باسمه تعالی

گزارش تحلیل باج‌افزار
CRYSIS

مقدمه

باج‌افزار Crysis برای اولین بار در سال ۲۰۱۶ مشاهده شد و به تازگی نیز در میان کاربران ایرانی شایع شده است. این باج‌افزار از تنظیمات ناامن RDP (کنترل دسکتاپ از راه دور) سوء استفاده می‌کند و با به‌دست آوردن نام کاربری و رمز عبور کاربران به سیستم قربانی از راه دور دسترسی پیدا کرده و فایل اجرایی خود را به صورت دستی در سیستم قربانی اجرا می‌کند. رمزعبورهای ضعیف تنظیم شده برای RDP راه ورود این باج‌افزار به سیستم را بسیار آسان می‌کند.

مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده بدین شرح است:

Property	Value
MD۵	۰۹۴۰۷۹۴AF۱۰۱۹۰BCEF۰۴۹۲۷۶۱۶D۸۳B۹C
SHA۱	a۲۳۲۸۱fbf۱۲b۱۲d۶۵۱۵۴۹fa۷۹۶d۸۷۳۵۹۳۸۲af۳۰۷
SHA۲۵۶	۹۱۶۶۶ac۰ca۹c۷۰۴b۹be۸۸۷۴۶c۰۴۹۴b۴f۰۲۵۸d۰۸۲۴۵۱ae۲dbe۷d۱۸db۰۰c۲۴d۱۱a
Tima Datastamp	Fri Nov ۱۰ ۱۱:۴۲:۵۳ ۲۰۱۷
Size (bytes)	۹۴,۷۲۰
type	Executable (GUI)

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 ۶۸ موتور تشخیص بدافزار ۵۶ عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

virustotal

SHA256:	91666ac0ca9c704b9be88746c0494b4f0258d082451ae2dbe7d18db00c24d11a
File name:	Local Host Proceses.exe
Detection ratio:	56 / 68
Analysis date:	2018-03-08 06:50:46 UTC (1 week, 3 days ago)

Analysis | File detail | Additional information | Comments 3 | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Ransom.Crysis.6	20180308
AegisLab	Troj.W32.Generic!c	20180308
AhnLab-V3	Trojan/Win32.Genasom.C1488611	20180307
ALYac	Trojan.Ransom.Crysis	20180308
Antiy-AVL	Trojan/Win32.AGeneric	20180307
Arcabit	Trojan.Ransom.Crysis.6	20180307
Avast	Win32:Malware-gen	20180308
AVG	Win32:Malware-gen	20180308
Avira (no cloud)	TR/Dropper.Gen	20180308
AVware	Trojan.Win32.Generic!BT	20180308
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9996	20180308

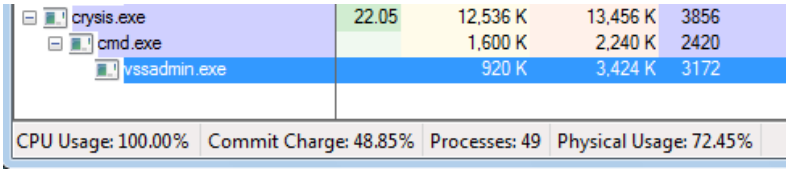
گزارش تحلیل

بررسی‌های اولیه نشان داد که این باج‌افزار برای گریز از تشخیص داده شدن توسط ضدبدافزارها، کتابخانه‌ها و رشته‌های مورد استفاده را رمز کرده و در زمان اجرا آن‌ها را بارگذاری می‌کند.

این باج‌افزار پس از اجرا شدن ابتدا نسخه‌ای از خود را در مسیر AppData\Roaming کپی می‌کند و برای کسب ماندگاری در سیستم نام این فایل را به عنوان مقداری برای کلیدهای رجیستری HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run و

HKCU\Software\Microsoft\Windows\CurrentVersion\Run تنظیم می‌کند. همچنین بدافزار نسخه‌هایی از خود را در مسیرهای AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup و %win dir%\System۳۲\crysis.exe نیز کپی می‌کند.

سپس بدافزار پردازه cmd.exe را اجرا و در cmd به ترتیب فرمان‌های Mode con cp select=۱۲۵۱ و Vssadmin delete shadows /all /quiet را اجرا می‌کند که برای پاکسازی حافظه بکاپ و غیرممکن ساختن بازیابی اطلاعات به کار می‌رود.



