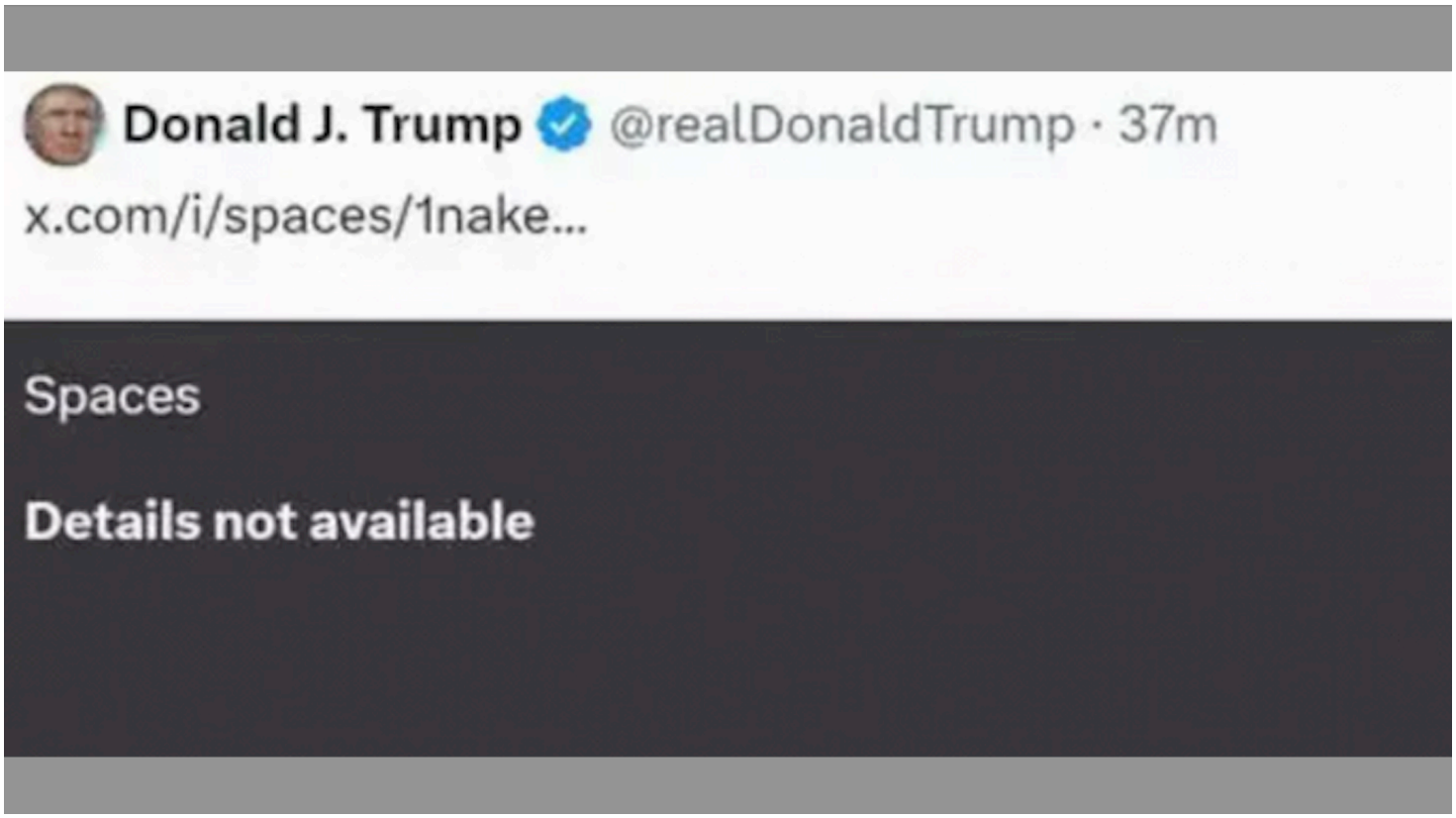
DDoS

Behind the Scenes: A Brief Overview of the DDoS Attack on the Trump-Musk Livestream

Acey9, Wang Hao, daji

2024年8月14日 • 3 min read



Note: There has been considerable discussion in both the media and the security community about whether the Trump and Musk interview livestream on X

yesterday was indeed the target of a DDoS attack. While many suggest that no attack took place, our analysis indicates that the attack did occur. Below is a brief overview of the situation.

Incident Review

As originally planned, at 8:00 PM Eastern Time on the 12th, Elon Musk was scheduled to conduct a live-streamed interview with Donald Trump, a candidate for the 60th U.S. Presidential Election, on the X platform through their personal accounts. However, when users attempted to access their live streams at the scheduled time, the system displayed the message "This livestream is unavailable." It wasn't until more than 40 minutes later that the platform returned to normal.

