

باسمه تعالی

تحلیل فنی باج افزار Dont_Worry

مقدمه :

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

AMBA >> Crypto_Lab > Dont_Worry

این باج افزار 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
MD5	۴df۸۴۶۰a۴۴۹۶۲۸۰ac۱۲۲۲۱۵aa۳۹fce۴d
SHA-۱	e۳۲۲ee۲۷۴۴۲d۱۰c۲۰۷۱۲۴eefab۹۴۴۵e۲۹aa۷۷b۹۸
SHA-۲۵۶	۹a۵۲۲b۳b۵a۵۱b۵e۰۲۱۹۷۷ad۵۵۷۸۰f۵۲۷d۵۸۱۹۳d۵۸۷b۱c۰۱۵۸۸e۰۷cc۴۰a۶۹f۸۸۴
اندازه فایل	۲.۵۲ MB

فایل اجرایی این باج افزار دارای ۹ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۱۸	۴۰۹۶	۱۹۲۴۷۵۲	۱۹۲۵۱۲۰
.data	۲.۲۶	۱۹۲۹۲۱۶	۱۲۳۶۴	۱۲۸۰۰
.rdata	۵.۶۸	۱۹۴۵۶۰۰	۲۵۳۶۳۲	۲۵۳۹۵۲
.eh_fram	۴.۹	۲۱۹۹۵۵۲	۴۳۷۴۰۴	۴۳۷۷۶۰
.bss	۰	۲۶۳۷۸۲۴	۴۱۷۶۰	۰
.idata	۵.۱۸	۲۶۸۲۸۸۰	۵۷۴۸	۶۱۴۴
.CRT	۰.۳۴	۲۶۹۱۰۷۲	۵۶	۵۱۲

۵۱۲	۳۲	۲۶۹۵۱۶۸	۰.۲۱	.tls
۱۵۳۶	۱۳۲۸	۲۶۹۹۲۶۴	۴.۷	.rsrc

تحلیل پویا :

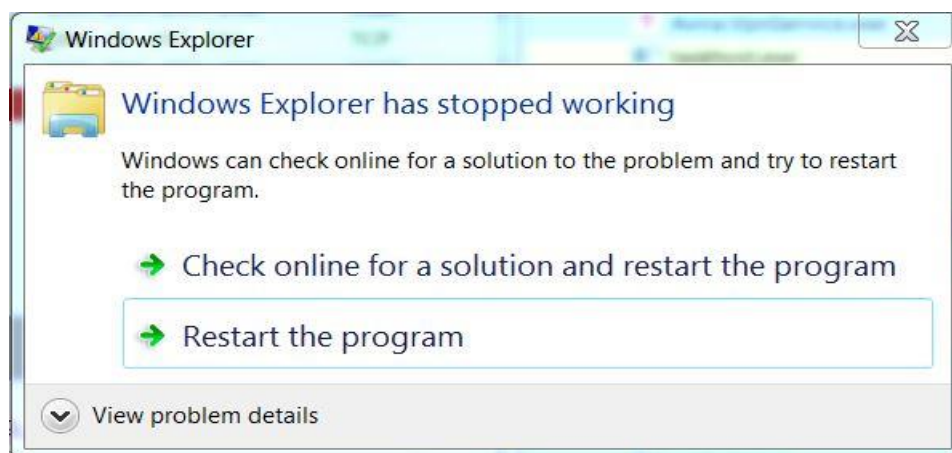
برای بررسی عمیق تر باج افزار Dont_Worry، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره پس از اجرا، شروع به رمزگذاری فایل ها می کند و پس از اتمام فرایند رمزگذاری، فایل با نام Dont_Worry.txt در کنار فایل های رمزگذاری شده و بر روی Desktop ایجاد می کند که شامل پیغام باج خواهی می باشد و قربانیان جهت رمزگشایی فایل ها باید از طریق آدرس ایمیل ups@torbox۳uiot۶wchz.onion با مهاجمین ارتباط برقرار نمایند.

همانطور که اشاره شد این باج افزار از الگوریتم های رمزنگاری RSA و AES برای رمزگذاری فایل ها استفاده می کند و فایل هایی با پسوندهای زیر را رمزگذاری می کند.

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[+-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, .rk۶, .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[+-9], .nd[+-9], .st[+-9], .kpm, .trec, .aad, .ipa, .isz, .zup, .data, .wsb, .dct, .etw, .rsz, .rszold, .rse, .stek, .mrimg, .gbr, .webp, .xslt, .p10, .psp, .pslic, .sldprt, .stop, .granit, .wallet, .ytbl, .rr0d, .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, .bnp, .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, .xg0, .yg0, .db, .backup, .vmdk, .mxlz, .export, .wbcats, .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, .fjf, .ps۱, .saved, .save, .bf۲, .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, .۶tr, .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, .md0, .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, .lay۶, .cui, .cuix, .keg, .ifm, .efm, .btr, .sna, .blb, .amp, .rgt, .bg, .arh, .cr۲, .\$\$\$\$, .[-9]+, .۶t[+-9]*, .fdb[+-9]*, .db[+-9]*, .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

