CrySiS勒索病毒变种分析

深信服千里目安全实验室 / 2018-03-19 18:57:05 / 浏览数 18556 安全技术 漏洞分析 顶(0) 踩(0)

样本简介

最近接到客户举报，服务器文件被勒索软件加密，联系客户远程应急之后拿到相应的样本，判定该样本为CrySiS家族的最新变种样本。

CrySiS勒索病毒在2017年5月万能密钥被公布之后，消失了一段时间，最近又发现这类勒索病毒的新的变种比较活跃，攻击方法同样是通过远程RDP爆力破解的方式，植入至

而且从文件的编译的时间上来看，样本相对较新，如图所示：

样本行为分析

(1)勒索病毒首先创建互斥变量，防止被多次运行，如图所示：

(2)拷贝自身到相应的目录，相应的目录列表如下：

%windir%\System32
%appdata%
%sh(Startup)%
%sh(Common Startup)%
样本拷贝自身到相应的目录下之后，设置自启动项，如图所示：

同时它还会在样本对应的目录下分别释放一个勒索信息的配置文件Info.hta，并设置为自启动项，用于弹出相应的勒索界面，如下图所示：

(3)枚举电脑里的对应的服务，并结束，如图所示：

相应的服务列表如下所示：

Windows Driver Foundation
User mode Driver Framework
wudfsvc
Windows Update
wuauserv
Security Center
wscsvc
Windows Management
Instrumentation
Winmgmt
Diagnostic Service Host
WdiServiceHost
VMWare Tools
VMTools.Desktop
Window Manager Session Manager
.....

相应的反汇编代码如下：

(4)枚举电脑里的相应的进程，并结束，如下图所示：

相应的进程列表如下：
1c8.exe
1cv77.exe
outlook.exe
postgres.exe
mysqld-nt.exe
mysqld.exe
sqlserver.exe
从上面的列表可以看出，此勒索病毒主要结束相应的数据库程序，防止这些程序占用相应的文件无法加密服务器的数据库文件,相应的反汇编代码如下所示：

(5)册除电脑里的相应的卷影，防止通过数据恢复的方式还原文件，如下图所示：

通过查看进程列表，如图所示：

相应的反汇编代码,如下图所示：

（6）遍历枚举局域网的共享目录文件，对共享目录文件进行加密，如下图所示：

(7)文件加密过程，如下所示：
(A)循环遍历文件目录，查找相关的文件，如果是以下文件，则不进行加密，保证电脑系统运行正常，相关的文件名如下：
boot.ini;bootfont.bin;ntldr;ntdetect.com;io.sys;
枚举文件的相关反汇编代码如下所示：

(B).通过内存解密字符串，得到要加密的文件的后缀名，如图所示：

勒索病毒加密的文件扩展名如下：
.1cd;.3ds;.3fr;.3g2;.3gp;.7z;.accda;.accdb;.accdc;.accde;.accdt;
.accdw;.adb;.adp;.ai;.ai3;.ai4;.ai5;.ai6;.ai7;.ai8;.anim;.arw;.as;.asa;.asc;.ascx;.asm;.asmx;.asp;.aspx;.asr;.asx;.avi;.avs;.backup;.bak;.bay;.bd;.bin;.bmp;
.bz2;.c;.cdr;.cer;.cf;.cfc;.cfm;.cfml;.cfu;.chm;.cin;.class;.clx;.config;.cpp;.cr2;.crt;.crw;.cs;.css;.csv;.cub;.dae;.dat;.db;.dbf;.dbx;.dc3;.dcm;.dcr;.der;
.dib;.dic;.dif;.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;.f4v;.fido;.flm;.flv;.frm;.fxg;.geo;.gif;.grs;.gz;.h;.hdr;.hpp;.hta;.htc;.htm;.html;.icb;.ics;.iff;.inc;.indd;.ini;.iqy;.j2c;.j2k;.java;.jp2;.jpc;
.jpe;.jpeg;.jpf;.jpg;.jpx;.js;.jsf;.json;.jsp;.kdc;.kmz;.kwm;.lasso;.lbi;.lgf;.lgp;.log;.m1v;.m4a;.m4v;.max;.md;.mda;.mdb;.mde;.mdf;.mdw;.mef;.mft;.mfw;.mht;
.mhtml;.mka;.mkidx;.mkv;.mos;.mov;.mp3;.mp4;.mpeg;.mpg;.mpv;.mrw;.msg;.mxl;.myd;.myi;.nef;.nrw;.obj;.odb;.odc;.odm;.odp;.ods;.oft;.one;.onepkg;.onetoc2;.op
.oqy;.orf;.p12;.p7b;.p7c;.pam;.pbm;.pct;.pcx;.pdd;.pdf;.pdp;.pef;.pem;.pff;.pfm;.pfx;.pgm;.php;.php3;.php4;.php5;.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;.r3d;.raf;.rar;.raw;.rdf;.rgbe;.rle;.rqy;.rss;.rtf;.rw2;.rwl;
.safe;.sct;.sdpx;.shtm;.shtml;.slk;.sln;.sql;.sr2;.srf;.srw;.ssi;.st;.stm;.svg;.svgz;.swf;.tab;.tar;.tbb;.tbi;.tbk;.tdi;.tga;.thmx;.tif;.tiff;.tld;.torrent;.tpl;.txt;
.u3d;.udl;.uxdc;.vb;.vbs;.vcs;.vda;.vdr;.vdw;.vdx;.vrp;.vsd;.vss;.vst;.vsw;.vsx;.vtm;.vtml;.vtx;.wb2;.wav;.wbm;.wbmp;.wim;.wmf;.wml;.wmv;.wpd;.wps;.x3f;.xl;.xla;.xlam;.xl
后面加密的时候会比较相应的文件扩展名，然后对上面的文件类型进行加密，相应的反汇编代码如下：

