

The data analysis behind the cyber attack on Beijing Healthbao

Summary

Beijing HealthCare suffered a DDoS attack on April 28. All support teams responded quickly and worked together to quickly eliminate the impact of the attack. Like a battlefield, an attack is eliminated, but as long as the underworld forces are still there, the next attack may already be on the way. To this end, it is necessary for us to deeply analyze the attack team behind it, to understand its scale and attack methods, so as to know the enemy and the enemy.

Through the multi-dimensional security threat data accumulated by 360Netlab, we can determine that the initiator of this incident is our internal gang named Rippr, which used the disclosed malicious code family Fbot as an attack weapon. Like viruses in the real world, malicious codes in the online world are often based on old malicious codes, and are constantly being controlled by batches of people with "malicious purposes" to evolve, spread, and use them. The Fbot variants of this incident, first discovered on February 10, have been unusually active in DDoS attacks since their discovery. As of today, in just three months, more than 15w attacks have been tracked.

This technical review will take you deep into the cyberspace and see the undercurrents of the abyss beneath the seemingly calm surface.

background

On April 28, the 318th press conference on the prevention and control of the new crown virus pneumonia epidemic in Beijing was held. At the meeting, Wei Bin, deputy director of the External Information Department of the Publicity Department of the Beijing Municipal Party Committee, said, "On April 28, the peak period for the use of health treasures in Beijing was In the event of a cyber attack, the guarantee team responded in a timely and effective manner, and Beijing HealthCare related services were not affected during the attack."

From what we saw in our field of vision, we can confirm that this is a typical network denial of service attack (DDoS attack) event, that is, the attacker uses a large number of compromised network devices, such as IOT devices, personal computers, servers, etc., Send massive network traffic to the victim server, affecting its normal service. To use a common example to compare, it is like someone controlled 1 million zombies to rush to a specific nucleic acid testing point for testing, resulting in the nucleic acid testing point being unable to provide services to those who really need testing.

这种攻击方式，往往都是利用网络安全领域熟知的“僵尸网络”，僵尸网络中大量被控制的机器和设备叫做Bot(肉鸡)，而控制这些机器、设备的核心主控服务器叫做C2 (command and controller)。在组织结构上,黑客从性能,安全,易调度等角度考虑,并不会直接去和这些大量被入侵感染的网络设备(Bot)一一对话,发送指令，而是会利用C2来统一控制。所有的Bot都和C2通讯，接受C2下发的各种攻击指令。这样黑客只需要通过控制一台或者多台C2,就可以轻松控制成千上万的Bot的行为。

对于活跃的僵尸网络,如果能够有效地发现和跟踪C2，甚至进一步能够实时获取黑客通过C2发出来的每一条具体的攻击指令，那么黑客的攻击活动每一个动作对安全守护方来说都是透明的。正是这个原因,DDoS研究中的C2的发现和跟踪一直可以算是“皇冠上的明珠”。

Netlab为什么能看到此次攻击？

360 Netlab的BotMon系统长期专门跟踪大网上活跃的DDoS攻击，这次攻击也被我们的系统第一时间捕获，并及时分享给相关机构对涉事僵尸网络做相应处置。

360 Netlab使用逆向分析手段完全掌握僵尸网络的通信协议后，可以打入僵尸网络内部，从而监听其内部通信信息和攻击指令。在本次安全事件中，我们就捕获了对应的攻击指令，从而将受害者和攻击发起者之间形成了牢固的证据链条。

本文我们就从C2的角度对这一安全事件进行分析，要点如下：

- 这次DDoS攻击通过僵尸网络发起，该僵尸网络源自于一个名为Fbot的家族。该家族存活已久，最早由我们在2018年首先发现并[公开](#)。
- 此次涉事的僵尸网络使用3个C2参与了对北京健康宝的攻击，我们对其有持续跟踪，截获了具体的攻击指令。
- 该僵尸网络最早于2月10日被发现，最开始有另外3个C2活跃，后经过一次安全团队联合反制，旧的被打掉,变为现在的3个新的C2。

