باسمه تعالی

عنوان مستند

بررسی و تحلیل باج افزار Fantom

فهرست مطالب

۱ مقدمه

یک باج افزار جدید به نام Fantom که بر پایه ی پروژه ی باج افزار متن باز EDA2 می باشد، توسط Jakub Kroustek ، محقق بدافزار AVG کشف شده است. این باج افزار از یک قابلیت جالب که یک صفحه ی به روز رسانی تقلبی ویندوز تحت عنوان اینکه ویندوز در حال نصب به روز رسانی های حیاتی می باشد استفاده می‌کند. این باج افزار صفحه ی به روز رسانی تقلبی ویندوز را به کاربر نشان می دهد ولی در پشت زمینه در حال رمزنگاری فایل های قربانی می باشد. لازم به ذکر است که این باج افزار فقط در سیستم عامل های ویندوز ۸ به بعد عملکرد واقعی خود را نشان می دهد.

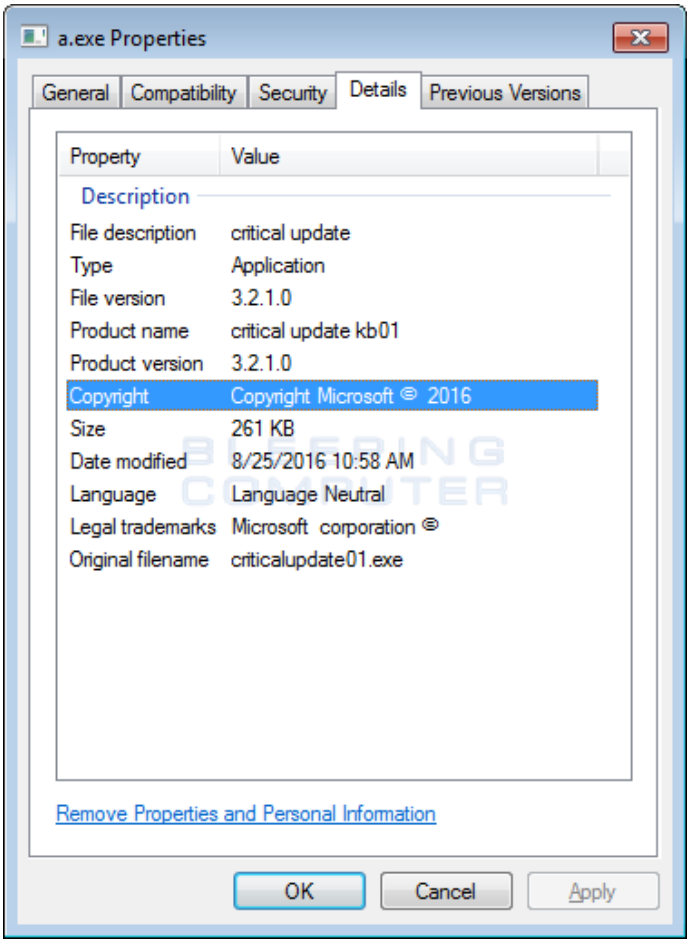
متاسفانه در حال حاضر هیچ راهی برای رمز گشایی کردن فایل های رمز شده با باج افزار Fantom وجود ندارد و راه های عادی برای گرفتن کلید های بر پایه باج افزار EDA2 هم برای این نوع باج افزار در دسترس نیستند.

۲ سناریوی آلودگی

توسعه دهندگان Fantom تلاش زیادی برای پنهان کردن عملکرد مخرب باج افزار پشت یک پیغام به روز رسانی حیاتی ویندوز کرده اند. پوشش اصلی باج افزار Fantom این است که خود را بجای یک به روز رسانی مهم جا می زند.

برای اضافه کردن درستی این به روز رسانی، ویژگی های باج افزار می گوید که این باج افزار از سمت ماکروسافت است و شامل به روز رسانی های حیاتی می باشد.

لازم به ذکر است که هیچ گاه به روز رسانی های ویندوز توسط ایمیل و در قالب یک فایل exe. دریافت نمی‌شود و حتی اگر دریافت شود، آنها همیشه یک امضای دیجیتال اضافه شده توسط ماکروسافت دارند.

