# 国家互联网应急中心（CNCERT/CC）

# 勒索软件动态周报

2022 年第 8 期（总第 16 期）　　2 月 19 日-2 月 25 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

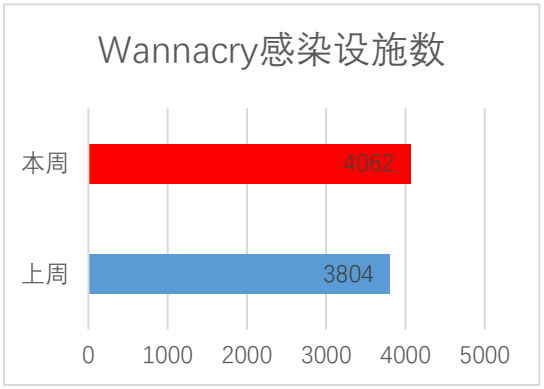
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1435559 个，监测发现勒索软件网络传播 1793 次，勒索软件下载 IP 地址 224 个，其中，位于境内的勒索软件下载地址 101 个，占比 45.1%，位于境外的勒索软件下载地址 123 个，占比 54.9%。

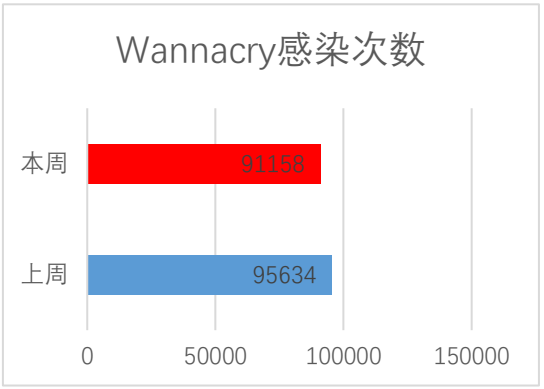
## 二、勒索软件受害者情况

### （一）Wannacry 勒索软件感染情况

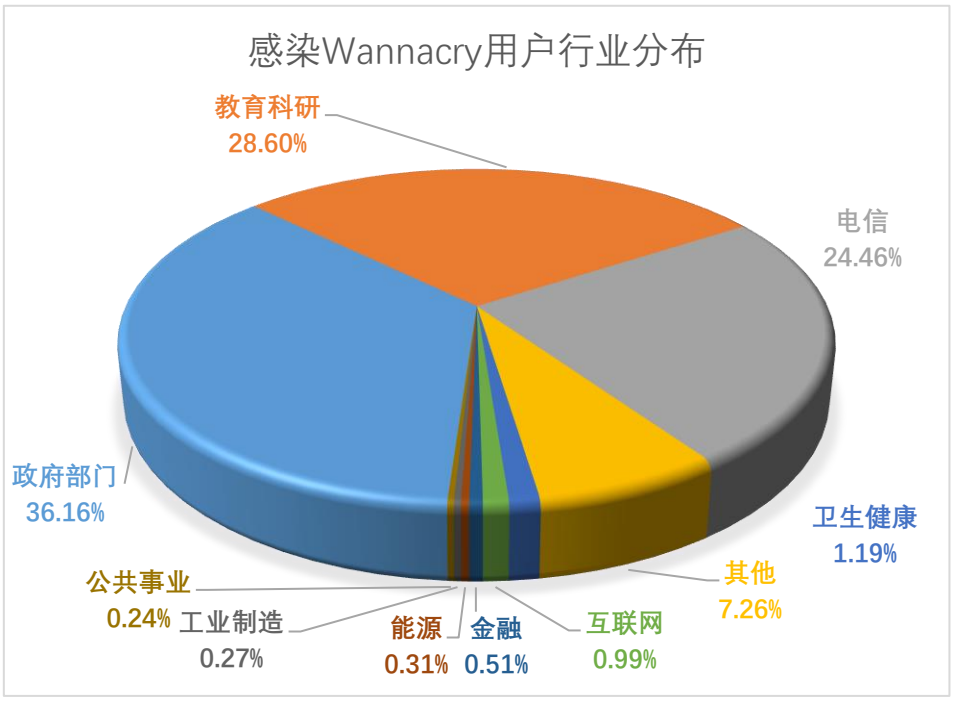
本周，监测发现 4062 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 6.8%，累计感染 91158 次，较上周下降 4.7%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



