关于通过一类仿冒网站实施网络诈骗的通报预警及情况分析

国家计算机网络应急技术处理协调中心

2018 年 1 月

国家计算机网络应急技术处理协调中心（以下简称“CNCERT”）近期监测发现互联网上出现大量仿冒最高人民检察院（以下简称“最高检”）网站的钓鱼页面。诈骗分子通过此类钓鱼网站，一方面可以诱骗受害者填写银行卡号、密码等信息诈骗钱财；另一方面可以在受害者计算机上安装木马恶意程序，窃取受害者计算机上的相关信息。CNCERT 已监测发现大量用户上当受骗，社会危害巨大。

在 2017 年 12 月份，CNCERT 共监测发现此类活跃的钓鱼网站达 254 个；监测发现“登录”此类钓鱼网站的 IP 达 3388 个，其中 31.22%的 IP 在“登录”此类钓鱼网站后提交了相关信息，属于实质受影响人群。

现将相关情况通报并分析如下。

致谢：

感谢阿里安全对本报告的贡献！

一、此类钓鱼网站的诈骗方式

诈骗分子通过在互联网上泄露的用户个人（以下简称“受害人”或“受害者”）隐私信息，拨打受害人电话，通知其涉及某类型案件，需要到“最高检网站”上进行“案件清查”。在受害者在仿冒网站上看到相关假的案件信息后，诈骗分子即通过话术一步步地诱骗受害人输入个人银行卡信息，甚至下载木马软件，对受害人的电脑进行远程控制，盗取受害人电脑上的敏感信息。

此类仿冒网站的页面非常简单，如图 1 所示，大部分网站需要输入诈骗分子提供的“案件编号”才可登陆后查看网站具体内容。

图 1：此类仿冒网站的“案件编号”登录界面

在受害者使用诈骗分子告知的“案件编号”登陆此类网站后，页面显示的是“中华人民共和国最高人民检察院”的相关内容，如图 2 所示，与真实的最高检网站极为相似，具有极大的欺骗性，受害者一般很难分辨。

图 2：登录此类仿冒网站后的“首页”

受害者登陆后，诈骗分子会告知其输入受害人的身份证号来查询自己涉及的“案件”信息，如图 3 所示，进一步提升仿冒网站的欺骗性。

图 3：此类仿冒网站的案件查询页面

该类网站的危害非常大，一方面是通过欺骗受害者填写银行卡号、密码等信息，如图 4 所示，给受害者造成大额的经济损失；另一方面可以在受害者电脑上安装木马恶意程序，如图 5 所示，对受害者电脑上的数据信息造成严重的泄漏风险。

图 4：此类仿冒网站的银行信息提交页面

图 5：此类仿冒网站的木马下载页面

此类仿冒网站可以实施较为精准的诈骗，是因为此类网站后台存有由诈骗分子提前预置的大量潜在受害用户的“案件编号”、姓名、身份证号、“案件名称”等多类信息，如图 6 所示。