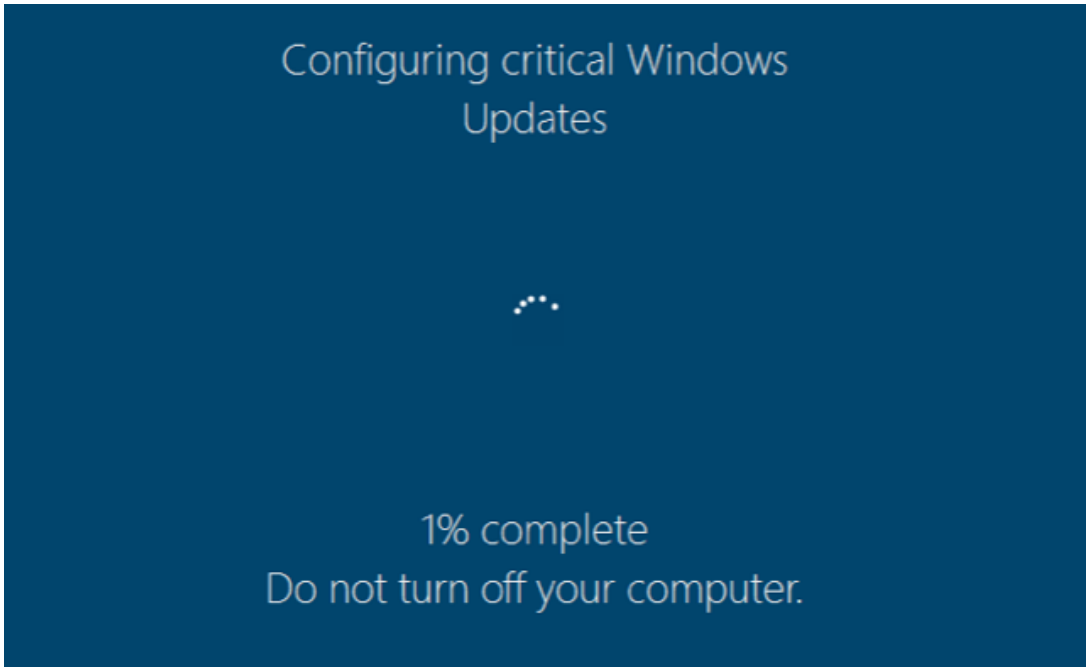

a.exe Properties
General
Compatibility
Security
Details
Previous Versions
Property
Value
Description
File description
critical update
Type
Application
File version
3.2.1.0
Product name
critical update kb01
Product version
3.2.1.0
Copyright
Copyright Microsoft © 2016
Size
261 KB
Date modified
8/25/2016 10:58 AM
Language
Language Neutral
Legal trademarks
Microsoft corporation ®
Original filename
criticalupdate01.exe
Remove Properties and Personal Information
OK
Cancel
Apply

۳ اجرای باج افزار

به محض اجرا شدن باج افزار Fantom، کاربر با دو فرایند مواجه می شود:

برنامه ای که تحت عنوان critical update وجود دارد در واقع کار دستکاری کردن اطلاعات در پس زمینه را بر عهده دارد. WindowsFormsApplication5 نام برنامه ای است که توسط برنامه ی اول اجرا می شود و به عنوان تله از آن استفاده می شود.

