国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 25 期（总第 33 期）　　6 月 18 日-6 月 24 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

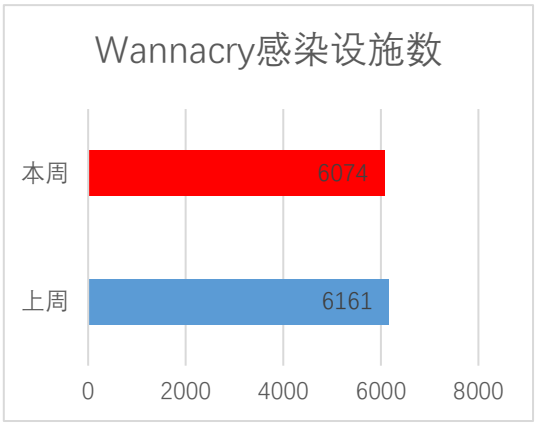
本周勒索软件防范应对工作组共收集捕获勒索软件样本 985424 个，监测发现勒索软件网络传播 1095 次，勒索软件下载 IP 地址 30 个，其中，位于境内的勒索软件下载地址 16 个，占比 53.3%，位于境外的勒索软件下载地址 14 个，占比 46.7%。

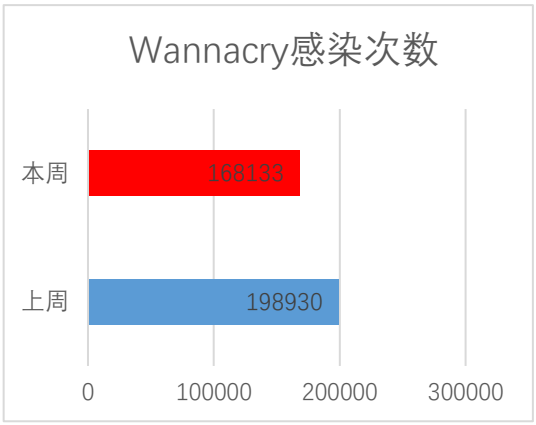
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

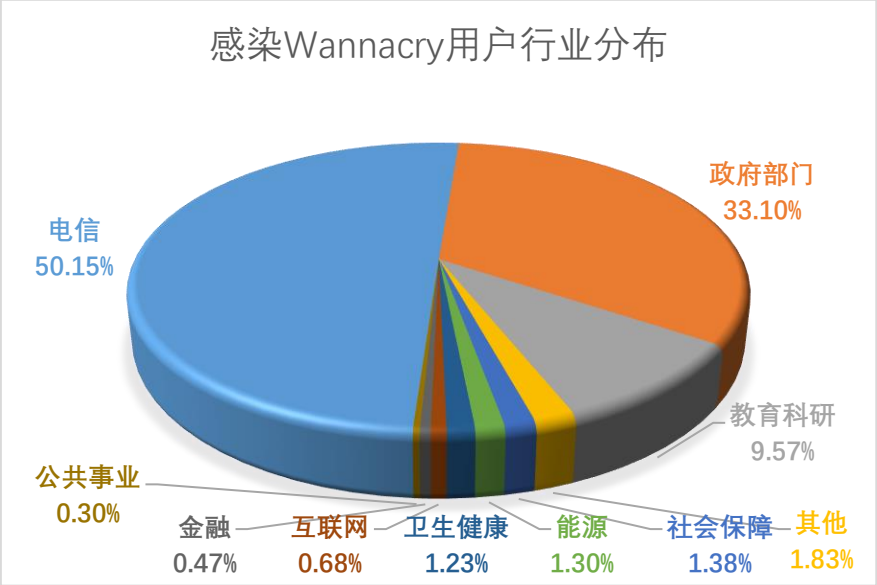
本周，监测发现 6074 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 1.4%，累计感染 168133 次，较上周下降 15.5%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



