国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 20 期（总第 28 期）　　5 月 14 日-5 月 20 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

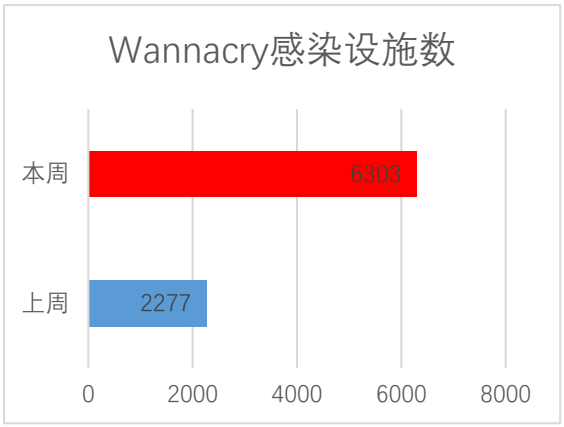
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1081141 个，监测发现勒索软件网络传播 1217 次，勒索软件下载 IP 地址 31 个，其中，位于境内的勒索软件下载地址 11 个，占比 12.1%，位于境外的勒索软件下载地址 80 个，占比 87.9%。

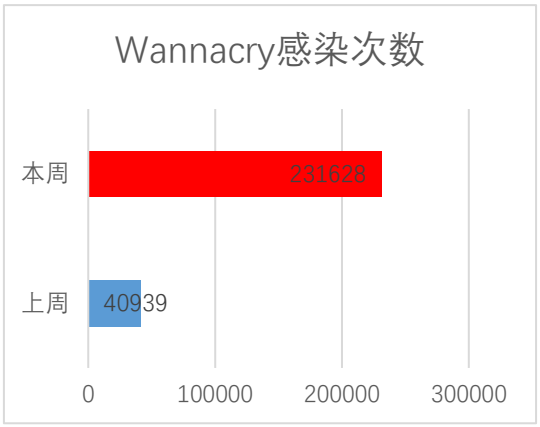
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

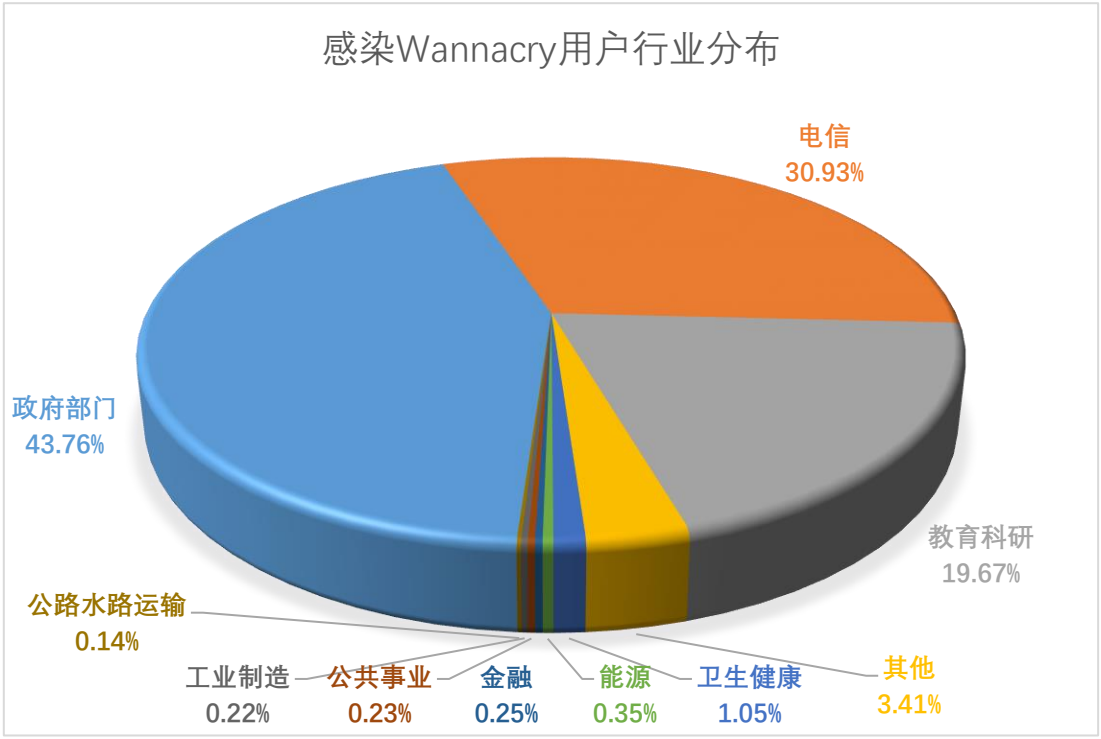
本周，监测发现 6303 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 176.8%，累计感染 231628 次，较上周上升 465.8%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机

