国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 21 期（总第 29 期）　　5 月 21 日-5 月 27 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

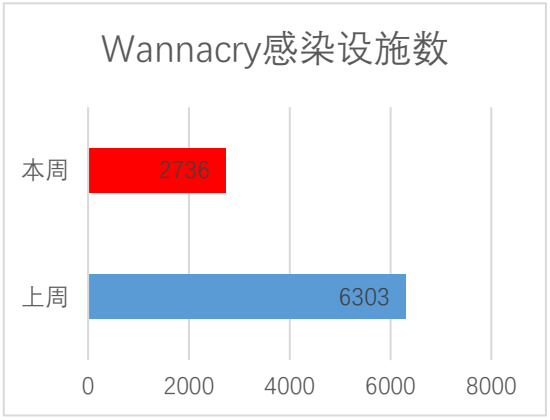
本周勒索软件防范应对工作组共收集捕获勒索软件样本 946282 个，监测发现勒索软件网络传播 1176 次，勒索软件下载 IP 地址 86 个，其中，位于境内的勒索软件下载地址 13 个，占比 15.1%，位于境外的勒索软件下载地址 73 个，占比 84.9%。

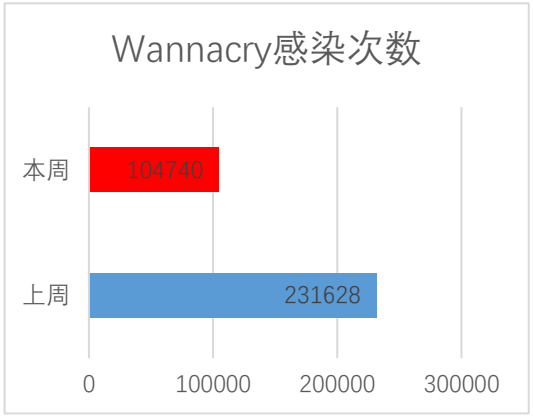
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

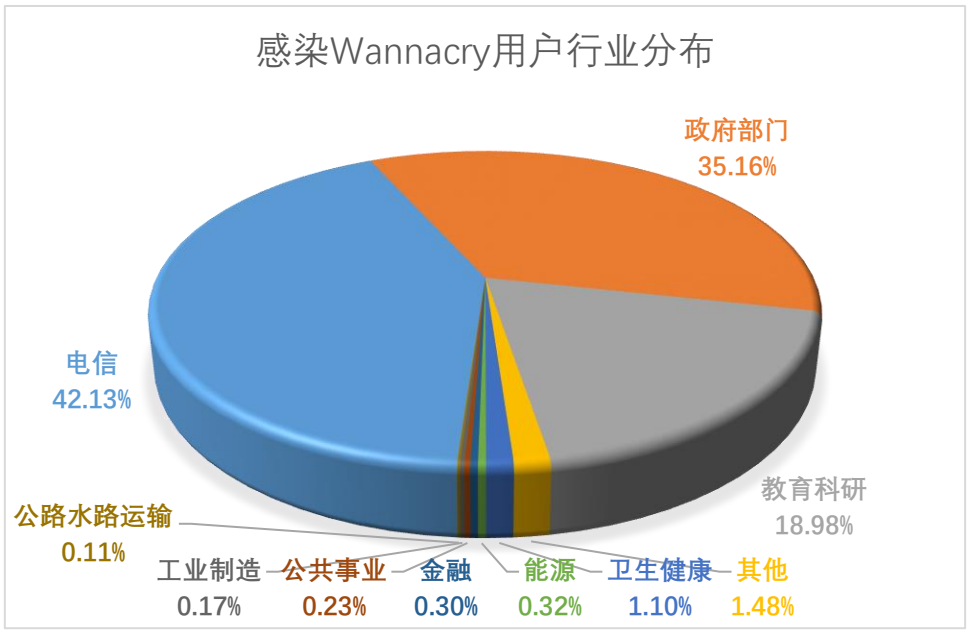
本周，监测发现 2736 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 56.6%，累计感染 104740 次，较上周下降 54.8%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对

