国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 4 期　　11 月 27 日-12 月 3 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

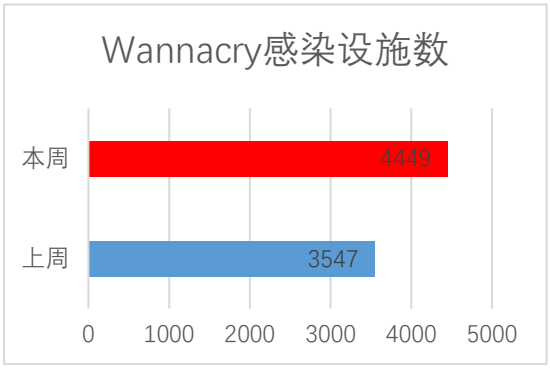
本周勒索软件防范应对工作组共收集捕获勒索软件样本 345196 个，监测发现勒索软件网络传播 1556 次，勒索软件下载 IP 地址 23 个，其中，位于境内的勒索软件下载地址 14 个，占比 60.9%，位于境外的勒索软件下载地址 9 个，占比 39.1%。

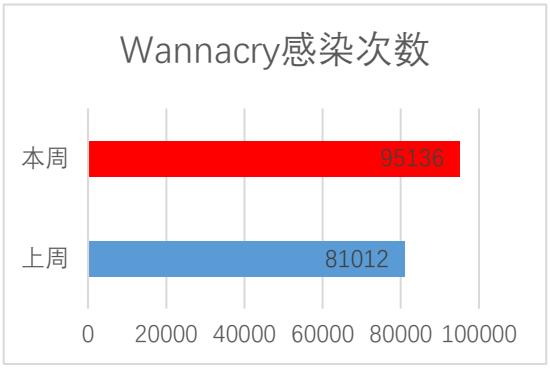
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

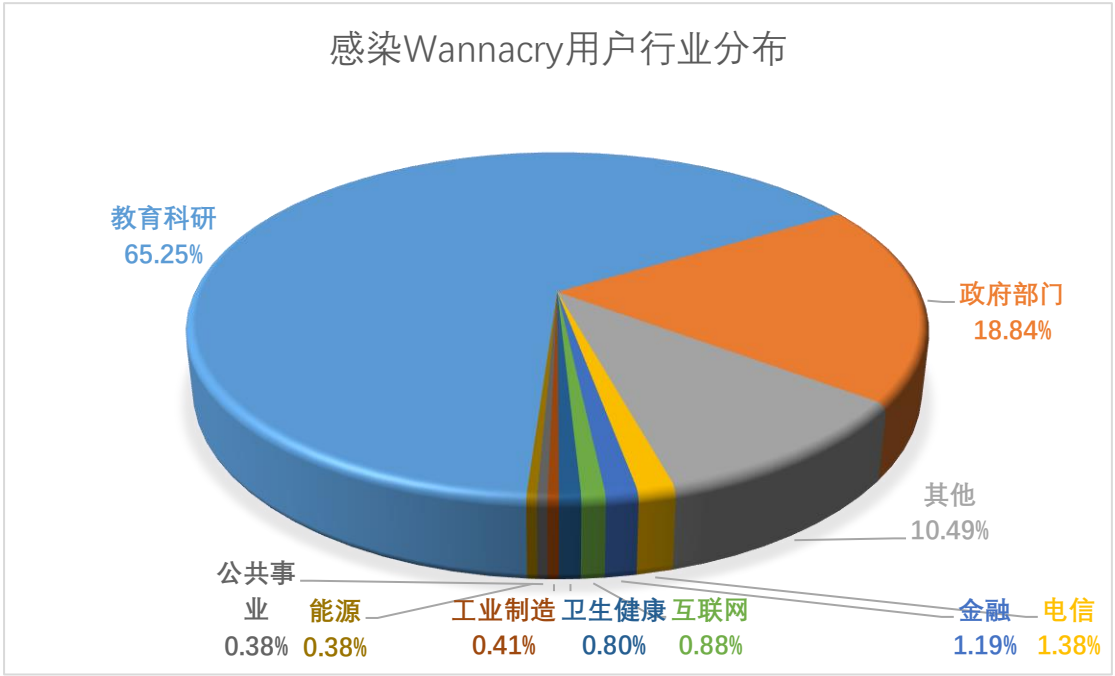
本周，监测发现 4449 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 25.4%，累计感染 95136 次，较上周上升 17.4%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



