

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 2 期

11 月 13 日-11 月 19 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

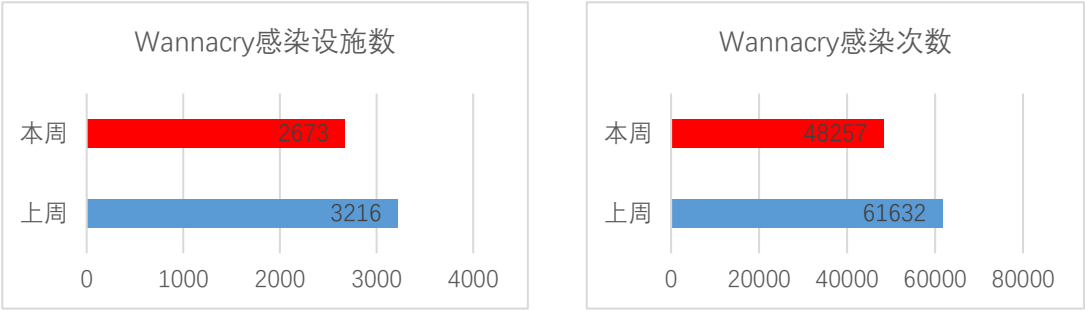
本周勒索软件防范应对工作组共收集捕获勒索软件样本 435872 个，监测发现勒索软件网络传播 4960 次，勒索软件下载 IP 地址 226 个，其中，位于境内的勒索软件下载地址 29 个，占比 12.8%，位于境外的勒索软件下载地址 197 个，占比 87.2%。

二、勒索软件受害者情况

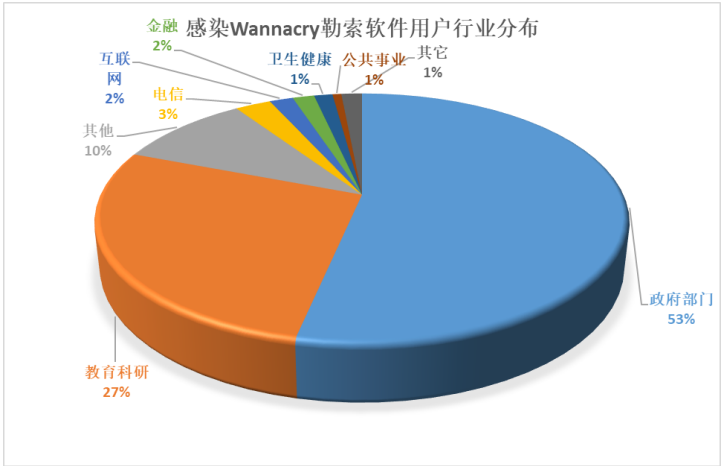
（一）Wannacry 勒索软件感染情况

本周，监测发现 2673 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 16.9%，累计感染 48257 次，较上周下降 21.7%。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。

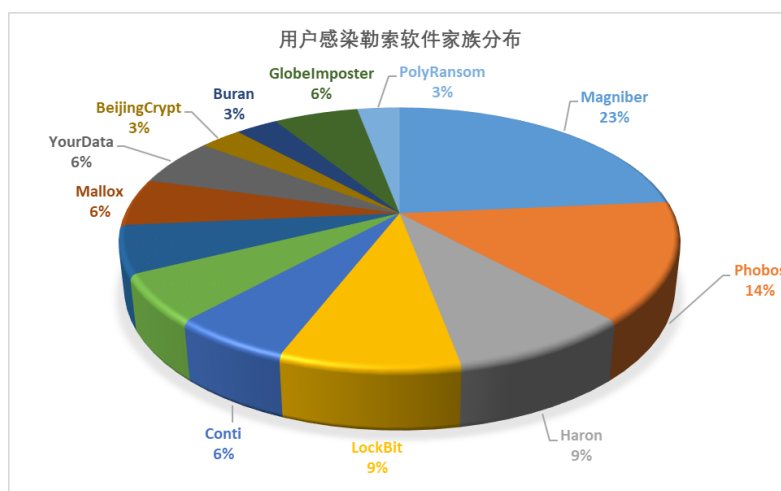


政府部门、教育科研、互联网、电信、金融行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反应，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

