国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 52 期（总第 60 期）　　12 月 24 日-12 月 30 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

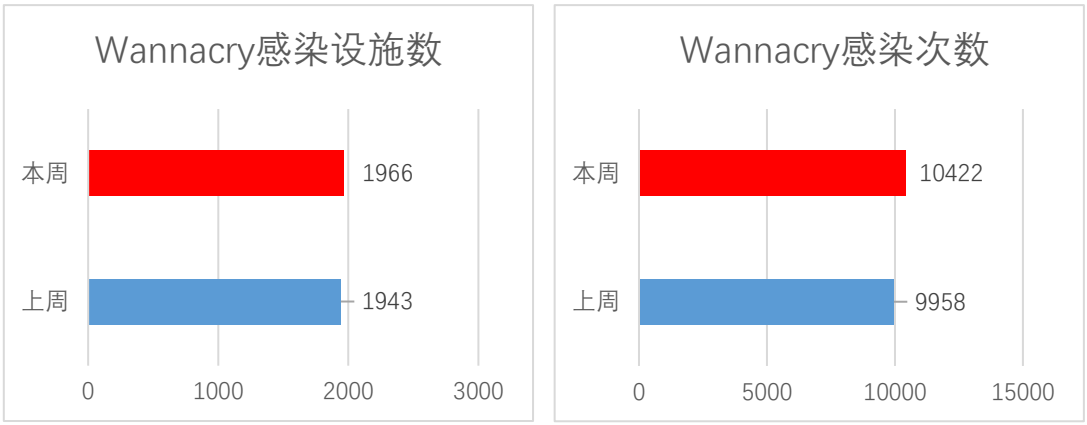
本周勒索软件防范应对工作组共收集捕获勒索软件样本 251326 个，监测发现勒索软件网络传播 139 次，勒索软件下载 IP 地址 40 个，其中，位于境内的勒索软件下载地址 13 个，占比 32.5%，位于境外的勒索软件下载地址 27 个，占比 67.5%。

二、勒索软件受害者情况

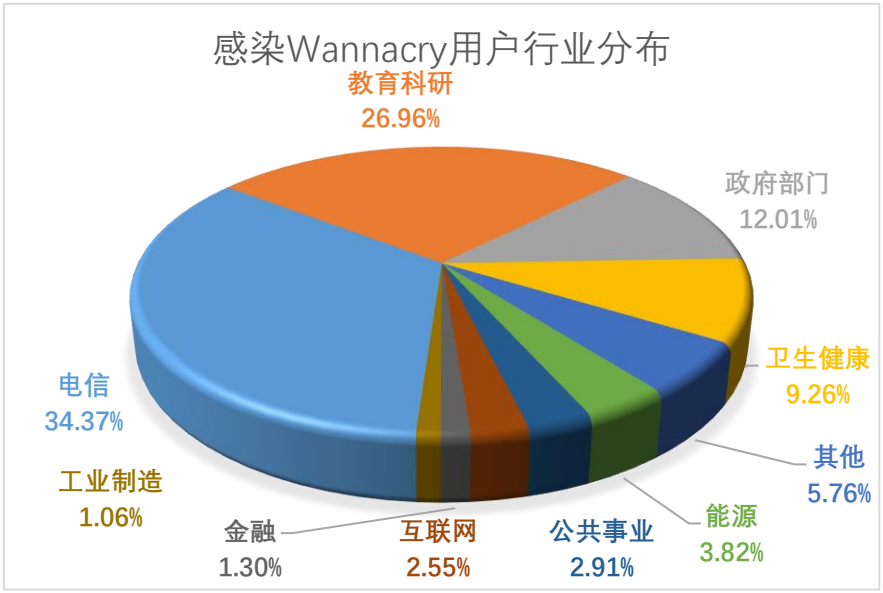
（一）Wannacry 勒索软件感染情况

本周，监测发现 1966 起我国单位设施感染 Wannacry 勒索软件事件，较上周增长 1.2%，累计感染 10422 次，较上周增长 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。