该僵尸网络由一个我们内部命名为Rippr的团伙运营，该团伙长期进行DDoS攻击，我们之前也曾跟踪到其对外发起的多次大型DDoS攻击事件。

- 截止到发稿时，全球范围内本僵尸网络仍在活跃，且仍在参与针对各种攻击的目标的DDoS攻击事件中。

对北京健康宝的攻击指令

我们的BotMon系统截获的原始攻击指令如下：

时间	僵尸网络家族	c2地址	c2端口	攻击类型	攻击方式	受害目标	受害端口	其他信息
2022-04-28_08:47:52+08:00	fbot	dota.iwishiwashappy.eu	9987	ddos	atk_256	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,
2022-04-28_08:47:52+08:00	fbot	dota.uiasuibasdbei.art	9987	ddos	atk_256	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,
2022-04-28_08:47:51+08:00	fbot	dota.zzzsleepisnicezzz.art	9987	ddos	atk_256	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,
2022-04-28_08:41:50+08:00	fbot	dota.zzzsleepisnicezzz.art	9987	ddos	atk_261	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,
2022-04-28_08:41:50+08:00	fbot	dota.uiasuibasdbei.art	9987	ddos	atk_261	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,
2022-04-28_08:41:50+08:00	fbot	dota.iwishiwashappy.eu	9987	ddos	atk_261	xx.xxx.194.137	80	src=beast,atk_time=60,netmask=32,

为了保护被攻击的目标，我们对上述指令中目标IP做了打码处理。从攻击时间上来看，指令发出的时间是28号早上8点41，跟北京卫健委发布的时间能对上；从攻击方法上来看，使用了我们内部命名为ATK_256，ATK_261的DDoS攻击方式。

ATK 256, ATK 261是什么攻击?

此次涉事的Fbot一共支持8种攻击方法，ATK_256，ATK_261分别对应UDP_PLAIN ,TCP_PushAck俩种非常经典的DDoS攻击方式。

```
prepare_cmd(0, 0, (int)sub_80487CF);
prepare_cmd(0, 1, (int)sub_8048774);
prepare_cmd(1, 0, (int)atk_256); → DDoS_UDP_PLAIN
prepare_cmd(1, 1, (int)atk_257);
prepare_cmd(1, 2, (int)atk_258);
prepare_cmd(1, 3, (int)atk_259);
prepare_cmd(1, 4, (int)&atk_260);
prepare_cmd(1, 5, (int)atk_261); → DDoS_TCP_PushAck
prepare_cmd(1, 7, (int)atk_263);
prepare_cmd(1, 6, (int)atk_262);
prepare_cmd(1, 8, (int)atk_262);
return prepare cmd(1, 9, (int)atk_262);
```

我们在测试环境下，通过技术手段对这两种攻击方法进行了模拟，我们向Bot端下发了以下2条攻击指令

atk_256 **target xx.xx.62.19:80**

00000000	00 10 01 00 01		3e 13 20 00 50 00 3c 05 81k> . .P.<..
00000010	00 10 01 05 01		3e 13 20 00 50 00 3c 05 81k> . .P.<..

atk_261 **target xx.xx.62.19:80**

它们的意思是向测试IP xx.xx.

62.19的80端口发起ATK 265,ATK 261攻击，时长60秒。Bot端在接收到指令后，如我们所料，向测试IP发起了DDoS攻击。

UDP PLAIN(ATK 256) 攻击效果如下：

TCP_PUSH_ACK(ATK_261) 攻击的效果如下：

Source	Destination	Protocol	Length	Info
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4133697249
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4133762785
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4133828321
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4133893857
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4133959393
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4134024929
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4134090465
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4134156001
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4134221537
110.148	.62.19	TCP	1463	[TCP Spurious Retransmission] 46968 → 80 [PSH, ACK] Seq=4134287073

