【独家】zepto勒索软件分析

diffway / 2017-01-18 05:09:13 / 浏览数 3857 安全技术 漏洞分析 顶(0) 踩(0)

1.概述

黑客通过群发邮件的方法，诱导用户点击，点击后，从黑客控制的网站服务器中下载加密的勒索软件，解密后经过分析发现是属于LOCKY家族的zepto勒索软件，zepto是今

2.详细分析

黑客通过将恶意的js下载者文件压缩的方式来逃避传统的杀毒软件的检测。下面是收集到的压缩文件。
0e1cc40d9f3d7eb97eacf618384ab7c70df3d9a2e38b23fde70c8269f5c33807
882af2ae159505681b146aac2092ae2f888a6cd28f08093de045155baadcc122
9779195cabb5547307cfad9e52d543fda56f3e8ff8eb517289d2ac15eba89ee4
a25e21c1a34f4639b8b816c0e7daf96bb1feaf65a4f32a9e629a2909d63c41bd
在用户将压缩文件打开就可以看到里面的hta文件，hta虽然用HTML、JS和CSS编写，

却是一个独立的应用软件。在用户双击后下载勒索软件。

hta文件hash如下
c28480a18bb444f1932cafe1ffe65544d3624840f82c204e045834b0e5004ac7
e970237971a88052964a8a57807a8315ce862dd2d8d5aa8fcd14e419bed1ebd5
aee3478b5f6782c9adcabf84bce7992e84634b9e4e7277f34bdb2fc678a7bf66
4e875a71ee290396c5bc3cb2db583d24fdf9bbb5e5b1bcd932ce12dd3cc2daaa
252c1e2ab29b8c077edbf5f69d9f0382554d0751dcb96e8c1a29c0ce331b035b
c28480a18bb444f1932cafe1ffe65544d3624840f82c204e045834b0e5004ac7
94c792d255b0afeaac9db3eff5fd72a654e9c5f726a70b061b550dc0564fcef
下面选择一个进行详细分析
样本信息
文件名称
XJCV3427.hta
文件SHA256
aee3478b5f6782c9adcabf84bce7992e84634b9e4e7277f34bdb2fc678a7bf66
文件类型
Hta

里面是经过混淆的js文件

经过解混淆，可以发现文件会从两个地址下载两个文件，将两个文件进行解密成一个dll文件，通过rundll32.exe进行加载。加载命令为C:\WINDOWS\system32\rundll32.e
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp/解密文件.dll,qwerty

发现从下面两个网址进行下载，下载的URL为
blivenews.com/746t3fg3
pvtltdregistration.com/746t3fg3
下载的两个文件是
da0c4063041c2e6111ebfb52e6ecaa1b3a5c5e978bf3544fae61c9620609d480
78900539b0e2907007f5de818ac69c89eaf7ff1b29f901ff84e65d0b1e718021
将下载的两个文件解密合成一个DLL文件，这样做的主要的目的主要是躲避安全软件的检查
下面详细分析下来的dll文件
文件信息
文件名称
IckGdv2.dll
SHA256
704eb9e3cc54bdafa1736f529ae0695d620a7c064e6d4fac591ab98ebe47fc0c
加壳
未知壳
文件大小
160 KB
编译时间
2016/9/22
数字签名
无
处理器架构
Intel386

详细分析，写个调用程序进行调用。

可以分析当文档遇到俄语系统时将不再进行感染

设置超长sleep进行睡眠，躲避沙箱跑出行为

通过使用哈希算法MD5为计算机磁盘的物理地址签名，系统版本和系统信息生成标识ID

[attachment=2943]

在加密的文件，还对网络共享目录进行搜索，如果有的话，也进行加密

枚举磁盘资源信息

修改文件访问权限
]

为了保证系统能正常运行来支付赎金下面文件夹和文件（系统文件夹）是不会被加密的]

对所有文件根据后缀名进行评比权重，其中权值最高的wallet.dat (比特钱包文件)为7，剩下的从6到-15之间 下面是加密的文件类型和权值。

.key
.crt
.csr
.p12
.pem
.doc
.odt
.ott
.sxw
.stw
6
6
6
6
6
5
5
5
5
5
.ppt
.xls
.pdf
.rtf
.uot
.csv
.txt
.xml
.3ds
.max
5
5
2
4
4
2
2
2
4
4
.3dm
.dot
.docx
.docm
.dotx
.dotm
.602
.hwp
.ods
.ots
4
4
4