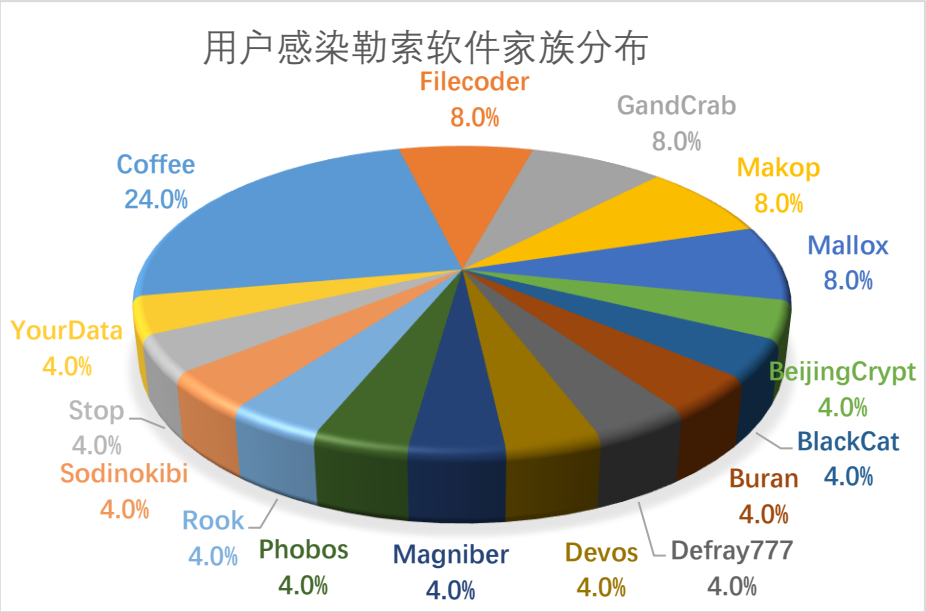




政府部门、教育科研、电信、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

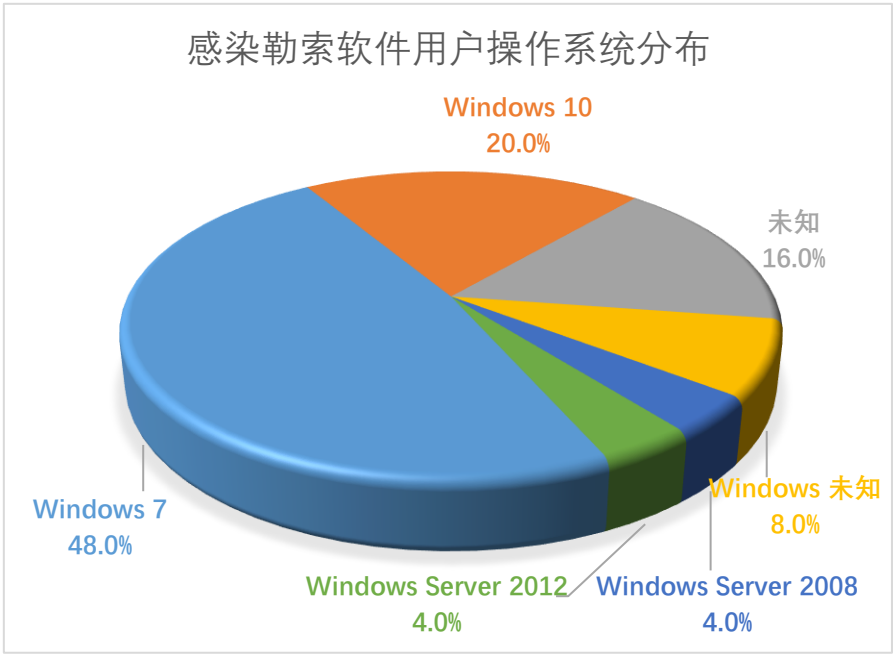



（二）其它勒索软件感染情况

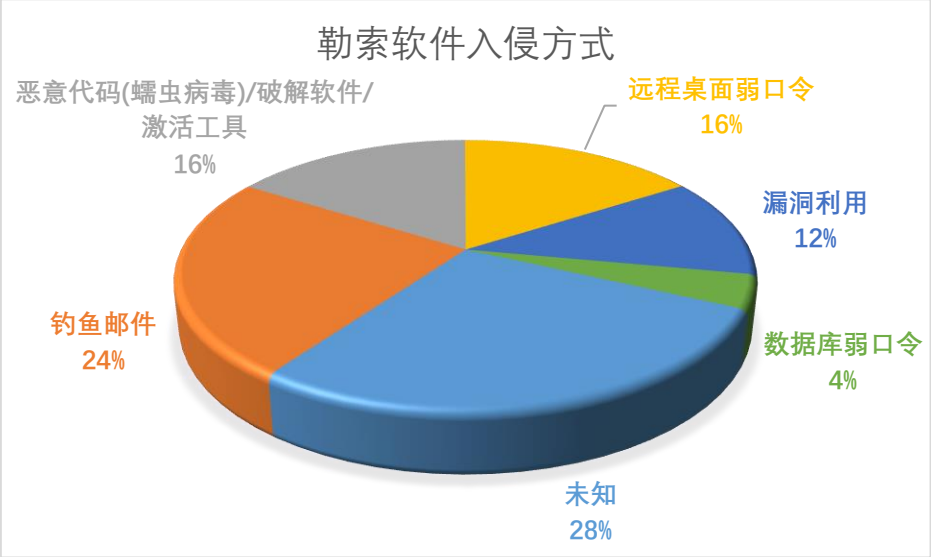
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 25 起非 Wannacry 勒索软件感染事件，较上周上升 13.6%，排在前三名的勒索软件家族分别为 Coffee（24%）、Makop（8%）和 GandCrab（8%）。




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 48%，其次为 Windows 10 系统，占比为 20%，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，钓鱼邮件和恶意代码(蠕虫病毒)/破解软件/激活工具占比较高，分别为 24%和 16%。Coffee 勒索软件利用钓鱼邮件和恶意代码频繁攻击我国用户，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、浙江某高校办公终端感染 Coffee 勒索软件

本周，工作组成员应急响应了浙江某高校办公终端感染 Coffee 勒索软件事件。攻击者通过发送钓鱼邮件诱使该高校教师点击邮件附件，进而植入勒索软件，随后对受害者的办公终端上的文件加密并索要赎金。

此事件中，攻击者通过钓鱼邮件传播勒索软件，建议用户加强网络安全意识，不下载来源不明的邮件附件，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

### （二） 国外部分

#### 1、物流和货运巨头 Expeditors 遭受勒索软件攻击

总部位于美国西雅图的物流和货运公司 Expeditors International 近日遭受勒索软件攻击，导致该组织关闭其全球大部分业务。Expeditors 在声明中表示其 IT 业务系统已几乎全部关闭，

业务能力受到较大限制，包括但不限于货物运输管理、客户管理和海关及配送管理等。该企业正在努力恢复其 IT 系统，但目前仍无法评估何时恢复正常运营。

## 四、威胁情报

**域名**

noc[.]social

bigblog[.]at

