莫步40亿数据泄漏事件后尘！针对金融、证券业攻击活动预警

By 奇安信病毒响应中心

Archived: 2026-04-06 01:09:02 UTC

01 **概览**

背景

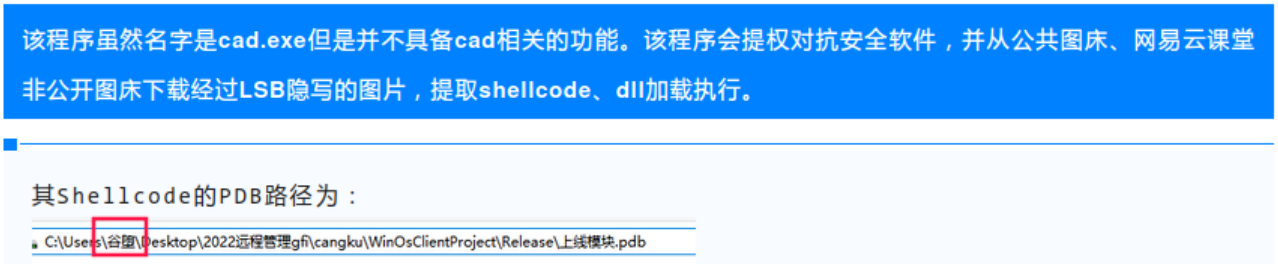
在我们上一篇公众号文章《后门程序正在通过知名搜索引擎广告位传播》提到了某团伙正在散发后门程序。本周奇安信病毒响应中心团队再次监测到了同一团伙的更多同类型样本。

本次攻击在溯源视角下呈现出通过微信等即时通讯途径投递的特点，且针对行业集中在证券、金融领域。虽然本次事件传播手段与我们上周发现的通过搜索引擎广告位传播的手段大相径庭，但样本在技术层面呈现出一致性，其技术手段主要分为两种：

1 从公共服务器加载载荷

2 通过白加黑加载载荷

由于连续发现该团伙的活动痕迹、考虑到该团伙可以调动的资源、根据该团伙传播的木马中某些样本的PDB路径以及该团伙使用的一些存储账户用户名，我们决定将此团伙命名为“谷堕大盗”，这里借用一张上篇公众号文章的图：



本次传播的样本依然可以在第零时间被我们的机器学习引擎（QDE）识别：

识别与防范

目前天擎对已收录样本具备查杀能力，请及时更新病毒库，打开云查可以获得更好的查杀效果。鉴于目前相关团伙正持续更新免杀钓鱼程序进行投递，钓鱼程序会针对性对安全防护软件做免杀，我们需要提升自身的网络安全防范意识对不法分子说”不”。

识别：

如何识别此次大规模钓鱼程序呢？ 通过整理此批钓鱼程序，我们发现文件名都是和证券行业相关的关键词进而引诱从事相关行业的人员点击。关键词整理如下：

开户视频
异常明细
记录明细
交易明细

成交明细
资金流水
龙虎榜
持仓
立案调查
…

这些文件都是exe扩展名的可执行程序，我们可以在查看选项卡中取消隐藏已知文件类型的扩展名以及时发现异常。

防范:

收到来历不明的文件后不直接点击，可以联系网络安全部以进一步甄别处理。或联系奇安信工程师协助处理。

02 **典型样本分析**

白加黑类

MD5	**定性**	**文件名**	**功能概述**
145B165769D86CB4837A81085F06CE68	黑	XX证券交易明细.exe	释放下面三个文件
4de7325349cdefae41ae6315a134c713	黑	ml.exe	黑月插件模拟点击df.exe加载panortc.dll
2ced5dffa01d8f0c0c3098c1fdd16e0b	白	df.exe	PanoVideo.exe 正常文件