4
4
4
4
4
5
5
.sxc
.stc
.dif
.xlc
.xlm
.xlt
.xlw
.slk
.xlsh
.xlsm
.xlsx
.xltm
.xltx
.wk1
.wks
.123
.wb2
.odp
.otp
.sxi
5
4
4
4
4
4
4
5
5
5
.sti
.pps
.pot
.sxd
.std
.pptm
.ppts
.potm
.potx
.uop
4
4
4
4
4
5
5
5
5
4
.odg
.otg
.sxm
.mml
.docb
.ppam
.ppsx
.ppsm
.sldx
.sldm
5
4

5
5
4
4
4
4
4
4
.ms11
.lay
.lay6
.asc
.onetoc2
.pst
.001
.002
.003
.004
4
4
4
4
5
5
2
2
2
2
.005
.006
.007
.008
.009
.010
.011
.SQLITE3
.SQLITEDB
.sql
2
2
2
2
2
2
2
3
3
3
.mdb
.db
.dbf
.odb
.frm
.MYD
.myi
.ibd
.mdf
.ldf
3
3
3
3
3
3
3
3
3
3
.php

.c
.cpp
.pas
.asm
.h
.js
.vb
.vbs
.pl
4
4
4
4
4
4
3
3
3
3
.dip
.dch
.sch
.brd
.cs
.asp
.rb
.java
.jar
.class
3
3
3
3
4
4
4
3
3
3
.pl
.sh
.bat
.cmd
.psd
.nef
.tiff
.tif
.jpg
.jpeg
3
3
3
3
1
-2
-3
-3
-3
-3
.cgm
.raw
.gif
.png
.bmp
.svg
.djvu
.zip
.rar
.7z

-3
-3
-4
-4
-4
-4
-4
-10
-10
-10
.gz
.tgz
.tar
.bak
.tbk
.tar.bz2
.paq
.arc
.aes
.gpg
-10
-10
-10
-10
-10
-10
-10
-10
-10
-10
-10
.apk
.asset
.assef
.bik
.bsa
.d3dbsp
.das
.forge
.iwe
.lbf
-10
-10
-10
-10
-10
-10
-10
-10
-10
-10
-10
.litemo
.litesq
.ltx
.re4
.sav
.upk
.wallet
.vmdk
.vdi
.qco2
-10
-10
-01
-10
-10
-10
-10
-12
-12

-12
.mp3
.wav
.swf
.wmv
.mpg
.vob
.mpeg
.avi
.mov
.mp4
-15
-15
-15
-15
-15
-15
-15
-15
-15
-15
.3gp
.mkv
.3g2
.flv
.wma
.mid
.m3u
.m4u
.m4a
.n64
-15
-15
-15
-15
-15
-15
-15
-15
-15
-15
4

在这些权值中还要比较文件大小，文件越大减的数值越多，最后出一个综合权值，文件越大，分数越小，在计算出文件分数后，分数越高越先被加密，分数低的，后被加密。

分数算法如下
如果文件大小大于0x100000字节
分数=基础分-5
如果文件大小大于0XA00000字节
分数=基础分-15
如果文件大小大于0x6400000字节
分数=基础分-25
如果文件大小大于0x3E800000字节
分数=基础分-35

可以看到使用的加密算法为

可以发现使用的密钥交换和签名算法为RSA

导入RSA公钥

导入的公钥

生成AES随机密钥，并对文档进行加密

并且删除所有卷影副本

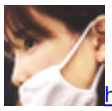
并且可以回传用户信息

将加密后的文件随机生成文件名
UUB6IMA8-TAQI-48FJ-BB4C-97E142067AC0.zepto

下面是显示给用户的支付赎金的界面

经过分析黑客入侵了很多站点，将勒索软件软件放在上面，下面是收集到的站点
http://abdulqadirmahar.com/
http://accentofficefurniture.co.nz
http://afzalbaloch.comli.com
http://appleappdeveloper.com/
http://attractions.com/
http://blivenews.com/
http://cardimax.com.ph/
http://celebratebanking.com/
http://deftr.com/
http://dmlevents.com/
http://emaster.4devlab.com/
http://flyingbtc.com/
http://graybowolson.com/
http://greenkeralatravels.com/
http://grimkonde.net/
http://hrx.net.au/
http://imsalud.gov.co/
http://indglobaldemo.com/
http://infosunsystem.com/
http://lsnsoft.info/
http://managedv2.4devlab.com/
http://micaraland.com/
http://muhammadyunus.org/
http://myownindia.com/
http://nsgroup.in/
http://prettynicewebsite.com/
http://pvtltdregistration.com/
http://ringspo.com/
http://satyagroups.in/
http://tvorbis.com.mk/
http://venussystems.in/
http://www.barodawebsolution.com/
http://www.bujod.in/
http://www.e-media.in/
http://www.mango-do.com

上一篇：微信小程序安全浅析 下一篇：针对俄罗斯社科院的定向勒索分析
1. 1 条回复

 hades 2017-01-21 09:58:42

楼主辛苦了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板