

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 7 期（总第 15 期）

2 月 12 日-2 月 18 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

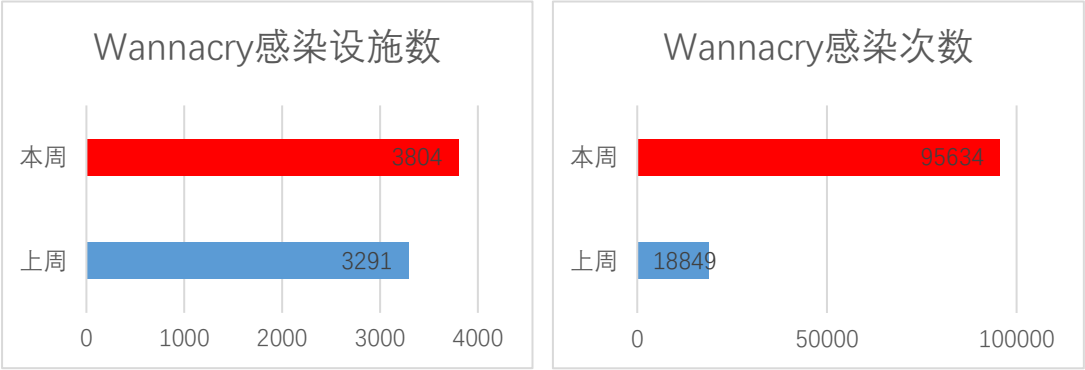
本周勒索软件防范应对工作组共收集捕获勒索软件样本 1480927 个，监测发现勒索软件网络传播 2194 次，勒索软件下载 IP 地址 522 个，其中，位于境内的勒索软件下载地址 201 个，占比 38.5%，位于境外的勒索软件下载地址 321 个，占比 61.5%。

二、勒索软件受害者情况

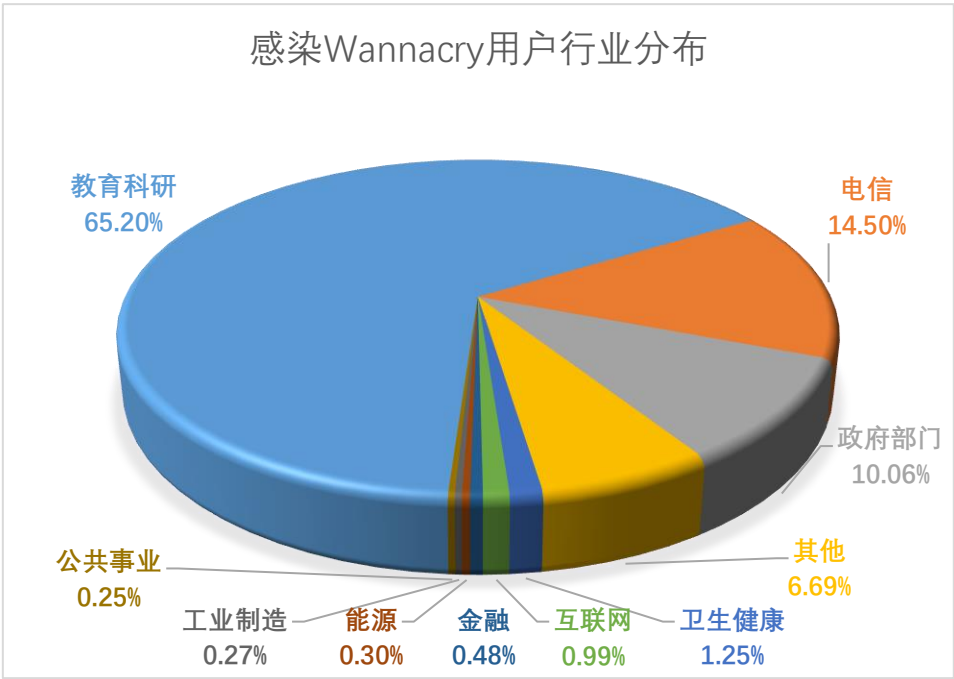
（一）Wannacry 勒索软件感染情况

本周，监测发现 3804 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 15.6%，累计感染 95634 次，较上周上升 407.4%。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。

