# 国家互联网应急中心（CNCERT/CC）

# 勒索软件动态周报

2022 年第 16 期（总第 24 期）　　4 月 16 日-4 月 22 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

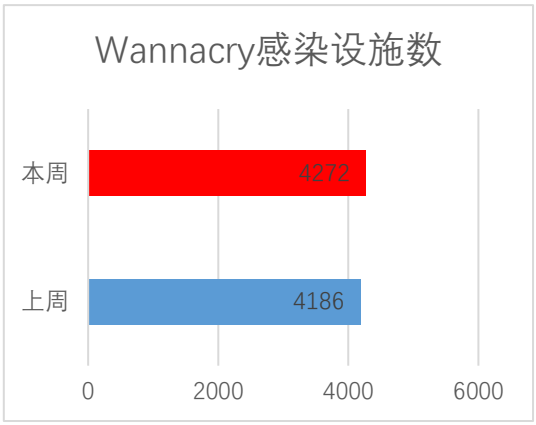
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1499202 个，监测发现勒索软件网络传播 552 次，勒索软件下载 IP 地址 81 个，其中，位于境内的勒索软件下载地址 13 个，占比 16.0%，位于境外的勒索软件下载地址 68 个，占比 84.0%。

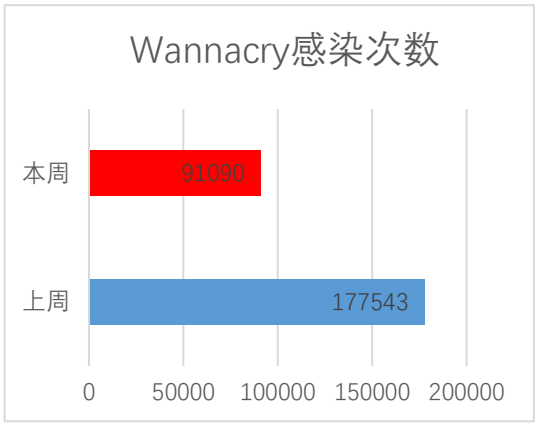
## 二、勒索软件受害者情况

### （一）Wannacry 勒索软件感染情况

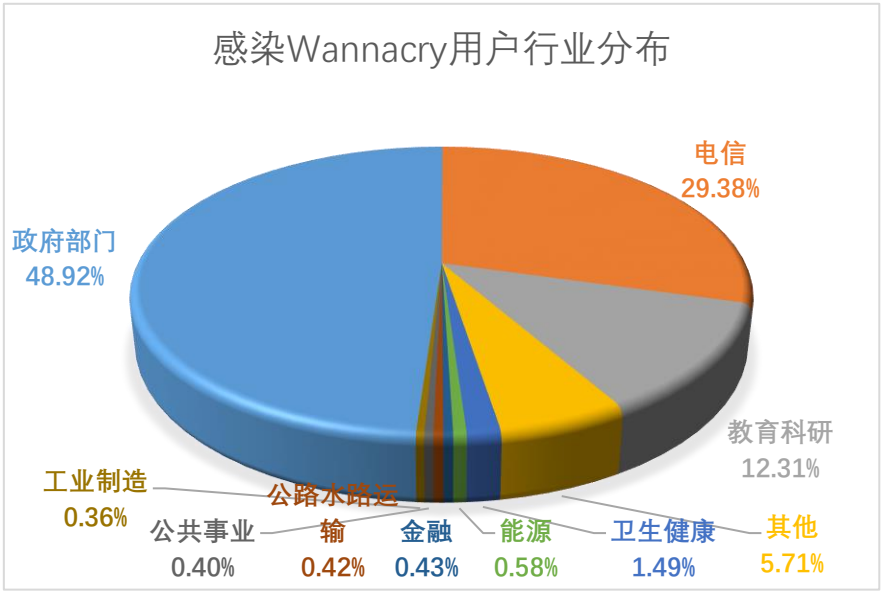
本周，监测发现 4272 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 2.1%，累计感染 91090 次，较上周下降 48.7%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



