国家互联网应急中心（CNCERT/CC）

勒索软件动态周报

2021 年第 1 期　　11 月 06 日-11 月 12 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

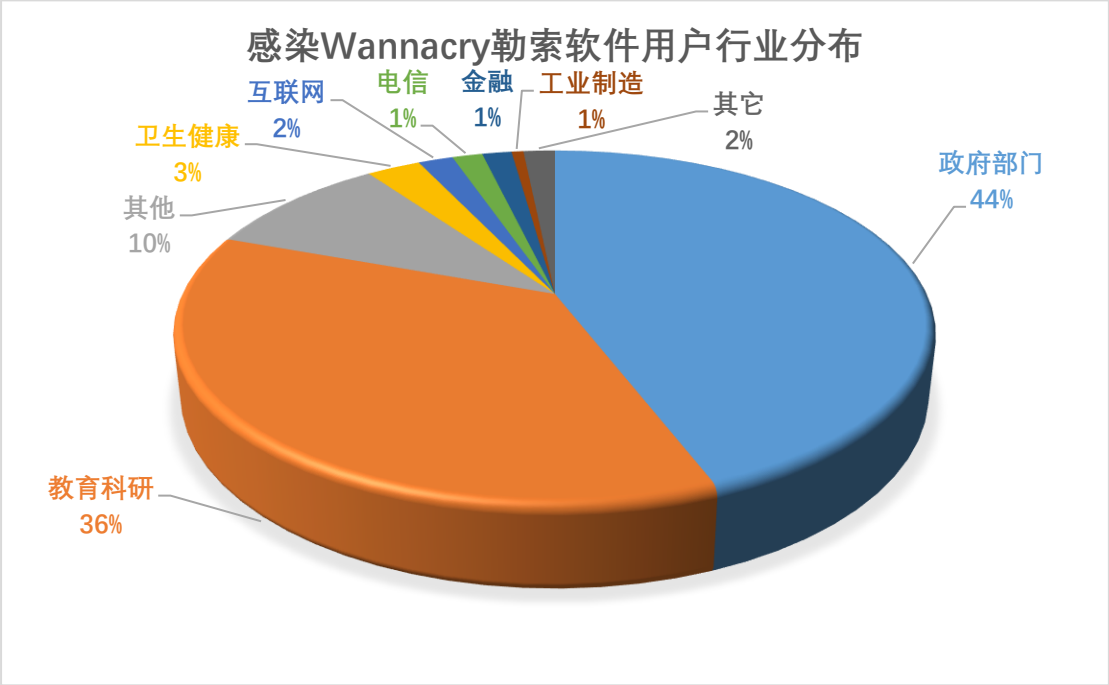
本周勒索软件防范应对工作组共收集捕获勒索软件样本 39257 个，监测发现勒索软件网络传播 2435 次，勒索软件下载 IP 地址 219 个，其中，位于境内的勒索软件下载地址 97 个，占比 44.3%，位于境外的勒索软件下载地址 122 个，占比 55.7%。

二、勒索软件受害者情况

（一）Wannacry 勒索软件感染情况

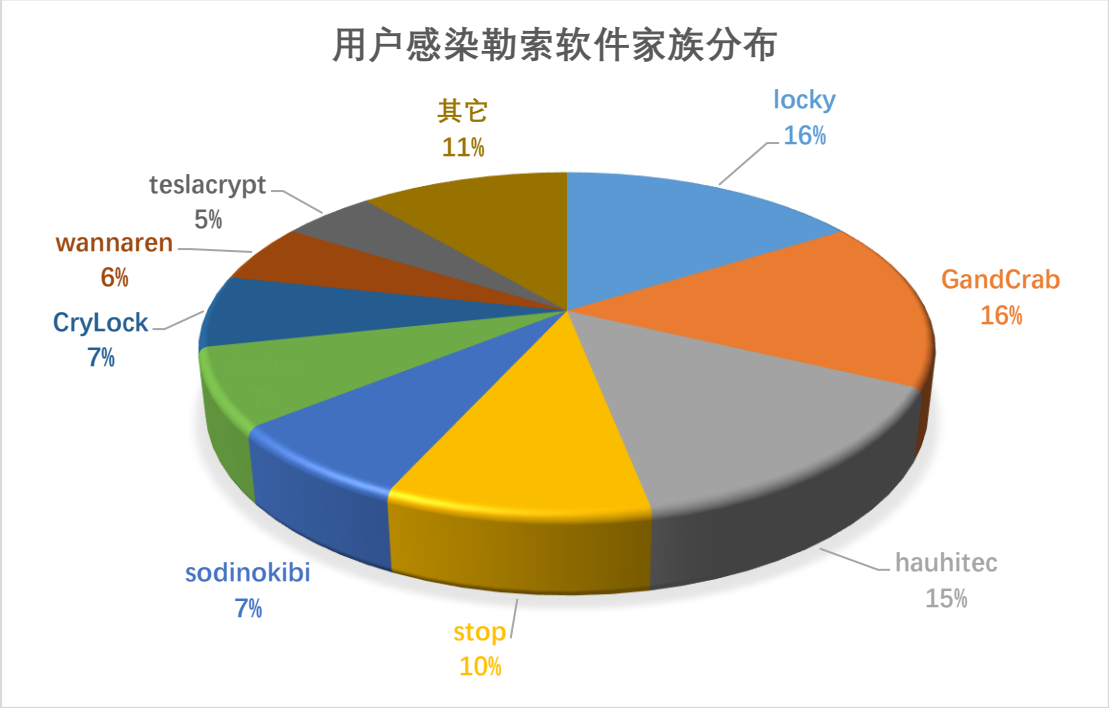
本周，监测发现 3216 起我国单位设施感染 Wannacry 勒索软件事件，累计感染 61632 次，与其它勒索软件家族相比，Wannacry 仍然依靠“永恒之蓝”漏洞（MS17-010）占据勒索软件感染量榜首，尽管 Wannacry 勒索软件在联网环境下无法触发加密，但其感染数据反映了当前仍存在大量主机没有针对常见高危漏洞进行合理加固的现象。

