国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 4 期（总第 12 期）　　1 月 22 日-1 月 28 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

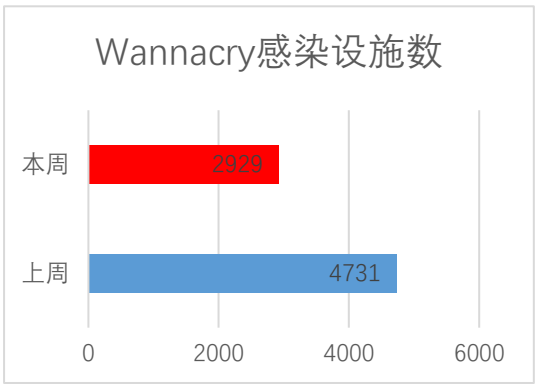
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1324822 个，监测发现勒索软件网络传播 603 次，勒索软件下载 IP 地址 21 个，其中，位于境内的勒索软件下载地址 13 个，占比 61.9%，位于境外的勒索软件下载地址 8 个，占比 38.1%。

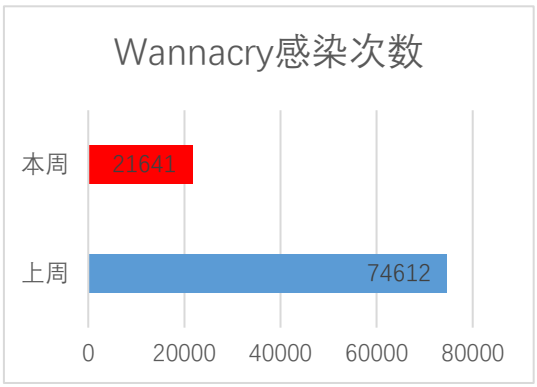
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

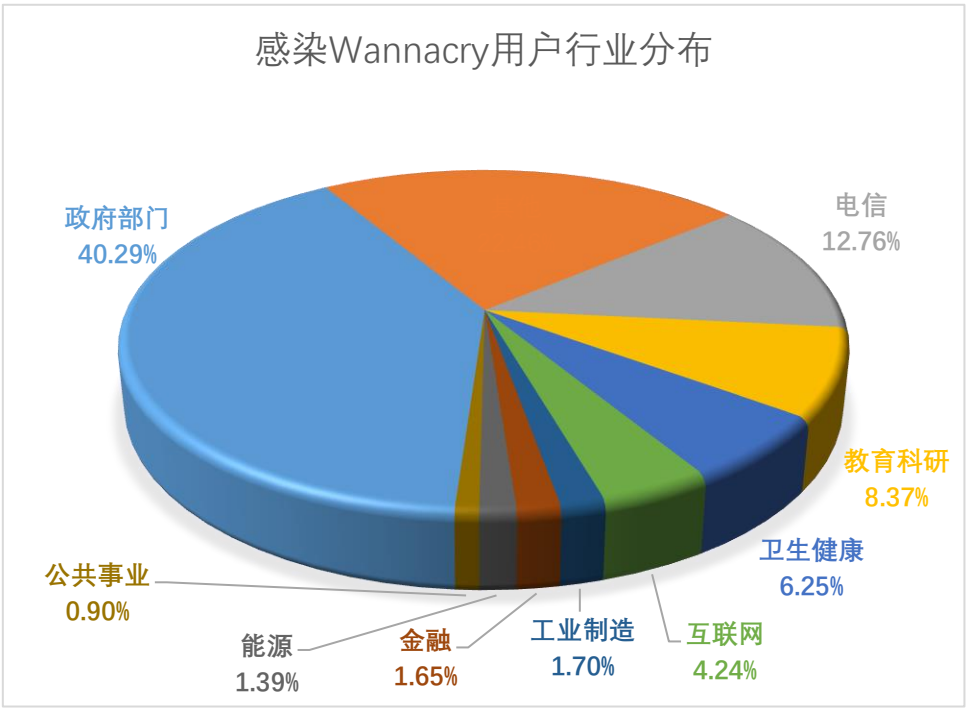
本周，监测发现 2929 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 38.1%，累计感染 21641 次，较上周下降 71%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



