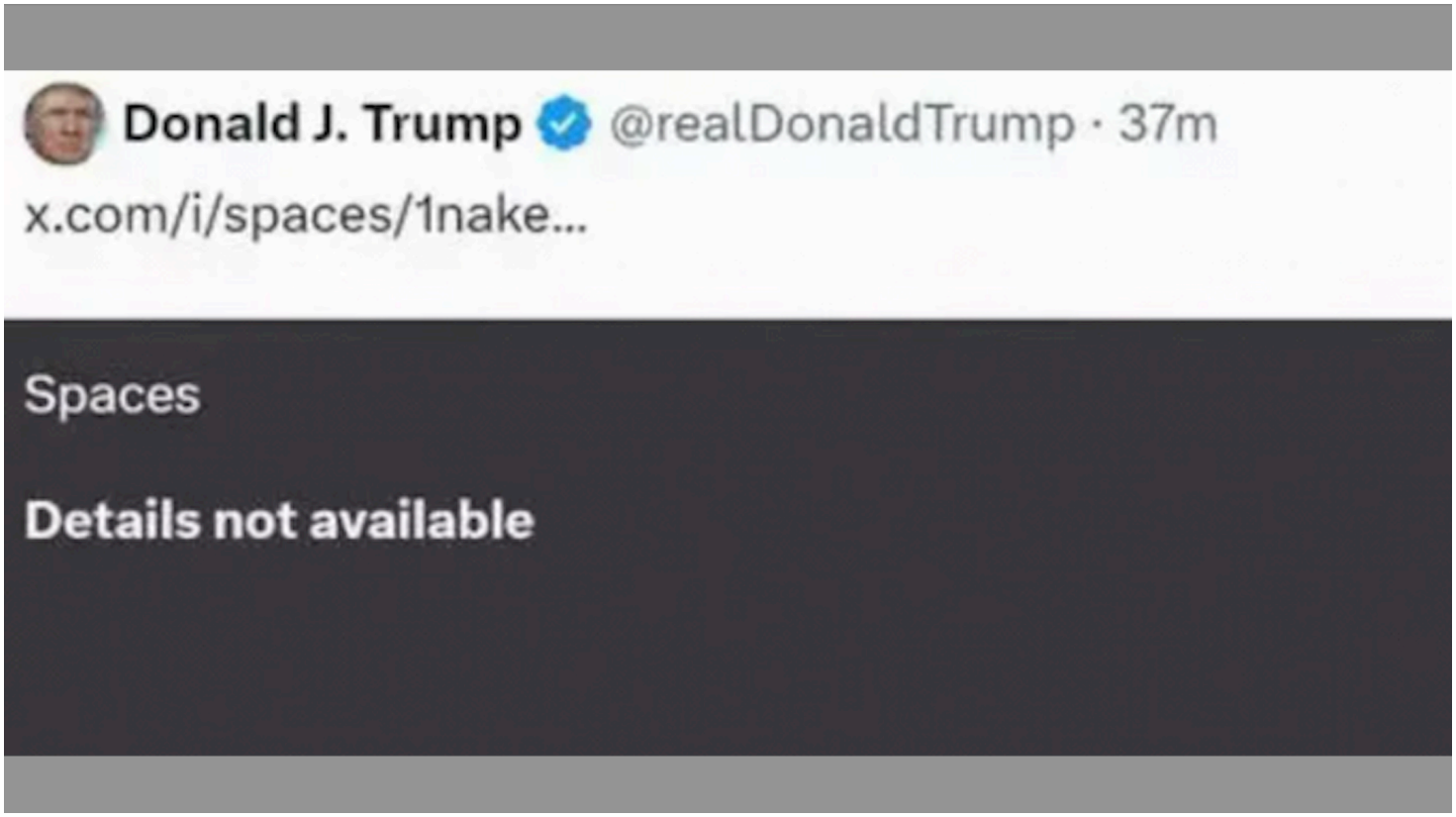
DDoS

关于特朗普与马斯克访谈直播遭遇DDoS攻击事件快速介绍

Acey9, Wang Hao, daji

2024年8月14日 • 4 min read



按: 昨天特朗普与马斯克访谈直播是否 x 真的遭受到了DDos攻击,我们看到安全社区有一些讨论,有一种倾向是认为实际上并没有攻击发生,从我们的视角看,攻击是真实的发生了,如下是一篇简要的情况介绍

