemaphore	GetStdHandle
CreateMutexW	GetFileType	RemoveVectoredExceptionHandler	GetSystemTimeAsFileTime
CreateSemaphoreA	GetHandleInformation	ResetEvent	GetThreadContext
DeleteCriticalSection	GetLastError	ResumeThread	GetThreadPriority
DuplicateHandle	GetModuleFileNameW	SetEvent	GetTickCount
EnterCriticalSection	GetModuleHandleA	SetFilePointerEx	GetVersion
FindClose	GetModuleHandleW	SetLastError	GetWindowsDirectoryW
FindFirstFileW	GetProcAddress	SetProcessAffinityMask	GlobalMemoryStatus
FindNextFileW	WaitForMultipleObjects	SetThreadContext	InitializeCriticalSection
FindResourceW	WaitForSingleObject	SetThreadPriority	IsDBCSLeadByteEx
FreeLibrary	WideCharToMultiByte	SetUnhandledExceptionFilter	IsDebuggerPresent
GetCurrentProcess	WriteFile	SizeofResource	LeaveCriticalSection
GetCurrentProcessId	UnhandledExceptionFilter	Sleep	LoadLibraryA
TlsAlloc	VirtualProtect	SuspendThread	LoadResource
TlsGetValue	VirtualQuery	TerminateProcess	LockResource
TlsSetValue	MultiByteToWideChar	TryEnterCriticalSection	MoveFileW
	OutputDebugStringA		
	QueryPerformanceCounter		

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند که آن هم به نام خود باج‌افزار می‌باشد :

```
Dont_Worry.exe
```

پس از بررسی‌های انجام شده مشخص گردید باج‌افزار Dont_Worry فایل‌های زیر را در مسیرهای مشخص شده باز می‌کند :

```
C:\WINDOWS\system٣٢\winime٣٢.dll

C:\WINDOWS\system٣٢\ws ٢_ ٣٢.dll

C:\WINDOWS\system٣٢\ws ٢help.dll
```

C:\WINDOWS\system۳۲\psapi.dll

C:\WINDOWS\system۳۲\imm۳۲.dll

C:\WINDOWS\system۳۲\lpk.dll

C:\WINDOWS\system۳۲\usp۱۰.dll

C:\WINDOWS\system۳۲\shell۳۲.dll

C:\WINDOWS\WinSxS\x۸٦_Microsoft.Windows.CommonControls_ ٦٥٩٥b٦٤۱٤٤ccf۱df_ ٦.۰.۲٦۰۰.٥٥۱۲_xww_۳٥ d٤ce۸۳\comctl۳۲.dll

C:\WINDOWS\WindowsShell.Manifest

C:\WINDOWS\system۳۲\comctl۳۲.dll

فایل نوشته شده توسط باج‌افزار :

C:\DiskX\Dont_Worry.txt

کلیدهای رجیستری زیر توسط باج‌افزار باز می‌شوند :

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.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-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File ExecutionOptions\comctl32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\ImageFileExecutionOptions\KERNEL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\ImageFileExecutionOptions\ADVAPI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image FileExecutionOptions\WS2HELP.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File ExecutionOptions\SHLWAPI.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PSAPI.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image FileExecutionOptions\winime32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP10.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Dont_Worry نشدیم.

شناسایی :

در حال حاضر تعداد ٤٠ مورد از ٦٥ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.WCryG.64BDA840	AegisLab	Virus.Ransom.Wcryg!c
ALYac	Trojan.Ransom.AMBA	Arcabit	Generic.Ransom.WCryG.64BDA840
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Ransom.keirp	AVware	Trojan.Win32.Generic!BT
BitDefender	Generic.Ransom.WCryG.64BDA840	CAT-QuickHeal	Ransom.WCryG.S2650646
Comodo	UnclassifiedMalware	Cyren	W32/Trojan.FBFO-5333
DrWeb	Trojan.Encoder.14940	Emsisoft	Generic.Ransom.WCryG.64BDA840 (B)
eScan	Generic.Ransom.WCryG.64BDA840	ESET-NOD32	a variant of Win32/Filecoder.Russenger.A
F-Secure	Generic.Ransom.WCryG.64BDA840	Fortinet	W32/Filecoder_Russenger.A!tr
GData	Generic.Ransom.WCryG.64BDA840	Ikarus	Trojan-Ransom.Russenger
K7AntiVirus	Trojan (00531d8d1)	K7GW	Trojan (00531d8d1)
Kaspersky	Trojan-Ransom.Win32.Crypmod.zhx	Malwarebytes	Ransom.DontWorry
MAX	malware (ai score=96)	McAfee	Artemis!4DF8460A4496
McAfee-GW-Edition	BehavesLike.Win32.Dropper.vh	Microsoft	Ransom:Win32/Genasom
NANO-Antivirus	Trojan.Win32.Filecoder.fceiru	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.8ba
Sophos AV	Mal/Generic-S	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	TROJ_FRS.VSN1DE18
TrendMicro-HouseCall	TROJ_FRS.VSN1DE18	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	ZoneAlarm	Trojan-Ransom.Win32.Crypmod.zhx