案件管理 新增案件

選	案件編號	姓名	身分證號	案件名稱	文件	更新日期	管理
☐	001317	330402	330402	网络诈骗案	3	2017/11/30 下午 05:34:46	修改 删除
☐	01685	410224	4102	拐卖儿童洗钱案	2	2017/11/30 下午 05:00:27	修改 删除
☐	000918	441421	44142	王斌 诈骗洗钱一案	2	2017/11/30 下午 04:52:33	修改 删除
☐	001317	310104	3208	网络诈骗案	3	2017/11/30 下午 04:22:37	修改 删除
☐	0728	340421	3404	非法洗钱案	2	2017/11/30 下午 03:51:38	修改 删除
☐	0921	510125	5101	王坤诈骗洗钱一案	1	2017/11/30 下午 03:50:55	修改 删除
☐	001317	320824	3208	网络诈骗案	3	2017/11/30 下午 03:36:58	修改 删除
☐	000857	510214	5102	赵冰金融诈骗案	1	2017/11/30 下午 03:26:14	修改 删除
☐	001317	321302	3213	网络诈骗案	3	2017/11/30 下午 03:20:29	修改 删除
☐	0728	310104	3404	冻 结 管 制 令	2	2017/11/30 下午 02:54:20	修改 删除
☐	000857	500231	5002	赵冰金融诈骗案	1	2017/11/30 下午 02:53:23	修改 删除
☐	000918	31010	4416	刑事拘捕令	2	2017/11/30 下午 02:52:04	修改 删除
☐	000369	310104	3522	反诈骗洗钱防治条例法	2	2017/11/30 下午 02:50:01	修改 删除
☐	1028	410703	410	金融诈骗案	1	2017/11/30 下午 02:31:53	修改 删除
☐	429829	31010	3206	刑事拘留命令	1	2017/11/30 下午 02:24:13	修改 删除
☐	001006	22010	2201	刑事拘留批捕令资产冻结管制令	1	2017/11/30 下午 01:37:10	修改 删除
☐	000918	3522	352	王斌 诈骗洗钱一案	2	2017/11/30 下午 01:34:18	修改 删除
☐	000857	3101	510	赵冰金融诈骗案	1	2017/11/30 下午 01:01:30	修改 删除
☐	01685	3101	5135	刑事拘捕令	3	2017/11/30 下午 12:50:24	修改 删除
☐	0728	3101	3404	冻 结 管 制 令	2	2017/11/30 下午 12:14:04	修改 删除
☐	01685	3101	410	刑事拘捕令	2	2017/11/30 上午 11:57:02	修改 删除
☐	357	500236	500	赵冰金融诈骗案	1	2017/11/30 上午 11:54:52	修改 删除

22 的数据...

图 6：此类仿冒网站后台中预置的“案件信息”

此外，在后台中也存有此类钓鱼网站收集到的受害用户银行卡信息，如图 7 所示。

材料管理

選	銀行名稱	戶名	銀行卡號	使用材料	身分證號	網銀密碼	取款密碼	U領密碼	更新日期
□	招商银行	张	6214	电子密码器	441 723	53	5		2017/11/30 下午 05:20:58
□	中国工商银行	戴	62220	u盾	11 424	0	0	44	2017/11/30 下午 04:46:28
□	其他地区农村商业银行	刘	6230	电子密码器	441 723	51	5		2017/11/30 下午 04:14:09
□	其他地区商业银行	李	6236	u盾	410 549	lh70	70	70	2017/11/30 下午 03:57:18
□	中国银行		6013	动态口令卡	220 520	lily7	70		2017/11/30 下午 03:31:46
□	中国工商银行		6212	电子密码器	513 027	157	15		2017/11/30 下午 02:46:41
□	重庆农村商业银行	向	622	电子密码器	500 804	xj	11		2017/11/30 下午 01:27:25
□	中国农业银行	向	622	电子密码器	50 804	11	11		2017/11/30 下午 01:19:08
□	中国建设银行	充	622	电子密码器	51 027	15	15		2017/11/30 下午 01:13:52
□	重庆农村商业银行	向	622	电子密码器	500 804	114	11		2017/11/30 下午 01:09:18
□	中国民生银行	彭	6226	电子密码器	370 941	wu	90		2017/11/30 下午 01:09:01
□	中国工商银行	充	6212	电子密码器	51 27	157	15		2017/11/30 下午 12:53:47
□	中国农业银行	伍	622	电子密码器	340 048	59	59		2017/11/30 下午 12:30:15
□	中国工商银行	向	622	电子密码器	500 804	114	114		2017/11/30 下午 12:26:25
□	中国农业银行	充	622	动态口令卡	513 0027	1	15		2017/11/30 下午 12:25:55
□	中国邮政储蓄银行	钟	621	电子密码器	441 03	z	zs		2017/11/30 上午 11:39:54
□	中国邮政储蓄银行	钟	62	电子密码器	441 03	zsf	96		2017/11/30 上午 11:24:00
□	交通银行	马	622	动态口令卡	342 320	ms	72		2017/11/29 下午 04:46:21
□	郑州银行	林	62	动态口令卡	41 14	3	3		2017/11/29 下午 02:28:37
□	中国工商银行	罗	622	电子密码器	4 28	lf	66		2017/11/29 下午 01:15:02