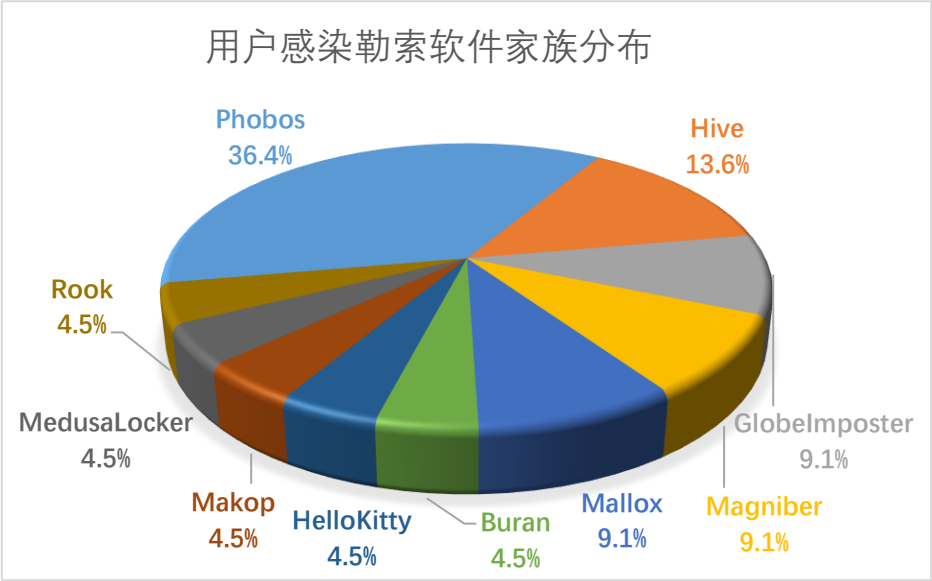


教育科研、电信、政府部门、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

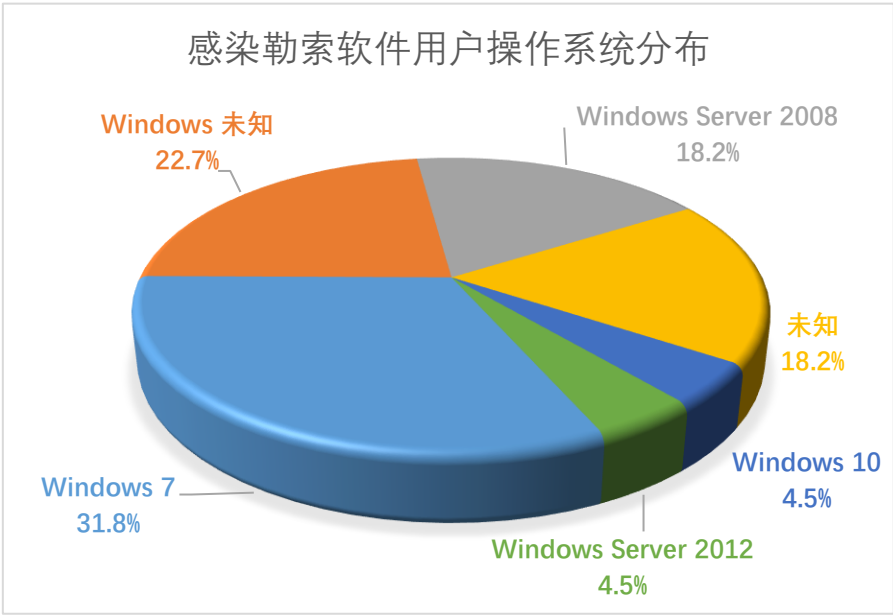


（二）其它勒索软件感染情况

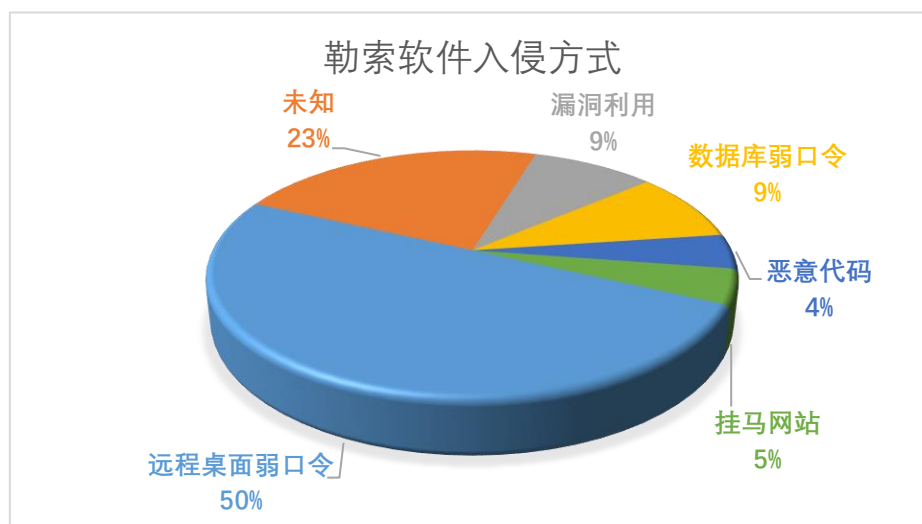
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 22 起非 Wannacry 勒索软件感染事件，事件数与上周相同，排在前三名的勒索软件家族分别为 Phobos（36.4%）、Hive（13.6%）和 GlobeImposter（9.1%）。



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 31.8%，其次为 Windows Server 2008 系统和 Windows 10 系统，占比分别为 18.2%和 4.5%，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，远程桌面弱口令和漏洞利用占比较高，分别为 50%和 9%。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、Coffee 勒索软件新型变种感染国内多所高校和科研机构

