国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 11 期（总第 19 期）　　3 月 12 日-3 月 18 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

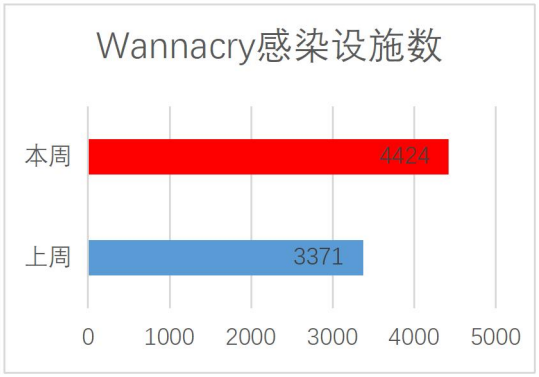
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1121725 个，监测发现勒索软件网络传播 1083 次，勒索软件下载 IP 地址 22 个，其中，位于境内的勒索软件下载地址 13 个，占比 59.1%，位于境外的勒索软件下载地址 9 个，占比 40.9%。

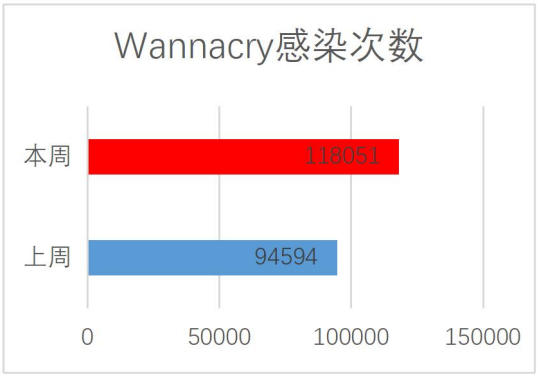
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

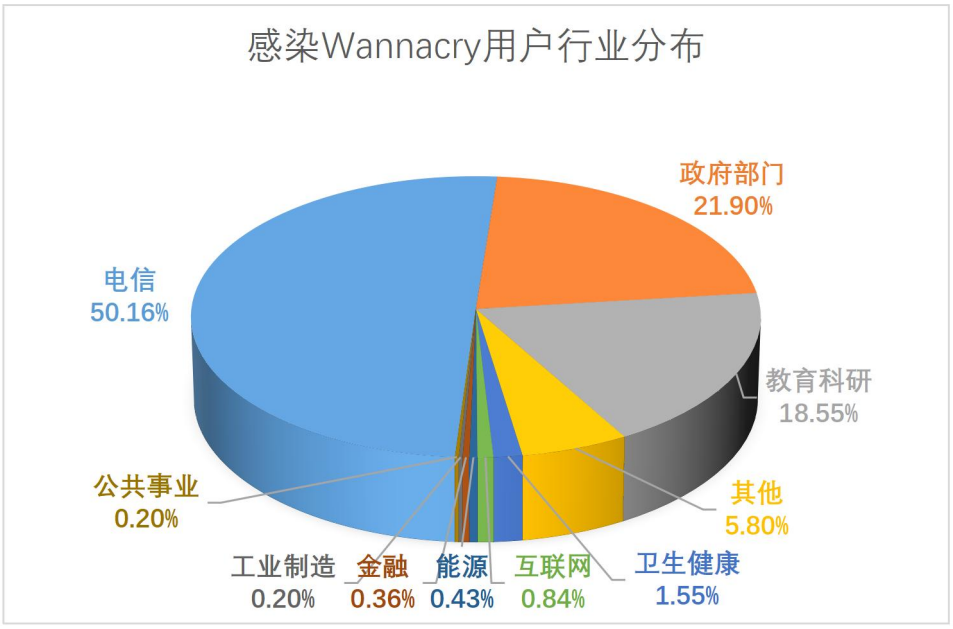
本周，监测发现 4424 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 31.2%，累计感染 118051 次，较上周上升 24.8%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机

