国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 7 期　　12 月 18 日-12 月 24 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

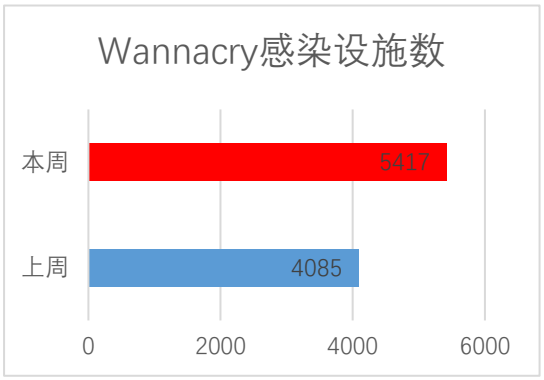
本周勒索软件防范应对工作组共收集捕获勒索软件样本 714121 个，监测发现勒索软件网络传播 798 次，勒索软件下载 IP 地址 39 个，其中，位于境内的勒索软件下载地址 24 个，占比 61.5%，位于境外的勒索软件下载地址 15 个，占比 38.5%。

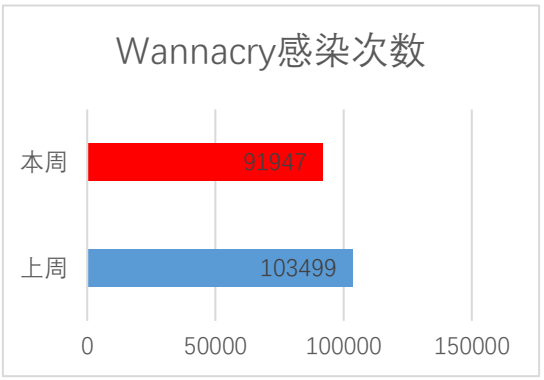
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

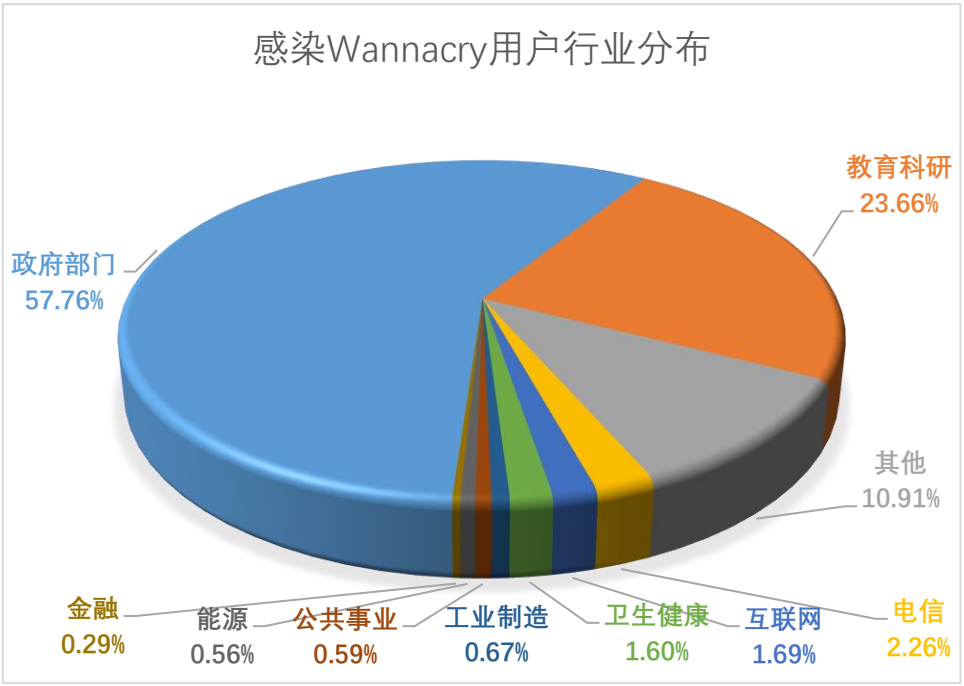
本周，监测发现 5417 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 32.6%，累计感染 91947 次，较上周下降 11.2%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



