国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 29 期（总第 37 期）　　7 月 16 日-7 月 22 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

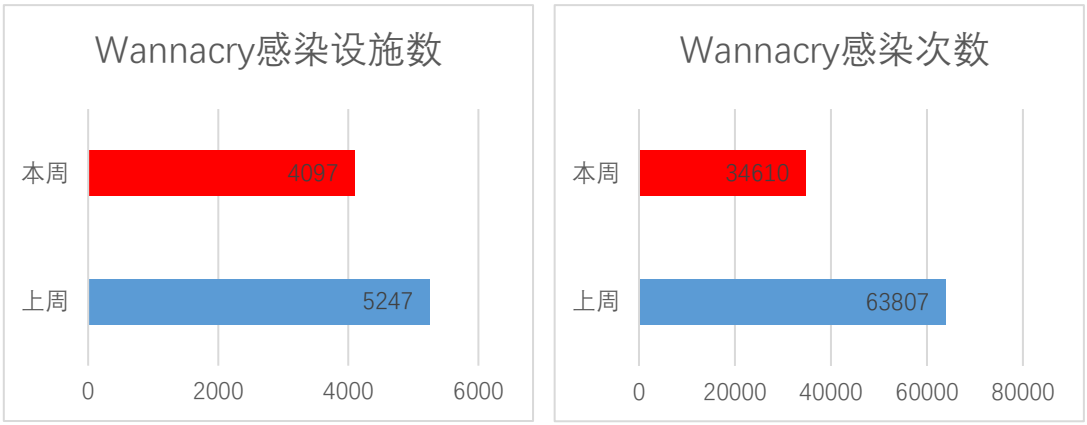
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1404897 个，监测发现勒索软件网络传播 76 次，勒索软件下载 IP 地址 22 个，其中，位于境内的勒索软件下载地址 13 个，占比 59.1%，位于境外的勒索软件下载地址 9 个，占比 40.9%。

二、勒索软件受害者情况

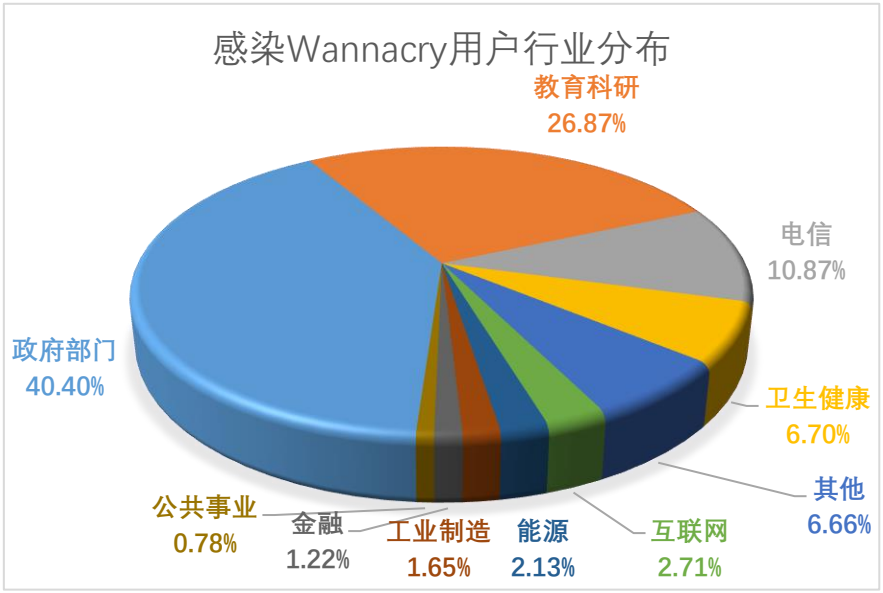
（一）Wannacry 勒索软件感染情况

本周，监测发现 4097 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 21.9%，累计感染 34610 次，较上周下降 45.8%。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。