图 7：此类仿冒网站后台收集的受害人信息

二、此类仿冒网站的活跃域名及服务器分析

CNCERT 对受害者在此类钓鱼网站上提交敏感信息的高危行为进行抽样监测，在 2017 年 12 月，共发现此类活跃的钓鱼网站 254 个，其中通过 IP 地址来直接访问的钓鱼网站有 252 个，通过域名访问的仅有 2 个，诈骗分子通过此种方式有效规避了被轻易溯源的风险。

同时，我中心发现此类钓鱼网站的服务器 IP 均位于境外，图 8 为钓鱼网站服务器 IP 按国家和地区分布情况，其中位于美国的服务器最多，占比高达 90.9%。

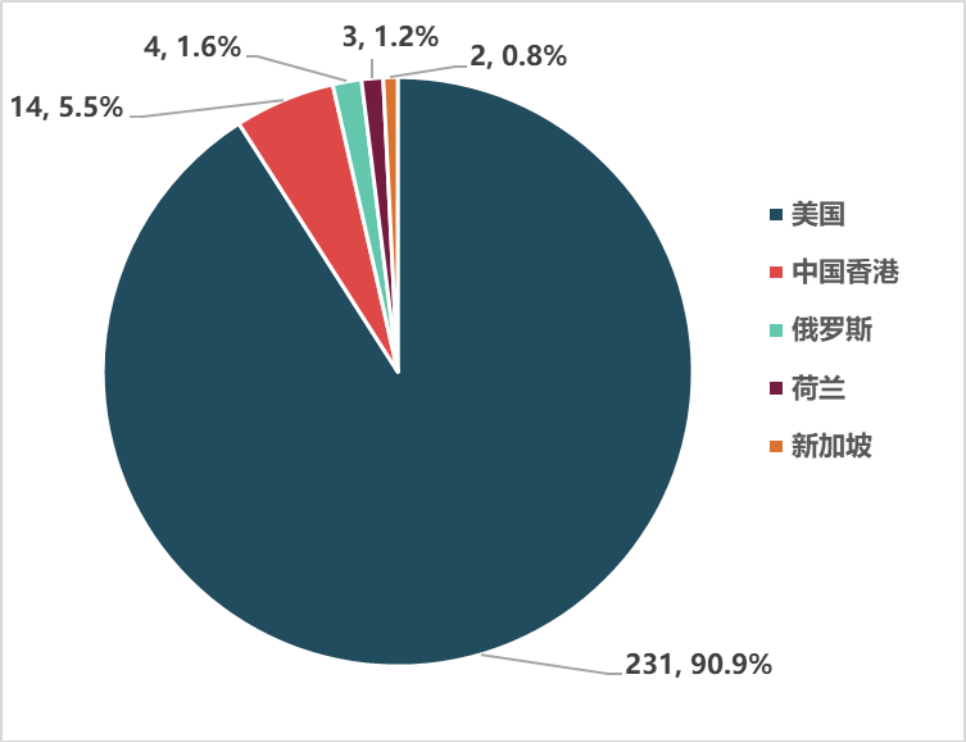

图 8：2017 年 12 月此类仿冒网站的服务器 IP 地理位置分布

钓鱼网站服务器 IP 地址呈现地址段聚集特点，疑似为网络诈骗团伙批量购买，用于集中诈骗。经统计，2017 年 12 月份发现的此类活跃钓鱼网站涉及的 254 个网站服务器 IP，共涉及到 67 个 C 类段地址，以及 27 个 B 类段地址。