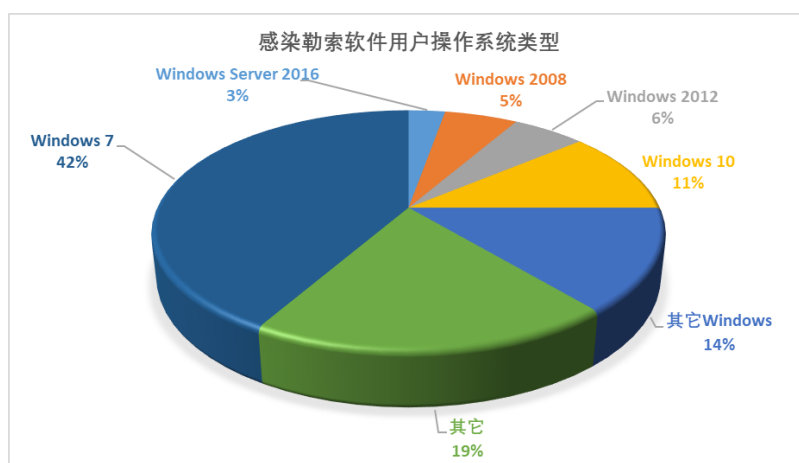


(二) 其它勒索软件感染情况

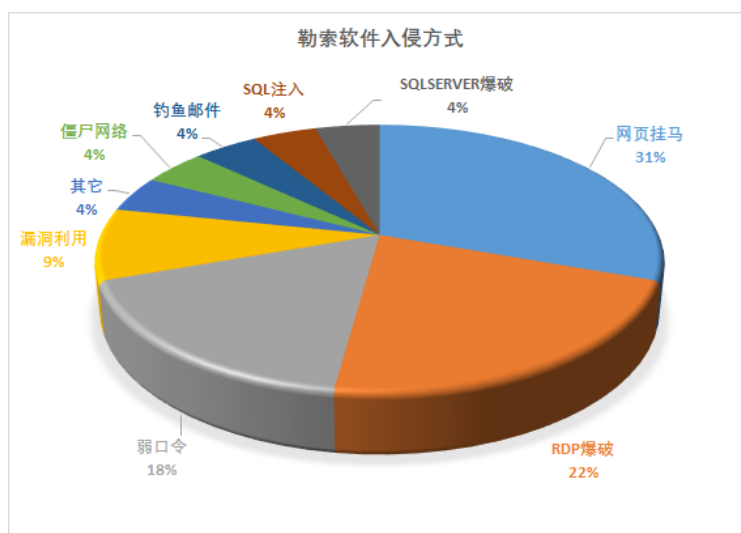
本周勒索软件防范应对工作组自主监测、接收投诉或应急响应 36 起非 Wannacry 勒索软件感染事件，排在前三名的勒索软件家族分别为 Magniber（23%）、Phobos（14%）和 Haron（9%）。Magniber 勒索软件攻击事件本周排名第一，主要是 11 月底 Magniber 利用 CVE-2021-40444 和 CVE-2021-26411 两个漏洞对我国境内用户频繁攻击，入侵主要方式为网页挂马，通过色情网站的广告进行传播。



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 42%，其次为 Windows10 系统，占比为 11%，除此之外还包括较多不同版本的 Windows 服务器系统，占比 14%。



本周，由于 Magniber 勒索软件通过网页放马传播攻击活动活跃，勒索软件入侵方式中，网页挂马排在第一位，其次为 Windows 远程桌面爆破和弱口令。



三、典型勒索软件攻击事件

(一) 国内部分

1、国内多家企业遭受泄密型勒索软件攻击

近日, LockBit、Haron、Conti 等多个勒索软件家族频繁发动攻击, 并对受害企业发起泄密威胁。目前已知受到此轮攻击影响的企业中, 有 9 家为国内企业, 涉及金融、能源、制造和零售等行业。