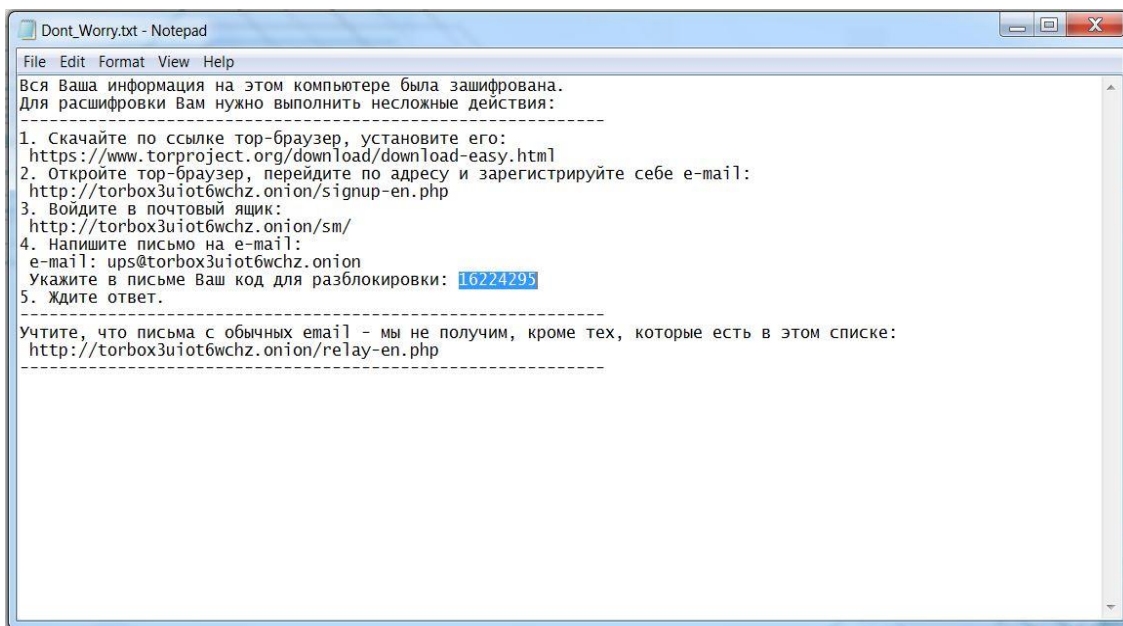
باج افزار در حین اجرا، فعالیت Windows Explorer را متوقف کرده و پیغام زیر به نمایش در می آید:



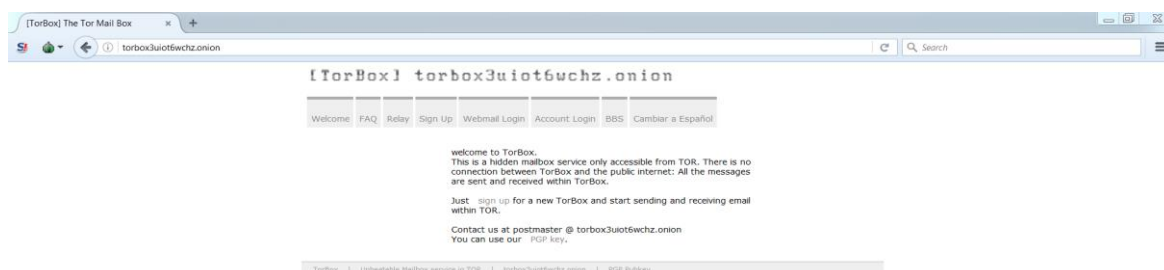
تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.

Name	Date modified	Type	Size
test file (1).kmz	3/14/2018 6:35 PM	KMZ File	1 KB
test file (1).m	1/22/2018 6:40 PM	M File	2 KB
test file (1).mp3	3/13/2018 3:07 PM	MP3 Format Sound	6,233 KB
test file (2).mp3	2/3/2018 4:45 PM	MP3 Format Sound	4,069 KB
test file (1).mp4	2/14/2018 6:20 AM	MP4 Video	48,437 KB
test file (2).mp4	3/2/2018 9:30 PM	MP4 Video	801 KB
test file (1).srt	5/28/2017 8:03 PM	SRT File	66 KB
test file (1).info	12/26/2006 7:12 PM	System Informatio...	2 KB
Dont_Worry.txt	5/31/2018 9:18 PM	Text Document	2 KB
test file (1).jpg.UPS-0ebf72a125f70cc6	5/31/2018 9:18 PM	UPS-0EBF72A125F...	406 KB
test file (3).jpg.UPS-1a0cedac06f3ca76	5/31/2018 9:18 PM	UPS-1A0CEDAC06...	228 KB
test file (1).rar.UPS-1fb6c03b58040359	5/31/2018 9:18 PM	UPS-1FB6C03B580...	72,217 KB
dnSpy.zip.UPS-2a45a64f686e11dd	5/31/2018 9:18 PM	UPS-2A45A64F686...	23,554 KB
test file (2).JPG.UPS-3c66b3b6374028b7	5/31/2018 9:18 PM	UPS-3C66B3B6374...	136 KB
test file (2).bak.UPS-3fd2c7356d6f27cb	5/31/2018 9:18 PM	UPS-3FD2C7356D...	92 KB
test file (2).docx.UPS-5b8fe7fd7fa30cf2	5/31/2018 9:18 PM	UPS-5B8FE7FD7FA...	541 KB
test file (1).PNG.UPS-6b5001776a8d11e4	5/31/2018 9:18 PM	UPS-6B5001776A8...	14 KB
test file (1).docx.UPS-52ff2dd92574d39f	5/31/2018 9:18 PM	UPS-52FF2DD9257...	14 KB
test file (1).key.UPS-76a8f38863535122	5/31/2018 9:18 PM	UPS-76A8F388635...	2 KB
test file (1).mov.UPS-092e8a77660b66e4	5/31/2018 9:18 PM	UPS-092E8A77660...	1,538 KB
test file (1).dwg.UPS-755b5ed943a3b09e	5/31/2018 9:18 PM	UPS-755B5ED943...	116 KB
test file (1).pdf.UPS-6512c70d02b2e6c2	5/31/2018 9:18 PM	UPS-6512C70D02...	512 KB
test file (2).rar.UPS-122766e779cb6295	5/31/2018 9:18 PM	UPS-122766E779C...	29,910 KB
test file (1).bak.UPS-2007122f49e7403d	5/31/2018 9:18 PM	UPS-2007122F49E...	85 KB

