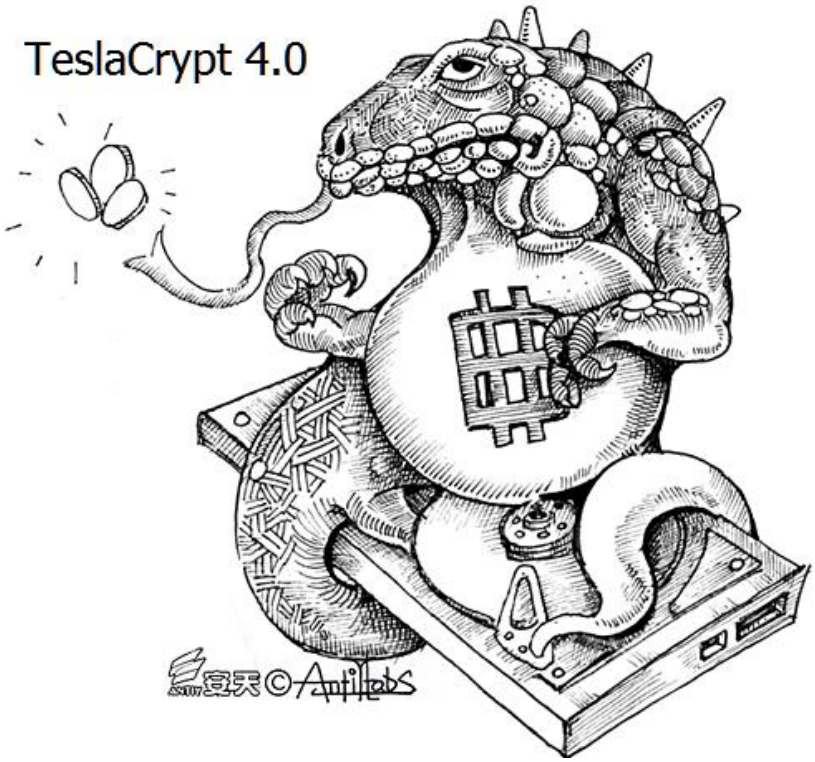
勒索软件家族 TESLACRYPT 最新变种技术特点分析

安天安全研究与应急处理中心（Antiv CERT）



报告初稿完成时间：2016 年 04 月 07 日 17 时 44 分

首次发布时间：2016 年 04 月 08 日 14 时 23 分

目 录

1 概述

安天安全研究与应急处理中心（Antiy CERT）近期发现勒索软件 TeslaCrypt 的最新变种 TeslaCrypt 4.0，它具有多种特性，例如：对抗安全工具、具有 PDB 路径、利用 CMD 自启动、使用非常规的函数调用、同一域名可以下载多个勒索软件等。尤其值得一提的是，通常勒索软件在感染受害主机后均会修改被加密文件的扩展名，如 TeslaCrypt 早期版本（.vvv、.mp3、.ccc、.abc、.ttt 等），其他勒索软件 Locky、CTB-Locker（.Locky，.oinpgca）。而 TeslaCrypt 的最新变种具有在加密文件后不修改原文件扩展名的特点。

勒索软件 TeslaCrypt 在 2015 年 2 月份左右被发现[1]，它是在 Cryptolocker 的基础上修改而成。在其第一个版本中，TeslaCrypt 声称使用非对称 RSA-2048 加密算法，但实际上使用的是对称的 AES 加密算法，由此 Cisco（思科）发布了一款解密工具，在找到可恢复主密钥的 key.dat 文件时，可以解密被 TeslaCrypt 勒索加密的文件[2]；但在之后的多个版本中，勒索软件 TeslaCrypt 开始使用非对称的 RSA 加密算法，被加密的文件在无密钥的情况下已经无法成功解密了，安天 CERT 发现，TeslaCrypt 4.0 在 2016 年 3 月份开始出现，使用的是 RSA-4096 加密算法。

勒索软件系列事件的出现，具有多方面原因，其中重要的一点是匿名网络和匿名支付的高度成熟。2016 年春节过后，勒索软件 **Locky** 开始爆发，全球多家安全厂商发布了相应的报告，安天 CERT 也在 2016 年 2 月 19 日发布了《首例具有中文提示的比特币勒索软件“LOCKY”》[3]；2016 年 3 月底，G-Data 和趋势先后发布了修改 MBR、加密整个硬盘的勒索软件 **Petya** 的报告；2016 年 4 月初，安天 CERT 开始跟踪勒索软件 **TeslaCrypt 4.0**。

