国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 1 期（总第 9 期）　　1 月 1 日-1 月 7 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

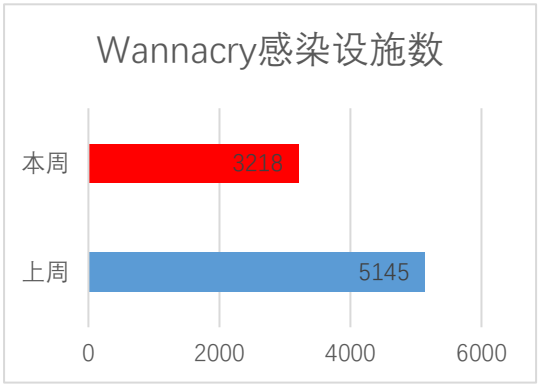
本周勒索软件防范应对工作组共收集捕获勒索软件样本 928351 个，监测发现勒索软件网络传播 1978 次，勒索软件下载 IP 地址 44 个，其中，位于境内的勒索软件下载地址 25 个，占比 56.8%，位于境外的勒索软件下载地址 19 个，占比 43.2%。

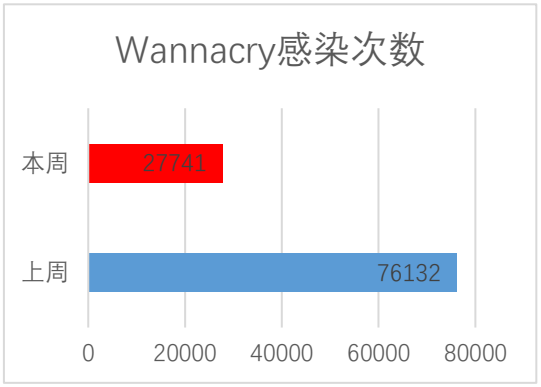
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

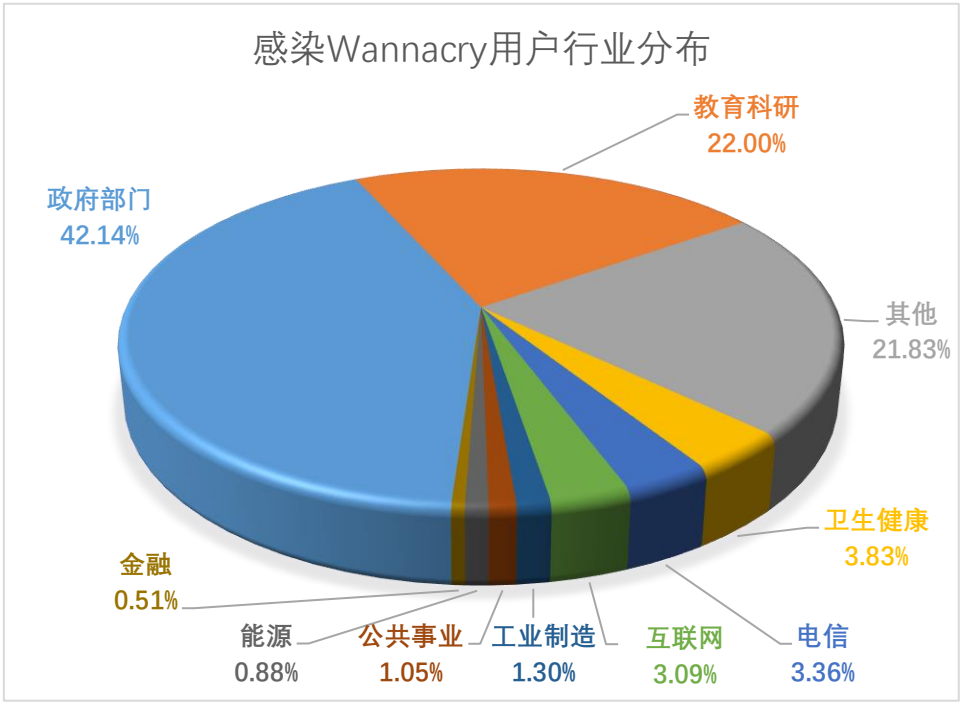
本周，监测发现 3218 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 37.5%，累计感染 27741 次，较上周下降 63.6%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