没有针对常见高危漏洞进行合理加固的现象。



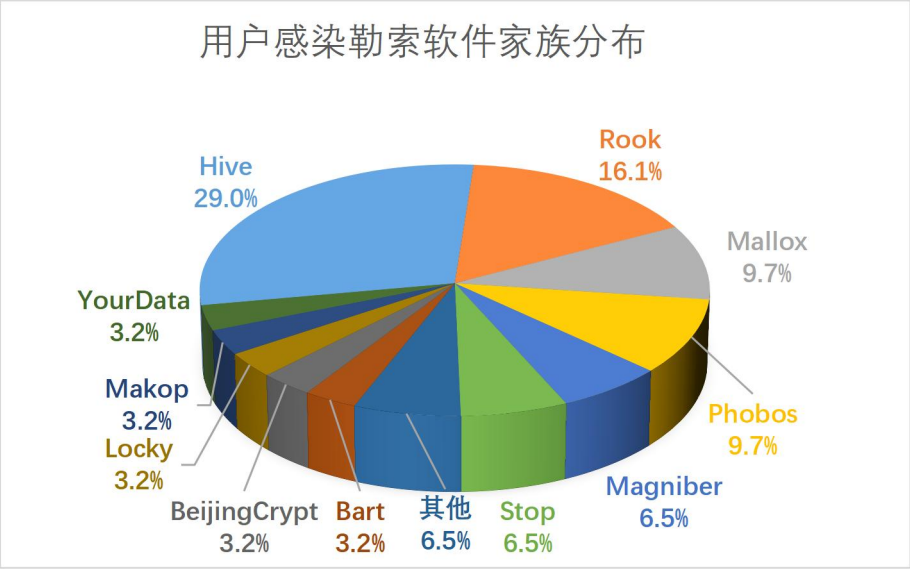


电信、政府部门、教育科研、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

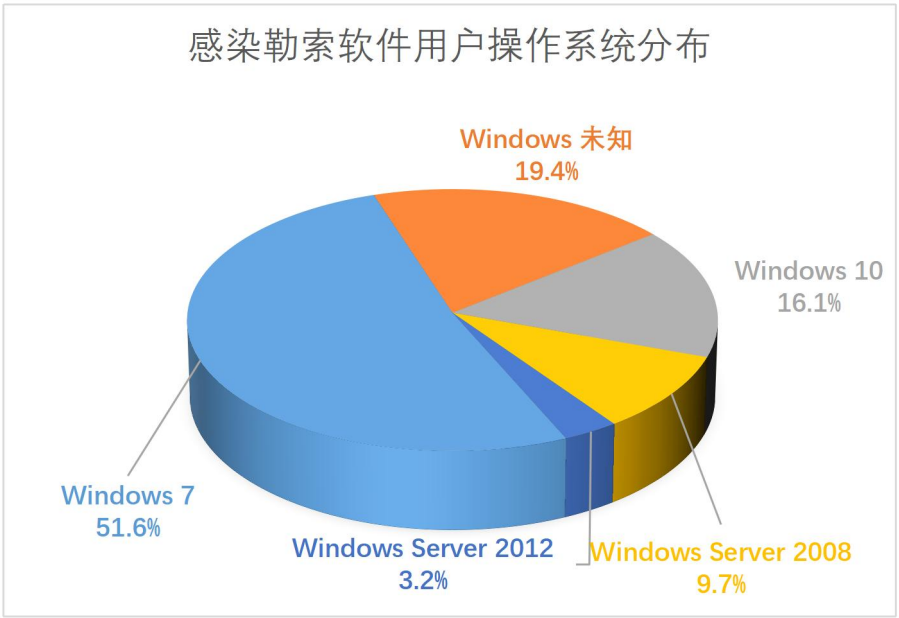


（二）其它勒索软件感染情况

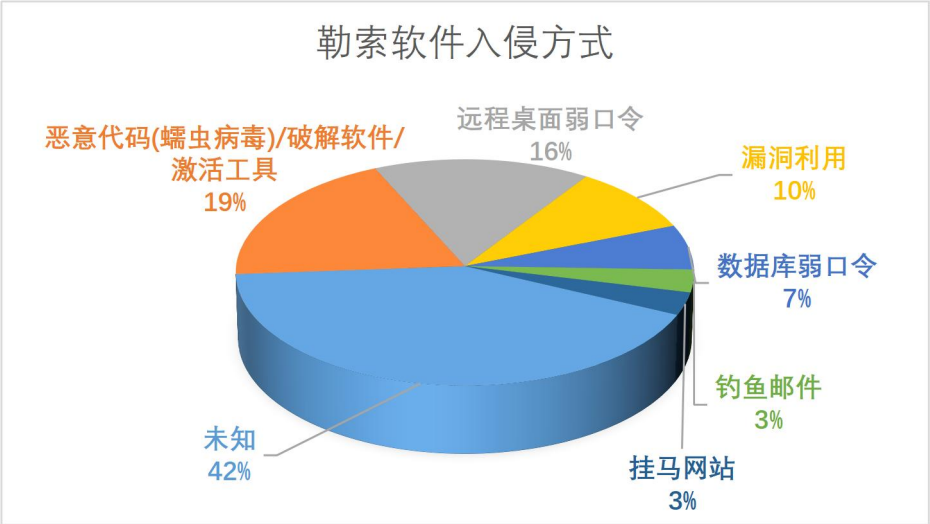
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 31 起非 Wannacry 勒索软件感染事件，较上周上升 138.5%，排在前三名的勒索软件家族分别为 Hive（29%）、Rook（16.1%）和 Mallox（9.7%）。



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 51.6%，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 16.1%和 9.7%，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/激活工具和远程桌面弱口令占比较高，分别为 19%和 16%。Rook 勒索软件利用恶意代码(蠕虫病毒)/破解软件/激活工具频繁攻击我国用户，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、广东某企业多台主机同时感染 Hive 和 Buran 勒索软件

本周，工作组成员应急响应了广东某企业多台主机同时感染 Hive 和 Buran 勒索软件事件。攻击者通过一台向互联网开放的服务器漏洞获得入侵的立足点，随后攻击了该企业的域控服务器，进而向逾 200 台主机植入勒索软件。本事件中，工作组成员同时发现 Hive 和 Buran 勒索软件样本，但目前尚未确认本次入侵为两个独立攻击团伙所为还是同一团伙的两次攻击活动。

近期利用软件安全漏洞来传播勒索软件从而实现成功入侵的案例越来越多，用户在日常工作和生活中应使用正版软件以及时获得安全补丁服务，定期检测系统漏洞并及时修复。