我们提取了攻击相关的特征，

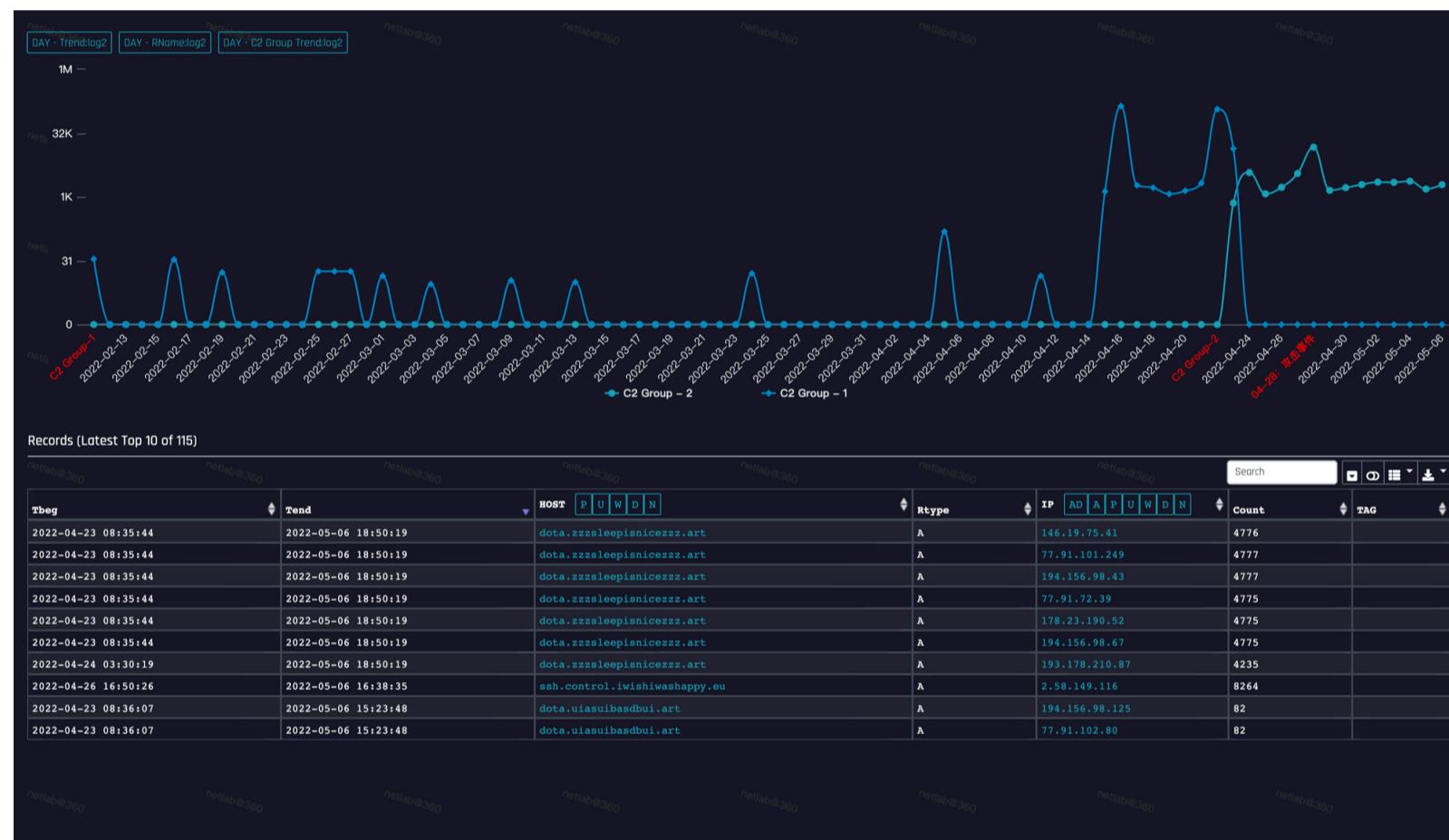
同步给有关部门后，经过比对，确定此家族确实参与了对北京健康宝的攻击。

该僵尸网络团伙的规模&发展趋势

上一章节我们回答了，谁参与了攻击这个问题，马上另一个问题就摆在我们面前了：“攻击者有能力造成破坏吗？”。这就要求度量涉事僵尸网络的规模。

和我们合作的社区安全伙伴相继给了我们一些从各自角度看到的实际数字，但是这些数字不方便公开公布，不过我们可以从我们自身的数据出发，对本次涉事僵尸网络的规模&发展趋势进行一些评估。

