国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 13 期（总第 21 期）　　3 月 26 日-4 月 1 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

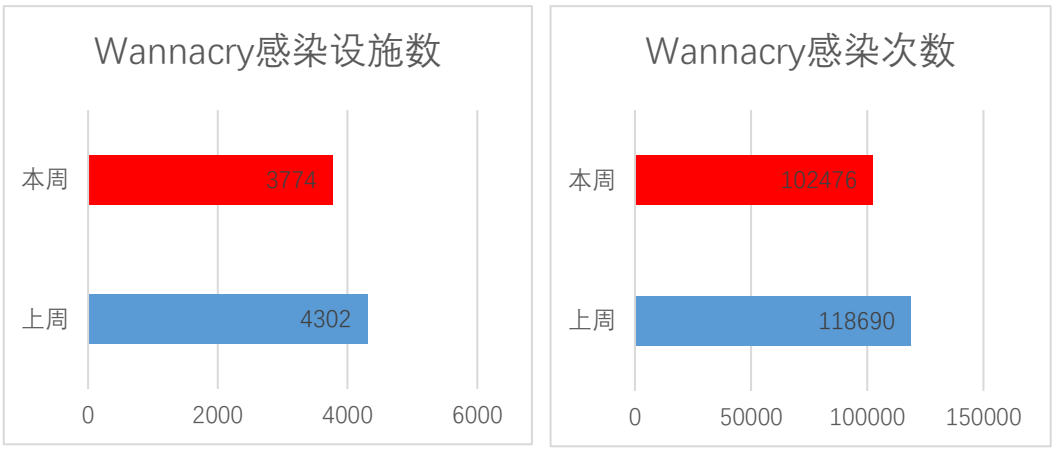
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1132823 个，监测发现勒索软件网络传播 391022 次，勒索软件下载 IP 地址 48 个，其中，位于境内的勒索软件下载地址 19 个，占比 39.6%，位于境外的勒索软件下载地址 29 个，占比 60.4%。

二、勒索软件受害者情况

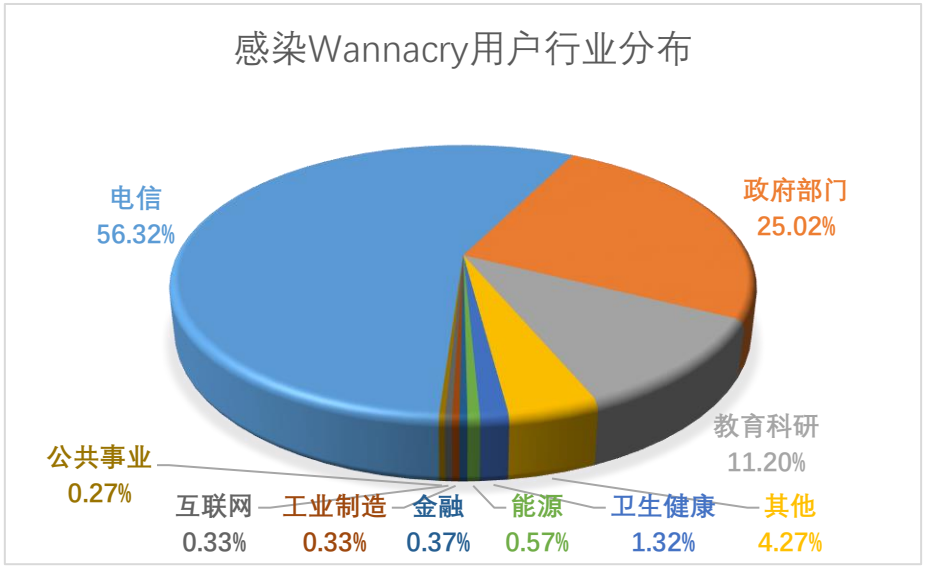
（一）Wannacry 勒索软件感染情况

本周，监测发现 3774 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 12.3%，累计感染 102476 次，较上周下降 13.7%。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。