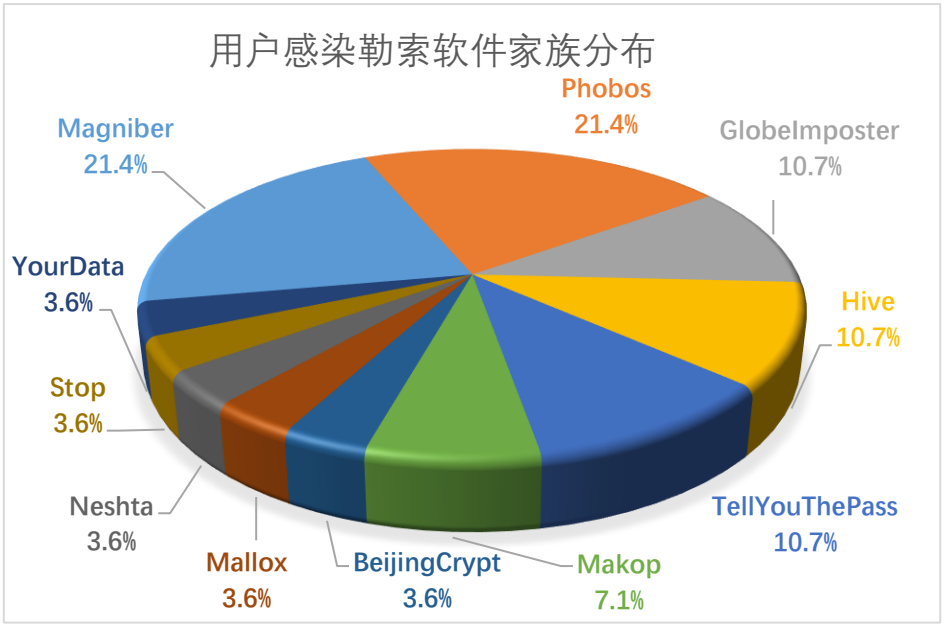


政府部门、教育科研、卫生健康、电信、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

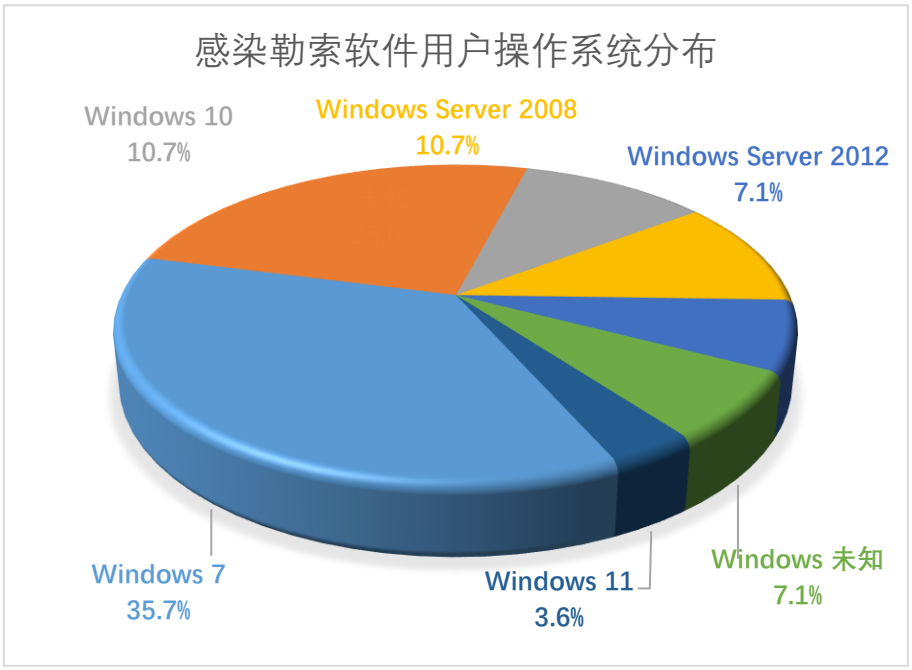


（二）其它勒索软件感染情况

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 28 起非 Wannacry 勒索软件感染事件，较上周下降 33.3%，排在前三名的勒索软件家族分别为 Magniber（21.4%）、Phobos（21.4%）和 GlobeImposter（10.7%）。

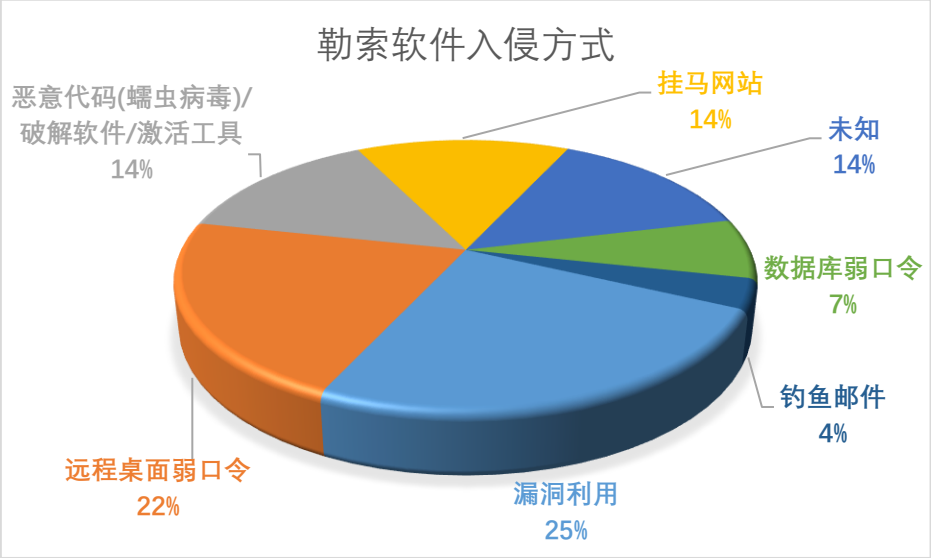


本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 35.7%，其次为 Windows10 系统，占比为 10.7%，多个版本的 Windows 服务器系统包括 Server 2008 和 Server 2012 分别占 10.7%和 7.1%，除此之外还包括多个其它不同版本的 Windows 系统和其它类型的操作系统。



