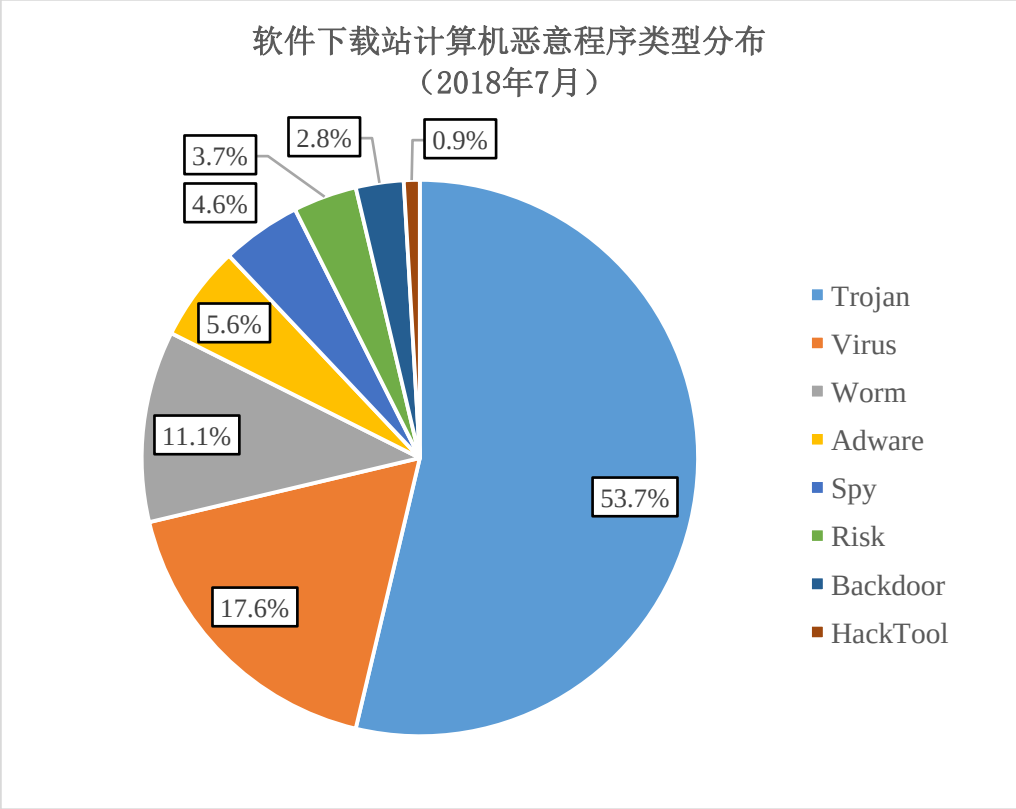
计算机恶意程序传播渠道安全监测报告

（2018 年 7 月）

2018 年 7 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 108 个，其中高危恶意程序 66 个，涉及 7 家软件下载站及应用商店。

计算机恶意程序类型分布情况

针对 108 个判定的计算机恶意程序，其中木马类占 53.7%，病毒类占 17.6%，蠕虫类占 11.1%，广告类占 5.6%，信息窃取类占 4.6%，风险类占 3.7%，后门类各占 2.8%，黑客工具类占 0.9%，分布如下图：