表 1 为涉及的 B 类地址段情况，可以看到 192.186.0.0/16 以及 104.224.0.0/16 等地址段承载的此类型仿冒网站最多。

表 1：2017 年 12 月发现的此类仿冒网站的服务器 IP 的 B 类地址段情况

地址 B 段	IP 地址个数
104.131.0.0/16	3
104.171.0.0/16	6
104.195.0.0/16	5
104.200.0.0/16	11
104.216.0.0/16	7
104.221.0.0/16	7
104.224.0.0/16	32
107.170.0.0/16	1
108.187.0.0/16	2
128.199.0.0/16	1
138.197.0.0/16	1
139.59.0.0/16	1
162.243.0.0/16	1
172.80.0.0/16	13
188.166.0.0/16	3
188.226.0.0/16	1
192.186.0.0/16	97
192.241.0.0/16	1
198.13.0.0/16	10
23.234.0.0/16	1
23.91.0.0/16	7
43.231.0.0/16	14
45.34.0.0/16	24
45.55.0.0/16	1
45.77.0.0/16	1
46.101.0.0/16	1
95.85.0.0/16	2

2017 年 12 月，CNCERT 每日监测发现的此类活跃的钓鱼网站的数量如图 9 所示，每日监测发现的有潜在受害人进行访问的钓鱼网站数量都在 20 个以上，有部分日期监测发现的活跃钓鱼网站超过了 60 个，影响范围较大。