2、重庆某医院服务器感染 Phobos 勒索软件

本周，工作组成员应急响应了重庆某医院服务器感染 Phobos 勒索软件事件。攻击者通过一台向互联网开放远程桌面服务的服务器，利用弱口令漏洞获得服务器控制权，进而植入勒索软件。

此事件中，攻击者利用远程桌面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、全球最大的轮胎制造商之一普利司通遭受 LockBit 勒索攻击

近日，LockBit 勒索病毒团伙声称对全球最大的轮胎制造商之一普利司通美洲公司进行了勒索攻击。该团伙宣称他们将泄露从该公司窃取的所有数据，并启动了一个倒计时器。普利司通公司已确认该攻击事件并展开调查，但目前尚不清楚 LockBit 团伙从普利司通窃取了哪些数据。普利司通宣称其对于可能遭受数据泄露的影响正在评估中。

四、威胁情报

域名

loki-locker[.]one

vbfqeh5nugm6r2u2qvghsdxm3fotf5wbxb5ltv6vw77vus5frdpuaiid[.]onion

IP

194.226.139.3

91.223.82.6

网址

http://c0c892b8de7cqqvoqbbkn.amjblanypjy2tews4maivajjj7zhb4yxafhbqv7yqzej3bjq4n3h2nyd[.]onion/qqvoqbbkn

http://c0c892b8de7cqqvoqbbkn.billfun[.]uno/qqvoqbbkn

http://c0c892b8de7cqqvoqbbkn.knewpen[.]space/qqvoqbbkn

http://c0c892b8de7cqqvoqbbkn.rawloop[.]fit/qqvoqbbkn

http://c0c892b8de7cqqvoqbbkn.veryits[.]quest/qqvoqbbkn

邮箱

AcepyRansom@protonmail.com

contact@pandoraxyz.xyz

Decoder@firemail.cc

Decryptfiles@goat.siIn

emcryptsupport@msgsafe.io

recovery2021@onionmail.org

ust29@aol.com