

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 23 期（总第 31 期）

6 月 4 日-6 月 10 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

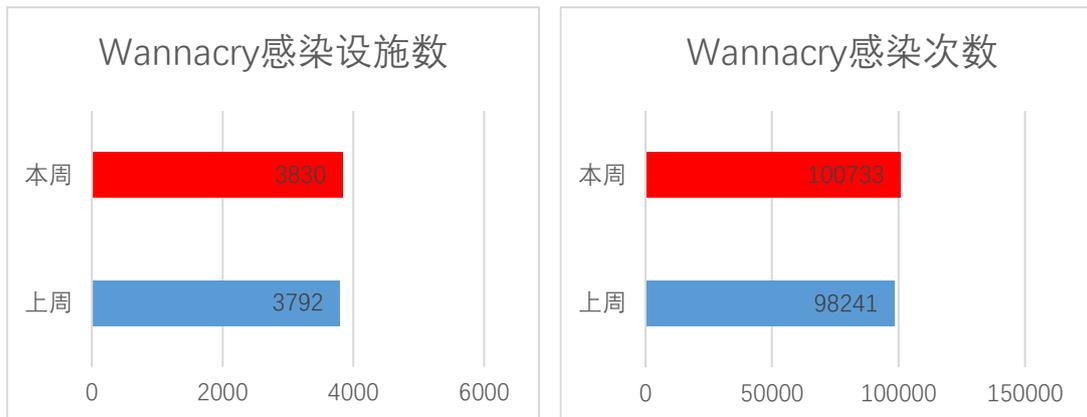
本周勒索软件防范应对工作组共收集捕获勒索软件样本 916707 个，监测发现勒索软件网络传播 372 次，勒索软件下载 IP 地址 22 个，其中，位于境内的勒索软件下载地址 14 个，占比 63.6%，位于境外的勒索软件下载地址 8 个，占比 36.4%。

二、勒索软件受害者情况

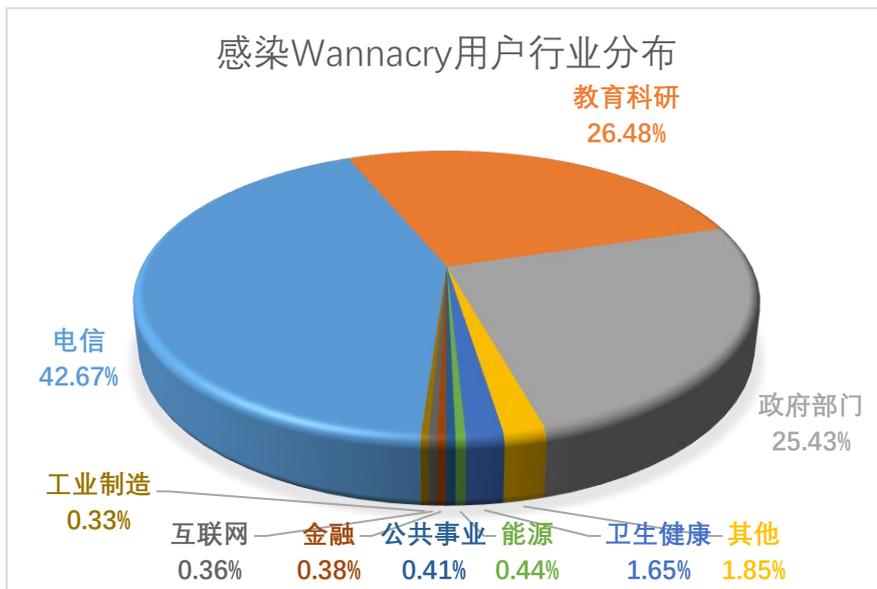
（一）Wannacry 勒索软件感染情况

本周，监测发现 3830 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 1.0%，累计感染 100733 次，较上周上升 2.5%。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、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。