2、国内多家医院感染勒索软件

11 月 13 日, 安徽某医院多台服务器感染 520 勒索软件, 攻击者通过 RDP 爆破方式获取服务器控制权, 并通过网络共享在内网传播勒索软件。

11 月 16 日, 广东省某医院 OA 共享磁盘文件被加密勒索, 加密文件后缀名为.devos, 勒索软件家族为老牌勒索软件 phobos。攻击者利用 RDP 爆破入侵医院主机, 并利用 RDP 或 SMB 暴力破解, 获取更多内网主机访问权限, 并利用内网设备间的文件共享对 OA 共享磁盘加密。

这些事件中攻击者利用不安全的 RDP 配置来入侵网络，并通过网络共享实现勒索软件在内网的传播和加密勒索行为。建议用户使用高强度密码来应对这种爆破攻击并引入多因素身份验证作为额外的安全保障，并严格控制共享文件夹权限。

(二) 国外部分

1、新黑客组织 “MosesStaff”以以色列公司为目标进行破坏性攻击

11 月初，一个名为 “MosesStaff” 的神秘黑客组织出于政治原因对以色列国防部发动了网络攻击，获取了一些 “军队部署信息”，并对外发布了一些声称是从以色列国防部服务器获取的文件和照片。

“MosesStaff” 在官网声称，该组织入侵了 165 个服务器和 254 个网站，收集了超过 11TB 的数据。

四、威胁情报

MD5

A00F2DA30BC03EEDD9D307826B36B48B
BB09E9B8DAEF63D4EBE21FCB2519C5D5
1CC5B508DA9567F032ED78375BB45959
7CD5B1D26AC2BBCC2D14C9AD93347292
7B760F60FFF500D3C7C408A8BC158E0E
A06C125E6DA566BE67AACF6C4E44005E
FC93ECB882FBC1BAC46AAF4232CE9B66
2C1BACB056654515171BEDADAECFE67E
2A37DA5634B1E4B188FC5EF86704E41B
34B2AAD3AB44EF46ECFE5C41F2DC2E9D
EC54D06ADD793A2642B7CEF9FF958B9D

31F6D8C58AD986E8AB428CBAEC5A10F6
DAC3710EB5C87843FD76996AF39E29CD
315AAF1F0128E50999FD5B82949A9267

IP

27.102.66.114
27.102.127.120
45.77.76.158:25643
190.144.115.54:443
195.201.124.214:10001
78.138.105.150:11180
51.141.64.54
78.138.105.150
27.102.127.120
123.45.67.89
190.144.115.54
169.51.60.221
183.110.224.164
195.201.124.214
27.102.66.114
45.77.76.158

域名

ovelupdate.com
checkvisa.xyz
google.onedriver-srv.ml

URL

<http://curlmyip.net>

<http://google.onedriver-srv.ml/gadfTs55sghsSSS>

<http://lurchmath.org/wordpress-temp/wp-content/plugins/xmrig.zip>

<http://78.138.105.150:11180/sv.php>

邮箱

friend.dec@yandex.ru

friend.dec@keemail.me

zsebas@arimail.cc

kameric@airmail.cc

sazepa@tuta.io

yourfriendz@techmail.info

bob_marley2021@libertymail.net

decrypt20@firemail.cc

钱包

1BTgrpARc6CoQy9M5Q9ivz4BbkqVjSwpoM

1MzQZfamKtJuckckh7DG7yMK5tpHBcQAoS

1AGXbb72TonM9yosKFh3y7bAViP5L57jsX

12VF6Zj5Sz1PVPuB4fWUtCPPtp43SYkTvf

12kZ3L5xU5cVFrPZayuFNSjmh4KFCMuaWt

13zghd1F8es1vGiXcox19CKpWbQ2PqR3h4