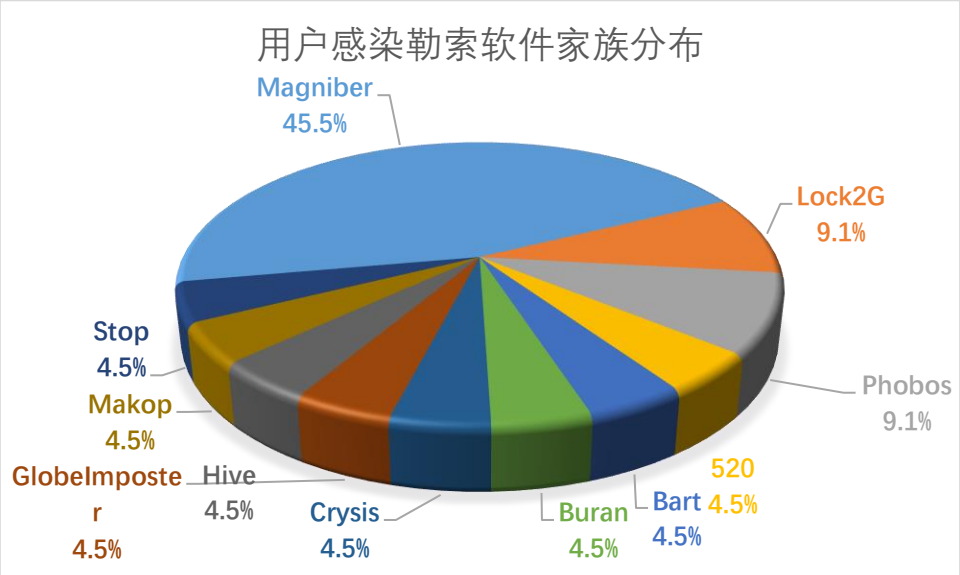


教育科研、政府部门、电信、金融、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反应，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