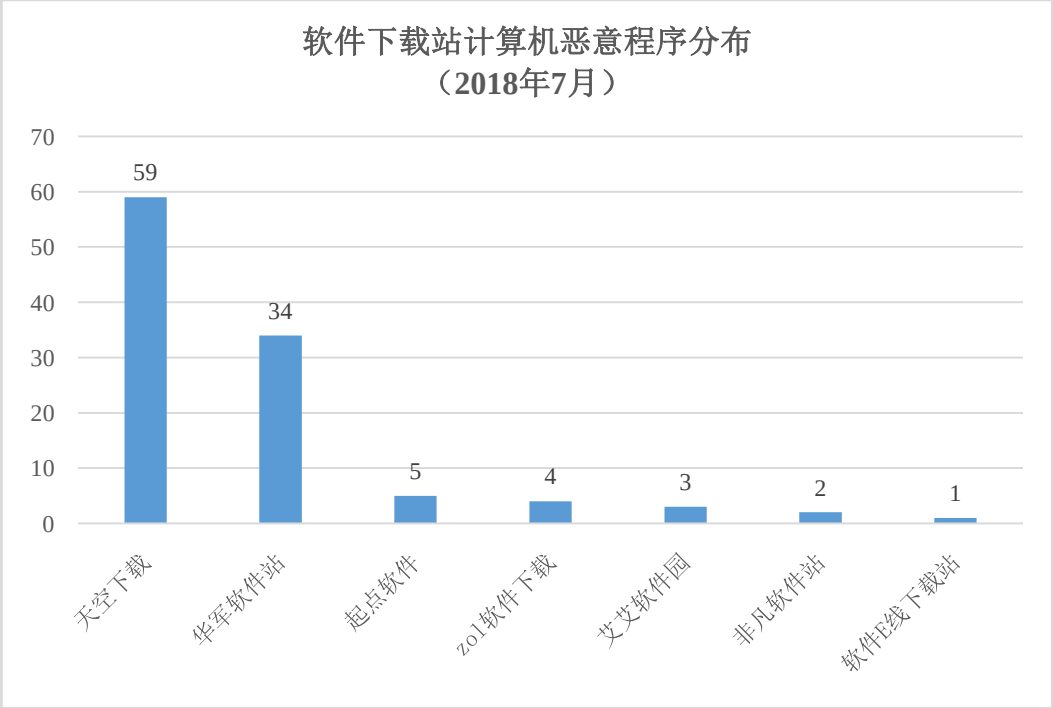


其中，经 CNCERT 判定为木马、后门、窃密等 3 类高危计算机恶意程序的数量共计 66 个，详细 MD5 列表及文件名称见附件 1。

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 7 家软件下载站，根据其网站备案信息，其备案地分别位于福建、广东、北京、浙江、山东等地。

其中通过“天空下载”传播计算机恶意程序的数量最多，数量达 59 个，其次是“华军软件站”，计算机恶意程序的数量为 34 个，第三名是“起点软件”，计算机恶意程序的数量为 5 个，其他软件下载站出现计算机恶意程序的数量分布如下：



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，及时通过福建分中心、广东分中心、北京分中心、浙江分中心、山东分中心等 5 个 CNCERT 分中心通知当地 7 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，7 家软件下载站均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	zol 软件下载	soft.zol.com.cn	北京
2	艾艾软件园	qh24.com	福建
3	非凡软件站	crsky.com	福建
4	华军软件站	onlinedown.net	广东
5	起点软件	cncrk.com	浙江
6	软件 E 线下载	edowning.net	山东
7	天空下载	skycn.com	北京

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	4a902904452456f9e7c94a7e2b35dedf	vcredist_x86 免费版
2	68d2be0f3a22a49dc94b8f838b6cbe2f	搜易口令钥匙(SeeKey) 3.0
3	5b0eda8934465c4f120bd4e71495f5e7	QQ 申请专家 v6.2 免费版
4	58ab7dff3ff57d06dc9dfedec3c58c13	??网视频播放器免验证精简版 v4.20
5	c7c4f495c49f2111e2efa7fd0dda3a94	QQ 坦白说查看工具 v1.2 免费版
6	1d6408ff4803a9f8ee259c98fcd05dfd	WinRAR(64 bit)
7	1f93eb487a2bfcb5660cfd71504d8340	Amazing Girls screensaver
8	273d9348d78095fff86c550a1feb1f12	心情记事本
9	3b73e5880dc2cce6c7e937eeee6b0971	U 盘小偷
10	6093d8af126de7f933cf3123e59d8904	sol 文件修改器 flashSolEditer1.3
11	7d5293bf4bd89fecbbea520ac8f7741f	P4 CPU 降温软件(所有 CPU 适用)
12	854998b3714c4e6b4af79461c140c1d9	NAT 类型测试工具
13	89115bdc68c83f4a64dc4fcb234d9683	IMPERATOR ˚FLA
14	95f04e77eac5e44f061a12d194c4f9ac	知心写作辅助软件
15	da7db29e783780f3a581e6e0bf4c595d	7-Zip
16	fe3dc7d46966e00c129c8b979ae46a2f	强力星号密码查看器|x-pass
17	2f0f5b811164ccf68de7ffc0c47f53bc	简尚自动按键
18	32481991542f8f5c9e2f487f2a6d1b56	二维码制作生成器
19	3d7c7f2f13df5b0b4c6b2fb3df9af3ff	Ams 定时内存优化大师最新版

