国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 49 期（总第 57 期）　　12 月 3 日-12 月 9 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

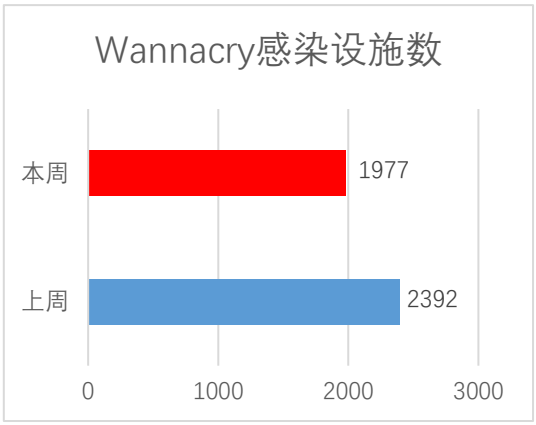
本周勒索软件防范应对工作组共收集捕获勒索软件样本 277393 个，监测发现勒索软件网络传播 158 次，勒索软件下载 IP 地址 30 个，其中，位于境内的勒索软件下载地址 9 个，占比 30.0%，位于境外的勒索软件下载地址 21 个，占比 70.0%。

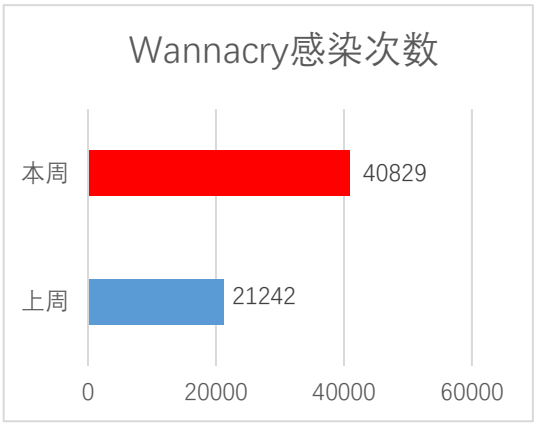
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

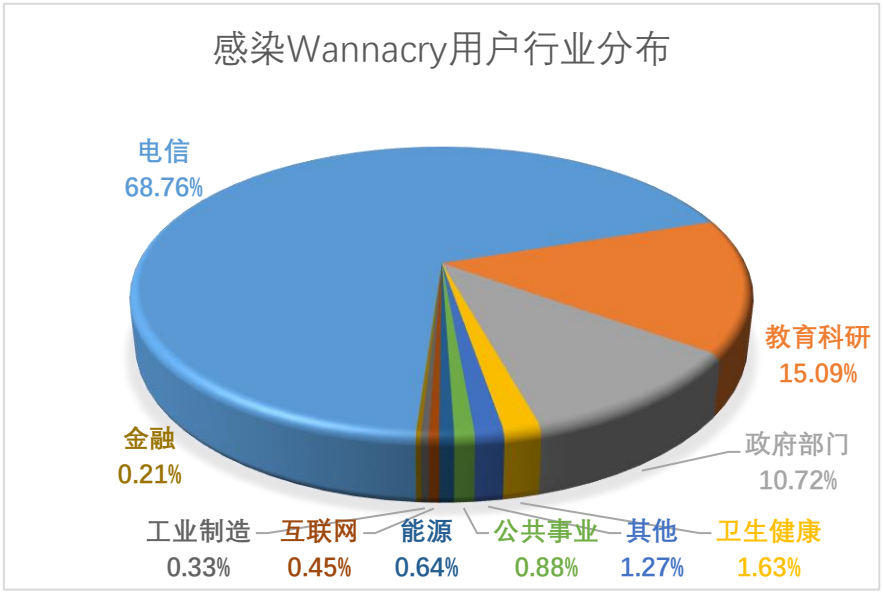
本周，监测发现 1977 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 17.3%，累计感染 40829 次，较上周增长 92.2%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。





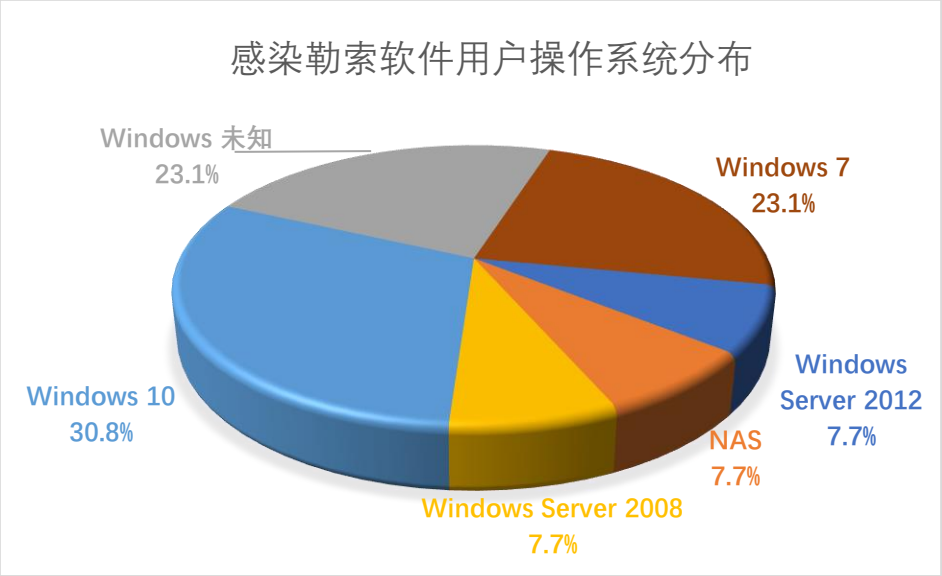
电信、教育科研、政府部门、卫生健康、公共事业行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。



