国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 50 期（总第 58 期）　　12 月 10 日-12 月 16 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

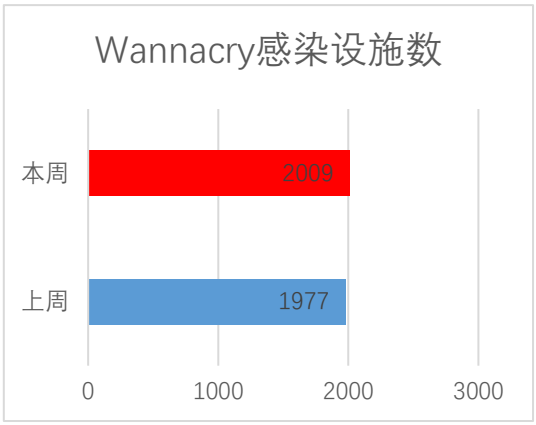
本周勒索软件防范应对工作组共收集捕获勒索软件样本 342810 个，监测发现勒索软件网络传播 198 次，勒索软件下载 IP 地址 38 个，其中，位于境内的勒索软件下载地址 10 个，占比 26.3%，位于境外的勒索软件下载地址 28 个，占比 73.7%。

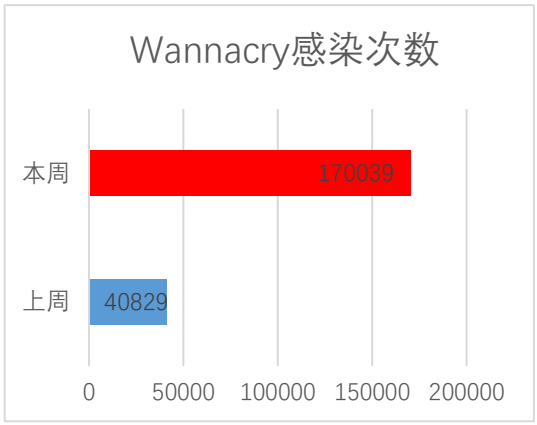
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

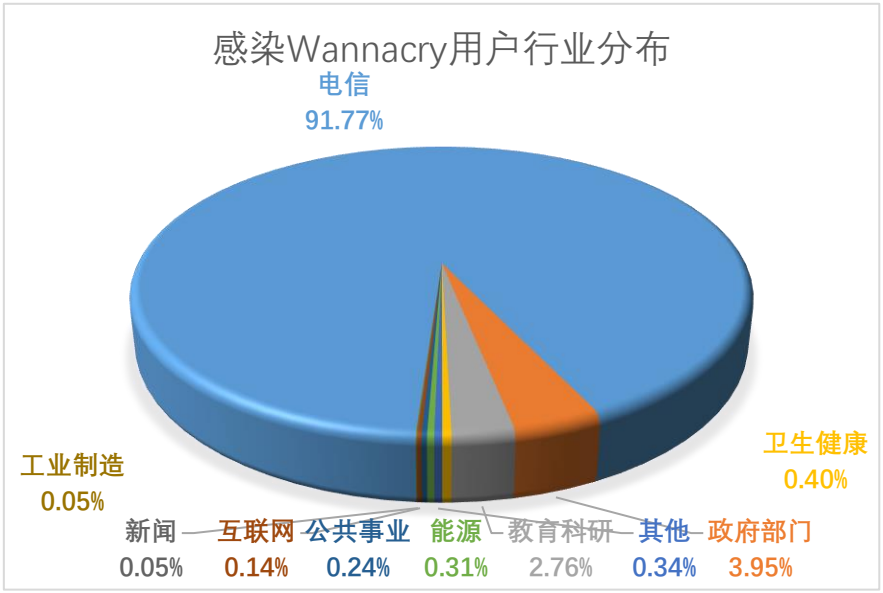
本周，监测发现 2009 起我国单位设施感染 Wannacry 勒索软件事件，较上周增长 1.3%，累计感染 170039 次，较上周增长 316.5%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



