国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 24 期 (总第 32 期)　　6 月 11 日-6 月 17 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

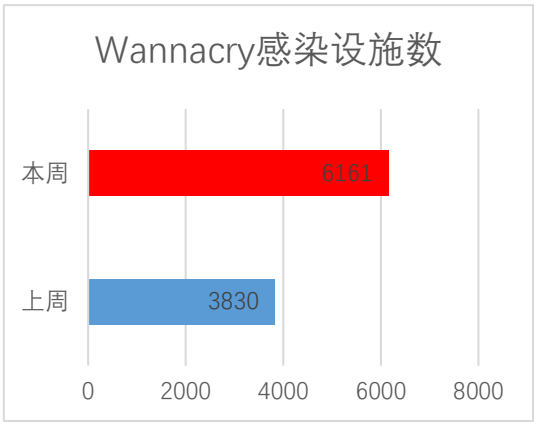
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1068414 个，监测发现勒索软件网络传播 550 次，勒索软件下载 IP 地址 23 个，其中，位于境内的勒索软件下载地址 14 个，占比 60.9%，位于境外的勒索软件下载地址 9 个，占比 39.1%。

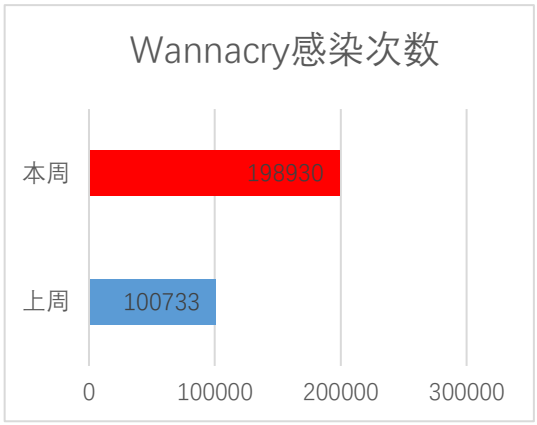
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

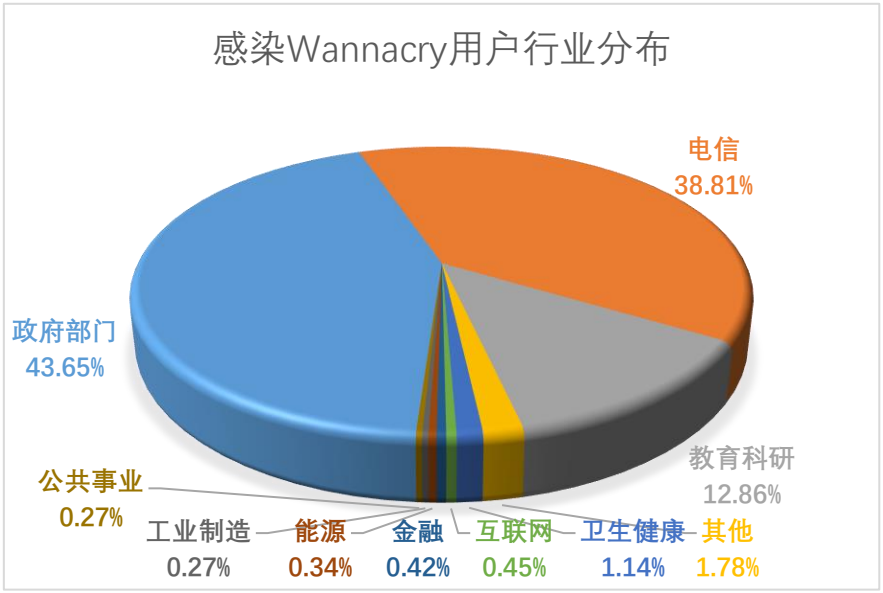
本周，监测发现 6161 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 60.9%，累计感染 198930 次，较上周上升 97.5%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