**IP**

93.190.143.101

**网址**

http://d47004803a3cae90b6a8dca8c6b80800vtoapyro.raredoe[.]uno/vtoapyro

http://d47004803a3cae90b6a8dca8c6b80800vtoapyro.gunfail[.]quest/vtoapyro

http://d47004803a3cae90b6a8dca8c6b80800vtoapyro.ranmuch[.]space/vtoapyro

http://d47004803a3cae90b6a8dca8c6b80800vtoapyro.gaplies[.]fit/vtoapyro

http://d47004803a3cae90b6a8dca8c6b80800vtoapyro.hjew6l4r3hpgj7qiloum5j7jwq7q3623v4fsbq5edbckeppeetpiihid[.]onion/vtoapyro

http://4e40baf8daf43600ba78amkciclkst.hjew6l4r3hpgj7qiloum5j7jwq7q3623v4fsbq5edbckeppeetpiihid[.]onion/mkciclkst

http://4e40baf8daf43600ba78amkciclkst.raredoe[.]uno/mkciclkst

http://4e40baf8daf43600ba78amkciclkst.ranmuch[.]space/mkciclkst

http://4e40baf8daf43600ba78amkciclkst.gaplies[.]fit/mkciclkst

http://4e40baf8daf43600ba78amkciclkst.gunfail[.]quest/mkciclkst

**邮箱**

newexploit@tutanota.com

ariakei@protonmail.com

JohnWilliams1887@gmx.com

suppmkp@msgsafe.io

suppmkp@tutanota.com

kardon@privatemail.com

**钱包地址**

1CjuWzBwgk5vhQhFxwprvYgwqYdbCi9GeZ

161aMxX4YEf3JVUysvpUP3wqJd2SrwL6PX

1C5QUhWxXZjHHGwH8BcyCNLighi5w8tszW

1GE6QouwG4HZQP1PBMfGzB68TVnJKoJAGe