590c99a38e4980f9dc1a360a232e44e2	黑	panortc.dll	恶意载荷

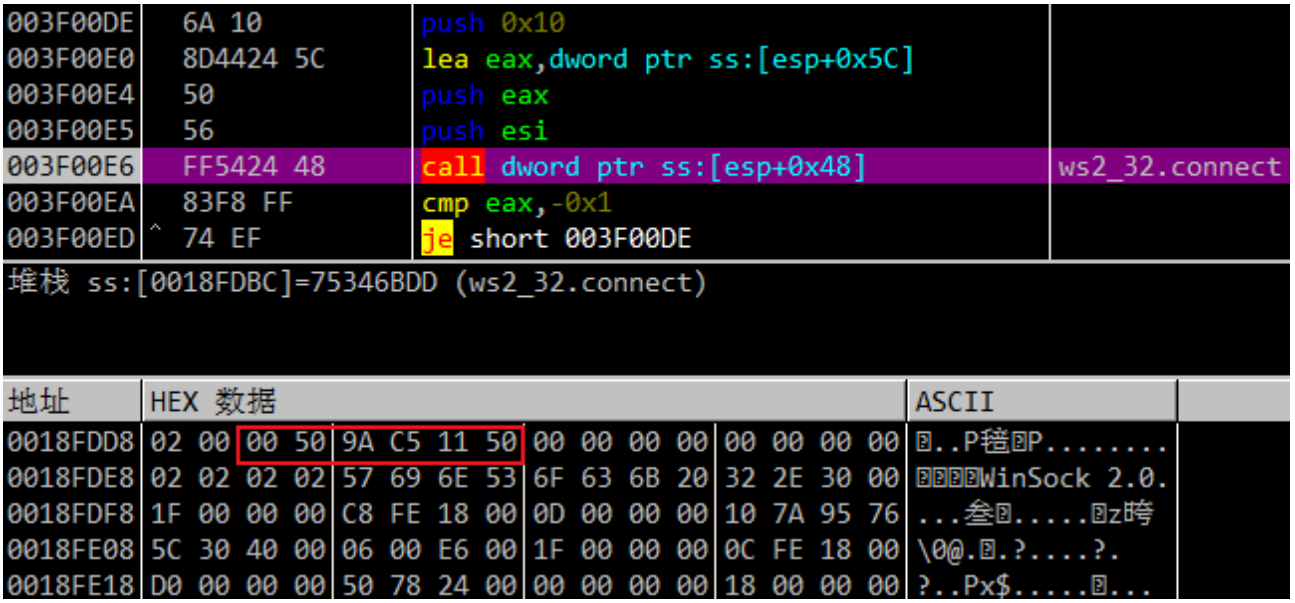
XX证券交易明细.exe即为邮件附件散发的木马程序入口文件，该文件由Autoit打包，执行会释放：ml.exe、df.exe、panortc.dll三个文件，最后调起ml.exe执行木马第二阶段模块：


```
#RequireAdmin
#NoTrayIcon
#AutoIt3Wrapper_Icon=C:\Program Files (x86)\Au3FZ\ico.ico
#AutoIt3Wrapper_UseX64=n
#AutoIt3Wrapper_Res_Comment=
#AutoIt3Wrapper_Res_Description=
#AutoIt3Wrapper_Res_Fileversion=
#AutoIt3Wrapper_Res_Field=Productname|
#AutoIt3Wrapper_Res_Field=ProductVersion|
#AutoIt3Wrapper_Res_LegalCopyright=
#AutoIt3Wrapper_Res_Language=
DIRCREATE("D:\ProgramData")
FILEINSTALL("C:\Users\86456\Desktop\分离小马模板\df.exe", "D:\ProgramData\df.exe", 0x00000000)
FILEINSTALL("C:\Users\86456\Desktop\分离小马模板\ml.exe", "D:\ProgramData\ml.exe", 0x00000000)
FILEINSTALL("C:\Users\86456\Desktop\分离小马模板\panortc.dll", "D:\ProgramData\panortc.dll", 0x00000000)
SLEEP(0x0000000A)
RUN("""& "D:\ProgramData\ml.exe"& """, "D:\ProgramData", @SW_SHOW)
```

ml.exe由易语言编写,黑月插件编译, 使用模拟点击的方式执行同路径下的df.exe

df.exe是个正常程序，执行会加载当前路径的 panortc.dll ,该dll被加载后首先将自己的绝对路径添加到注册表启动项, 然后再分别异或解密三段shellcode, 拼接后创建svchost.exe进程并通过远程线程注入的方式执行shellcode:

