国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 3 期　　11 月 20 日-11 月 26 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

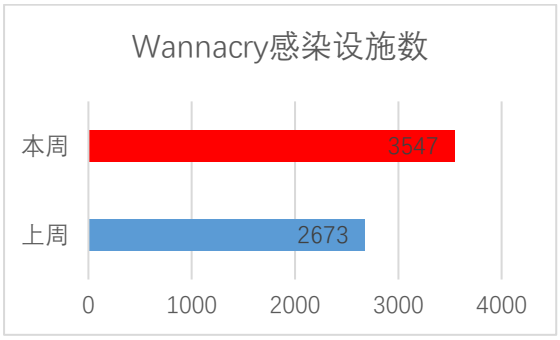
本周勒索软件防范应对工作组共收集捕获勒索软件样本 122635 个，监测发现勒索软件网络传播 2955 次，勒索软件下载 IP 地址 15 个，其中，位于境内的勒索软件下载地址 8 个，占比 53.3%，位于境外的勒索软件下载地址 7 个，占比 46.7%。

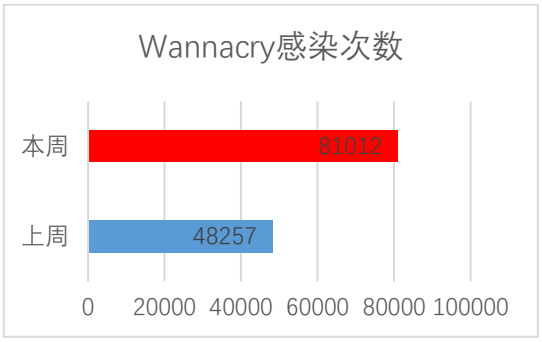
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

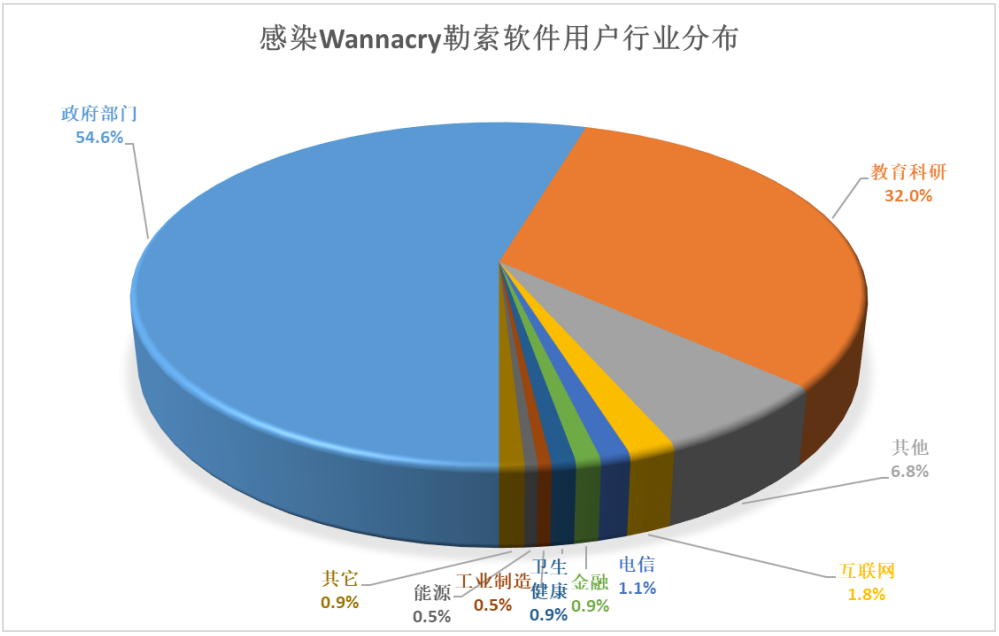
本周，监测发现 3547 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 32.7%，累计感染 81012 次，较上周上升 67.9%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



