计算机恶意程序传播渠道安全监测报告

（2018 年 10 月）

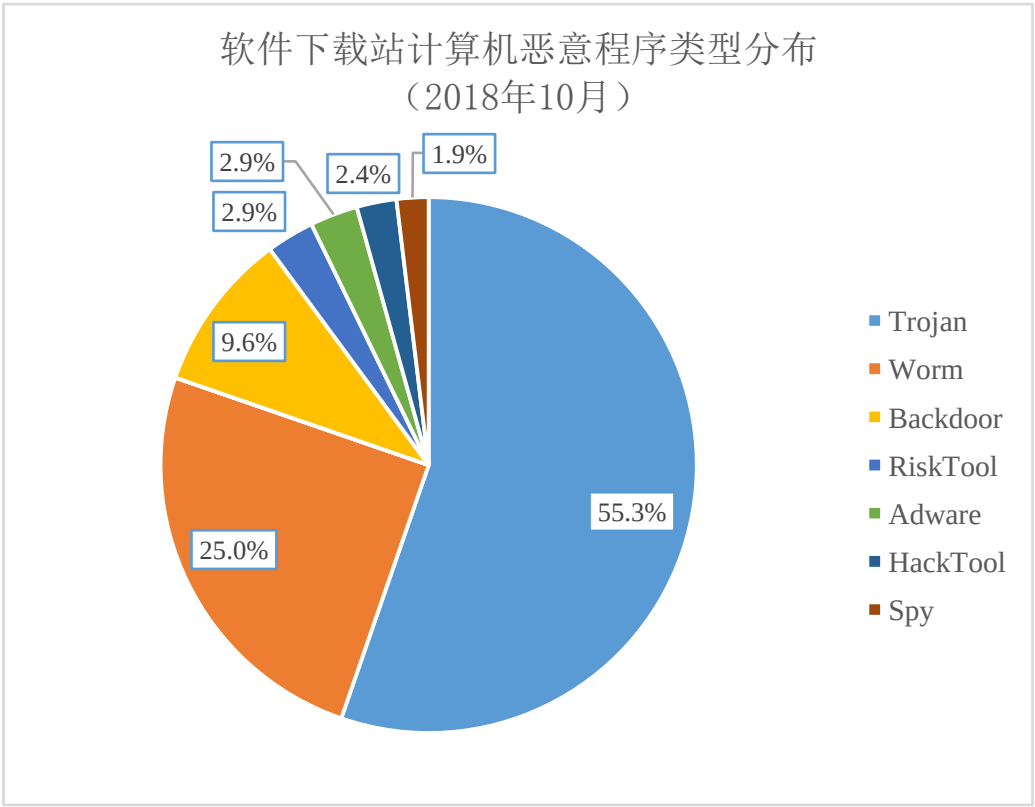
国家计算机网络应急技术处理协调中心

2018 年 12 月

2018年10月期间，国家互联网应急中心（简称“CNCERT”）在全国范围内继续开展计算机恶意程序传播渠道安全监测工作，对已备案的计算机软件下载站进行安全监测，判定计算机恶意程序208个，其中高危恶意程序139个，涉及8个省份的11家软件下载站及应用商店。

一、计算机恶意程序类型分布情况

针对208个判定的计算机恶意程序，其中木马类占55.3%，蠕虫类占25.0%，后门类占9.6%，风险类和广告类各占2.9%，黑客工具类占2.4%，信息窃取类占1.9%，分布如下图：