Shellcode执行后会连接远端服务器154.197.17.80:80并发送“nbclass”:



然后接收远端返回的一段payload并在内存中执行. Payload执行后会在内存中加载一个DLL, 该DLL为gh0st相关变种远控木马, 其CC地址为154.197.17.80:80。

公共图床类

此类型样本可以参考我们近期的文章《后门程序正在通过知名搜索引擎广告位传播》。

03 **危害**

近期再次惊闻有40亿+数据泄漏，如果该事件属实，大概率是因为其可以访问这些信息的关键设施被木马控制造成——此次投递的程序即为同功能程序，理论上可以造成如下危害：

1 投递勒索

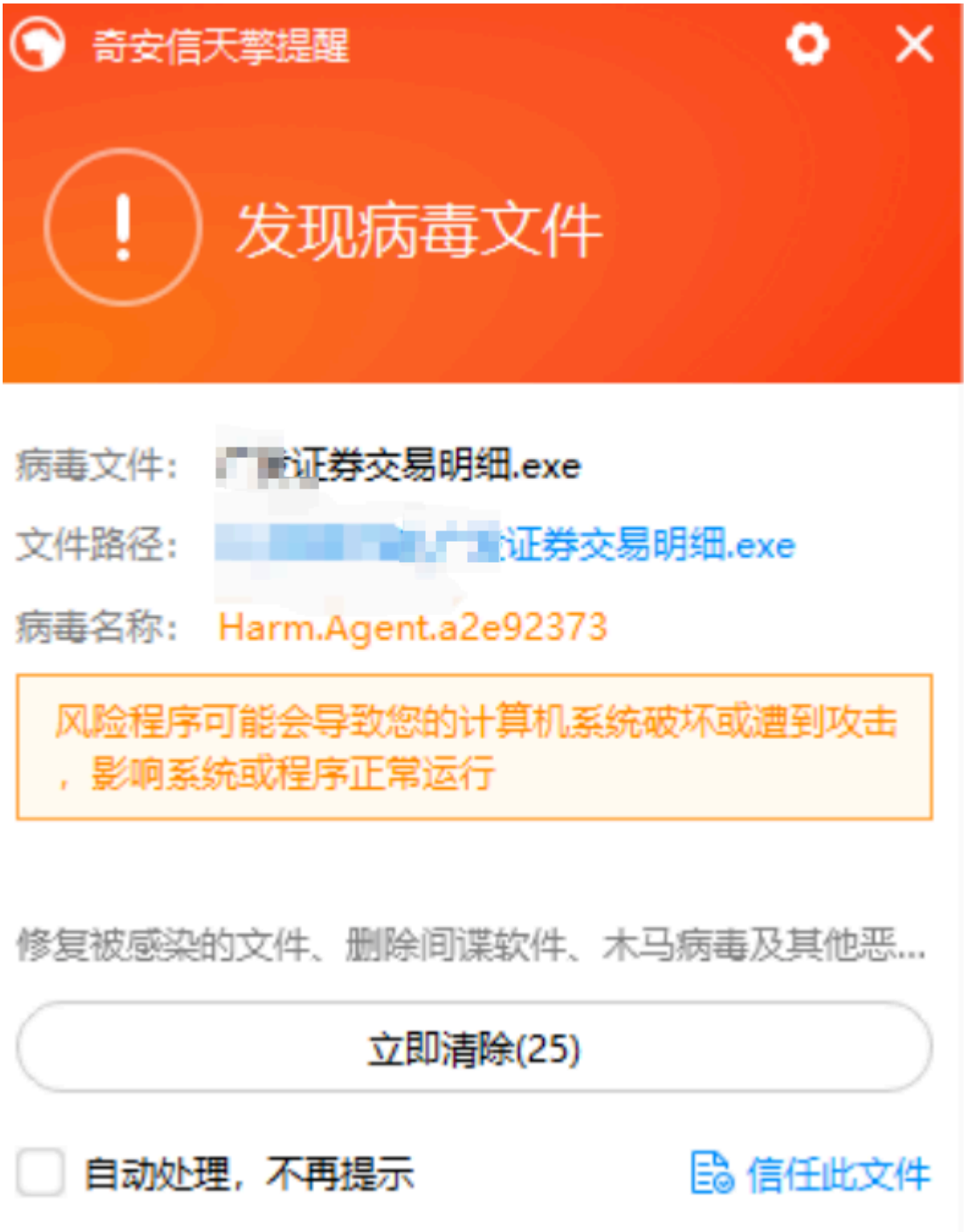
2 数据篡改

3 内网横移

考虑到近期连续两次大范围投递事件均是有明确目标的行业客户——特别是本次发现的是金融行业——因此一旦关键设施被控制其后果可能要比信息泄漏更为严重。

04 **安全防范**

目前天擎已支持对这些样本进行查杀,且QDE AI引擎可以在第零时间对其loader及DLL进行查杀:


奇安信天擎提醒
发现病毒文件
病毒文件：
证券交易明细.exe
文件路径：
证券交易明细.exe
病毒名称：
Harm.Agent.a2e92373
风险程序可能会导致您的计算机系统破坏或遭到攻击，影响系统或程序正常运行
修复被感染的文件、删除间谍软件、木马病毒及其他恶...
立即清除(25)
自动处理，不再提示
信任此文件


奇安信天擎提醒
发现病毒文件
病毒文件： ml.exe
文件路径： \ml.exe
病毒名称： QDE.V2.3.ECB9DKU2LJL
风险程序可能会导致您的计算机系统破坏或遭到攻击，影响系统或程序正常运行
修复被感染的文件、删除间谍软件、木马病毒及其他恶...
立即清除(26)
自动处理，不再提示
信任此文件


奇安信天擎提醒
发现病毒文件
病毒文件： panortc.dll
文件路径： \panortc.dll
病毒名称： QDE.V2.3.ECB9LVQQBJL
风险程序可能会导致您的计算机系统破坏或遭到攻击，影响系统或程序正常运行
修复被感染的文件、删除间谍软件、木马病毒及其他恶...
立即清除(27)
自动处理，不再提示
信任此文件

对已安装天擎的终端可以更新最新病毒库进行全盘查杀，对未安装天擎的终端可以使用奇安信顽固病毒专杀工具进行全盘查杀，也可以联系奇安信相关人员协助处置。