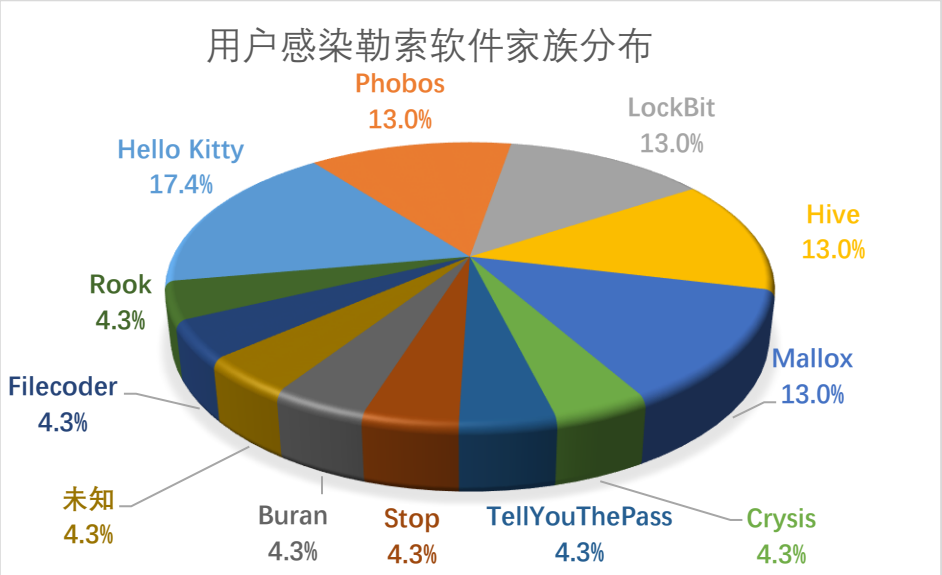




政府部门、电信、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

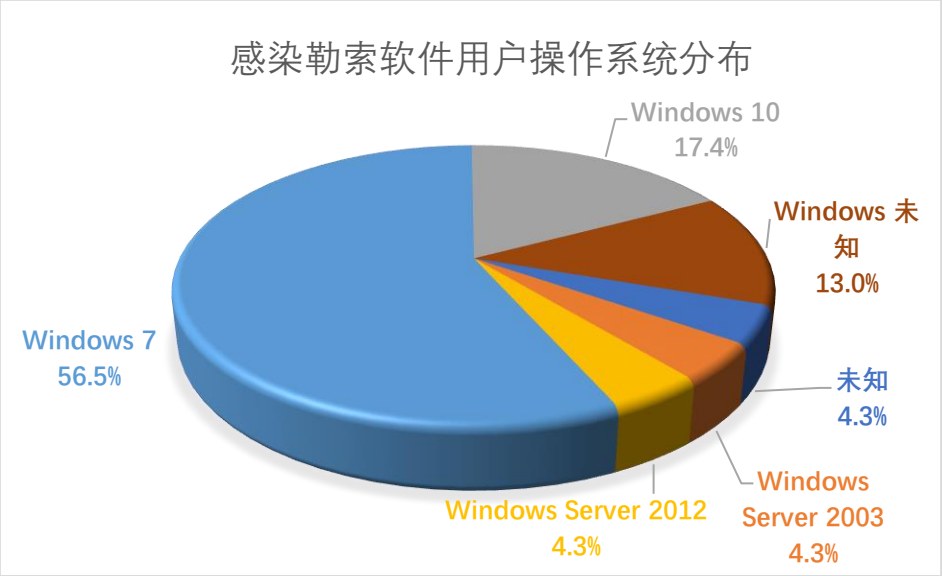



## （二）其它勒索软件感染情况

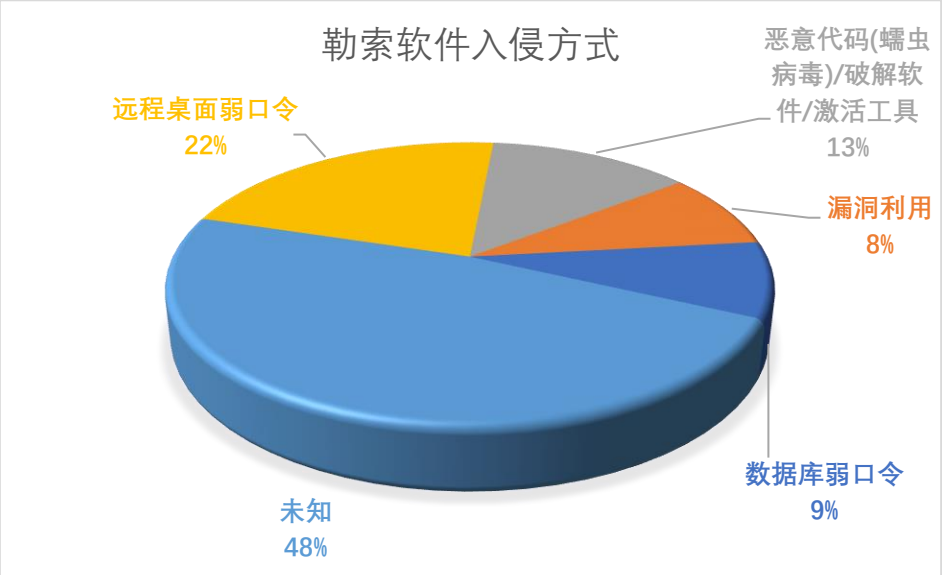
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 23 起非 Wannacry 勒索软件感染事件，较上周增长 27.8%，排在前三名的勒索软件家族分别为 Hello Kitty（17.4%）、Phobos（13.0%）和 LockBit（13.0%）。




本周，被勒索软件感染的系统中 Windows 7 系统占比较高，占到总量的 56.5%，其次为 Windows 10 系统和 Windows Server 2003 系统，占比分别为 17.4%和 4.3%，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，远程桌面弱口令和恶意代码(蠕虫病毒)/破解软件/激活工具占比较高，分别为 22%和 13%。Hello Kitty 勒索软件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

本周，工作组成员单位在自助监测和应急响应中未发现典型勒索软件攻击事件。

### （二） 国外部分

#### 1. 风力涡轮机公司 Nordex 遭受 Conti 勒索病毒攻击

Conti 勒索病毒声称对风力涡轮机巨头 Nordex 的攻击负责，此次攻击时间导致了 4 月初该公司被迫关闭其 IT 系统同时禁用了对其设备的远程访问权限。4 月 13 日，Nordex 发布了一份更新声明，解释说他们禁用托管涡轮机的远程访问是为了保护客户的资产。他们进一步表示：调查表明，攻击仅限于公司内部系统，并不涉及客户资产。

目前，Conti 团伙尚未开始泄露任何数据，这表明该公司可能正在与威胁参与者进行谈判，或者在攻击期间没有数据被盗。

## 四、威胁情报

**域名**

na47pldl5eoqxt42[.]onion

wqmfzni2nvbbpk25[.]onion

**IP**

139.60.161.228

139.60.161.56

91.208.52.149

185.70.184.8

193.34.166.165

