

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 2 期（总第 10 期）

1 月 8 日-1 月 14 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

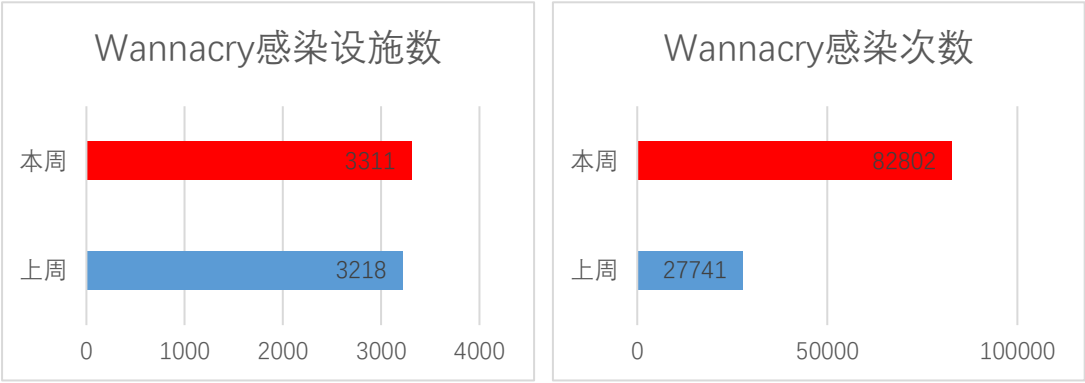
本周勒索软件防范应对工作组共收集捕获勒索软件样本 2027863 个，监测发现勒索软件网络传播 1078 次，勒索软件下载 IP 地址 46 个，其中，位于境内的勒索软件下载地址 21 个，占比 45.7%，位于境外的勒索软件下载地址 25 个，占比 54.3%。

二、勒索软件受害者情况

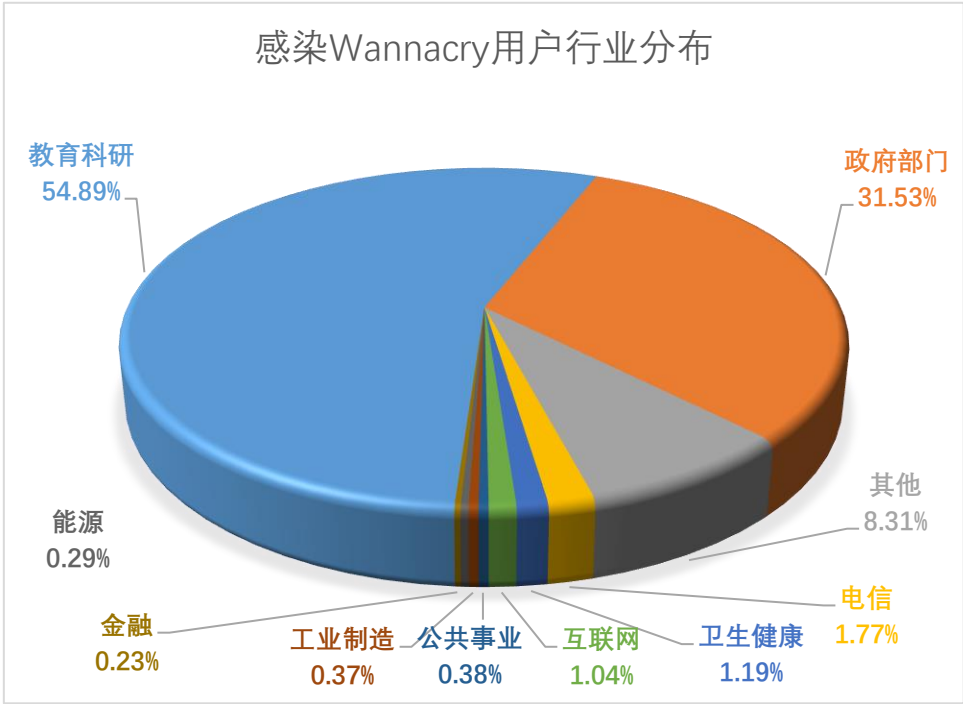
（一）Wannacry 勒索软件感染情况

本周，监测发现 3311 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 2.9%，累计感染 82802 次，较上周上升 198.5%。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。