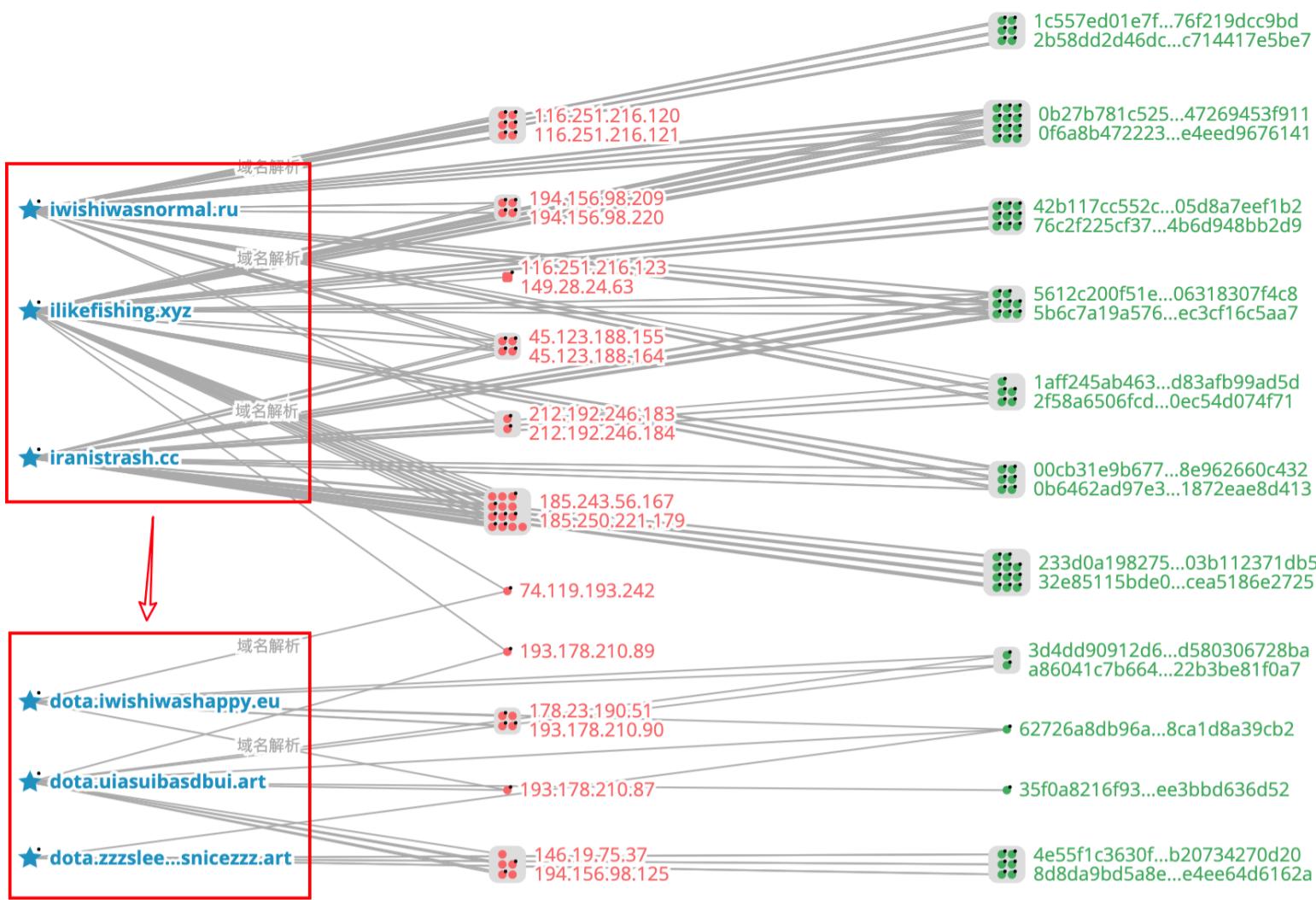
通过PDNS(passive DNS)数据，我们可以直观地感受到该僵尸网络家族的历史变化。