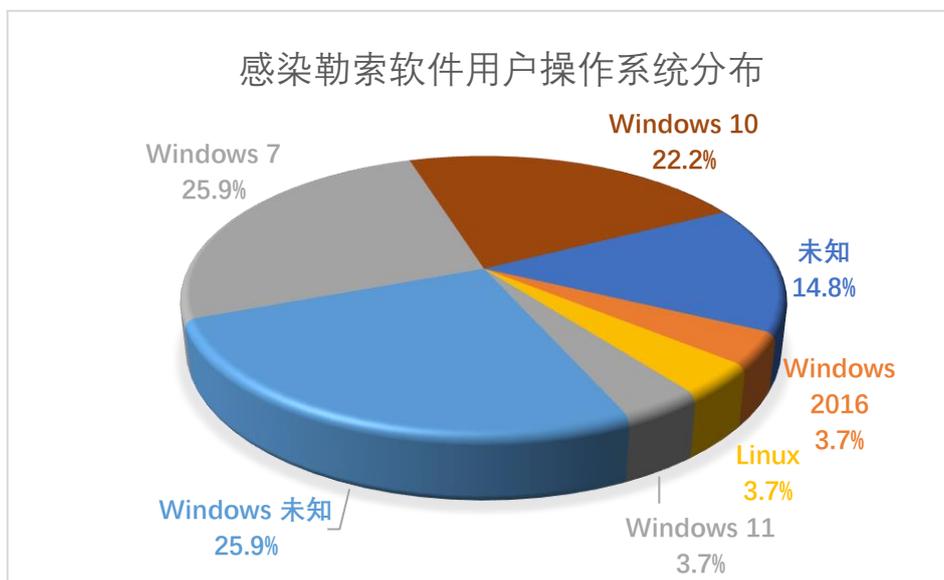


(二) 其它勒索软件感染情况

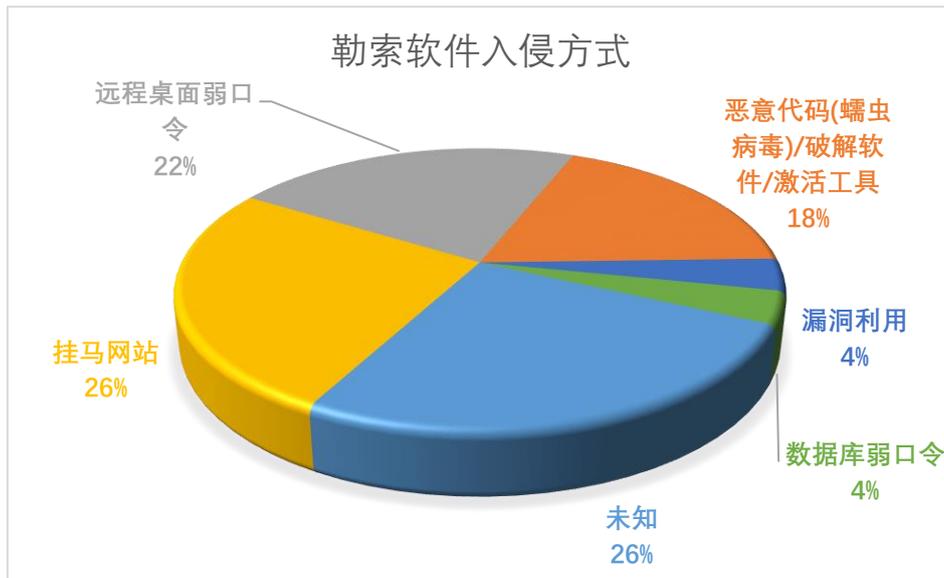
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 27 起非 Wannacry 勒索软件感染事件，较上周增长 145.5%，排在前三名的勒索软件家族分别为 Magniber(33.3%)、Hive(14.8%)和 Bart(7.4%)。



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 25.9%，其次为 Windows 10 系统和 Windows 2016 系统，占比分别为 22.2%和 3.7%，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，挂马网站和远程桌面弱口令占比较高，分别为 26%和 22%。Magniber 勒索软件通过挂马网站的方式频繁攻击我国用户，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. Lockbit 勒索软件团伙称入侵网络安全公司 Mandiant