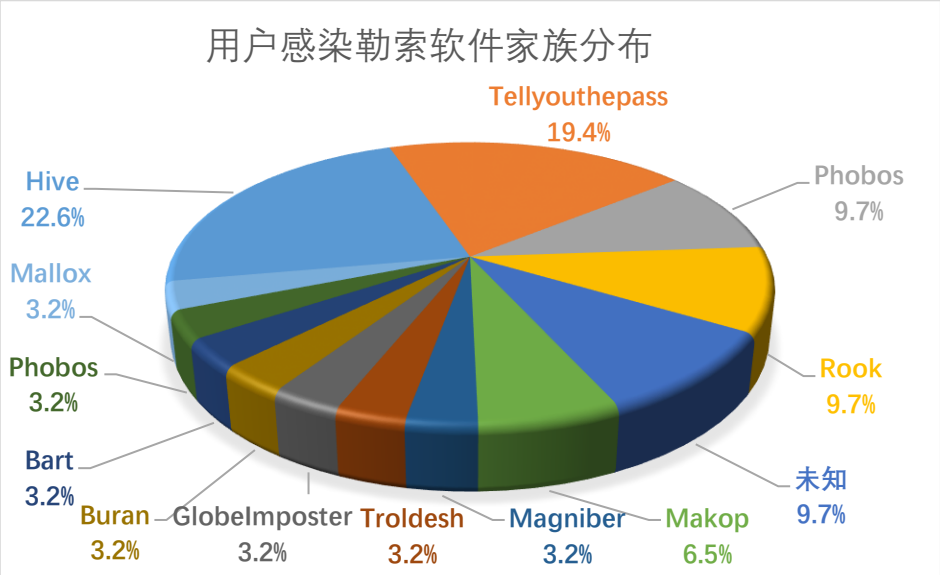


电信、政府部门、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

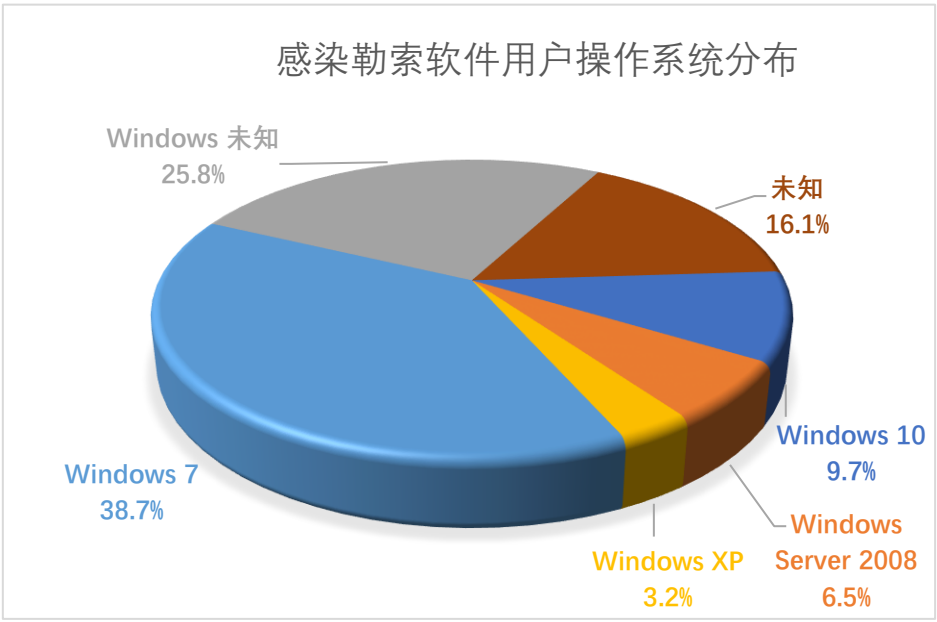


（二）其它勒索软件感染情况

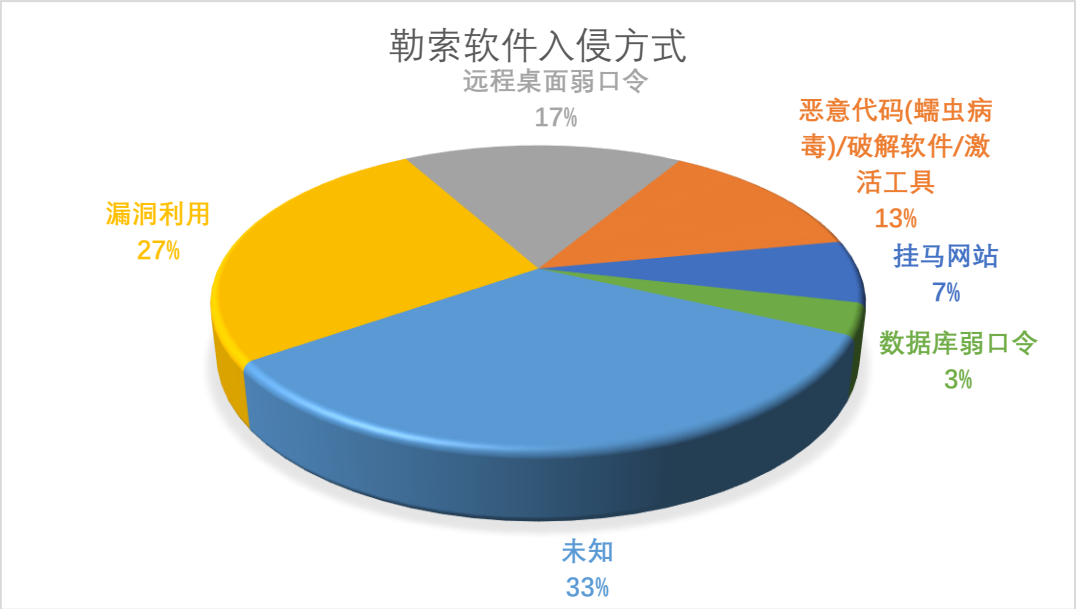
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 31 起，非 Wannacry 勒索软件感染事件，较上周下降 16.2%，排在前三名的勒索软件家族分别为 Hive（22.6%）、Tellyouthepass（19.4%）和 Phobos（9.7%）。



