国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 19 期（总第 27 期）　　5 月 7 日-5 月 13 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

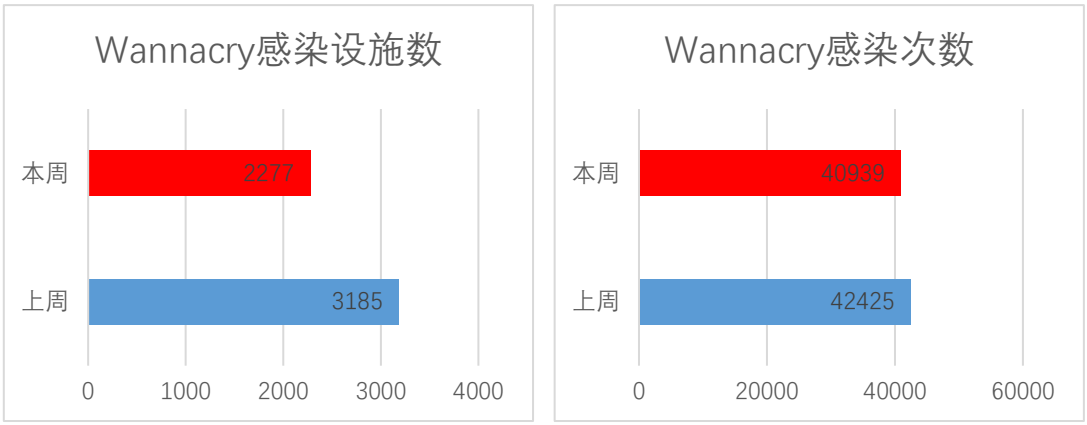
本周勒索软件防范应对工作组共收集捕获勒索软件样本 5861043 个，监测发现勒索软件网络传播 977 次，勒索软件下载 IP 地址 88 个，其中，位于境内的勒索软件下载地址 20 个，占比 22.7%，位于境外的勒索软件下载地址 68 个，占比 77.3%。

二、勒索软件受害者情况

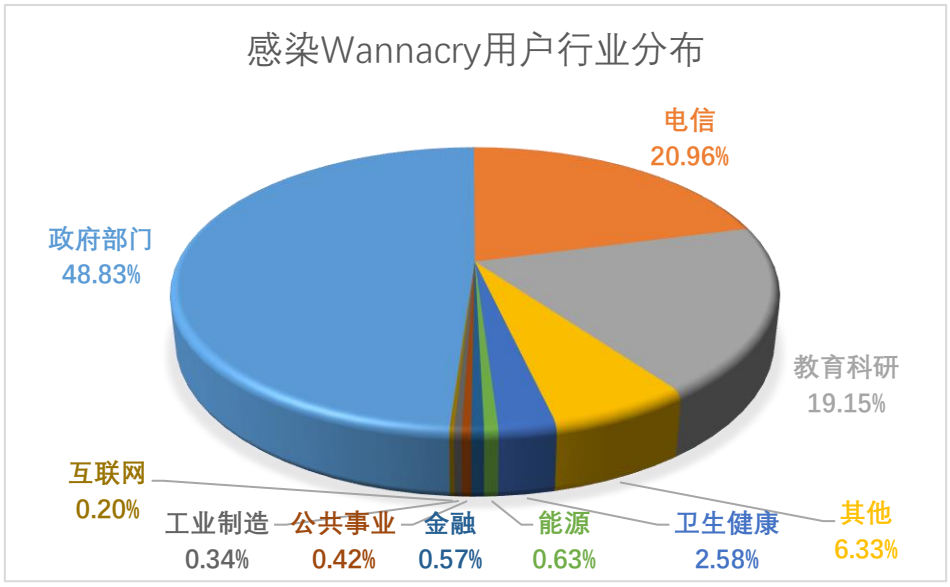
（一）Wannacry 勒索软件感染情况

本周，监测发现 2277 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 28.5%，累计感染 40939 次，较上周下降 3.5%。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。