事件回顾

按照原定计划，美东时间12日晚8时，埃隆·马斯克将对第60届美国总统大选候选人唐纳德·特朗普进行一次连麦直播访谈，并在X平台上通过马斯克和特朗普的个人账号进行现场直播。然而，当直播时间开始用户访问两人的直播间时，系统却提示“此直播间不可用”。直至40多分钟后，直播平台才恢复正常。

访谈结束后，马斯克在其X平台账号上发文称X平台遭受了大规模的DDoS攻击。

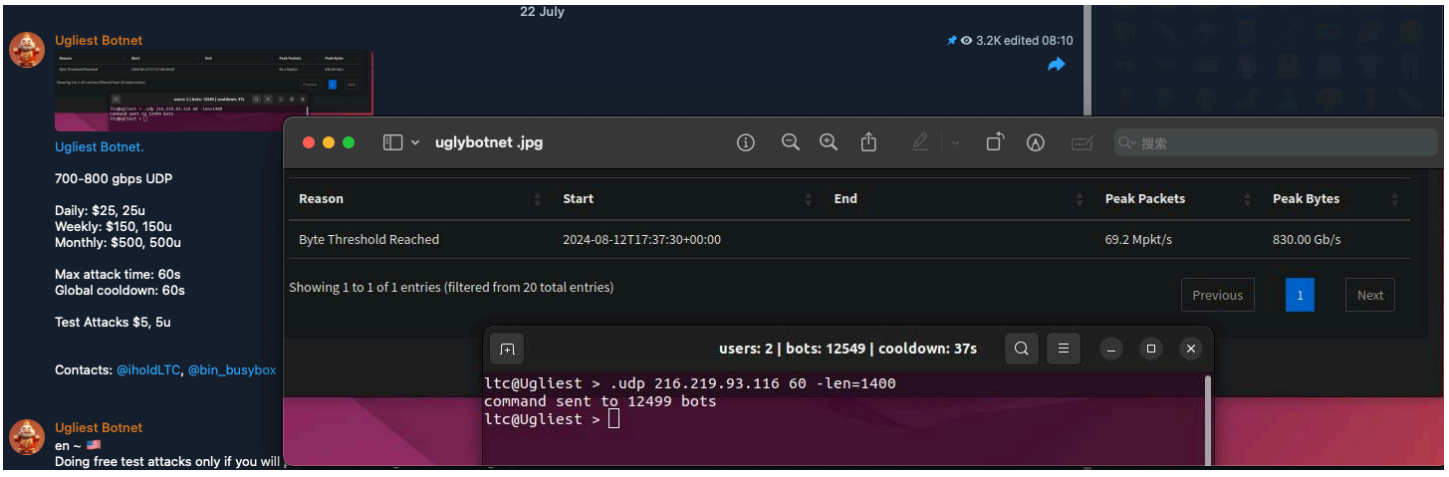
马斯克表示：“我对延迟启动表示歉意。不幸的是，我们的服务器遭到了大规模的DDoS攻击，我们所有的数据线路都饱和了，基本上数百GB的数据都饱和了。”