常见高危漏洞进行合理加固的现象。



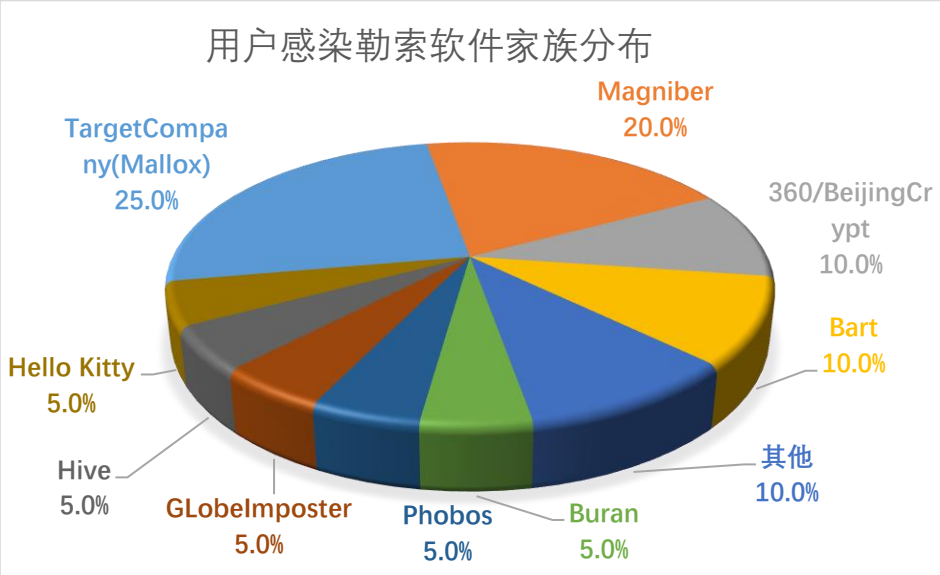


电信、政府部门、教育科研、卫生健康、能源行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

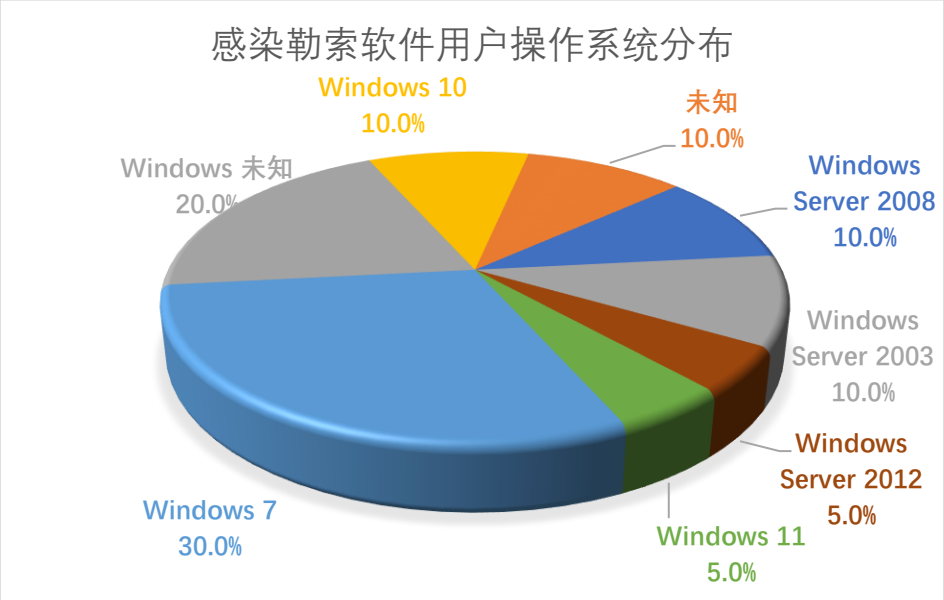


（二）其它勒索软件感染情况

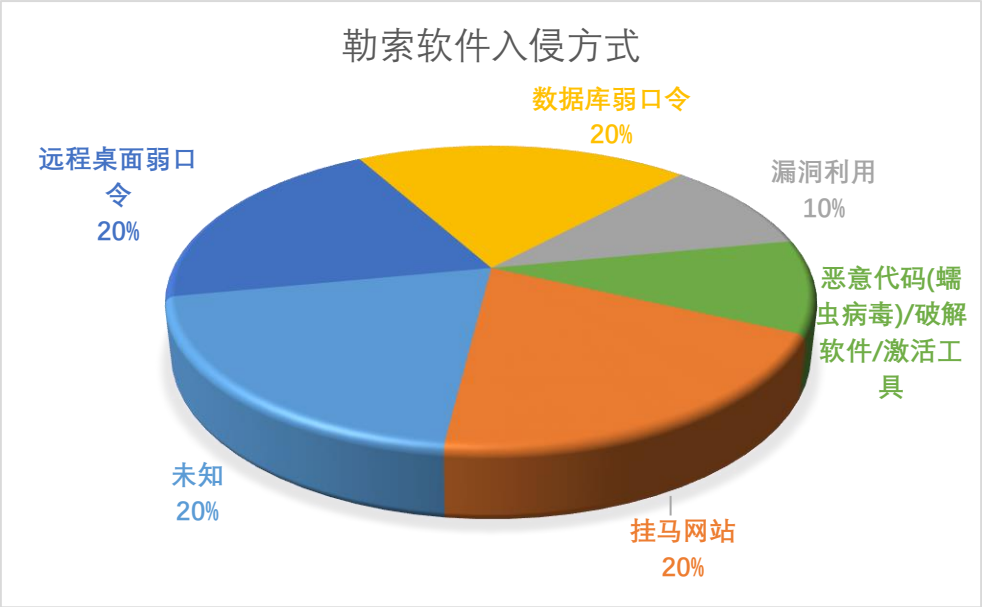
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 20 起，非 Wannacry 勒索软件感染事件，较上周下降 4.8%，排在前三名的勒索软件家族分别为 TargetCompany(Mallox)（25%）、Magniber（20%）和 360/BeijingCrypt（10%）。



