国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 15 期（总第 23 期）　　4 月 9 日-4 月 15 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

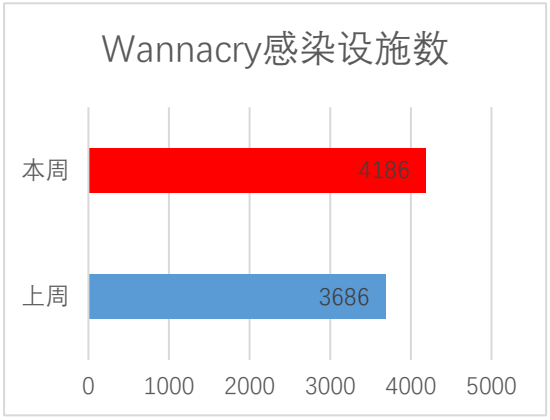
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1099087 个，监测发现勒索软件网络传播 959 次，勒索软件下载 IP 地址 29 个，其中，位于境内的勒索软件下载地址 14 个，占比 48.3%，位于境外的勒索软件下载地址 15 个，占比 51.7%。

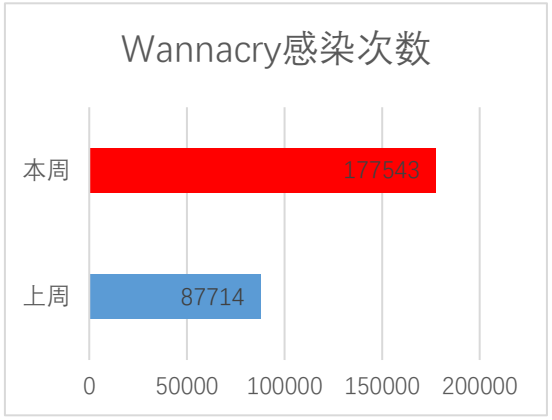
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

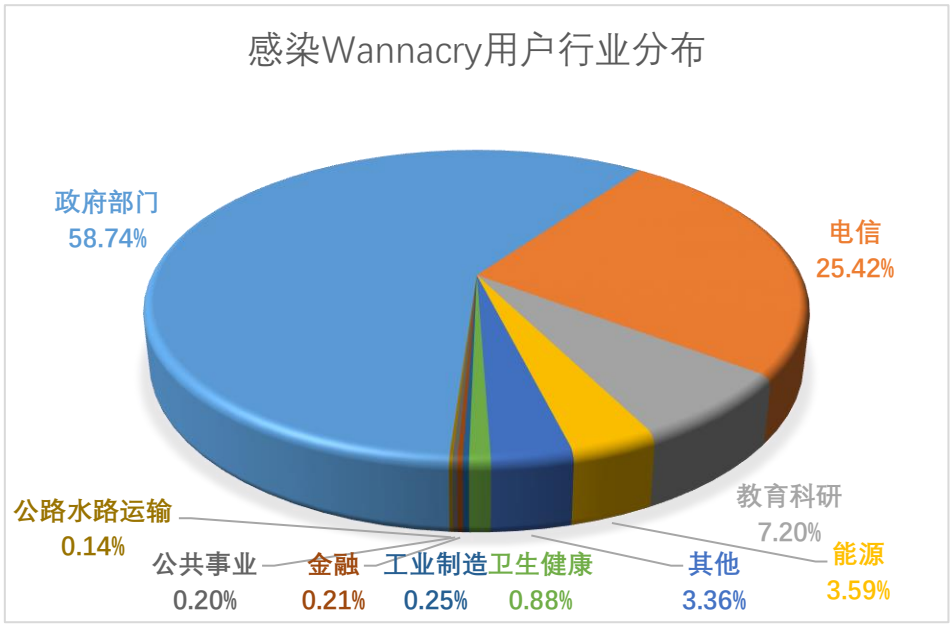
本周，监测发现 4186 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 13.6%，累计感染 177543 次，较上周下降 102.4%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机

