国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 51 期（总第 59 期）　　12 月 17 日-12 月 23 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

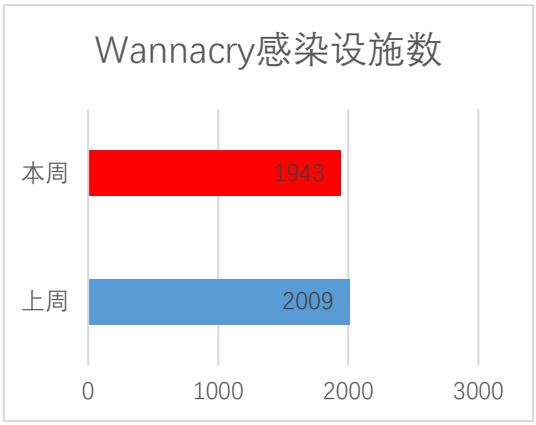
本周勒索软件防范应对工作组共收集捕获勒索软件样本 295551 个，监测发现勒索软件网络传播 154 次，勒索软件下载 IP 地址 45 个，其中，位于境内的勒索软件下载地址 13 个，占比 28.9%，位于境外的勒索软件下载地址 32 个，占比 71.1%。

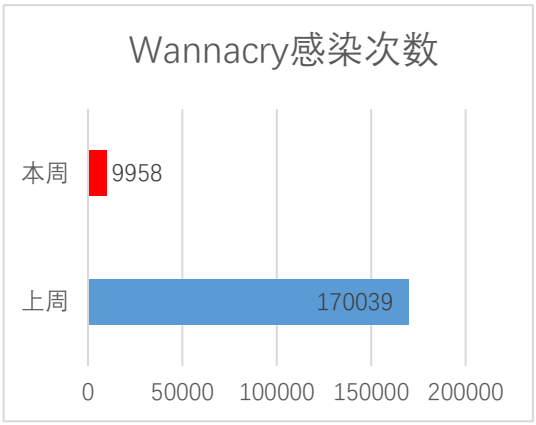
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

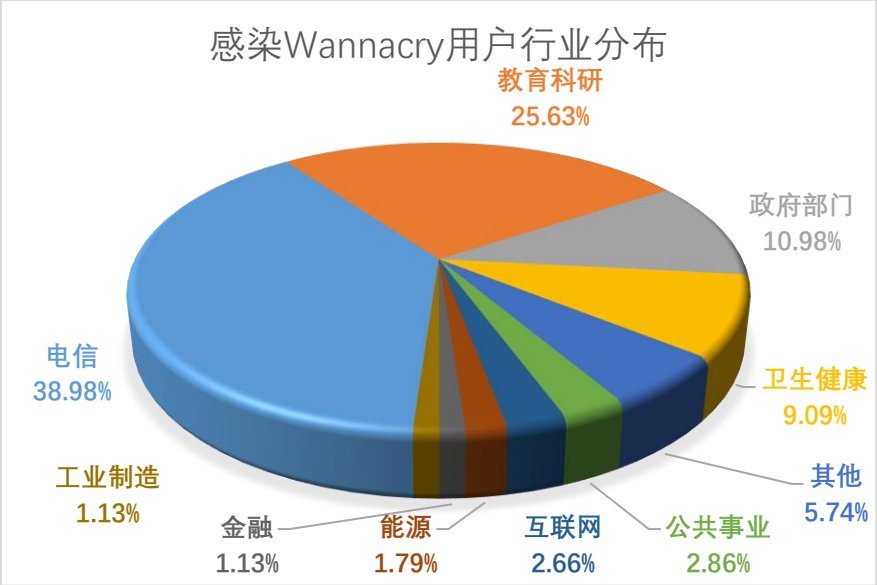
本周，监测发现 1943 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 3.3%，累计感染 9958 次，较上周降低 94.1%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