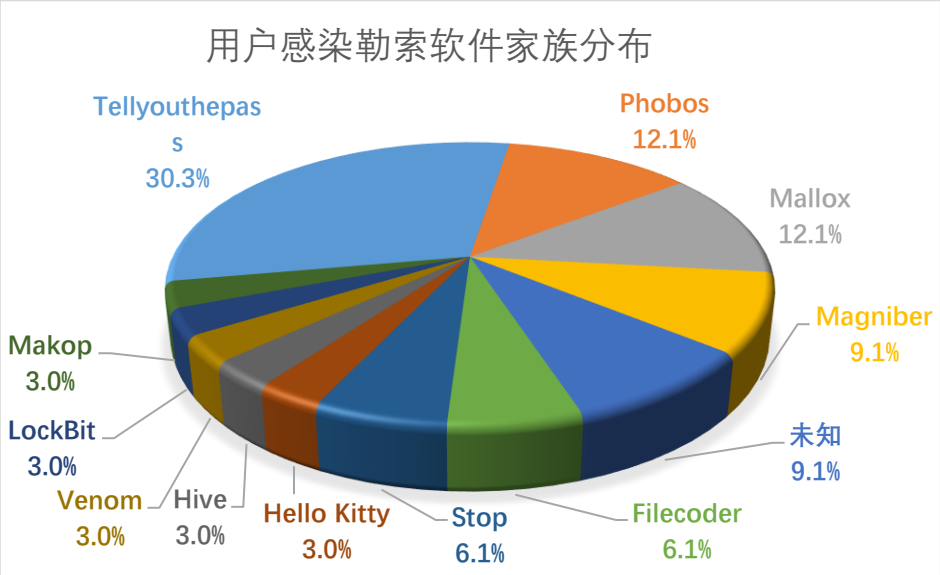


政府部门、电信、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

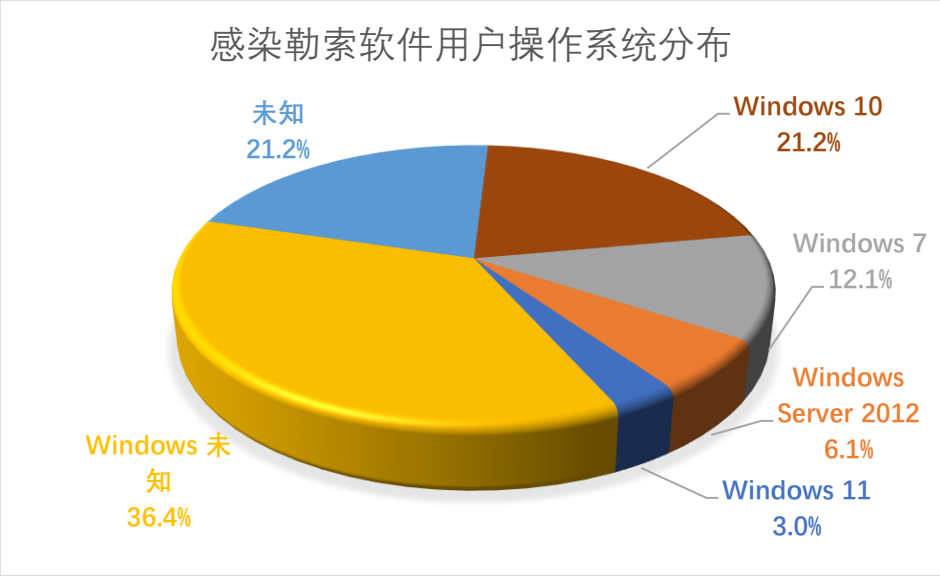


（二）其它勒索软件感染情况

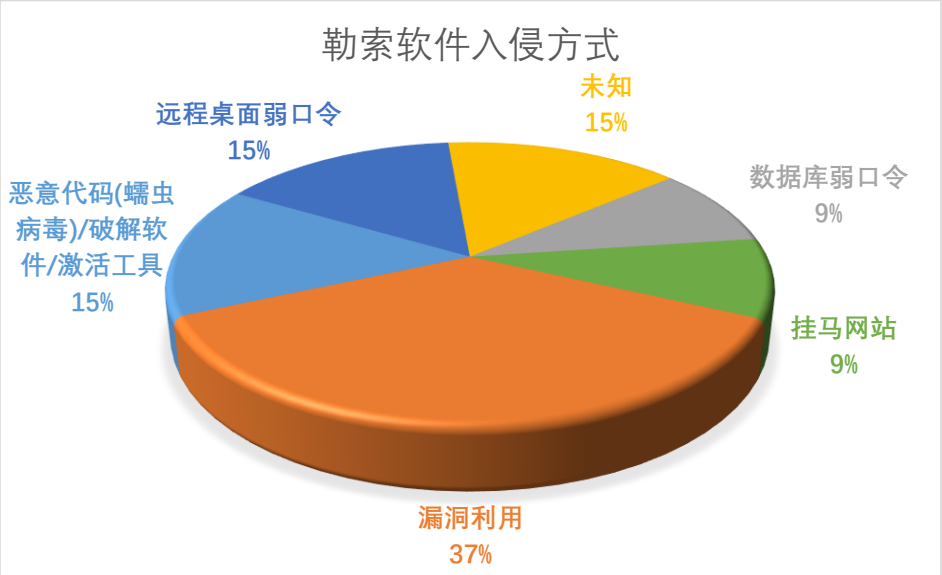
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 33 起非 Wannacry 勒索软件感染事件，较上周上升 50.0%，排在前三名的勒索软件家族分别为 Tellyouthepass（30.3%）、Phobos（12.1%）和 Mallox（12.1%）。