专杀工具地址：https://www.qianxin.com/other/qaxvirusremoval

05 **总结**

通过溯源关联，该团伙的恶意样本最早于2021年5月活跃，目前主要传播途径有即时通讯工具、搜索引擎，其利用的技术主要是白加黑、公共服务器挂载荷。目前该团伙仍然在更新活跃，并持续做免杀对抗。

在此提醒各位用户，不要轻易点击来历不明的文件，不要相信搜索引擎推广。

06 **IOCS**

MD5s	**145b165769d86cb4837a81085f06ce68**
	4de7325349cdefae41ae6315a134c713
	4de7325349cdefae41ae6315a134c713
	37b870122547aef88179af7033c6748c
	de1ebe0ae72ac494a3e8f3bcdd206529
	7f70581a6fb86c93edd920f56574b32c
	cfc712ea170d4da7f8cee9d71601eeaf
	e426e00ecfcfbea0b2d7a353011a5177
	016748167be06b13e66a19b3b460e30c
	814d2e28d0ed9ace82f43d6953fe6193

a30819f2fcd6ac0d3358d133f526c67d
ed8f5be63be4516a45c2c784217045e9
d8c04debad7f8be93aaaaaaa757601cc
9aad47c5311d7589dba638ed3b1d50df
3d6af896b80eeaa27c16a8ed432a0561
23a9276e96b7baa6273fc15efe6a3ecf
34e1f962f830861344113f4eb24dcd78
c97b3919b2e8dedff14e09847b7f9c1e
9b22da139b66f888de35198e6d338b33
f983b2127a8608f0f244fdc8a4935c3e
3618640a0d1c5d8c0fe024aacd8e1b97
0c0b75e0fbc4bb9900395472727dc808
abdf62294f43012d06f06aac504bfe36
6c512cc43c024e06aef7dc08f47ce109
fcc688c6019db263fc98672c5b377d5c

