国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 26 期（总第 34 期）　　6 月 25 日-7 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

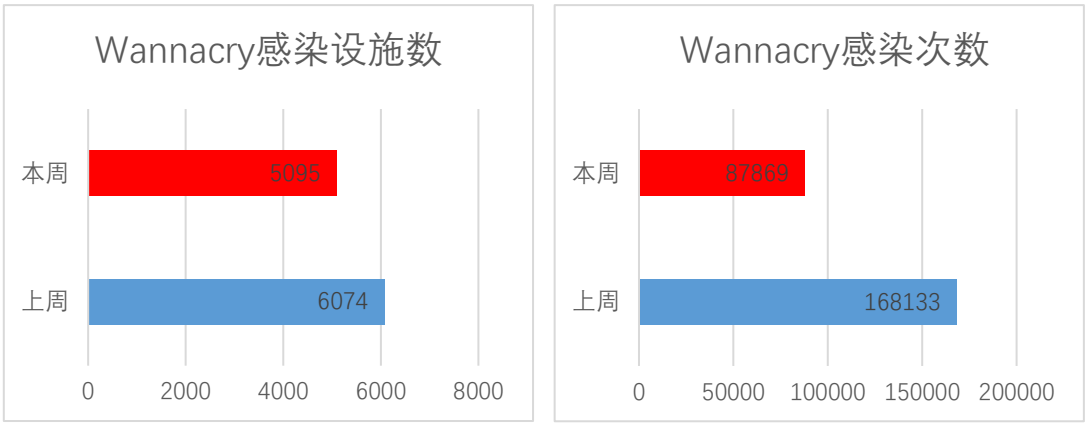
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1298427 个，监测发现勒索软件网络传播 129 次，勒索软件下载 IP 地址 19 个，其中，位于境内的勒索软件下载地址 13 个，占比 68.4%，位于境外的勒索软件下载地址 6 个，占比 31.6%。

二、勒索软件受害者情况

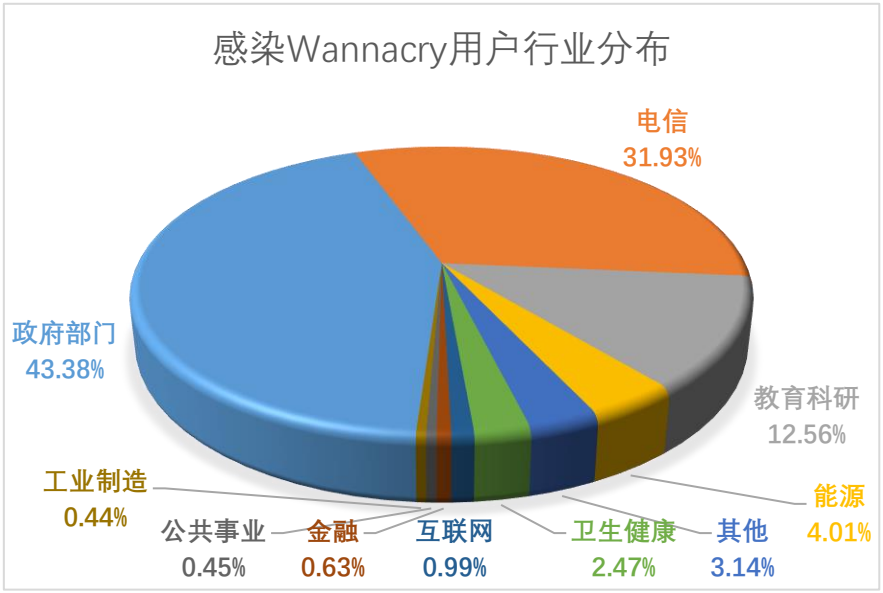
（一）Wannacry 勒索软件感染情况

本周，监测发现 5095 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 16.1%，累计感染 87869 次，较上周下降 47.7%。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。