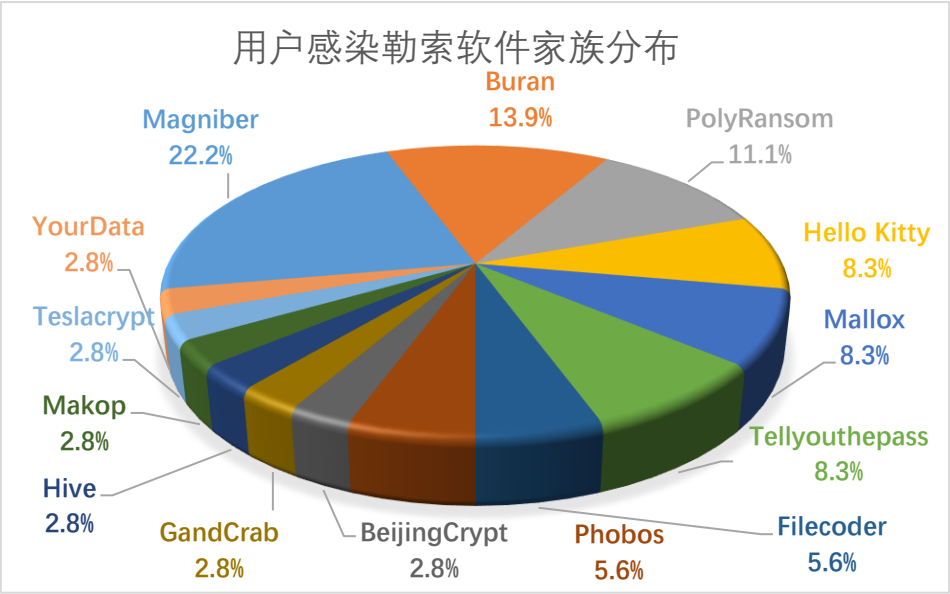


政府部门、教育科研、电信、互联网、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

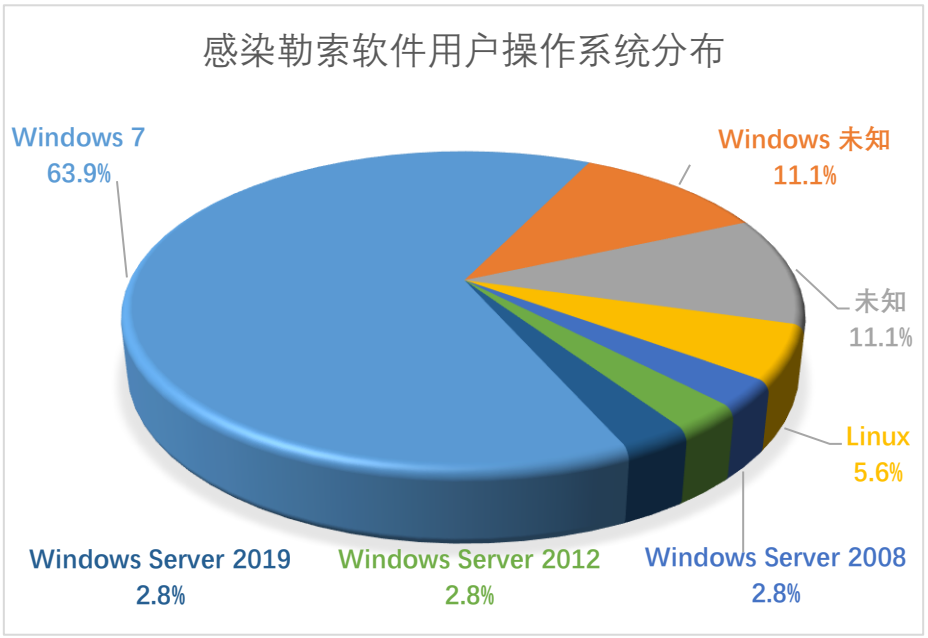


（二）其它勒索软件感染情况

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 36 起非 Wannacry 勒索软件感染事件，较上周下降 89.9%，排在前三名的勒索软件家族分别为 Magniber（22.2%）、Buran（13.9%）和 PolyRansom（11.1%）。

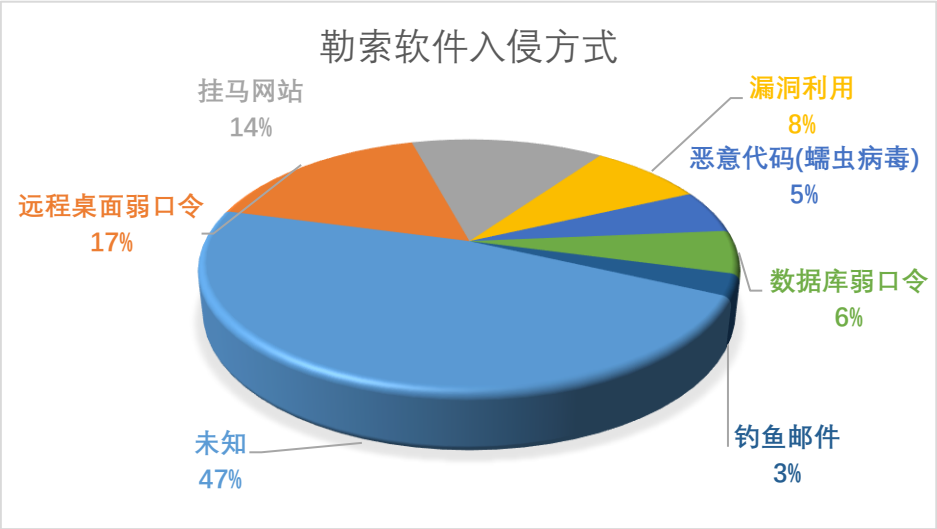


本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 63.9%，其次为 Linux 系统，占比为 5.6%，多个版本的 Windows 服务器系统包括 Server 2012、Server 2008 和 Server 2019 占比均为 2.8%，除此之外还包括多个其它不同版本的 Windows 系统和其它类型的操作系统。