95025e10ca64e231abe981fff181ffbd
50f808898e2041ac5bb4869d6a5acce5
50bf0f3aa74bf5407aaa7e224c245ce7
be9487b0b2065e08fb6ce74dd89f7c2c
a52db4aa579ed157432364359d2e5608
ff543a713c87b84b8d3a6665595ea25e
b18b1640e56fd5d731fae3b7847bb1b1
c1d63c46a890c2888f8573b39b296290
2201bf9860f3302ea0a510cda4be3b87
09c52e29171337420d0199446559d04b
b2c28ff0edff07add935361a6b1f3702
73145354660a386ef364b6537a86f56f
ec3ef936e5dade1c9c7fc59c697e08d7
7a34aa24fbdaa2cf6529bfa32fd9efeb
991534b1274441188eda4c60d227214b

a42cb0b886d93affdc0fd9db3f8d1843
124ee75edab8f80a386ee6cca66f90e4
2a1c052128e9d9a14acfeaec70ab0c1e
04f87d8327ce2c29ca6f12cf292a764d
74c5b0071d2df2d6b251066b17b9825d
b1935648e186da3c62359c3578cb47db
dfadefb32316126e541c6443c0ed3ba0
66eafa072898df45147dbcf4fc5865bc
fab37e0bb12699e2d125c5cb8d7aa931
0dcdf37e9fbcf9cff0a0ce4f76a308d7
2746204afa927e333bda4f31cac306ee
94cd171ac03d3bbd85662107f99bc0ec
efc4a0f3728f004a52820d4b0249c5d0
9488afff784a15cb1e44dc5ae661f654
24441f238a13c27a7f3b379b8428c235

2c4dae7dd4976c07b87b1f3ebe4931f1
2d33f309c7218c851cd65b84903f3fa7
3c5a1214dc6b78e8f626e309ced314de
58ecdcfdf64470cf2840525056d9c757
71cc3b4acbea224ac40baabeb1e35b8d
7ac6187e7d750a49ca61a15031124ba1
e29393011726a3ebe5b946c9f568be33
42ef8c0f094639faabf78cf57bae8534
8787c7f9b1b6025d19650a32d6562259
317c09ceb64d45737293e4bfc176a71c
e04f5c7e6b06a244b2684b3ef44dbe62
f342d64b919582f19d4ac1143a1fd7f5
0dd7146d3dd05f4451f2489ef9108e77
d0dfe652b2b7b430586fb6284c24d6a5
cdbab880770c6a1cad3275ec6473221c

4636ebdfb341b016fdd2eba5a3f4f4bc
b8891c132788b999d861872d9ff5e711
49305f707f342c2a884bb875fb62a602
d56e514c1069ce5d9570f1fb7f55706a
fc1dfdb9e4fe44f24ced6e608f265d8b
cbd3e1539305b1a3e3e163dc3f76b934
760c7a525dd1554636aee1aa439411ea
ee9f4b7799446f961b41653f304b44c3
ad4160b89f0463a94c333f0f65f8f81a
7d8252be34ffcda096eb43ebe2b61e61
9a22a649948644371cbe2b58c13b876b
604bfb809465d59cf531fcd5c762d5c3
3674f44cca5d723518ae76ae5737ed40
17fc3328c158fd38f6aca7cba4b97577
b075109545d7d90305b0597c3ae72f97

