国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 18 期（总第 26 期）　　4 月 30 日-5 月 6 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

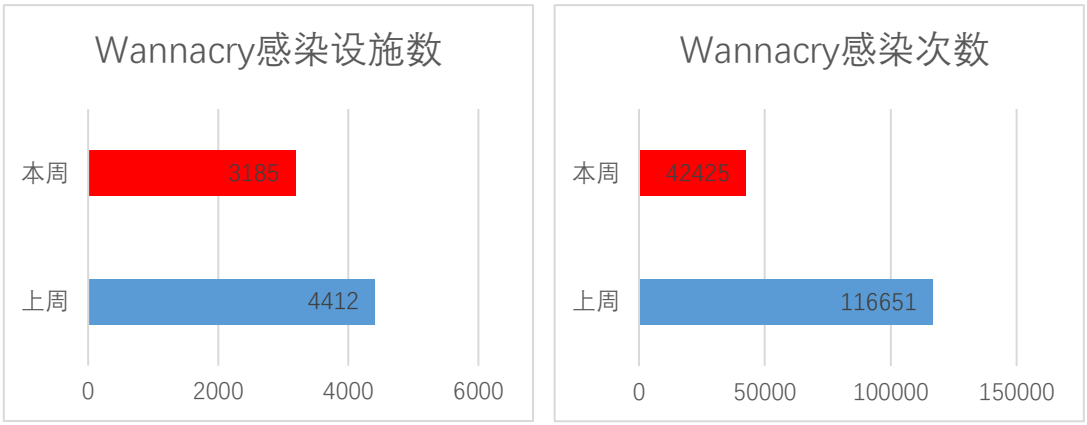
本周勒索软件防范应对工作组共收集捕获勒索软件样本 780124 个，监测发现勒索软件网络传播 64 次，勒索软件下载 IP 地址 17 个，其中，位于境内的勒索软件下载地址 10 个，占比 58.8%，位于境外的勒索软件下载地址 7 个，占比 41.2%。

二、勒索软件受害者情况

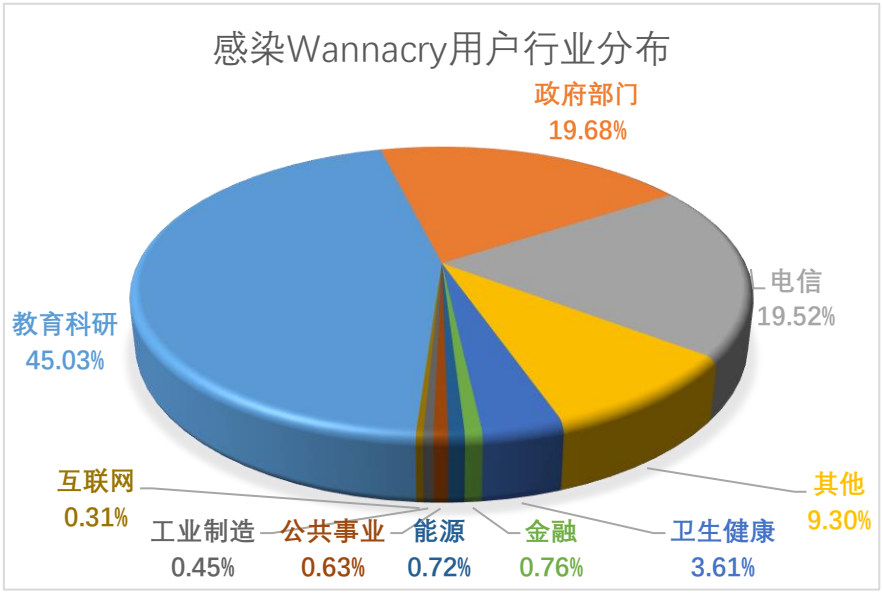
（一）Wannacry 勒索软件感染情况

本周，监测发现 3185 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 27.8%，累计感染 42425 次，较上周下降 63.6%。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。

