国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 9 期（总第 17 期）　　2 月 26 日-3 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

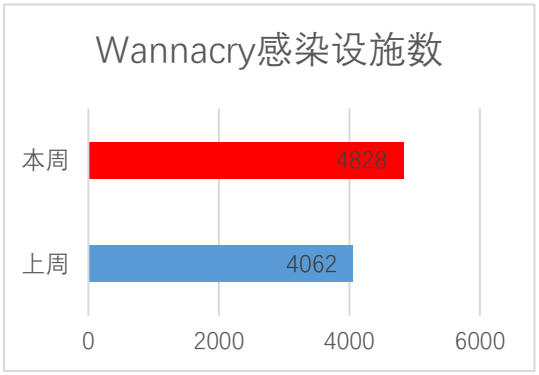
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1110668 个，监测发现勒索软件网络传播 4216 次，勒索软件下载 IP 地址 39 个，其中，位于境内的勒索软件下载地址 19 个，占比 48.7%，位于境外的勒索软件下载地址 20 个，占比 51.3%。

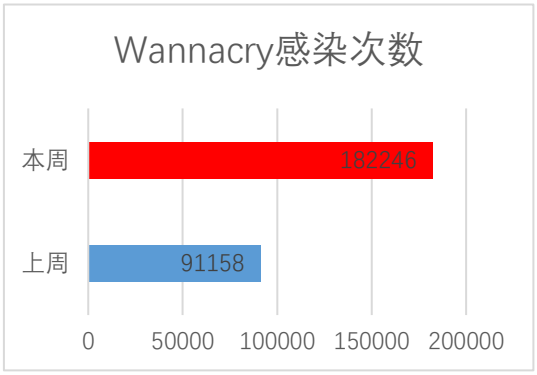
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

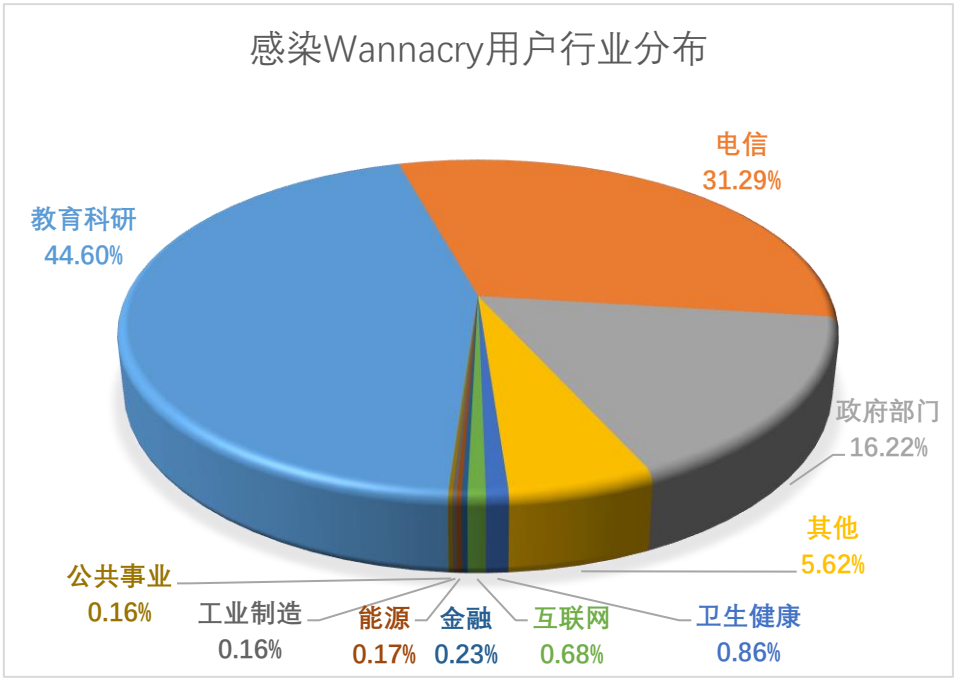
本周，监测发现 4828 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 18.9%，累计感染 182246 次，较上周上升 99.9%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