本周，勒索软件入侵方式中，漏洞利用排在第一位，其次为远程桌面弱口令和恶意代码(蠕虫病毒)/破解软件/激活工具。Magniber 勒

索软件利用漏洞利用频繁攻击我国用户，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、浙江某企业云服务器感染 GlobeImposter 勒索软件

本周，工作组成员应急响应了浙江某企业云服务器感染 GlobeImposter 勒索软件事件。攻击者通过该服务器开放的远程桌面 RDP 服务和数据库服务进行口令暴力破解，并利用远程桌面弱口令漏洞获得了服务器控制权，进而植入勒索软件。

此事件中，攻击者利用服务器所开放服务的弱口令漏洞获取服务器主机控制权后并植入勒索软件。建议用户配置口令复杂度策略、修改弱口令、关闭不必要的服务。

2、新兴本土勒索软件家族 Coffee 在国内传播

根据工作组成员单位监测数据，近期国内新出现一种勒索软件家族 Coffee，因其加密后的文件后缀名包含 coffee 而得名。Coffee 家

族勒索软件向受害者索要 ZEC（零币）这一较为罕见的虚拟货币作为赎金，在被感染的主机上，其提供了详细的中文勒索信息，包括指导用户如何安装、购买和支付 ZEC 赎金。监测结果显示，Coffee 勒索软件通常采用网页挂马方式传播，并向受害者索要价值 500 美元的 ZEC 作为赎金。

建议用户加强网络安全意识，不打开来源不明的邮件附件，不从非官方不可信网站下载软件，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

（二） 国外部分

1、葡萄牙媒体巨头 Impresa 遭受勒索软件攻击

新年伊始，拥有葡萄牙最大电视台和报纸的传媒巨头 Impresa 因遭遇勒索软件攻击而瘫痪。勒索软件团伙 Lapsus$通过在 Impresa 网站上展示的勒索信声称对此事件负责。这次攻击包括 Impresa 旗下的 SIC 电视台和 Expresso 报纸，除此之外，Lapsus$团伙声称其已获得对 Impresa 的 Amazon Web Services 账户的访问权限。截至 1 月 5 日，Lapsus$勒索团伙仍能控制该公司的信息基础设施，且 Impresa 的官网仍未完全恢复。此外，Lapsus$组织通过一个经过 Impresa 验证的 Twitter 账户发送推文，以展示其依然有能力访问 Impresa 的资源。

四、威胁情报

域名

Wwbaidu[.]com

IP

40.115.162.72

37.120.193.123

157.245.70.127

31.44.184.82

185.153.199.176

网址

http://bc74e8b87ec046e0f6bc3tpttoymg.eatlist[.]space/tpttoymg

http://0ed03060fa90b2a036f02418efkspkzd.crypack[.]fit/fkspkzd

http://0ed03060fa90b2a036f02418efkspkzd.laintin[.]uno/fkspkzd

http://f2d0c210a62830706eb8b638efzofhqi.laintin[.]uno/fzofhqi

http://f2d0c210a62830706eb8b638efzofhqi.crypack[.]fit/fzofhqi

http://f2d0c210a62830706eb8b638ekkkkxqz.forrain[.]fit/kkkkxqz

http://f2d0c210a62830706eb8b638ekkkkxqz.mensell[.]uno/kkkkxqz

http://f8fcacf072f444f06af408f8rfijmsp.hillbe[.]space/rfijmsp

http://80f8d8c024e0fe20d4b0d6d0dnoiauxk.orseen[.]casa/noiauxk

http://80f8d8c024e0fe20d4b0d6d0dnoiauxk.areedit[.]uno/noiauxk

http://91.243.44[.]75/hbatka.jpeg

http://loki-locker[.]one/index.php

邮箱

beijing520@horsefucker.org

BillScars@gmx.com

ecrypt24@nerdmail.co

johnwilliams1887@gmx.com

yourlovelysupport@xmpp.jp

securityrook@securityrook.com

d4rkw4ve@tutanota.com

dark4wave@yandex.com

钱包地址

1K7rFg7uVjq2MEHSAv19U8BfrjTj2J1mYr

1AVBKGV4YcVVsEH8eHHYSSoHvn3wz4TCRQ

16RymC1BtgR4sU19L27HDDUwjTeQPWTmRj

173Ubc6dyhdS5o9q2mNja3nA2kvLBbpm11

1FuFg1Vxrm9Yc3c5amrk1j6PjYGRWWeJZr

14jDwqRjndKE4HWC8wWg2mFLjWrKM8fhnR

1JSqV6uESKTV8DL6SZRAehV4Q1mTuhpM39

1PgAW1fhDBPGn6UX7tTELbQ1tyhyJQjcXg

1BmZaMoztsRBf2XTgTBkrkkw6qEL5Y7rYP

1M9g5u1W7Cn39EPaDQbzxNEdWHc8Bdvu2T