

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 8 期

12 月 25 日-12 月 31 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

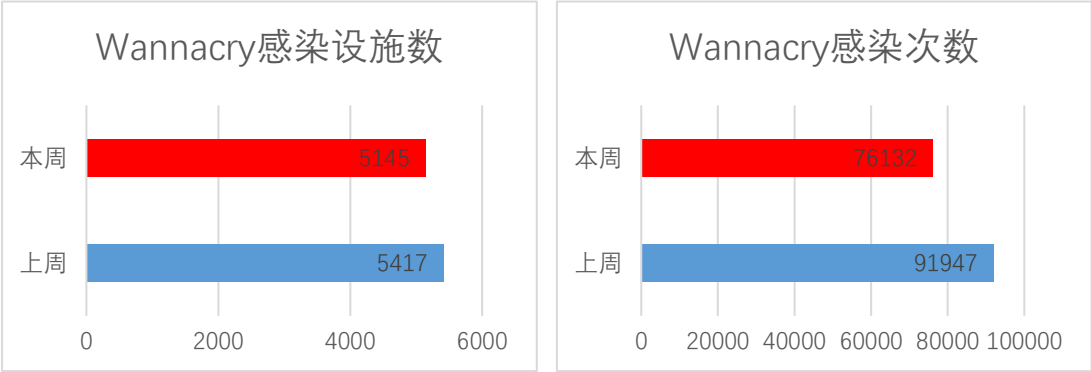
本周勒索软件防范应对工作组共收集捕获勒索软件样本 785490 个，监测发现勒索软件网络传播 100 次，勒索软件下载 IP 地址 5 个，其中，位于境内的勒索软件下载地址 2 个，占比 40%，位于境外的勒索软件下载地址 3 个，占比 60%。

二、勒索软件受害者情况

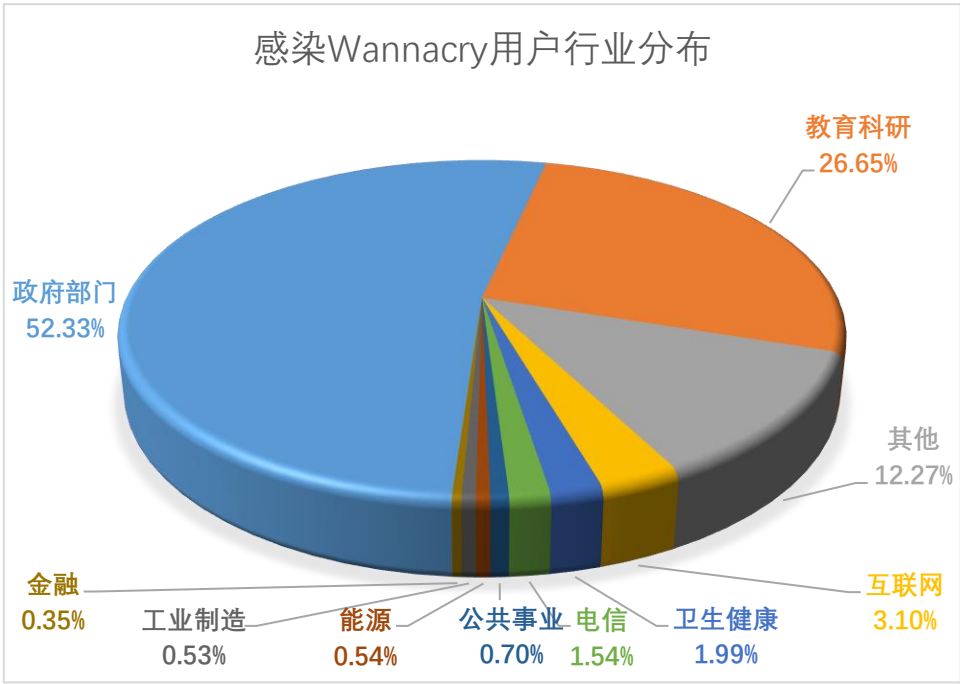
（一）Wannacry 勒索软件感染情况

本周，监测发现 5145 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 5%，累计感染 76132 次，较上周下降 17.2%。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。