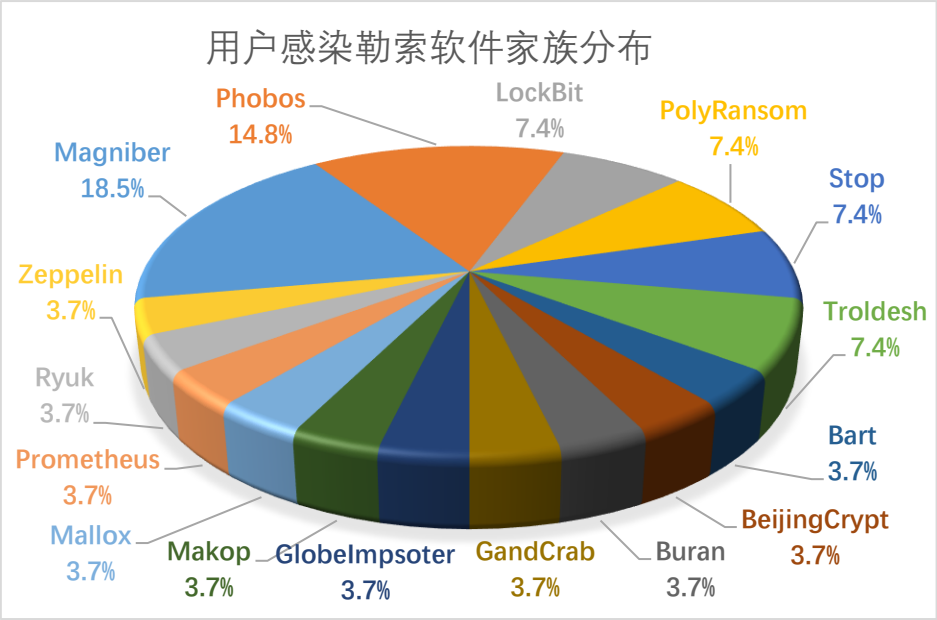


政府部门、电信、教育科研、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

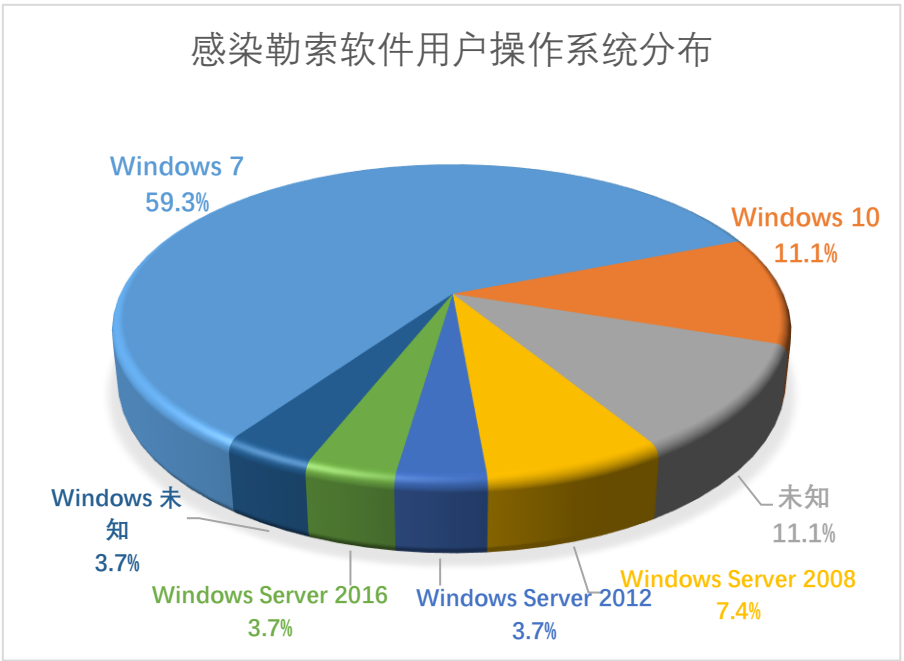


（二）其它勒索软件感染情况

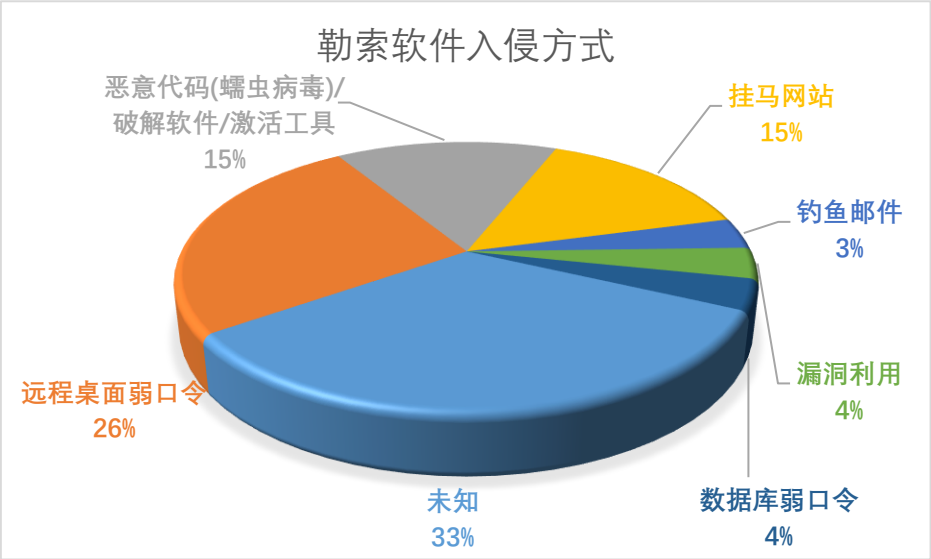
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 27 起非 Wannacry 勒索软件感染事件，较上周下降 28.9%，排在前三名的勒索软件家族分别为 Magniber（18.5%）、Phobos（14.8%）和 LockBit（7.4%）。



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 59.3%，其次为 Windows 10 系统，占比为 11.1%，除此之外还包括多个其它不同版本的 Windows 桌面版本和服务器版本系统。



本周，勒索软件入侵方式中，远程桌面弱口令排在第一位，其次为恶意代码（蠕虫病毒）/破解软件/激活工具和挂马网站。Phobos 勒索软件利用弱口令漏洞特别是远程桌面弱口令频繁攻击我国用户，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

本周，工作组成员单位在自助监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、LockBit 勒索软件最新变种攻击 VMware ESXi 服务器

LockBit 勒索软件一度是最活跃的勒索软件家族，被认为主要针对 Windows 系统。然而，近期有安全人员发现了 LockBit Linux-ESXi Locker 版本，其拥有额外的 VMware ESXi 变体。与其他勒索软件类似，LockBit 采用“双重勒索”模式，即同时加密数据和威胁公开敏感数据从而索取赎金，其赎金高达数百万美元。研究人员认为，LockBit 的 VMware ESXi 变体使得勒索软件可能会进一步传播，加密更广泛的服务器文件，建议服务器所有者或管理员及时安装最新安全补丁，配置口令复杂度策略，关闭不必要的服务。

