国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 5 期（总第 13 期）　　1 月 29 日-2 月 4 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

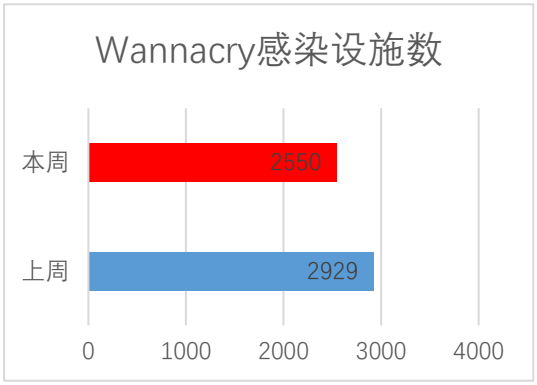
本周勒索软件防范应对工作组共收集捕获勒索软件样本 625906 个，监测发现勒索软件网络传播 1021 次，勒索软件下载 IP 地址 41 个，其中，位于境内的勒索软件下载地址 23 个，占比 56.1%，位于境外的勒索软件下载地址 18 个，占比 43.9%。

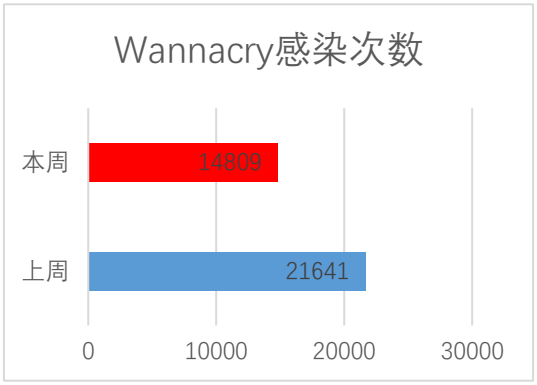
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

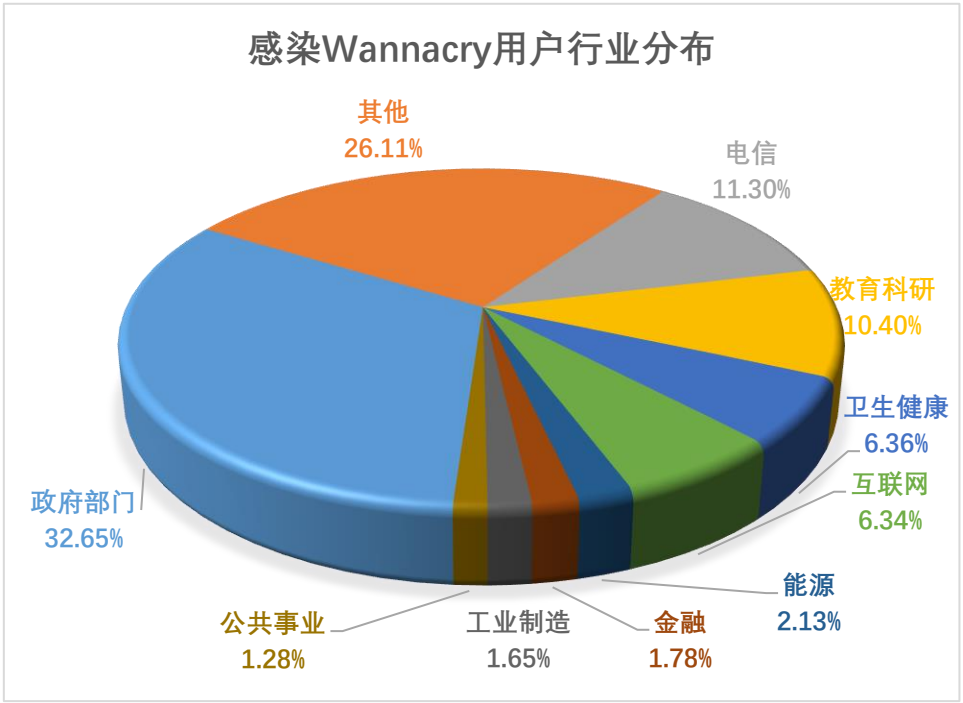
本周，监测发现 2550 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 12.9%，累计感染 14809 次，较上周下降 31.6%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