没有针对常见高危漏洞进行合理加固的现象。





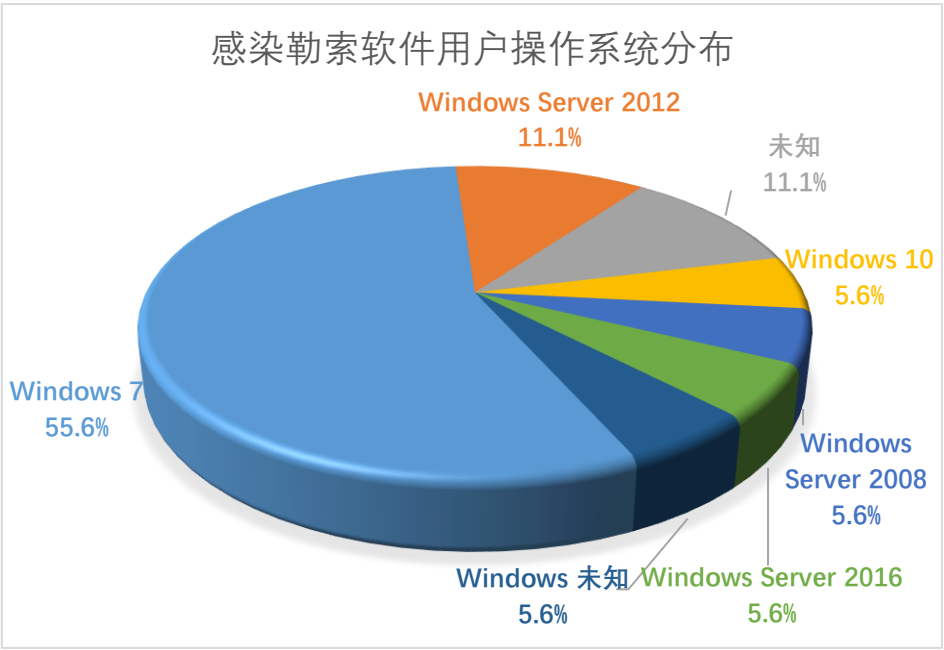
政府部门、电信、教育科研、能源、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。



（二）其它勒索软件感染情况

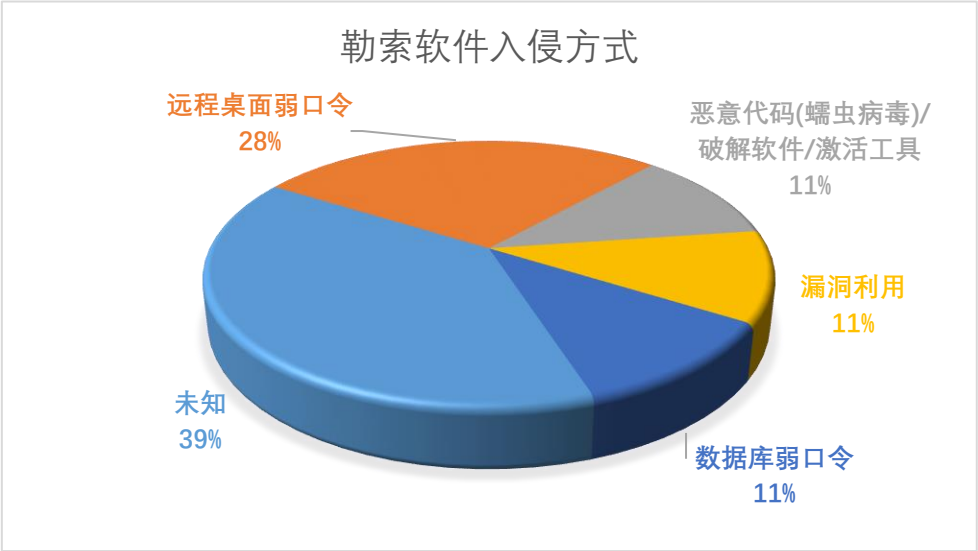
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 18 起，非 Wannacry 勒索软件感染事件，较上周上升 63.6%，排在前三名的勒索软件家族分别为 Hive（38.9%）、Makop（11.1%）和 Mallox（11.1%）。