四、威胁情报

域名

104-168-132-128.nip[.]io

IP

176.123.8.228

网址

http://14cc4e4090e0325024a8a200be6c48gwkgiokp.gunfail[.]quest/gwkgiokp

http://14cc4e4090e0325024a8a200be6c48gwkgiokp.ranmuch[.]space/gwkgiokp

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.gaplies[.]fit/kqqqefjv

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.raredoe[.]uno/kqqqefjv

http://be843c00ba84fc00e6d0e210ec50c470myjitis.gunfail[.]quest/myjitis

http://be843c00ba84fc00e6d0e210ec50c470myjitis.ranmuch[.]space/myjitis

http://ca9cc6a04268dc10b0e0a2a004fc32e0msvgsup.gunfail[.]quest/msvgsup

http://ca9cc6a04268dc10b0e0a2a004fc32e0msvgsup.ranmuch[.]space/msvgsup

http://d848c0c0dc1404205850ac48e6184c00fteherut.gaplies[.]fit/fteherut

http://d848c0c0dc1404205850ac48e6184c00fteherut.raredoe[.]uno/fteherut

邮箱

360helper@mailfence.com

6lilium6@protonmail.com

anony.alex22@gmail.com

decypt20@firemaill.cc

ghxyz@fonix.email

recovery2020@cock.li

tsuppor@privatemail.com