国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 6 期（总第 14 期）　　2 月 5 日-2 月 11 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

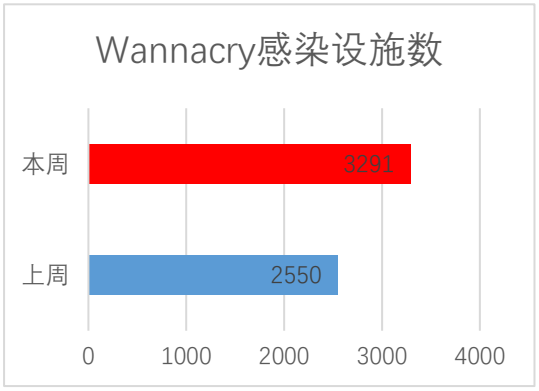
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1006033 个，监测发现勒索软件网络传播 4909 次，勒索软件下载 IP 地址 972 个，其中，位于境内的勒索软件下载地址 272 个，占比 28%，位于境外的勒索软件下载地址 700 个，占比 72%。

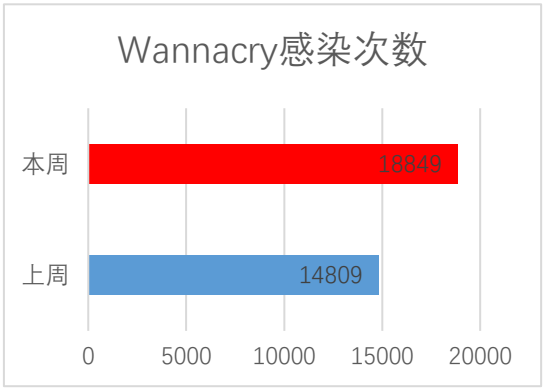
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

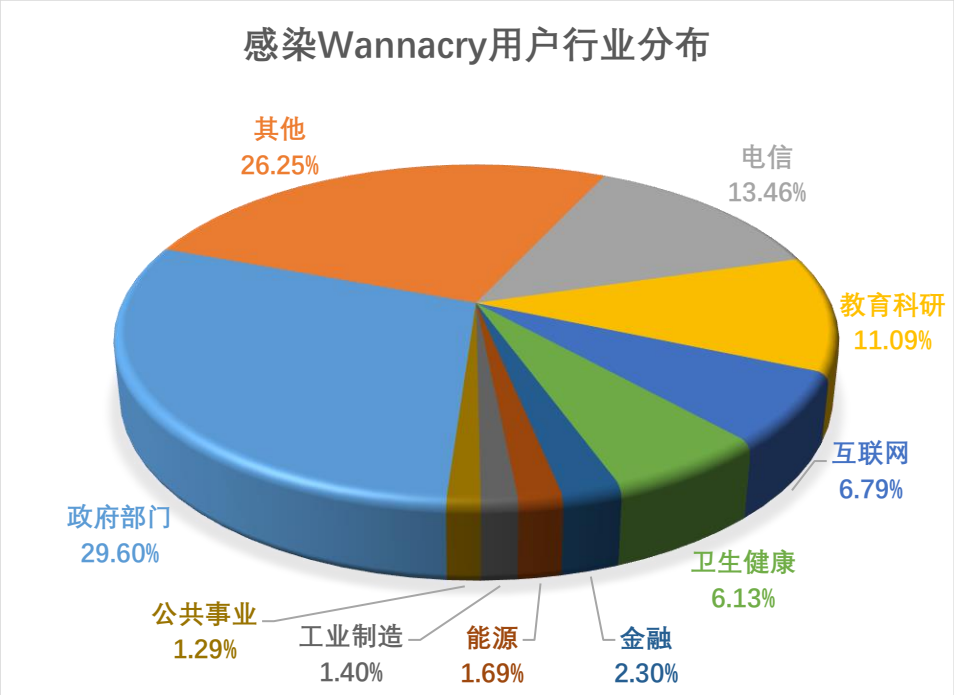
本周，监测发现 3291 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 29.1%，累计感染 18849 次，较上周上升 27.3%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