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、上海某证券监管平台服务器感染 Tellyouthepass 勒索软件

本周，工作组成员应急响应了上海某证券监管平台服务器感染 Tellyouthepass 勒索软件。攻击者通过该服务器所运行 Web 应用程序中的 Log4j 组件漏洞（CVE-2021-44228），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、广东某金融单位多台服务器感染 YourData 勒索软件

本周，工作组成员应急响应了广东某金融单位多台服务器感染 YourData 勒索软件。攻击者通过服务器漏洞获得主机控制权并注入勒索软件，并向内网中存在安全漏洞的主机传播勒索软件，共 7 台业务服务器受到勒索软件攻击。

此事件中，攻击者利用对外网开放的服务器中的安全漏洞获取服务器主机控制权后植入勒索软件，并在内网中横向移动。建议用户及时升级软件至最新版本或安装补丁，此外，规划和实施网络隔离、健全安全审计体系也是缓解此类风险的重要手段。

（二） 国外部分

1、Clop 勒索软件团伙在暗网上发布英国警方掌握的机密数据

Clop 勒索软件团伙在对 IT 服务提供商 Dacoll 进行了一次成功的网络钓鱼攻击后，获取了大量资料，包括由 Dacoll 负责管理的英国警方国家计算中心(PNC)上的数据。在 Dacoll 拒绝支付赎金后，攻击者在暗网中上传了数百份文件。在上传的 PNC 文件中，有来自英国国家自动车牌识别系统(ANPR)的司机特写照片。执法机构表示其持有的数据遭到泄露将带来严重的后果，这些敏感数据可能扰乱刑事调查，更为严重的是，这些信息如果落入不法分子手中，将给犯罪受害者和证人带来严重风险。

四、威胁情报

域名

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

IP

139.60.160.200

168.100.11.72

174.138.62.35

185.182.193.120

193.38.235.234

88.80.147.102

93.190.139.223

网址

http://38acfc18f86c6c406424ea780asndoxskw.laintin[.]uno/asndoxskw

http://e8a4ce20a890b460942c44701relemeh.mensell[.]uno/relemeh

http://e8a4ce20a890b460942c44701relemeh.forrain[.]fit/relemeh

http://e8a4ce20a890b460942c44701relemeh.luckymy[.]quest/relemeh

http://e8a4ce20a890b460942c44701relemeh.dayeven[.]space/relemeh

http://3cacc8c054f492c00ef4daa0bjmzyauun.forrain[.]fit/jmzyauun

http://9ac426c8ce3c7aa078d89ea83nkzlkvrpx.enddare[.]fit/nkzlkvrpx

http://9ac426c8ce3c7aa078d89ea83nkzlkvrpx.tillpop[.]uno/nkzlkvrpx

http://9ac426c8ce3c7aa078d89ea83nkzlkvrpx.wartell[.]quest/nkzlkvrpx

http://9ac426c8ce3c7aa078d89ea83nkzlkvrpx.soknew[.]space/nkzlkvrpx

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

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

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

邮箱

encrypt11@cock.li

arnoldgladys88@gmx.com

willettamoffat@yahoo.com

code1024@keemail.me

malloxx@tutanota.com

GoodDay@privatemail.com

钱包地址

1CLmYDUjWtJeZPSujgfddGsg1D4DgRkHp3

19Kx5yAr7KhyUAb6G3CjjdnX9MzZems6GP

158yxcgryXCrCpCfAMBN39U5zsUdqmQaQm

15izxSPCQ2dVL3CKxi459nwamJ1PhEuipk

1DY3ft3Ny6XHgP7bEWW4Qgeu9iVWBZJo15

17ZDb4VQbuDWc5FutNwhNspFjS8vKdWdGK

1HkdZnTKrLjPw4vYHxEQLg4KVQe3ddDgac

173Ubc6dyhdS5o9q2mNja3nA2kvLBbpm11

14hCRYw9i5PF88eGEqH84GMKfkiZgJLTrd

1H6Jr2GATnnh6HPXTAP2az5JF6f4ApNSwP