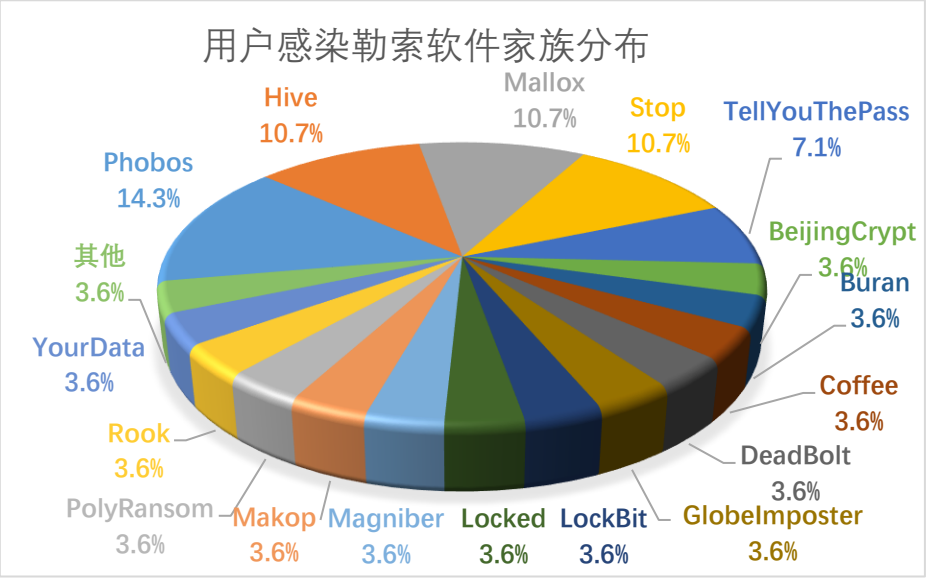


教育科研、电信、政府部门、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

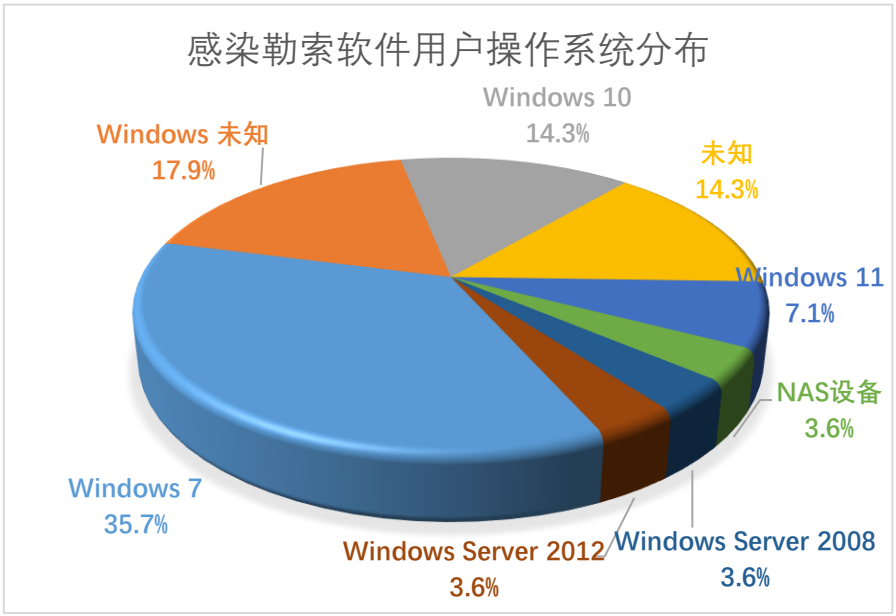


（二）其它勒索软件感染情况

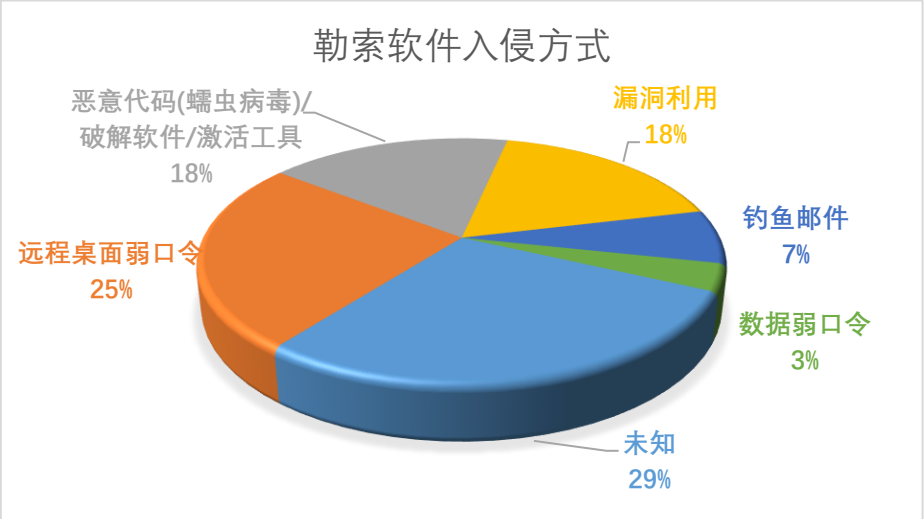
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 28 起非 Wannacry 勒索软件感染事件，事件数与上周相同，排在前三名的勒索软件家族分别为 Phobos（14.3%）、Hive（10.7%）和 Mallox（10.7%）。