بررسی انواع فایل‌های مختلف موجود در سیستم برای رمز کردن و شیوه نام‌گذاری

این باج‌افزار انواع مختلف فایل‌های موجود در سیستم را رمز کرده و با نام زیر ذخیره می‌کند:

<Original file name>.id-<volume serial number of drive C >.{mazma@india.com}.java

مقدار ایمیل مورد استفاده در نام‌گذاری فایل‌ها در نسخه‌های مختلف این باج‌افزار متفاوت است. برخی از ایمیل‌های استفاده شده در این باج‌افزار عبارتند از:

- faremar@cock.li
- decrypthelp@qq.com
- habibi.habibi۳@aol.com
- black.mirror@qq.com
- chivas@aolonline.top

انواع مختلف فایل‌هایی که این باج‌افزار آن‌ها را رمز می‌کند عبارتند از:

lcd,۳ds,۳fr,۳g۲,۳gp,۷z,accda,accdb,accdc,accde,accdt,accdw,adb,adp,ai,ai۳,ai۴,ai۵,ai۶,ai۷,ai۸,
anim,arw,as,asa,asc,ascx,Asm,asmx,asp,aspx,asr,asx,avi,avs,backup,bak,bay,bd,bin,bmp,bz۲,c,
cdr,cfm,cfml,cfu,chm,cin,class,clx,config,cpp,cr۲,crt,crw,cs,css,csv,cub,dae,dat,db,dbf,dbx,dcm,
dcr,der,dib,dic,divx,djvu,dng,doc,docm,docx,dot,dotm,dotx,dpx,dqy,dsn,dt,dtd,dwg,dwt,dx,dxf,

edml,efd,elf,emf,emz,epf,eps,epsf,epsp,erf,exr,f۴v,fido,flm,flv,frm,fxg,geo,gif,grs,gz,h,hdr,hpp,
hta,htc,htm,html,icb,ics,iff,inc,indd,ini,iqy,j۲c,j۲k,java,jp۲,jpc,jpe,jpeg,jpf,jpg,jpx,js,jsf,json,jsp,
kdc,kmz,kwm,lasso,lbi,lgf,lgp,log,m۱v,m۴v,max,md,mda,mdb,mde,mdf,mdw,mef,mft,mfw,mht,
mhtml,mka,mkidx,mkv,mos,mov,mp۳,mp۴,mpeg,mpg,mpv,mrw,msg,mxl,myd,myi,nef,nrw,obj,
odb,odc,odm,odp,ods,oft,one,onepkg,onetoc۲,opt,oqy,orf,p۱۲,p۷b,p۷c,pam,pbm,pct,pcx,pdd,pdf
,pdb,pef,pem,pff,pfm,pfx,pgm,php,php۳,php۴,php۵,phtml,pict,pl,pls,pm,png,pnm,pot,potm,potx,
ppa,ppam,ppm,pps,ppsm,ppt,pptm,pptx,prn,ps,psb,psd,pst,ptx,pub,pwm,pxr,py,qt,r۳d,raf,rar,raw
,rdf,rgbe,rle,rqy,rss,rtf,rw۲,rwl,safe,sct,sdpx,shtm,shtml,slk,sln,sql,sr۲,srf,srw,ssi,stm,svg,svgz,
swf,tab,tar,tbb,tbi,tbk,tdi,tga,thmx,tif,tiff,tld,torrent,tpl,txt,u۳d,udl,uxdc,vb,vbs,vcs,vda,vdr,vdw,
vdx,vrp,vsd,vss,vst,vsw,vsx,vtm,vtml,vtx,wb۲,wav,wbm,wbmp,wim,wmf,wml,wmv,wpd,wps,
x۳f,xl,xla,xlam,xlk,xls,xlsb,xlsm,xlsx,xlt,xltm,xltx,xlw,xml,xps,xsd,xsf,xsl,xslt,xsn,xtp,xtp۲,
xyze,xz,zip.

برای امکان ادامه به کار سیستم و عملیات رمز کردن فایل‌ها، این باج‌افزار از فایل‌های سیستمی و فایل‌های اجرایی خود و نیز فایل راهنمای رمزگشایی در برابر رمز شدن مراقبت می‌کند. همچنین برای رمز کردن فایل پایگاه داده‌ها، بدافزار سرویس‌های مربوط به برخی از پایگاه داده‌ها شامل fbguard، Fbserver، mysql، postgres، Sqlwriter، mssqlserv، mssqlserver و ssqlserveradhelper را در صورت وجود متوقف می‌کند.