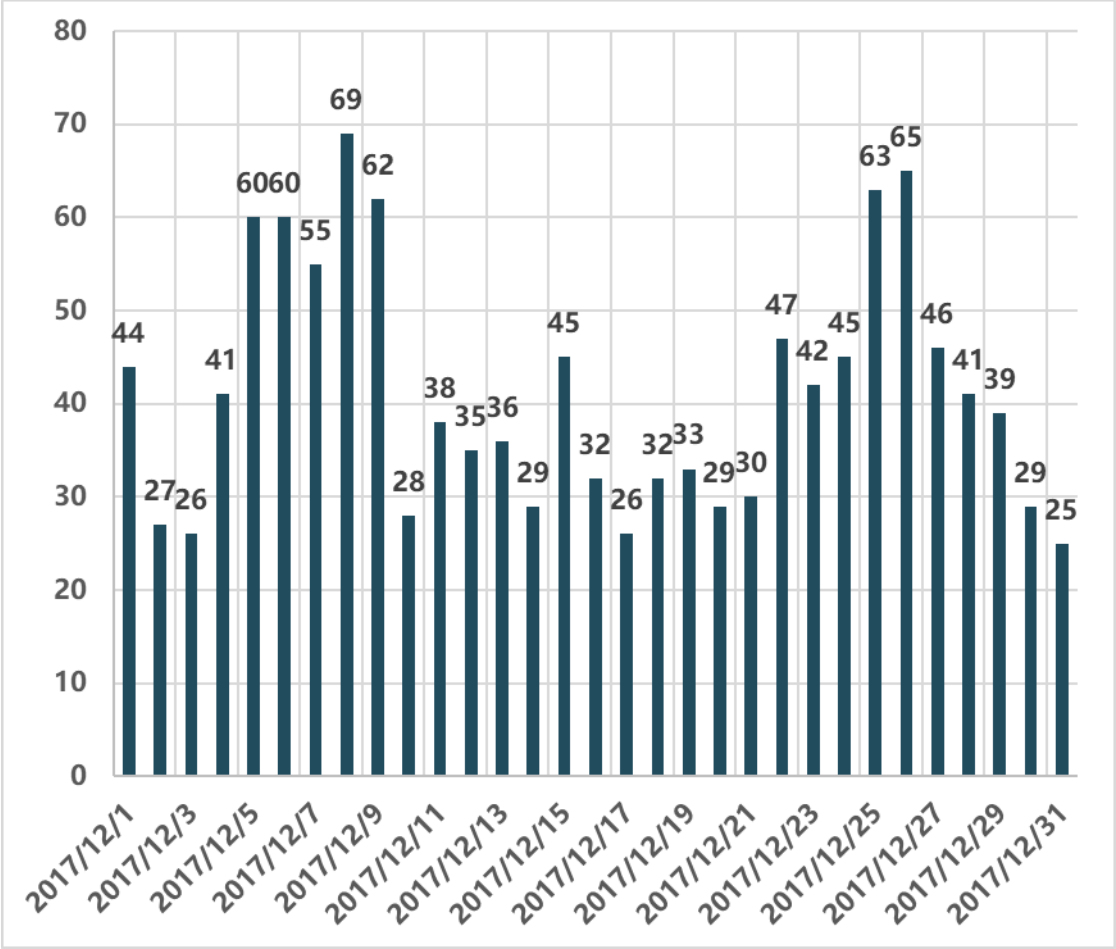

图 9：2017 年 12 月每日监测发现的此类活跃的钓鱼网站数量

三、受影响用户情况分析

CNCERT 抽样监测发现，有大量的用户访问并通过“案件编号”登录了此类钓鱼网站，其中提交了个人银行卡信息的受害人比利很大。

2017 年 12 月，国内通过“案件编号”登录此类钓鱼网站的用户 IP 地址数量有 3388 个，地理位置分布情况如图 10 所示。从图中可以看出，广东省内登陆过此类仿冒网站的 IP 地址最多，占 23.79%，其次是北京市、河北省、江苏省等地的 IP 地址。