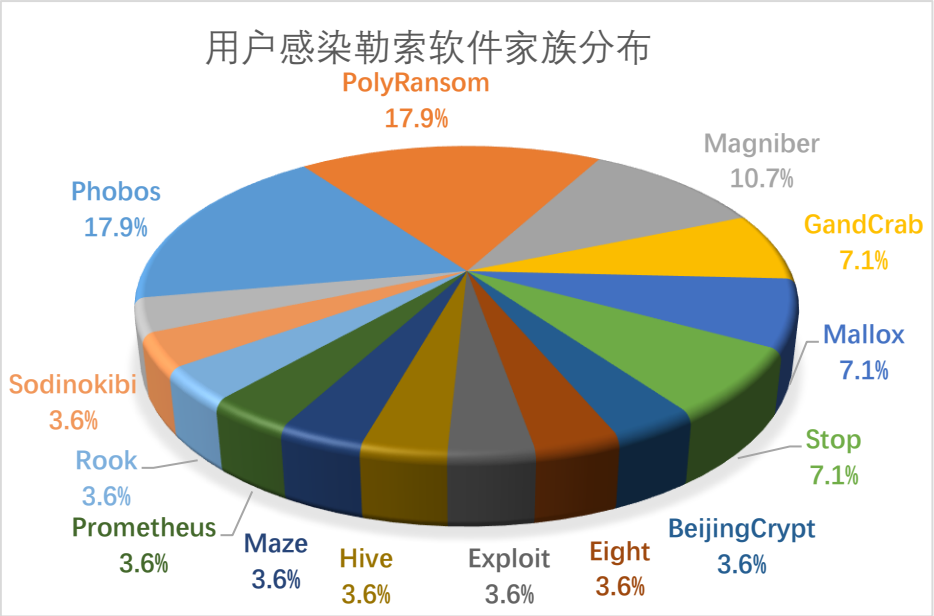


政府部门、电信、教育科研、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

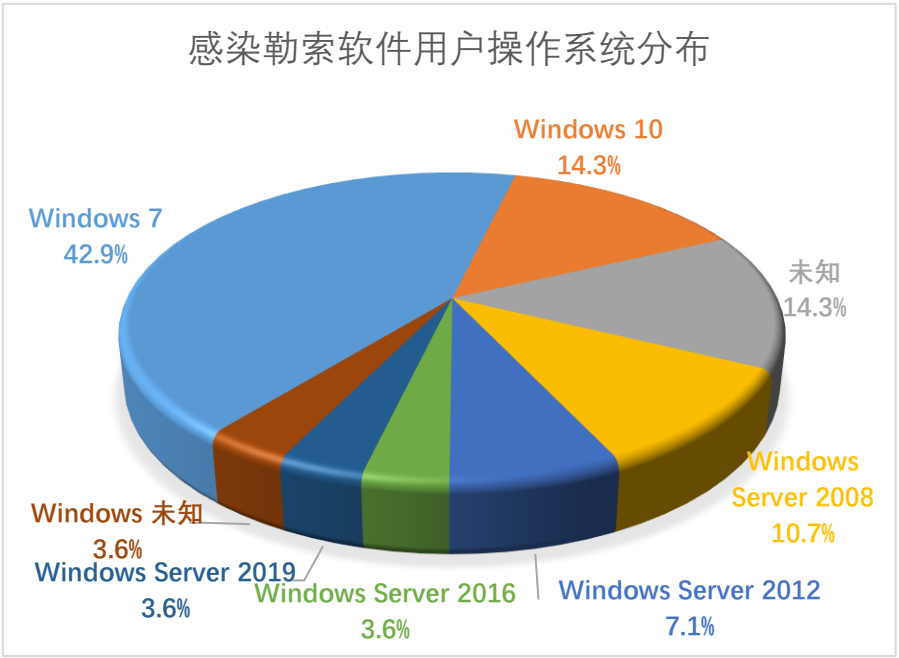


（二）其它勒索软件感染情况

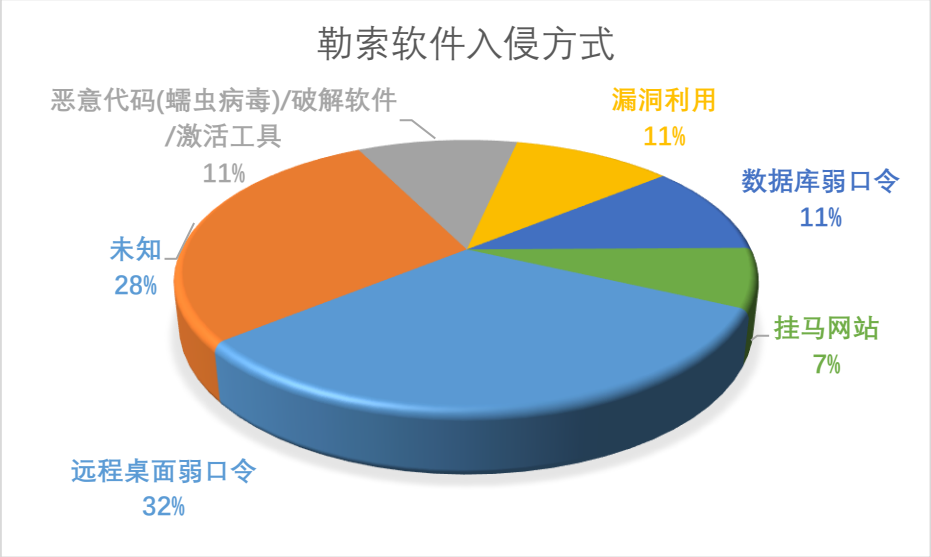
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 28 起非 Wannacry 勒索软件感染事件，较上周上升 3.7%，排在前三名的勒索软件家族分别为 Phobos（17.9%）、PolyRansom（17.9%）和 Magniber（10.7%）。



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 42.9%，其次为 Windows 10 系统，占比为 14.3%，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/激活工具和漏洞利用。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

1、河北某医院多台云服务器感染 BeijingCrypt 勒索软件

本周，工作组成员应急响应了河北某医院多台云服务器感染 BeijingCryp 勒索软件。攻击者通过一台向互联网开放的数据库弱口令获得服务器控制权，进而植入勒索软件，随后攻击者进行内网渗透，在医院内网中进一步传播勒索病毒，共导致该医院 8 台云服务器数据被勒索软件加密。

此事件中，攻击者利用数据库弱口令获得服务器控制权后植入勒索软件。建议用户配置口令复杂度策略、修改弱口令、关闭不必要的服务。

（二） 国外部分

1、零食生产商 KP Snacks 遭受 Conti 勒索软件攻击

英国知名的零食生产商 KP Snacks 近日遭受 Conti 勒索病毒攻击，其向大型超市的供货计划已被推迟或完全取消，造成的影响可能

会持续到 3 月。据报道，该公司的内部网络已被入侵，威胁者可以访问和加密敏感文件，包括员工记录和财务数据等。此外，Conti 团伙发布了该公司员工的信用卡对账单、出生证明、员工地址、电话号码和其他敏感文件的示例文件。