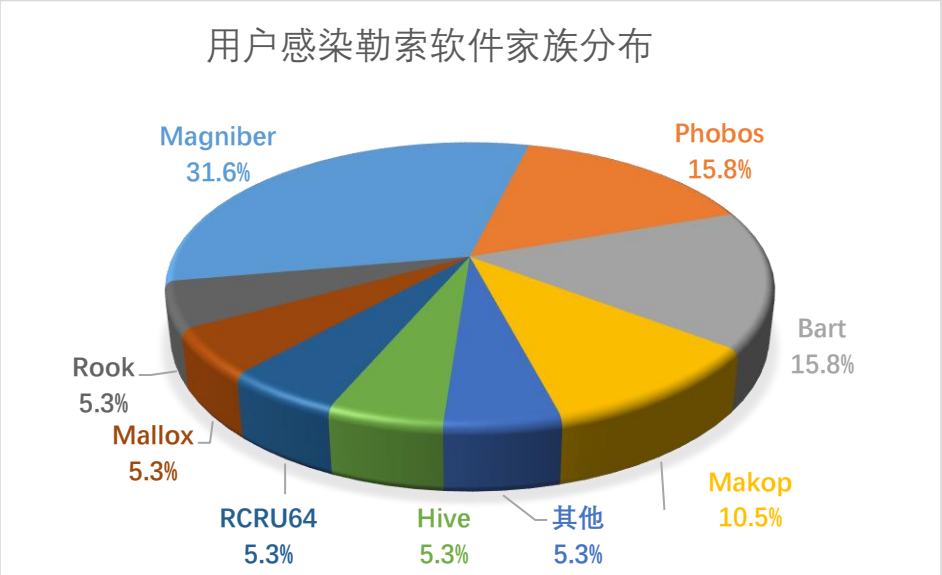


政府部门、电信、教育科研、能源、卫生健康行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

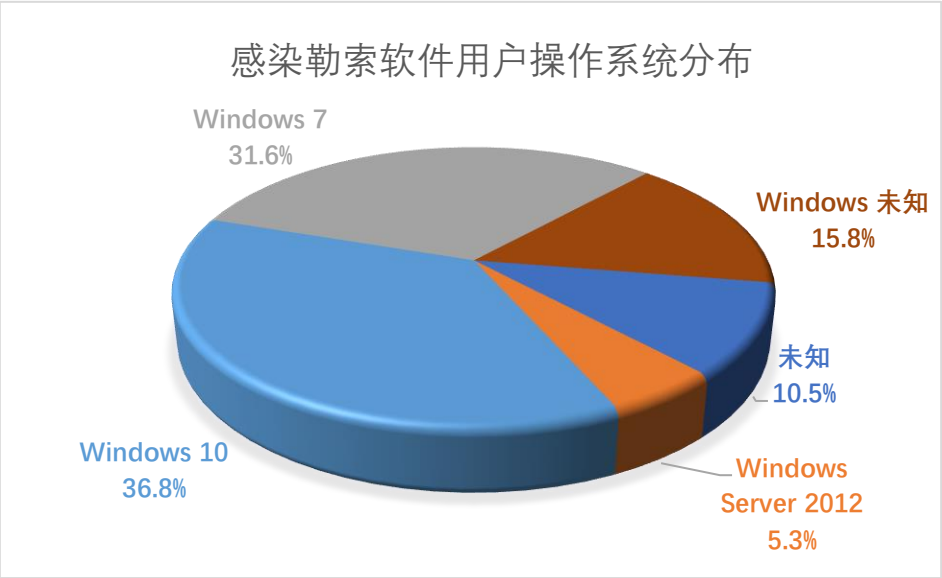


（二）其它勒索软件感染情况

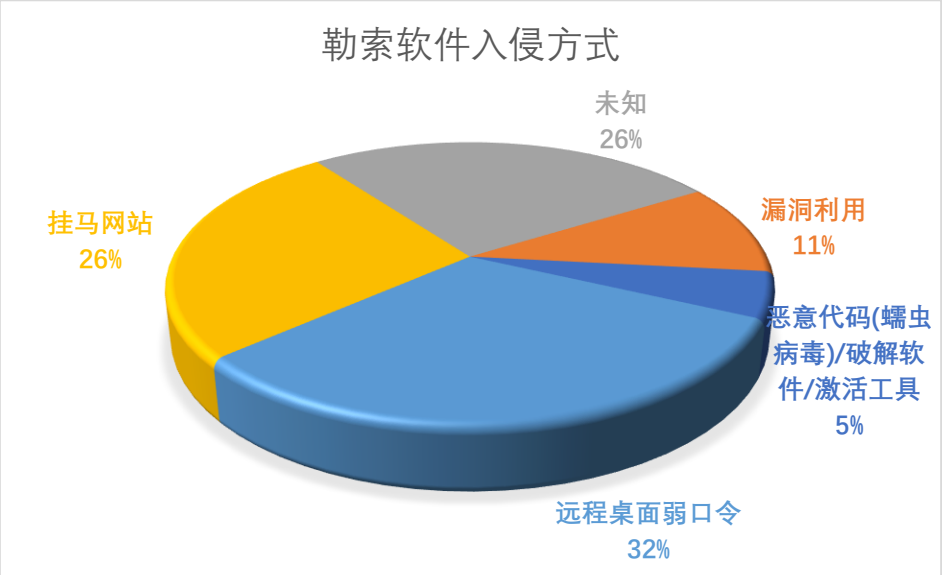
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 19 起非 Wannacry 勒索软件感染事件，较上周下降 17.4%，排在前三名的勒索软件家族分别为 Magniber（31.6%）、Phobos（15.8%）和 Bart（15.8%）。



