# 国家互联网应急中心（CNCERT/CC）

# 勒索软件动态周报

2022 年第 10 期（总第 18 期）　　3 月 5 日-3 月 11 日

国家互联网应急中心（CNCERT/CC）联合国内头部安全企业成立“中国互联网网络安全威胁治理联盟勒索软件防范应对专业工作组”，从勒索软件信息通报、情报共享、日常防范、应急响应等方面开展勒索软件防范应对工作，并定期发布勒索软件动态，本周动态信息如下：

## 一、勒索软件样本捕获情况

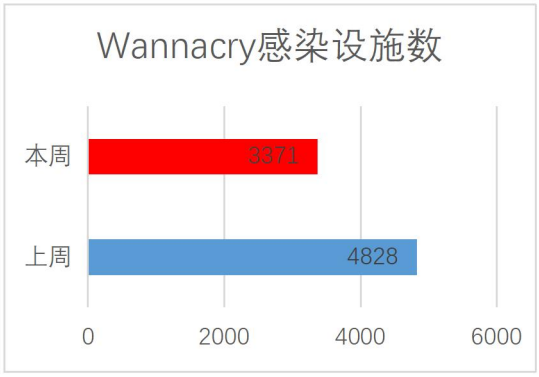
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1109205 个，监测发现勒索软件网络传播 1692 次，勒索软件下载 IP 地址 25 个，其中，位于境内的勒索软件下载地址 14 个，占比 56%，位于境外的勒索软件下载地址 11 个，占比 44%。

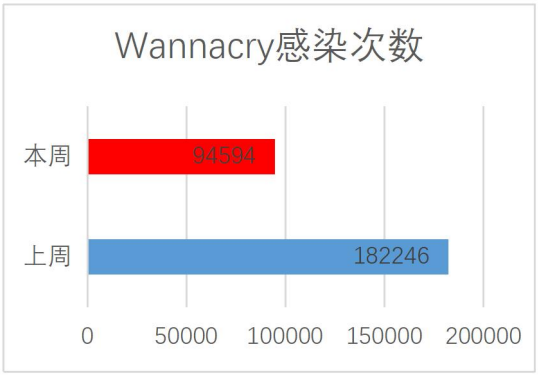
## 二、勒索软件受害者情况

### （一）Wannacry 勒索软件感染情况

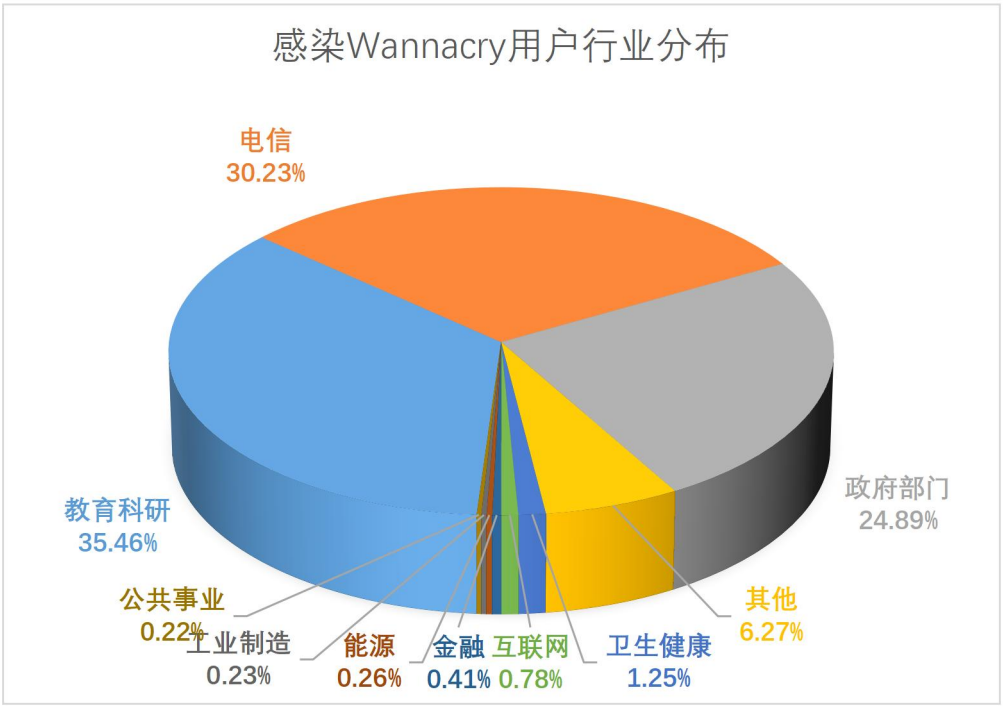
本周，监测发现 3371 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 30.2%，累计感染 94594 次，较上周下降 48.1%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机

