国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 12 期（总第 20 期）　　3 月 19 日-3 月 25 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

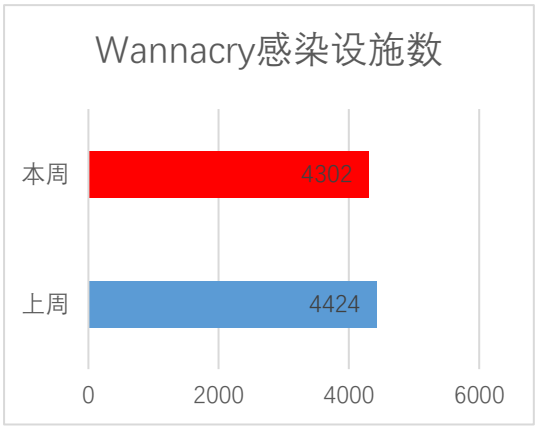
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1366567 个，监测发现勒索软件网络传播 4463 次，勒索软件下载 IP 地址 336 个，其中，位于境内的勒索软件下载地址 151 个，占比 44.9%，位于境外的勒索软件下载地址 185 个，占比 55.1%。

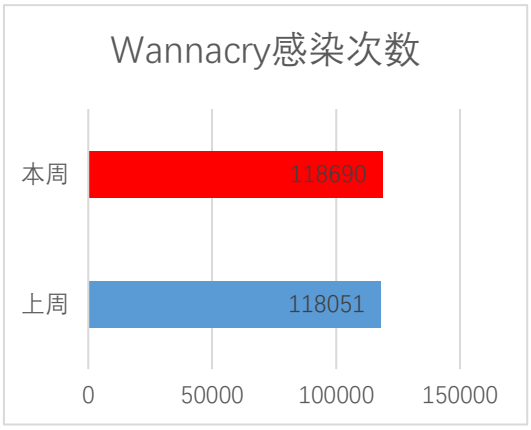
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

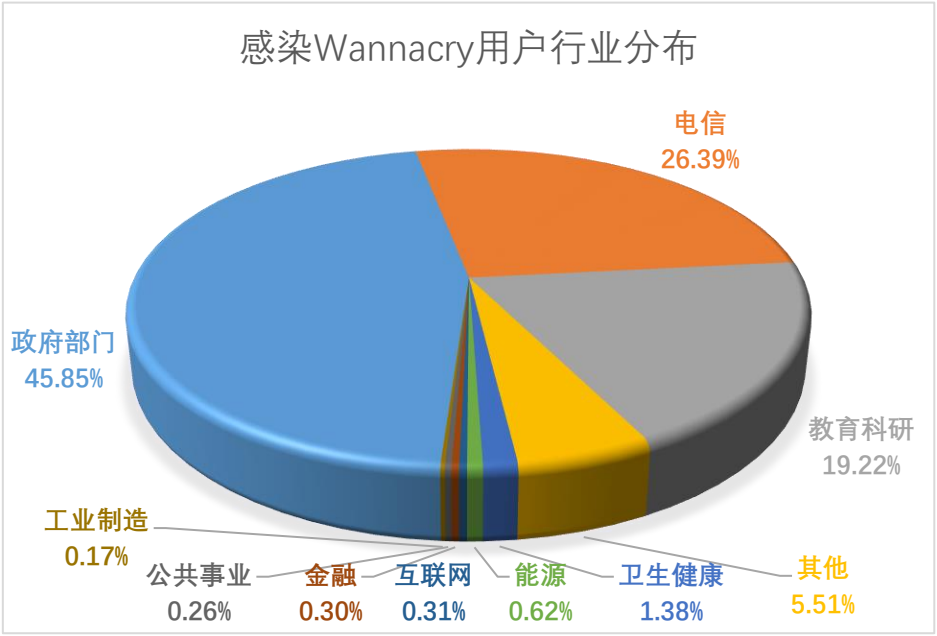
本周，监测发现 4302 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 2.8%，累计感染 118690 次，较上周上升 0.5%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