همانطور که در تصویر نیز مشخص است، این باج افزار فایل هایی با پسوندهای خاص را رمزگذاری می کند و یک فایل تحت عنوان Dont_Worry.txt را در دایرکتوری های مختلف ایجاد می کند که شامل پیغام باج خواهی به زبان روسی می باشد. همچنین به دلیل رمزگذاری برخی از فایل های مربوط به نرم افزارهای نصب شده بر روی سیستم قربانی، ممکن است برخی از آنها قابل استفاده نباشند. تصویر زیر پیغام باج خواهی باج افزار Dont_Worry را نشان می دهد.



بر اساس پیغام باج خواهی، یک کد شناسایی منحصر بفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید به آدرس <http://torbox3uiot6wchz.onion> در دارک وب 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@torbox3uiot6wchz.onion می‌باشد. تصاویر زیر مربوط به موارد اشاره شده می‌باشد :



تصویر ۱: صفحه وب سایت <http://torbox3uiot6wchz.onion>

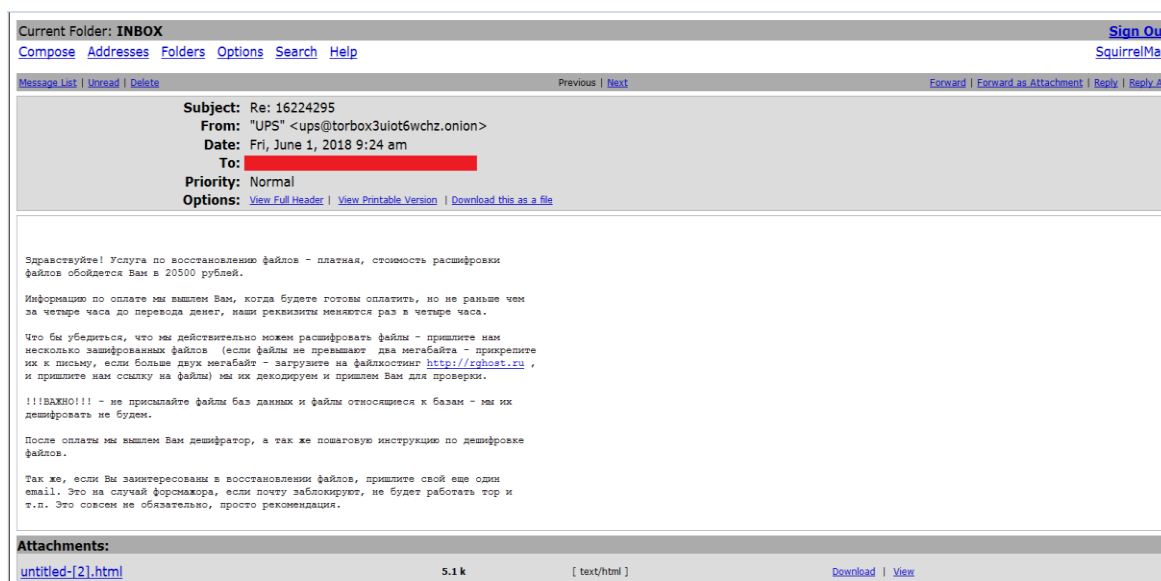


تصویر ۲: صفحه مربوط به ایجاد ایمیل به آدرس <http://torbox3ulot6wchz.onion/signup-en.php>



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 نحوه 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 نحوه پرداخت را برای ما ارسال نمودند. در این پیغام اعلام شده است که مبلغ باج فقط از طریق کیف پول بیت‌کوین به آدرس

مدت زمان ۴۸ ساعت از بین می‌رود. تصاویر زیر مربوط به موارد اشاره شده می‌باشد :

۱۹SzdQXNCXT۱۴۸wPcBeYNqXzMdqxcobWJQ برای مهاجمین ارسال گردد. ضمناً این آدرس پس از

The screenshot shows a webmail interface with a left sidebar containing folders: INBOX (1), Drafts, Sent, Trash, and Community. The main content area displays an email with the following text:

Мы принимаем только биткоины, в связи с предостережением ЦБ от 27.01.2014 о виртуальных валютах, оплата может затянуться на срок банковской транзакции.