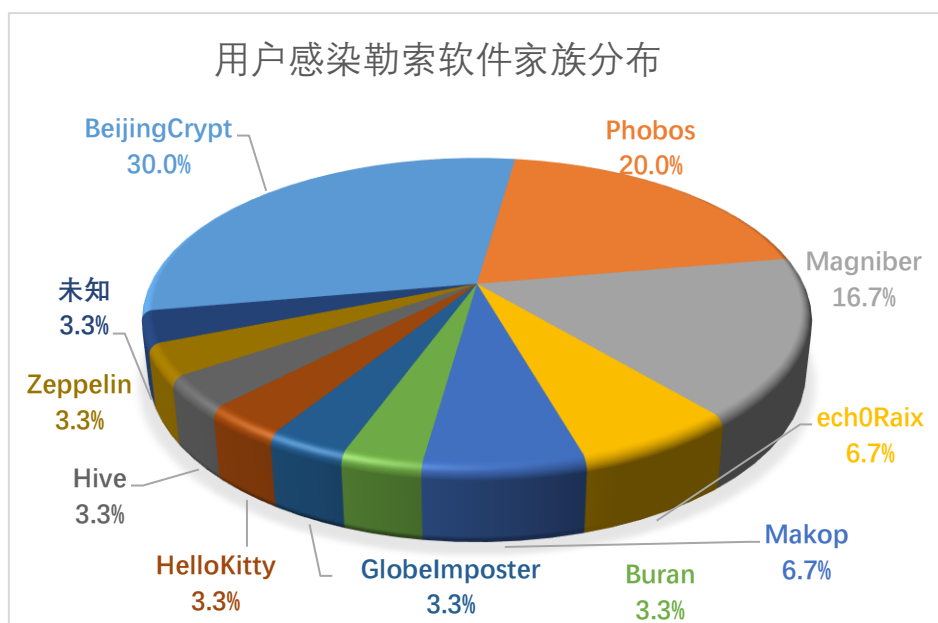


教育科研、政府部门、电信、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

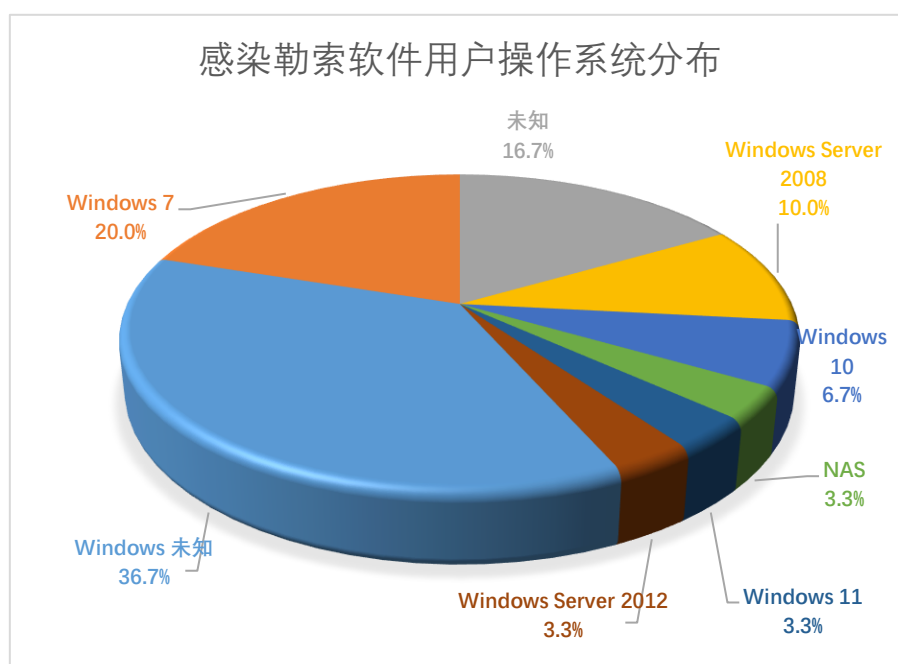


（二）其它勒索软件感染情况

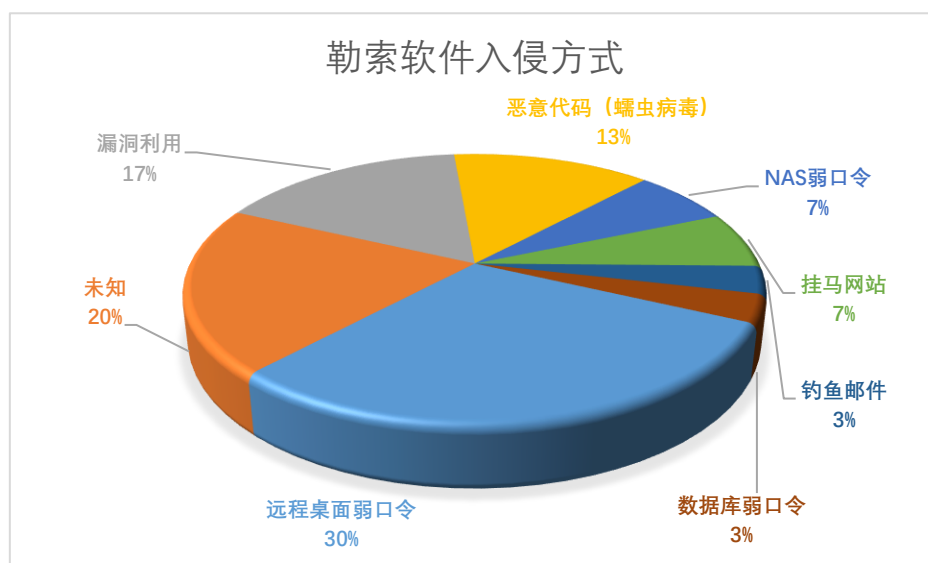
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 30 起非 Wannacry 勒索软件感染事件，较上周上升 7.1%，排在前三名的勒索软件家族分别为 BeijingCrypt（30%）、Phobos（20%）和 Magniber（16.7%）。



本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 20%，其次为 Windows Server 2008 系统，占比为 10%，除此之外还包括多个其它不同版本的 Windows 系统和 NAS 系统等。



本周，勒索软件入侵方式中，远程桌面弱口令排在第一位，其次为漏洞利用和恶意代码（蠕虫病毒）。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、北京某金融企业员工终端感染 Magniber 勒索软件

本周，工作组成员应急响应了北京某金融企业员工终端感染 Magniber 勒索软件事件。攻击者通过挂马网站进行水坑攻击，该企业员工访问挂马网站时触发 CVE-2021-40444 漏洞，随后攻击者获得员工终端的控制权，进而植入勒索软件。