近日，LockBit 勒索软件团伙已将网络安全公司 Mandiant 添加到其暗网泄密网站上发布的受害者名单中。该网络犯罪组织宣称从 Mandiant 窃取了 356841 份文件，并计划将这些文件泄露到网上。该团伙计划于 2022 年 6 月 6 日 22 时 35 分公布被盗文件。据称被窃取的文件似乎包含在一个名为“mandiantyellowpress.com.7z”的档案中。本月初，Mandiant 发布了一份报告，称网络犯罪团伙 Evil Corp 转向了 LockBit 2.0 勒索软件，以逃避制裁。

四、威胁情报

域名

iplogger[.]org

IP

23.106.160.188

20.82.210.154

88.221.144.179

208.95.112.1

网址

[http://f244d0484418d8e032dc12b824749220tvzcsynez.eatsoff\[.\]info/tvzcsynez](http://f244d0484418d8e032dc12b824749220tvzcsynez.eatsoff[.]info/tvzcsynez)

[http://f244d0484418d8e032dc12b824749220tvzcsynez\[.\]6gqs7qyjono2jdywd4w7lsyj](http://f244d0484418d8e032dc12b824749220tvzcsynez[.]6gqs7qyjono2jdywd4w7lsyj)

[2fsygsljqxp5z5km3cbhgv7vr7z4rpad\[.\]onion/tvzcsynez](http://f244d0484418d8e032dc12b824749220tvzcsynez[.]2fsygsljqxp5z5km3cbhgv7vr7z4rpad[.]onion/tvzcsynez)

[http://f244d0484418d8e032dc12b824749220tvzcsynez.myeight\[.\]info/tvzcsynez](http://f244d0484418d8e032dc12b824749220tvzcsynez.myeight[.]info/tvzcsynez)

[http://f244d0484418d8e032dc12b824749220tvzcsynez.catgos\[.\]info/tvzcsynez](http://f244d0484418d8e032dc12b824749220tvzcsynez.catgos[.]info/tvzcsynez)

[http://f244d0484418d8e032dc12b824749220tvzcsynez.joblate\[.\]info/tvzcsynez](http://f244d0484418d8e032dc12b824749220tvzcsynez.joblate[.]info/tvzcsynez)

[http://8a503c382e50ec50d0a406d03614cusxwlbx.hascuts\[.\]info/usxwlbx](http://8a503c382e50ec50d0a406d03614cusxwlbx.hascuts[.]info/usxwlbx)

<http://8a503c382e50ec50d0a406d03614cusxwlbx.xjvfi2lce4nriceqdhue4ftdrs7gongo>

[mm3ffpso3ng3znrwzbahekqd\[.\]onion/usxwlbx](http://8a503c382e50ec50d0a406d03614cusxwlbx.mm3ffpso3ng3znrwzbahekqd[.]onion/usxwlbx)

[http://8a503c382e50ec50d0a406d03614cusxwlbx.tiedlaw\[.\]info/usxwlbx](http://8a503c382e50ec50d0a406d03614cusxwlbx.tiedlaw[.]info/usxwlbx)

<http://ee7c18e09e2c4cf0321c3e104eecd430scrdnaash.6gqs7qyjono2jdywd4w7lsyj2fs>

[ygsljqxp5z5km3cbhgv7vr7z4rpad\[.\]onion/scrdnaash](http://ee7c18e09e2c4cf0321c3e104eecd430scrdnaash.ygsljqxp5z5km3cbhgv7vr7z4rpad[.]onion/scrdnaash)

[http://8a503c382e50ec50d0a406d03614cusxwlbx.pollof\[.\]info/usxwlbx](http://8a503c382e50ec50d0a406d03614cusxwlbx.pollof[.]info/usxwlbx)

邮箱

xats@privatemail.com

teamdecrypt@disroot.org

snowbox@tuta.io

helpforyou@gmx.com

钱包地址

1BdDpJbmPvbEJYctKPEwVP8B9RginigTJw

1HgfuEWn7VpTmwXpt6EkCtUEob5SCxkrPe

19LNKq1c8nACRgMJMHbKS2y6LdQiP9ewbx

bc1qwtj9y4zj52aa58thkfsaw6v9hj944su0xj8da2