趋势分析：

- 2月10日，该团伙域名首次被发现活跃迹象，最开始的3个C2域名（C2-Group-1）为：iwishiwasnormal.ru, ilikefishing.xyz, iranistrash.cc
- 4月14日开始，该家族迅速的繁荣起来，C2的请求量有了明显的上升
- 4月22日，该家族已有的3个C2域名下线，并同时有3个新的C2域名（C2-Group-2）上线：dota.iwishiwashappy.eu, dota.uiasuibasdbui.art, dota.zzzsleepisnicezzz.art
- 4月28日，该团伙发起了对健康宝的DDoS攻击

同时，从IP的层面我们也能看到该团伙运营者的“用心程度”，下图揭露了C2域名迁移过程中对应IP的变迁：



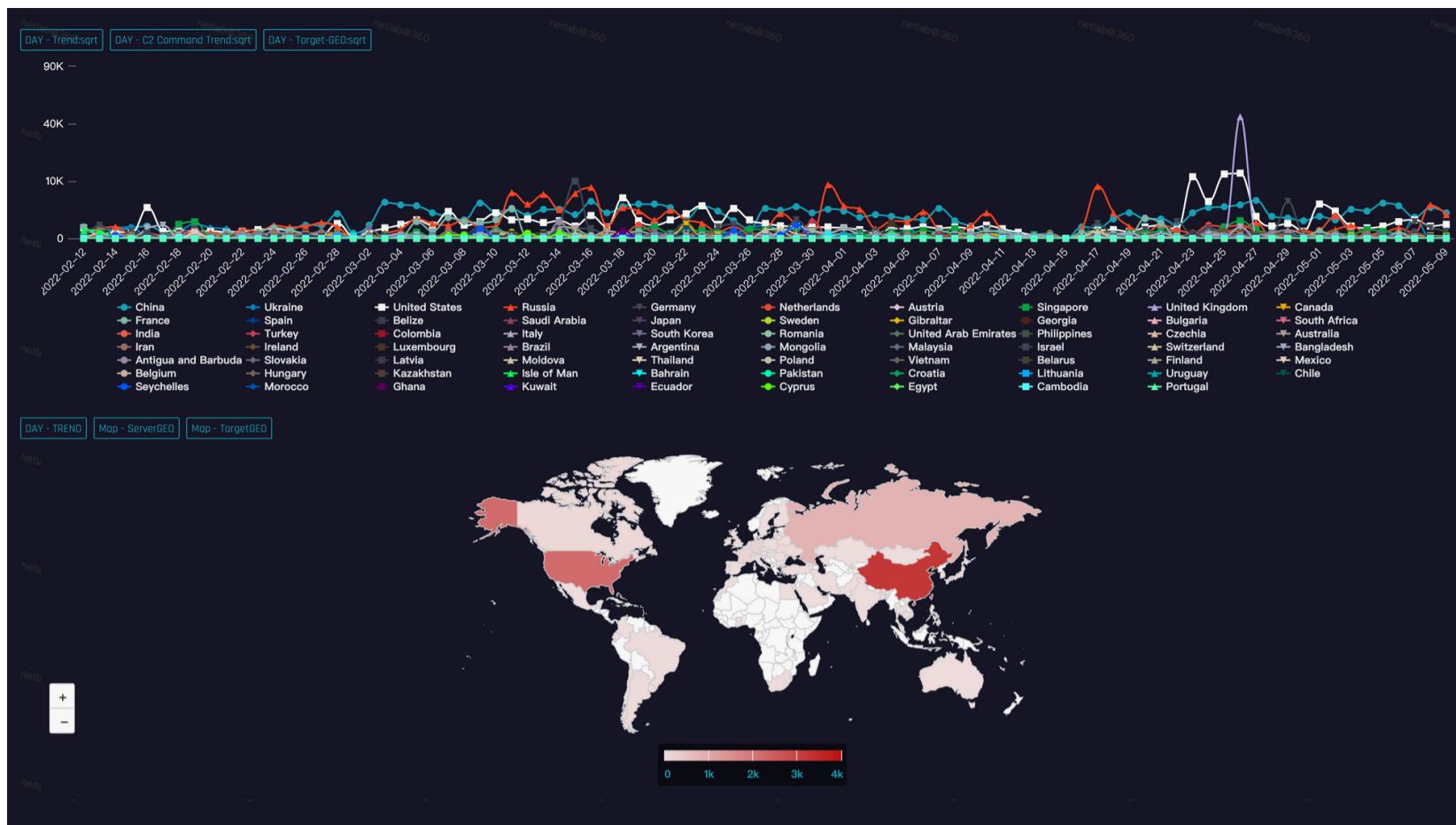
- 通过安全社区的合作我们得知，A国某头部云服务商的服务曾多次被此家族攻击，严重影响其业务，以至于该服务商利用影响力封禁该家族主控域名（这才导致C2-Group-1 到 C2-Group-2的转变）这可以变相说明该家族的攻击能力不容小觑。
- 僵尸网络传播过程中，会有流量扫描到我们的机器，因此我们将该家族扫描流量和其他已知规模的僵尸网络的扫描流量做对比，进而估算该僵尸网络家族的规模。结论是：峰值上线日活机器应该数以万计。