(C)通过内存解密，得到加密后的文件名字符串特征，如下图所示：

加密后的文件的后缀名被：文件名.id-AC8D65A2.[debugs@protonmail.com].java的形式
（D)加密文件的时候，先判断文件的大小，当文件大小大于0x180000字节时，直接对文件内容进行加密，并将文件重命名，当文件大小小于等于0x180000字节时，则创建

加密文件之后，对于文件大小小于0x180000字节的文件，在文件未尾部分写入如下信息，以供黑客解密文件时使用，相关的反汇编代码如下所示：

加密后的文件未尾布局如下所示：

动态调试如下图所示：

加密完文件之后，删除掉原文件，如下图所示：

对于文件大小大于0x180000字节的文件，加密文件之后，在文件的未尾写入如下信息，以供黑客解密文件时使用，如下图所示：

加密后的文件未尾布局如下所示：

然后重命名原文件，动态调试的相关代码如下所示：

加密后的文件未尾数据如下所示：

(E)加密的密钥大小块为184字节，前32字节存放RC4加密后的随机数密钥，该密钥用于之后加密文档。为了加强随机性，程序通过RDTST函数读取时间计数器，最后通过RC

密钥块第33字节存放系统序列号GUID:
905D7E25h，用于唯一标记符。之后的128字节存放RSA加密后的随机密钥，而RSA公钥的SHA-1值则存放在最末端的20字节中，相关的反汇编代码如下所示：

生成的密钥分部结构如下图所示：

(8)勒索病毒还会连接远程服务器进行相关操作，由于调试的时候服务器数据已关闭，只能通过相应的反汇编代码进行程查看，动态调试发现如下相关函数：
00418804 socket
00418808 send
0041880C recv
00418810 connect
00418814 closesocket
00418818 gethostname
0041881C inet_addr
00418820 ntohl
00418824 htonl
00418828 ntohs
猜测相关功能有可能是将密钥数据和系统相关信息发送到黑客的服务器上，具体功能已无法还原。
(9)勒索病毒会在前期解密相关的API函数名称，并获取相关地址，如下图所示：

动态调试跟踪，获取IAT表地址的过程，如下所示：

(10)整个勒索病毒的主函数反汇编代码如下所示：

(11)勒索病毒运行之后，感染用户电脑，相关行为如下所示：

勒索病毒会通过调用rundll32.exe或mshta.exe进程，执行勒索病毒的勒索信息文件Info.hta，弹出几个如上图所示的勒索界面，执行的命令如下所示：

防御方式

千里目安全实验室提醒广大用户，平时注意以下安全防范措施：

1.不要点击来源不明的邮件以及附件
2.及时给电脑打补丁，修复漏洞
3.对重要的数据文件定期进行非本地备份
4.安装专业的终端/服务器安全防护软件
5.CrySis勒索软件主要通过RDP爆力破解的方式进行传播，建议用户关闭相应的RDP服务，同时它会加密用户的共享目录文件下的文件，建议用户关闭共享目录文件
6.尽量关闭不必要的文件共享权限以及关闭不必要的端口，如：445,135,139,3389等