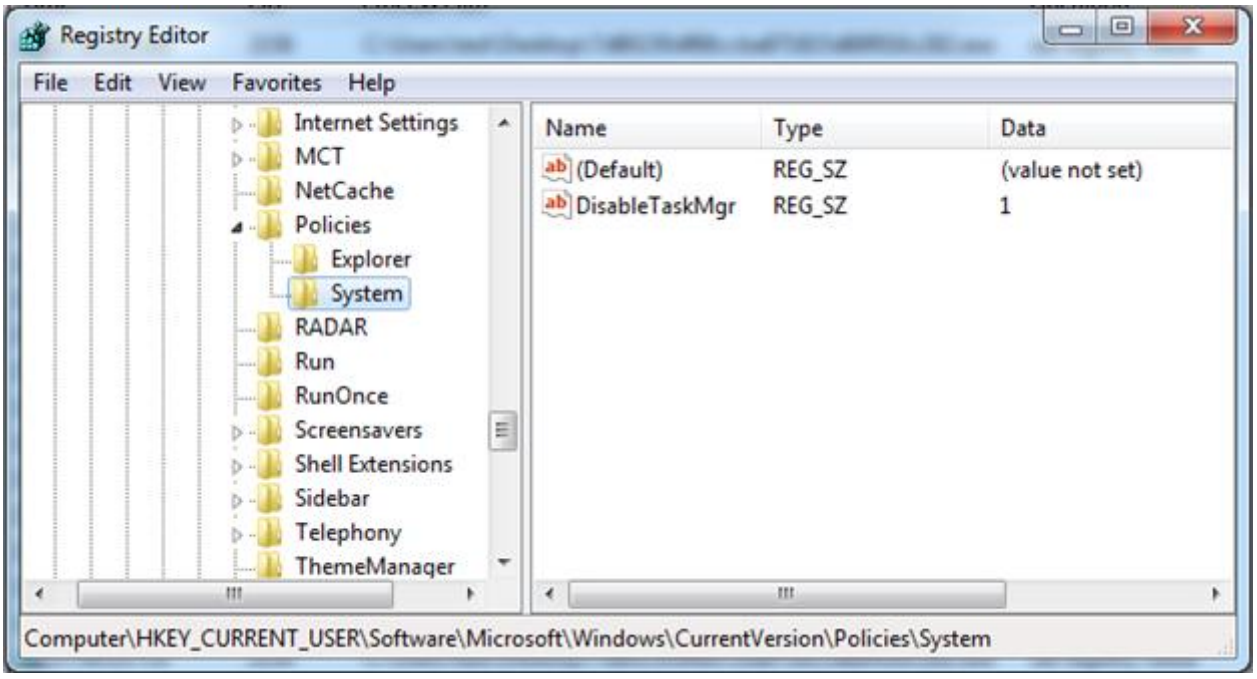
WindowsFormsApplication5 یک صفحه ی تقلبی به روز رسانی ویندوز می سازد. این صفحه تمام صفحات فعال ویندوز را می پوشاند و به کاربر اجازه‌ی رفتن به برنامه های دیگر را نمی دهد. هدف وجود WindowsFormsApplication5 این است که ذهن کاربر را از پروسه ی دستکاری فایل ها تا زمانی که بتواند منحرف کند و مانع متوجه شدن کاربر از خراب شدن فایل ها شود.



صفحه ی به روز رسانی تقلبی حتی یک عدد پیشرفت به صورت درصد هم دارد که نشان دهنده ی میزان فایل های رمز نگاری شده ی قربانی می باشد. این صفحه برای این است که به کاربر نشان دهد بروز رسانی تقلبی در حال نصب است و همچنین فعالیت های زیاد شده ی روی هارد درایو کاربر را توجیه کند.

امکان بستن این پنجره با زدن کلید های Ctrl+F4 وجود دارد ولی این کار فقط صفحه ی بروز رسانی تقلبی را می بندد و باج افزار همچنان در پس زمینه در حال رمز نگاری فایل ها می باشد.

این باج افزار همچنین با استفاده از کلید های رجیستری Task Manager را نیز غیر فعال می کند.



۴ پی لود اصلی بدافزار

این باج افزار فایلها با پسوند زیر را رمز کرده و از کاربر درخواست باج می کند:

.3d, .3d4, .3df8, .3fr, .3g2, .3gp, .3gp2, .3mm, .7z, .aac, .abk, .abw, .ac3, .accdb, .ace, .act, .ade, .adi, .adpb, .adr, .adt, .ai, .aim, .aip, .ais, .amf, .amr, .amu, .amx, .amxx, .ans, .ap, .ape, .api, .apk, .arc, .arch00, .ari, .arj, .aro, .arr, .arw, .asa, .asc, .ascx, .ase, .asf, .ashx, .asmx, .asp, .aspx, .asr, .asset, .avi, .avs, .bak, .bar, .bay, .bc6, .bc7, .bck, .bdp, .bdr, .bib, .bic, .big, .bik, .bkf, .bkp, .blob, .blp, .bmc, .bmf, .bml, .bmp, .boc, .bp2, .bp3, .bpl, .bsa, .bsp, .cag, .cam, .cap, .car, .cas, .cbr, .cbz, .cc, .ccd, .cch, .cd, .cdr, .cer, .cfg, .cfr, .cgf, .chk, .clr, .cms, .cod, .col, .cp, .cpp, .cr2, .crd, .crt, .crw, .cs, .csi, .cso, .css, .csv, .ctt, .cty, .cwf, .d3dbsp, .dal, .dap, .das, .dayzprofile, .dazip, .db0, .dbb, .dbf, .dbfv, .dbx, .dcp, .dcr, .dcu, .ddc, .ddcx, .dem, .der, .desc, .dev, .dex, .dic, .dif, .dii, .dir, .disk, .divx, .diz, .djvu, .dmg, .dmp, .dng, .dob, .doc, .docm, .docx, .dot, .dotm, .dotx, .dox, .dpk, .dpl, .dpr, .dsk, .dsp, .dvd, .dvi, .dvx, .dwg, .dxe, .dxf, .dxg, .elf, .epk, .eps, .eql, .erf, .err, .esm, .euc, .evo, .ex, .exif , .f90, .faq, .fcd, .fdr, .fds, .ff, .fla, .flac, .flp, .flv, .for, .forge, .fos, .fpk, .fpp, .fsh, .gam, .gdb, .gho, .gif, .grf, .gthr, .gz, .gzig, .gzip, .h3m, .h4r, .hkdb, .hkx, .hplg, .htm, .html, .hvpl, .ibank, .icxs, .idx, .ifo, .img, .indd, .ink, .ipa, .isu, .isz, .itdb, .itl, .itm, .iwd, .iwi, .jar, .jav, .java, .jc, .jfif, .jgz, .jif, .jiff, .jpc, .jpe, .jpeg, .jpf, .jpg, .jpw, .js, .json, .kdb, .kdc, .kf, .kmz, .kwd, .kwm, .layout, .lbf, .lbi, .lcd, .lcf, .ldb, .lgp, .litemod, .log, .lp2, .lrf, .ltm, .ltr, .ltx, .lvl, .m2, .m2v, .m3u, .m4a, .mag, .man, .map, .max, .mbox, .mbx, .mcd, .mcgame, .mcmeta, .md, .md3, .mdb, .mdbackup, .mddata, .mdf, .mdl, .mdn, .mds, .mef, .menu, .mic, .mip, .mkv, .mlx, .mod, .mov, .moz, .mp3, .mp4, .mpeg, .mpg, .mpqge, .mrw, .mrwref, .msg, .msp, .mxp, .nav, .ncd, .ncf, .nds, .nef, .nfo, .now, .nrg, .nri, .nrw, .ntl, .odb, .odc, .odf, .odi, .odm, .odp, .ods, .odt, .odtb .oft, .oga, .ogg, .opf, .orf, .owl, .oxt, .p12, .p7b, .p7c, .pab, .pak, .pbf, .pbp, .pbs, .pcv, .pdd, .pdf, .pef, .pem, .pfx, .php, .pkb, .pkh, .pkpass, .pl, .plc, .pli, .pm, .png, .pot, .potm, .potx, .ppd, .ppf, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prc, .prt, .psa, .psd, .psk, .pst, .ptx, .puz, .pwf, .pwi, .pwm, .pxp, .py, .qbb, .qdf, .qel, .qic, .qif, .qpx, .qtq, .qtr, .r3d, .ra, .raf, .rar, .raw, .rb, .re4, .res, .rev, .rgn, .rgss3a, .rim, .rng, .rofl, .rrt, .rsrc, .rsw, .rte, .rtf, .rts, .rtx, .rum, .run, .rv, .rw2, .rwl, .sad, .saf, .sav, .sb, .sc2save, .scm, .scn, .scx, .sdb, .sdc, .sdn, .sds, .sdt, .sen, .sfs, .sfx, .sh, .shar, .shr, .shw, .sid, .sidd, .sidn, .sie, .sis, .slm, .sln, .slt, .snp, .snx, .so, .spr, .sql, .sqx, .sr2, .srf, .srt, .srw, .ssa, .std, .stt, .stx, .sud, .sum, .svg, .svi, .svr, .swd, .swf, .syncdb, .t12, .t13, .tar, .tax, .tax2015, .tax2016, .tbz2, .tch, .tcx, .text, .tg, .thmx, .tif, .tlz, .tor, .tpu, .tpx, .trp, .tu, .tur, .txd, .txf, .txt, .uax, .udf, .umx, .unity3d, .unr, .unx, .uop, .upk, .upoi, .url, .usa, .usx, .ut2, .ut3, .utc, .utx, .uvx, .uxx, .val, .vc, .vcd, .vdf, .vdo, .ver, .vfs0, .vhd, .vmf, .vmt, .vob, .vpk, .vpp_pc, .vsi, .vtf, .w3g, .w3x, .wad, .war, .wav, .wave, .waw, .wb2, .wbk, .wdgt, .wks, .wm, .wma, .wmd, .wmdb, .wmmp, .wmo, .wmv, .wmx, .wotreplay, .wow, .wpd, .wpk, .wpl, .wps, .wsh, .wtd, .wtf, .wvx, .x3f, .xf, .xl, .xla, .xlam, .xlc, .xlk, .xll, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xltx, .xlv, .xlwx, .xml, .xpi, .xpt, .xvid, .xwd, .xxx, .yab, .yps, .z02, .z04, .zap, .zip, .zipx, .zoo, .ztmp