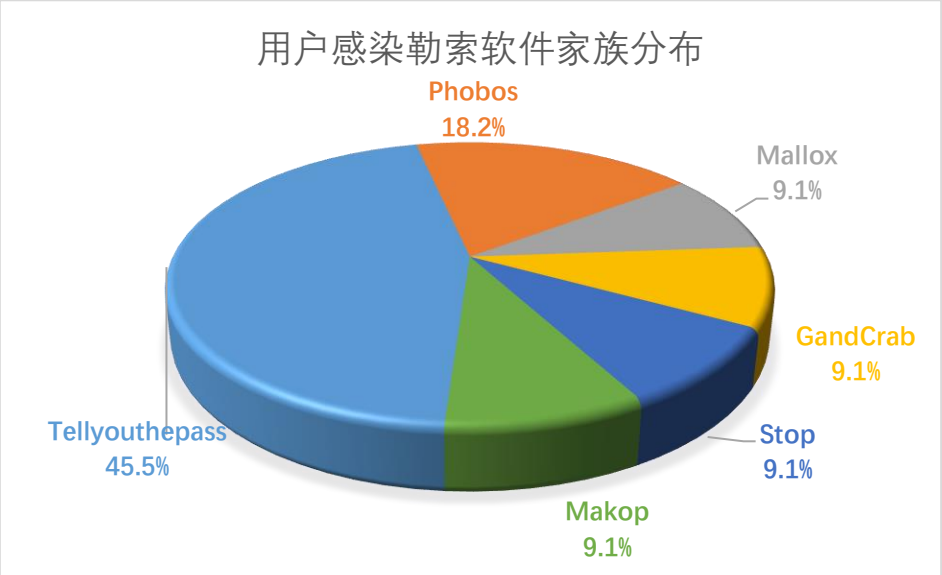


电信、教育科研、政府部门、卫生健康、公共事业行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

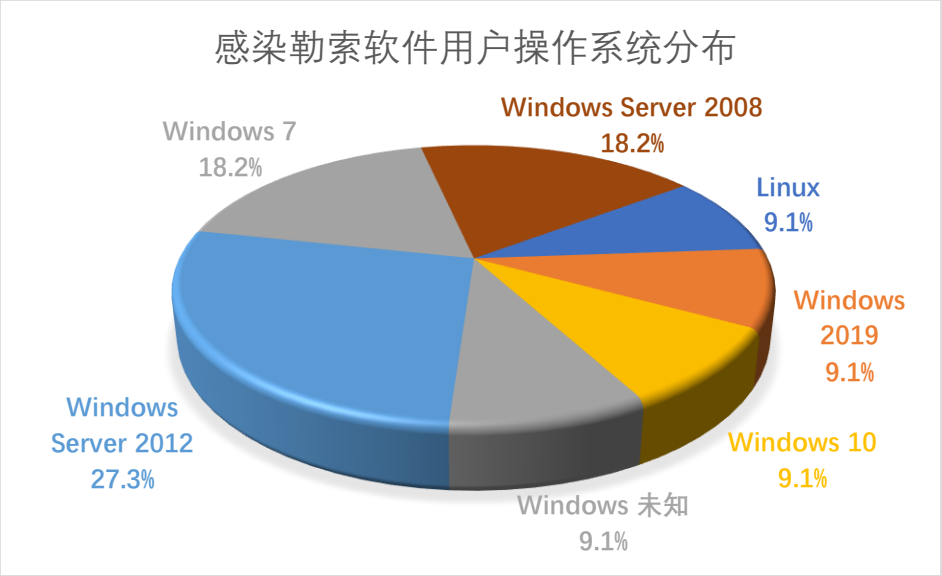


（二）其它勒索软件感染情况

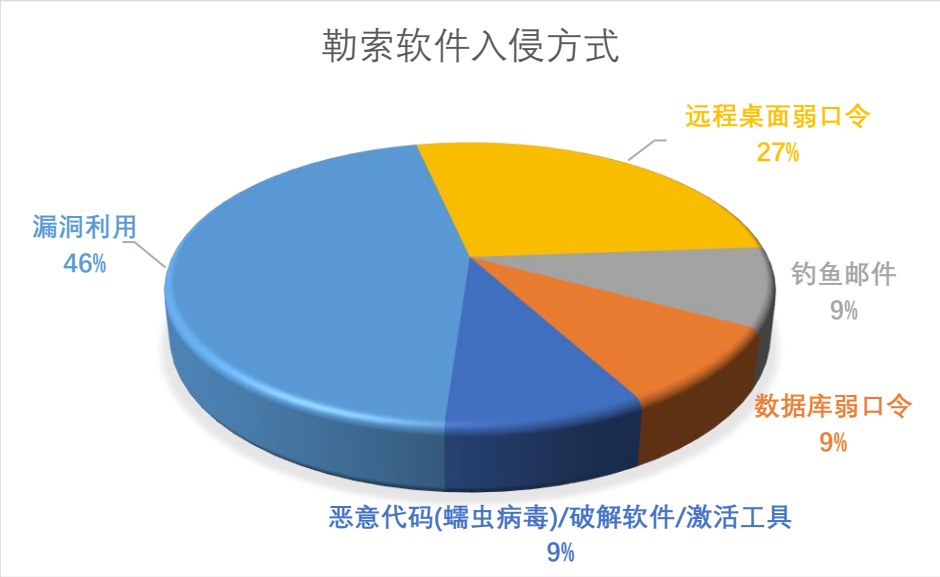
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 11 起非 Wannacry 勒索软件感染事件，较上周下降 70.3%，排在前三名的勒索软件家族分别为 Tellyouthepass（45.5%）、Phobos（18.2%）和 Mallox（9.1%）。



本周，被勒索软件感染的系统中 Windows Server 2012 系统占比较高，占到总量的 27.3%，其次为 Windows 7 系统和 Windows Server 2008 系统，占比分别为 18.2%和 18.2%，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 45%和 27%。Tellyouthepass 勒索软件通过远漏洞利用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

1.湖北省某企业遭受 Phobos 勒索病毒攻击

本周，工作组成员应急响应了湖北省某企业服务器被攻击的安全事件。经工作人员对设备日志等信息的排查后发现，两个分别来自美国纽约以及俄罗斯莫斯科的境外 IP 成功登录过该服务器，且存在大量的暴力破解情况约 2 万余次，由此推断攻击者是通过远程桌面的 3389 端口，RDP 爆破的方式登录服务器之后横向传播，从而实现加密。

建议企业的服务器等设备关闭 RDP 等相关运维端口，防止被攻击者暴力破解，另外要修改日志的保存时长，建议是 6 个月以上，以便于攻击发生时进行溯源排查。