没有针对常见高危漏洞进行合理加固的现象。





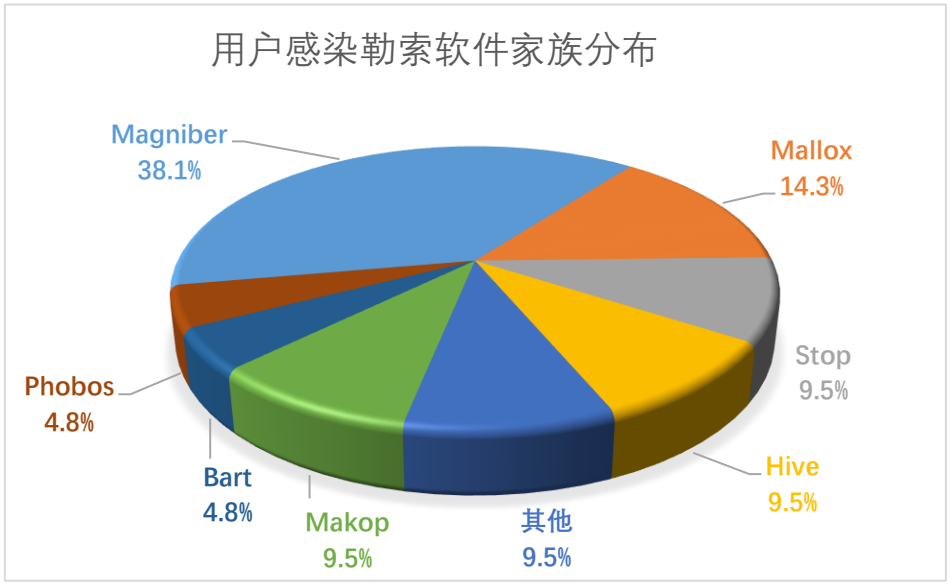
政府部门、电信、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。



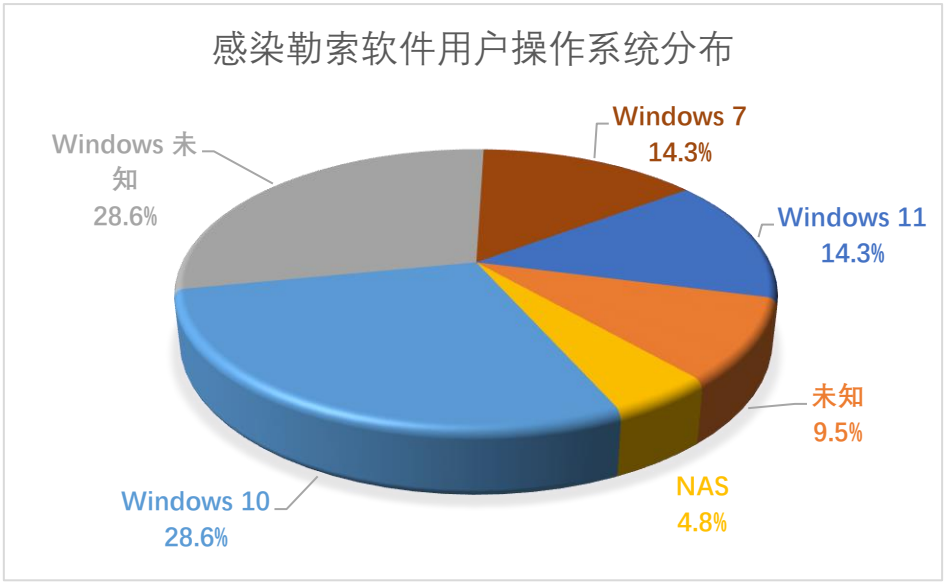
（二）其它勒索软件感染情况

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 21 起，非 Wannacry 勒索软件感染事件，较上周下降 36.4%，排在前三名的勒索软件家族分别为 Magniber（38.1%）、Mallox（14.3%）和 Stop

