

国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 6 期

12 月 11 日-12 月 17 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

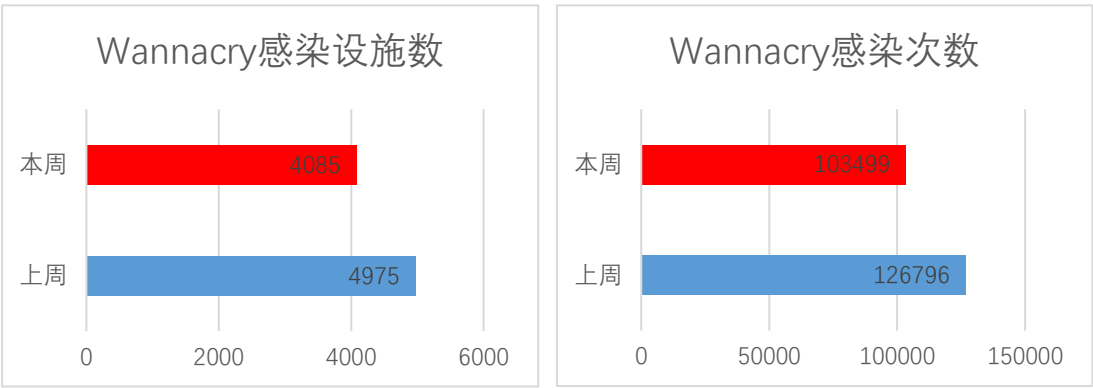
本周勒索软件防范应对工作组共收集捕获勒索软件样本 434755 个，监测发现勒索软件网络传播 2699 次，勒索软件下载 IP 地址 33 个，其中，位于境内的勒索软件下载地址 18 个，占比 54.5%，位于境外的勒索软件下载地址 15 个，占比 45.5%。

二、勒索软件受害者情况

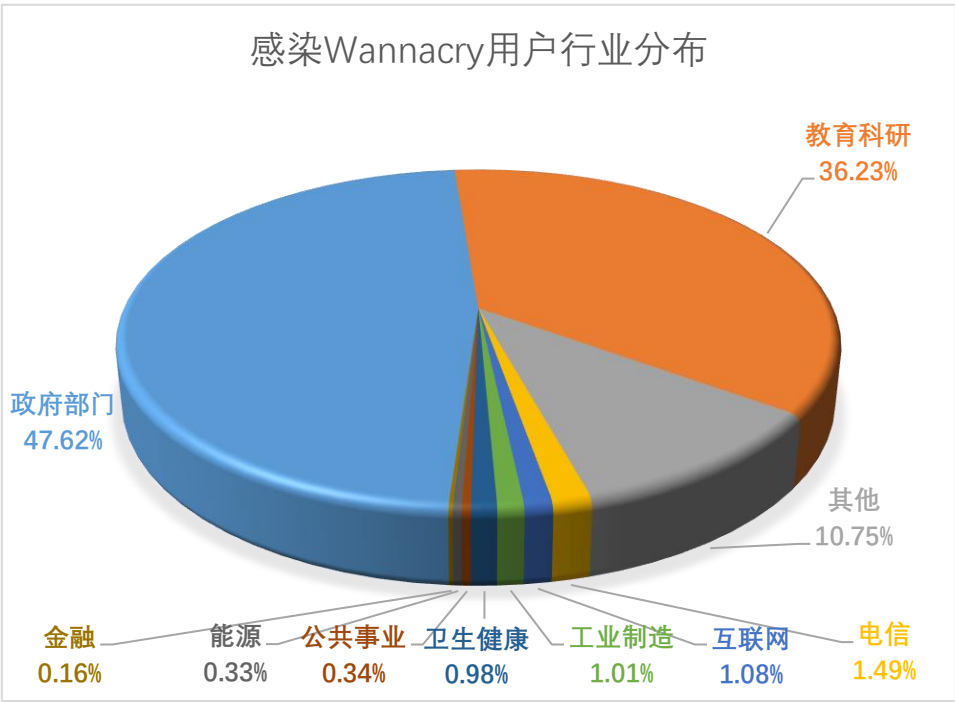
（一）Wannacry 勒索软件感染情况

本周，监测发现 4085 起我国单位设施感染 Wannacry 勒索软件事件，较上周下降 17.9%，累计感染 103499 次，较上周下降 18.4%。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。