۵ روشهای انتشار بدافزار

- پیوست مخرب پست های الکترونیکی

۶ مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده بدین شرح است:

Filename: criticalupdate01.exe

Type: Win32 EXE

MD5: 7d80230df68ccba871815d68f016c282

SHA-1: e10874c6108a26ceedfc84f50881824462b5b6b6

SHA256: f4234a501edcd30d3bc15c983692c9450383b73bdd310059405c5e3a43cc730b

۷ سطح تهدید فایل تحلیل شده

نتیجه بررسی فایل تحلیل شده با استفاده از تارنمای Virustotal.com در جدول ذیل ارایه شده است. همانطور که مشاهده می‌شود از بین ۵۶ موتور تشخیص بدافزار ۴۹ عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

Antivirus	Result	Update
ALYac	Trojan.Ransom.Fantom	20161203
AVG	Ransom_c.ALF	20161202
AVware	Trojan.Win32.Generic!BT	20161203
Ad-Aware	Trojan.Agent.BXUU	20161203
AegisLab	Troj.Downloader.Axzu!c	20161203
AhnLab-V3	Trojan/Win32.Tear.C1532669	20161202
Antiy-AVL	Trojan[Ransom]/MSIL.Tear	20161203
Arcabit	Trojan.Agent.BXUU	20161203
Avast	Win32:Malware-gen	20161203
Avira (no cloud)	TR/Downloader.axzu	20161202
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9990	20161202
BitDefender	Trojan.Agent.BXUU	20161203
Bkav	W32.Clod9d2.Trojan.3c04	20161202
CAT-QuickHeal	Trojan.Skeeyah	20161202
ClamAV	Win.Ransomware.Fantom-2	20161203
CrowdStrike Falcon (ML)	malicious_confidence_100% (W)	20161024
Cyren	W32/Trojan.CLYD-1190	20161203
DrWeb	Trojan.Encoder.5654	20161203
ESET-NOD32	a variant of Win32/Filecoder.Fantom.A	20161203
Emsisoft	Trojan.Agent.BXUU (B)	20161203
F-Secure	Trojan.Agent.BXUU	20161203
Fortinet	PossibleThreat	20161203
GData	Trojan.Agent.BXUU	20161203
Ikarus	Trojan.MSIL.EzirizNetReactor	20161202
Invincea	trojan.win32.skeeyah.a!rfn	20161202
Jiangmin	TrojanDownloader.Small.cbns	20161203
K7AntiVirus	Riskware (0040eff71)	20161202
K7GW	Riskware (0040eff71)	20161203
Kaspersky	Trojan-Ransom.MSIL.Tear.bf	20161203
Malwarebytes	Ransom.Fantom	20161203
McAfee	Generic.grp	20161203
McAfee-GW-Edition	BehavesLike.Win32.FakeAlert.dc	20161202
eScan	Trojan.Agent.BXUU	20161203
Microsoft	Ransom:MSIL/Fantomcrypt.A	20161202
NANO-Antivirus	Trojan.Win32.CLYD1190.efuods	20161203
Panda	Trj/CI.A	20161202
Qihoo-360	Trojan.Generic	20161203
Sophos	Troj/Fantom-B	20161203

