国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 17 期（总第 25 期）　　4 月 23 日-4 月 29 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

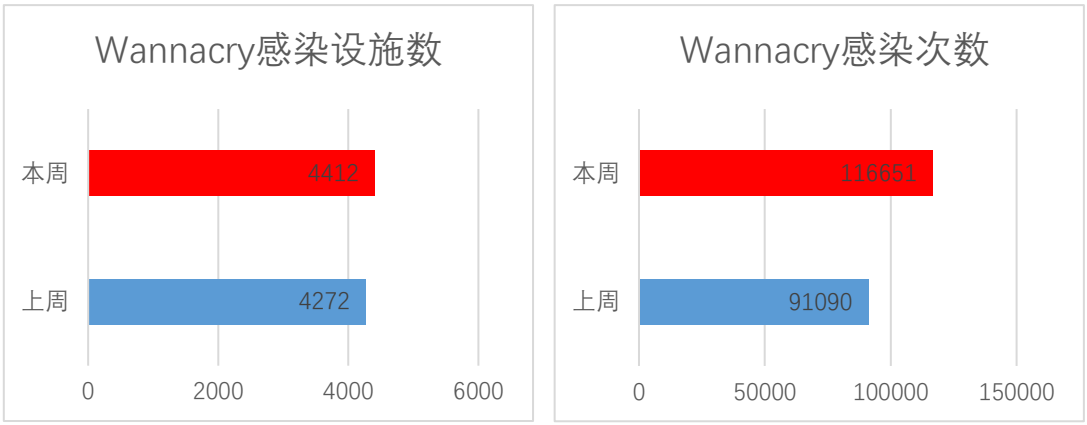
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1312903 个，监测发现勒索软件网络传播 4681 次，勒索软件下载 IP 地址 38 个，其中，位于境内的勒索软件下载地址 20 个，占比 52.63%，位于境外的勒索软件下载地址 18 个，占比 47.37%。

二、勒索软件受害者情况

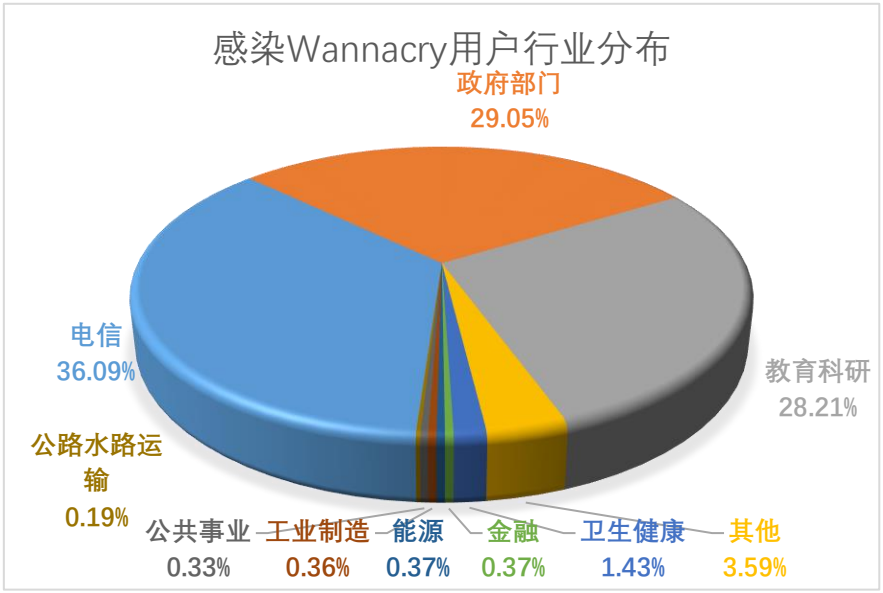
（一）Wannacry 勒索软件感染情况

本周，监测发现 4412 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 3.3%，累计感染 116651 次，较上周上升 28.1%。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。

