国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 27 期（总第 35 期）　　7 月 2 日-7 月 8 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：

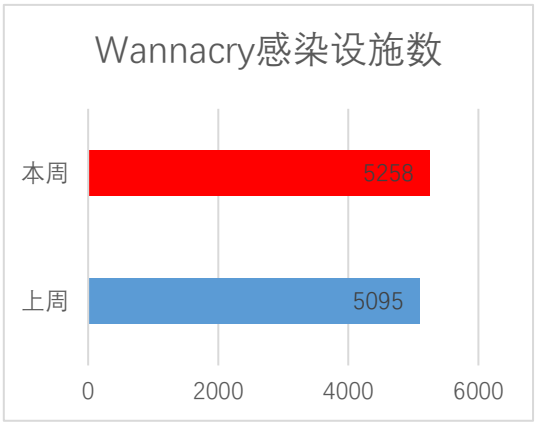
一、勒索软件样本捕获情况

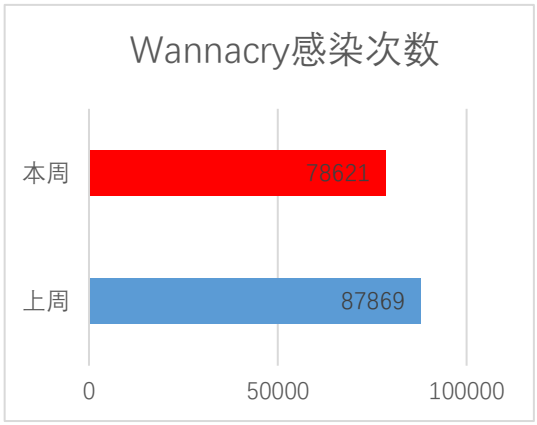
本周勒索软件防范应对工作组共收集捕获勒索软件样本 821659 个，本周未监测发现勒索软件网络传播。

二、勒索软件受害者情况

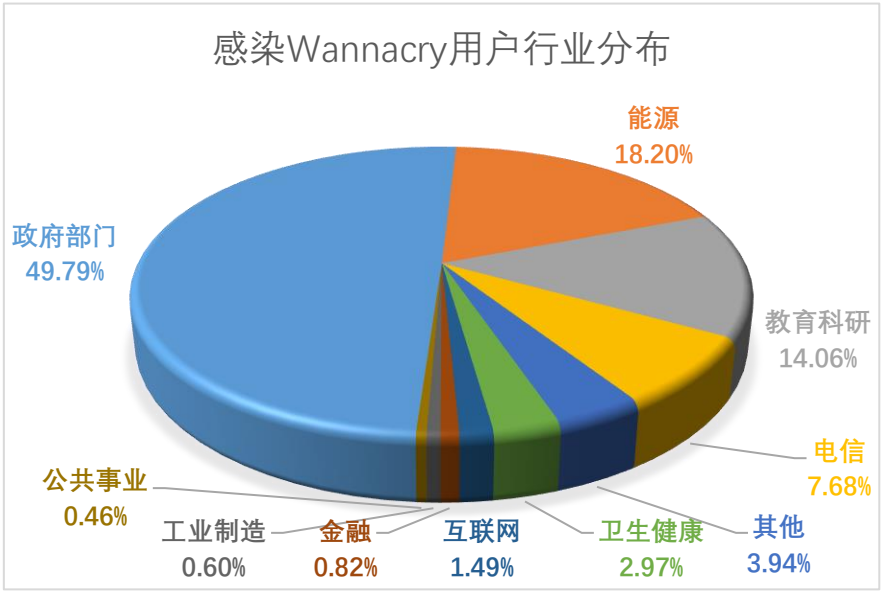
（一）Wannacry 勒索软件感染情况

本周，监测发现 5258 起我国单位设施感染 Wannacry 勒索软件事件，较上周增长 3.2%，累计感染 78621 次，较上周下降 10.5%。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。