Symantec	Trojan.Gen	20161203
Tencent	Win32.Trojan.Raas.Auto	20161203
TheHacker	Trojan/Filecoder.Fantom.a	20161130
TrendMicro	Ransom_FANTOMCRYPT.A	20161203
TrendMicro-HouseCall	Ransom_FANTOMCRYPT.A	20161203
VBA32	Hoax.MSIL.Tear	20161202
VIPRE	Trojan.Win32.Generic!BT	20161203
ViRobot	Trojan.Win32.Z.Agent.267776.AW[h]	20161203
Yandex	Trojan.Tear!	20161202
Zillya	Trojan.Tear.Win32.10	20161202
nProtect	Trojan/W32.Agent.267776.GC	20161203

۸ خلاصه نحوه عملکرد و شناسایی بدافزار

در جدول زیر مشخصات بدافزار مذکور به همراه رویکرد تشخیص و پاکسازی به صورت خلاصه مشاهده می‌شود.

شناسنامه بدافزار	نام	Fantom
	سال کشف	۲۰۱۶
	روش انتشار	- پست الکترونیک حاوی لینک فایل باج افزار
	تاثیرات	- رمزگذاری کردن فایل های کاربر

راهکارهای پیشگیری	سطح شبکه	✓ استفاده از ضد ویروس های تحت شبکه و بروز نگه داشتن آنها
	سطح میزبان	✓ به روز بودن نرم افزار ضدبدافزار نصب شده برروی سیستم ✓ اجتناب از دانلود و باز کردن فایل های ضمیمه ایمیل های ناشناس و نامعتبر ✓ محدودسازی سطح دسترسی کاربر ✓ نظارت بر ترافیک شبکه برای ارتباطات C&C به طور مداوم

۹ گزارش تحلیل

۹-۱ ایجاد چندین فایل

هنگامی که فایل مخرب اجرا شود، چند فایل در سیستم ایجاد می کند:

- فایل عکس پس زمینه:

%UserProfile%\2d5s8g4ed.jpg

- ایجاد فایل bat برای پاک کردن فایل های Shadow سیستم:

- %AppData%\delback.bat
    - vssadmin delete shadows /all /quiet

- ایجاد فایل اجرایی برای نمایش صفحه جعلی بروزرسانی ویندوز

- [Executable_Path]\WindowsUpdate.exe

- ایجاد فایل bat برای پاک کردن فایل اصلی باج افزار

- [Executable_Path]\update.bat
    - @echo off
      del fantom.exe
      del %0

۹-۲ تغییرات رجیستری

این باج افزار با استفاد از کلید های رجیستری Task Manager را غیر فعال می کند

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System "DisableTaskMgr" = 1

همچنین تصویر پس زمینه را نیز تغییر می دهد:

HKCU\Control Panel\Desktop\ "Wallpaper" "%UserProfile%\How to decrypt your files.jpg"

