国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 5 期　　12 月 4 日-12 月 10 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

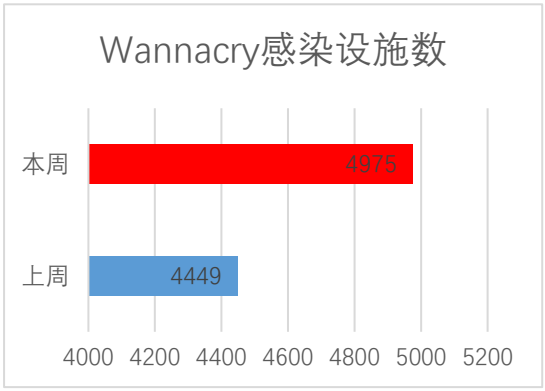
本周勒索软件防范应对工作组共收集捕获勒索软件样本 301662 个，监测发现勒索软件网络传播 2653 次，勒索软件下载 IP 地址 23 个，其中，位于境内的勒索软件下载地址 14 个，占比 60.9%，位于境外的勒索软件下载地址 9 个，占比 39.1%。

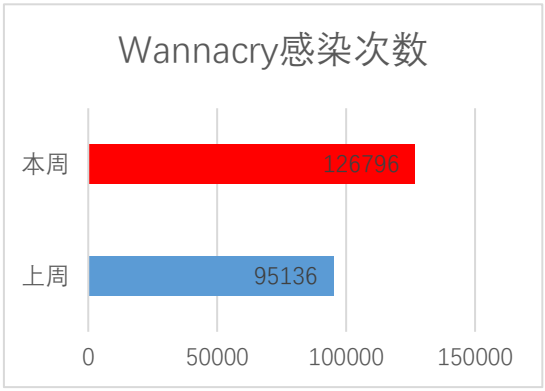
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

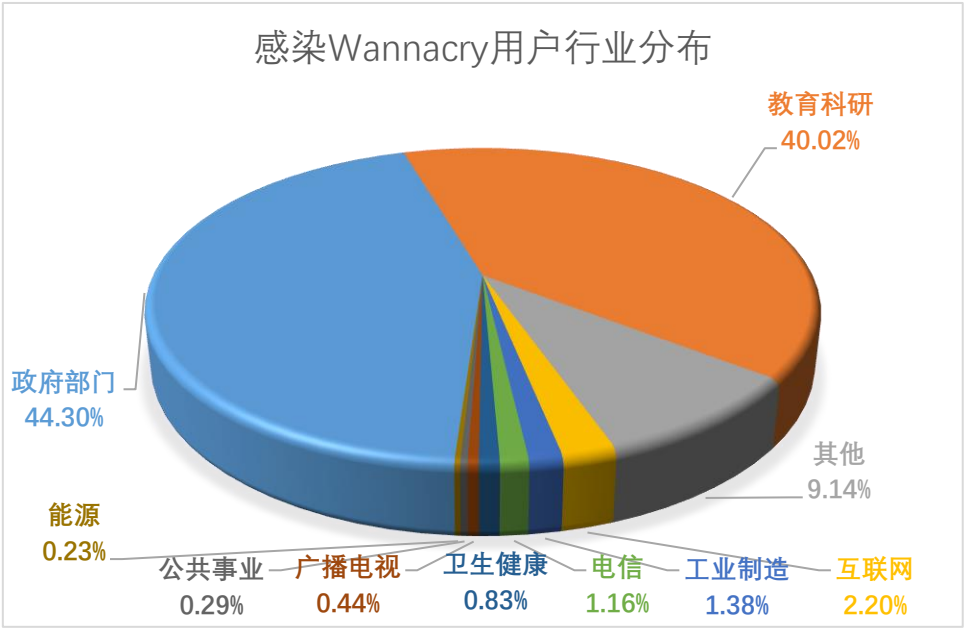
本周，监测发现 4975 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 11.8%，累计感染 126796 次，较上周上升 33.3%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