2 传播方式

勒索软件 TeslaCrypt 4.0 利用网站挂马和电子邮件进行传播，在国内网站挂马发现的较少，通常利用浏览器漏洞（Chrome、Firefox、Internet Explorer）、Flash 漏洞和 Adobe Reader 漏洞进行传播；而利用电子邮件传播的数量较多，安天 CERT 发现的多起勒索软件事件也都是通过电子邮件传播的。

图 1 利用电子邮件传播勒索软件

在分析 TeslaCrypt 的下载地址时，安天 CERT 研究人员发现，相同域名下存放多个 TeslaCrypt 4.0 程序，且文件 HASH 各不相同。例如：域名 http://***pasqq.com，可以下载 TeslaCrypt 4.0 的地址如下：

```
http://***pasqq.com/23.exe
http://***pasqq.com/24.exe
http://***pasqq.com/25.exe
http://***pasqq.com/42.exe
http://***pasqq.com/45.exe
http://***pasqq.com/48.exe
http://***pasqq.com/69.exe
http://***pasqq.com/70.exe
http://***pasqq.com/80.exe
http://***pasqq.com/85.exe
http://***pasqq.com/87.exe
http://***pasqq.com/93.exe
```

另外，其他域名中勒索软件的下载地址同上，如：23.exe、24.exe、25.exe … 93.exe。至 2016 年 4 月 7 日 14 时，安天 CERT 共发现具有下载勒索软件 TeslaCrypt 4.0 的域名共 50 多个，部分域名已经失效。

部分下载勒索软件 TeslaCrypt 4.0 的域名：

```
***pasqq.com
***uereqq.com
***ghsqq.com
***rulescc.asia
***rulesqq.com
```

3 样本分析

安天 CERT 共发现近 300 个勒索软件 TeslaCrypt 4.0。研究人员在其中选择了时间较新的样本进行分析。

3.1 样本标签

病毒名称	Trojan[Ransom]/Win32.Teslacrypt
原始文件名	80.exe
MD5	30CB7DB1371C01F930309CDB30FF429B
处理器架构	X86-32
文件大小	396 KB (405,504 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	5704939E -->2016-04-06 12:42:06
数字签名	NO
加壳类型	未知
编译语言	Microsoft Visual C++
VT 首次上传时间	2016-04-06 04:07:00 UTC
VT 检测结果	28/57

3.2 使用 RSA4096 加密算法加密文件，但不修改原文件名

该样本运行后复制自身至%Application Data%文件夹中，重命名为 wlrmdr.exe，设置自身属性为隐藏，然后使用 CreateProcessW 为其创建进程。

```
00129944  00408090  CALL 到 CreateProcessW 来自 80.0040808E
00129948  00000000  ModuleFileName = NULL
0012994C  0012D9D8  CommandLine = "C:\Documents and Settings\Administrator\Application Data\wlrmdr.exe"
00129950  00000000  pProcessSecurity = NULL
00129954  00000000  pThreadSecurity = NULL
00129958  00000000  InheritHandles = FALSE
0012995C  00000020  CreationFlags = NORMAL_PRIORITY_CLASS
00129960  00000000  pEnvironment = NULL
00129964  00000000  CurrentDir = NULL
00129968  00129978  pStartupInfo = 00129978
0012996C  001299C4  pProcessInfo = 001299C4
00129970  7C800000  kernel32.7C800000
```

图 2 创建 wlrmdr.exe 进程

样本在新创建的进程中使用 CreateThread 开启线程，对全盘文件进行加密。首先样本使用 GetLogicalDriveStringsW 获取所有逻辑驱动器，成功后使用 FindFirstFileW 与 FindNextFileW 遍历全盘所有文件，进行加密。

```
0186B50C  00401A4D  CALL 到 FindFirstFileW 来自 wlrmdr.00401A4B
0186B510  0186D778  FileName = "C:\*.*"
0186B514  0186B528  pFindFileData = 0186B528
0186B518  00000000
0186B51C  0186FBB0  UNICODE "C:\"
0186B520  00A45AC8
```