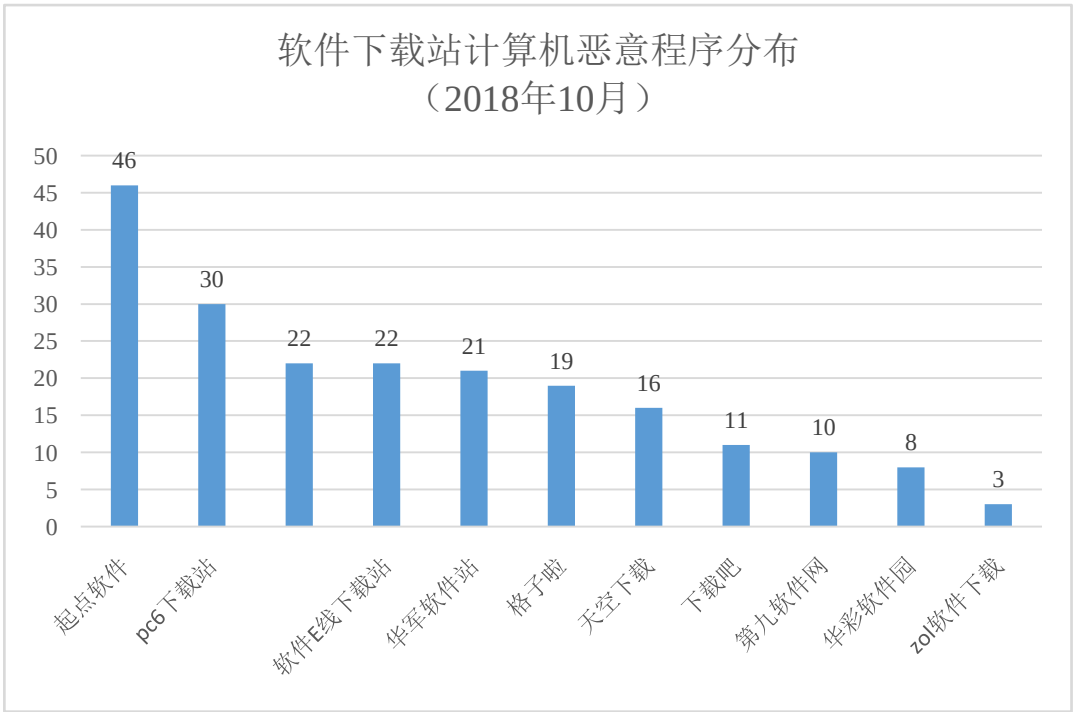
其中，经CNCERT判定为木马、后门、窃密等3类高危计算机恶意程序的数量共计139个，详细MD5列表及文件名

称见附件 1。

二、计算机恶意程序传播渠道情况

经 CNCERT 监测发现，涉及传播计算机恶意程序的传播渠道有 11 家软件下载站，根据其网站备案信息，其备案地分别位于北京、福建、广东、湖北、湖南、江西、山东、浙江等地。

其中通过“起点软件”传播计算机恶意程序的数量最多，数量达 46 个，其次是“PC6 下载站”，计算机恶意程序的数量为 30 个，第三名是“东坡下载”及“软件 EE 线下载站”，计算机恶意程序的数量为 22 个，其他软件下载站出现计算机恶意程序的数量分布如下：



三、计算机恶意程序处置情况

CNCERT 在判定计算机恶意程序后，根据软件下载站的网站备案情况，及时通过北京分中心、福建分中心、广东分中心、湖北分中心、湖南分中心、江西分中心、山东分中心、浙江分中心等 8 个 CNCERT 分中心通知当地 11 个软件下载站，对 CNCERT 监测发现的计算机恶意程序进行“清除”。

截至目前，已有 9 家软件下载站对其站内计算机恶意程序进行了下架或删除处理。CNCERT 对其在抵制计算机恶意程序方面所做的积极工作和坚决态度予以充分肯定，具体名单如下:

CNCERT 予以肯定的 7 家软件下载站 （按名称排序，排名不分先后）			
序号	**下载站名称**	**域名**	**所属省份**
1	PC6 下载站	pc6.com	湖南
2	zol 软件下载	soft.zol.com.cn	北京
3	格子啦	gezila.com	江西
4	华彩软件园	huacolor.com	广东
5	华军软件站	onlinedown.net	广东
6	起点软件	cncrk.com	浙江
7	软件 E 线下载	edowning.net	山东
8	天空下载	skycn.com	北京
9	下载吧	xiazaiba.com	广东