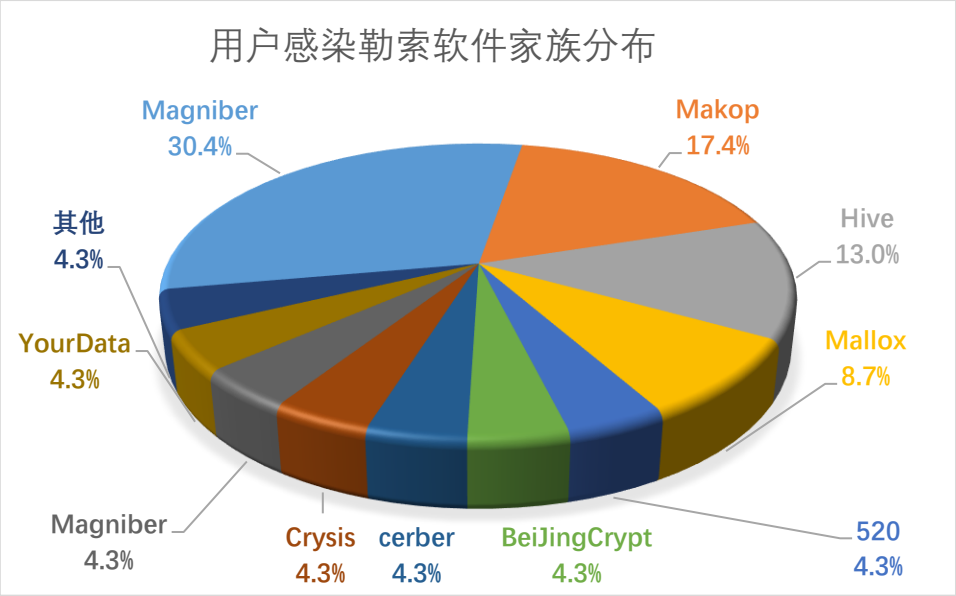


政府部门、教育科研、互联网、工业制造、电信行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反应，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

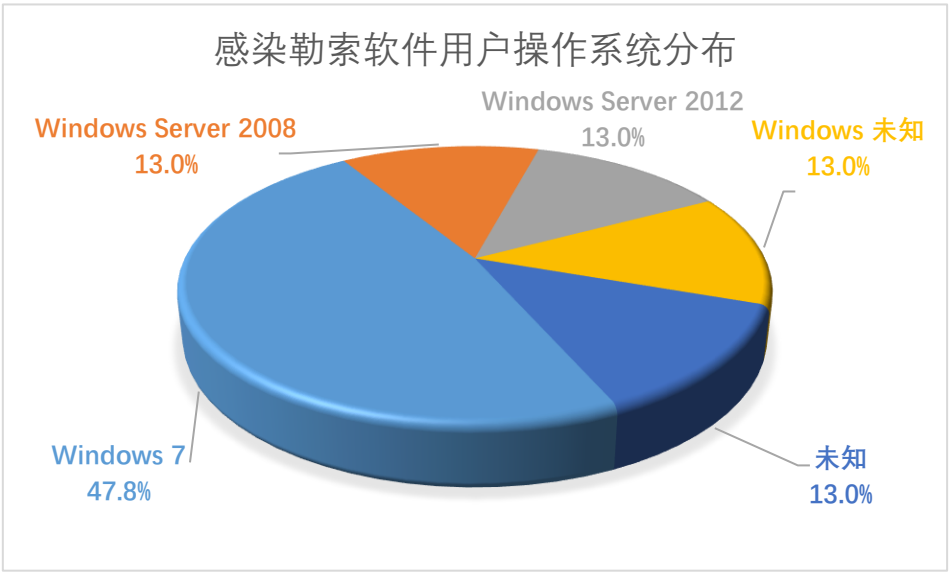


（二）其它勒索软件感染情况

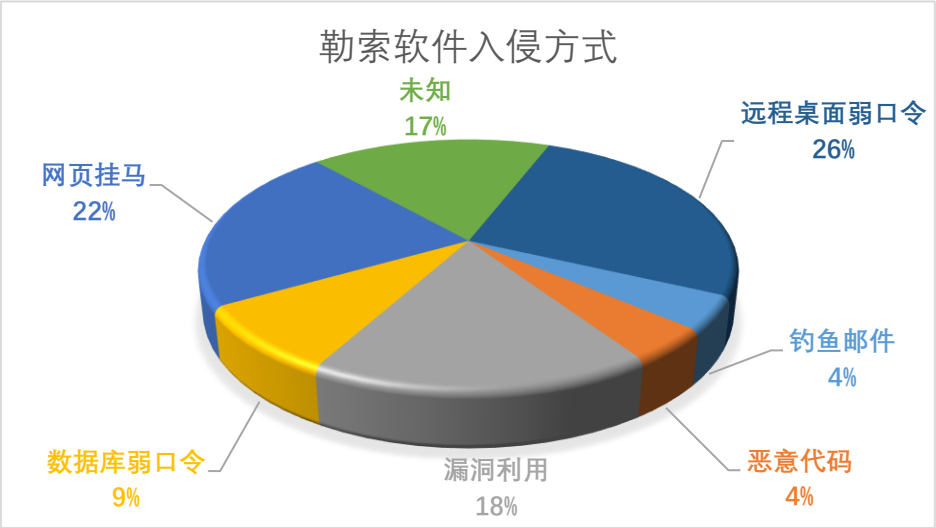
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 23 起非 Wannacry 勒索软件感染事件，较上周上升 4.5%，排在前三名的勒索软件家族分别为 Magniber（30.4%）、Makop（17.4%）和 Hive（13%）。