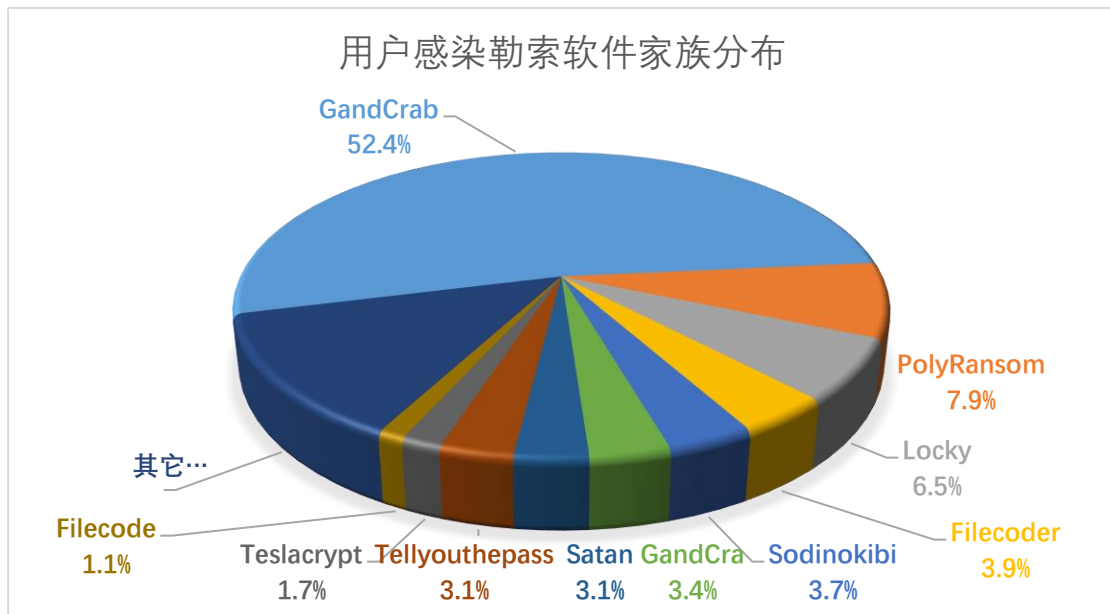


政府部门、教育科研、电信、互联网、工业制造行业成为 Wannacry 勒索软件主要攻击目标，从另一方面反映，这些行业中存在较多未修复“永恒之蓝”漏洞的设备。

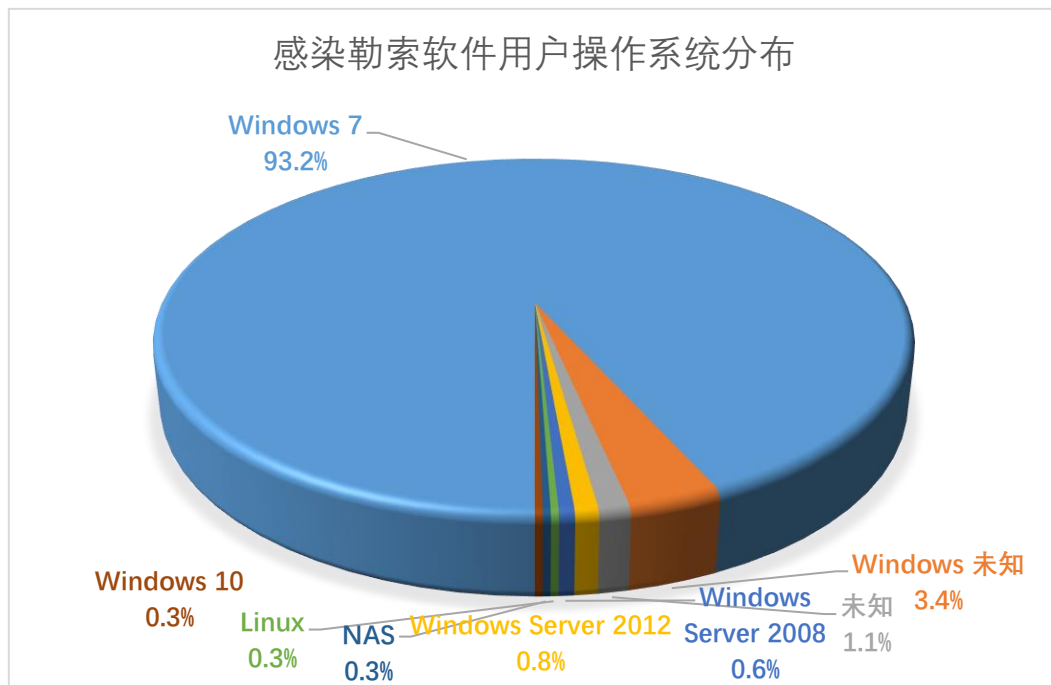


（二）其它勒索软件感染情况

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 355 起非 Wannacry 勒索软件感染事件，较上周上升 