CNCERT 监测判定的高危恶意应用程序		
序号	MD5	名称
20	90fe00855a2d66aa1ef1142265102507	ScanPort 端口扫描工具
21	93e8fe6d75eba54a9bc86add1335c454	酷我音乐 VIP 破解补丁 Patch
22	d9c47ad608034a5b3f5d8e942d6e2e9f	TGS 造梦大师 v3.1.8.2 官方版
23	03daad9569512fb94e08eec4deb89156	QQ 空间小秘书
24	11bf8fab7a975127c1b96d82a29913f3	隐形墨水绿色免费版
25	170977c24c40f222aacf210672477b17	收藏夹管理软件绿色汉化版
26	1953b4cbf5de1b29557291e0c5abf7bd	IE 修复工具 (ie 不能打开新窗口修复) 绿色免费版
27	1b089cb887866ffa37c404048430bbb2	Windows XP 系统快速设置工具简体中文绿色免费版
28	1b605b505ec0ab25944cdab67277d23b	淘宝抢拍器绿色免费版
29	3ecfa8847577ffb57ac016691ab3c4e6	迅雷上传免疫小工具绿色版
30	4e70fbf2efc1e186c088c24b9cf24c66	MSI 修复工具(Repair MSI) 绿色版
31	51d9e21d843c6252b8dc6cc4b1536645	迅雷会员账号分享器
32	58ac445b0ea864bcb9c2a6aa6f417205	股票 F10 检索工具
33	643c7f34c68971843a79811ecb46f57f	dnf 角色批量扫号器绿色版
34	754601746d15072fbb77f21bc35b90cd	Handy Shortcuts(给系统功能建立桌面快捷) 英文绿色版
35	80505a168e64025d2919d3126680b5d1	PHPnow 模板引擎
36	8df2a0e13d44df7058aea2154302b243	一键结束飞速网后台进程绿色免费版
37	9100193782822ccde8dbc0bff16bc3c3	桌面屏幕录像软件
38	92c43fa57641b8840cb46b46c6887714	HashChecker(最好用的文件哈希值计算工具) 绿色版
39	9ae18e92d9f337f81b90ade4e2032c87	文本搜索软件绿色版

CNCERT 监测判定的高危恶意应用程序		
序号	MD5	名称
40	b3024fe36f1fb9dd90284ba81a77922a	teleport 网??下载器自动修复工具绿色免费版
41	b8017ac28a5022754501e3ef73ba04c8	小巧好用的电子阅读器: Foxit PDF Reader 单文件绿色版
42	d9a531739a5267feaa28da5c9bc36d1e	tt 盒子种子搜索神器绿色版
43	dd2daae12cc7979aad53a5ecafee3c5e	全拼输入法安装版
44	e57fb1554e36f1648cac3a2ceb8cd3b8	万能单位换算器绿色版
45	f3e1ca7fc613b24896333d75998e8b7c	Win7 右键菜单管理工具(Easy Context Menu) 绿色版
46	f76ebbb3273cc455175088e06a0ca9c2	网页照相机简体中文绿色特别版
47	f966ed11c5162d47b6e0f5498ac4c66b	图片去水印软件(Photoupz) 绿色版
48	00dd1918ce10ae9fbc68e1af25477933	xwinkey|键盘按键屏蔽器绿色中文版
49	2b68941176fed54eb6d2ff891cc8fc15	玩玩 TXT 小说阅读器
50	37890f80d538106f0718a7e16d1cdf6f	图片外链助手绿色版
51	3dabecdcc075295033f5ec89cd7421cd	汉字转拼音软件绿色版
52	78d056c89cea1a0da81bf48a36306687	文件字符替换器绿色免费版
53	7e01c8534b10f7ceceddca07d5a89e9d	U 盘开关器绿色免费版
54	7f5460b206c73c5917a1212d81c792a2	专业定时关机助手绿色版
55	b30abc725b47aeda187e3e9edb15dfca	屏幕亮度调节 2012 9.15 绿色版
56	dd81c93600fbb181726edd9c99b2d265	好友导出工具绿色版
57	eccf70cf57cdefa20c7f7e65cddb2dc7	新浪微博图片下载器绿色版
58	f3c2e87e9693d6b4f7e30171b1eca994	北方网视频合并器绿色版
59	285e458c62798cb068a917abc1ad77e9	网站克隆器

CNCERT 监测判定的高危恶意应用程序		
序号	MD5	名称
60	e415e9bc4b35b7fa5219dfdeac92f465	RAR 文件强力修复软件
61	32b7c611b95bf50f6a371189dc7a40e9	ARPR (可同时破解多个压缩文件) 绿色汉化版
62	01a456f04ba732a48a4daed4ad013e35	千图网 VIP 素材解析下载器
63	4ef9d44931e931ee9400f8af4ed2ec43	种子搜索神器
64	5e298ef869171d96277f1d30f4459d2e	明星三缺一免光盘补丁
65	a09a34378552f8cb5a6a86b2472fe212	捷贝淘宝一键装修系统
66	eff36915d7c8b2832355f4289c724b63	向日葵远程控制主控端