此事件中，攻击者利用 IE 浏览器漏洞获得终端控制权后植入勒索软件。建议用户加强网络安全意识，不访问来源不明的网页，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

2、重庆某企业服务器感染 Makop 勒索软件

本周，工作组成员应急响应了重庆某企业服务器感染 Makop 勒索软件事件。攻击者利用该企业财务服务器远程桌面弱口令漏洞通过暴力破解获得服务器控制权，进而植入勒索软件，随后攻击者进行横向移动，OA 服务器等相继感染勒索软件。

此事件中，攻击者利用远程桌面弱口令获得终端控制权后植入勒索软件。建议用户配置口令复杂度策略、修改弱口令、关闭不必要的服务。

(二) 国外部分

1、教育行业云服务提供商 FinalSite 遭受勒索软件攻击

FinalSite 是一家教育行业云服务提供商，为全球 115 个国家逾 8000 所学校提供 SaaS 服务。近日，FinalSite 遭到勒索病毒攻击，导致约 5000 所学校网站被迫关停，受影响的功能包括组织管理、人员管理、注册管理、活动管理、日历管理等。在勒索软件攻击发生 3 天后，FinalSite 恢复了有限的服务，并宣称经过评估在此次事件中并未发现学校敏感数据遭泄露。

四、威胁情报

域名

[www.capitalqi\[.\]com](http://www.capitalqi[.]com)

[sedna-aca\[.\]com](http://sedna-aca[.]com)