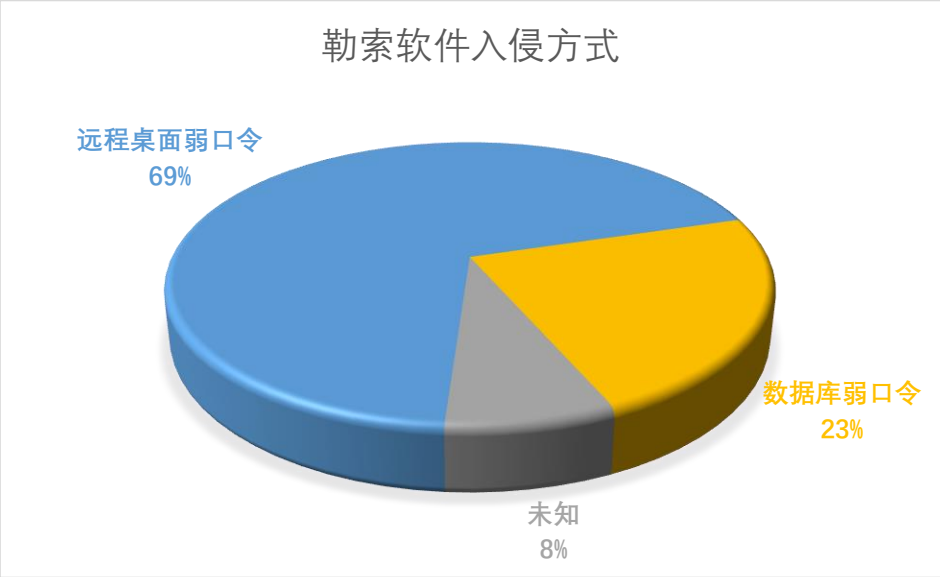
（二）其它勒索软件感染情况

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 13 起非 Wannacry 勒索软件感染事件，较上周下降 40.9%，排在前三名的勒索软件家族分别为 Phobos（46.2%）、Mallox（15.4%）和 Sodinokibi（7.7%）。

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 30.8%，其次为 Windows 7 系统和 Windows Server 2012 系统，占比分别为 23.1%和 7.7%，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，远程桌面弱口令和数据库弱口令占比较高，分别为 69%和 23%。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.浙江省某政府单位遭受勒索病毒攻击

本周，工作组成员应急响应了浙江省某政府单位服务器遭到勒索病毒攻击的安全事件。由于该服务器使用了弱口令，攻击者通过暴力破解的方式登录服务器后部署勒索病毒，并利用该勒索病毒篡改了系统时间。此后以该服务器为跳板，同样通过暴力破解的手段登录另一台使用弱口令的服务器，释放勒索病毒。该勒索病毒伪装为微软系统软件“svchost.exe”，经提取分析认证为 Phobos 勒索病毒家族。由于服务器无连接信息，系统日志无具体登录信息，无法追溯攻击者具体来源。

建议企业的系统、服务器等设备禁止使用弱口令，且禁止密码重用的情况出现。同时限制服务器登录密码次数，限制相同 IP 访问失败次数，从而将被攻击者暴力破解的可能性降至最低。

（二） 国外部分

1. 勒索软件攻击迫使法国医院转移病人

位于巴黎郊区的安德雷·米格诺教学医院因 12 月 3 日晚发生的勒索软件攻击，不得不关闭其电话和电脑系统。据称，这起勒索软件事件背后的攻击者已经要求赎金。但院方并不打算支付。目前，医院已取消了部分手术。据法国卫生与预防部长弗朗索瓦·布劳恩表示，院方还被迫将 6 名患者从新生儿和重症监护室转移到其他医疗机构。

负责数字转型和电信的部长代表让·诺埃尔·巴罗表示，医院已隔离了受感染的系统来限制勒索软件向其他设备的传播，并向法国国家信息系统安全与防御局（ANSSI）发出了警报。

四、威胁情报

IP

162.159.128.233

162.159.135.232

162.159.137.232

162.159.138.232

193.106.191.141

3.232.242.170

52.20.78.240

216.45.55.30

209.76.253.84

212.192.241.230

107.189.10.143

10.133.78.41

37.44.253.21

128.31.0.39

217.79.43.148

45.86.162.34

域名

wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd[.]onion

gunyhng6pabzcurl7ipx2pbmjxpvqnu6mxf2h3vdeenam34inj4ndryd[.]onion

Cuba-supp[.]com

Encryption-support[.]com

Mail.supports24[.]net

网址

http://80.66.75.28/aa-Fqsertugh[.]png

http://193.106.191.141/QWEwqdsvsf/ap[.]php