After the interview, Musk posted on his X platform account, stating that the X platform had suffered a large-scale DDoS attack

Elon Musk stated: "I apologize for the delayed start. Unfortunately, our servers were hit by a massive DDoS attack, saturating all our data lines with hundreds of gigabytes of data."

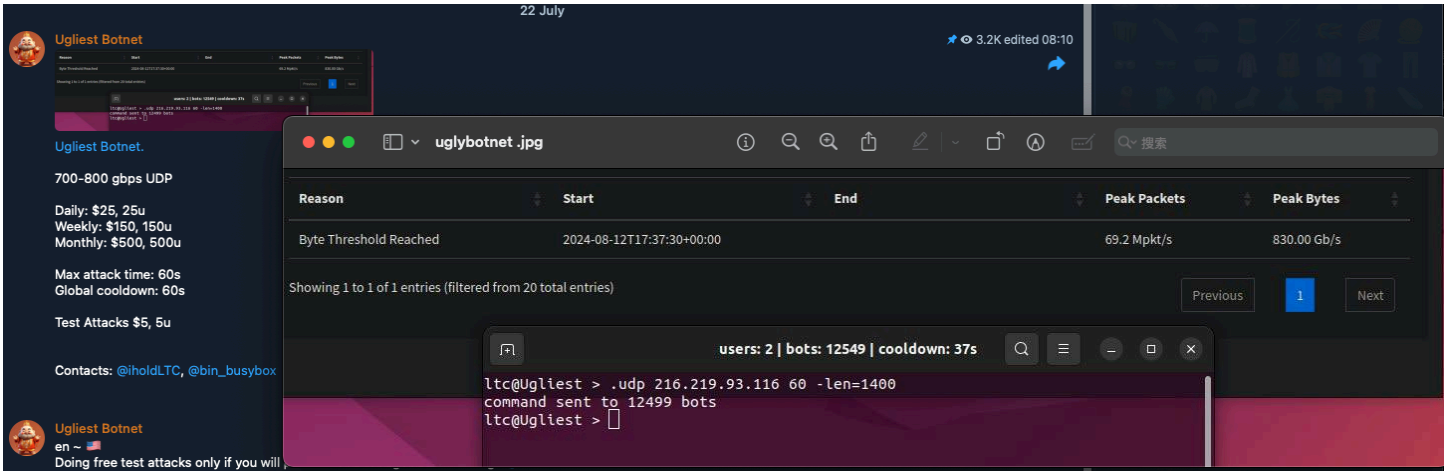
Observations from XLab Regarding This Incident

As noted earlier, we did observe the DDoS attack incident. We identified four Mirai botnet C2s (command and controllers) involved in the attack. Additionally, other

attack groups also participated using methods like HTTP proxy attacks. The attack lasted from 8:37 AM to 9:28 AM Beijing time, with a duration of 50 minutes, which closely matches the delay durations in the start time of the interview.

Mirai.zushi Attack

The four `Mirai` C2s involved in the attack belong to a new mirai variant botnet we internally named `Mirai.zushi`. The `Mirai.zushi` botnet, a relatively new variant in the Mirai family, has been evolving since June of this year and has already infected approximately ten thousand devices. It uses RC4 encryption for communication traffic. The operators of `Mirai.zushi` are associated with the social media channel `https://t.me/uglybotnet`.



Interestingly, we discovered on social media that the `Mirai.zushi` operators claimed responsibility for generating 800G of attack traffic during this incident. Below is a screenshot of their chat records.

HTTP Proxy DDoS

In addition to the above mentioned botnet attacks, Our system also detected another highly destructive attacks. This attack involved flooding the target with massive amounts of HTTP requests, utilizing numerous proxies and VPS machines, until the target's resources were fully exhausted. The payloads of these HTTP requests indicate a highly targeted operation, specifically aimed at Donald Trump's personal Twitter account at `https://x.com/realdonaldtrump/` The exact attack payloads are detailed below:

```
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
```

Conclusion

The following screenshot displays all the attacks we mentioned and captured during this incident, with timestamps noted in GMT+8 (screenshot here).

This article is just a quick introduction, but based on the above information, we can see that from a data perspective, the attack did indeed occur, and its duration closely matches the delay in the interview's start time. We will provide a more detailed analysis at the sample level in a future article.

Contact Us

Readers are always welcomed to reach us on twitter.

What do you think?

8 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