۹-۳ ارتباط با C&C

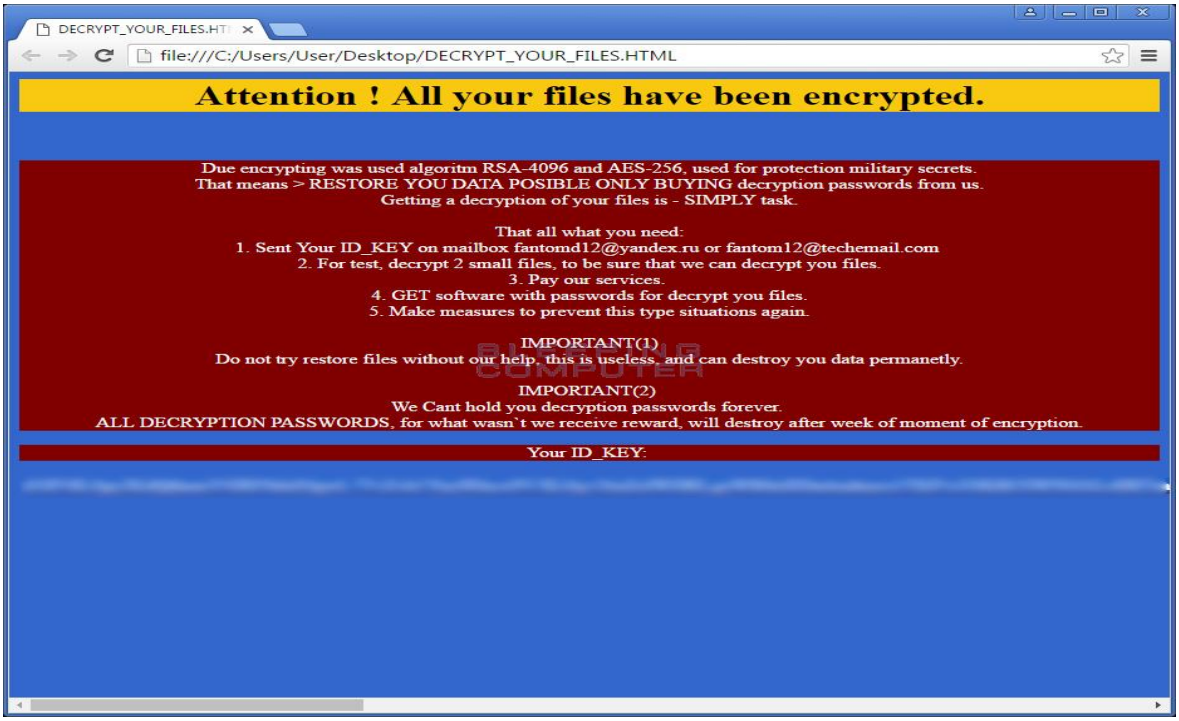
این باج افزار برای ارتباط با سرور C&C خود از آدرس های زیر استفاده می کند:

http://powertoolsforyou.com/themes/prestashop/cache/stats.php

http://templatesupdates.dlinkddns.com/falssk/fksgieksi.php

۹-۴ عملیات رمزنگاری

عملیلت رمز نگاری این باج افزار دقیقا مانند سایر باج افزار های بر پایه ی EDA2 است، این باج افزار یک کلید تصادفی AES-128 درست می کند، با استفاده از RSA آن را رمز نگاری به سرور C&C توسعه دهندگان بدافزار می فرستد. سپس این باج افزار شروع به گشتن درایو های محلی برای پیدا کردن فایل هایی که مورد هدف هستند کرده و آن ها را با استفاده از روش AES-128 رمز نگاری می کند. وقتی این باج افزار فایلی را رمز نگاری می کند، به فایل پسوند .fantom اضافه می کند. برای مثال apple.jpg به apple.jpg.fantom تبدیل می شود. در هر پوشه ای که عملیات رمزنگاری صورت بگیرد یک نوشته‌ی باج خواهی با نام DECRYPT_YOUR_FILES.HTML هم تولید می شود.



کد داخلی Fantom که به زبان سی شارپ نوشته شده است شامل توابع زیر است:

- extractResource(string embeddedFileName, string destinationPath)
- GetInt(RNGCryptoServiceProvider rnd, int max)
- CreatePassword(int length)
- RandomRansom(int length)
- AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
- KillCtrlAltDelete()
- RSAEncrypt(byte[] data, int keySize, string publicKeyXml)
- SelfDeleteWinupdate()
- SelfDelete()
- DelBack()

فایل صفحه ساختگی Update ویندوز به صورت رمز شده درون resource فایل اصلی وجود دارد. پس از اجرای باج افزار، تابع extractResource عملیات استخراج فایل مربوطه را انجام می دهد.

عملیات غیر فعال سازی TaskManager که از طریق دستکاری رجیستری صورت می گیرد توسط تابع KillCtrlAltDelete انجام می پذیرد.

توابع SelfDelete و SelfDeleteWinupdate برای حذف فایل باج افزار و فایل صفحه ساختگی بروزرسانی ویندوز نوشته شده اند.

