国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 28 期（总第 36 期）　　7 月 9 日-7 月 15 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

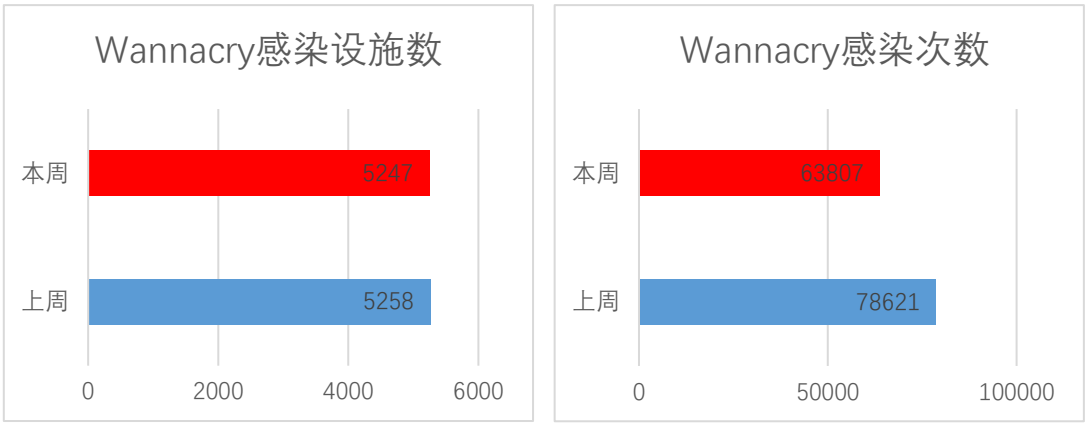
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1127557 个，监测发现勒索软件网络传播 29 次，勒索软件下载 IP 地址 12 个，其中，位于境内的勒索软件下载地址 7 个，占比 58.3%，位于境外的勒索软件下载地址 5 个，占比 41.7%。

二、勒索软件受害者情况

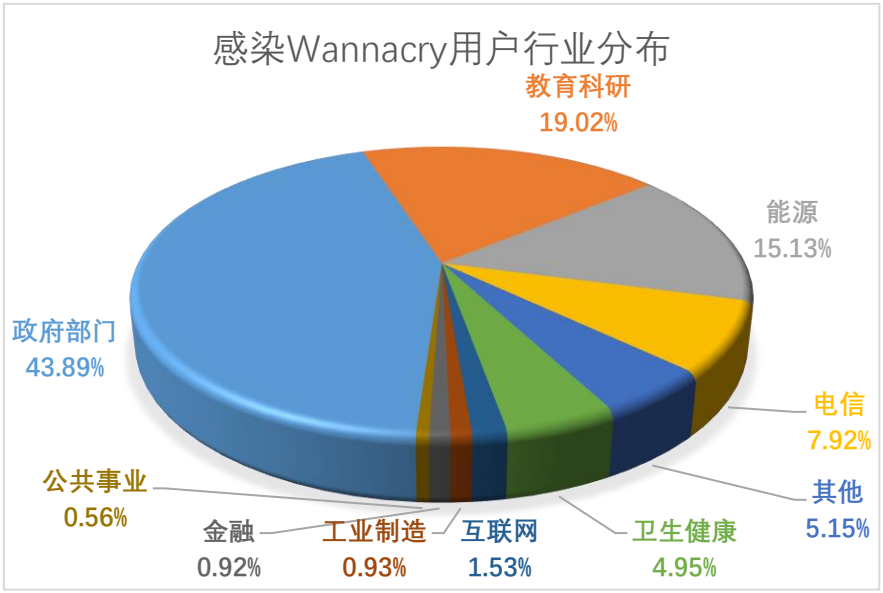
（一）Wannacry 勒索软件感染情况

本周，监测发现 5247 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 0.2%，累计感染 63807 次，较上周下降 18.8%。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。

