国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2022 年第 3 期（总第 11 期）　　1 月 15 日-1 月 21 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

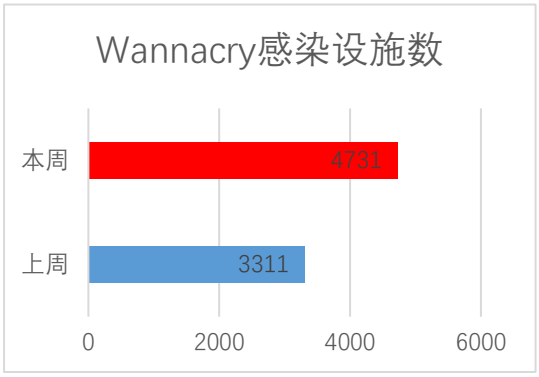
本周勒索软件防范应对工作组共收集捕获勒索软件样本 2430061 个，监测发现勒索软件网络传播 1078 次，勒索软件下载 IP 地址 46 个，其中，位于境内的勒索软件下载地址 21 个，占比 45.7%，位于境外的勒索软件下载地址 25 个，占比 54.3%。

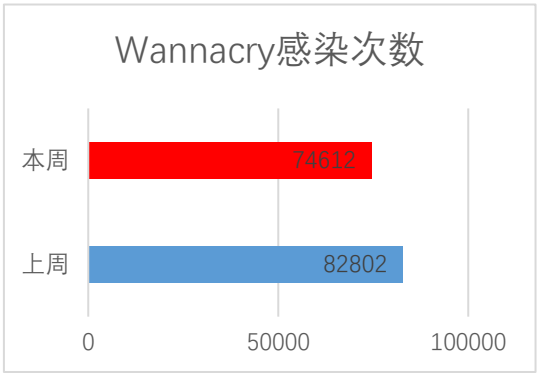
二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

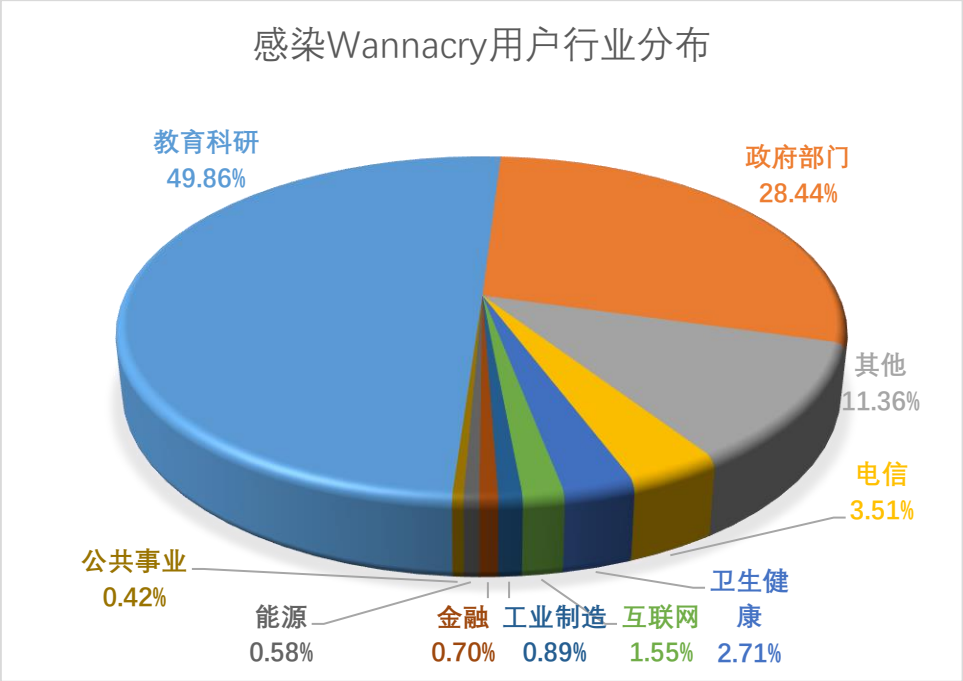
本周，监测发现 4731 起我国单位设施感染 Wannacry 勒索软件事件，较上周上升 42.9%，累计感染 74612 次，较上周下降 9.9%。与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见

