2020 年虚假小额贷款类网络诈骗的态势情况分析

前言

虚假小额贷款诈骗是一类互联网上流行的网络诈骗。其典型的诈骗套路为：诈骗分子通过泄露的用户个人信息，拨打受害人电话或发送诈骗短信，以“提供无抵押、无担保”的快速贷款为诱饵，骗取受害人交纳风险保证金，或以需证明还款能力为借口诱使受害人转账，从而获取经济利益。这种诈骗方式往往会要求受骗人多次转账打款，受骗人一但生疑，诈骗分子则消失不见。大量网民难以分辨贷款的真实性，从而受骗上当。

常见的虚假小额贷款诈骗网站/APP 如下图 1—图 2 所示：

图 1：某诈骗 APP 首页

图 2：某诈骗 APP 首页

长期以来，CNCERT/CC 在对此类流行的网络诈骗行为进行监测分析的过程中，积累了相关数据，并开展了受害用户预警及案件分析支撑等工作。现将 2020 年虚假小额贷款类网络诈骗的全年态势情况向社会公众共享。

主要发现如下：

- 抽样监测发现 3461 个诈骗服务器上共承载 19420 个虚假小额贷款类诈骗网站/APP。位于中国香港的诈骗服务器数量最多，有 1986 个，占所有监测发现的诈骗服务器数量的 57.4%，其次是美国，有 322 个，占比为 9.3%。
- 抽样监测发现 7909820 个用户注册或登录了此类虚假贷款网站或 APP，其中提交了个人敏感身份信息的深度受害用户占所有提交个人信息的受害用户的 11.3%，且年龄在 20-30 岁之间的受害用户最多，占到了 41.8%，男性人数更是占到了深度受害用户人数的 78.3%。

注：以下分析是从 2020 年获取了受害用户敏感信息（例如手机号、身份证号、银行卡号）的网站/APP 的相关访问数据中分析得到的。

一、虚假小额贷款类诈骗服务器分析

通过抽样监测，CNCERT/CC 共发现 3461 个诈骗服务器 IP 地址承载了虚假小额贷款类诈骗相关网站或者 APP。其中位于境外的 IP 地址有 3157 个，占比达到了 91.3%。