关于此次事件XLab的观察

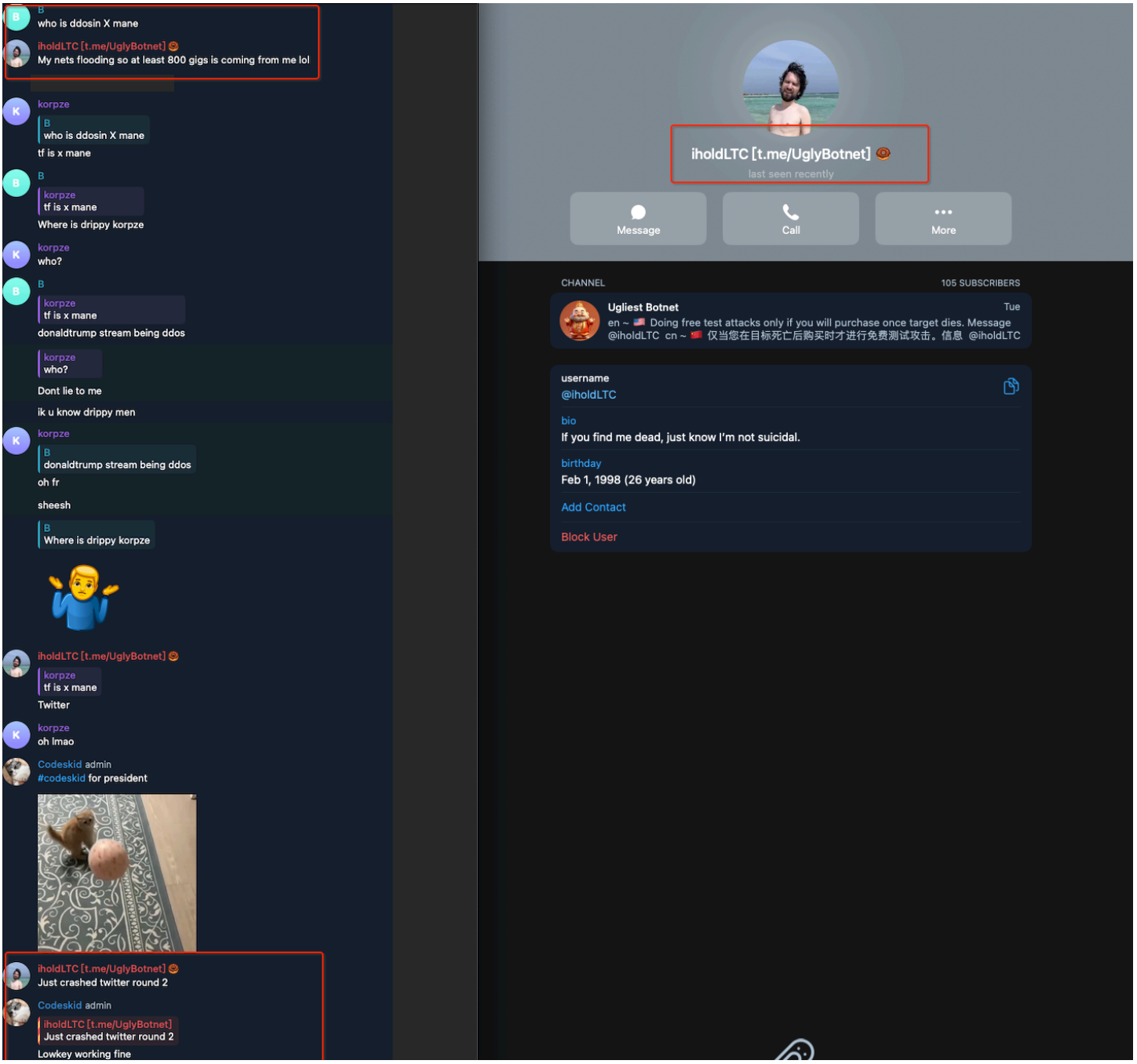
XLAB大网威胁感知系统观察到了此次DDoS攻击事件。我们观察到有4个Mirai僵尸网络主控参与了此次攻击。另外还有其他攻击团伙使用HTTP代理攻击等方式也参与了此次攻击事件。攻击时间从北京时间8点37持续到9点28，攻击时长50分钟。攻击时长和此次访谈的延迟开时间基本吻合。

Mirai.zushi 攻击

其中参与攻击的4个Mirai C2都属于我们内部命名为 `Mirai.zushi` 的Mirai变种僵尸网络， `Mirai.zushi` 从今年6月份开始发展，目前大概万级别BOT，使用RC4加密通信流量。 `Mirai.zushi` 运营者相关的社交频道 `https://t.me/uglybotnet`



我们不仅观察到了 `Mirai.zushi` C2发起的攻击 `x.com` 平台的攻击指令，也从社交媒体观察到了 `Mirai.zushi` 运营者声称他们为此次攻击 `x.com` 贡献了 `800G` 的攻击流量。下图是他们的聊天记录截图



HTTP代理攻击

除了前文提到的僵尸网络攻击外，XLAB大网威胁感知系统还观察到了另一种破坏力极强的攻击。这种攻击通过大量代理或VPS机器向被攻击目标发送海量的HTTP请求，直到耗尽目标机器资源。从我们观察到的HTTP请求Payload看，此次攻击非常有针对性。攻击请求的的目标地址为特朗普的个人推特账号 `https://x.com/realdonaldtrump/` 。具体的攻击Payload如下：

```
GET /realdonaldtrump/ HTTP/1.1
Host: x.com
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: "Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
```

```
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.7
```

结语

相关攻击记录如下图：

本文只是一篇快速的介绍, 但通过上述内容我们可以看到 从数据的角度看,攻击的确发生了,且时长和此次访谈的延迟开时间基本吻合。我们会有更加具体的样本层面的分析文章。

Contact Us

Readers are always welcomed to reach us on twitter.

What do you think?

0 Responses

 Upvote

 Funny

 Love

 Surprised

 Angry

 Sad

0 Comments Login ▾

G Start the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS

Name

♡ Share Best Newest Oldest