عملیات رمز کردن فایل‌ها

این باج‌افزار برای رمز کردن اطلاعات از الگوریتم سفارشی‌سازی شده AES-۱۲۸ استفاده می‌کند. کلید رمز با استفاده از الگوریتم SHA-۱ تولید می‌شود و به نظر می‌رسد برای هر فایل، نام تغییر یافته آن است (نام فایل با پسوند java. در پایان آن) و به همین دلیل کاربران نباید نام جدید فایل را تغییر بدهند تا رمزگشایی داده‌ها ممکن باشد. پس از رمز کردن کامل فایل‌ها، پردازه mshta.exe اجرا می‌شود که پیام زیر را برای کاربر نمایش می‌دهد. این فایل به عنوان مقدار برای کلید رجیستری HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run تنظیم می‌شود.

همچنین فایلی به نام Decryption Instructions.txt در صفحه نمایش ذخیره می‌شود که دستورالعمل رمزگشایی فایل‌ها به شرح زیر در آن دیده می‌شود:

All of your files are encrypted, to decrypt them write me to email: mazma@india.com

این باج‌افزار برای کسب اعتماد کاربر این امکان را فراهم می‌کند که ۵ فایل که اندازه کلی آن‌ها از ۱۰ مگابایت بیشتر نباشد را به صورت رایگان رمزگشایی کنند. شیوه پرداخت برای رمزگشایی فایل‌ها با استفاده از خرید بیت‌کوین انجام می‌شود. هزینه رمزگشایی تعیین نشده و به مدت زمان ارسال درخواست برای رمزگشایی بستگی دارد.

نتیجه‌گیری

باج‌افزار CRYSIS(Dharma) که برای اولین بار در سال ۲۰۱۶ شایع شد، از تنظیمات ناامن RDP (کنترل دسکتاپ از راه دور) سوء استفاده می‌کند و با به‌دست آوردن نام کاربری و رمز عبور کاربران به سیستم قربانی از راه دور دسترسی پیدا کرده و فایل اجرایی خود را به صورت دستی در سیستم قربانی اجرا می‌کند. رمزعبورهای ضعیف تنظیم شده برای RDP راه ورود این باج‌افزار به سیستم را بسیار آسان می‌کند.

این باج‌افزار، فایل‌های موجود در سیستم کاربر را رمزگذاری کرده و (در نمونه تحلیل شده) آن‌ها را با پسوند java. ذخیره می‌کند. توصیه می‌شود کاربران برای جلوگیری از آلوده شدن به این باج‌افزار در صورت عدم نیاز به RDP آن را غیر فعال کرده و در صورت نیاز به این سرویس از رمزعبورهای قوی استفاده نمایند؛ همچنین وصله‌های امنیتی را نصب کنند.

با توجه به این که باج‌افزار قادر به رمز کردن فایل‌های موجود در پوشه اشتراکی سیستم و حذف اطلاعات بکاپ سیستم است، توصیه می‌شود کاربران به پشتیبان‌گیری از فایل‌های موجود در سیستم خود و فایل‌های به اشتراک گذاری شده در شبکه نیز اقدام نمایند و در مکانی خارجی ذخیره نمایند.

این باج‌افزار در فروم‌های مختلف به فروش می‌رسد. نسخه‌های مختلف این باج‌افزار به طور کلی رفتار مشابهی دارند اما از ایمیل‌ها و پسوندهای مختلفی برای فایل‌های رمز شده استفاده می‌کنند. برای نمونه در نمونه باج‌افزار مشابهی به نام Saraswati از شیوه زیر برای نام‌گذاری فایل‌ها استفاده شده است.

id-????????.{mahasaraswati@india.com}.xtbl
id-????????.[webmafia@asia.com].wallet

تصویر نمایش داده شده برای کاربر و نیز راهنمای رمزگشایی نیز در نسخه‌های مختلف متفاوت است. پیش‌بینی می‌شود همان گونه که تاکنون این باج‌افزار روند رو به رشد و قابل توجهی از آلودگی در میان کاربران ایرانی داشته است، از این پس نیز با نسخه‌های مختلفی از این باج‌افزار مواجه خواهیم بود.