本周，被勒索软件感染的系统中 Windows 10 系统占比较高，占到总量的 36.8%，其次为 Windows 7 系统和 Windows Server 2012 系统，占比分别为 31.6%和 5.3%，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，远程桌面弱口令和挂马网站占比较高，分别为 32%和 26%。Magniber 勒索软件通过挂马网站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.浙江某学校遭 Phobos 勒索软件攻击

本周，工作组成员应急响应了浙江某学校服务器遭 Phobos 勒索软件攻击的事件。经工作组成员调查分析，攻击者是通过存在该学校内网上的另一台主机对该服务器进行爆破，并成功登录过该系统。攻击者在该服务器的多个磁盘目录下植入了勒索软件程序，在系统的注册表项中也发现了加密程序的注册项及系统启动项。

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，加强网络安全防御意识，建立有效的防火墙策略。

2. 福建某生活服务行业单位遭勒索软件攻击

本周，工作组成员应急响应了福建某生活服务行业单位的多台服务器和终端遭受勒索软件攻击事件。攻击者利用了该单位某台设备接入了互联网访问的网线，导致 3389 端口暴露在公网的漏洞，对该设

备进行了暴力破解，破解成功后以该设备为跳板对内网进行横向渗透，并向多台服务器植入勒索软件。

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。企业和用户要杜绝使用弱口令，不在非正规渠道下载安装软件，不点击不明邮件，提高安全意识。

（二） 国外部分

1. 汽车软管制造商 Nichirin 的美国子公司被勒索软件攻击

日本汽车软管生产商 Nichirin 的一家美国子公司最近遭到勒索软件攻击。该公司表示，针对日信 Nichirin-Flex USA 的攻击是在 6 月 14 日发现的，Nichirin 的其他子公司似乎没有受到影响。网络攻击的全面影响正在调查中，该事件迫使该公司关闭了一些生产控制系统，改用手工流程。在其网站上，Nichirin 警告客户警惕明显来自该公司的虚假电子邮件。Nichirin 的警告写道:“如果你回复这些邮件，就有被欺诈、病毒感染、泄露和滥用个人信息的风险。请不要回复任何未知的电子邮件，访问列出的 URL，打开任何附件等等，应立即删除邮件。”

四、威胁情报

域名

myphotoload[.]com

buvpbsq[.]pw

jetxtfwv[.]pw

hubvdqgfcoierc[.]pw

网址

stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion

aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd[.]onion

http://268086b8e0gnapxjnh.ohgig7nhgjh5ddsyh2x344plk5mbzuwhlkoedardqqf4mg3g675lrrad[.]onion/gnapxjnh

http://268086b8e0gnapxjnh.sadby[.]info/gnapxjnh

http://268086b8e0gnapxjnh.outdeem[.]info/gnapxjnh

http://268086b8e0gnapxjnh.didbuys[.]info/gnapxjnh

http://268086b8e0gnapxjnh.keysask[.]info/gnapxjnh

邮箱

hudsonL@cock.li

pipikaki@privatemail.com

hpsupport@cyberfear.com

for_recovery@privatemail.com

myers@cock.li

trust03@tutanota.com

newSanta@protonmail.com

andreihelp@cyberfear.com

钱包地址

1LjZUspMGpvx8Gk6uCMPnfphMRun52k5vB