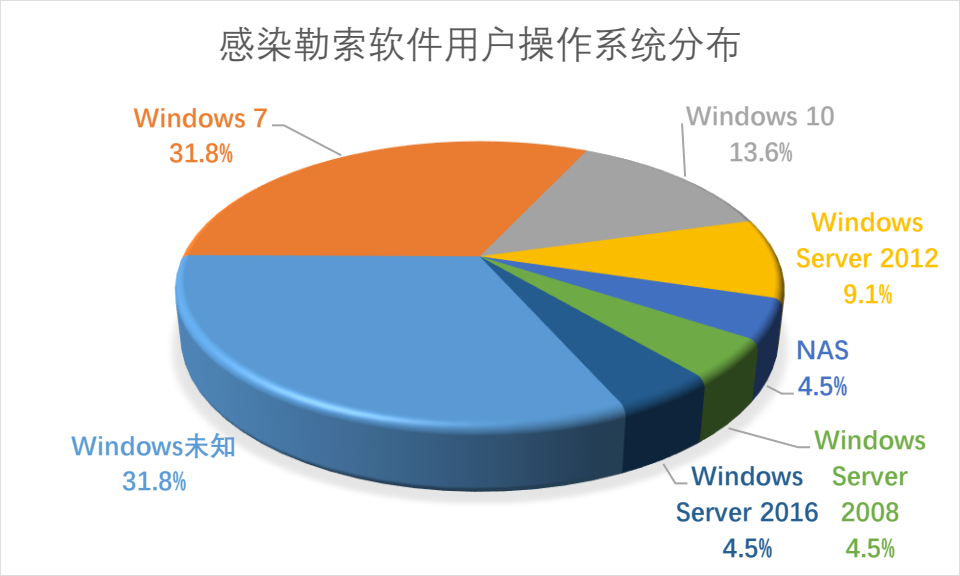


（二）其它勒索软件感染情况

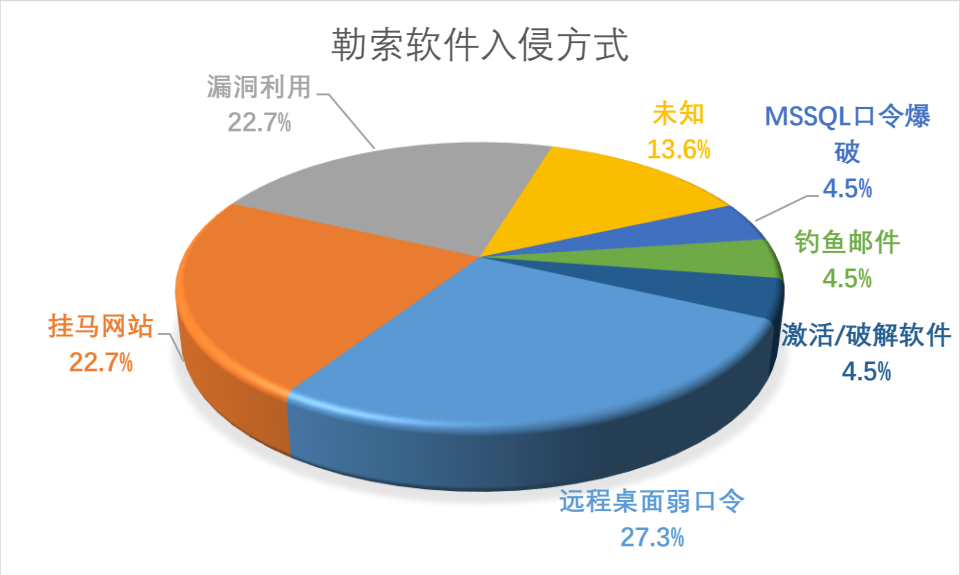
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 22 起非 Wannacry 勒索软件感染事件，较上周下降 12%，排在前三名的勒索软件家族分别为 Magniber（45.5%）、Lock2G（9.1%）和 Phobos（9.1%）。



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 31.8%，其次为 Windows10 和 Windows Server 2012 系统，占比分别为 13.6%和 9.1%，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、上海某大学内网主机感染 Phobos 勒索软件

近日，工作组成员单位应急响应了上海某大学内网主机感染 Phobos 勒索软件事件。攻击者通过口令爆破利用 VPN 远程登录了内网 OpManager 网络监控管理主机，并通过弱口令爆破获取了另外一台服务器的账号密码，进而植入勒索软件。

此事件中，攻击者利用口令爆破先后攻入内网并横向移动植入勒索软件。建议用户修改默认管理员账号名，并设置强度较高的密码。

2、境内多家企业主机感染 Magniber 勒索软件

近日，工作组成员单位应急响应了广东、山东等地多起 Magniber 勒索软件攻击事件。事件起因均为企业员工使用带有漏洞的 IE 浏览器访问恶意网站，触发了网页中的漏洞利用代码，进而感染 Magniber 勒索软件，导致 PC 主机被加密，在个别单位中，勒索软件还加密了共享服务器中的共享文件。

Magniber 攻击者在一些非法网站或一些网站的广告位上，投放植入恶意漏洞攻击代码，当用户访问到相关页面时，攻击代码就会尝试执行，从而感染 Magniber 勒索软件。用户在日常工作和生活中应避免打开来历不明的邮件、链接和网址等，尽量不要在非官方渠道下载非正版的应用软件，定期检测系统漏洞并及时修复。