193.34.166.214

193.34.166.189

193.34.166.181

193.34.167.240

193.34.166.92

193.34.167.230

**网址**

http://626cc2f81cc80610dc388270nxiooerw.rawloop[.]fit/nxiooerw

http://626cc2f81cc80610dc388270nxiooerw.knewpen[.]space/nxiooerw

http://626cc2f81cc80610dc388270nxiooerw.billfun[.]uno/nxiooerw

http://626cc2f81cc80610dc388270nxiooerw.veryits[.]quest/nxiooerw

http://626cc2f81cc80610dc388270nxiooerw.amjblanypjy2tews4maivajjj7zhb4yxafhb
qv7yqzej3bjq4n3h2nyd[.]onion/nxiooerw

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv[.]gaplies.fit/kqqqefjv

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.gunfail[.]quest/kqqqefjv

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.ranmuch[.]space/kqqqefjv

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.raredoe[.]uno/kqqqefjv

http://3e54fc18ec08b8204c88866018e492b0kqqqefjv.hjew6l4r3hpgj7qiloum5j7jwq7q
3623v4fsbq5edbckeppeetpiihid[.]onion/kqqqefjv

**邮箱**

mallox@stealthypost.net

ironse2022@tutanota.com

2022blue@mailfence.com

sparemail@onionmail.org

**钱包地址**

1HMptiRyKZcsw2riV9afXMd88Fk4awVRfR

bc1qw5mzzfe0kduygtppk37sfhh45a5rezvjtsns7v