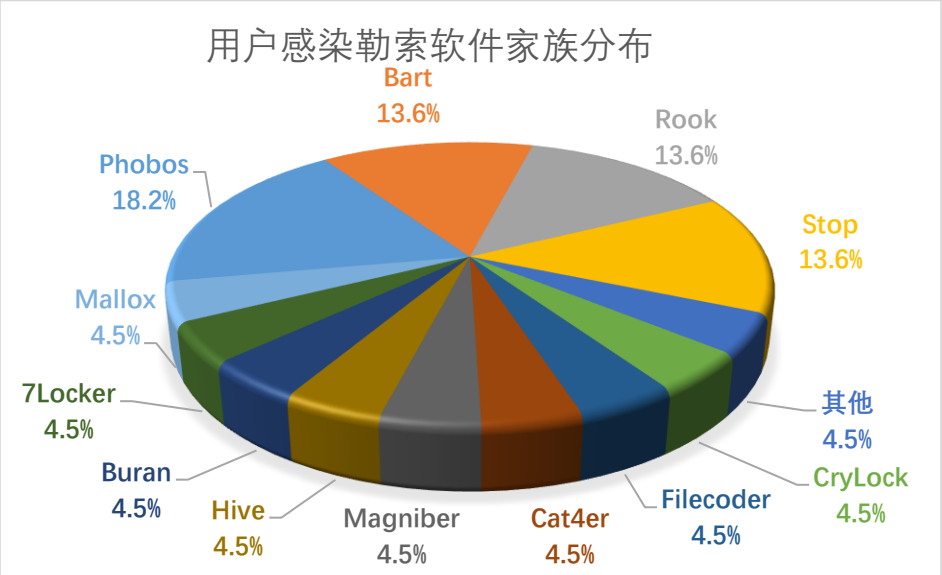


政府部门、电信、教育科研、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

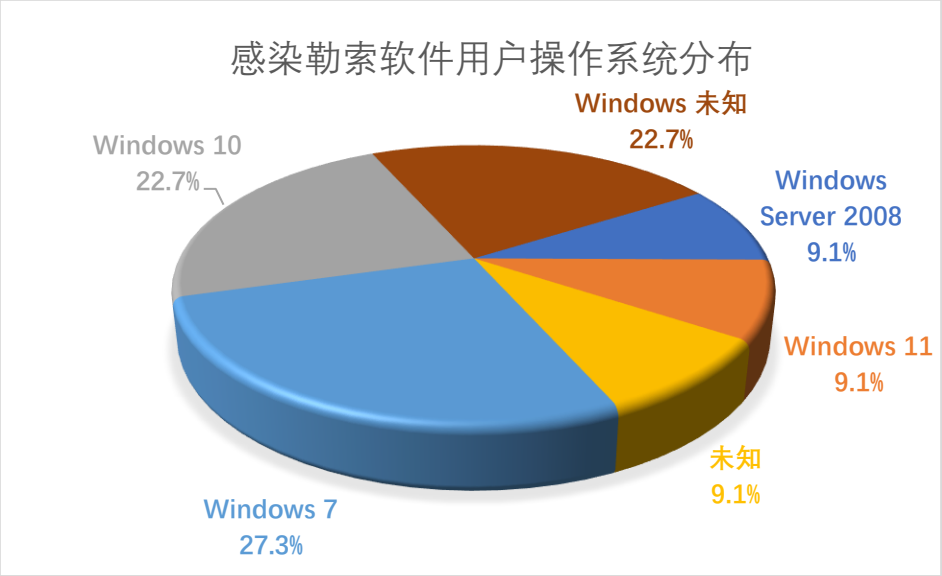


（二）其它勒索软件感染情况

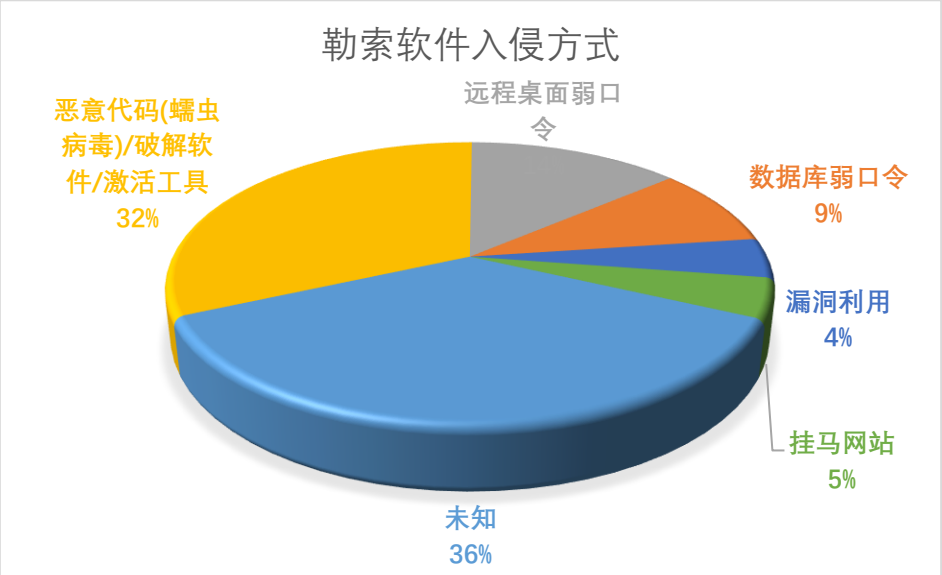
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 22 起非 Wannacry 勒索软件感染事件，较上周下降 18.5%，排在前三名的勒索软件家族分别为 Phobos（18.2%）、Bart（13.6%）和 Rook（13.6%）。