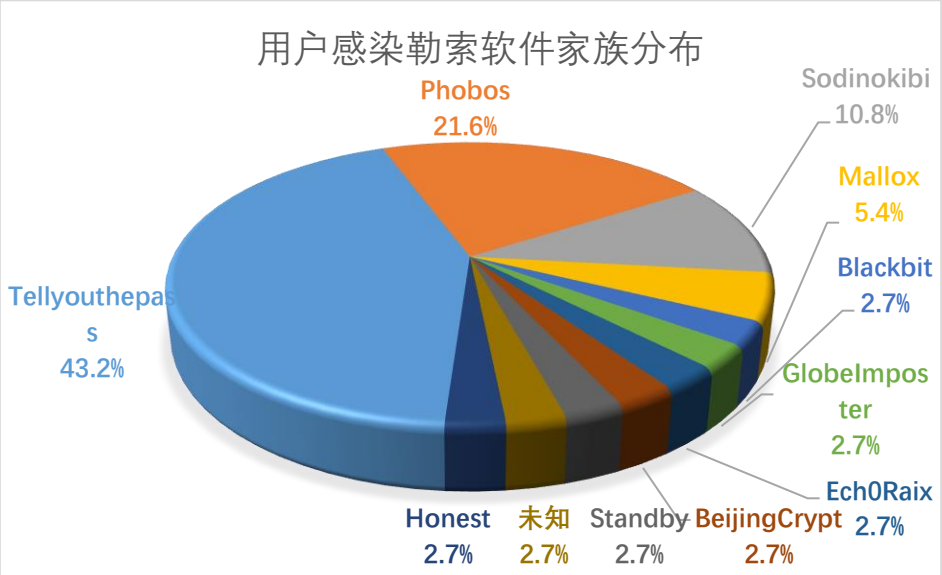


电信、政府部门、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

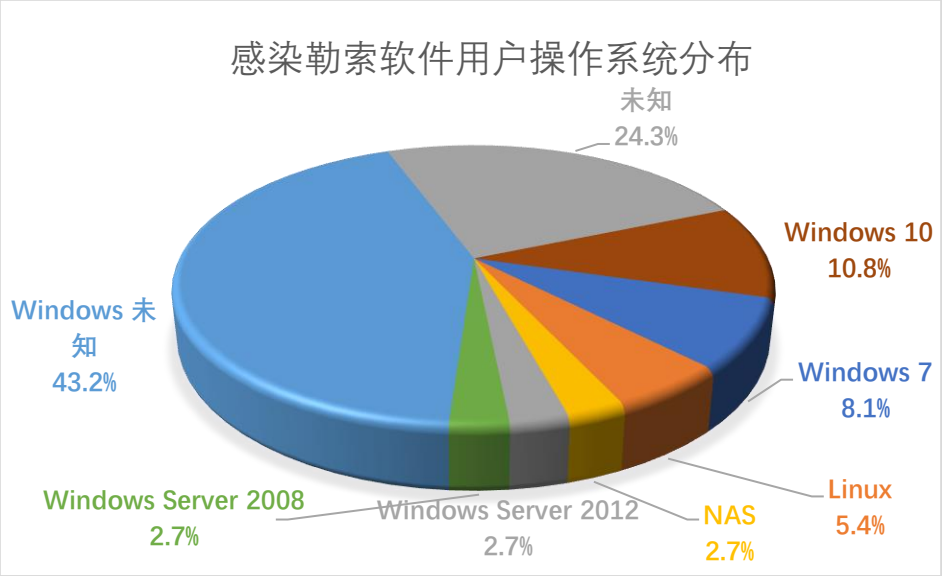


（二）其它勒索软件感染情况

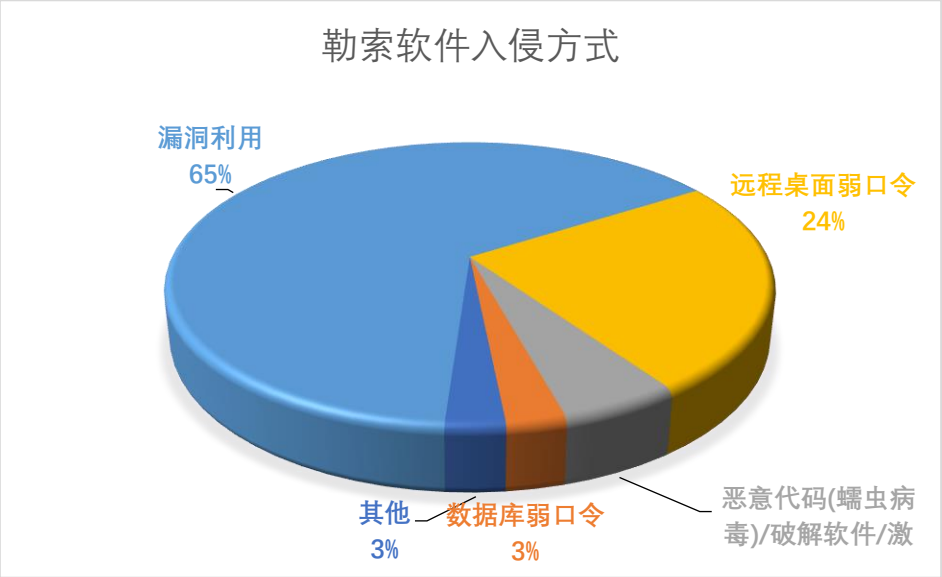
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 37 起非 Wannacry 勒索软件感染事件，较上周增长 184.6%，排在前三名的勒索软件家族分别为 Tellyouthepass（43.2%）、Phobos（21.6%）和 Sodinokibi（10.8%）。



本周，被勒索软件感染的系统中 Windows 10 系统占比较高，占到总量的 10.8%，其次为 Windows 7 系统和 Linux 系统，占比分别为 8.1%和 5.4%，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，漏洞利用和远程桌面弱口令占比较高，分别为 65%和 24%。Tellyouthepass 勒索软件通过漏洞利用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

1.北京市某金融行业单位遭受勒索病毒攻击

本周，工作组成员应急响应了北京市某金融行业单位遭受勒索病毒攻击的安全事件。经工作人员排查，发现攻击者于近日利用用友 NC 反序列化漏洞攻击成功，并上传 webshell，后续对服务器文件进行加密，造成应用无法正常运行。对设备流量分析，未发现其他内网攻击痕迹。

近日，攻击者利用用友NC反序列化漏洞，对我国企业频繁攻击，造成了巨大的安全威胁。建议企业有针对性的进行安全排查，主动发现目前所用系统、应用存在的安全隐患。

2.江苏省某生活服务业单位遭受勒索病毒攻击