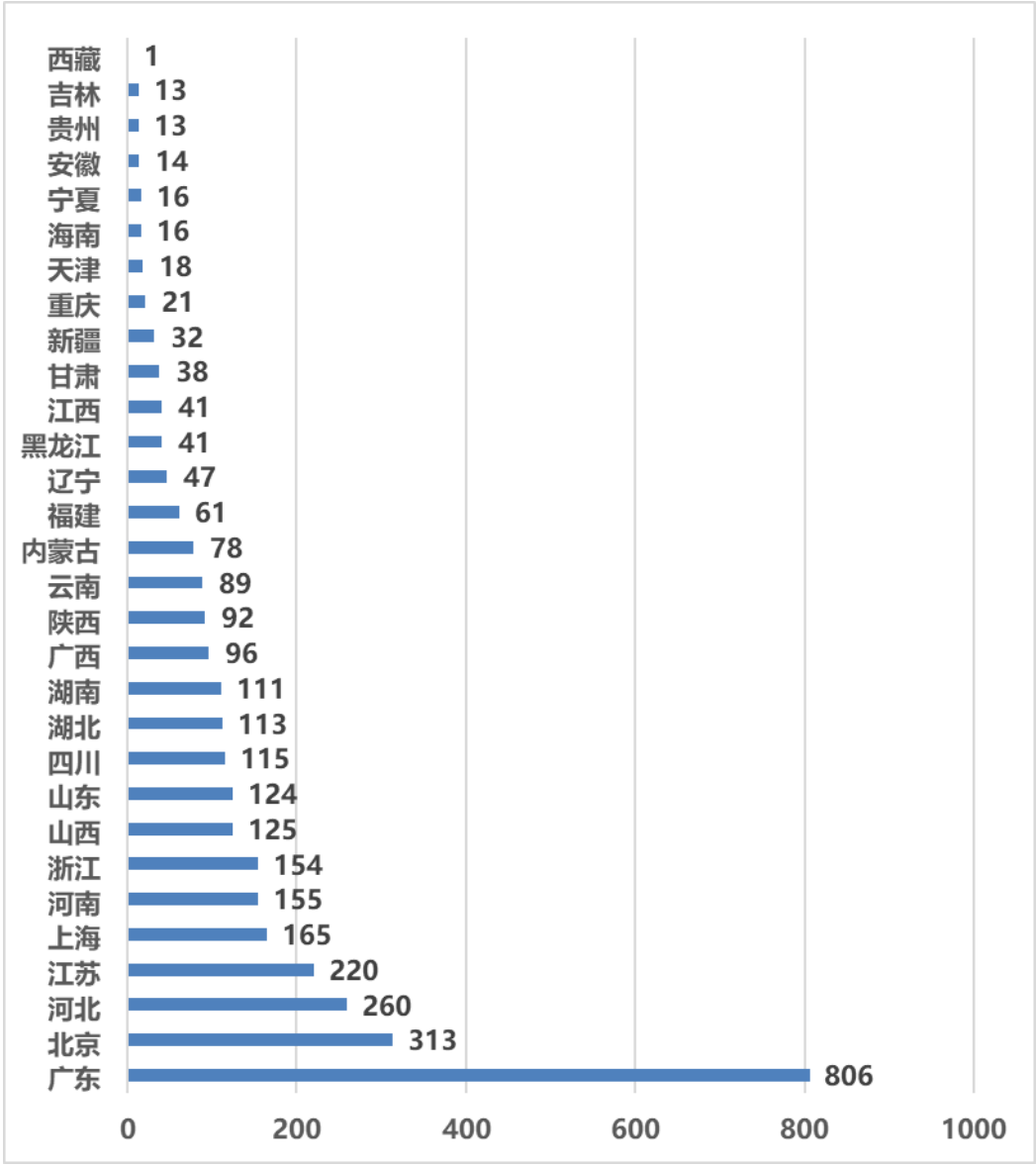

图 10：2017 年 12 月“登录”此类钓鱼网站的 IP 地理位置分布

在 3388 个通过“案件编号”登陆此类钓鱼网站的用户 IP 地址中，通过“案件清查”入口提交敏感信息的受害者 IP 地址数量有 1058 个，说明了31.22%的用户在登录此类钓鱼网站后会提交相关信息，受害风险较高。