本周，工作组成员自主监测并响应了多起 Coffee 勒索软件新型变种感染国内高校和科研机构事件。攻击者通过钓鱼邮件、社交软件或捆绑软件等方式传播勒索软件并对受害者主机上的文件进行加密，将文件后缀修改为.coffee，随后向受害者索要一种不常见的 ZEC 数字货币作为赎金。

此事件中，攻击者通过钓鱼邮件或社交软件等传播勒索软件，建议用户加强网络安全意识，不下载、不接收来源不明的文件，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

（二） 国外部分

1、BlackByte 勒索软件团伙攻击美国关键基础设施

近日，美国联邦调查局（FBI）披露，在过去三个月中，BlackByte 勒索软件团伙至少入侵了三个美国关键基础设施（政府设施、金融、食品和农业）实体。BlackByte 是一个自 2021 年 7 月以来十分活跃的

勒索软件即服务（RaaS）组织，该团伙利用软件安全漏洞获得对其目标网络的初始访问权限，进而植入勒索软件。在 2 月份的最近一次攻击活动中，BlackByte 团伙声称攻击了美国旧金山橄榄球队 49ers 的信息系统，并泄露了近 300MB 的数据文件。

四、威胁情报

IP

104.16.154.36

104.18.30.182

179.43.160.195

72.21.91.29

82.146.53.237

网址

[http://4e40baf8daf43600ba78amkciclkst.gaplies\[.\]fit/mkciclkst](http://4e40baf8daf43600ba78amkciclkst.gaplies[.]fit/mkciclkst)

[http://4e40baf8daf43600ba78amkciclkst.gunfail\[.\]quest/mkciclkst](http://4e40baf8daf43600ba78amkciclkst.gunfail[.]quest/mkciclkst)

[http://4e40baf8daf43600ba78amkciclkst.hjew6l4r3hpgj7qiloum5j7jwq7q3623v4fsbp5edbckeppeetpiihid\[.\]onion/mkciclkst](http://4e40baf8daf43600ba78amkciclkst.hjew6l4r3hpgj7qiloum5j7jwq7q3623v4fsbp5edbckeppeetpiihid[.]onion/mkciclkst)

[http://4e40baf8daf43600ba78amkciclkst.ranmuch\[.\]space/mkciclkst](http://4e40baf8daf43600ba78amkciclkst.ranmuch[.]space/mkciclkst)

[http://4e40baf8daf43600ba78amkciclkst.raredoe\[.\]uno/mkciclkst](http://4e40baf8daf43600ba78amkciclkst.raredoe[.]uno/mkciclkst)

[http://82.146.53\[.\]237/1_cp/gate/gate.php](http://82.146.53[.]237/1_cp/gate/gate.php)

[http://ac6cca681cbcd6d0hqzserk.d7dax5u5qidlzlu73qxscm7r45iix43mc3oycumixp4hfs7cupfp3yd\[.\]onion/hqzserk](http://ac6cca681cbcd6d0hqzserk.d7dax5u5qidlzlu73qxscm7r45iix43mc3oycumixp4hfs7cupfp3yd[.]onion/hqzserk)

[http://ac6cca681cbcd6d0hqzserk.hecould\[.\]xyz/hqzserk](http://ac6cca681cbcd6d0hqzserk.hecould[.]xyz/hqzserk)

[http://ac6cca681cbcd6d0hqzserk.keyspu\[.\]site/hqzserk](http://ac6cca681cbcd6d0hqzserk.keyspu[.]site/hqzserk)

[http://ac6cca681cbcd6d0hqzserk.mybasic\[.\]cyou/hqzserk](http://ac6cca681cbcd6d0hqzserk.mybasic[.]cyou/hqzserk)

[http://ac6cca681cbcd6d0hqzserk.penbit\[.\]space/hqzserk](http://ac6cca681cbcd6d0hqzserk.penbit[.]space/hqzserk)

[http://cdn2546713.cdnmegafiles\[.\]com/data23072021_1.dat](http://cdn2546713.cdnmegafiles[.]com/data23072021_1.dat)

[http://cdnmegafiles\[.\]com/data.dat](http://cdnmegafiles[.]com/data.dat)

[http://chat5sqrnzqewampznybomgn4hf2m53tybkarxk4sfaktwt7oqpkcvyd\[.\]onion/gate](http://chat5sqrnzqewampznybomgn4hf2m53tybkarxk4sfaktwt7oqpkcvyd[.]onion/gate)

.php

[http://get.geojs\[.\]io/v1/ip/geo.js](http://get.geojs[.]io/v1/ip/geo.js)

[http://ocsp.comodoca\[.\]com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU=](http://ocsp.comodoca[.]com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU=)

邮箱

China.Helper@aol.com

equalitytrust@disroot.org

indyan@airmail.cc

Kardon@privatemail.com

Rheinland01@privatemail.com

ustedesfil@cock.li

votredatei@ctemplar.com

钱包地址

1GE6QouwG4HZQP1PBMfGzB68TVnJKoJAGe