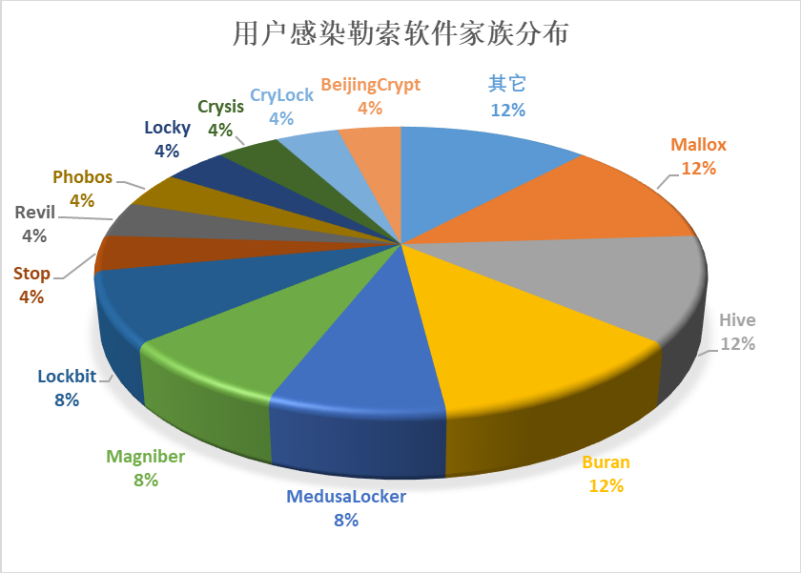


政府部门、教育科研、互联网、电信、金融行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反应，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

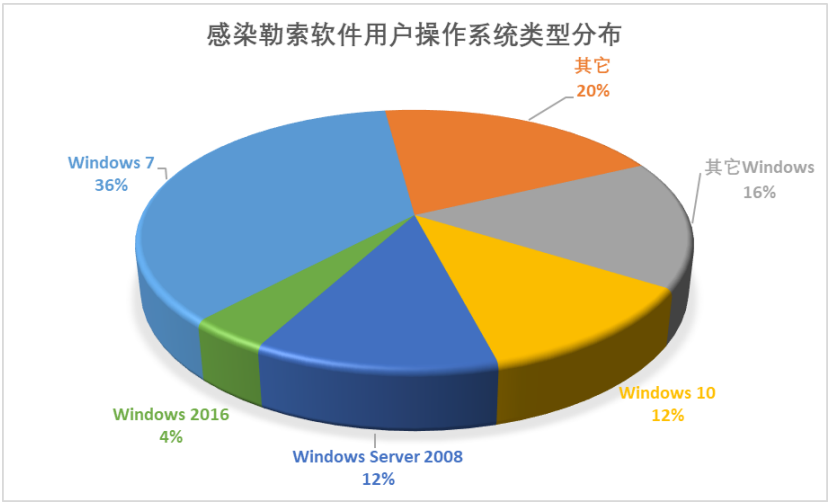


（二）其它勒索软件感染情况

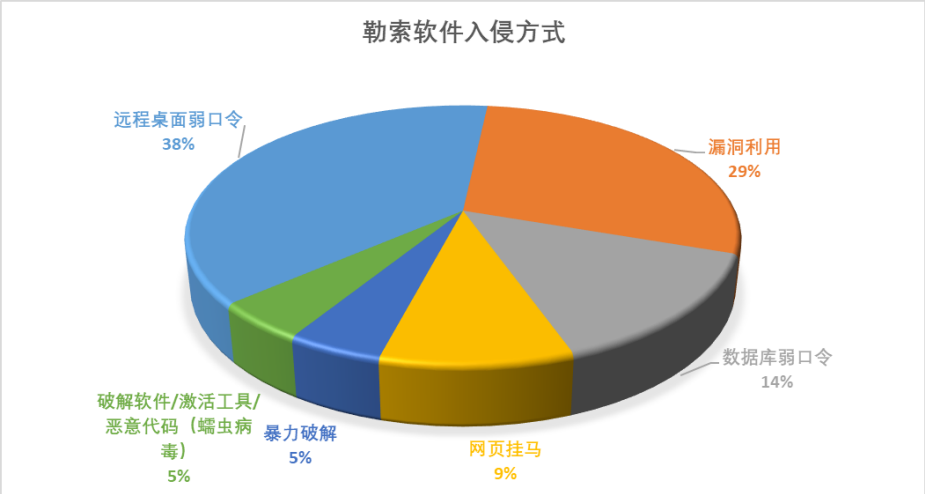
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 25 起非 Wannacry 勒索软件感染事件，较上周下降 30.6%，排在前三名的勒索软件家族分别为 Mallox（12%）、Hive（12%）和 Buran（12%）。



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 36%，其次为 Windows10 和 Windows Server 2008 系统，占比均为 12%，除此之外还包括较多不同版本的 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，远程桌面弱口令排在第一位，其次为漏洞利用和数据库弱口令。综合发现，各种类型的弱口令依然是勒索软件攻击最常用的入侵手段。勒索软件常常伪装成破解工具、激活工具等软件，用户下载使用时需要警惕，不要运行来历不明的软件。



三、典型勒索软件攻击事件

（一） 国内部分

1、上海某金融公司感染 Magniber 勒索软件

近日，工作组成员单位应急响应了上海某金融公司 PC 办公电脑感染 Magniber 勒索软件事件。该公司一名员工使用带有 CVE-2021-26411 漏洞的 IE 浏览器浏览可疑网站，触发漏洞代码执行，下载执行 Magniber 勒索软件。