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 21.2%，其次为 Windows 7 系统和 Windows Server 2012 系统，占比分别为 12.1%和 6.1%，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 36%和 15%。Tellyouthepass 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. 上海某企业遭 Phobos 勒索病毒攻击

本周，工作组成员应急响应了上海某企业服务器遭 Phobos 勒索病毒攻击事件。攻击者对该企业服务器的 administrator 账号密码进行爆破，爆破成功后通过荷兰某 IP 远程登录服务器并对内网端口进行扫描。之后对内网上的数台设备持续进行密码爆破以及远程登录 administrator 账号操作，并放置恶意程序，运行恶意程序实施勒索。

Phobos 家族勒索病毒近期频繁攻击我国企业和用户，造成了较大的安全威胁。建议企业和用户定期进行服务器、网络设备的操作系统和中间件的漏洞扫描、修复工作，并关闭不必要的服务和端口。

（二） 国外部分

1. 美国农业机械制造商 AGCO 遭受勒索软件攻击

美国农业机械制造商 AGCO 宣布遭受勒索软件攻击，影响了其生产设施。该公司被迫关闭部分 IT 系统以应对这一事件。该公司发

布的公告表示，在 2022 年 5 月 5 日，该公司受到了勒索软件的攻击，其一些生产设施受到了影响。AGCO 仍在调查此次攻击的程度，但预计其业务运营将受到不利影响数日，甚至可能更长时间才能完全恢复所有服务，具体取决于公司修复系统的速度。

四、威胁情报

域名

newdesk[.]top

my-logford[.]ml

gupdate[.]us

microsoft-updateserver[.]cf

msupdate[.]us

onedriver-srv[.]ml

symantecserver[.]co

winstore[.]us

aptmirror[.]eu

IP

104.18.32.68

183.78.205.92

190.219.109.25

190.219.54.242

196.200.111.5

23.216.147.64

网址

http://0c1068a0b4d82250f64cd2b80e24aed0sjoxisq.diedsad[.]info/sjoxisq

http://0c1068a0b4d82250f64cd2b80e24aed0sjoxisq.aresika[.]info/sjoxisq

http://0c1068a0b4d82250f64cd2b80e24aed0sjoxisq.vbmpkajxyygcqos2luorb5p66yr5wb5v6lj2dy6acqhhuch5ssuq7xqd[.]onion/sjoxisq

http://0c1068a0b4d82250f64cd2b80e24aed0sjoxisq.oldfree[.]info/sjoxisq

http://0c1068a0b4d82250f64cd2b80e24aed0sjoxisq.rawrow[.]info/sjoxisq

http://f4244ad036184a00229008a8ba4cdalgvfvagyg.tinper[.]info/lgvfvagyg

http://f4244ad036184a00229008a8ba4cdalgvfvagyg.onlylot[.]info/lgvfvagyg

http://f4244ad036184a00229008a8ba4cdalgvfvagyg.gravehe[.]info/lgvfvagyg

http://f4244ad036184a00229008a8ba4cdalgvfvagyg.oddpoll[.]info/lgvfvagyg

http://f4244ad036184a00229008a8ba4cdalgvfvagyg.mjrdx5u4vripjuw7rha2oyjguf6v

wtbttkn4srof3kwuezgquez6y5yd[.]onion/lgvfvagyg

邮箱

dear_decript2022@mail2tor.com

dear_decript2022@jabbim.com

avastdata@privatemail.com

mallox@stealthypost.net

uped97@mail.ee

ginnydterrell@onionmail.org

martin1993douglas@pressmail.ch

back2023@proxy.tg

uped97@mail.ee

uped98@mail.ee