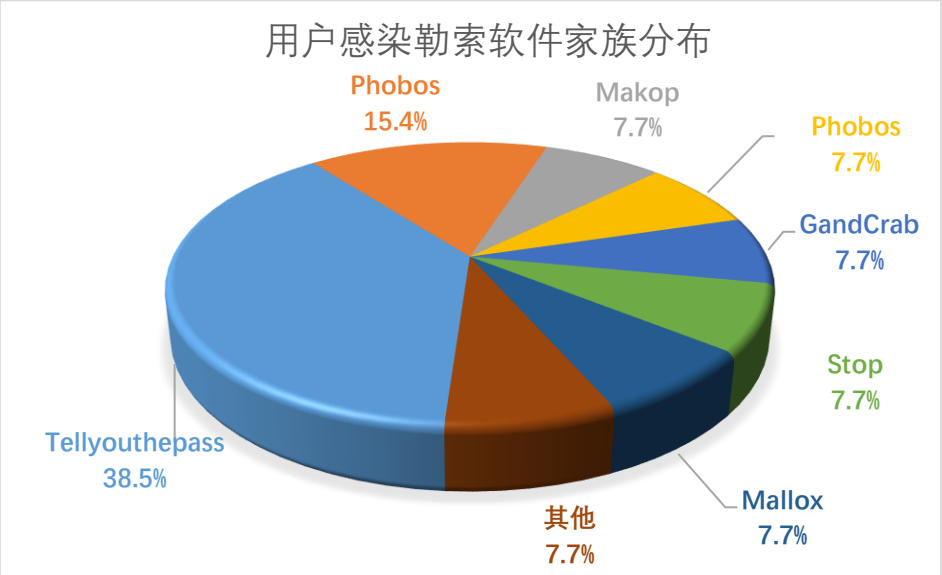


电信、教育科研、政府部门、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

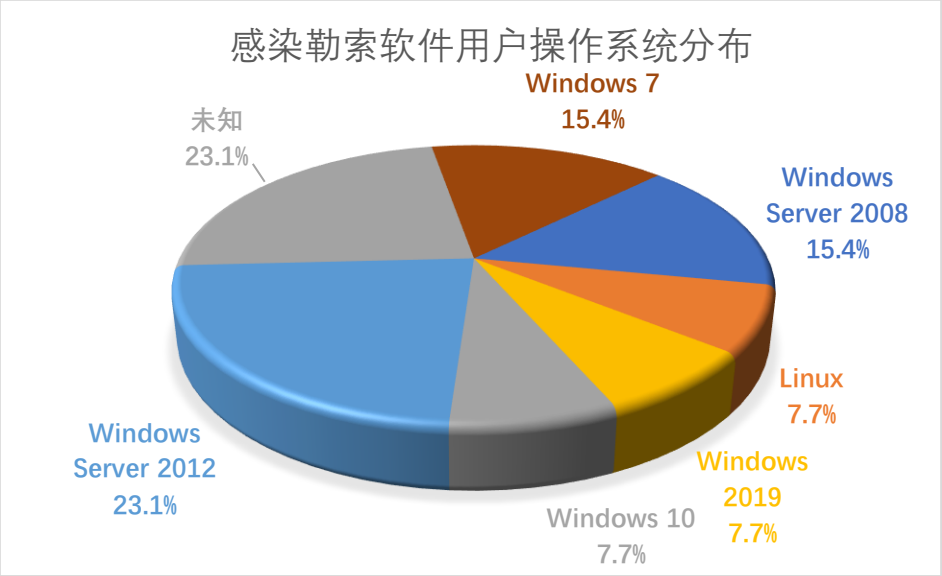


（二）其它勒索软件感染情况

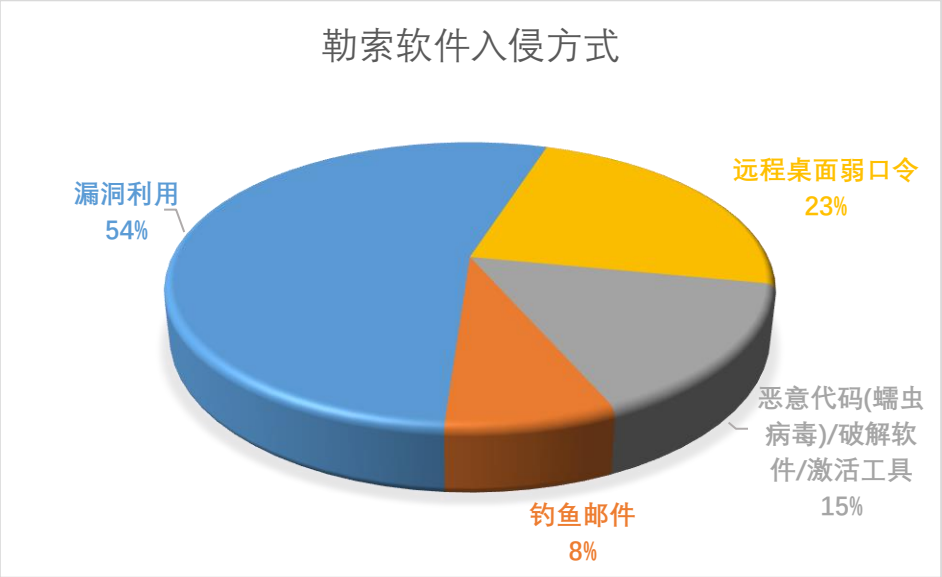
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 13 起非 Wannacry 勒索软件感染事件，较上周增长 18.2%，排在前三名的勒索软件家族分别为 Tellyouthepass（38.5%）、Phobos（15.4%）和 Makop（7.7%）。



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 23.1%，其次为 Windows 7 系统和 Windows Server 2008 系统，占比分别为 15.4%和 15.4%，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 54%和 23%。Tellyouthepass 勒索软件通过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.江西省某制造业公司遭受 Pipikaki 勒索病毒攻击

本周，工作组成员应急响应了江西省某制造业公司遭受勒索病毒攻击的安全事件。本次事件中，共有 50 余台服务器感染勒索病毒，经工作人员对部分受害服务器的系统日志进行分析，发现攻击者首先获取到了域管理员权限，通过公司的一台服务器远程控制受害服务器，再利用受害服务器作为跳板，进一步利用域管理账号 RDP 远程服务、Windows 共享服务漏洞对其他服务器投递扩散勒索病毒。