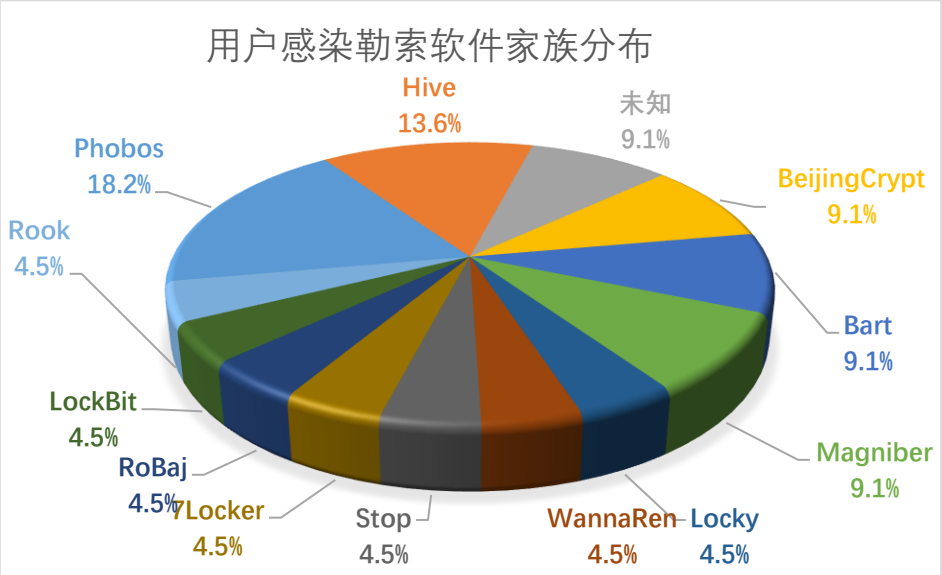


政府部门、教育科研、电信、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

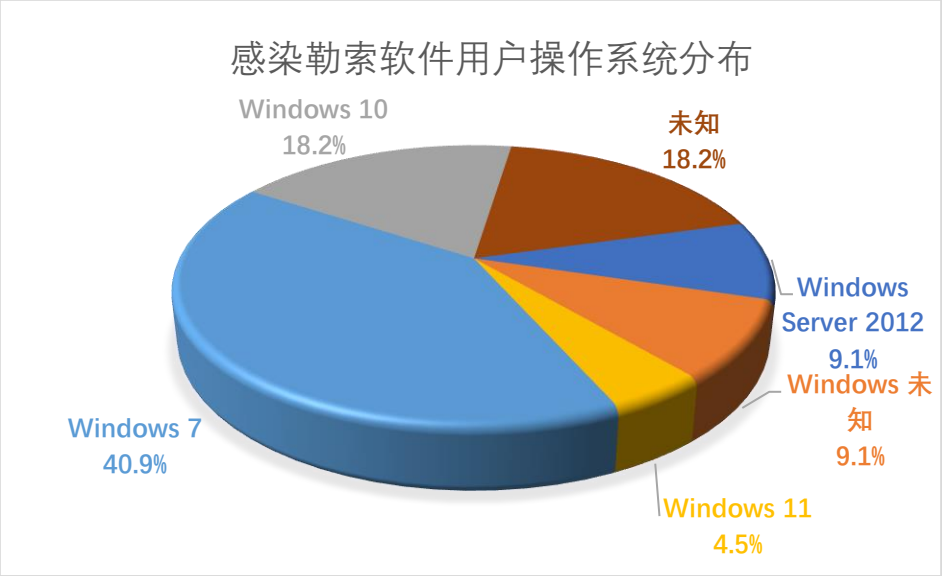


（二）其它勒索软件感染情况

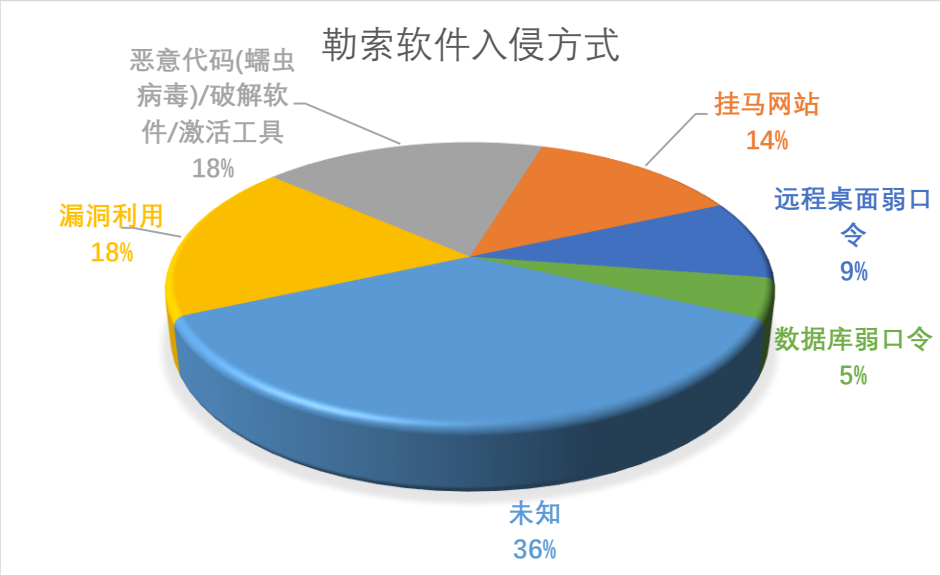
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 22 起非 Wannacry 勒索软件感染事件，较上周下降 24.1%，排在前三名的勒索软件家族分别为 Phobos（18.2%）、Hive（13.6%）和 BeijingCrypt（9.1%）。



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 40.9%，其次为 Windows 10 系统和 Windows Server 2012 系统，占比分别为 18.2%和 9.1%，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，漏洞利用和恶意代码(蠕虫病毒)/破解软件/激活工具占比较高，分别为 18%和 18%。Phobos 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.深圳某企业遭 Phobos 勒索病毒攻击

本周，工作组成员应急响应了深圳某生活服务行业单位遭 Phobos 勒索病毒攻击的事件。经工作组成员调查分析，攻击者通过 3389 端口登录子公司的电脑，并向总部传播，释放勒索病毒，使得总部公司某主机遭受勒索病毒攻击。

近期，Phobos 频繁攻击我国的用户，给企业和用户带来了巨大的安全威胁。建议企业删除映射到互联网的端口策略，关闭 135、137、138 等高危端口并限制 RDP 的访问连接。