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 27.3%，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 22.7%和 9.1%，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，恶意代码(蠕虫病毒)/破解软件/激活工具和远程桌面弱口令占比较高，分别为 32%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. 广西某企业遭勒索病毒攻击

本周，工作组成员应急响应了广西某单位服务器被攻击的事件。经工作人员分析，攻击过程可能是通过下级单位进入，在今年 4 月份，通过未知途径将以 txt 后缀伪装的恶意程序植入主机，由于监管不严密，导致勒索事件发生。日志信息已经在近日被清除，因此工作人员未能获知具体攻击途径。

为防止此类勒索病毒攻击事件发生，企业和个人应加强安全意识，注意对日志或数据进行实时备份，减少损失。此外要定期对相关管理人员和技术人员进行安全培训，提高安全技术能力和实际操作能力。

2. 沈阳某公司疑似被俄罗斯勒索组织入侵

本周，工作组成员应急响应了沈阳某公司设备被俄罗斯勒索团伙入侵的事件。本次事件由工作组成员单位的安全监测系统检测发现，该设备被另一台设备通过 Guest 账户远程控制，并尝试使用

AccountRestore.exe 程序暴力获取管理员账户凭据。通过对 AccountRestore.exe 进行 hash 关联，发现此次攻击很大概率是由俄罗斯勒索团伙发起。

境外勒索组织的活动给我国企业和用户的信息安全带来了较大威胁，企业应定期对设备进行专业评估，要及时掌握信息系统的安全状况，从而降低被入侵的风险。

（二） 国外部分

1. Tenafly 公立学校遭受勒索软件攻击导致考试被取消

上周，Tenafly 公立学校发现勒索软件对学区网络中的一些计算机上的数据进行了加密，导致考试和课程被取消，重新使用纸、铅笔和投影仪。官员们表示，该学校试图在网络安全顾问的帮助下恢复系统上线，该学区所有高中生的期末考试也被取消。地区通讯经理说，Tenafly 公立学区管理人员首先发现了这起安全事件，该事件涉及通过勒索软件对学区网络中某些计算机上的数据进行加密。

四、威胁情报

域名

btc-trazer[.]xyz

sandbox.x4k[.]me

malware.x4k[.]me

f.x4k[.]me

0.x4k[.]me

pwn.x4k[.]me

docker.x4k[.]me

apk.x4k[.]me

x4k[.]me

IP

164.68.114.29

167.86.87.27

63.250.53.180

45.15.19.130

46.39.229.17

网址

7245iwyqbwwgaxwjklvitrjyof4hzp7ohmgonsy5nh2lnbdnwvfutryd[.]onion

http://98748ec032f80cd058dc82c0caa8f020qywtemeia.eyeflat[.]info/qywtemeia

http://98748ec032f80cd058dc82c0caa8f020qywtemeia.themits[.]info/qywtemeia

http://98748ec032f80cd058dc82c0caa8f020qywtemeia.barmiss[.]info/qywtemeia

http://98748ec032f80cd058dc82c0caa8f020qywtemeia.matchor[.]info/qywtemeia

http://98748ec032f80cd058dc82c0caa8f020qywtemeia.qt7xt3gtmmzu22myu7e7rgcj5ise6kkttijb4kskbk4tgxzyegh644id[.]onion/qywtemeia

http://78382658f0b45a80149c62c0daf05030ysmvpqra.themits[.]info/ysmvpqra

http://78382658f0b45a80149c62c0daf05030ysmvpqra.barmiss[.]info/ysmvpqra

http://78382658f0b45a80149c62c0daf05030ysmvpqra.matchor[.]info/ysmvpqra

http://78382658f0b45a80149c62c0daf05030ysmvpqra.eyeflat[.]info/ysmvpqra

邮箱

d3add@privatemail.com

supportx@privatemail.com

yoshihama@privatemail.com

ariakei@protonmail.com

buybackdate@privatemail.com

tomas1991goldberg@medmail.ch