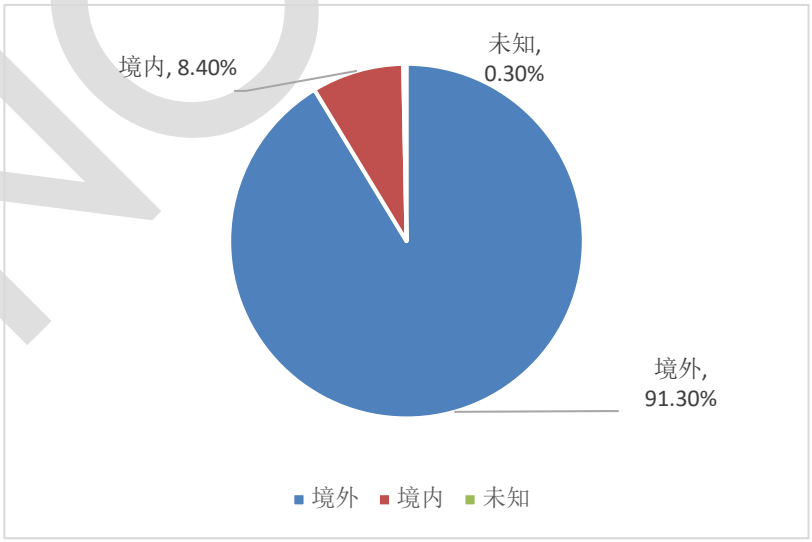

图 3:诈骗服务器的境内外分布

位于中国香港的诈骗服务器数量最多，达 1986 个，占所有服务器数量的

57.4%，其次是美国，有 322 个，占所有监测发现服务器地址的 9.3%。

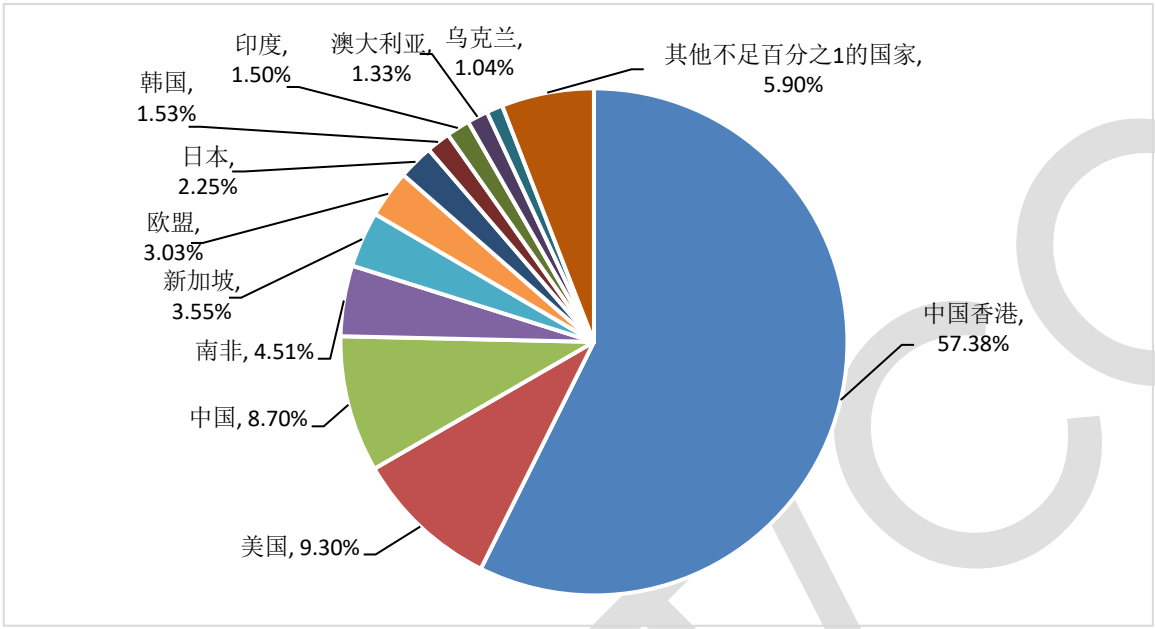

图 4：诈骗服务器的国家归属分布

3461 个诈骗服务器 IP 中，2240 个是 IDC 机房类型 IP，占所有诈骗服务器 IP 数量的 64.7%。

部分诈骗服务器承载了多个诈骗域名。其中位于中国香港的 IP 地址（45.**.**.58）所承载的诈骗域名数量最多，全年共承载诈骗域名 3452 个。下表列出的是全年承载虚假小额贷款类诈骗域名最多的前 20 个 IP、IP 上所承载的域名数量，以及 IP 所在地。

表 1:全年承载域名最多的前 20 个 IP 地址

IP	承载域名数量	IP 归属地
45.**.**.58	3452	中国香港
119.**.**.91	1830	中国香港
45.**.**.98	903	中国香港
119.**.**.54	757	中国香港
45.**.**.184	622	中国香港
119.**.**.90	580	中国香港
185.**.**.105	480	中国香港
119.**.**.3	437	中国香港
101.**.**.68	296	中国香港
93.**.**.244	288	中国香港
118.**.**.184	171	中国香港

43.**.**.76	164	中国香港
103.**.**.33	161	中国香港
103.**.**.1	153	中国香港
103.**.**.120	138	中国香港
103.**.**.238	122	中国香港
185.**.**.208	113	中国香港
101.**.**.172	94	中国香港
93.**.**.66	91	中国香港
93.**.**.19	83	中国香港

二、虚假小额贷款类诈骗网站/APP 分析

CNCERT/CC 抽样监测发现 19420 个诈骗网站/APP。其中仅有 328 个网/APP 是通过 IP 地址直接访问。部分网站/APP 在存活期间获取了大量用户的个人敏感信息，例如，dz2.****.cn 获取了 7320 个用户的敏感信息（包括手机号、身份证号、银行卡号等）。下表为获取敏感信息最多的前二十个网站域名。

表 2:全年获取敏感信息最多的前 20 个网站域名

域名	个人敏感信息条数
dz2.****.cn	7320
dz5.****.cn	4665
www.****.top	4409
dz10.****.cn	3716
qzjrqqt.****.top	3439
msjqt.****.top	3154
www.****.top	3051
dz9.****.cn	3036
dz9.****.cn	2859
dz5.****.cn	2852
****.cn	2776
rrd6.user. ****.cn	2681
www.****.top	2657
dz3.****.cn	2601
dz7.****.cn	2598
118.**.**.157:5001	2534
www.****.top	2526
fusenqqt.****.top	2488
app.11.****.cn	2469
www.****.com	2415