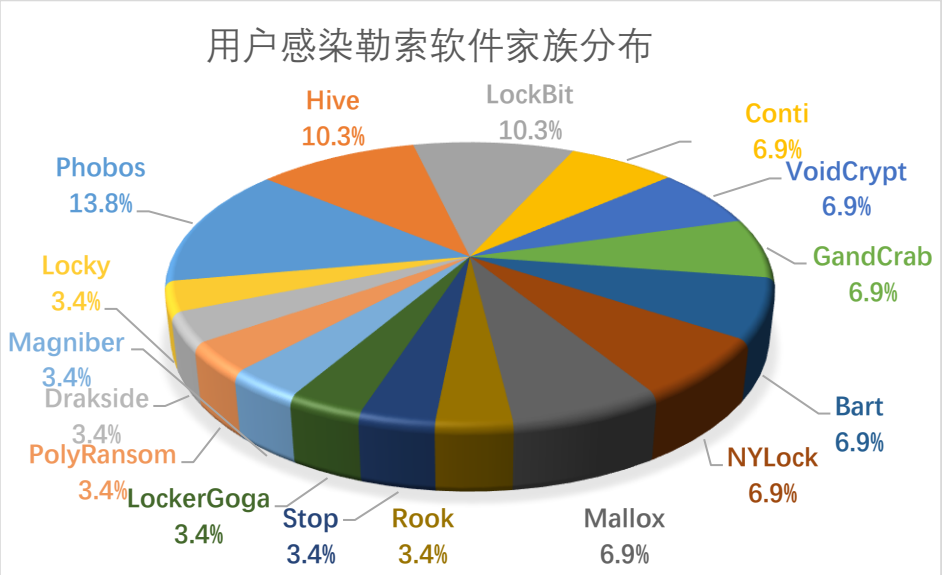


政府部门、教育科研、能源、电信、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

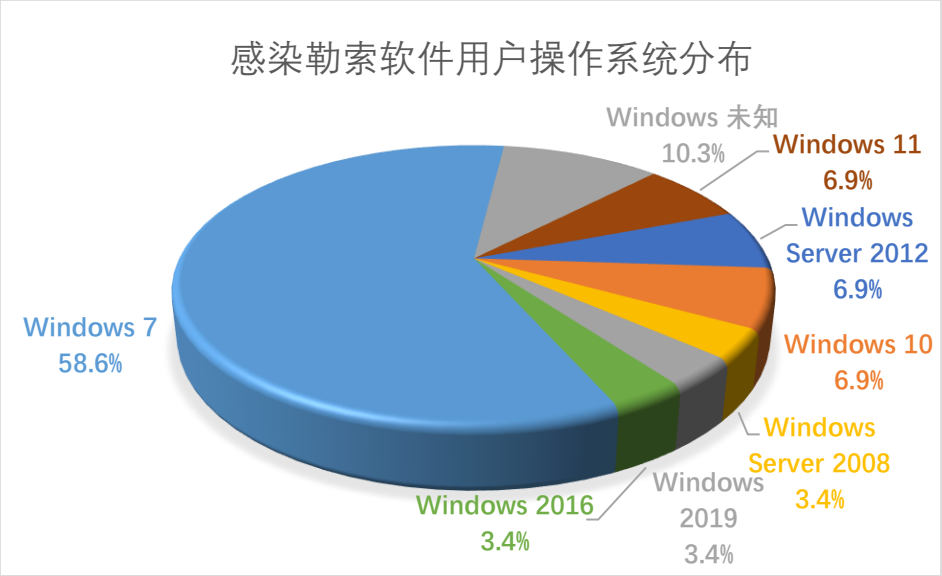


（二）其它勒索软件感染情况

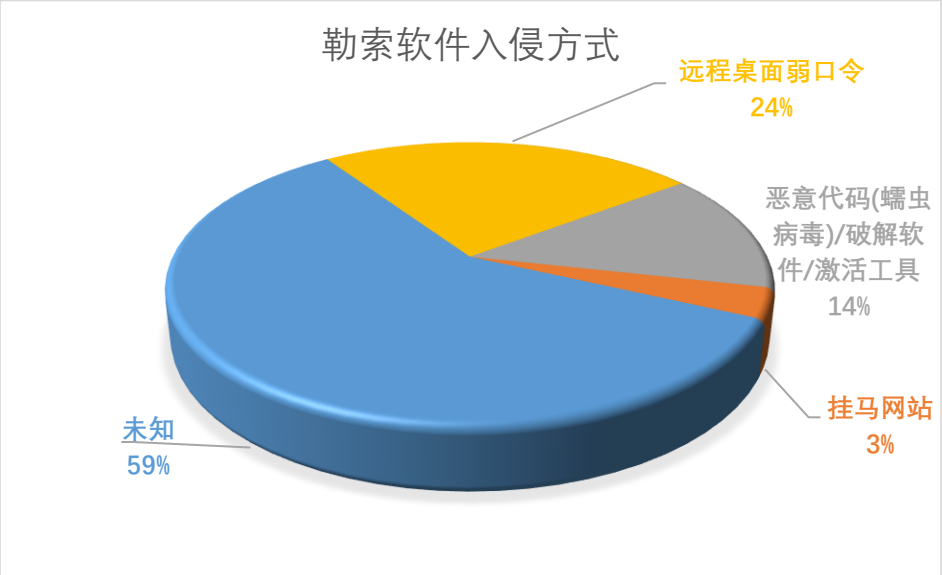
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 29 起非 Wannacry 勒索软件感染事件，较上周增长 45.0%，排在前三名的勒索软件家族分别为 Phobos（13.8%）、Hive（10.3%）和 Lockbit（10.3%）。



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 58.6%，其次为 Windows 11 系统和 Windows Server 2012 系统，占比分别为 6.9%和 6.9%，除此之外还包括多个其它不同版本的 Windows 服务器系统和其它类型的操作系统。



本周，勒索软件入侵方式中，远程桌面弱口令和恶意代码(蠕虫病毒)/破解软件/激活工具占比较高，分别为 24%和 14%。Phobos 勒索软件通过远程桌面弱口令的方式频繁攻击我国用户，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.上海某企业遭勒索病毒攻击

本周，工作组成员应急响应了上海某企业服务器遭勒索病毒攻击的事件。经工作组成员调查分析，攻击者是通过 RDP 端口，对该公司设备发起远程桌面 Administrator 账户密码爆破，爆破成功后放置勒索病毒恶意程序 svchost.exe。

该类勒索病毒的主要传播途径为 RDP 爆破，建议企业和个人用户不要轻易点击不明邮件的可疑链接和可执行附件，同时设置相关密码为无序密码并定时更新。

（二） 国外部分

1. 法国电话运营商 La Poste Mobile 遭勒索软件攻击

法国虚拟移动电话运营商 La Poste Mobile 于近日遭到勒索软件攻击，导致行政和管理服务瘫痪。该公司指出，威胁行为者可能已经访问了其客户的数据。La Poste Mobile 表示，当得知此事件后，该公

司立即采取了必要的保护措施，暂停了相关的计算机系统。另一方面，La Poste Mobile 员工计算机中的文件可能已受到影响。其中一些文件可能包含个人数据。据报道，Lockbit 勒索软件上周在其泄密网站上添加了 La Poste Mobile 的名称。

四、威胁情报

域名

namanstationers[.]com

0mega-connect[.]biz

网址

http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd[.]onion

http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd[.]onion

http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd[.]onion

http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad[.]onion

http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd[.]onion

http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd[.]onion

http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd[.]onion

http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd[.]onion

http://lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd[.]onion

http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead[.]onion.ly

IP

20.227.128.33

23.254.229.90

192.119.110.47

192.119.110.22

192.119.111.25

192.236.178.3

192.236.177.251

192.236.193.152

192.236.193.150

192.236.193.148

192.236.193.151

192.236.193.149

192.236.193.141

192.236.193.140

192.236.177.20

192.236.176.79

邮箱

niss.brook@onionmail.org

niss.brandon@mailfence.com

Juli1992@mailfence.com

Juli1990@mailfence.com

stephenjoffe@privatemail.com

henderson@cock.li

helprecovery@gnu.gr

energyhack@cock.li