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 35.7%，其次为 Windows 10 系统和 Windows 11 系统，占比分别为 14.3%和 7.1%，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，远程桌面弱口令和漏洞利用占比较高，分别为 25%和 18%。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、安徽省某企业服务器感染 TellYouThePass 勒索软件

本周，工作组成员应急响应了安徽省某企业服务器感染 TellYouThePass 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。

2、广东省某企业多台服务器感染 Phobos 勒索软件

本周，工作组成员应急响应了广东省某企业服务器感染 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员工终端，利用弱口令漏洞获得终端主机控制权，随后以该终端作为跳板机进行内网渗透获取多台服务器的控制权，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终端控制权后进行横

向移动并多台服务器植入勒索软件。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、微软 Exchange 服务器被攻击用于部署 Cuba 勒索软件

近日，勒索软件团伙 Cuba 利用微软 Exchange 服务器的安全漏洞进入企业网络并对设备进行加密。美国联邦调查局 FBI 指出，Cuba 勒索软件使用 Hancitor 这个已经存在了 5 年的恶意软件作为第一阶段攻击手段并为后续攻击提供威胁加载程序，Hancitor 操作员通过微软 Exchange 漏洞或远程桌面弱口令获得对目标主机的初始访问权限，进而植入勒索软件。建议用户及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

四、威胁情报

域名

Irrislaha[.]com

leptengthinete[.]com

siagevewilin[.]com

surnbuithe[.]com

IP

141.136.44.54

144.172.83.13

185.153.199.164

185.43.7.120

188.120.247.108

190.114.254.116

23.227.197.229

45.32.229.66

45.9.190.135

64.235.39.82

64.52.169.174

72.21.81.240

网址

http://807ce800469cb8e0aa347ef81c1cdnljknj.57s6smgyi4sgbjrsa5dotbcu5sait5aaly3gg6zqnfdb5l53aebyqhyd[.]onion/dnljknj

http://88ec3668c81828b030d08238znwafnwh.dayeven[.]space/znwafnwh

http://88ec3668c81828b030d08238znwafnwh.forrain[.]fit/znwafnwh

http://88ec3668c81828b030d08238znwafnwh.luckymy[.]quest/znwafnwh

http://88ec3668c81828b030d08238znwafnwh.mensell[.]uno/znwafnwh

http://e21c96780a5880f0ee28ea905e142ce0tchhtwcf.gaplies[.]fit/tchhtwcf

http://e21c96780a5880f0ee28ea905e142ce0tchhtwcf.gunfail[.]quest/tchhtwcf

http://e21c96780a5880f0ee28ea905e142ce0tchhtwcf.hjew6l4r3hpgj7qiloum5j7jwq7q3623v4fsbq5edbckeppeetpiihid[.]onion/tchhtwcf

http://e21c96780a5880f0ee28ea905e142ce0tchhtwcf.ranmuch[.]space/tchhtwcf

http://e21c96780a5880f0ee28ea905e142ce0tchhtwcf.raredoe[.]uno/tchhtwcf

邮箱

asistchinadecryption2022@goat.si

bambam988@tuta.io

china_decr2021@xmpp.jp

Dec_youfile1986@mailfence.com

fastwindGlobe@mail.ee

restauera@safeswiss.com

restorefiles69@cock.li

钱包地址

12V777zwYAvtjKocEsmeYdcTpdK14XdKZZ

bc1qlmcur2rwt89d2r3v5javjht39933g7npjktfw7