图 3 遍历磁盘文件

加密函数地址为 0x0040190A。

图 4 调用加密函数对遍历到的文件加密

利用 RSA4096 算法加密后，调用 WriteFile 将加密后的数据由内存写入文件，没有对文件名做修改。

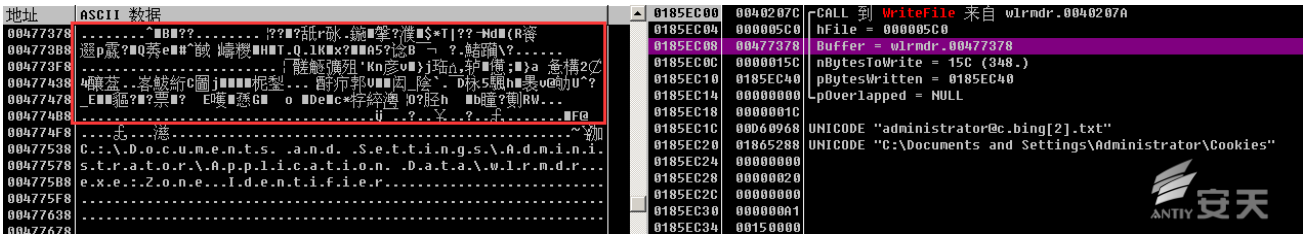


图 5 将加密后的数据写入文件

加密前后的文件对比：

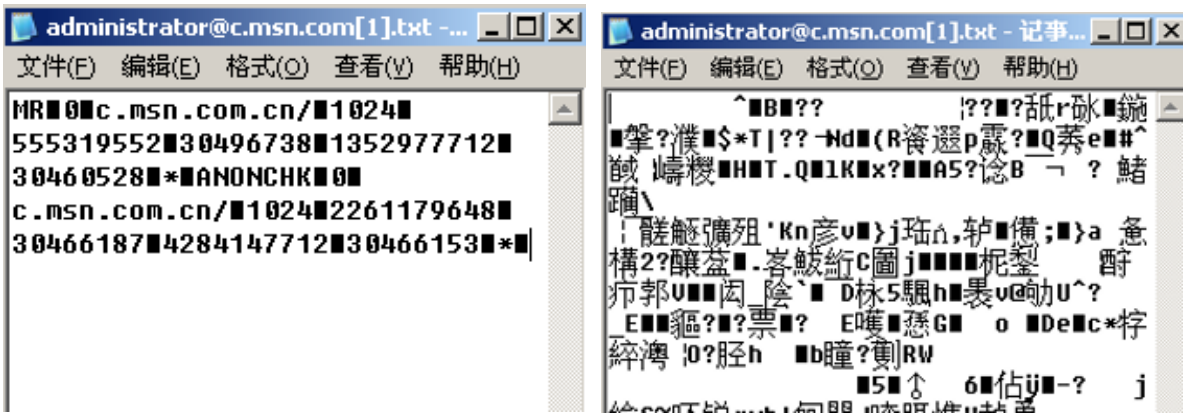


图 6 加密前后的文件对比

3.3 对抗安全工具

样本会查找系统中是否存在包含字符串的进程并将其隐藏，使用用户无法“看到”这些工具：

“taskmg”	*任务管理器*
“regedi”	*注册表管理器*
“procex”	*进程分析工具*
“msconfi”	*系统配置*
“cmd”	*命令提示符*

图 7 隐藏 cmd 界面

3.4 具有 PDB 信息

样本具有 PDB 信息，其文件名为“wet problem i yuoblem i_x.pdb”