کد این توابع در شکل زیر قابل مشاهده است:

```
// Token: 0x06000017 RID: 23 RVA: 0x00004B78 File Offset: 0x00002D78
public void SelfDelete()
{
    string executablePath = Application.ExecutablePath;
    StreamWriter streamWriter = new StreamWriter("update.bat");
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("del \"" + executablePath + "\"");
    streamWriter.WriteLine("del %0");
    streamWriter.Close();
    Process.Start("update.bat");
    Application.Exit();
}

// Token: 0x06000015 RID: 21 RVA: 0x00004A50 File Offset: 0x00002C50
public void SelfDeleteWinupdate()
{
    try
    {
        Process[] processesByName = Process.GetProcessesByName("WindowsUpdate");
        for (int i = 0; i < processesByName.Length; i++)
        {
            Process process = processesByName[i];
            process.Kill();
        }
    }
    catch
    {
    }
    StreamWriter streamWriter = new StreamWriter("update0.bat");
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("del \"" + this.string_5 + "\"");
    streamWriter.WriteLine("del %0");
    streamWriter.Close();
    Process.Start("update0.bat");
}
```

توسط توابع AES_Encrypt و RSAEncrypt عملیات رمزنگاری انجام می شود. کلید های مورد نیاز برای عملیات رمزنگاری توسط توابع CreatePassword و RandomRansom ایجاد می شود.

وقتی Fantom کار دستکاری کردن فایل های کاربر را تمام کرد، یک پنجره ی دیالوگ به شکل زیر نمایش می دهد (اگر کاربر Administrator نباشد):

اگر کاربر به اسکریپت delback.bat که در بالا ذکر شده اجازه ی اجرا شدن دهد، در واقع دستورات زیر را وارد کرده است:

vssadmin delete shadows /all /quiet

این دستور نسخه های پشتیبان فایل ها را روی دیسک حذف می کند. این اسکریپت توسط تابع DelBack واقع در کد اصلی باج افزار تولید می شود.

در آخر هم باج افزار یک فایل نوشته ی باج خواهی با عنوان DECRYPT_YOUR_FILES.HTML را به کاربر نشان می دهد که شامل ID قربانی بوده و راه هایی برای برگرداندن اطلاعات قربانی به او پیشنهاد می دهد.

اگر تصاویر باج خواهی سایر باج افزار ها را دیده باشید، می دانید که در این مرحله معمولا چیزی شبیه به حالت های زیر را میبینید:

- پولی که باید پرداخت کنید باید از طریق Bit Coin پرداخت شود.
- یک آدرس ناشناخته ی Tor (onion) برای برقراری تماس با کلاهبرداران وجود دارد.

بر خلاف باج افزارهای دیگر که یک شماره حساب بیتکوین و یک آدرس در شبکه Tor برای ارتباط با کلاهبرداران می دهند ، Fantom فقط از قربانی می خواهد که با یکی از دو آدرس ایمیل رایگان برای گرفتن دستورات بعدی ارتباط برقرار کند. این موضوع به این معنی است که عاملان می توانند به راحتی ردیابی و دستگیر شوند.

در نهایت باج افزار یک فایل عکس را دانلود کرده و آن را در آدرس

%UserProfile%\2d5s8g4ed.jpg

ذخیره می کند. این عکس از آدرس زیر دانلود شده که ممکن است درباره ی هویت توسعه دهنده ی باج افزار اطلاعاتی دهد:

http://content.screencast.com/users/Gurudrag/folders/Default/media/9289aabe-7b4a-4c7f-b3bb-bdf3407e7a2f/fantom1.jpg

عکس دانلود شده به شکل زیر می باشد و به عنوان تصویر پس زمینه ی کاربر استفاده می شود.

۱۰ جمع بندی

باج افزار Fantom یک باج افزار جدید است که بر پایه ی پروژه ی باج افزار متن باز EDA2 می باشد و اقدام به رمزنگاری فایل های کاربر می کند. این باج افزار از یک صفحه ی به روز رسانی تقلبی ویندوز تحت عنوان اینکه ویندوز در حال نصب به روز رسانی های حیاتی می باشد استفاده می کند. این باج افزار صفحه ی به روز رسانی ویندوز تقلبی را به کاربر نشان می دهد ولی در پشت زمینه در حال رمزنگاری فایل های قربانی می باشد. متاسفانه در حال حاضر هیچ راهی برای رمز گشایی کردن فایل های رمز شده با باج افزار Fantom وجود ندارد.

۱۱ منابع

- https://blog.threattrack.com/fantom-ransomware-windows-update/
- https://github.com/utkusen/eda2
- https://nakedsecurity.sophos.com/2016/09/02/fantom-ransomware-pretends-to-be-a-windows-critical-update/
- http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/
- https://blog.kaspersky.com/fantom-ransomware/12891/