综上，我们认为此僵尸网络团伙有能力对北京健康宝的业务造成有效攻击。

此次攻击是否为对我国的定向攻击？

该僵尸网络将涉事的3个C2域名通过DNS域名映射到多个IP的方式做负载均衡。目前他们分别解析到18个不同的ip地址,分布在4个国家/地区。基于我们有完备的攻击跟踪指令记录,我们可以从这3个C2的历史攻击指令发现一些基本特征:

- 从分发的指令频度来看，截至目前，被跟踪到的攻击事件超过15w次。似乎表明该家族并不介意暴露，缺乏国家/地区级别网络攻击的潜伏性。
- 从攻击目标的角度，当我们把该团伙攻击目标对应的国家/地区按照时间轴来统计，并映射到地图上，可以清楚的看到该家族累计攻击的目标地理分布遍布全球，包括美国、中国、俄罗斯、英国、法国以及欧洲若干国家/地区，这可以表明攻击者的目的选择上与地缘政治没有明确的关联关系
 - 从时间轴上来看，攻击目标到国别的走势一直是比较随机的状态，不存在持续针对特定国家/地区的攻击，也不存在特定时间点突然针对特定国家/地区的攻击
 - 从地图分布上看，中美两国颜色较深，说明两国累计被攻击目标及次数较多，综合考虑到两国在互联网上业务的比重原本就比较大，这里的“看起来多”是一种正常状况



综上，以及我们对该家族运营团伙Rippr历史认识，我们认为它的主要目的是通过对外提供DDoS服务，以及挖矿来盈利，不涉及政治诉求。

背后黑手Rippr

Rippr团伙进入我们的视野已经长达18个月，团伙的名称源于其长期运营的僵尸网络riprrbot，2022年2月10日，该团伙使用泄露的Fbot源码，开始运营Fbot家族，作为一个经验丰富的团伙，它修改了Fbot的上线特征和加密算法。其中上线特征如下所示，前4字节为magic，包长36字节：

```
00000000: D7 0C 63 A8 61 6D 63 72 65 73 74 2E 61 72 6D 37 ..c.amcrest.arm7
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000020: 00 00 00 00 ..... .
```

在经过1个版本的测试之后，Rippr团伙利用其丰富的0DAY/NDAY武器库帮助Fbot快速扩张，当时活跃的C2是前述的 C2-Group-1。

实际上这3个C2也被Rippr团伙的riprrbot僵尸网络使用，在Fbot扩张的同时，Rippr并没有停下攻击的脚步，我们的BotMon系统监控到Rippr旗下的riprrbot，fbot僵尸网络对全球知名的重大互联网站国某云服务商的发起数次大型DDoS攻击活动。

2022年4月22日，我们从安全社区到到确认，A国某头部云服务商协同安全社区针对该恶意代码家族做过一次封堵。可惜这次封禁并没有对Rippr团伙形成有效的打击，该团伙发现C2被禁后，快速更新将C2切换到C2-Group-2，即本次攻击使用的三个C2域名，在极短的时间内恢复了DDoS攻击的能力。