诈骗域名也存在二级域名聚集特点，在某些二级域名上，存在多个子域名均用于实施虚假小额贷款诈骗的情况。例如，**ibg.cn 上，用于虚假小额贷款诈骗的子域名有 478 个，***ingsuo.cn 次之，有 382 个。下表列出这些诈骗域名中，二级域名上，子域名是做虚假小额贷款诈骗的数量最多的前 20 个二级域名及对应的子域名数量。

表 3：二级域名上用于实施小额贷款诈骗的子域名数量

二级域名	子域名数量
***ibg.cn	478
***ingsuo.cn	382
**inzai1431.com.cn	246
***dord.com.cn	236
***qi.com.cn	198
**th.com.cn	196
***inhotel.com.cn	176
***bn.cn	159
***in-tour.com	146
****ite.cn	144
***dh3576.cn	133
***dczs.com	118
***ieye.cn	112
***2p.cn	112
***4fe.cn	112
***fhy.cn	104
***otels.com.cn	104
***ionasia.com	103
***ome.com	100
***dt5533.cn	100

三、虚假小额贷款类诈骗受害用户分析

CNCERT/CC 抽样监测发现，共有 7909820 个用户注册或登录了此类虚假贷款网站或 APP，其中部分用户在此类诈骗网站/APP 上提交了个人敏感信息，包括**手机号、身份证号、银行卡号、工作单位、家庭住址、家庭成员、月薪**等。一方面提交此类信息说明此用户深度受骗，另一方面此类敏感信息也可被用于诈骗团伙开展其他形式的诈骗，对用户个人信息安全和财产安全都影响极大。

2020 年全年，CNCERT/CC 抽样监测发现 940582 个用户的敏感信息被用户“主动”提交至此类诈骗网站/APP 上，属于**深度受害用户**。年龄在 21-30 岁之间

的人数最多，有 393608 人，占比达到了 41.8%，其次为 31-40 岁之间的人群，有 301075 人，占比为 32%。下图为提交了个人敏感身份信息的受害用户的年龄分布情况。