В связи с тем, что покупатели биткоинов стали говорить, что их карту украли и незаконно перевели деньги, продавцы биткоинов ввели дополнительные проверки (может не быть, а могут попросить дополнительные сведения).
Могут просить оплатить только - Cash in (внесение наличных на счет карты через банкомат) или платежи с подтверждением оплаты (чек и комментарий).
Или продавец может попросить фотографию банковской карты на развороте паспорта (очень редкая просьба).
Как бы то ни было - это самый быстрый и безопасный способ оплаты для Вас и для меня практически беспроцентный перевод биткоинов - это очень важно, так как есть минимумы на зачисления.

Операция покупки биткоинов проходит в ручном режиме.
Перейдите на сайт - <https://localbitcoins.com/ru/> или <https://localbitcoins.net/ru/> (Слеш в конце адреса - обязателен).
Зарегистрируйтесь в нем.
На сайте у вас появится свой кошелек биткоин, на него поступит перевод от продавца, и через этот кошелек вам нужно будет перевести деньги нам.
Весь процесс занимает от 15 до 30 минут, все зависит от того, как быстро Вы свяжетесь с продавцом и переведете ему деньги.
Примите к сведению, оплата через WebMoney проходит только, если ваш аттестат выше начального и перевод может затянуться на несколько суток.
Если Вы хотите провести обмен через Яндекс Деньги, то Вам нужно знать следующее - в сутки можно обменять 10т.р., обмен длится около 24 часов (сделано это для защиты от незаконных переводов средств), если Вы все же решили купить биткоины за Яндекс Деньги - напишите нам, мы вышлем инструкцию на другой обменник.

Перейдите по этой ссылке: <https://localbitcoins.com/ru/buy-bitcoins-online/rub/> или <https://localbitcoins.net/ru/buy-bitcoins-online/rub/>
Способ оплаты можете менять по своему усмотрению. Так же Вы можете купить биткоины у нескольких продавцов, допустим если у одного продавца не хватает биткоинов. Только не выбирайте продавцов с низким курсом, как правило самые выгодные предложения обмена - сверху.

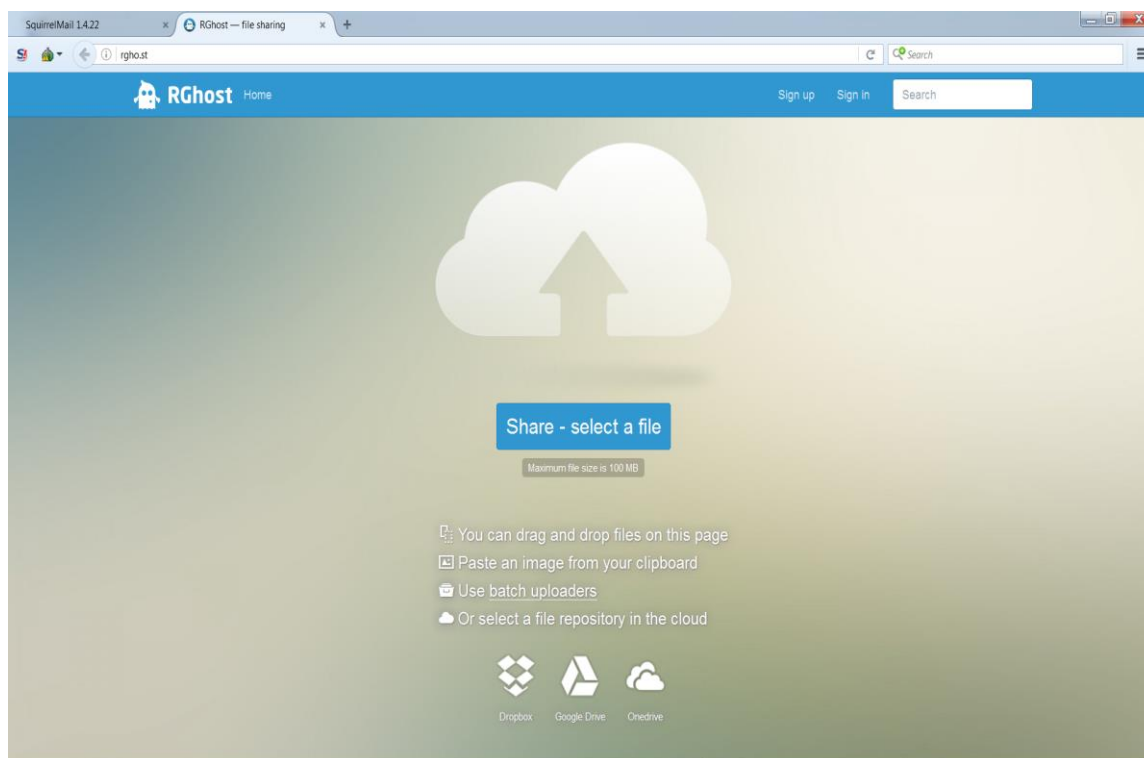
После того, как выберете продавца, Вам нужно на страничке обмена ввести:
В поле "RUB" - 20500.
Поле "BTC" - изменится автоматически

Так же читайте "Условия сделки", которые будут на страничке обмена.
Реквизиты для перевода денег и варианты перевода удобные для вас - вам пришлет продавец биткоинов, после того, как Вы свяжетесь с ним.
После того, как Вы переведете деньги продавцу, а продавец переведет вам Биткоины, вам нужно будет перевести биткоины на адрес ниже (делается это из меню "кошелька")

Принимающий адрес биткоин: 19SzdQXNCXT148wPcBeYNqXzMdqxcobWJQ

Адрес Биткоин кошелька будет действовать 48 часов.
по этому адресу - можно отследить все транзакции по счету - [https:// blockchain . info/address/19SzdQXNCXT148wPcBeYNqXzMdqxcobWJQ](https://blockchain.info/address/19SzdQXNCXT148wPcBeYNqXzMdqxcobWJQ)
Как только по ссылке нули сменяются цифрами - мы сразу вышлем дешифратор.