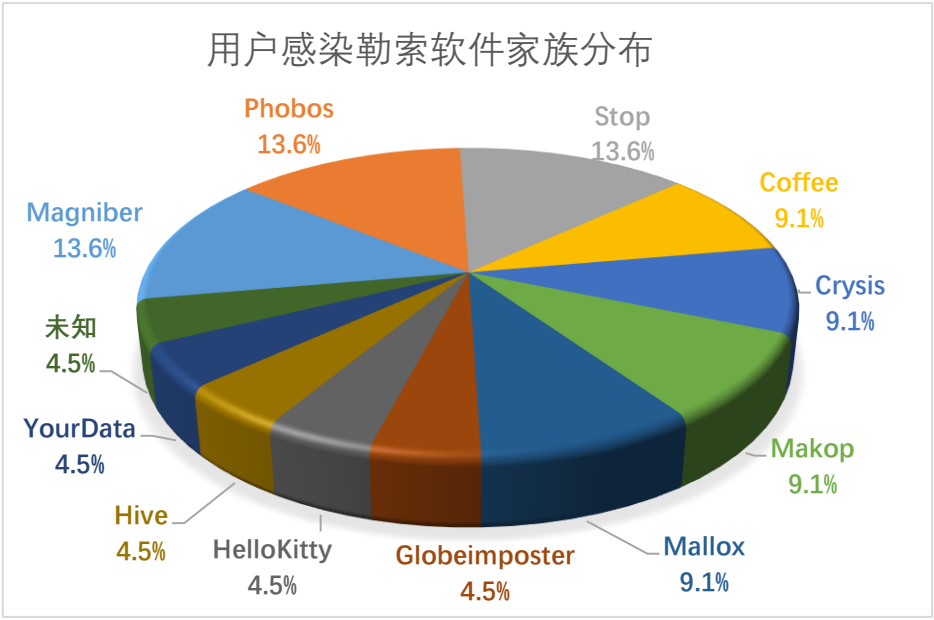


政府部门、电信、教育科研、互联网、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

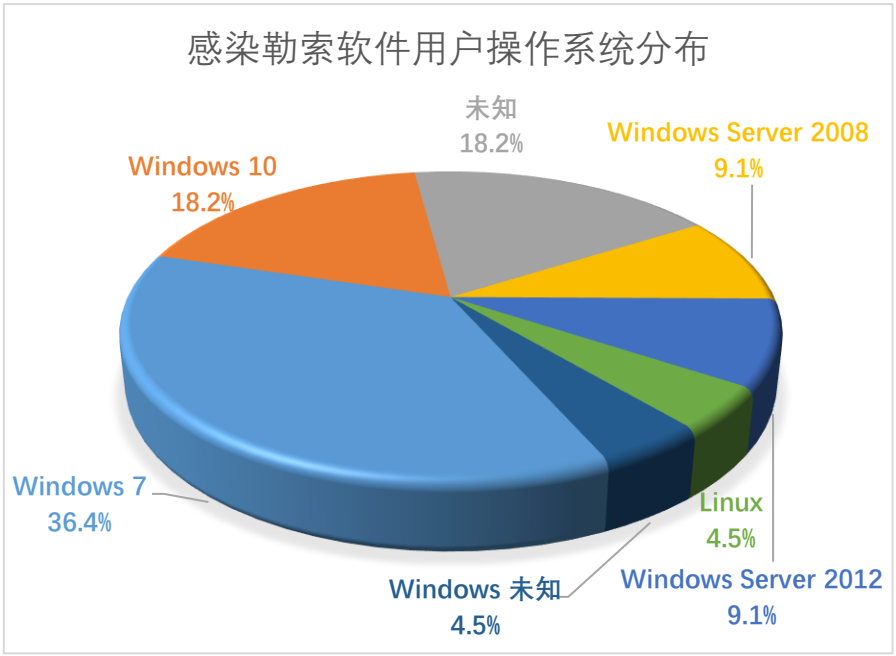


（二）其它勒索软件感染情况

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 21.4%，排在前三名的勒索软件家族分别为 Magniber、Phobos 和 Stop，占比均为 13.6%。