高危漏洞进行合理加固的现象。



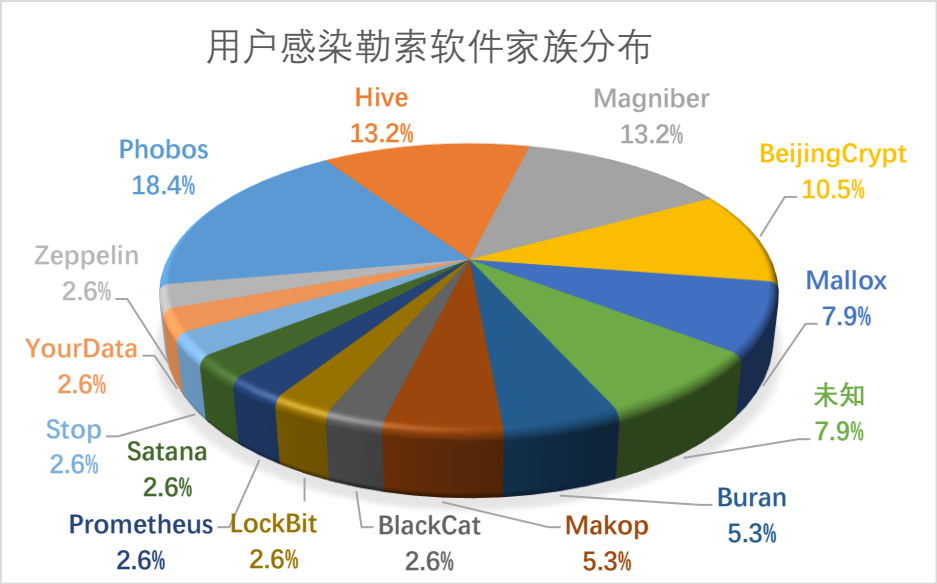


教育科研、政府部门、电信、卫生健康、互联网行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

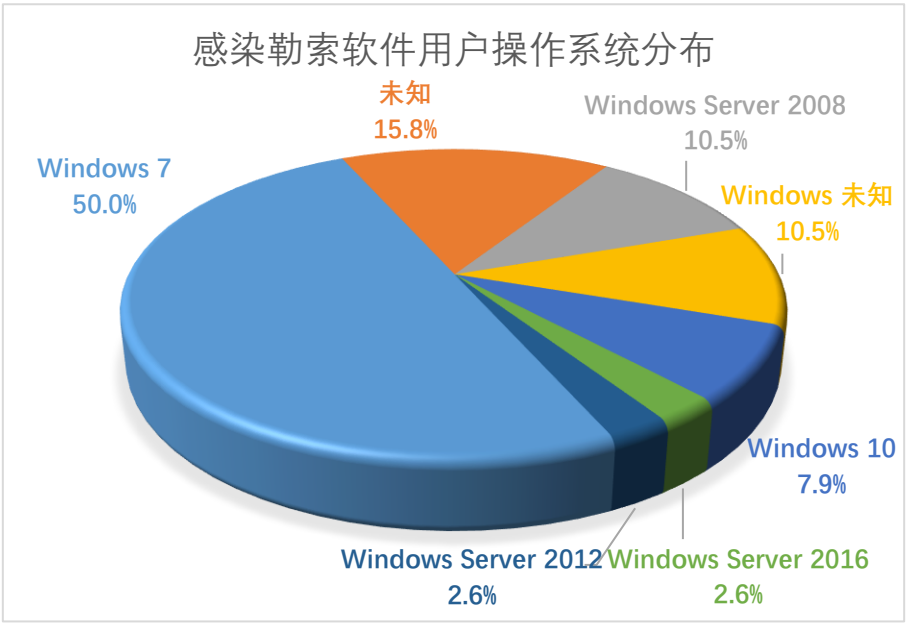


（二）其它勒索软件感染情况

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 38 起非 Wannacry 勒索软件感染事件，较上周上升 26.7%，排在前三名的勒索软件家族分别为 Phobos（18.4%）、Hive（13.2%）和 Magniber（13.2%）。

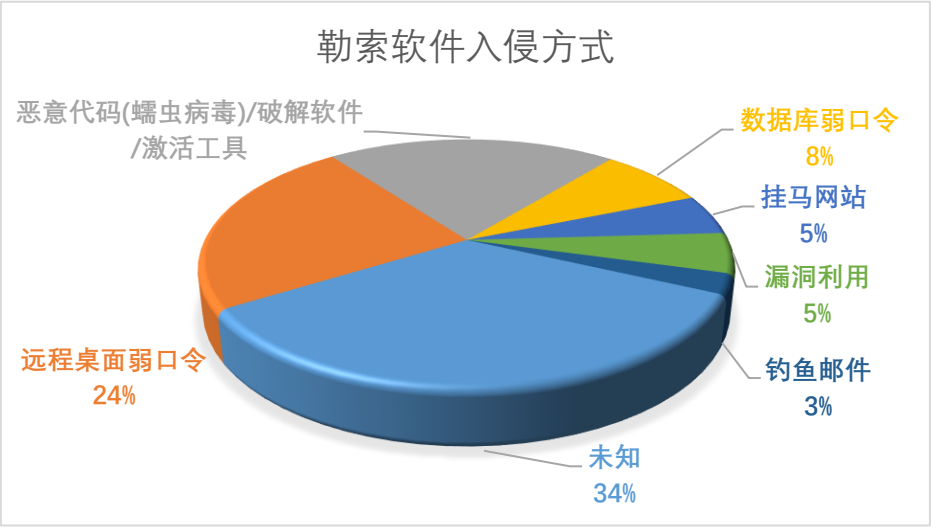


本周，被勒索软件感染的系统中 Windows 7 系统占比较高，占到总量的 50%，其次为 Windows Server 2008 系统，占比为 10.5%，除此之外还包括多个其它不同版本的 Windows 桌面版本和服务器版本系统。