附件 1：恶意应用程序列表

CNCERT 监测判定的高危恶意应用程序		
序号	**md5**	**名称**
1	00fb5882fa827563b7b1a08ff771bdd3	欧洲卡车模拟 2 系统改进 mod
2	030b68d71bc66146336b9f81c96b83ec	NsasoftSpotAuditor
3	033c0237cb7bed6ffd8110caaaf0ffbc	批量删除文件
4	036a25ae955e05f75dd803c447e52bcf	劲乐团无限戒指圣诞版
5	042f11f0380623b261805ce412359c64	古剑奇谭 1 多功能修改器
6	049811c93626d470c8b1248ab653e547	本地网络信息 IP 查询工具
7	056b983aa8355c00218a10e8fc8dea23	说说助手
8	07388bad261755b48c196736683f118e	银河文明 3 自制母星系与种族 MOD
9	073b2d1529b8615edde777f161257c06	闲鱼搜索小工具
10	08289b7c14e7c47ce0524c2e52f02fb1	新木魔法文件夹
11	08435aabee881096c02993db53e19416	植物大战僵尸禅意花园修改器
12	088b53134c93936dab139469ac244b14	扫描文件
13	0920b2a907cf37467266ce86cf7b574a	可轩网站源代码批量搜索修改器
14	09844c636740d13c04354ca6ebe84132	小贝鼠标连点器
15	0acf0fd173d05adf79558c891b3427a8	网络设置备份工具(IPbacker)
16	0ad75164f5c49b05ffa131a5b4068dc3	职业自行车队经理 2014CDkey 生成器
17	0b609dc61a651cb3f372cd3906086099	项目 9 修改器
18	0ba73e75c677476b49083c3282e4298d	游击队劲舞团组合多功能综合 1.0 版
19	0babf7fa884db61973c7081c45fd79f8	3366 小游戏刷分器
20	0c2136fd54fd77cb30b530a3b4019b33	比乐阁 TXT 小说下载工具
21	0cf83f0b6f49cb77c99755c0cc5aab0e	上帝也疯狂 2 修改器
22	0885fe1ff23a59ddaaa87f4170f6dd90	爆枪英雄修改器
23	0a7dd52feda36b427ff59f6836ddff5d	神仙道懒娃伴侣 1.47
24	0aec6fd3b4e40d51b406025bb5240064	公司取名测算软件
25	0a19965eb29c0bb148acc882cfcf38f2	QQ 好友 QQ 号批量导出工具
26	00dac0d84f843b1231f973fc08a583eb	汉化浪子 Svg Image 文件格式转换工具
27	030106f3da50560d24373877425ff6e7	manycam 破解补丁
28	04215d8270a70fc749cc5ebe1d52cb7d	上兴超强加壳免杀器(Main)
29	048056c36dbe8b56eca9ff19b7add787	文件强制删除一切顽固文件工具
30	059992132e7ffabf3f767e2cdbec69b0	QQ 空间人气工具(猎人在线刷 QQ 空间人气)
31	073db8bf2854756c2f9a0aa83aeee9ef	域名缩短工具
32	0771b9a3e411a6ffaf17d5fc7294771f	Mimi 全网通影音视频播放器
33	07debd1b9a0b342121e29cd8fb8e1ff8	ezConverter
34	083aae378e92d0cdcad5ea3c7b7f3556	西藏专业技术继续教育助手
35	085f7e4a3a7401b95ff4b9ceff01aa99	半梦 QQ 工具集合
36	089cd5336ef77f9270d8158f907212ac	哔哩哔哩批量直播弹幕工具
37	0af610af379d16c72da4b82b5bc21ff8	文本相似性百度检测(论文相似性检测)
38	18f4b19cffbd088663922e041b8b4343	里诺电视广告管理软件