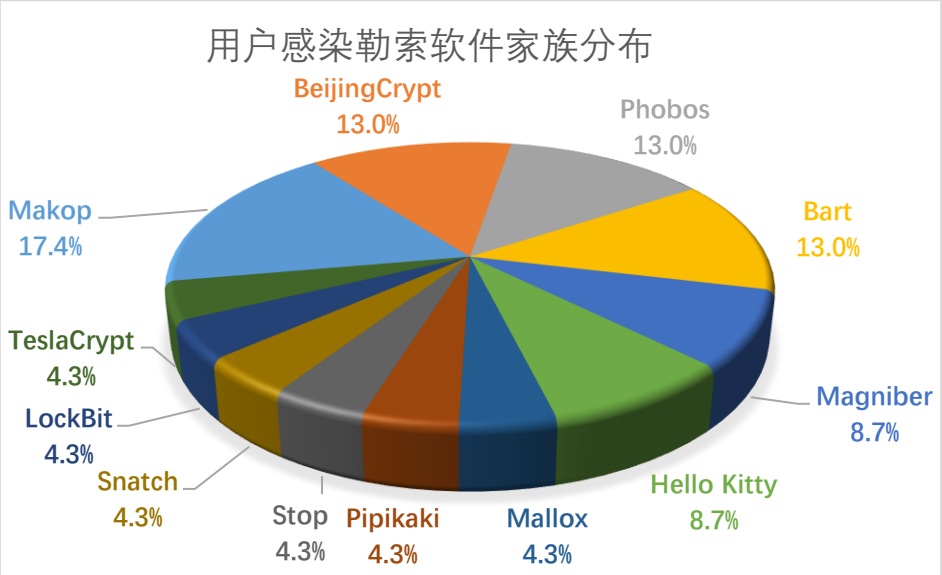


政府部门、电信、教育科研、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

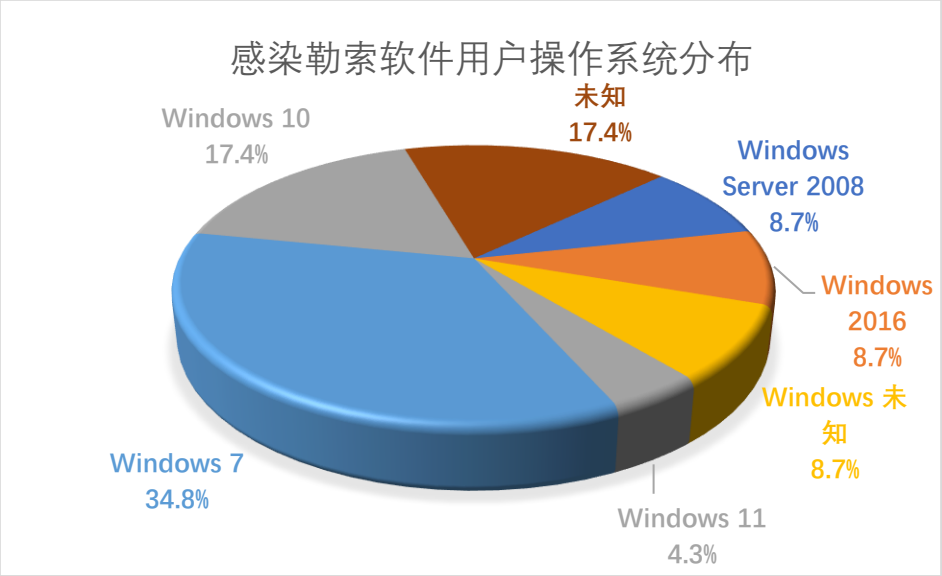


（二）其它勒索软件感染情况

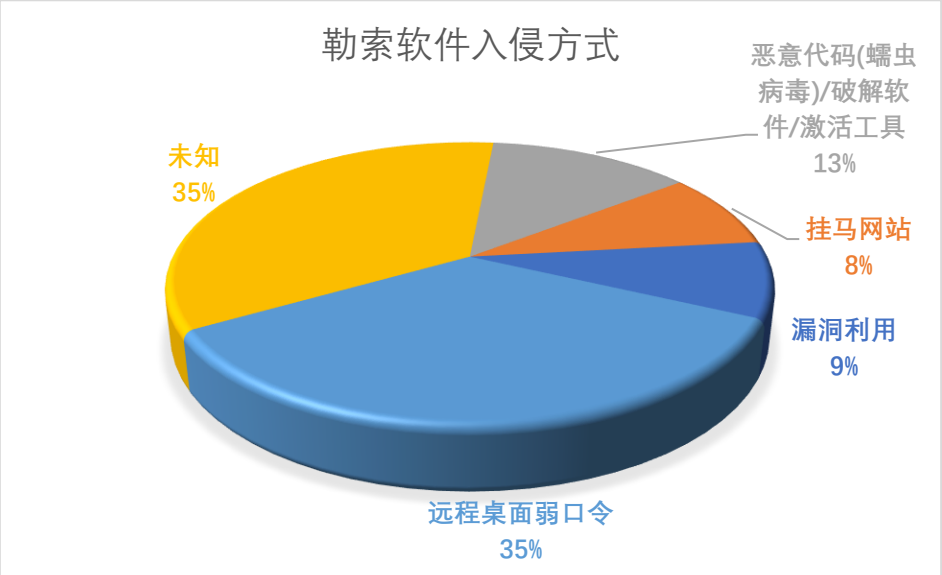
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 23 起非 Wannacry 勒索软件感染事件，较上周上升 4.5%，排在前三名的勒索软件家族分别为 Makop（17.4%）、BeijingCrypt（13.0%）和 Phobos（13.0%）。