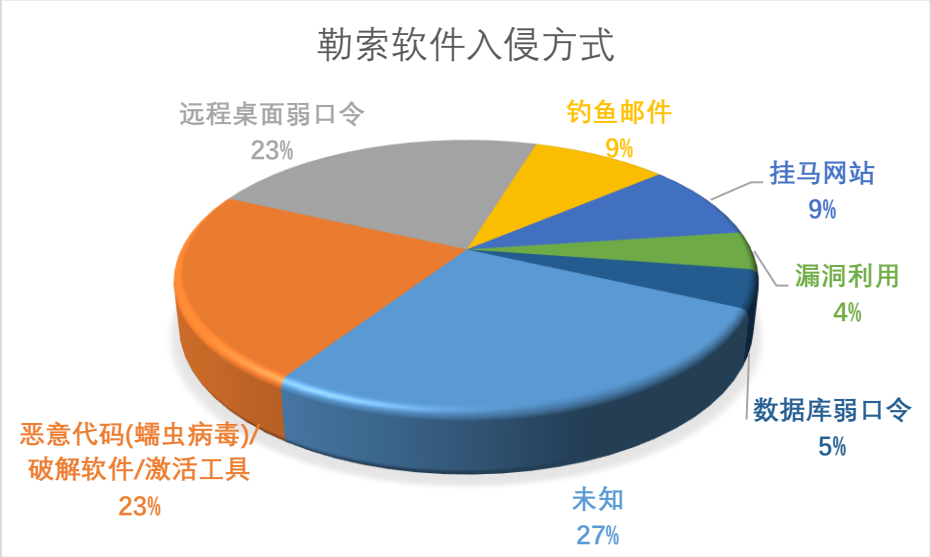


本周，被勒索软件感染的系统中 Windows 7 系统占比较高，占到总量的 36.4%，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 18.2%和 9.1%，除此之外还包括多个其它不同版本的 Windows 服务器系统和其它类型的操作系统。



本周，勒索软件入侵方式中，远程桌面弱口令和恶意代码（蠕虫病毒）/破解软件/激活工具占比较高，均为 23%。Phobos 勒索软件利用弱口令漏洞特别是远程桌面弱口令频繁攻击我国用户，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、福建某企业内网多台主机感染 BeijingCrypt 勒索软件

本周，工作组成员自主监测并响应了福建某企业内网多台主机感染 BeijingCrypt 勒索软件事件。攻击者通过入侵该企业官方网站并获得了一台内网主机权限，随后通过横向移动在内网中的其他主机植入 Anydesk 远程控制软件并投递勒索软件。

此事件中，攻击者通过入侵企业网站服务器随后向内网主机植入勒索软件，建议用户实施网络隔离和边界防护，实施服务器主机系统安全加固和部署终端安全解决方案。

（二） 国外部分

1、航空服务企业 Swissport 遭受 BlackCat 勒索软件攻击

Swissport International Ltd.是一家年收入 30 亿欧元、且在 50 个国家的 310 个机场开展业务的航空服务企业，近日该企业遭受

勒索病毒攻击，其位于全球的多个 IT 基础设施被入侵或破坏，对公司运营造成严重影响，并导致多个航班延误。BlackCat 勒索团伙随后宣布对此次攻击事件负责，并威胁将窃取的 1.6TB 敏感数据出售给潜在买家。

四、威胁情报

域名

bottomcdnfiles[.]com

cdnmegafiles[.]com

chat5sqrnzqewampznybomgn4hf2m53tybkarxk4sfaktwt7oqpkcvyd[.]onion

gg5ryfgogainisskdvh4y373ap3b2mxafcibeh2lvq5x7fx76ygcosad[.]onion

isqtoimht5llucldrw7flyak2n5zdu4dmd7kdfs6tuasrxq7qydqs2qd[.]onion

pflujznptk5lmuf6xwadfqy6nffykdvahfbljh7liljailjbxrgvhfid[.]onion

IP

179.43.160.195

68.183.8.207

82.146.53.237

网址

http://ea78ce30dc7044b0aa58feb0ozrgvmpw.megrow[.]site/ozrgvmpw

http://ea78ce30dc7044b0aa58feb0ozrgvmpw.ofideas[.]uno/ozrgvmpw

http://ea78ce30dc7044b0aa58feb0ozrgvmpw.shepain[.]quest/ozrgvmpw

邮箱

ithelp02@decorous.cyou

ithelp02@wholeness.business

LilliBTC@tuta.io

ljubisupporte@protonmail.com

mrcrypt@msgsafe.io

mrcrypt2@mailfence.com

钱包地址

bc1qd3hk7g8dnsyw7sxledlje2twz9vk3fex95prlr