本周，工作组成员应急响应了江苏省某生活服务业单位服务器遭受 Blackbit 变种勒索病毒攻击的事件。经工作人员对设备日志、防火墙 NAT 配置等信息进行排查，发现服务器对外开放了 3389 端口，攻

击者通过 RDP 登录服务器，并释放勒索病毒，随后删除记录。

建议企业有效加强访问控制 ACL 策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员 IP 可对管理端口进行访问，如 FTP、数据库服务、远程桌面等管理端口。

（二） 国外部分

1. LockBit 声称攻击加利福尼亚财政部

12 月 12 日，LockBit 勒索软件团伙在其泄露网站上发布消息称，他们入侵了加利福尼亚州财政部并窃取了其数据库、机密数据、财务文件和 IT 文件等多种数据。为了证明他们的说法，黑客发布了几张据称是从加州财政部系统中窃取的文件截图。此外，黑客还发布了目录和存储文件数量的截图。属性框显示了 114000 多个文件夹中超过 246000 个文件——总计大小为 75.3GB 的数据。LockBit 的数据泄露网站同时声称要在 12 月 24 日之前收到赎金，否则将公布所有文件。

四、威胁情报

IP

94.242.61.186

域名

vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad[.]onion

Qu5dci2k25x2imgki2dbhcwegqqsqsrjj5d3ugcc5kpsgbtj2psaedqd[.]onion

gunyhng6pabzcurl7ipx2pbmjxpvqnu6mxf2h3vdeenam34inj4ndryd[.]onion

Wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd[.]onion

网址

http://application-api.xyz/api/index[.]php