1443.5%，排在前三名的勒索软件家族分别为 GandCrab（52.4%）、PolyRansom（7.9%）和 Locky（6.5%）。

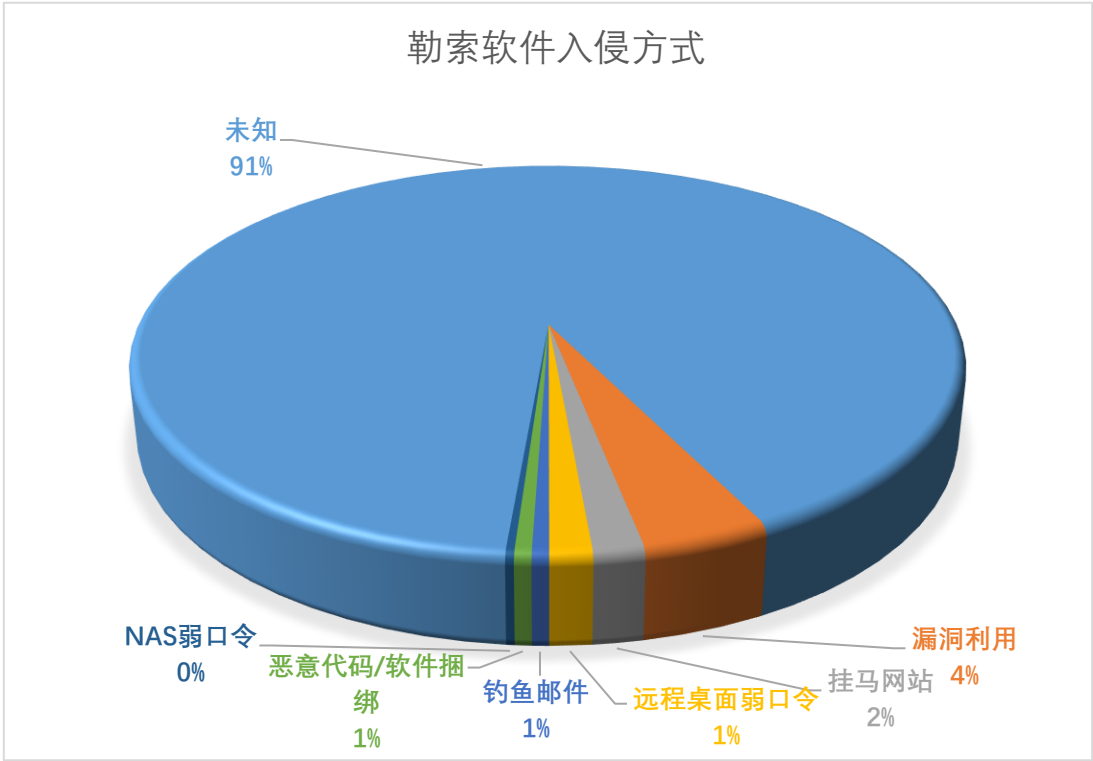


本周，被勒索软件感染的系统中 Windows7 系统占比较高，占到总量的 93.2%，其次为 Windows Server 2012 和 Windows Server 2008 系统，占比分别为 0.8%和 0.6%，除此之外还包括多个其它不同版本的 Windows 服务器系统和其它类型的操作系统。