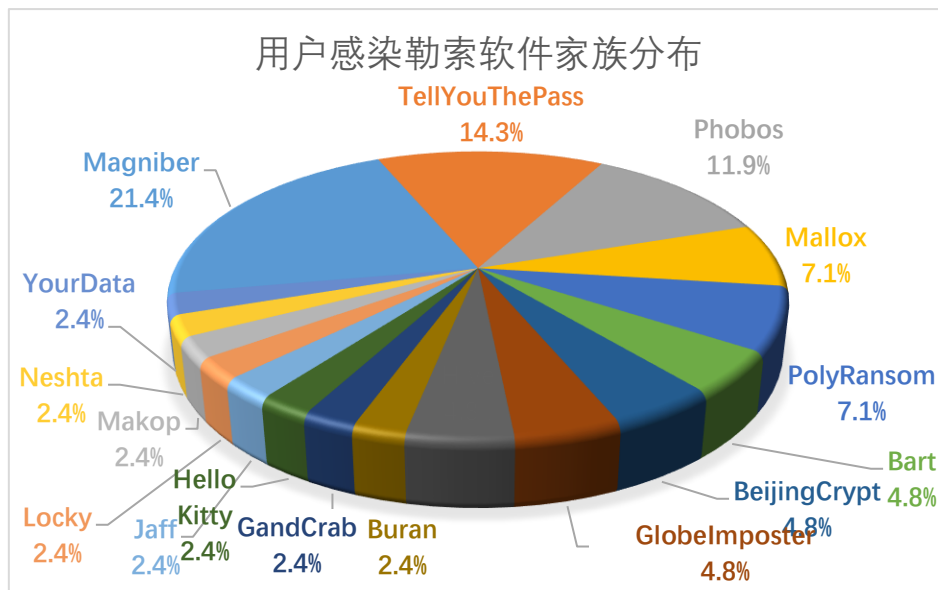


政府部门、教育科研、互联网、卫生健康、电信行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

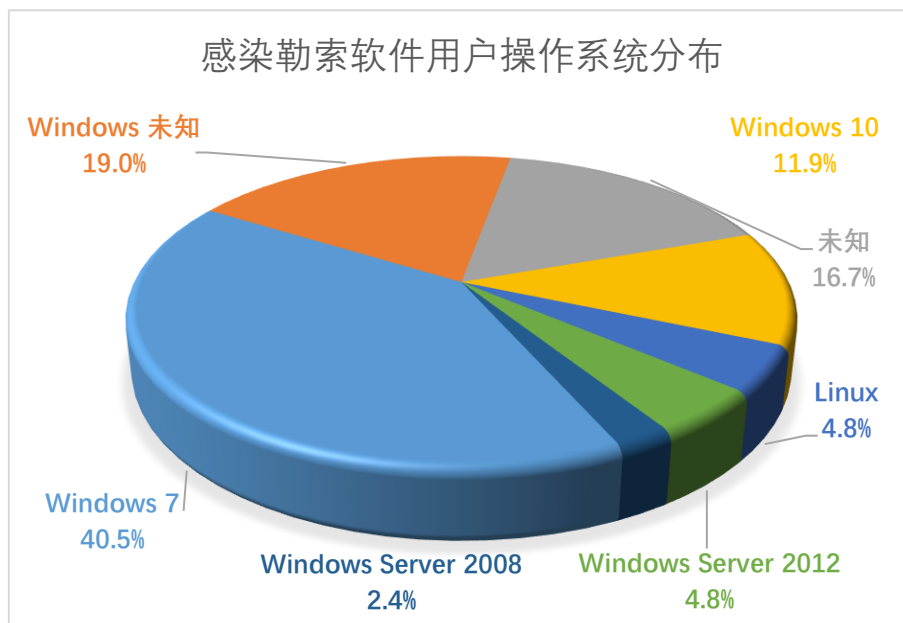


（二）其它勒索软件感染情况

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 42 起非 Wannacry 勒索软件感染事件，较上周上升 16.7%，排在前三名的勒索软件家族分别为 Magniber（21.4%）、TellYouThePass（14.3%）和 Phobos（11.9%）。