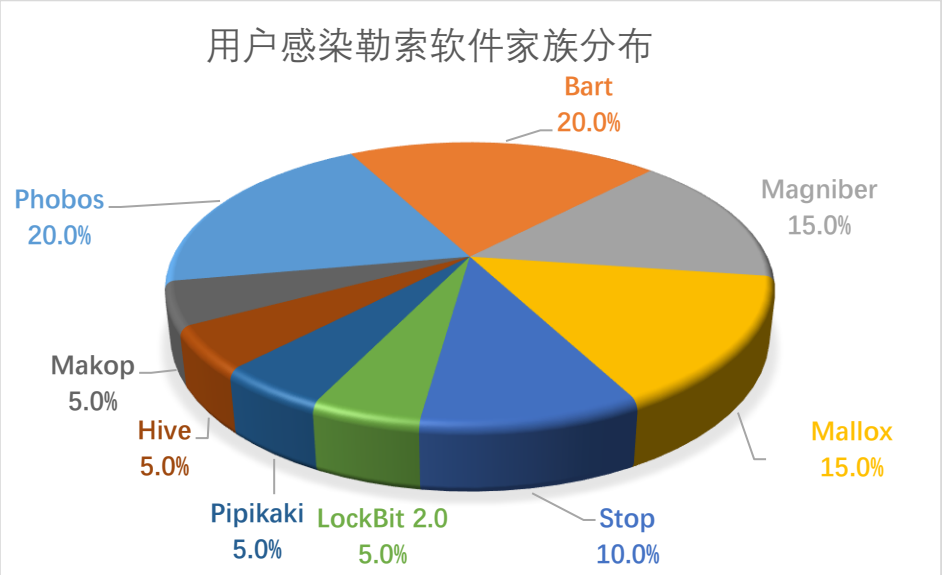


政府部门、能源、教育科研、电信、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

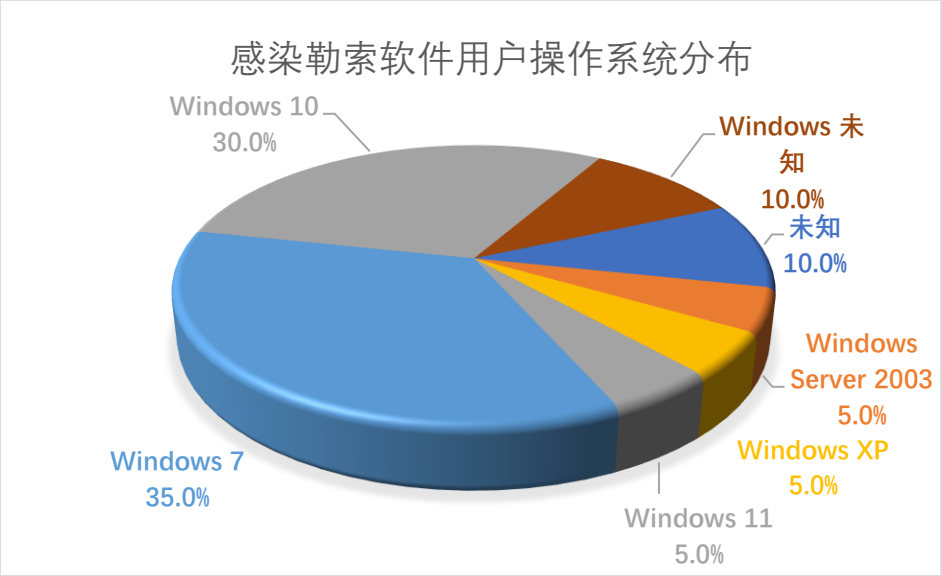


（二）其它勒索软件感染情况

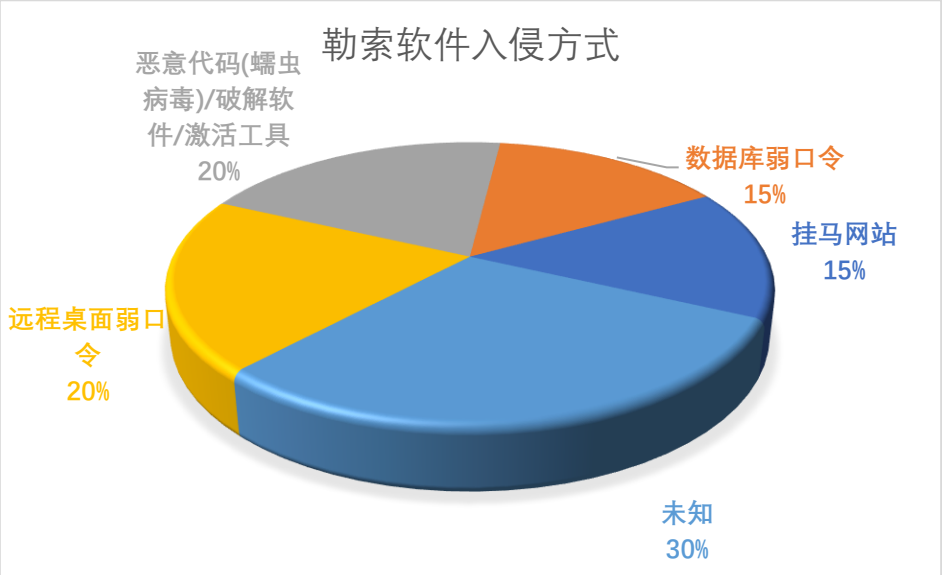
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 20 起非 Wannacry 勒索软件感染事件，较上周增长 5.3%，排在前三名的勒索软件家族分别为 Phobos（20.0%）、Bart（20.0%）和 Magniber（15.0%）。