本周，勒索软件入侵方式中，漏洞利用排在第一位，其次为挂马网站和远程桌面弱口令。Tellyouthepass 勒索软件利用最近爆出的

Apache Log4j 漏洞攻击我国多个行业用户，对我国企事业单位带来较大安全威胁。



三、典型勒索软件攻击事件

（一）国内部分

1、多起利用最新 Log4j 漏洞感染 Tellyouthepass 勒索软件

本周，工作组成员单位自主监测结果显示，多起投递 Tellyouthepass 勒索软件的攻击者使用 Apache Log4j 漏洞对网络上暴露的某品牌 OA 产品发起勒索攻击，近 300 台部署了存在上述漏洞的 OA 服务器遭到攻击。

此事件中，攻击者利用存在最新 Apache Log4j 漏洞（CVE-2021-44228）的某 OA 产品发起勒索攻击，首先获得服务器的控制权，再植入 Tellyouthepass 勒索软件。建议用户尽快修复 CVE-2021-44228 漏洞。

2、山西某医院多台服务器感染 LockBit 勒索软件

近日，工作组成员单位应急响应了山西某医院 HIS 系统、PACS 系统等服务器感染 LockBit 勒索软件事件。攻击者通过软件捆绑勒索软件的方式传递攻击载荷，医院用户在其中一台服务器上下载并激活了 LockBit 勒索软件，随后 LockBit 勒索进行横向移动，扫描并持续感染本地网络中存在漏洞的其他主机。

LockBit 勒索病毒目前尚没有公开的解密工具，感染后造成目标主机的服务中断和数据破坏。建议用户加强信息安全意识宣贯，定期检测系统漏洞并及时修复。

（二） 国外部分

1、美国弗吉尼亚州 IT 机构遭受勒索软件攻击

弗吉尼亚州官员周一表示，为弗吉尼亚州立法机构提供服务的信息技术机构遭到勒索软件攻击，严重影响了其运营。州长发言人证实了这起对弗吉尼亚州立法自动化系统部门的攻击事件。在提供给美联社的一份简短声明中显示，州长已听取了有关此事的简报并指示行政部门提供帮助，以“评估和应对这种持续的情况”。

立法自动化系统司(DLAS)是议会的 IT 下属机构。此次袭击发生的时机尤为敏感，因为议员和工作人员正在为定于 1 月开始的立法会议做深入准备。此次攻击也标志着过去一年爆发的勒索病毒大规模事件迎来了的最新一波针对政府、关键基础设施和大公司的攻击。

四、威胁情报

域名

test.verble[.]rocks

abidu[.]com

wwbaidu[.]com

test.verble[.]rocks

gawocag[.]com

turkcell[.]info

hiduwu[.]com

IP

108.62.141.87

152.32.216.78

154.247.218.44

158.247.216.148

159.223.31.75

159.69.92.223

18.228.7.109

192.52.167.210

193.56.28.159:80

206.189.49.239

23.152.0.22

23.81.246.32

3.145.115.94

45.130.229.168

47.76.99.222

网址

[http://08005e7062f8f6a058386400yrexcygf.bothbox\[.\]quest/yrexcygf](http://08005e7062f8f6a058386400yrexcygf.bothbox[.]quest/yrexcygf)

[http://08005e7062f8f6a058386400yrexcygf.owepeak\[.\]space/yrexcygf](http://08005e7062f8f6a058386400yrexcygf.owepeak[.]space/yrexcygf)