政府部门、教育科研、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。

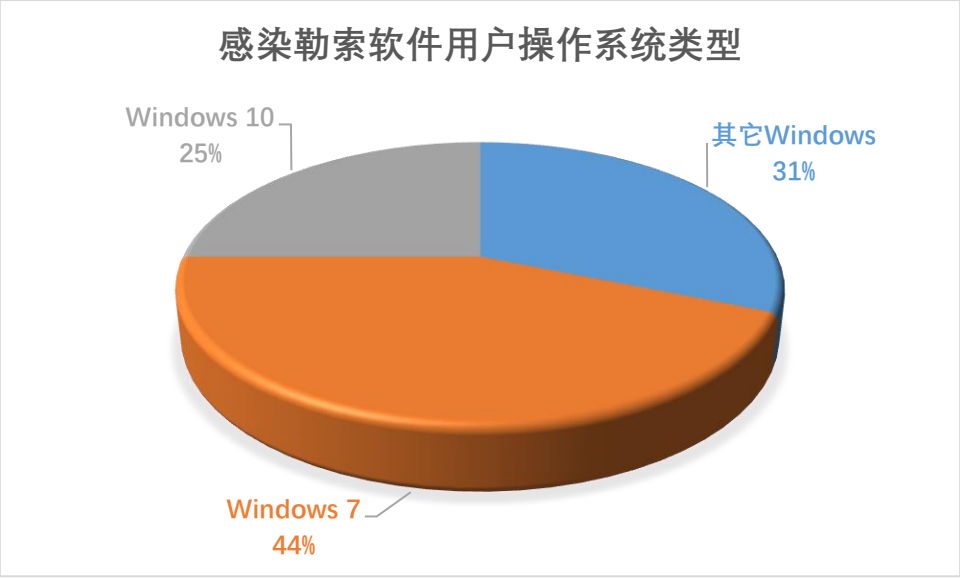


（二）其它勒索软件感染情况

本周勒索软件防范应对工作组接收或监测发现 162 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 locky（16%）、GandCrab（16%）和 hauhitec（15%）。



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 44%，其次为 Windows10 系统，除此之外还包括少量 Windows 服务器系统。



三、典型勒索软件攻击事件

（一） 国内部分

1、YourData 勒索软件正在利用“匿影”僵尸网络大肆传播

近期，安全研究人员发现，YourData 勒索软件正通过“匿影”僵尸网络在国内大肆传播，对个人电脑的威胁愈加强烈。

YourData 勒索软件又被称作 Hakbit、Thanos 家族，最早出现于 2019 年 11 月。但在今年 1 月之前，国内极少出现被该病毒或变种攻击案例。2021 年 1 月开始在国内出现该家族的变种。

在前几个月的病毒传播中，该病毒家族主要采用的攻击手段是 RDP 爆破，在爆破成功后会进行手动投毒，为每一个受害用户生成专属页面。从今年 7 月开始，该病毒家族开始通过“匿影”僵尸网络进行传播，在 10 月开始出现大面积感染的情况。

“匿影”僵尸网络将病毒捆绑在非正规渠道的 BT 下载器、安装包、激活/破解软件等工具中，当用户安装使用这些工具时，“匿影”将会下载释放各类病毒，感染用户设备，同时还将利用被感染设备进行横向移动。

2、Magniber 通过色情网站吸引用户，利用 IE 漏洞进行传播

11 月 10 日消息，Magniber 勒索软件攻击事件频发，利用 IE 浏览器漏洞进行无文件传播。

Magniber 是一种利用 IE 漏洞的无文件勒索软件，于 2017 年开始作为 Cerber 勒索软件的继承者，最初只感染韩国的用户，近期在国内有大肆传播趋势。