CNCERT 监测判定的高危恶意应用程序		
序号	md5	名称
39	01c91c6a5d36df90844729f34e3c692d	绿洲 PHP 木马扫描助手 v1.0 纯净版
40	02de0d554c8c268d98a27c2a6c99c064	爱宝淘宝会员吸纳打标 v3.3 免费版
41	02f309eb4216edba330bfa99ef11fd5d	爱坑位淘宝聚划算竞拍器 V3.31 绿色版
42	076676f97f1a6babca86d3b35ecfd72e	水淼软件盒子 v1.0.9.1 绿色版
43	08d2ee9edfbd58eb96abb0629ed32eb4	精准 QQ 说说日志关键词筛选 20150130 版
44	09a924c98e89dfd06146daee656d310f	QQ 活动盒子 v1.1 官方正式版
45	09ece0770cb08176246d0bb800e2f013	teleport 网站下载器自动修复工具 v2.0 绿色免费版
46	0a6a14f6fe2f8dc5d98372fdbbc06175	YY 保镖免费批量多开器 V1.5.0(不掉线适合 YY 最新 4.14)
47	0aef139646275a2801c4210bdd856441	吾爱免费云点播 v1.0 绿色版
48	0bfc8f892c00070bc9347bcf1c9c003d	淘宝图片抓取工具 1.0 绿色免费版
49	010000be50034bec98941934b54f6a20	DrvAnti 驱动防火墙终结者 1.0（病毒专杀工具）中文绿色版
50	04a39d65cdb99ec0f4873bff0834c7d7	NOD32 升级专家 V1.1(获取 NOD32 升级帐号密码)中文绿色版
51	0668bef424682696e791dffce57abfc8	Ken Rename 0.88 (文件重命名工具) 多国语言绿色版
52	075bb8b1551372ae228c9ef66d48f57a	通用按键精灵 1.55 下载(键盘自动按键软件)
53	07cf08a2f8f5f4cdef9cd3473057e171	凌峰关机小助手 3.1 绿色版(它可以完全支持长时间的倒记时关机)
54	0104168dfdc582f821bdc5aa0d41b111	Directory Printer
55	01db38feae142c5b44d22af825790088	日程精灵
56	01eb5a7f2fae456079f92a30346ff72e	qq 加密相册查看器
57	02ef22ff126c40d28dc78117991f280b	彩虹岛小草最新版
58	052c7e44b59420f00937f72647334405	睿达纺织贸易管理软件
59	0859f0e42698f3217250b48b9858a27d	大便启动
60	08ea81f155718cfff9ab1f956a6ec021	008 IE 广告拦截器
61	09585ebc3b9806e0962e0700ccc2deb9	生死狙击体验服 50000 金币登陆器
62	0ba4bde26101d0e3a8625806c9b3a4e2	发电厂车辆管理系统
63	0b1f3cdac6a7c62bd4b307f97d0f6c71	seo 自动发布外链工具
64	1db6fa8cd666a40af949b9821a07a636	果核 QQ 通用一键绿化破解补丁
65	003f4d2953b5ab2d45529d4bc80c2855	傲剑夫子镇副本辅助器 V1.0 简体中文绿色免费版
66	006bd3b91e8126501d24c5e438a66830	一键精灵 V5.7.0 简体中文绿色免费版
67	00a8f6f14af66d10cdb2d4a6ee44abe5	多玩穿越火线解封器下载 4.4 最新版
68	00fc7aa8781f9fde8e2290afb59adb32	全网音乐 MV 下载小助手 V1.0 免费版
69	0148badea16e11f7221f66d6f91eb9d9	获取机器码小工具绿色版
70	01a93126449e64a867b0058df0896ece	loluu 皮肤助手 v21.0 免费版
71	025c24395a73bc217b1097f3030929d6	造梦西游 4 圣域辅助下载 1.5 免费版