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 55.6 %，其次为 Windows Server 2012 系统和 Windows 10 系统，占比分别为 11.1%和 5.6%，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，远程桌面弱口令和恶意代码(蠕虫病毒)/破解软件/激活工具占比较高，分别为 28%和 11%。Makop 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、贵州某单位服务器感染 Zeppelin 勒索软件

本周，工作组成员应急响应了贵州某单位服务器感染 Zeppelin 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、勒索团伙 NB65 利用 Conti 勒索软件攻击俄罗斯多个目标

近期，勒索团伙 NB65 使用 Conti 勒索软件变种攻击俄罗斯境内多个目标，包括俄罗斯国家电视广播公司（VGTRK）和俄罗斯航天局 Roscosmos 等机构。Conti 是一种提供勒索软件即服务（RaaS）的勒

索软件家族，核心团队负责管理恶意软件和 Tor 站点，NB65 团伙使用了 Conti 勒索软件家族的变体，被加密的文件名后附加了.nb65 扩展名。

四、威胁情报

域名

a3c65c[.]org

eccbc8[.]com

i-love-evilnominatuscrypt.000webhostapp[.]com

mirfinance[.]org

ns1.eccbc8[.]com

ns2.a3c65c[.]org

ns2.eccbc8[.]com

ns3.a3c65c[.]org

ns3.eccbc8[.]com

ns4.a3c65c[.]org

ns4.eccbc8[.]com

IP

1.248.122.240

104.18.11.39

115.88.24.202

116.121.62.237

161.35.41.9

192.248.176.138

192.64.119.190

20.82.210.154

46.101.113.161

72.21.81.240

72.21.91.29

74.119.194.37

网址

http://ac509c8002d8fcd0d8887a501qkvqqmi.hateme[.]uno/qkvqqmi

http://ac509c8002d8fcd0d8887a501qkvqqmi.legcore[.]space/qkvqqmi

http://ac509c8002d8fcd0d8887a501qkvqqmi.oddson[.]quest/qkvqqmi

http://ac509c8002d8fcd0d8887a501qkvqqmi.vyewxn2lkxrihikeunagqqoakralogk5ze5vaxrkahvkjdug6rcwdsqd[.]onion/qkvqqmi

http://e0147c08ac2072b06c243e60bujgzrlrg.crypack[.]fit/ujgzrlrg

http://e0147c08ac2072b06c243e60bujgzrlrg.duethat[.]quest/ujgzrlrg

http://e0147c08ac2072b06c243e60bujgzrlrg.eatlist[.]space/ujgzrlrg

http://e0147c08ac2072b06c243e60bujgzrlrg.laintin[.]uno/ujgzrlrg

http://e0147c08ac2072b06c243e60bujgzrlrg.mhpraylv6n2wpf4s6toapyab6uljsuwamd5qejw3aif466ipxjcxmuyd[.]onion/ujgzrlrg

http://f2d0c210a62830706eb8b638ekkkkxqz.vlqeedkmbvqdjzongyi6py6o5osehjze6r52mb2ijmx6qbh3lnb3zwid[.]onion/kkkkxqz

http://fuyt[.]org/fhsgtsspen6/get.php?pid=F7E0EF544C5C35BFCBAE00FDCB4667E1&first=true

http://fuyt[.]org/files/1/build3.exe

http://zerit[.]top/dl/build2.exe

https://iplogger[.]org/1rJeg7.tar

邮箱

back2023@proxy.tg

Blackrose786@disroot.org

fcsupport@mailfence.com

helpdecrypt@kolabnow.com

helplocker@my.com

ironse2022@tutanota.com

paid-files@email.tg