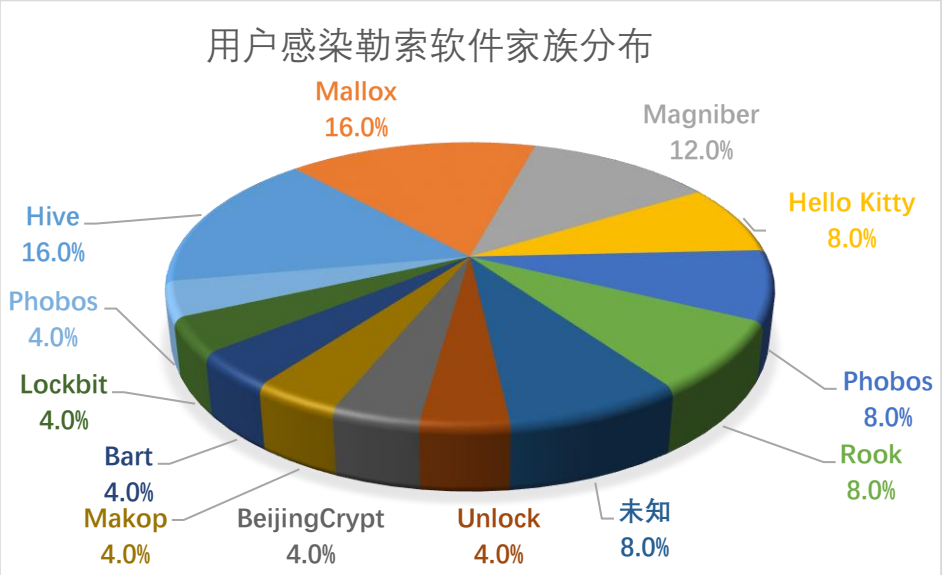


电信、政府部门、教育科研、卫生健康、金融行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

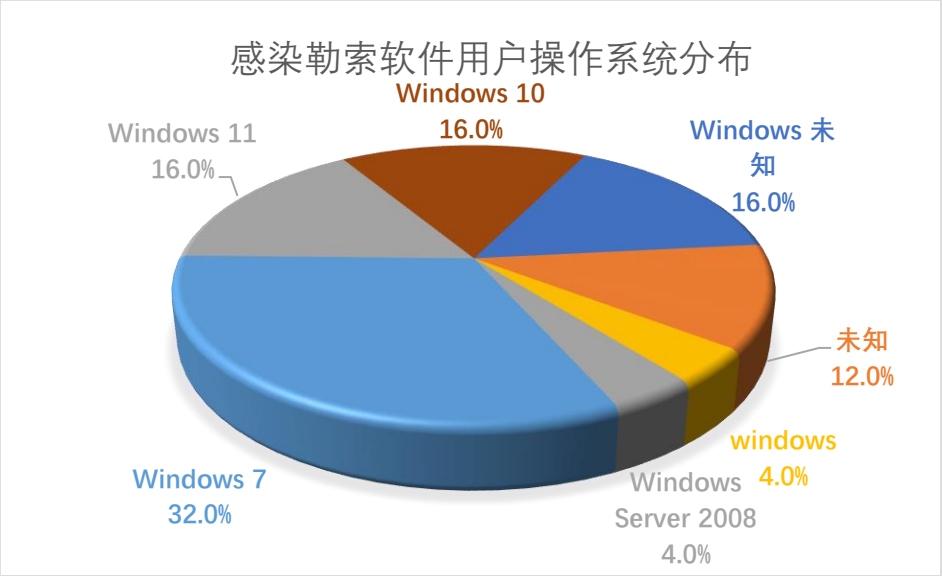


（二）其它勒索软件感染情况

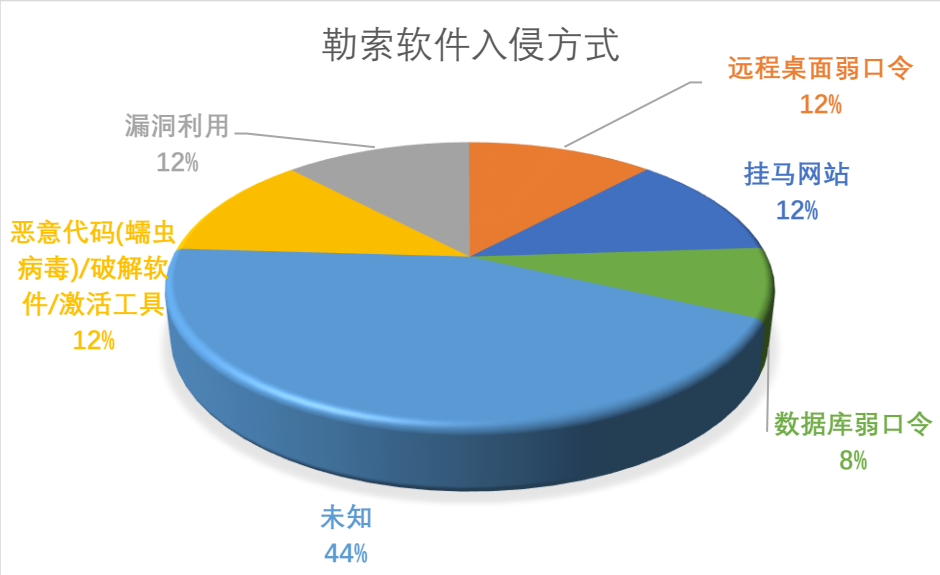
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 25 起非 Wannacry 勒索软件感染事件，较上周增长 8.7%，排在前三名的勒索软件家族分别为 Hive（16.0%）、Mallox（16.0%）和 Magniber（12.0%）。