2. 深圳某公司遭勒索病毒攻击

本周，工作组成员应急响应了深圳市某公司的服务器遭受勒索病毒攻击事件。综合相关日志和服务器中毒信息，此次事件的攻击路径是服务器直连公网，且服务器在早期有感染远控木马的情况，攻击者可能通过开启“允许远程协助连接这台计算机”即 3389 端口进行入

侵，另外由于业务需要，服务器直连公网，从而导致攻击者通过 RDP 方式直接登录服务器进行了投毒等勒索行为。

目前，攻击者通过开放端口对服务器进行暴力破解的攻击行为十分频繁。建议企业采用白名单机制，只允许开放特定的业务必要端口，其他端口一律禁止访问，并定期进行安全扫描。

（二） 国外部分

1. 建材巨头可耐福遭到 Black Basta 勒索软件攻击

可耐福（Knauf）是一家总部位于德国的跨国建筑和建筑材料生产商，可耐福集团宣布遭到网络攻击，攻击导致其业务中断，迫使其全球 IT 团队关闭所有 IT 系统以隔离事件。Black Basta 勒索软件团伙已通过在其勒索网站上的公告对此次攻击负责，并在 2022 年 7 月 16 日将可耐福列为受害者。该勒索软件团伙公布了据称在可耐福攻击中窃取的 20%的文件，超过 350 名访问者访问了这些文件。

四、威胁情报

域名

rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd[.]onion

jostat.mygoodsday[.]org

myexternalip[.]com

mygoodsday[.]org

网址

http://myexternalip[.]com/raw

http://jostat[.]mygoodsday.org/addrecord[.]php?apikey=kok08_api_key&compuser=WALKERPC|WALKER&sid=UhpHWe6OkkiK1rsN&phase=[SHARES]60

IP

34.107.221.82

208.95.112.1

193.56.29.123