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 :

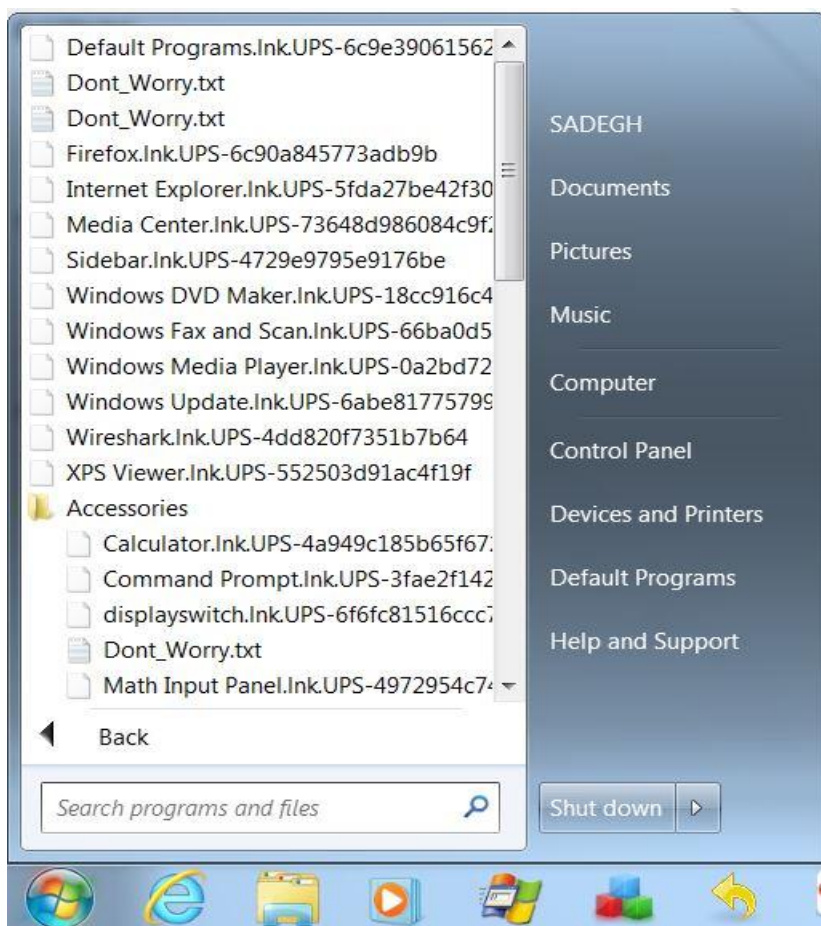
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	19SzDQXNCXT148wPcBeYNqXzMdqcobWJQ	No. Transactions	0
Hash 160	5cab2a41abca423e544567c60f90bd6e772efdf7	Total Received	0 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC

[Request Payment](#) [Donation Button](#)



این باج‌افزار فایل‌های موجود در Recycle Bin را نیز حذف می‌نماید و تمام ابزارهای کاربردی ویندوز 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 راه‌های 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 باج‌افزار Dont_Worry ساختار فایل‌ها را پس از رمزگذاری به کلی تغییر نمی‌دهد. نتایج این بررسی‌ها در تصویر زیر قابل مشاهده است.

قبل از رمزگذاری

بعد از رمزگذاری

Type	Offset (Source)	Offset (Dest)	Size
Inserted	0	0	1,542
Modified	0	1,542	11,668
Matched	11,668	13,210	13
Modified	11,681	13,223	50
Matched	11,731	13,273	13
Modified	11,744	13,286	54
Matched	11,798	13,340	13
Modified	11,811	13,353	50
Matched	11,861	13,403	13

مربوط به پسوند اضافه شده به انتهای فایل ها

بخش هایی از فایل که پس از رمزگذاری نیز تغییر نکرده است.

مقدار کلید عمومی باج افزار جهت رمزگذاری فایل ها در زیر قابل مشاهده می باشد.