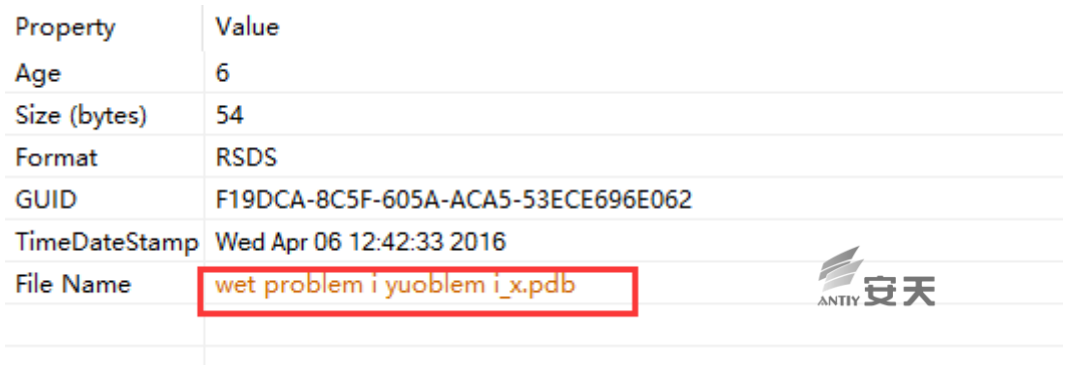


图 8 样本的调试信息中包含 PDB 信息

3.5 利用 CMD 自启动

样本调用 RegCreateKeyExW，将使用 CMD 启动自身的代码写入至注册表中，使其随系统开机启动。

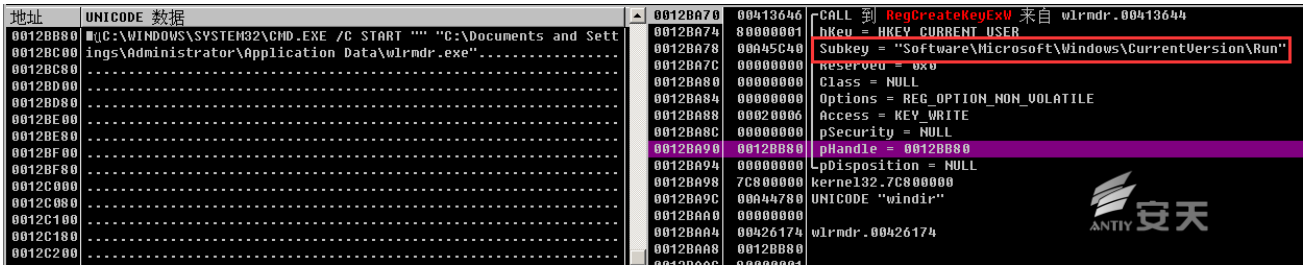


图 9 利用 CMD 达到随系统开机启动的目的

3.6 使用非常规的函数调用和跳转

样本使用了很多非常规的函数调用和跳转，用来阻止安全人员分析该病毒。

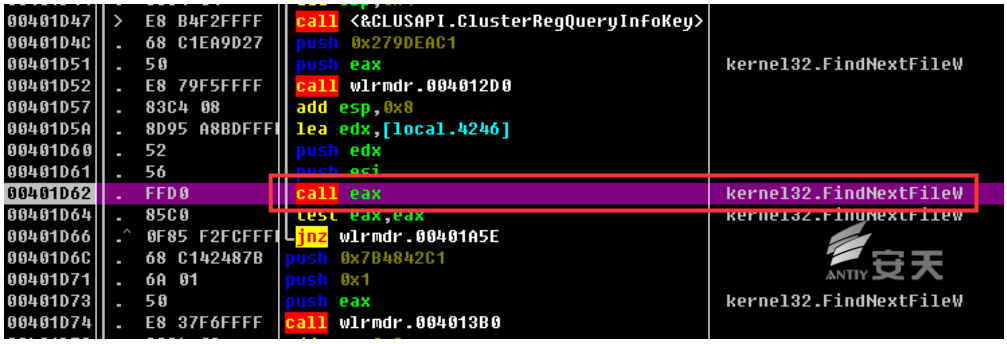


图 10 非常规的函数调用

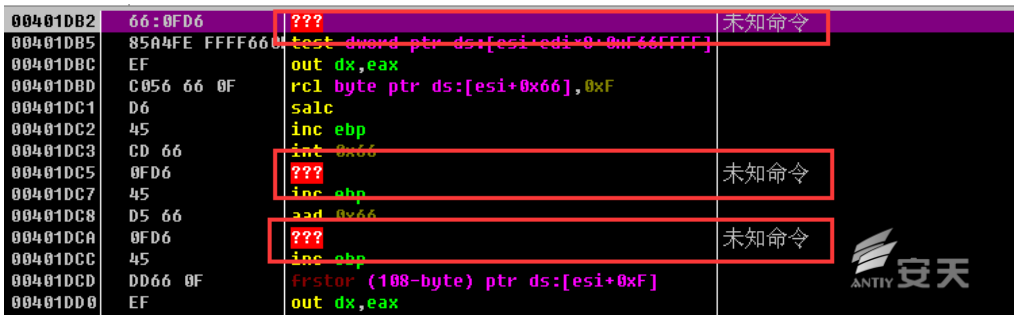


图 11 非常规的跳转

3.7 TeslaCrypt 4.0 加密的文件格式

地址	UNICODE 数据
00A44228	.r3d;.ptx;.pef;.srw;.x3f;.der;.cer;.crt;.pem;.odt;.ods;.odp;.odm
00A442A8	;.odc;.odb;.doc;.docx;.kdc;.mef;.mrwref;.nrw;.orf;.raw;.rwl;.rw2
00A44328	;.mdf;.dbf;.psd;.pdd;.pdf;.eps;.jpg;.jpe;.dng;.3fr;.arw;.srf;.sr
00A443A8	2;.bay;.crw;.cr2;.dcr;.ai;.indd;.cdr;.erf;.bar;.hkx;.raf;.rofl;.
00A44428	dba;.db0;.kdb;.mpqge;.vfs0;.mcmeta;.m2;.lrf;.vpp_pc;.ff;.cfr;.sn
00A444A8	x;.lvl;.arch00;.ntl;.fsh;.itdb;.itl;.mddata;.sidd;.sidn;.bkf;.qi
00A44528	c;.bkp;.bc7;.bc6;.pkpass;.tax;.gdb;.qdf;.t12;.t13;.ibank;.sum;.s
00A445A8	ie;.zip;.w3x;.rim;.psk;.tor;.vpk;.iwd;.kf;.mlx;.fpk;.dazip;.vtf;
00A44628	.vcf;.esm;.blob;.dmp;.layout;.menu;.ncf;.sid;.sis;.ztmp;.vdf;.mo