Magniber 勒索软件利用 IE 浏览器漏洞对 IE 浏览器用户进行网页挂马攻击，建议用户及时升级浏览器版本或使用 chrome 内核浏览器上网。不访问博彩、色情网站等高风险网站，对重要文件进行异地备份，即使被加密勒索也能通过备份恢复。

2、浙江某公司感染 520 勒索软件

近日，工作组成员单位应急响应了浙江某公司感染 520 勒索软件事件。攻击者利用 Windows 远程桌面服务漏洞（CVE-2019-0708）漏洞入侵到公司服务器，提升权限后，植入勒索软件，对用户服务器全盘加密，并攻击了内网中另外一台服务器。

此事件中攻击者利用未打补丁的 RDP 漏洞入侵到用户网络，并在内网横向移动，攻陷更多设备。建议用户及时更新安全补丁，安装部署必要的安全防护手段。

（二） 国外部分

1、Everest 勒索软件团伙公开售卖某政府的内部网络访问权限

据 Twitter 爆料，Everest 勒索软件团伙在其网站上挂出公告，宣称自己掌握了阿根廷政府各种内部服务的访问权限，甚至可以访问并编辑其数据库。该公告的目的主要是为了兜售以上权限，售价 20 万美元。

四、威胁情报

MD5

24095D5F0FB8533C72508FBECD40B516

34B2AAD3AB44EF46ECFE5C41F2DC2E9D

64C7B946266FEE18F854D36065A9C264

EBC2661A409A3A743BBA237BA1BFC4E8

2A37DA5634B1E4B188FC5EF86704E41B

FC93ECB882FBC1BAC46AAF4232CE9B66

1D2B8FEC867DC55D7DBF4E8E939624E9

F4D8BB082B0D03EFD6990CC2F4336165

80174956B0D1849EE802490817A2748F

A3E082A0E395339F5FD6A57AD3F71899

6963889B7FDBD40F274E074465392785

42E3099A1C51406B6C6CF448D738CF91

域名

novelengine.com

heckvisa.xyz

lurchmath.org

transfer.sh

google.onedriver-srv.ml

checkvisa.xyz

IP

78.138.105.150

27.102.127.120

123.45.67.89

190.144.115.54

169.51.60.221

183.110.224.164

195.201.124.214

27.102.66.114

45.77.76.158

网址

http://8e8cf43068846c0008ecobrbuz.ballhas.quest/cobrbuz

http://8e8cf43068846c0008ecobrbuz.leftan.space/cobrbuz

http://8e8cf43068846c0008ecobrbuz.boatsix.fit/cobrbuz

http://8e8cf43068846c0008ecobrbuz.filedme.uno/cobrbuz

http://a10c30yc2279530m.drawsbe.space/

http://a10c30yc2279530m.drawsbe.space/favicon.ico

veqlxhq7ub5qze3qy56zx2cig2e6tzsgxdspkubwbayqije6oatma6id.onion/order/14cYV

dg9gtEHExxpbMxjAn5A7h8a7dn2Vz

5e6c16401c90b2d010cc44905ccknsfw.o7wgk5cbzp7ecuiwwh5rkw5jsahwhfqc5v5ito

ebkzrpou2rfjck2dqd.onion/ccknsfw

d8d8522026fc3ab046d072401qocpvlx.o7wgk5cbzp7ecuiwwh5rkw5jsahwhfqc5v5itoe

bkzrpou2rfjck2dqd.onion/qocpvlx

4c0810900a00541078f89ac0fjksknrtv.w3disbrllt7cfknxuutwevchixw5vbyc4ujvg5cz3u57nryezwqgwnad.onion/jksknrtv

66141a782afc6a30a4803010fmkxzbyvqg.ckenzpyyu4oxd3zheye37qprryuiqbfvrqukfkqfzt66mxb33roeltid.onion/mkxzbyvqg

邮箱

harpoonlocker@onionmail.com

datarecovery@ctemplar.com

helpservisee@elude.in

jericoni@pm.me

cnlock@danwin1210.me

RansHelp@tutanota.com

钱包地址

14cYVdg9gtEHExxpbMxjAn5A7h8a7dn2Vz

16ezpVSXUFwhdzwp6X4o2kAXR65mTSJxDM

1MSYtA1q4u5HxTfV5D8purgmi1RV7ABYuf

3JG36KY6abZTnHBdQCon1hheC3Wa2bdyqs

1XmSC4sZskBmLXQbtngpRoGTzKHkvnwGx

15Yn6GLoDUmuSi7geP5STDMnZEW2JViFBS