[http://159.69.92\[.\]223/freebl3.dll](http://159.69.92[.]223/freebl3.dll)

[http://159.69.92\[.\]223/vcruntime140.dll](http://159.69.92[.]223/vcruntime140.dll)

[http://3.145.115\[.\]94/Main.class](http://3.145.115[.]94/Main.class)

[http://3.145.115\[.\]94/zambo/groenhuyzen.exe](http://3.145.115[.]94/zambo/groenhuyzen.exe)

[http://30b4c248c6fc3ab03cf44c106haxqiwaot.gapgun\[.\]fit/haxqiwaot](http://30b4c248c6fc3ab03cf44c106haxqiwaot.gapgun[.]fit/haxqiwaot)
[http://3e2450a82e446c40560c1ae8ixrwjxmay.aerrors\[.\]fit/ixrwjxmay](http://3e2450a82e446c40560c1ae8ixrwjxmay.aerrors[.]fit/ixrwjxmay)
[http://5e6078a018d06ce090a83488dqtvxzxo.bothbox\[.\]quest/dqtvxzxo](http://5e6078a018d06ce090a83488dqtvxzxo.bothbox[.]quest/dqtvxzxo)
[http://5e6078a018d06ce090a83488dqtvxzxo.owepeak\[.\]space/dqtvxzxo](http://5e6078a018d06ce090a83488dqtvxzxo.owepeak[.]space/dqtvxzxo)
[http://7074ac3818005420d2203e701luidyhjxj.hesair\[.\]uno/luidyhjxj](http://7074ac3818005420d2203e701luidyhjxj.hesair[.]uno/luidyhjxj)
[http://9ac426c08aec3c202ca8f428aobevxphbt.gapgun\[.\]fit/obevxphbt](http://9ac426c08aec3c202ca8f428aobevxphbt.gapgun[.]fit/obevxphbt)
[http://b8c49830e2f82a6044906018onmadnmso.enddare\[.\]fit/onmadnmso](http://b8c49830e2f82a6044906018onmadnmso.enddare[.]fit/onmadnmso)
[http://b8c49830e2f82a6044906018onmadnmso.tillpop\[.\]uno/onmadnmso](http://b8c49830e2f82a6044906018onmadnmso.tillpop[.]uno/onmadnmso)
[http://tzgl\[.\]org/fhsgtsspen6/get.php?pid=78649785D38AABDF26106633CC62FD6F
&first=true](http://tzgl[.]org/fhsgtsspen6/get.php?pid=78649785D38AABDF26106633CC62FD6F&first=true)
[http://tzgl\[.\]org/files/1/build3.exe](http://tzgl[.]org/files/1/build3.exe)
[https://koyu\[.\]space/@sergeev45](https://koyu[.]space/@sergeev45)

邮箱

helpstoremanager@airmail.cc
malloxx@tutanota.com
manager@mailtemp.ch
520hard@cock.li
recover520@mailfence.com
520hard@mailfence.com

钱包地址

12Wrpfn8LQh3NPHy6tBpaLAaq2dV813m4c
14wAUrK82EwJunxDDisHnZs57fP4jqUKhx
169soadhr2wSWfVoe5gdG4s8KzhF8wjZWz
17umfMWXdCct5PatyDnz1dUFbE8Dx8QaCF
1AGuPEaGAYagw3NTsE4gjXGtfionmZkxYE
1Cp62HCECArozMHKBu9VQi5Dv7U5sHRjdL
1EW1oXBSnduixrV1Gch2pD38CGk1sfEBth
1Ge1MvxQUqsZJtpWm1xnnEJYfFc56aQwqQ
1K25DjGJuqpK3cgKW15WmHXahuvAfUomVU
1PT5gmsM9BfCSnv8QAcGrMwF8tJiH6gVrK

1Q1wcwtt4hfMmUX3wxYjchLYX5wvxMzg5o
bc1qqxck7kpzgvud7v2hfyk55yr45fnml4rmt3jasz