（二） 国外部分

1、澳大利亚昆士兰州政府能源公司遭到勒索软件攻击

CS Energy 是昆士兰州三大主要发电公司之一，隶属于昆士兰州政府。勒索攻击发生在周末，勒索团伙入侵了该公司系统，攻击发生后，CS Energy 迅速采取行动，将公司网络与其他内部网络隔离，并制定业务连续性流程，以遏制这一事件。该公司表示，此次事件并未影响 Callide 和 Kogan Creek 电站的发电，发电站将继续发电并将电力输送到全国电力市场。

四、威胁情报

域名

tcp.symantecserver[.]co

probes[.]space

tinysidney[.]com

gordonzon[.]com

cofeeloveers[.]com

doratir[.]com

markettc[.]biz

farhadl[.]com

frankir[.]com

greentuks[.]com

probes[.]site

aimee0febai5phoht2ti.probes[.]website

aequuira1aedeezais5i.probes[.]space

datatransferdc[.]com

helpgoldr[.]com

probes[.]website

jeithe7eijeefohch3qu.probes[.]site

myeeducationplus[.]com

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]cam

IP

37.139.3.208

148.251.71.182

18.221.115.241

86.57.38.156

217.23.5.42

198.144.189.74

45.79.55.129

45.147.230.137

45.141.84.182

45.146.166.24

45.147.230.221

185.53.46.115

185.93.6.31

网址

http://buclemylhtpbsxd7g2opjib3pzc5jgami5c3oya56j4kdo26ha4wcoad[.]onion

http://be843c002e8c0e60drpcjfiwex.areedit[.]uno/rpcjfiwex

http://be843c002e8c0e60drpcjfiwex.orseen[.]casa/rpcjfiwex

http://be843c002e8c0e60drpcjfiwex.hotplus[.]quest/rpcjfiwex

http://be843c002e8c0e60drpcjfiwex.saydoes[.]space/rpcjfiwex

http://6cf0a298ee806e10a43406a8fhfylawsl.3g5twxggjkc76oy6itmdvhliayffjfv23vg3r

p372nn7ohfnnylfclid[.]onion/hfylawsl

http://0a88f4f8362cf68068b8ecb8fndkoak.cj5e2mlnwfnvfurw3qq7b3ztyeuni345taxkfw7kbjoweeqewr2bosqd[.]onion/fndkoak

http://ec241898708c64505eccf6c8vafsaemxl.cj5e2mlnwfnvfurw3qq7b3ztyeuni345taxkfw7kbjoweeqewr2bosqd[.]onion/vafsaemxl

http://fed892f04850c00mxqnlxdd.o7wgk5cbzp7ecuiwwh5rkw5jsahwhfqc5v5itoebkzrpou2rfjck2dqd[.]onion/mxqnlxdd

http://6c4ca0e0f2c06aygxostl.cj5e2mlnwfnvfurw3qq7b3ztyeuni345taxkfw7kbjoweeqewr2bosqd[.]onion/ygxostl

邮箱

grepmord@protonmail.com

Vasco_Alonso@tutanota.com

Vasco_Alonso@protonmail.com

steven1973parker@libertymail.net

fileback@cock.li

fileback@tuta.io

admin@crypteyourdata.com

钱包地址

1FTSSEbEMTgxT26NTQzZueD5MZtSsF2ea2

1CVY1j7rWftBza6DdrWQjBBEHk53uqR5TW

1E4DHunAQsAXp4M9mb62ojCvFwd1KNnofr

1NCNySGzfjW1rYEpiQxAoC13JPtuY7sAVe

1PWWetapeRgy4mScYpVvWeEFGJi9W3VcuU

1FfYtL31vRviRidyTpzwyX2khZAC2HE5Wh