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 34.8%，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 17.4%和 8.7%，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，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 35%和 13%。Makop 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. 江苏省某医疗单位遭勒索病毒攻击

本周，工作组成员应急响应了江苏省某医疗单位内网的多台服务器被勒索病毒攻击事件。经分析，攻击者极可能是通过服务器上的 Web 应用漏洞获取到了一定的服务器权限，上传 Anydesk 远程控制工具，并登录成功。随后在内网横向爆破其他服务的 3389 口令进而人工投放勒索病毒。

企业和用户应定期对重要业务资产与映射到外网的资产进行渗透测试排查，挖掘潜在安全隐患，避免造成财产损失以及更大的安全事件发生。

2. 深圳某制造业单位遭 Makop 勒索病毒攻击

本周，工作组成员应急响应了深圳某制造业单位多台服务器遭受 Makop 勒索病毒攻击事件。经过工作人员结合防火墙策略、日志信息等数据进行分析，基本判定攻击者通过外网对服务器某端口进行暴力

破解，后在内网中横向爆破服务器，进行人工投放勒索病毒。

近日，Makop 勒索病毒频繁攻击我国用户，给企业和个人造成了较大的安全威胁。建议企业关闭不必要的服务器端口，同时避免使用弱口令，提高安全意识。

（二） 国外部分

1. 蒙特罗斯环境集团遭勒索软件攻击导致实验室检测业务中断

总部位于美国的环境服务提供商蒙特罗斯环境集团透露，该公司上周末受到勒索软件攻击，导致其实验室检测业务中断。该公司表示:“这起事件主要影响了焓分析实验室网络中的计算机和服务器，某些实验室结果将被推迟。”蒙特罗斯的子公司焓分析公司(Enthalpy Analytical)在美国各地运营着 11 个环境测试实验室，测试空气、土壤、水和其他物质的毒性和污染物。在发现网络入侵后，蒙特罗斯暂停了受影响的系统，通知了执法部门，并开始在网络安全专家的帮助下修复系统。

四、威胁情报

IP

13.107.4.52

23.216.147.64

网址

http://789018886094744048f49eb8240c5030jwgthqcs.redbuy[.]info/jwgthqcs

http://789018886094744048f49eb8240c5030jwgthqcs.mlqtijwa4o5tajkxjlmhr2dkkjllrfovfeiux5olf3cmkz7ou2fnzkid[.]onion/jwgthqcs

http://789018886094744048f49eb8240c5030jwgthqcs.tooend[.]info/jwgthqcs

http://789018886094744048f49eb8240c5030jwgthqcs.plugto[.]info/jwgthqcs

http://789018886094744048f49eb8240c5030jwgthqcs.linksad[.]info/jwgthqcs

http://fca08460eee4c0508cf87250544c2e60gweyrkc.didbuys[.]info/gweyrkc

http://fca08460eee4c0508cf87250544c2e60gweyrkc.outdeem[.]info/gweyrkc

http://fca08460eee4c0508cf87250544c2e60gweyrkc.sadby[.]info/gweyrkc

http://fca08460eee4c0508cf87250544c2e60gweyrkc.keysask[.]info/gweyrkc

http://fca08460eee4c0508cf87250544c2e60gweyrkc.ohgig7nhgjh5ddsyh2x344plk5m

bzuwhlkoedardqqf4mg3g675lrrad[.]onion/gweyrkc

邮箱

Starmoon@my.com

bsupport@email.tg

brendasrivera@tutanota.com

poolhackers@tutanota.com

shadowghosts@tutanota.com

takunoya@tutanota.com

钱包地址

19YoZErfvQybkwWppADhVFprRdvvf3Rcxv