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 30 %，其次为 Windows 10 系统和 Windows Server 2008 系统，占比分别为 10%和 10%，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，挂马网站和数据库弱口令占比较高，分别为 20%和 20%。TargetCompany(Mallox)勒索软件通过数据库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、浙江某企业测试服务器遭勒索病毒攻击

本周，工作组成员应急响应了浙江某公司测试服务器遭受勒索病毒攻击事件。攻击者通过外网同账号口令的主机，利用 redis 未授权的漏洞进入内网，通过 netpass 工具进行横向入侵，获取到服务器的 rdp 密码后在备份服务器上使用 msf 来进行内网攻击。应急响应团队已完成现场检查与病毒扫描处理，暂时无法对加密文件进行解密。

针对勒索软件频发的安全状况，企业应定期进行专业的安全评估，及时掌握系统的安全状况。同时配备专业的 Web 应用安全防护设备，应对来自互联网的主流 Web 应用安全攻击。

2、沈阳某公司遭 7Locker 勒索病毒攻击

本周，工作组成员应急响应了沈阳某公司遭遇 7Locker 勒索病毒攻击事件。攻击者通过利用 OA 漏洞尝试向被攻击设备下发 7Locker 勒索病毒，但该次攻击已被工作组成员安全系统拦截。对攻击者的溯

源显示，近期还有多家国内公司遭受到此攻击。

在此事件中，攻击者利用 OA 漏洞多次进行攻击，为避免某次攻击成功导致系统文件被加密，相关企业应尽快升级 OA 系统。

（二） 国外部分

1、勒索软件攻击导致 50 万芝加哥学生数据泄露

5 月 20 日芝加哥公立学校（CPS）学区披露，12 月 1 日对 Battelle for Kids 的勒索软件攻击暴露了其学校系统中 495448 名学生和 56138 名员工的存储数据。学校系统与 Battelle for Kids 合作，上传学生课程信息和评估数据以供教师评估。存储在 Battelle for Kids 服务器上的数据是 2015 至 2019 学年的数据，泄露了学生的个人信息和评估分数。对于员工，威胁参与者可能访问了他们的姓名、学校、员工 ID 号、CPS 电子邮件地址和 Battelle for Kids 用户名。此次攻击中没有暴露任何社会安全号码、家庭住址、健康数据或财务信息。

四、威胁情报

域名

Ugll[.]org

Zerit[.]top

IP

123.213.233.194

172.64.155.188

180.69.193.102

183.78.205.92

104.18.32.68

23.216.147.64

网址

http://20146eb8ae48a040065032e8f628a230rfrwclkp.pitanks[.]info/rfrwclkp

http://20146eb8ae48a040065032e8f628a230rfrwclkp.formto[.]info/rfrwclkp

http://20146eb8ae48a040065032e8f628a230rfrwclkp.beown[.]info/rfrwclkp

http://20146eb8ae48a040065032e8f628a230rfrwclkp.areeye[.]info/rfrwclkp

http://20146eb8ae48a040065032e8f628a230rfrwclkp.lkbvnxzoryoupixdvv5quq7cgeq

q6j2w5ewhwjn7wdmin53jxf4zaiqd[.]onion/rfrwclkp

https://casbin[.]info/campid=18

https://flatis[.]uno/src=6584

https://agorule[.]fun/src=98411

https://vocoto[.]info/src=1990

https://iherda[.]info/src=98457

邮箱

dec_keys@tutanota.com

mallox@stea1thypost.net

maliflynanth@aol.com

devicezzz@tutanota.com

helprecoverthis@mailfence.com

qamrani@airmail.cc

dec_keys@tutanota.com

johnhelper@gmx.de

file_decryption@privatemail.com

supportx@onionmail.com