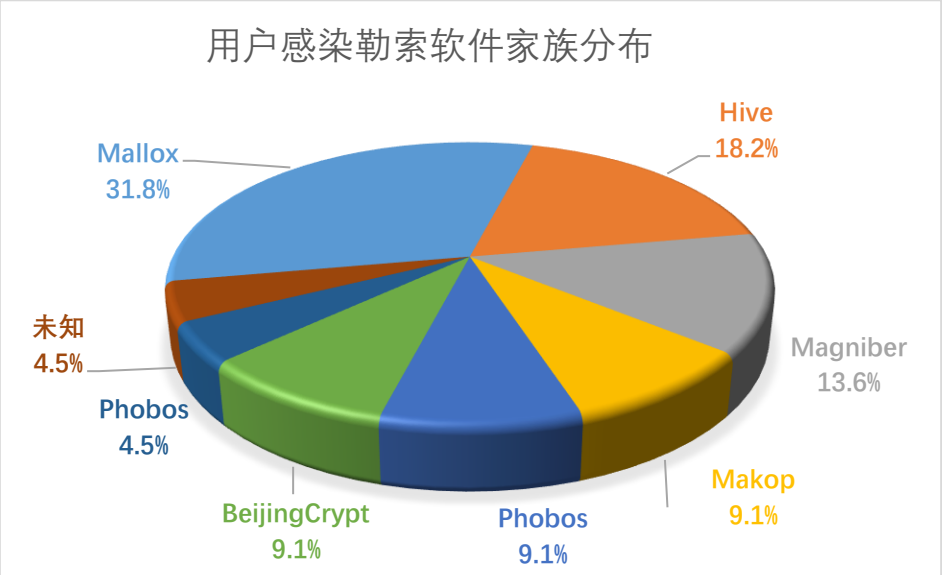


教育科研、政府部门、电信、卫生健康、金融行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

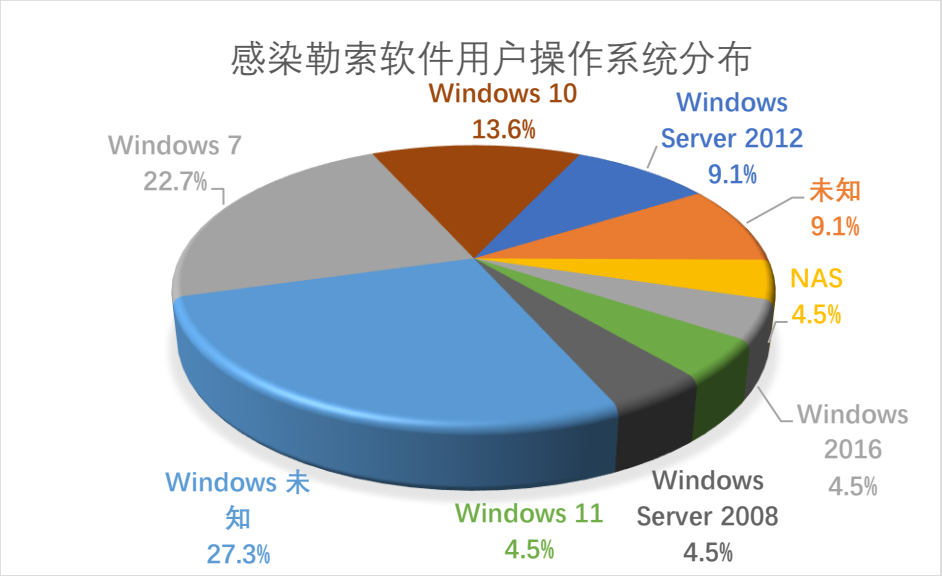


（二）其它勒索软件感染情况

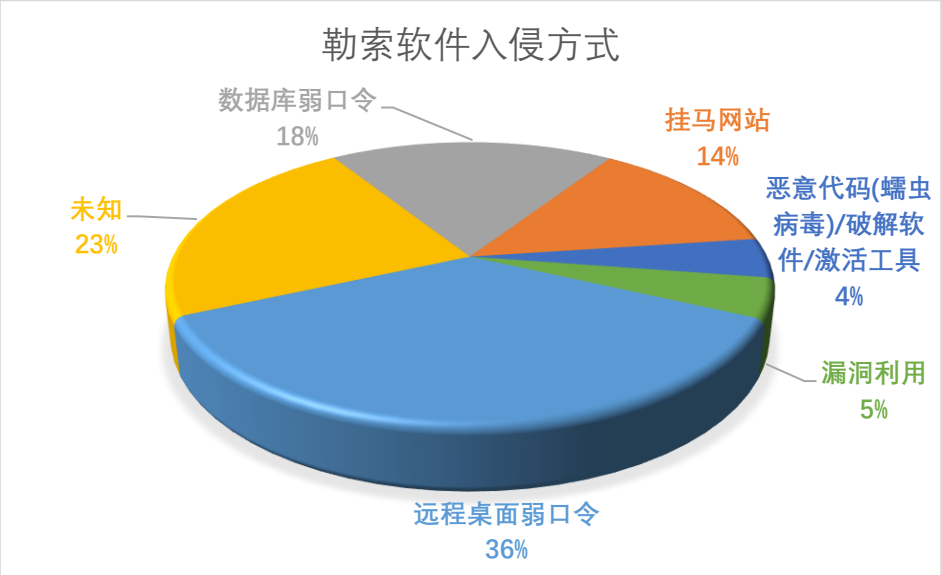
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 22 起非 Wannacry 勒索软件感染事件，较上周下降 12.0%，排在前三名的勒索软件家族分别为 Mallox（31.8%）、Hive（18.2%）和 Magniber（13.6%）。