CNCERT 监测判定的高危恶意应用程序		
序号	md5	名称
72	02ca13fc5164ca0a35cf4f4dc7fd6d2e	csol 火神多功能透视辅助下载 1219 最新版
73	036db4020dcea91564a209b1087ccaab	602 完美红颜微端官方下载 v5.8.7.9 最新版
74	04013bad0dc5bf34b4a78b95357bfb6b	一流按键精灵 V1.01 简体中文绿色免费版
75	050b6a6486c5b8479b563da61948e298	QQ 成长值领取器 v1.3 绿色免费版
76	05d3993a6fcebb51ff9d58173022883e	创想 DLL 大全下载器 2.0 简体中文绿色免费版
77	0600b9b6a2d85ca9ee311e11fa95a14b	邮政区号速查 V2.82 绿色免费版
78	071a4014880ff6c6cc6bf035d623f184	色色牌 G++编辑器 V1.0 绿色免费版
79	0744c6c2d62c5e1dabf0d0ff097e0f7b	cf 大飞解封器 1.0 免费绿色版
80	0756bc6fb1cdd7cd76adec6b5aeb0aa4	DNF 补丁删除器下载 1.0 绿色版
81	07e2668ebda57dc1c0c6103d20ac6dc3	CF 蘑菇自动喊话刷屏器 1.4 最新版
82	085292e7c180cb5ede310ce92b77359e	左轮网吧计费软件 v1.0.29.0 绿色免费版
83	08c9dc370ca5a46283a985112cad3845	ImTOO CD Ripper V1.0.33.1013 注册机
84	09bd227f1f12b1f66b8e311507ae19ad	QQ 泡妞专家 V1.0 简体中文绿色免费版
85	09e2108e923dcb1e1d84408f89dc4c2e	星号密码查看器 V1.14 绿色免费版
86	0a15467db714b13405566a5c5dbb1fd3	River Past Screen Recorder Pro V6.6 注册机
87	0ac07b6f49a83d030df64c3dbf9f90a7	靓点下载地址转换 V1.0 绿色免费版
88	0b3aca03a6f8da1eb4e5bfcd165253a9	百度网盘直连解析 v1.0 绿色版
89	0bc71903ef87b439a1ceef847f5186c4	QQ 牧场守望者 V3.6 简体中文绿色免费版
90	0beddb7b2d6e9585710df173f3ae5766	等你 YY 摇骰子器 v4.17 免费版
91	0beed50cda3133575899b329efeba365	英雄杀刷分器下载 v3.56 官方版
92	0bfeaaf483eb43c6d7e9b7e6352a6fd0	易步零用钱大作战助手 V1.4 绿色版
93	1cf7f44da414abc1bfee13a2148e4a75	驱逐舰指挥官修改器下载 +1 绿色版
94	008de9c0ec1e6f56f0183178d0480e48	疯看工作室迅雷账号获取工具(迅雷会员资源获取器)V1.1.0 绿色精简版下载
95	0115b9943b1f97f04c0d722ca239b0d3	潜行者普里皮亚季的召唤十二项修改器免费版下载
96	02b01fc9cb5db9645b7f4a2571b7cba6	逗你玩儿百度无损音乐下载器 v1.0 绿色版下载
97	03db87d320042c6256933c1cedee5223	小乱文件加解密工具 v1.0 绿色版下载
98	04b0463d3c772561de6a58c73adb7b0e	网页刷新器 v1.0 绿色免费版下载
99	07e7d5d7f4395136066117a38997667c	街头霸王 4 修改器(全版本通用) V1.0 绿色免费版下载
100	092884d463573e65db9b718439c3b1ab	文字变成图片 v1.0 绿色中文版下载
101	092ea336768340c765c4ca12d1be1d9b	Ams 系统密码修改器 v1.0 绿色版下载
102	09c80d770b53fd6f112be4611f1f9001	多米音乐去弹窗广告工具绿色版下载