2.北京某企业遭受勒索病毒攻击

本周，工作组成员应急响应了北京市某企业的服务器遭受勒索病毒攻击的安全事件。该服务器为一台 NC 服务器，通过对 AILPHA 原

始流量日志的分析，发现某个来自中国香港的 IP 于近日通过用友 NC 的反序列化漏洞对该公司的用友 NC 服务器发起攻击。攻击者通过该漏洞上传了 webshell 文件，随后释放勒索病毒，对服务器文件进行加密。

近日，由用友 NC 反序列化漏洞导致的勒索攻击事件频出不穷，建议企业将 NC 服务器通过防火墙、VPN 等方式隔离，使得外部网络无法直接访问 NC 服务器，同时建立应用程序访问控制策略，对应用程序访问设定访问权限。

（二） 国外部分

1. 哥伦比亚能源供应商 EPM 遭 BlackCat 勒索软件攻击

Sobeys 是加拿大两家全国性杂货零售商之一， 在周一发布的新闻稿中，Sobeys 的母公司 Empire 透露，虽然其杂货店仍在营业，但一些服务受到了这一全公司范围内的 IT 问题的影响。根据员工报告，受影响的 Sobeys 商店的所有计算机都被锁定，销售点 (POS) 和支付处理系统仍然在线并工作，因为它们设置为在单独的网络上工作。

虽然该公司尚未披露任何将此次持续中断与网络攻击联系起来的信息，但当地媒体报道称，来自魁北克省和阿尔伯塔省的加拿大省级隐私监管机构已确认收到来自该零售商的“保密事件”通知。此外，根据媒体看到的赎金票据和谈判聊天记录，攻击者部署了 Black Basta 勒索软件有效负载来加密 Sobeys 网络上的系统。多个消息来源告诉媒体，袭击发生在周五晚些时候或周六早上。Sobeys 员工在网上分享的照片还显示了一张 Black Basta 赎金票据。

四、威胁情报

IP

64.185.227.156

域名

static.212.56.214.153.mldnet[.]com

whyers[.]io

网址

https://whyers.io/QWEwqdsvsf/ap[.]php