114aa65ce6a2edc916dc211eed9320e3
a1d5dec080c558948387f534faa69dc9
77cf560c0e9706cfa0b83f1bc3b95f1b
502a66ed264f603ed53e4604b44566f7
0c9b3f56b6eec7bd8f7610a98f624d8c
dcd10219640ae009b42fa4d4a9960930
373311eff7700469d25717fe2e7b6266
e12c5a6f14ed2bf61ef9e9da2095c70f
c46a1d39528f693090b162faff059644
5d7ad40c4dd71205a388bdcd7641c2ed
feea8094945d67b0ee7928f5ddbf919c
71ccc84f3853808387e21e97e9fbb07a
ca8477949fc73c7ac52dd7c95f5e05e2
7e053ddacbbafcf270a7e2270a909c47
7e0dcf4bf56bd3b466030045bb830c0b

9ad568858e804557b9c138d3a473b5d0
e48ff3084393448766eef3a695d7f498
95e19827ccf6c8dc04603b47eb0336ad
4559b748f0e5696d89fbac732431b75f
122821abde5f3b49268bc466ae81c600
4519c8b24ec4f18928c65bfcd103a101
8150fe77964ed0f034a6135e1c7fda41
9efdb140784f9ea3b8be94f91a9c5c39
ff3031e0ea7ae58d4f5bc0cec342b6ba
c8f4faed917f41686b6487da39ff2ef9
2595b6a3695d90dd8bb8762cd294da24
afea2ef12ab888cb9e97f7878a880e2b
d82397fbb236c86fdd352c86b4871045
c3530bf03226ff93de37cbf5e01dc887
027d0cc7b56355543cc2e205b0b11377

1a366cb47f23d53b6919171f5e838739
3195bb6d12164e133c855e15c7b0865c
3584a7f18838a183d64b46ba4408a8d9
3c8b116b2d18d503c8e8f1b6c2c3a3f9
4a36493f7c8f9cdf791494ba8dd5a722
9d44ab6824ac1e85fae37dcb9924fc74
a34557c25044b9dd1df9c5a404895386
aa1c6c9aa496d0b1724bfd1d56ac05c6
b141d522eff33a9e1a15e2db595c09ad
ceff79b2161ed06c9115dbd20d35b79b
e21cfc4c63ca75d73997f7a2c12ac412
e27f74c07a03e28c5f934459176e873b
39970f254b9b88a8879ce5322c6112a9
81f05061c87f756b8c0059c45e0fc3f6
9079c93423dc0b5bca683d132699630b

988ea8d5e91d74b9e50357097f3a6350
a9e45182be525736ecbe530a79495ad1
b1e2e647ff20fbf2292f54fb71bc6b66
ccd47ec4ee320a8f9f5324d747855ac9
dbe43b01c4fffa6423b8032048006ec0
dd6e78bf5c307fae95ce5b778d5163b7
e0fa5bd634abf97f355127567eeac31b
e54d0d0e9dec12cfe9fa41caa872619f
ecfcaa803a8eb31dfec1931bab0aca1d
65ede890146dfc29c479047a5d9d995f
8761b7df1832dcbc0cba89eb0692760d
93c0f8ca70ef7d4ec0d964417db72f73
a2923adf251c7b47ba601ca6cb6a4926
e80bd511b46784f1dd1014dd00c65197
8c7c8fdc71bc17a9a5d71594932c6ea5

51ef8217938926b0fad69480680463f8
4b4bd2d93c407bb38bb2c1abeca8d4bf
17cbf7d391e02572a78cb31dcc444ea6
a641b3b81153936c6a3d3d99fe8d9736
6f620710482253c05b68c340a20e0e9a
d66fadcea89ba069b0a85f3bb9005751
6cb6caeffc9a8a27b91835fdad750f90
91029a49744faa6a98ad400ac451412d
fce55d866b0aebb55da4b1bc99590922
7f3704f80b63cd37ed1ba086221452b7
47cf6c87996d8ba1274140cec9fa3f24
d16dc8675179da5b5bd926004e88d520
453342449e3acbd1c81b4513a469b3cd
7efbe121f819cdee4cda6bb6fc73ca1e
e9e0548ee29c7879c813053333ae9d59