这 1058 个受害者 IP 地址地理位置分布情况如图 11 所示，可以看出分布情况与图 10 基本一致。

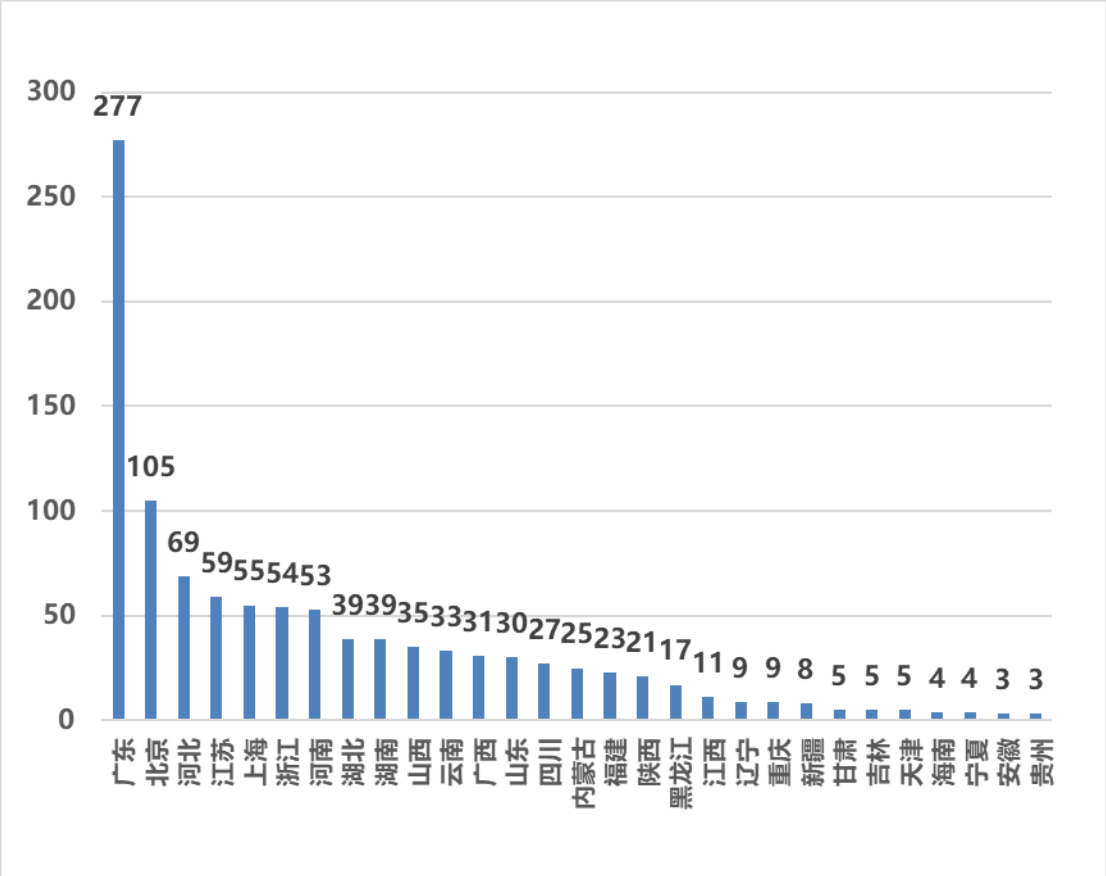

图 11：2017 年 12 月在此类钓鱼网站上提交银行卡信息的受害人 IP 地理分布

我中心监测发现，2017 年 12 月，1058 个受害者 IP 提交的信息共有 1618 条，经过初步分析，共涉及到 927 条有效身份信息。通过对这些有效身份信息分析发现，受害者年龄段分布情况如图 12 所示，覆盖了 18-84 岁的人群，其中 20-40 岁区间内占到了有效信息的 50%以上，为主要的受害用户群体；受害者性别如图 13 所示，女性占比高达 90%，说明女性更易受骗，值得高度关注。