本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 47.8%，其次为 Windows Server 2008 和 Windows Server 2012 系统，占比均为 13%，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，远程桌面弱口令依然排在第一位，其次为挂马网站和漏洞利用。Magniber 勒索软件利用挂马网站和漏洞利用频繁攻击我国用户，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、陕西某企业代码存储服务器感染 Cerber 勒索软件

近日，工作组成员单位应急响应了陕西某企业代码存储服务器感染 Cerber 勒索软件事件。攻击者通过该服务器所运行的 Bitbucket 代码管理服务的远程命令执行漏洞，获得了服务器控制权，进而植入勒索软件。

此事件中，攻击者利用存在已知漏洞的服务程序获取服务器主机控制权后并植入勒索软件。建议用户及时升级软件至最新版本或安装补丁程序。

2、境内多个单位主机感染 Magniber 勒索软件

近日，工作组成员单位应急响应了北京、山东、山东等地多起 Magniber 勒索软件攻击事件。攻击者利用 Microsoft MSHTML 远程代码执行漏洞（CVE-2021-40444），手动或者自动安装 ActiveX 控

件。在访问攻击者特定入侵篡改的页面后，会触发下载执行恶意代码程序，导致目标主机被感染。

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。

（二） 国外部分

1、北欧精选酒店集团遭到勒索软件攻击

北欧精选酒店集团是一家大型连锁酒店集团,其拥有超过16,000名员工,在斯堪的纳维亚半岛、芬兰和波罗的海地区拥有200家酒店。该酒店确认其系统遭到了Conti勒索软件团伙的网络攻击,主要影响酒店的客人预订和房卡系统。酒店方面称没有迹象表明密码或支付信息受到影响，但与客人预订相关的信息可能会泄露。该事件的攻击者所使用的Conti勒索软件是一种勒索软件即服务(RaaS)，与Ryuk 家族共享部分代码,此前曾攻击十多个医疗和急救组织以及警察部门系统。今年早些时候,Conti成功入侵了爱尔兰卫生服务执行局(HSE)和卫生部(DoH)的网络，并要求支付2000万美元的赎金。

四、威胁情报

域名

newkm.tkamc[.]com

IP

40.115.162.72

37.120.193.123

157.245.70.127

31.44.184.82

185.153.199.176

157.245.84.162

168.119.93.163

128.199.118.202

185.93.6.31

网址

http://157.245.84[.]162/tmp.conf.2w

http://pigetrzlperjreyr3fbytm27bljaq4eungv3gdq2tohnoyfrqu4bx5qd[.]onion/bt01

http://fbi[.]fund/tortillas/tortillas.exe

http://ead8cef892546a3zbspullr.knewpen[.]space/zbspullr

http://ead8cef892546a3zbspullr.veryits[.]quest/zbspullr

http://1acc02c8e0d8be5ffhpgxcs.knewpen[.]space/ffhpgxcs

http://1acc02c8e0d8be5ffhpgxcs.veryits[.]quest/ffhpgxcs

http://bc0000e8e088d800hajwhgc.veryits[.]quest/hajwhgc

http://bc0000e8e088d800hajwhgc.knewpen[.]space/hajwhgc

http://d8ecea407838d8c0mvuxbvk.hotplus[.]quest/mvuxbvk

http://d8ecea407838d8c0mvuxbvk.saydoes[.]space/mvuxbvk

http://ead8cef892546a3zbspullr.rawloop[.]fit/zbspullr

http://ead8cef892546a3zbspullr.billfun[.]uno/zbspullr

邮箱

520hard@mail.ee

520hard@cock.li

rpd@keemail.me

rapid@aaathats3as.com

Helper@privatemail.com