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 32.0%，其次为 Windows 11 系统和 Windows 10 系统，占比分别为 16.0%和 16.0%，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，恶意代码(蠕虫病毒)/破解软件/激活工具和漏洞利用占比较高，分别为 12%和 12%。Mallox 勒索软件通过漏洞利用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. 浙江某企业遭 Phobos 勒索病毒攻击

本周，工作组成员应急响应了浙江某企业遭受 Phobos 勒索病毒攻击事件。通过阿里云控制台发现，荷兰的某 vps 于 4 月 19 日晚使用远程登录连接上了该公司服务器，随后运行勒索病毒脚本，该勒索病毒家族为 Phobos。在排查阶段，勒索病毒样本已经被删除。后经工作人员排查，发现该服务器开放了大量端口，包括大量的 Web 应用、数据库、以及存在漏洞的服务等。

近期，Phobos 家族勒索病毒在国内较为活跃，对我国的企业和个人用户造成巨大网络安全威胁，企业和用户应加强对服务器或个人设备的安全保护，定期进行安全扫描，及时排查安全隐患。

2. 上海某企业遭勒索病毒攻击

本周，工作组成员应急响应了上海某企业遭受勒索软件攻击事件。攻击者利用 Web 漏洞或弱口令漏洞进入该企业一台服务器主机，并

对内网进行扫描。随后在服务器上安装了 AnyDesk 软件，并通过远程桌面登录成功登录该公司另一服务器，横向获取到权限。之后利用黑客工具进行攻击，并运行勒索加密程序。

目前，弱口令仍是勒索病毒入侵的主要途径之一。为避免遭受勒索病毒的攻击，从而给企业和个人造成损失，应进行定期的服务器、网络设备的操作系统和中间件的漏洞扫描。还应进行定期的基线核查工作，重点在于弱口令账号、密码有效期等方面。

（二） 国外部分

1. 美国牙科协会受到 Black Basta 勒索病毒攻击

4 月 22 日，美国牙科协会（ADA）遭受了网络攻击，迫使被攻击的服务器下线。此次攻击严重干扰了其各种在线服务、电话、电子邮件和网络通信等功能。ADA 网站目前仅显示一条公式，表明他们的网站正在努力恢复系统运行。

目前，一个名为 Black Basta 的新型勒索病毒团伙声称对此次攻击事件负责，并已经开始泄露据称是在 ADA 攻击期间窃取到的数据。该团伙的数据泄露网站声称已经泄露了大约 2.8 GB 的数据，同时其还指出这是攻击中被盗数据的 30%。这些数据包括 W2 表单、NDA、会计电子表格以及数据泄漏页面上共享的屏幕截图中有关 ADA 的会员信息。

四、威胁情报

域名

dilimoretast[.]com

antnosience[.]com

oceriesfornot[.]top

IP

138.68.42.130

157.245.142.66

188.166.154.118

185.203.118.227

138.68.42.130

157.245.142.66

188.166.154.118

185.203.118.227

网址

http://0208fa9836d0143044ccvnjmseu.wetanks[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.mostpen[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.illbite[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.icedeal[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.53e4qdmhprpevdrbfoxmniolnyhmk4g7fbh7x4v4a3nrie6qzjf24oid[.]onion/vnjmseu

ismina[.]info/src=324398

dalako[.]info/src=435787

http://0208fa9836d0143044ccvnjmseu.icedeal[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.mostpen[.]info/vnjmseu

http://0208fa9836d0143044ccvnjmseu.illbite[.]info/vnjmseu

邮箱

Starmoon@my.co

starmoonio@tutanota.com

deviceZz@mailfence.com

acookies@tutanota.com

acookies@onionmail.org

consult.raskey@tutanota.com

consult.raskey@onionmail.org

avos@thesecure.biz

avos@mail2tor.com

maxoll@tutanota.com

钱包地址

1M1tGFGcEB6EhtF1Z89JSH2ZT2g2asCbuH

18nqcaWdo35xFsk17LJPHuqsedyEYqtW2E