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 38.7%，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 9.7%和 6.5%，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 27%和 17%。Tellyouthepass 勒索软件通过 Log4j 漏洞频繁攻击我国用户，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、重庆某企业遭勒索病毒攻击

本周，工作组成员应急响应了广东某企业遭受勒索病毒攻击事件。攻击者通过票务系统应用服务器攻击票务系统数据库服务器，并加密了票务系统数据库服务器重要文件。根据分析人员初步判断，攻击者可能采取的是通过应用服务器的应用漏洞或数据库弱口令的问题，直接利用了 SQLserver 数据库管理员账号 sa 执行了 PowerShell 脚本运行勒索病毒。

近期勒索软件攻击我国企业的安全事件频发，企业应针对已上线的系统定期开展安全测试工作，同时加强日常管理技术人员的安全意识培训，相关服务器、系统、数据库的账号口令应设置为较复杂密码。

2、浙江某运营商遭勒索病毒攻击

本周，工作组成员应急响应了浙江某运营商遭受勒索软件攻击的安全事件。攻击者尝试进行 CVE-2021-44228 Apache Log4j2 远程代码

执行漏洞攻击的行为，但部分关键日志已被加密，无法判断是否利用成功。根据勒索信邮箱查询到该勒索病毒为 TellYouThePass 勒索，且发现该勒索团伙近期多次使用 Log4j 漏洞攻击迹象，推测攻击者很可能利用 Log4j 漏洞，进行远程命令执行，部署远控木马，释放勒索病毒。

近期，Log4j 漏洞给我国的企业和用户带来巨大的安全威胁。企业应定期进行渗透测试工作，由专业的安全渗透服务工程师模拟黑客从外到内进行攻击，发现存在的安全隐患，如任意文件上传，弥补检测工具类的盲点。

（二） 国外部分

1、Shutterfly 被 Conti 勒索病毒攻击后遭数据泄露

在线零售和摄影平台 Shutterfly 公布了一起数据泄露事件，其声称此次事件是在遭到 Conti 勒索病毒攻击期间被后者窃取到了涉及员工信息的相关数据。

据 Shutterfly 披露，由于勒索病毒攻击，其网络于 2021 年 12 月 3 日遭到入侵。在勒索病毒攻击期间，攻击者将获得了对公司网络的访问权，并成功窃取到了其中的数据和文件。

Shutterfly 表示，攻击期间被盗的文件可能包含员工的个人信息，如员工的姓名、工资和薪酬信息以及 FMLA 休假或工人赔偿要求等信息。

四、威胁情报

域名

service-5inxpk6g-1304905614.gz.apigw.tencentcs[.]com

service-kibkxcw1-1305343709.bj.apigw.tencentcs[.]com

IP

103.146.179.89

1.15.80.102

175.178.62.140

84.32.188.238

网址

http://ea68181022e02a6080bc3e08lrqfqgwll.hemore[.]uno/lrqfqgwll

http://ea68181022e02a6080bc3e08lrqfqgwll.trapbe[.]quest/lrqfqgwll

http://ea68181022e02a6080bc3e08lrqfqgwll.hotgame[.]fit/lrqfqgwll

http://ea68181022e02a6080bc3e08lrqfqgwll.vansban[.]space/lrqfqgwll

http://ea68181022e02a6080bc3e08lrqfqgwll.3g5twxggjkc76oy6itmdvhliayffjfv23vg3rp372nn7ohfnnylfclid[.]onion/lrqfqgwll

http://061436882afc3ab05a4478488tjqvamoca.suredie[.]space/tjqvamoca

http://061436882afc3ab05a4478488tjqvamoca.o7wgk5cbzp7ecuiwwh5rkw5jsahwhfqc5v5itoebkzrpou2rfjck2dqd[.]onion/tjqvamoca

http://061436882afc3ab05a4478488tjqvamoca.pifour[.]uno/tjqvamoca

http://061436882afc3ab05a4478488tjqvamoca.tiesyou[.]sbs/tjqvamoca

http://061436882afc3ab05a4478488tjqvamoca.hitby[.]quest/tjqvamoca

邮箱

prismchigo@tutanota.com

KalajaTomorr@ctemplar.com

KalajaTomorr@firemail.cc

Bomani@Email.Com

jbomani@protonmail.com

lord_bomani@keemail.me