该勒索软件自 3 月 15 号以来，利用 CVE-2021-26411 漏洞进行分发传播，在 9 月 14 日微软推送了安全补丁之后，于近日被发现

增加对 CVE-2021-40444 漏洞的利用。在被感染后，该病毒还会利用 PrintNightmare 漏洞进行提权。

安全人员分析表示，该勒索软件团伙主要在色情网站的广告位投放带有攻击代码的广告，在用户访问到广告时，就可能会中招，感染勒索软件。

（二） 国外部分

1、美国国务院对多个勒索软件作者发出千万美元悬赏

本周，美国国务院的“跨国有组织犯罪奖励计划（TOCRP）”对外发出悬赏。该悬赏称最高可提供 1000 万美元用于识别、定位 Sodinokibi(REvil)勒索软件家族或 DarkSide 勒索软件家族的制作组织主要成员，另外还对能够提供定位任何参与过这两家勒索软件攻击事件的人员信息的举报者 500 万美元的奖励。

该计划主要用于打击各种跨国的有组织犯罪集团，定位组织的关键领导人。除了上述有针对性的对两个勒索软件家族提出悬赏外，该计划还悬赏 1000 万美元，奖励有国家资助的黑客攻击美国基础设施的相关信息举报者。

2、罗马尼亚警方逮捕 REvil 相关嫌疑人

11 月 8 日消息，两名 REvil 勒索软件团伙相关人员于 11 月 4 日在罗马尼亚被捕，据称被捕二人应对遭其勒索软件攻击感染的数千名受害者负责。目前，布加勒斯特法庭已下令对两名被捕嫌疑人进行 30 天的审前拘留。

同期，科威特当局还逮捕了一个 GandGrab 勒索软件团伙关联组

织，其中三人涉嫌发起了近 7000 次勒索软件攻击，索要赎金超 2 亿欧元。今年年初以来，另有三名被认为是 REvil 勒索软件团伙关联组织的人员分别在韩国、欧洲被警方逮捕，一定程度上遏制了勒索软件的势头。

3、德国医疗软件提供商 Medatixx 遭受勒索软件攻击

本周披露，11 月初，德国医疗软件巨头 Medatixx 遭到勒索攻击，影响了医疗机构的内部 IT 系统，导致其运营系统瘫痪。攻击者很可能在攻击过程中窃取了 Medatixx 客户的密码。因此 11 月 9 日，Medatixx 披露了此次攻击，敦促用户重置密码。德国大约 25% 的医疗中心使用了 Mediatixx 解决方案，此次勒索攻击可能是德国医疗系统有史以来遭受的最严重的网络攻击。

4、欧洲电子零售巨头 MediaMarkt 遭 Hive 勒索软件攻击

电子零售巨头 MediaMarkt 在当地时间 11 月 7 日至 11 月 8 日期间，遭到勒索软件攻击。其服务器及工作站等设备数据被加密，最终公司只能关闭 IT 系统以阻止事态蔓延。据了解，此次攻击影响了整个欧洲的众多零售店，其中荷兰和德国的相关商店受影响最严重，运营一度中断。

根据目前公开的消息，受到此次攻击影响的共有 3100 余台服务器。而攻击的幕后黑手可能是 Hive 勒索软件，该病毒对 MediaMarkt 开出了高达 2.4 亿美元的巨额赎金。

2021 年 6 月，Hive 勒索软件首次出现在大众视野，和成名已久的勒索软件相似，都是通过网络钓鱼活动开展网络攻击行动。 一旦

获得攻击目标网络的访问权限，立即通过网络横向传播，同时窃取未加密的文件用于敲诈勒索。

另外，当攻击者获得 Windows 域控制器的管理员访问权限时，会在整个网络中部署勒索软件用于加密所有设备。

四、威胁情报

MD5

8fa81c255de6369047674e112f8da58f

bfa8d66509e07faba724dc0f9035c0d3

b52bd4632956921b14bbdc8ca778fa25

db0dbd31d75cf146b3c400282e6bb40a

ad6687656ce8c983e53246f2941fb384

21b69f5b7c0153e14ee41333eae34f5d

5677a7cce44531214657a81fc55fcd2a

c1ec31554f0efc16ed07d7fa954dae04

625baee6425e2cf1b9cd5fb33bc2633c

ad113aac83ec6568b0ead8e9000c438c

3b2c18e4cb5044642de996ffed338583

21b69f5b7c0153e14ee41333eae34f5d

5677a7cce44531214657a81fc55fcd2a

c1ec31554f0efc16ed07d7fa954dae04

625baee6425e2cf1b9cd5fb33bc2633c

ad113aac83ec6568b0ead8e9000c438c

3b2c18e4cb5044642de996ffed338583

9e609932c59d043565c5d3e5260f571b

域名

vyewxn2lkxrihikeunagqqoakralogk5ze5vaxrkahvkjdug6rcwdsqd.onion

Fitdbud.uno

paymenthacks.com

nowautomation.com

fluentzip.org

mojobiden.com

邮箱

coronaviryz@gmail.com

korona@bestkoronavirus.com

coronavirus@exploit.im

anton_rozhko1991.05@mail.ru