[oldhim\[.\]website](http://oldhim[.]website)

[bypile\[.\]uno](http://bypile[.]uno)

[raredoe\[.\]uno](http://raredoe[.]uno)

IP

87.249.50.201

网址

[http://9ac426c8fe989ed08ee85080dvhpeiesml.hillbe\[.\]space/vhpeiesml](http://9ac426c8fe989ed08ee85080dvhpeiesml.hillbe[.]space/vhpeiesml)

[http://ded0884890cc56d0b6805c709lhbrfqvej.hillbe\[.\]space/lhbrfqvej](http://ded0884890cc56d0b6805c709lhbrfqvej.hillbe[.]space/lhbrfqvej)

[http://d6641eb832f444e048d4e8a8ztjyqtdwo.vastlow\[.\]quest/ztjyqtdwo](http://d6641eb832f444e048d4e8a8ztjyqtdwo.vastlow[.]quest/ztjyqtdwo)

[http://38acfc1854005420c67cec087lhbrfqvej.hillbe\[.\]space/lhbrfqvej](http://38acfc1854005420c67cec087lhbrfqvej.hillbe[.]space/lhbrfqvej)

[http://c0c892b80e98b830dcc420a8f4685pxqcskm.netlaws\[.\]fit/pxqcskm](http://c0c892b80e98b830dcc420a8f4685pxqcskm.netlaws[.]fit/pxqcskm)

[http://c0c892b80e98b830dcc420a8f4685pxqcskm.cellgot\[.\]uno/pxqcskm](http://c0c892b80e98b830dcc420a8f4685pxqcskm.cellgot[.]uno/pxqcskm)

[http://dcc8ae407c58fe20cc58b8c80uczxpgyf.selllet\[.\]quest/uczxpgyf](http://dcc8ae407c58fe20cc58b8c80uczxpgyf.selllet[.]quest/uczxpgyf)

[http://dcc8ae407c58fe20cc58b8c80uczxpgyf.hotknew\[.\]space/uczxpgyf](http://dcc8ae407c58fe20cc58b8c80uczxpgyf.hotknew[.]space/uczxpgyf)

[http://1c90c83076fc6c40c45482c05lhbrfqvej.drymile\[.\]fit/lhbrfqvej](http://1c90c83076fc6c40c45482c05lhbrfqvej.drymile[.]fit/lhbrfqvej)

[https://documentprotect\[.\]live/](https://documentprotect[.]live/)

[http://apps.identrust\[.\]com/roots/dstrootcax3.p7c](http://apps.identrust[.]com/roots/dstrootcax3.p7c)

[https://bit\[.\]ly/2vQQ9Xo](https://bit[.]ly/2vQQ9Xo)

[http://loki-locker\[.\]one/index.php](http://loki-locker[.]one/index.php)

[http://b5305c364336bqd.bytesoh\[.\]cam](http://b5305c364336bqd.bytesoh[.]cam)

[http://hadhill\[.\]quest/376s53290a9n2j](http://hadhill[.]quest/376s53290a9n2j)

邮箱

walter1964@mail2tor.com

Elbowtalk@my.com

beijing5200@mailfence.com

isecondhelperforunlockyourfiles@airmail.cc

guan_yu@tutanota.com

veronikstreem@protonmail.com

钱包地址

1K25DjGJuqPK3cgKW15WmHXahuvAfUomVU

14jM4D2EEFDabh9AYbdNyf8vUXecLxN6YP

15ZbYFRyKyPA2rSauKX3YEF5KiJ6eLhT4V

17N1gQLD5XGe4fuo8akpBf1SWz8cEfUahq

1CBVqeKU2WJPsLYKgg6bndcc4rVuYXwCMu

1DF6iohtKNvQYNZmKX9z8DTevnBbaZWn7c

1FKuAv8ydAww498yev7wEhau5YmQfeJ8DA

1FsUiCDjPMVq3sq8R33viQxVu61tAHj9Aa

1G3oeG3fFs9Eo5Uc1cMfqsFgkd4yCCC1sh

1FEkT4oSkaFiaSfDYpKt1RZx2inoHXjpx7