四、威胁情报

域名

sugarpanel[.]space

IP

222.186.43.199

179.43.160.195

网址

http://44e48480feb0rivbuxpxc.handfry[.]site/rivbuxpxc

http://44e48480feb0rivbuxpxc.lowlegs[.]space/rivbuxpxc

http://44e48480feb0rivbuxpxc.numbhis[.]top/rivbuxpxc

http://44e48480feb0rivbuxpxc.warnwe[.]xyz/rivbuxpxc

http://cdn2546713.cdnmegafiles[.]com/data23072021_1.dat

http://f2d0c210a62830706eb8b638ekkkkxqz.dayeven[.]space/kkkkxqz

http://f2d0c210a62830706eb8b638ekkkkxqz.forrain[.]fit/kkkkxqz

http://f2d0c210a62830706eb8b638ekkkkxqz.luckymy[.]quest/kkkkxqz

http://f2d0c210a62830706eb8b638ekkkkxqz.mensell[.]uno/kkkkxqz

http://f8fcac88fef810108eacd420e4a856e0lblwdugpw.handfry[.]site/lblwdugpw

http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd[.]onion/

邮箱

dec0ding@tutanota.com

raincry@dr.com

robud@ctemplar.com

robud@outlookpro.net

writeme@onionmail.org

xena@airmail.cc

钱包地址

18UCkpCFZd9do9ECoAJWckevxCJF3cGCQn

13W5c6dS37jCfDHLVJxQj2HujQRsM11SAt

19pqj9SeBTVmoo5NNxhWeBKV7uCiAgwxy8