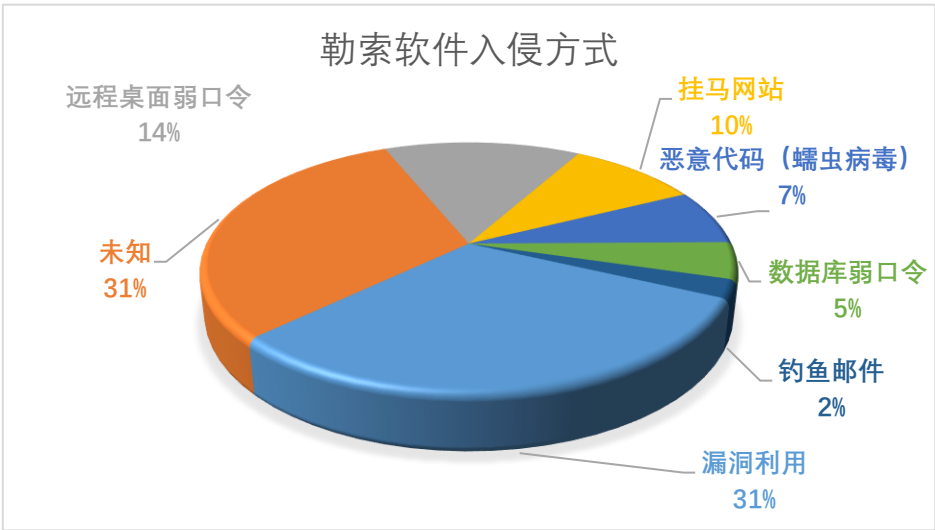


本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 40.5%，其次为 Windows10 系统，占比为 11.9%，多个版本的 Windows 服务器系统包括 Server 2012 和 Server 2008 分别占 4.8%和 2.4%，除此之外还包括多个其它不同版本的 Windows 系统和其它类型的操作系统。



本周，勒索软件入侵方式中，漏洞利用排在第一位，其次为远程桌面弱口令和挂马网站。Magniber 勒索软件利用漏洞利用和挂马网站

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） 国外部分

1、NAS 设备制造商威联通（QNAP）遭受 eCh0raix 勒索软件攻击

网络附加存储（NAS）设备制造商威联通（QNAP）用户在圣诞节期间遭遇 eCh0raix 勒索软件（也称为 QNAPCrypt）攻击。据悉，大规模的勒索软件攻击始于圣诞节前一周，并于 12 月 26 日左右结束。本次事件中，eCh0raix 勒索软件的传播途径被认为可能是由于用户的安全意识薄弱而将 NAS 设备接入了不安全的网络链接，此外，QNAP Photo Station 中的一个安全漏洞也可能加速勒索软件的传播。

QNAPCrypt 勒索软件在加密文件前从命令和控制服务器（C&C）请求钱包地址和公共 RSA 密钥，并为每个攻击目标分配一个唯一的比特币钱包。建议用户遵循 QNAP 的安全加固建议，以保护其 NAS 设备及其存储的数据安全。

四、威胁情报

域名

gamol6n6p2p4c3ad7gxmx3ur7wwdwlywebo2azv3vv5qlmj mole2zbyd[.]onion

IP

139.60.160.200

155.94.154.170

158.247.216.148

168.100.11.72

174.138.62.35

185.182.193.120

193.38.235.234

205.185.117.115

45.76.99.222

88.80.147.102

93.190.139.223

网址

[http://ccc0ac18e6bca09030305a0044e452f0bftgecmo.hotknew\[.\]space/bftgecmo](http://ccc0ac18e6bca09030305a0044e452f0bftgecmo.hotknew[.]space/bftgecmo)