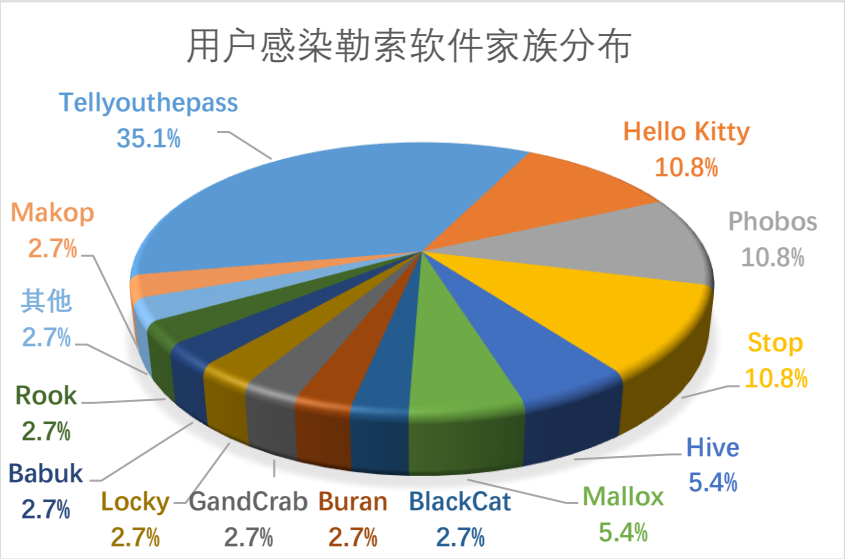


政府部门、电信、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

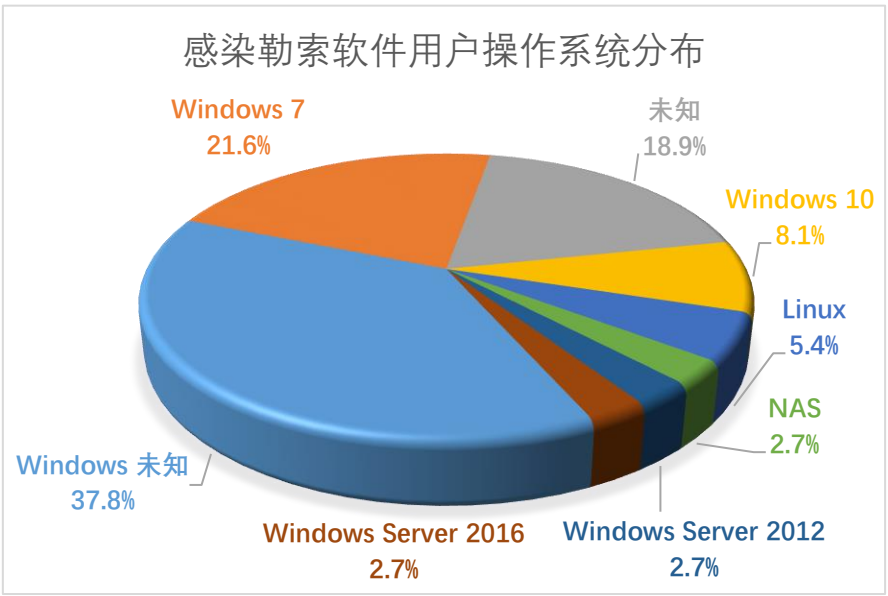


（二）其它勒索软件感染情况

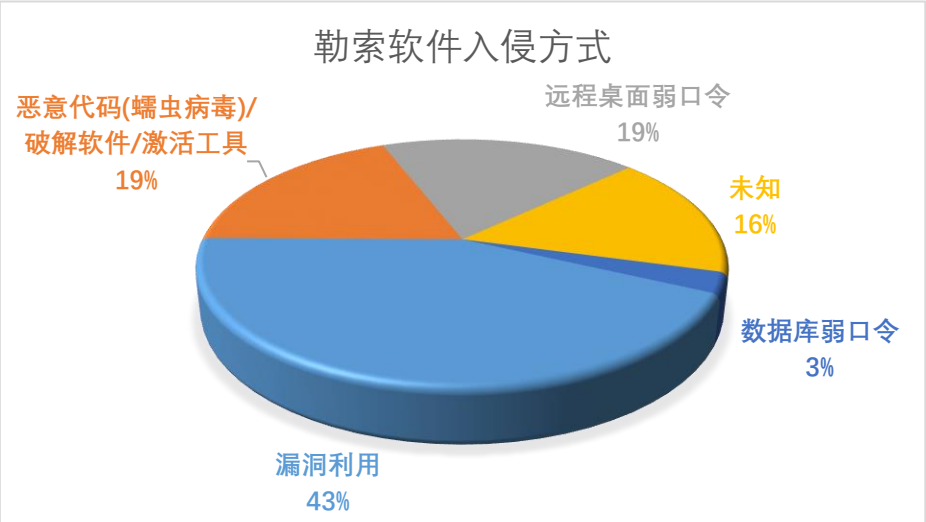
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 37 起，非 Wannacry 勒索软件感染事件，较上周上升 19.4%，排在前三名的勒索软件家族分别为 Tellyouthepass（35.1%）、Hello Kitty（10.8%）和 Phobos（10.8%）。



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 21.6%，其次为 Windows 10 系统和 Linux 系统，占比分别为 8.1%和 5.4%，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 43%和 19%。Log4j 漏洞的出现，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、希腊邮政公司 ELTA 遭到勒索软件攻击服务中断

希腊国有邮政服务提供商 ELTA 披露了周日检测到的一起勒索软件事件，该事件仍使该组织的大部分服务处于中断状态。根据最新的消息，网络攻击的最终目标是对 ELTA 公司业务运营的关键系统进行加密。该组织没有提到任何关于赎金的要求。目前，ELTA 不能提供邮件、账单支付或处理任何形式的金融交易订单的服务。该组织没有估计这些服务何时会再次提供。

四、威胁情报

IP

118.33.109.122

1.248.122.240

104.18.30.182

109.102.255.230

175.120.254.9

175.126.109.15

网址

http://ccc0ac1890ec7gqbhbyjyc.bothadd[.]uno/gqbhbyjyc

http://ccc0ac1890ec7gqbhbyjyc.sitesif[.]sbs/gqbhbyjyc

http://ccc0ac1890ec7gqbhbyjyc.isworth[.]space/gqbhbyjyc

http://ccc0ac1890ec7gqbhbyjyc.leddays[.]quest/gqbhbyjyc

http://ccc0ac1890ec7gqbhbyjyc.ua364popk6btkojuj6wzngq2rele7afowr3f35hufih6gid

t4gd44sad[.]onion/gqbhbyjyc

http://aa4cf0e8a0a832709814ee588xlycoihfk.wartell[.]quest/xlycoihfk

http://aa4cf0e8a0a832709814ee588xlycoihfk.tillpop[.]uno/xlycoihfk

http://aa4cf0e8a0a832709814ee588xlycoihfk.enddare[.]fit/xlycoihfk

http://aa4cf0e8a0a832709814ee588xlycoihfk.soknew[.]space/xlycoihfk

邮箱

rikyrank113@protonmail.com

jokers777@tutanota.com

antistress.ir@yandex.ru

anticrypto@tutanota.com

crypt22@aol.com

rikyrank113@protonmail.com