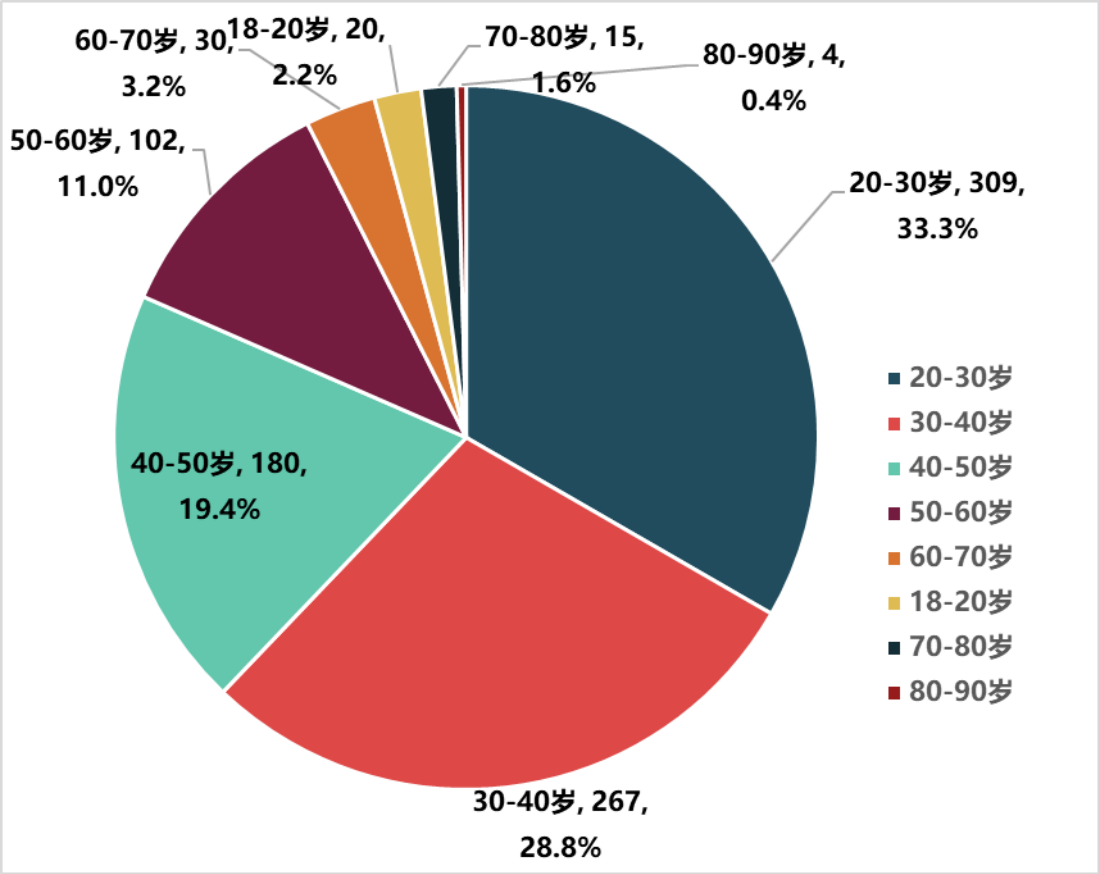

图 12：2017 年 12 月在此类钓鱼网站上提交银行卡信息的受害人年龄段分布

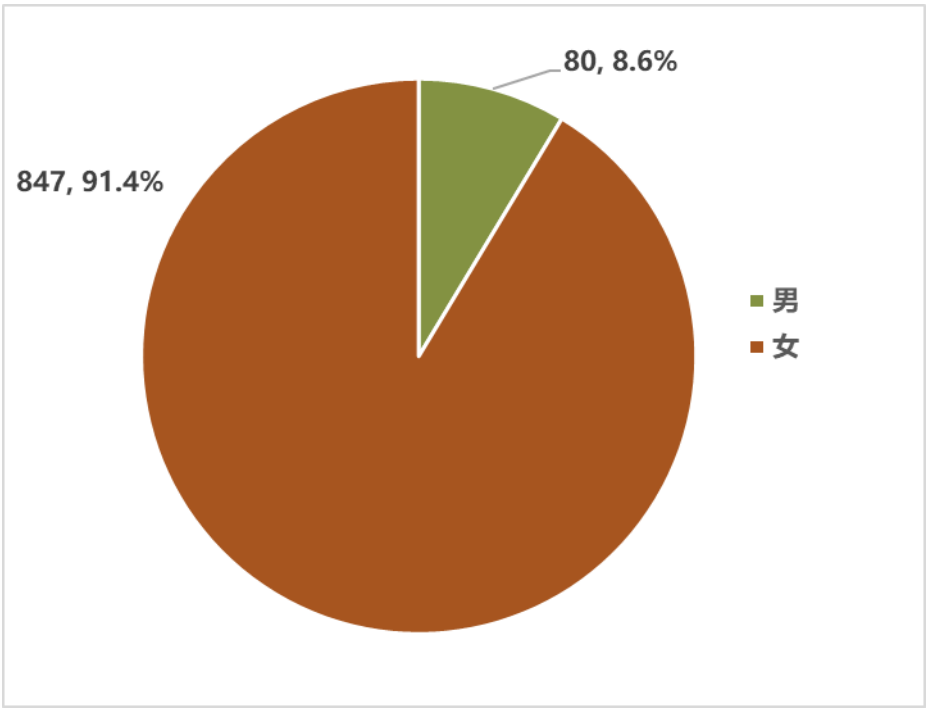

图 13：2017 年 12 月在此类钓鱼网站上提交银行卡信息的受害人性别分布

四、防范建议

此类仿冒最高检的网站已经猖獗多年，但近期依旧有大量用户上当受骗，经济受到损失。CNCERT 建议广大网民在接收到此类电话、短信后注意以下几点，防范受骗：

第一：最高检的网站为 http://www.spp.gov.cn/，不要轻易打开任何电话、短信，以及社交软件中的所谓的最高检网站，尤其是以 IP 地址直接访问的网站。

第二：最高检网站上不会有案件清查的相关内容，不会要求用户输入银行卡信息，也不会要求用户下载相关“安全软件”。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2017 年，CNCERT 与 72 个国家和地区的 211 个组织建立了“CNCERT 国际合作伙伴”关系。

联系方式

网址：http://www.cert.org.cn/

电子邮件：cncert@cert.org.cn

热线电话：+861082990999（中文）

+861082991000（English）

传真：+861082990399