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQAMIIBCgKCAQEAAqeTtiZsRIVcrF7sWj5JQ9D2YoMsCCI
DafvUmSPRaU/5Lq13thUVU0X0yZ1YK3UZZ/knsqu49Yh7NATDTtXHU^knNAD+p1OCFZuhob
pZgNDREZ/WcfXmOFw1hMGhWdQTgNzO9FRPeP/vLJ20Ljg5607N/H7I9D//erRCrS506po317SKjTjExK781JomUtQsDu495vzVTJY+BAW+tDSgAE+xFcl7zbCW0jeO9A+IPZLQqrYF7PpXZAbpmdK0
KjTjExK781JomUtQsDu495vzVTJY+BAW+tDSgAE+xFcl7zbCW0jeO9A+IPZLQqrYF7PpXZAbpmdK0
wXVFEq49NP0CQYQGQGHHAZdWEEdmsucMnOjTiQCwoif5Xats8/U5y+1dBcGtBhtoQ0xHIU9yKf
XVgpd4DUeqWVbA0/gTXwIDAQAB
```

قطعه کد زیر این موضوع را نشان می دهد :

همانطور که اشاره نمودیم باج افزار Dont_Worry از الگوریتم های رمزنگاری RSA و AES برای رمزگذاری فایل ها استفاده می کند در قطعه کد زیر استفاده از الگوریتم رمزنگاری RSA توسط این باج افزار مشهود است:

```

IDA View-A
Hex View-1
Structures
Enums

.text:00405252 mov [esp+8], eax
.text:00405256 mov [esp+4], ebp
.text:0040525A mov eax, [esp+2Ch]
.text:0040525E mov [esp], eax
.text:00405261 call sub_417000
.text:00405266 test eax, eax
.text:00405268 mov ecx, [esp+3Ch]
.text:00405272 jnz loc_405350
.text:00405272 loc_405272: ; CODE XREF: .text:00405247fj
.text:00405272 mov [esp], ebx ; .text:00405378fj ...
.text:00405275 call sub_418F70
.text:0040527A loc_40527A: ; CODE XREF: .text:00405213fj
.text:0040527A mov dword ptr [esp+10h], 003h ; .text:00405217fj ...
.text:00405282 mov dword ptr [esp+8Ch], offset aRsa_crpt_c ; "rsa_crpt.c"
.text:0040528A mov dword ptr [esp+8], 8Ch
.text:00405292 mov dword ptr [esp+4], 88h
.text:0040529A mov dword ptr [esp], 4
.text:004052A1 call sub_408F80
.text:004052A6 xor ebp, ebp
.text:004052A8 jmp loc_405140
.text:004052AD ;
.text:004052B0 align 10h
.text:004052B0 loc_4052B0: ; CODE XREF: .text:0040512Afj
.text:004052B0 mov dword ptr [esp+10h], 0EBh
.text:004052B8 mov dword ptr [esp+8Ch], offset aRsa_crpt_c ; "rsa_crpt.c"
.text:004052C0 mov dword ptr [esp+8], 3
.text:004052C8 mov dword ptr [esp+4], 88h
.text:004052D0 mov dword ptr [esp], 4
.text:004052D7 call sub_408F80
.text:004052DC jmp loc_405140
.text:004052E1 ;
.text:004052E1 jmp short loc_4052F0
.text:004052E3 ;
.text:004052E3 align 10h
.text:004052F0 loc_4052F0: ; CODE XREF: .text:0040515Cfj
.text:004052F0 mov [esp], esi ; .text:004052E1fj
.text:004052F3 call sub_417740
.text:004052F8 jmp loc_405162
.text:004052FD ;
.text:004052FD align 10h
.text:00405300 loc_405300: ; CODE XREF: .text:004050A9fj
.text:00405300 mov dword ptr [esp+10h], 0CCh
.text:00405308 mov dword ptr [esp+8Ch], offset aRsa_crpt_c ; "rsa_crpt.c"
.text:00405310 mov dword ptr [esp+8], 41h
.text:00405318 mov dword ptr [esp+4], 88h
.text:00405320 mov dword ptr [esp], 4
.text:00405327 call sub_408F80
.text:0040532C xor ebp, ebp
.text:0040532E jmp loc_405140
.text:0040532E ;
00004652 00405252: .text:00405252
    
```

در بخش تحلیل پویا به پسوند فایل هایی که مورد هدف باج افزار قرار می گیرند، اشاره شد. پس از بررسی کد منبع باج افزار این موضوع اثبات شد، که در قطعه کد زیر می توان آن را مشاهده نمود :