没有针对常见高危漏洞进行合理加固的现象。



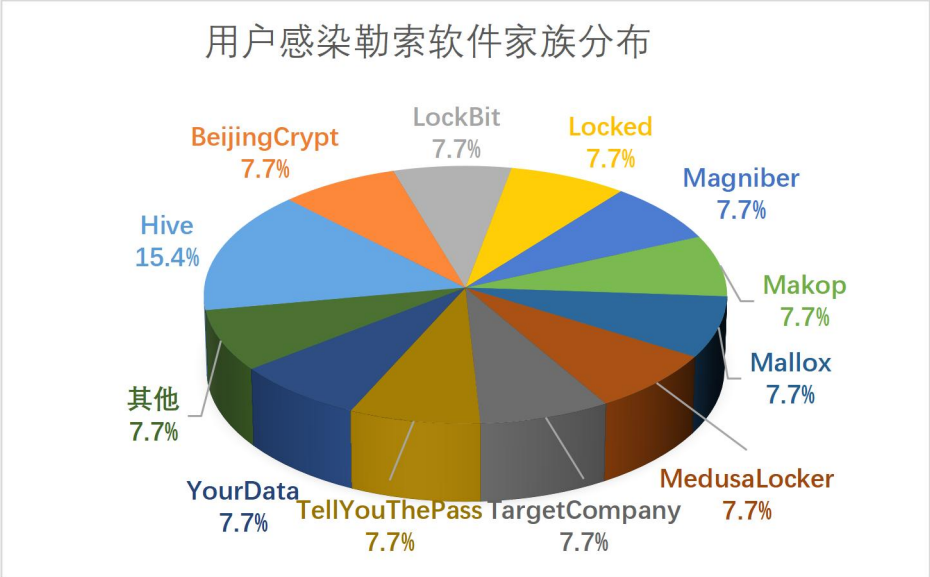




教育科研、电信、政府部门、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

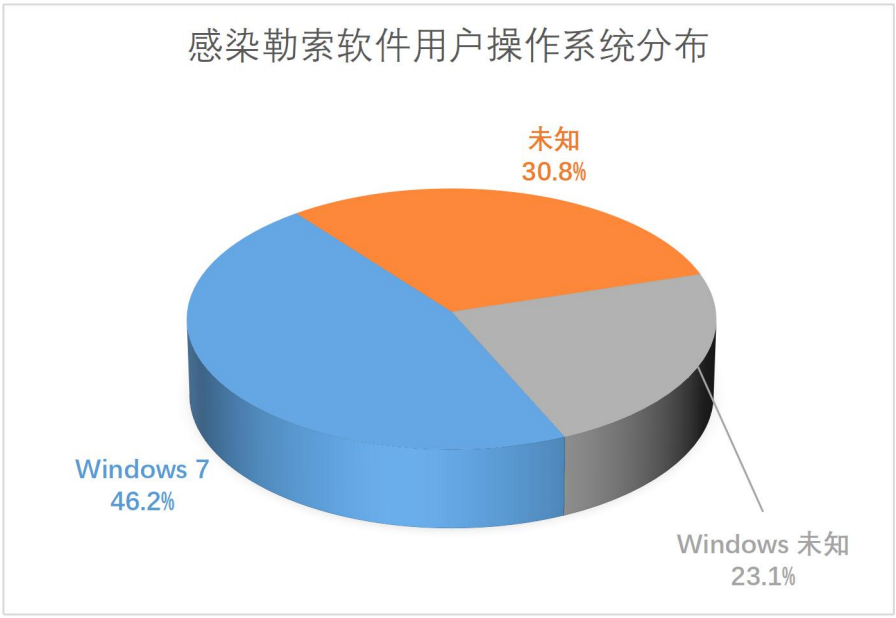



（二）其它勒索软件感染情况

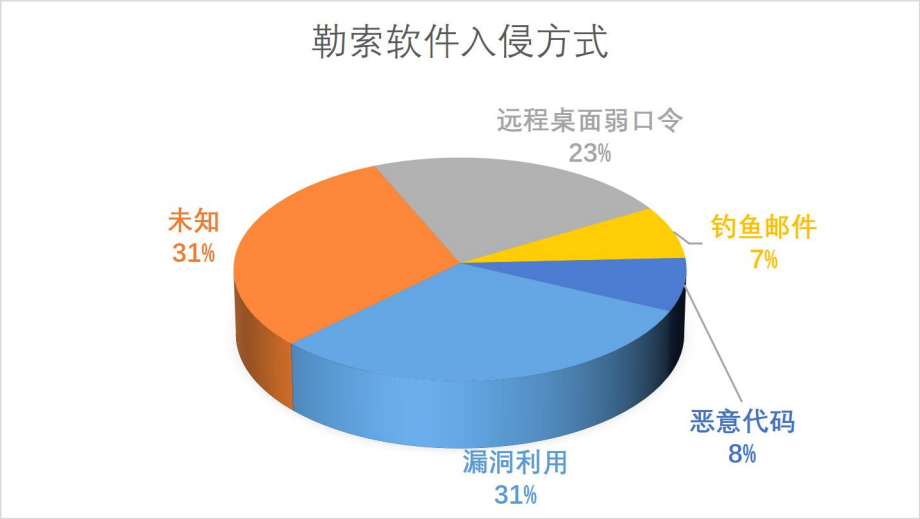
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 13 起非 Wannacry 勒索软件感染事件，较上周下降 53.6%，排在前三名的勒索软件家族分别为 Hive（15.4%）、BeijingCrypt（7.7%）和 LockBit（7.7%）。