00A446A8	v;.fos;.sb;.itm;.wmo;.itm;.map;.wmo;.sb;.svg;.cas;.gho;.syncdb;.
00A44728	mdbackup;.hkdb;.hplg;.hvpl;.icxs;.docm;.wps;.xls;.xlsx;.xlsm;.xl
00A447A8	sb;.xlk;.ppt;.pptx;.pptm;.mdb;.accdb;.pst;.dwg;.xf;.dxg;.wpd;.rt
00A44828	f;.wb2;.pfx;.p12;.p7b;.p7c;.txt;.jpeg;.png;.rb;.css;.js;.flv;.m3
00A448A8	u;.py;.desc;.xxx;.litesql;wallet;.big;.pak;.rgss3a;.epk;.bik;.sl
00A44928	m;.lbf;.sav;.re4;.apk;.bsa;.ltx;.forge;.asset;.litemod;.iwi;.das
00A449A8	;.upk;.d3dbsp;.csv;.wmv;.avi;.wma;.m4a;.rar;.7z;.mp4;.sql;.bak;.
00A44A28	tiff.■■■¦■■.Ÿ▯■▯.....

图 12 TeslaCrypt 4.0 加密的文件格式

4 总结

勒索软件对企业和个人用户都具有极大的威胁，被加密后的文件无法恢复，将给用户造成巨大的损失。解决勒索软件的威胁问题除安装安全产品、防护产品、备份产品外，更需要用户在接收邮件时谨慎小心，慎重打开邮件附件或点击邮件内的链接，尤其是陌生人邮件。

安天智甲终端防护系统（IEP）可以在用户误点击运行勒索软件时阻止其对用户文件进行加密。

安天追影高级威胁鉴定系统（PTD）具有自动识别未知勒索软件的能力。

附录一：参考资料

[1] 安天发布：揭开勒索软件的真面目

http://www.antiy.com/response/ransomware.html

[2] 思科发布：针对勒索软件 TeslaCrypt 的解密工具

http://www.freebuf.com/sectool/66060.html

http://blogs.cisco.com/security/talos/teslacrypt

[3] 首例具有中文提示的比特币勒索软件“LOCKY”