```

.text:005CA010 ; ----- SUBROUTINE -----
.text:005CA010 ; Attributes: bp-based frame
.text:005CA010 sub_5CA010 proc near ; DATA XREF: .text:005CED5810
.text:005CA010 var_28 = dword ptr -28h
.text:005CA010 var_4 = dword ptr -4
.text:005CA010
.text:005CA010 push ebp
.text:005CA010 mov ecx, offset unk_68B408
.text:005CA016 mov ebp, esp
.text:005CA018 push ebx
.text:005CA019 sub esp, 24h
.text:005CA01C call sub_5B98B0
.text:005CA021 mov [esp+28h+var_28], offset sub_4048D0 ; _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:005CA049 call sub_5C9FD0
.text:005CA052 sub esp, 4
.text:005CA055 mov ecx, offset unk_687DF0
.text:005CA058 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_5DE3A2 ; "."
.text:005CA085 call sub_5C9FD0
.text:005CA08E sub esp, 4
.text:005CA091 mov ecx, offset unk_687E38
.text:005CA094 mov [esp+28h+var_28], offset a_gz ; ".*\\.gz"
.text:005CA097 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:005CA0C1 call sub_5C9FD0
.text:005CA0C6 sub esp, 4
.text:005CA0C9 mov ecx, offset unk_687E80
.text:005CA0CE mov [esp+28h+var_28], offset asc_5DE382 ; "."
.text:005CA0D1 call sub_5C9FD0
.text:005CA0D6 sub esp, 4
.text:005CA0D9 mov ecx, offset unk_687E98
.text:005CA0DE mov [esp+28h+var_28], offset asc_5DE392 ; "."
.text:005CA0E1 call sub_5C9FD0
.text:005CA0E6 sub esp, 4
.text:005CA0E9 mov ecx, offset unk_687EB0
.text:005CA0EE mov [esp+28h+var_28], offset a_psd ; ".*\\.psd"
.text:005CA0F1 call sub_5C9FD0
.text:005CA0F6 sub esp, 4
.text:005CA0F9 mov ecx, offset unk_687EC8
.text:005CA0FE mov [esp+28h+var_28], offset a_cdr ; ".*\\.cdr"
.text:005CA101 call sub_5C9FD0
.text:005CA106 sub esp, 4
.text:005CA109 mov ecx, offset unk_687EE0
.text:005CA10E mov [esp+28h+var_28], offset a_dwg ; ".*\\.dwg"
.text:005CA111 call sub_5C9FD0
.text:005CA116 sub esp, 4
.text:005CA119
.text:005CA12E sub esp, 4
001c9410 005CA010: sub_5CA010

```

بررسی ها نشان میدهد باج افزار Dont_Worry از OPENSsl (یک مجموعه نرم افزار و کتابخانه از توابع رمزنگاری است) برای رمزگذاری فایل ها استفاده می کند :

```

HonestSample_Dont_Worry5b07c80a4b24264120bc64fec
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     HINSTANCE 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 lpModuleNames; // [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) & 0xFFFFFEE,

```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هرکدام از کتابخانه ها استفاده می کند، در تصویر استفاده از این کتابخانه ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه ها به همراه توابع مورد استفاده نیز در ادامه ی متن آمده است.

```

    .idata:0068F3F4 ; Imports from GDI32.dll
    .idata:0068F3F4 ; HBITMAP __stdcall CreateCompatibleBitmap(HDC hdc, int cx, int cy)
    .idata:0068F3F4 extrn CreateCompatibleBitmap:dword
    .idata:0068F3F4 ; CODE XREF: .text:00432E09Tp
    .idata:0068F3F4 ; DATA XREF: .text:00432E09Tp
    .idata:0068F3F8 ; BOOL __stdcall DeleteObject(HDCOBJ hobj)
    .idata:0068F3F8 extrn DeleteObject:dword ; CODE XREF: .text:00432F6Ftp
    .idata:0068F3F8 ; DATA XREF: .text:00432F6Ftp
    .idata:0068F3FC ; int __stdcall GetDIBits(HDC hdc, HBITMAP hbm, UINT start, UINT cLines, LPVOID lpvBits, LPBITMAPINFO lpbmi, UINT usage)
    .idata:0068F3FC extrn GetDIBits:dword ; CODE XREF: .text:00432F80tp
    .idata:0068F3FC ; DATA XREF: .text:00432F80tp
    .idata:0068F400 ; int __stdcall GetDeviceCaps(HDC hdc, int index)
    .idata:0068F400 extrn GetDeviceCaps:dword ; CODE XREF: .text:00432DE1tp
    .idata:0068F400 ; .text:00432DF3tp
    .idata:0068F400 ; DATA XREF: ...
    .idata:0068F404 ; int __stdcall GetObjectA(HANDLE h, int c, LPVOID pv)
    .idata:0068F404 extrn GetObjectA:dword ; CODE XREF: .text:00432E2Btp
    .idata:0068F404 ; DATA XREF: .text:00432E2Btp
    .idata:0068F408
    .idata:0068F40C ; Imports from KERNEL32.dll
    .idata:0068F40C ; PUOID __stdcall AddVectoredExceptionHandler(ULONG First, PVECTORED_EXCEPTION_HANDLER Handler)
    .idata:0068F40C extrn AddVectoredExceptionHandler:dword
    .idata:0068F40C ; CODE XREF: TlsCallback_2+10Ftp
    .idata:0068F40C ; DATA XREF: TlsCallback_2+10Ftp
    .idata:0068F410 ; BOOL __stdcall CloseHandle(HANDLE hObject)
    .idata:0068F410 extrn CloseHandle:dword ; CODE XREF: sub_4023C0+7D3tp
    .idata:0068F410 ; sub_4023C0+8A9tp ...
    .idata:0068F414 ; HANDLE __stdcall CreateEventA(LPSECURITY_ATTRIBUTES lpEventAttributes, BOOL bManualReset, BOOL bInitialState, LPCWSTR lpName)
    .idata:0068F414 extrn CreateEventA:dword ; CODE XREF: sub_528DE0+FFtp
    .idata:0068F414 ; sub_528F50+162tp ...
    .idata:0068F418 ; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess, DWORD dwShareMode, LPSECURITY_ATTRIBUTES lpSecurityAttributes,
    .idata:0068F418 extrn CreateFileW:dword ; CODE XREF: sub_4023C0+AAtp
    .idata:0068F418 ; sub_403180+87tp
    .idata:0068F418 ; DATA XREF: ...
    .idata:0068F41C ; HANDLE __stdcall CreateMutexW(LPSECURITY_ATTRIBUTES lpMutexAttributes, BOOL bInitialOwner, LPCWSTR lpName)
    .idata:0068F41C extrn CreateMutexW:dword ; CODE XREF: sub_404DC0+3Ctp
    .idata:0068F41C ; DATA XREF: sub_404DC0+3Ctp
    .idata:0068F420 ; HANDLE __stdcall CreateSemaphoreA(LPSECURITY_ATTRIBUTES lpSemaphoreAttributes, LONG lInitialCount, LONG lMaximumCount, LPCWSTR lpName)
    .idata:0068F420 extrn CreateSemaphoreA:dword ; CODE XREF: sub_527E10+8Dtp
    .idata:0068F420 ; sub_527E10+84tp
    .idata:0068F424 ; void __stdcall DeleteCriticalSection(LPCRITICAL_SECTION lpCriticalSection)
    .idata:0068F424 extrn DeleteCriticalSection:dword
    .idata:0068F424 ; CODE XREF: sub_518900+8Ctp
    .idata:0068F424 ; sub_5267A0+23tp ...
    .idata:0068F428 ; BOOL __stdcall DuplicateHandle(HANDLE hSourceProcessHandle, HANDLE hTargetProcessHandle, LPHANDLE lpTargetHandle,
    .idata:0068F428 extrn DuplicateHandle:dword ; CODE XREF: sub_529B00+EAtp
    .idata:0068F428 ; DATA XREF: sub_529B00+EAtp
    .idata:0068F42C ; void __stdcall EnterCriticalSection(LPCRITICAL_SECTION lpCriticalSection)
    .idata:0068F42C extrn EnterCriticalSection:dword ; CODE XREF: sub_518770+ETp
    
```

ADVAPI32.dll	GDI32.dll	USER32.dll	SHELL32.dll
DeregisterEventSource RegisterEventSourceA ReportEventA	CreateCompatibleBitmap DeleteObject GetDeviceCaps GetDIBits GetObjectA	GetDC GetProcessWindowStation GetUserObjectInformationW MessageBoxA ReleaseDC	ShellExecuteW

msvcrt.dll	msvcrt.dll	msvcrt.dll	msvcrt.dll
__dllonexit __doserrno __getmainargs __initenv __lconv_init __mb_cur_max __pioinfo __set_app_type __setusermatherr _acmdln _amsg_exit _beginthreadex _cexit _endthreadex _errno _exit _fdopen _filelengthi64 _fileno	fopen fprintf fputc fputs fread free fseek fsetpos ftell fwrite getc getenv getwc gmtime isalnum isspace isupper iswctype isxdigit	strcmp strcoll strcpy strerror strftime strlen strncmp strncpy strchr strtol strtol strxfrm time tolower toupper ungetc ungetwc vfprintf	_lock _lseeki64 _onexit _read _setjmp _setmode _strdup _strnicmp _ultoa _unlock _vsprintf _wopen _write abort atoi calloc exit fclose feof

_fmode	localeconv	wcscmp	ferror
_fstat ^{٦٤}	localtime	wscoll	fflush
_getch	longjmp	wscopy	fgetpos
_initterm	malloc	wcsftime	fgets
_job	memchr	wcslen	putc
realloc	memcmp	wcsstr	putwc
setlocale	memcpy	wcsxfrm	qsort
setvbuf	memmove	sprintf	raise
signal	memset	sscanf	strchr
	printf	strcat	

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.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\system۳۲\winime۳۲.dll

C:\WINDOWS\system۳۲\ws۲_۳۲.dll

C:\WINDOWS\system۳۲\ws۲help.dll

```
C:\WINDOWS\system32\psapi.dll  
C:\WINDOWS\system32\imm32.dll  
C:\WINDOWS\system32\pk.dll  
C:\WINDOWS\system32\usp10.dll  
C:\WINDOWS\system32\shell32.dll  
C:\WINDOWS\WinSxS\x-wwww-7695b641e4ccf1df-6.0.2600.5512_xww-35  
d8ce83\comctl32.dll  
C:\WINDOWS\WindowsShell.Manifest  
C:\WINDOWS\system32\comctl32.dll
```

فایل نوشته شده توسط باج افزار :

```
C:\DiskX\Dont_Worry.txt
```

کلیدهای رجیستری زیر توسط باج افزار باز می شوند :

```
\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\CodelIdentifiers  
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodelIdentifiers\TransparentEnabled  
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-  
500\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers  
\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\msvcr.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 میزبان در نقطه‌ی جغرافیایی خاص توسط باج افزار Dont_Worry نشدیم.

شناسایی :

در حال حاضر تعداد ۴۰ مورد از ۶۵ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

Ad-Aware	Generic.Ransom.WCryG.64BDA840	AegisLab	Virus.Ransom.Wcrygic
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.Crypmo.d.zh	Malwarebytes	Ransom.DontWorry
MAX	malware (ai score=96)	McAfee	Artemis!4DF8460A4496
McAfee-GW-Edition	Behaves.Like.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/Generi-S	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	TROJ_FRS.VSN1 DE18
TrendMicro-HouseCall	TROJ_FRS.VSN1 DE18	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	ZoneAlarm	Trojan-Ransom.Win32.Crypmo.d.zh