本周，勒索软件入侵方式中，远程桌面弱口令排在第一位，其次为恶意代码（蠕虫病毒）/破解软件/激活工具和数据库弱口令。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、安徽某医院运维服务器感染 Phobos 勒索软件

本周，工作组成员应急响应了安徽某医院运维服务器感染 Phobos 家族勒索软件事件。攻击者发布包含勒索病毒的网络运维工具（端口扫描类）提供给用户下载，受害用户通过运行该网络运维工具进而被勒索病毒感染。

此事件中，攻击者通过捆绑了勒索病毒的工具软件感染并控制受害者主机，建议用户加强网络安全意识，不下载来源不明的软件，及时安装软件安全补丁修复漏洞，对重要的数据定期备份。

2、山西某企业服务器感染 Zeppelin 勒索软件

本周，工作组成员应急响应了山西某企业服务器感染 Zeppelin 勒索软件事件。攻击者通过该企业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，在企业内网中进一步传播勒索病毒。

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、国防承包商 Hensoldt 遭 Lorenz 勒索软件攻击

Hensoldt 是一家总部位于德国的跨国国防承包商，为包括美国海军陆战队等多国防务部门提供雷达、航电设备等解决方案。近日，Hensoldt 发言人证实其英国子公司的部分系统感染了 Lorenz 勒索软件。Lorenz 勒索软件组织也声称在攻击期间从 Hensholdt 的网络中窃取了大量敏感文件。该事件是一起典型的双重勒索模式，即在加密数据之前先窃取数据，并在受害者不支付勒索金的情况下威胁公开其敏感数据。

四、威胁情报

域名

104-168-132-128.nip[.]io

b5305c364336bqd.bytesoh[.]cam

hadhill[.]quest

iplogger[.]org

IP

20.82.210.154

162.159.129.233

162.159.130.233

162.159.135.233

网址

http://193.201.9.212/enc[.]exe

http://66083a00683c8txzbnxw.gaplies[.]fit/txzbnxw

http://66083a00683c8txzbnxw.raredoe[.]uno/txzbnxw

http://b8ccdea8663c7fteherut.gaplies[.]fit/fteherut

http://b8ccdea8663c7fteherut.raredoe[.]uno/fteherut

http://dweb.link/ipns/help.none[.]sbs/help.pdf

http://help.none.sbs.ipns.cf-ipfs[.]com/help.pdf

http://ipfs.cf-ipfs.com/ipns/help.none[.]sbs/help.pdf

http://iplogger[.]org/1DLTt7.gz

http://ocsp.comodoca[.]com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uF
qgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5
IrdR19NsEN0xNZU=

https://cdn.discordapp[.]com/attachments/928503440139771947/93010863768118476
8/Tbopbh.jpg

https://gateway.pinata[.]cloud/ipns/help.none.sbs/help.pdf

https://help.none.sbs.ipns.ipfs.overpi[.]com/help.pdf

https://ipfs.fleek.co/ipns/help.none[.]sbs/help.pdf

邮箱

helpunlock@aol.com

monster666@tuta.io

proper12132@tutanota.com

qazqwe@msgsafe.io

qazqwe@onionmail.org

recoveryfiles@techmail.info

钱包地址

bc1qqxck7kpzgvud7v2hfyk55yr45fnml4rmt3jasz

1K25DjGJuqpK3cgKW15WmHXahuvAfUomVU

12AhNbxfWKQsNGrJQGLVkVTHidKKiFh9Lm

17b4LrnmyRWQAFsz4chyruvT6DypPzwS69

1MwMXpkdgBVWabgGYQZinCGhBbLpLPUrrq

1LqVRgyNUQjEh1cFXJq6woKPJnpsiCbJca

16ZWEeHnck7RLEtBLdPc9bRzGbWJtaGSxo

13LiiH6H6R2HDfQ1JFCJ5Ww3nZ6W1JBy88

1FCRWevHobMdN2pVgvLk8GqrABUZT99pyn

13aZ1hTdjNKQmfJNTRCeyvWgVSgUcWLLfH