http://www.antiy.com/response/locky/locky.html

附录二：安天 CERT 发现的 50 多个传播勒索软件的域名

marvellrulescc.asia	witchbehereqq.com	ohelloguymyff.com
arendroukysdqq.com	isityouereqq.com	joecockerhereff.com
blablaworldqq.com	jeansowghsqq.com	howisittomorrowff.com
fromjamaicaqq.com	marvellrulesqq.com	giveitalltheresqq.com
goonwithmazerqq.com	greetingseuropasqq.com	giveitallhereqq.com
gutentagmeinliebeqq.com	grandmahereqq.com	ohelloguyzzqq.com
hellomississmithqq.com	mafiawantsyouqq.com	jeansowghtqq.com
hellomisterbiznesqq.com	spannflow.com	grandaareyoucc.asia
hellomydearqq.com	ohelloguyqq.com	imgointoeatnowcc.com
helloyoungmanqq.com	bonjovijonqq.com	washitallawayff.com

howareyouqq.com	joecockerhereqq.com	greetingsjamajcaff.com
invoiceholderqq.com	itsyourtimeqq.su	hpalsowantsff.com
itisverygoodqq.com	blizzbauta.com	ohellowruff.com
lenovomaybenotqq.com	yesitisqqq.com	ohelloweuqq.com
lenovowantsyouqq.com	thisisitsqq.com	ujajajgogoff.com
mafianeedsyouqq.com	soclosebutyetqq.com	ohiyoungbuyff.com
mommycantakeff.com	isthereanybodyqq.com	helloyungmenqq.com
thisisyourchangeqq.com	ohelloguyff.com	

附录三：安天 CERT 发现的 C&C 地址

addagapublicschool.com/binfile.php

kel52.com/wp-content/plugins/ajax-admin/binstr.php

closerdaybyday.info/wp-content/plugins/google-analytics-for-wordpress/vendor/composer/installers/tests/Composer/Installers/Test/binfile.php

coldheartedny.com/wp-content/plugins/wordpress-mobile-pack/libs/htmlpurifier-4.6.0/library/HTMLPurifier/DefinitionCache/Serializer/URI/binfile.php

thejonesact.com/wp-content/themes/sketch/binfile.php

theoneflooring.com/wp-content/themes/sketch/binfile.php

mahmutersan.com.tr/wp-content/plugins/contact-form-maker/images/02/03/stringfile.php

myredhour.com/blog//wp-content/themes/berlinproof/binstr.php

controlfreaknetworks.com/dev/wp-content/uploads/2015/07/binstr.php

sappmtraining.com/wp-includes/theme-compat/wcspng.php

controlfreaknetworks.com/dev/wp-content/uploads/2015/07/wcspng.php

vtechshop.net/wcspng.php

sappmtraining.com/wp-includes/theme-compat/wcspng.php

shirongfeng.cn/images/lurd/wcspng.php

198.1.95.93/~deveconomytravel/cache/binstr.php

helpdesk.keldon.info/plugins/editors/tinymce/jscripts/tiny_mce/plugins/inlinepopups/skins/clearlooks2/img/binfile.php

hotcasinogames.org/binfile.php

goldberg-share.com/wp-content/plugins/contact-form-7/includes/js/jquery-ui/themes/smoothness/images/binfile.php

opravnatramvaji.cz/modules/mod_search/wstr.php

studiosundaytv.com/wp-content/themes/sketch/binfile.php

theoneflooring.com/wp-content/themes/sketch/binfile.php

hotcasinogames.org/binfile.php

pcgfund.com/binfile.php

kknk-shop.dev.onnetdigital.com/stringfile.php

forms.net.in/cgi-bin/stringfile.php

casasembargada.com/wp-content/plugins/formcraft/php/swift/lib/classes/Swift/Mime/HeaderEncoder/stringfile.php

csskol.org/wp-content/plugins/js_composer/assets/lib/font-awesome/src/assets/font-awesome/fonts/stringfile.php

grosirkecantikan.com/wp-content/plugins/contact-form-7/includes/js/jquery-ui/themes/smoothness/images/binarystings.php

naturstein-schubert.de/modules/mod_cmscore/stringfile.php

vtc360.com/wp-content/themes/vtc360_maxf3d/ReduxFramework/ReduxCore/inc/extensions/wbc_importer/demo-data/Demo2/binarystings.php

starsoftheworld.org/cgi-bin/binarystings.php

holishit.in/wp-content/plugins/wpclef/assets/src/sass/neat/grid/binarystings.php

minteee.com/images/binstr.phpnewculturemediablog.com/wp-includes/fonts/wstr.php

drcordoba.com/components/bstr.php

附录四：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn