国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 14 期（总第 22 期）　　4 月 2 日-4 月 8 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

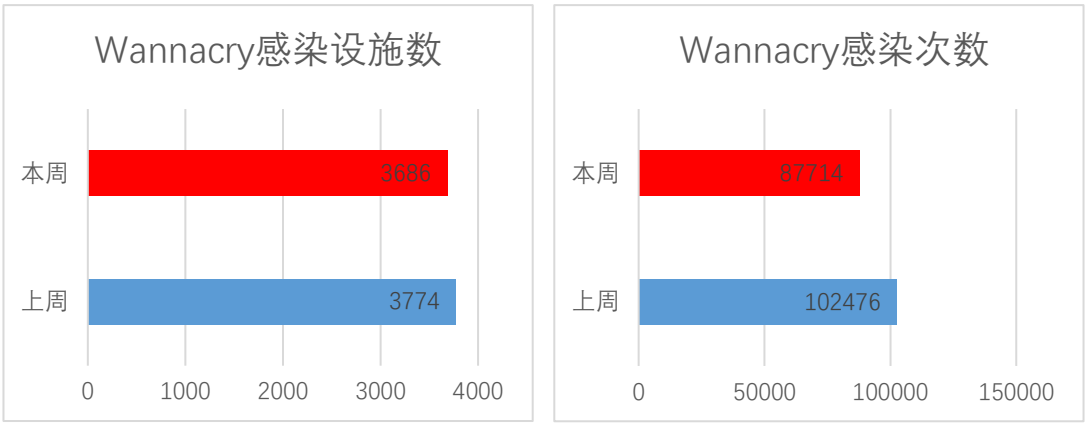
本周勒索软件防范应对工作组共收集捕获勒索软件样本 629728 个，监测发现勒索软件网络传播 1680 次，勒索软件下载 IP 地址 644 个，其中，位于境内的勒索软件下载地址 275 个，占比 42.7%，位于境外的勒索软件下载地址 369 个，占比 57.3%。

二、勒索软件受害者情况

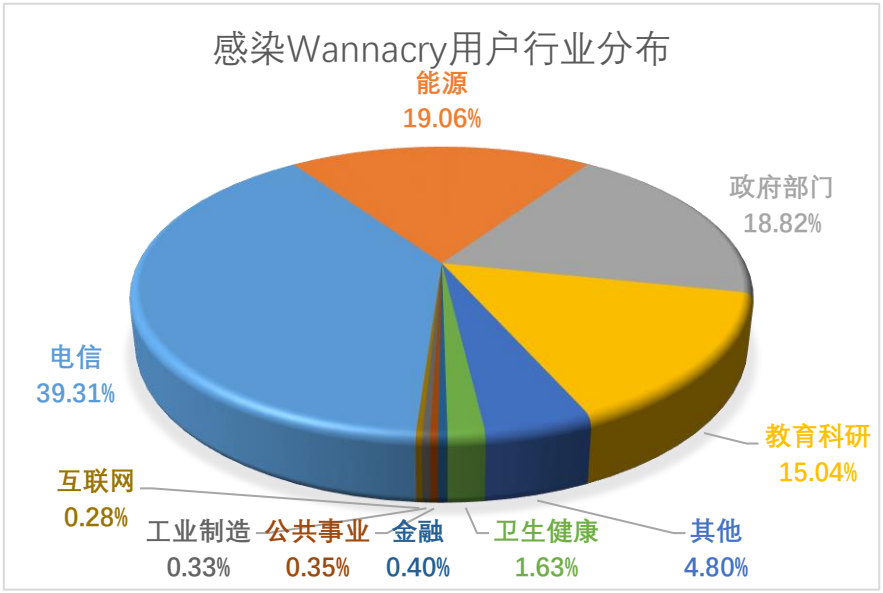
（一）Wannacry 勒索软件感染情况

本周，监测发现 3686 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 2.3%，累计感染 87714 次，较上周下降 14.4%。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。

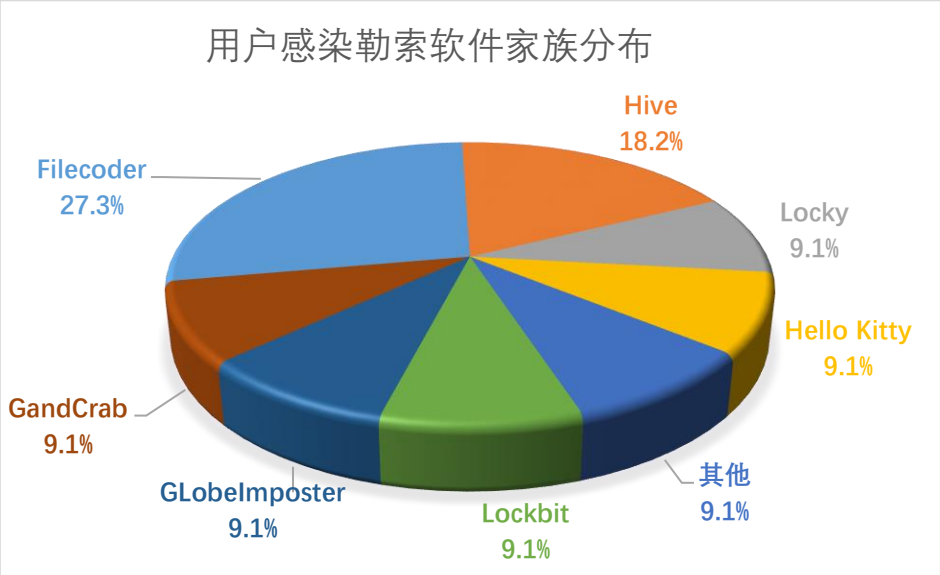


电信、能源、政府部门、教育科研、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

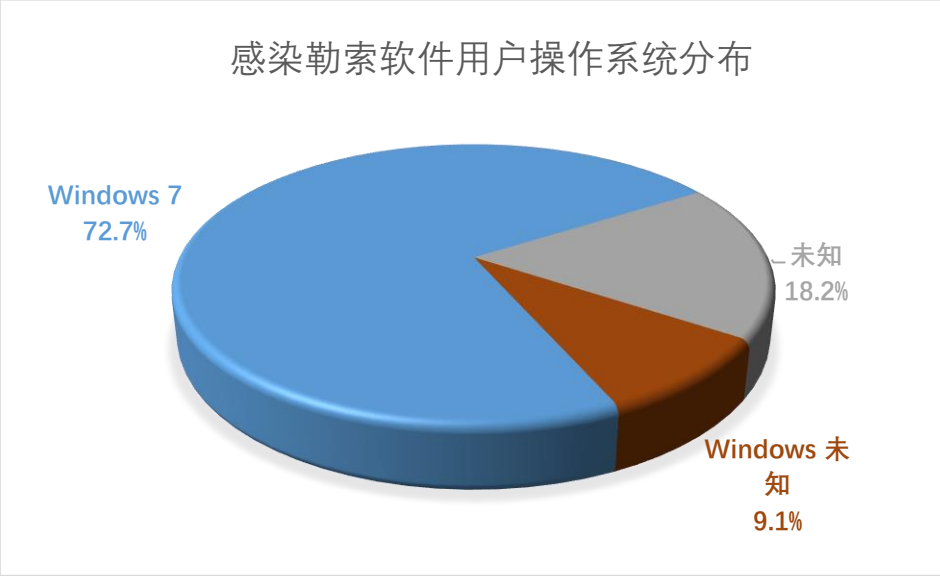


（二）其它勒索软件感染情况

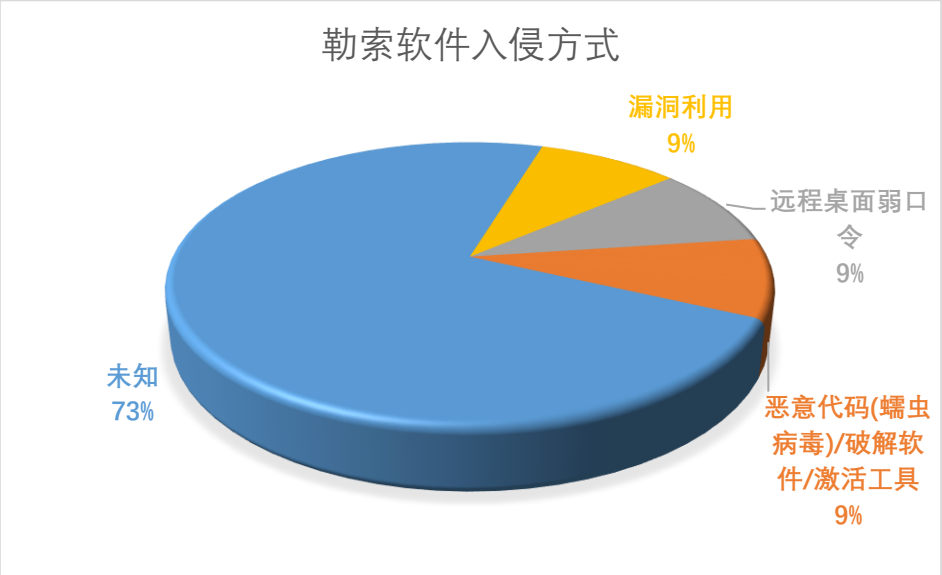
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 11 起，非 Wannacry 勒索软件感染事件，较上周下降 64.5%，排在前三名的勒索软件家族分别为 Filecoder（27.3%）、Hive（18.2%）和 Locky（9.1%）。



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 72.7%，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，漏洞利用和远程桌面弱口令占比较高，分别为 9%和 9%。Filecoder 勒索软件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主检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、美国利福尼亚州一医疗保健组织遭 Hive 勒索软件攻击

Partnership HealthPlan of California 是一个帮助美国加州数十万人获得医疗保健服务的非营利组织，正受到 Hive 勒索软件团伙的攻击。目前还不清楚攻击是何时开始的，Partnership HealthPlan 目前也无法回应置评请求，但加州当地报纸在 3 月 24 日率先报道了该组织面临技术问题。该组织在其网站上说，它开始遇到技术困难，导致某些计算机系统中断。目前该组织已聘请网络安全专家处理中断并恢复系统。威胁分析师分享了 Hive 勒索软件页面的屏幕截图，Hive 勒索软件团伙称其攻击了 Partnership HealthPlan 并窃取了超过 85 万人的个人信息，还声称从该组织的服务器上窃取了 400GB 的文件。

四、威胁情报

IP

131.107.255.255

34.107.221.82

网址

http://91.243.44[.]142/arx-Ymkdlg_Egohmqht.jpg

http://91.243.44[.]142/arx2-Lnjqrlfmk_Dtskvkje.png