本周，被勒索软件感染的系统中 Windows 7 系统占比较高，占到总量的 46.2%，除此之外还包括多个其它不同版本的 Windows 系统和其它类型的操作系统。




本周，勒索软件入侵方式中，漏洞利用和远程桌面弱口令占比较高，分别为 31%和 23%。Hive 勒索软件利用弱口令漏洞特别是远程桌面弱口令频繁攻击我国用户，对我国企业和个人带来较大安全威胁。




## 三、典型勒索软件攻击事件

### （一） 国内部分

#### 1、深圳某医疗行业单位办公终端感染 TargetCompany 勒索软件

本周，工作组成员应急响应了深圳某医疗行业单位办公终端感染 TargetCompany 勒索软件事件。攻击者通过发送钓鱼邮件和在社交软件发送钓鱼链接诱使该单位员工点击链接下载并植入勒索软件，随后对受害者的办公终端上的文件进行加密并索要赎金。

此事件中，攻击者通过社会工程传播勒索软件，建议用户加强网络安全意识，不下载来源不明的邮件附件，不访问来源不明的网页链接，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

### （二） 国外部分

#### 1、FBI 披露美国关键基础设施遭到勒索软件攻击

本周，美国联邦调查局（FBI）与美国网络安全与基础设施安全局(CISA)合作发布了等级为 TLP:WHITE 的安全警报,FBI 表示,Ragnar Locker 勒索软件团伙已经入侵了美国多个关键基础设施部门中的至少 52 个组织的 IT 网络，“受影响的实体包括关键制造业、能源、金

融服务、政府和信息技术等部门”。安全警报提供了可用于检测和阻止 Ragnar Locker 勒索软件攻击的 IoC，此外 FBI 还分享了阻止此类攻击的缓解措施。

## 四、威胁情报

**域名**

badiwaw[.]com

balacif[.]com

barovur[.]com

basicem[.]com

bimafu[.]com

bujoke[.]com

buloxo[.]com

bumoyez[.]com

bupula[.]com

cajeti[.]com

cilomum[.]com

codasal[.]com

comecal[.]com

dawasab[.]com

derotin[.]com

dihata[.]com

dirupun[.]com

dohigu[.]com

dubacaj[.]com

fecotis[.]com

fipoleb[.]com

fofudir[.]com

fulujam[.]com

ganobaz[.]com

gerepa[.]com

gucunug[.]com

guvafe[.]com

hakakor[.]com

hejalij[.]com

hepide[.]com

hesovaw[.]com

hewecas[.]com

hideja[.]com

hidusi[.]com

hoguyum[.]com

jecubat[.]com

jegufe[.]com

joxinu[.]com

kelowuh[.]com

Kidukes[.]com

kipitep[.]com

kirute[.]com

kogasiv[.]com

kozoheh[.]com

kuxizi[.]com

kuyeguh[.]com

lipozi[.]com

lujecuk[.]com

masaxoc[.]com

mebonux[.]com

mihojip[.]com

modasum[.]com

moduwoj[.]com

movufa[.]com

nagahox[.]com

nawusem[.]com

nerapo[.]com

newiro[.]com

paxobuy[.]com

pazovet[.]com

pihafi[.]com

pilagop[.]com

pipipub[.]com

pofifa[.]com

radezig[.]com

raferif[.]com

ragojel[.]com

rexagi[.]com

rimurik[.]com

rinutov[.]com

rusoti[.]com

sazoya[.]com

sidevot[.]com

solobiv[.]com

sufebul[.]com

suhuhow[.]com

sujaxa[.]com

tafobi[.]com

tepiwo[.]com

tifiru[.]com

tiyuzub[.]com

tubaho[.]com

vafici[.]com

vegubu[.]com

vigave[.]com

vipeced[.]com

vizosi[.]com

vojefe[.]com

vonavu[.]com

wezeriw[.]com

wideri[.]com

wudepen[.]com

wuluxo[.]com

wuvehus[.]com

wuvici[.]com

wuvidi[.]com

xegogiv[.]com

xekezix[.]com

**IP**

108.26.193.165

108.56.142.135

116.203.132.32

142.44.236.38

149.28.200.140

162.55.38.44

178.32.222.98

185.138.164.18

185.150.117.186

185.172.129.215

185.73.126.105

190.211.254.181

193.111.153.24

193.42.36.53

193.42.39.10

198.12.127.199

198.12.81.56

209.197.3.8

217.25.93.106

23.106.122.192

23.227.202.72

3.220.57.224

3.232.242.170

37.120.238.107

45.144.29.2

45.146.164.193

45.63.89.250

45.90.59.131

45.91.93.75

47.35.60.92

49.12.212.231

5.45.65.52

50.201.185.11

54.91.59.199

79.141.160.43

89.40.10.25

95.216.196.181

**网址**

https://api.ipify[.]org/

**邮箱**

consultransom@tutanota.com