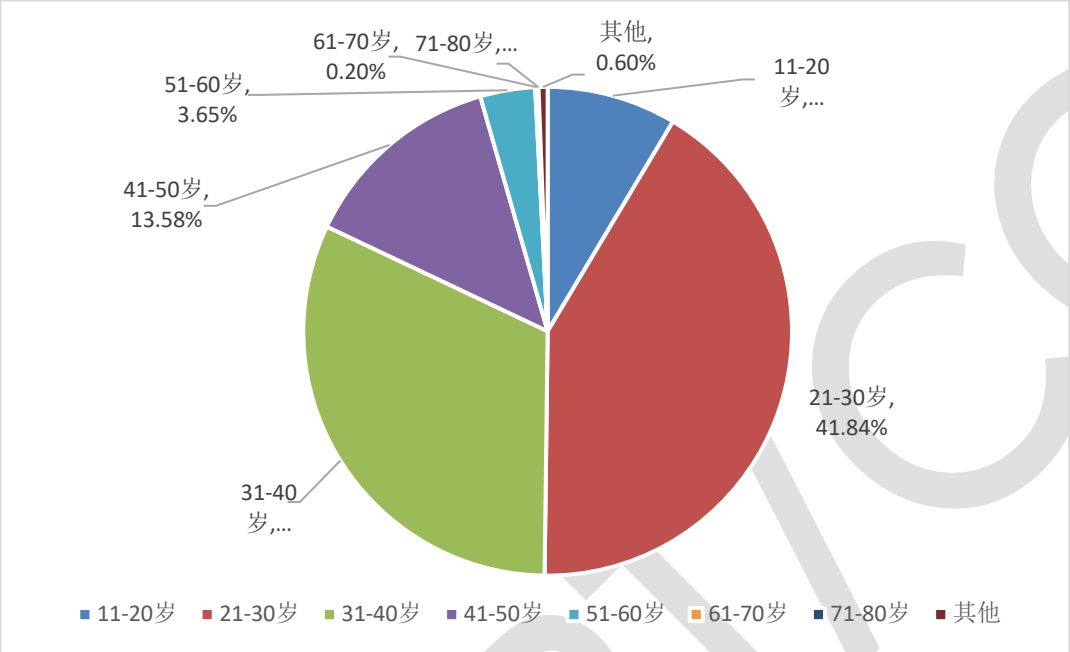

图 5：深度受害用户年龄分布情况

940582 个深度受害用户以男性为主，人数为 736680 人，占比达到了 78.3%。此外，从受害人的地理位置归属来看，四川、贵州、湖南等地受害用户个数最多。下图为受害用户 IP 归属分布情况。

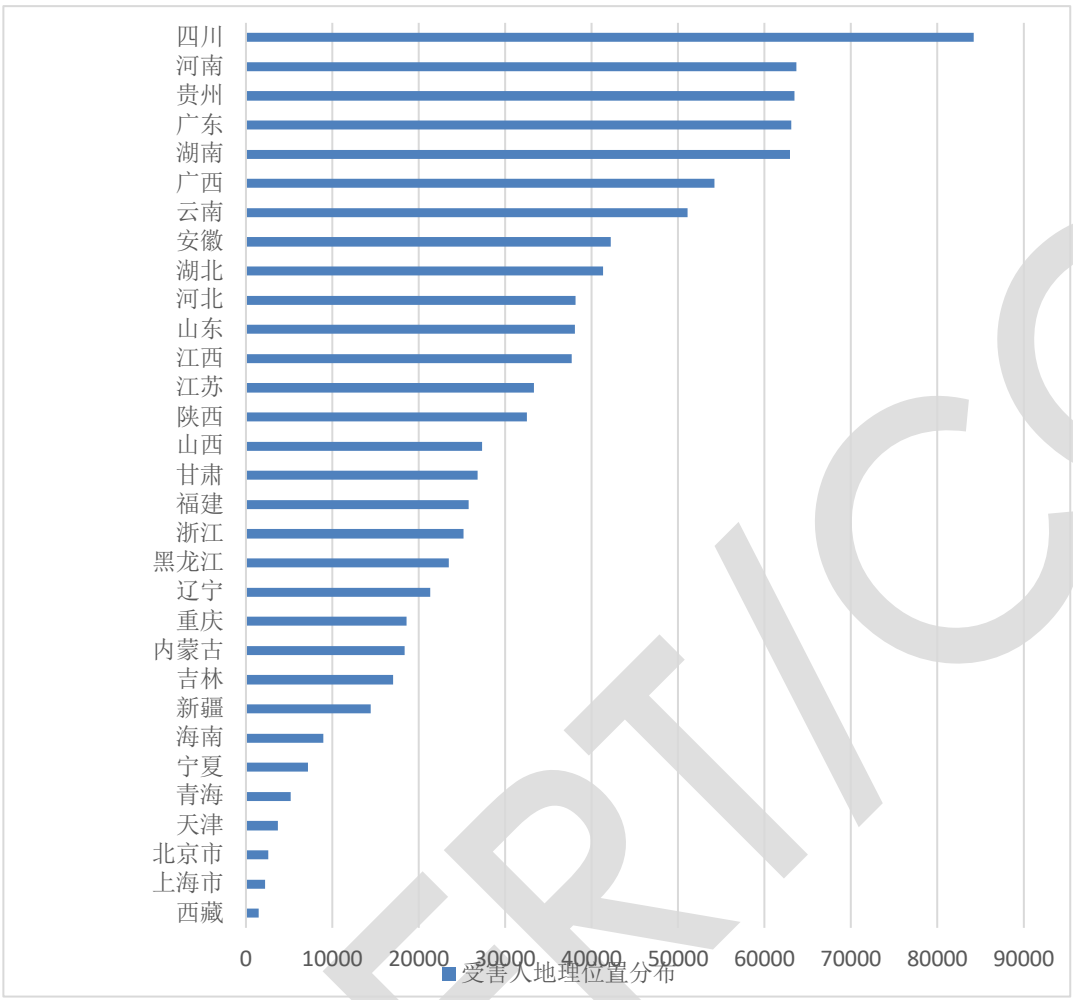

图 6：深度受害用户的地理位置分布情况