CNCERT 监测判定的高危恶意应用程序		
序号	md5	名称
103	0a52211517c3ed91a63a4d423f951c14	影音嗅探神器(影音嗅探专家) v3.1 绿色版下载
104	0b830c173f7eaa8b6af83fb94699642c	Kid QQ 群一键???到工具(qq 群一键签到软件) 1.0.1 绿色版下载
105	0087a6d86533697eb9c0560a1d9200c9	子域名查询工具绿色免费版
106	025bb9baeb6dd660f8606a6e2d492f01	epaper 批量下载绿色版
107	030492b74f0e6398fbfa6560522b6a93	晨曦网络电视直播绿色版
108	0359728adc9d8020e559870a821a3f8c	一键清理内存(FLY Memory Cleaner) 绿色版
109	04435c071d8f7b401d4a452bc154ae06	游街网络电视绿色版
110	074f160690570639c28f0cf9e7287af1	深海 QQ 空间说说批量删除软件绿色免费版
111	07b56a434e1d67981ea9e2287f0c8d97	酷狗去广告补丁绿色免费版
112	085d11393dfe0312cafb055774c8a2d3	爱 Q 绝版 QQ 秀领取工具绿色免费版
113	0a02750775fbc4fa6747e96b806e7756	淘宝自动发货软件-E 速达
114	0282d58d4d1df96fb5137df228b2bb9d	慧达快递单号生成器 10.5.1 官方版
115	03b1661e17739af18a1a953676888127	FreeMP3 Player1.0.0 官方版
116	06bca6608d90c568db153400cdb97e75	小米卡刷包精简器 3.1 中文版
117	07f378073cdbf4face47be56bc078998	吉特盒子(Gidot Box)1.1.0.0 官方版
118	0a52f5f7b06d8a1ffb5540bfd9ad0b75	RAMPro2.3 免费版
119	0c655f85694d80b3a747816a52defcd0	好友导出工具 2013 官方版
120	02bae46b6f6268ed16e0768ad186a704	桌面股票
121	0521817605259cf5263c136d6445a102	轩猫浏览器
122	058a923df7707758086066390f3d05ae	宽带加速器
123	06d66c2a7864afc852cd1cb4945de977	扬皓文件批量处理器 2012(GFileBat)
124	09813afcff844a7413d54a3a4f180637	广告屏蔽专家
125	0cbfb2df63daa1d0cb68a9a2a168a704	酷星云播放 V1.1.0.4 绿色版
126	061731c05a79b56197ceb2a899d98a57	BWMeter 4.3.0┆带宽测试和监控、测量和显示出网络所有流量┆英文官方安装版
127	047c08491980e5d29dcdc4e29372373c	淘帮手
128	07e34a0d0e7f19c995e27a007fdff955	芯烨 xp58iim 打印机驱动
129	0ac5f804b4554101b926f42bc5bd4a0b	商城评分计算工具
130	0b168978164356a1f93d1e91dfb00083	Fast Note
131	03ae11cd5f448df6694d4dd65f06a9b3	庄岩功夫派辅???最新下载 0.5 免费版
132	04b1d3ad071ba592f392467b11b7ef3b	顽固文件粉碎工具 V1.0 绿色免费版
133	040f0e6b4bea6d51294546cbcfde515a	酷奇可视化图片批量水印软件 v1.1 绿色版下载
134	07387685dbd573f2c0b0cf51d200e465	手机高清壁纸截图工具 v1.1 绿色版下载
135	079998560e361bee7b2efbeb5ed91034	骄阳在线广播电台 1.0 中文绿色版下载
136	08c58d65a578693b618d3a6f6fbfa302	懒虫外链小工具(利用站长工具网站提高网站外链) V4.0 绿色版下载

CNCERT 监测判定的高危恶意应用程序		
序号	md5	名称
137	0a3bb6adcdfb6bddb7666c1ac4c0ef44	小黑快速骂人工具(自动骂人软件) 2014 v1.1 绿色免费版下载
138	09fb0ea4fef5022f1780fe85790a67c1	小刀精确截图工具 1.0 官方版
139	0bbe3d40cc4f00409d0bb47b3acbb7ba	多行字符替换工具 1.1 官方版