从他们上线伊始，我们就一直在实时的捕捉他们的指令，上图是根据他们历史上发出的15万+攻击指令做出的统计。可以看出，该团伙从上线之初就异常活跃，受到反制措施之后 C2-Group-1 到 C2-Group-2 的切换也非常的迅速，攻击趋势没有任何停滞，且在4月26日达到攻击的一个最高峰。

截至目前为止，本僵尸网络在全球范围内依然活跃，预期随着我们文章的登出，涉及的C2和恶意样本会被安全社区提取使用，黑客也许会通过再一次更新C2地址来应对。

总结

伴随信息活动越来越多，网络空间的安全性也愈发重要。本次健康宝通报抵御了网络攻击，引起了百姓的热切关注，在新媒体上热度很高。我们认为这也是向公众宣传网络安全的一个窗口。

从国计民生关键基础设施的安全性角度来说，本次攻击提醒我们，北京健康宝已经毫无疑问应当纳入到关键基础设施的范畴。反过来，如果任何原因导致任何地区的健康码崩溃，当地的抗疫工作毫无疑问会受到迟滞。从这个角度说，我们应该为北京健康宝的提前预案、及时应对、有效保障点赞。

从抵御网络空间僵尸网络的控制者和攻击者角度来说，僵尸网络是网络空间里的顽疾，国家执法机关和安全社区已经协作抵御僵尸网络多年。不仅国内如此，国际也是如此。例如针对本次攻击者，360公司就协同国家机关处置了对应的恶意控制域名，起到减缓攻击者发展的作用。但是仍需指出，成本方面这是一场“非对称战争”，防御者投入的精力和成本要远大于单一攻击者。除非所有防御者通力合作，否则我们很难将全部攻击者绳之以法，而只能是相对有限的打击重点攻击者，防御重点保护对象。

最后请允许我们为360威胁情报中心打个广告。本次攻击相关的恶意控制域名，已经早于本次攻击事件就入库，在360及其生态产品中保护最终用户的安全。

IoC

C2

iwishwasnormal.ru ilikefishing.xyz iranistrash.cc dota.zzzsleepisnicezzz.art dota.iwishwashappy.eu
dota.uiasuibasdbui.art

MD5

0de8e79862f846887821240ff0a7c67e 116abdf010b43b5269e5e5dd6e45a4 1a904a1210e26a6da0d139824aba7309
1b675da617a856cad8d6aa20de6c186 24f89312c3319df8627347924bac4ea7 28d6bd52d227daa488fd14432d613d89
2bc1ab65659f9b3f3e2efbfa05ab4172 35f0a8216f939b117e54ee3bbd636d52 3c87a4925292c8dc11694afe847fbfdf
48fd995f44fc5317c9aa9585f85f3ac7 4e55f1c3630f86edb695b20734270d20 636f8430c263a9d2d798a89809df0874
807c54466bfb076db66c0212a52fdc22 813950fa1a9c00dce7eed71984a65100 8d68390fddfa42a0e60a5dd247a4c243
8d8da9bd5a8e2709c21ee4ee64d6162a 93292a43949fa22a70a3221287792042 a608f8e7cb61e5273c4d057fd27353d1
aa3f65eddc437ff38f9df67a88bc5edc ab9a5bff3d16576d01b4bc7190fb84ab b0ab8faa5809b3957a050000e13a6d8b
b43cae51b13cf9bb3c16d40b2a3c7a6 b659aecf1ea18b82018d44b401f9252a b91fe7ba96c896e459f0744cd7db4722
bd3bd14fc0a0f047bb03e67c2099849b c060e23d6369c12a60db59261b7552f2 c42e41ee6486a7dc38cf3c098fde31c3
daad900f19e9f0a720f24e51dbc495cb df53e7d0c15392035deabeaf7ea0a44a fe2e89e54771588ce4638eac84c5f367

URL

<http://31.44.185.237/arm4> <http://31.44.185.237/arm5> <http://31.44.185.237/arm6> <http://31.44.185.237/arm7>
<http://31.44.185.237/mips> <http://31.44.185.237/mips64> <http://31.44.185.237/mipsel> <http://31.44.185.237/powerpc> <http://31.44.185.237/x> <http://31.44.185.237/x86> http://31.44.185.237/x86_64