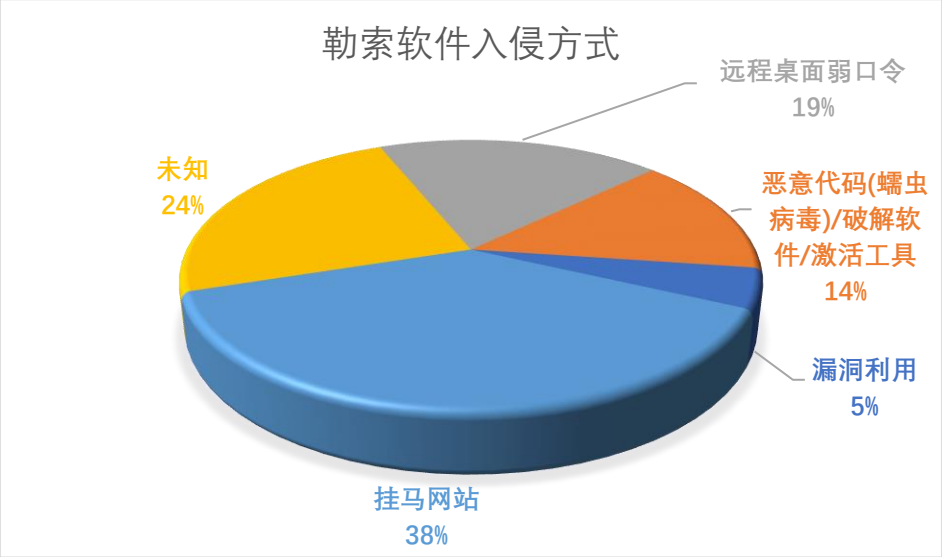
（9.5%）。



本周，被勒索软件感染的系统中 Windows 10 系统占比较高，占到总量的 28.6%，其次为 Windows 7 系统和 Windows 11 系统，占比分别为 14.3%和 14.3%，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，挂马网站和远程桌面弱口令占比较高，分别为 38%和 19%。Magniber 勒索软件利用挂马网站频繁攻击我国用户，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

本周，工作组成员单位在自助监测和应急响应中未发现典型勒索软件攻击事件。

（二） 国外部分

1. 加拿大战斗机培训公司遭 LockBit 勒索软件攻击

5 月 11 日，加拿大战斗机培训公司 Top Aces 表示已经遭到勒索软件攻击。Top Aces 总部位于加拿大蒙特利尔，自称其拥有“全球规模最大的私营作战战斗机”。 Top Aces 公司目前已经出现在 LockBit 勒索软件组织的泄密网站上。 LockBit 勒索软组织将 5 月 15 日设为最后期限，如未支付赎金，则将泄露其窃取的 44GB 数据。

四、威胁情报

域名

tor2web.blutmagie[.]de

24u4jf7s4regu6hn.tor2web[.]org

24u4jf7s4regu6hn.fenaow48fn42[.]com

ugll[.]org

zerit[.]top

IP

104.18.32.68

23.216.147.64

175.120.254.9

149.154.167.99

115.88.24.202

网址

http://3c189aa0ea24b020fa68f0c016d86coyvknmvy[.]fightof.info/coyvknmvy

http://3c189aa0ea24b020fa68f0c016d86coyvknmvy[.]penbars.info/coyvknmvy

http://3c189aa0ea24b020fa68f0c016d86coyvknmvy[.]rowarea.info/coyvknmvy

http://3c189aa0ea24b020fa68f0c016d86coyvknmvy[.]scanold.info/coyvknmvy

http://3c189aa0ea24b020fa68f0c016d86coyvknmvy.y4mo334ccjujtl36swabwndobil2j
dywn2eg5cplmicrbbjurh4ggcid[.]onion/coyvknmvy

http://c4241a5006b838901a2c2ee82c906pjckojid.lookits[.]info/pjckojid

http://c4241a5006b838901a2c2ee82c906pjckojid.h6rkhuaewx5qtwxikinvfmrn4gmpw
2kzdru2fsmpqtsqk2no7lnagiyd[.]onion/pjckojid

http://c4241a5006b838901a2c2ee82c906pjckojid.barshow[.]info/pjckojid

http://c4241a5006b838901a2c2ee82c906pjckojid.doeof[.]info/pjckojid

http://c4241a5006b838901a2c2ee82c906pjckojid.catomit[.]info/pjckojid

邮箱

Spiderlock@email.tg

ginnydterrell@onionmail.org

yoshihama@tutanota.com

fine3412@mailfence.com

fine3413@mailfence.com

hughclapperton1877@gmx.com

help24@nerdmail.co

millenniumcrypt@msgsafe.io

ironse2022@tutanota.com

NormanBaker1929@gmx.com

钱包地址

3DkXKnWRPmVVm6Nwm6Hyu8eFXc5rvZ8f5y