在每次投递勒索病毒前，先利用黑客工具破坏掉本地的杀毒软件及其他的系统保护机制，以此达到实施勒索加密的过程不会被中断的目的。

建议企业对服务器等设备部署统一病毒防护软件，通过限制异常登录行为、开启防爆破功能、禁用或限用危险端口、防范漏洞利用等方式，提高系统安全基线。

（二） 国外部分

1. Royal 勒索软件声称攻击了 Intrado 通信公司

Royal 勒索软件团伙声称对 12 月 27 日针对电信公司 Intrado 的网络攻击负责。虽然 Intrado 尚未透露有关这起事件的任何信息，但消息人士本月初曾透露袭击始于 12 月 1 日，最初的赎金要求为 6000 万美元。据称，Royal 勒索团伙从 Intrado 的系统中窃取到了一些敏感数据，并威胁称除非该公司支付赎金，否则将在其数据泄露网站上发布这些数据。

据攻击者声称，他们从受到破坏的 Intrado 设备中获取了内部文件、护照和员工驾照。尽管勒索软件团伙尚未泄露任何据称从 Intrado 网络中窃取的文件，但他们共享了一个 52.8MB 的档案，其中包含护照、商业文件和驾驶执照的扫描副本作为提升自身声明可信度的证据。

四、威胁情报

IP

145.14.144.37

145.14.145.134

34.160.111.145

64.185.227.156

域名

000webhostapp[.]com

fredstat.000webhostapp[.]com

jostat.mygoodsday[.]org

网址

http://crl.comodoca.com/AAACertificateServices[.]crl