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 35%，其次为 Windows 10 系统和 Windows Server 2013 系统，占比分别为 30.0%和 5.0%，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，分别为 20%和 20%。Phobos 勒索软件通过远程桌面弱口令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.山西某医院遭 Phobos 勒索病毒攻击

本周，工作组成员应急响应了山西某医院遭 Phobos 勒索病毒攻击的事件。经工作组成员排查发现，该医院存在暴露在互联网上的 RDP 端口，攻击者通过暴力破解的方式入侵医院系统。随后投放扫描工具和勒索病毒，利用口令 dump 和弱口令陆续感染了数台 Windows 主机。

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。建议企业和个人提高系统用户口令强度，避免将内网的 SSH、RDP 等服务端口映射到公网。

2. 山东某制造业单位遭勒索病毒攻击

本周，工作组成员应急响应了山东某制造业单位的多台服务器和终端遭受勒索病毒攻击事件。攻击者首先入侵了某台应用服务器，通过 PE 修改系统密码登录服务器，后利用该服务器作为跳板机，以爆

破的方式入侵了该单位的某台终端设备，在设备中投放勒索病毒，并进行了安全日志清理的操作。

目前，攻击者通过弱口令对服务器、终端等设备进行爆破仍为主要攻击方式，企业和个人用户应该杜绝使用弱口令，同时定期开展对系统、应用以及网络层面的安全评估。

（二） 国外部分

1. Macmillan 疑似遭到勒索病毒攻击导致系统关闭

近日，出版巨头 Macmillan 疑似遭到勒索病毒攻击，迫使该公司关闭了所有 IT 系统以防止攻击的传播。一封来自 Macmillan 内部的电子邮件显示他们遭受了“安全事件，涉及加密我们网络上的某些文件”。这代表了该公司极有可能是遭到了勒索病毒的攻击。

目前 Macmillan 已经开始重新上线其网络系统，员工也能够访问电子邮件。但尚不清楚此次攻击背后的是哪家勒索病毒团伙以及数据是否被盗。

四、威胁情报

域名

www.myob[.]live

login.myob[.]live

smaugrwmaystthfxp72tlmdbrzlwdp2pxtpvtzvhkv5ppg3difiwonad[.]onion

mtr.ddns[.]mobi

网址

http://f24c04683e00f2204cfcfe28e604a4myijvzjue.tiedlaw[.]info/myijvzjue

http://f24c04683e00f2204cfcfe28e604a4myijvzjue.lendhit[.]info/myijvzjue

http://f24c04683e00f2204cfcfe28e604a4myijvzjue.hascuts[.]info/myijvzjue

http://f24c04683e00f2204cfcfe28e604a4myijvzjue.pollof[.]info/myijvzjue

http://f24c04683e00f2204cfcfe28e604a4myijvzjue.xjvfi2lce4nriceqdhue4ftdrs7gongo
mm3ffpso3ng3znrwzbahekqd[.]onion/myijvzjue

http://e228b6203624b020f4407aa00658e4a0uuxsnhbjj.chaosme[.]info/uuxsnhbjj

http://e228b6203624b020f4407aa00658e4a0uuxsnhbjj.wasyes[.]info/uuxsnhbjj

http://e228b6203624b020f4407aa00658e4a0uuxsnhbjj.kideasy[.]info/uuxsnhbjj

http://e228b6203624b020f4407aa00658e4a0uuxsnhbjj.legslip[.]info/uuxsnhbjj

http://e228b6203624b020f4407aa00658e4a0uuxsnhbjj.vrgdmg5tsfnsbs3l5xdstqoilar4l
jgn522tu6x4urzbhpjj42byt7id[.]onion/uuxsnhbjj

邮箱

wixawm@gmail.com

helpshadow@india.com

helprecovery@gnu.gr

cyborgyarraq@protonmail.cn

webroothooks@tutanota.com

kardon@firemail.cc

henderson@cock.li

Trebaler@goat.si

钱包地址

15G6YvWH9hFp6BetJdVs4xgsx2wyimcHc1

1BoKgLAR71Jq975cS1YahK2PdcWwKf4ddf