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 22.7%，其次为 Windows 10 系统和 Windows Server 2012 系统，占比分别为 13.6%和 9.1%，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 36%和 18%。Mallox 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. 某医院遭 Phobos 勒索病毒攻击

本周，工作组成员应急响应了某医院前置机遭 Phobos 勒索病毒攻击事件。此次勒索软件变种使用“RSA+AES”加密算法对文件进行加密，根据勒索信息与文件后缀名初步确定为 Phobos 家族勒索病毒。通过分析发现前置机对外开放了 3389 端口，攻击者通过暴力破解的方式成功登录服务器，并投放 Phobos 家族勒索病毒，病毒母体伪装成 cmd.exe 恶意文件，双击触发即会将服务器文件加密。

Phobos 家族的勒索病毒一直在国内保持一定的活跃程度，为避免遭受勒索软件攻击，建议企业和用户关闭不必要的端口，使用强口令，且避免多台设备使用同样的口令，同时对于业务上无需使用 RDP 的，建议关闭 RDP。

（二） 国外部分

1. 美国凯洛格社区学院遭到勒索软件攻击暂停授课

美国密歇根州的凯洛格社区学院遭到网络攻击后关闭了校园并取消了课程，该学院上周五成为勒索软件的目标。在周日发布在其网站上的一份声明中，该学院宣布取消所有周一的课程，并关闭其位于巴特尔克里克、阿尔比恩、科尔德沃特和黑斯廷斯的五个校区。该学院表示，在调查安全事件期间，其校园将保持关闭，还将对所有学生、教职员工实施“强制密码重置”，以改善其网络安全。

四、威胁情报

域名

7oukjxwkbnwyg7cekudzp66okrchbuubde2j3h6fkpis6izywoj2eqad[.]onion

fyk4jl7jk6viteakzzrxntgzecnz4v6wxaefmbmtmcnscsl3tnwix6yd[.]onion

IP

109.98.58.98

116.121.62.237

172.64.155.188

175.126.109.15

195.158.3.162

203.228.9.102

104.200.23.95

网址

http://046cd64896849410dc9dkkhcuqo.oddpoll[.]info/dkkhcuqo

http://046cd64896849410dc9dkkhcuqo.gravehe[.]info/dkkhcuqo

http://046cd64896849410dc9dkkhcuqo.onlylot[.]info/dkkhcuqo

http://046cd64896849410dc9dkkhcuqo.tinper[.]info/dkkhcuqo

http://046cd64896849410dc9dkkhcuqo.mjrdx5u4vripjuw7rha2oyjguf6vwtbttkn4srof3kwuezgquez6y5yd[.]onion/dkkhcuqo

http://26f4d6e8546048c0fed4e628a4e428pvtcbqm.onlylot[.]info/pvtcbqm

http://26f4d6e8546048c0fed4e628a4e428pvtcbqm.oddpoll[.]info/pvtcbqm

http://26f4d6e8546048c0fed4e628a4e428pvtcbqm.tinper[.]info/pvtcbqm

http://26f4d6e8546048c0fed4e628a4e428pvtcbqm.gravehe[.]info/pvtcbqm

http://26f4d6e8546048c0fed4e628a4e428pvtcbqm.mjrdx5u4vripjuw7rha2oyjguf6vwt

bttkn4srof3kwuezgquez6y5yd[.]onion/pvtcbqm

邮箱

martin1993douglas@pressmail.ch

mallox@stealthypost.net

paid-files@email.tg

avastdata@privatemail.com

filerecoveryassistant@privatemail.com

peekaboom@tuta.io

avastdata@airmail.cc

avastdata@privatemail.com

blackcatcc@airmail.cc