[http://ccc0ac18e6bca09030305a0044e452f0bftgecmo.selllet\[.\]quest/bftgecmo](http://ccc0ac18e6bca09030305a0044e452f0bftgecmo.selllet[.]quest/bftgecmo)

[http://c4a81098ae7492408ccc8a60a440fc30qecobhee.selllet\[.\]quest/qecobhee](http://c4a81098ae7492408ccc8a60a440fc30qecobhee.selllet[.]quest/qecobhee)

[http://c4a81098ae7492408ccc8a60a440fc30qecobhee.hotknew\[.\]space/qecobhee](http://c4a81098ae7492408ccc8a60a440fc30qecobhee.hotknew[.]space/qecobhee)

[http://3ac824b0908824b0f8ac7ce0a4f09020nbxprbjs.hotknew\[.\]space/nbxprbjs](http://3ac824b0908824b0f8ac7ce0a4f09020nbxprbjs.hotknew[.]space/nbxprbjs)

[http://3ac824b0908824b0f8ac7ce0a4f09020nbxprbjs.selllet\[.\]quest/nbxprbjs](http://3ac824b0908824b0f8ac7ce0a4f09020nbxprbjs.selllet[.]quest/nbxprbjs)

[http://d8b470e82e4c90801e681e48de081ee0sdgvftzdu.netlaws\[.\]fit/sdgvftzdu](http://d8b470e82e4c90801e681e48de081ee0sdgvftzdu.netlaws[.]fit/sdgvftzdu)

[http://d8b470e82e4c90801e681e48de081ee0sdgvftzdu.cellgot\[.\]uno/sdgvftzdu](http://d8b470e82e4c90801e681e48de081ee0sdgvftzdu.cellgot[.]uno/sdgvftzdu)

[http://bc70bc207450ba309c6816b00688b8srzbxfdit.hotknew\[.\]space/srzbxfdit](http://bc70bc207450ba309c6816b00688b8srzbxfdit.hotknew[.]space/srzbxfdit)

[http://3.145.115\[.\]94/zambo/groenhuyzen.exe](http://3.145.115[.]94/zambo/groenhuyzen.exe)

[http://158.247.216\[.\]148/jquery.js?v=142](http://158.247.216[.]148/jquery.js?v=142)

[http://158.247.216\[.\]148/ss64](http://158.247.216[.]148/ss64)

[http://45.76.99\[.\]222/jquery.js?v=999999](http://45.76.99[.]222/jquery.js?v=999999)

[http://loki-locker\[.\]one/index.php](http://loki-locker[.]one/index.php)

[http://loki-locker\[.\]one/tg.php](http://loki-locker[.]one/tg.php)

邮箱

Victorcrou@privatemail.com

recover520@mailfence.com

helpstoremanager@airmail.cc

datarecover@protonmail.com

johnwilliams1887@gmx.com

Dekrypt24@tutanota.com

钱包地址

1K25DjGJuqpK3cgKW15WmHXahuvAfUomVU

bc1qqxck7kpzgvud7v2hfyk55yr45fnml4rmt3jasz

19k2hXH5F3ZcGXnmB5HKQqgrokSXMLRix6

1Dw2cWypK4yn8NmAemJ4XJ1HFpT7Sf6okN

1P6ZH9WfSHDmA6SKHUpGzWJpw1DzvDC5Ja

1GGC2dAjdN767roinoxqYNrxDKfZYieBEi

17CTjL8aGkdP2BbMSDqvqg36R7QNAfc43K

15yL7k7Ua8dUNjq2u3ionPC72rU9a6FjPP

1PMiKktbHeLAxJCutDSV4rCF7Fw5s9D2xD

1Je7jvg88h4tN3rw3yFSztTQivXGkoHWmV