29dbae992117ab4c126469615de07417
653bc4e4d85bf4d0cdf5a3b0627c1254
84e9532f3b59458cfb56a23c1700eb87
8a2c56c1136bd1fea8195a7d412456d6
196b771ca2f946b022eabeb5ffbc779c
c2941a68705e663bc83ca43fd3897b2f
713aaa10ae456753f8c3e747166ae351
c332b9988b009be8711b83201a365141
31b5218d8e2da60bd628d27877626993
9d2622777a2e7a169ab667e75f1e1abf
56c9df6731fe87d17c2ce00e8b5fd077
d8d7e97794cd44695b40dd521e3b4911
613f9bb61e1d02e8119ed5528a67f1ff
af66a96e79c243708e1f25849665e174
f60136dd2ec6d25e97b07f327decaf3f

801ddd5f3f845ee461f6da644512652d
2fcbe2f71af73ea70200a17ecdfcd22f
763c15cd6242f8376d848b003d3a5bd0
cc157f13c4a92454f36c022692f4e02a
c087e3f13fbf9ebb5a0d1c965d895ff1
0a0f14a60ae7259df79c24fa690ba9b2
4384c4bf1956b20e138b07feba4829cc
a99a3391c54578ed784a92e2ec24ccb6
9022edf69f06a0255b1414cb40527707
593cd933877154e52c60228c5a81e341
a1dcfca07e575813a6f5b2d334a8f305
37f1d7569485f23fe6a0fc03fa2904e7
9d3072f7682084fcd20666b082e3a13b
bc6974d6da1e90ba961bf06a44a4f27d
dc50916da625c8a8daf24abdc762f41f

1de5c109be7f60f27f344ee23b2ed524
6c6e5526ba654ac2a6098607beff3053
10efc62bb61fe71dd261f90cde0edec2
ddf4bbda4a80c9f9e4f6bbc3eb5787a3
a22aab37469fbeee68577a16e7c1a959
533c19c3cd33d6e77a41ec7655a10c6c
d902ac1d8968633de209b9e7f677ff87
837164cd1b45bf11b9187f4ed4d2ac64
44ca28bd7670909431d48d468be79716
ba794b3ceb2da5ab1a02fd9db6c72f59
734dc62f546b4a2864f58a51af78b2a4
4e6ee1f86985c9965cb803c043391aaf
7afc125e48a5e33396079fcdbf0a1c68
dbab1572d4bade41ef56b39abb28d5b2
f2e4b6424af94d9e0c7484247137b233

	3c8f47c3acc45edb41882dd1a60a23de
	659ef5c0eac661007d9bca1e0983dd12
	82df641a76ee4b8393fa287a1fe0c7cc
	4a0c2fa4fe1744e911c59a9c436040e2
	db0952028b834345de9e7192077ece75
	f7b8f58556a9ee22a678e8ad59037c6a
	c4f7f6613f80a4468f5227acdd4ed38d
CC	180.97.215.92:80
	154.39.66.37:80
	43.155.62.10:80
	103.97.131.225:80
	154.197.14.66:81
	154.211.13.58:81
	137.175.50.61:81
	154.197.14.66:80

	154.197.17.80:80
	45.194.20.64:80
	154.39.66.87:80

07 附录 奇安信病毒响应中心

奇安信病毒响应中心是北京奇安信科技有限公司（奇安信集团）旗下的病毒鉴定及响应专业团队，背靠奇安信核心云平台，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的QOWL和QDE（人工智能）引擎，形成跨平台木马病毒、漏洞的查杀与修复能力，并且具有强大的大数据分析以及实现全平台安全和防护预警能力。

奇安信病毒响应中心负责支撑奇安信全线安全产品的病毒检测，积极响应客户侧的安全反馈问题，可第一时间为客户排除疑难杂症。中心曾多次处置重大病毒事件、参与重大活动安全保障工作，受到客户的高度认可，提升了奇安信在业内的品牌影响力。
