Reverse engineering
hate

Liz Fong-Jones, on behalf of End Kiwi Farms
2023-11-07
What is Kiwi Farms?
A web forum that facilitates the discussion and harassment of online figures and communities. -
Targets are often subject to organized group trolling and stalking, as well as doxxing and real-life harassment."
Hundreds of threads on individuals
3 documented suicides of victims (all trans/NB)
Typical consequences of being targeted

Personal information doxxed (including government ID numbers, home address)

Family members, friends, acquaintances, colleagues also named and targeted

Massive copyright infringement of photographs & defacement for derogatory purposes

“Fanfiction” written to create and refine lies to cast individual in worst possible light

Unwanted contact via email, telephone, and sometimes in-person, threatening harm

Unwanted contact spreading lies to employer, landlord to cause firing & eviction

Attempts to poison SEO to make unhireable
Thousands of collateral targets
“When something is ours, it’s ours forever. We might get bored with it and put it down. We might play with it a little too hard and break it. But it never stops being ours, and someday in the future we’ll remember it, and pick it back up again. Would you like to become ours, my dear?”
How is Kiwi Farms hosted?
How most sites are hosted

All-in-one package - domain, servers in a datacentre, IP addresses, network transit, DNS servers, email MX, etc

Optional DDoS protection services by a reputable provider eg Fastly, Cloudflare, Akamai, GCP/Amazon etc

At most, 3-5 different providers in use, not dozens.
Hate sites migrate to shithosts/self-hosting

Each component obtained a la carte from cooperating or unwitting hosts (often “bulletproof” hosters)

Shell companies for IP addresses, ASNs/BGP routing, network contracts for transit, subleasing datacentre floor space, hand-written DDoS protection, different providers for frontend vs backend vs MX

Payment ban evasion/laundering; multiple nested LLCs
Example network diagram circa November 2022

103.114.191.1 (Flow Chemical)

1776

Cosmic/GSK

Veilios/PR

AS397702

AS30456

AS1002

AS56655

AS29695

AS32914

AS3257

AS6453

AS174

AS6461

AS3356

AS12956

AS6762

AS1299

AS3320

AS6830

AS1239

AS5511

AS3491

AS6762

AS6461

AS12956

AS1299

AS3320

AS6830

AS1239

AS5511

Tier 1 ISPs

Domain reg by Epik

DNS servers on VSYS (AS30860) & AS208046

Additional peering via AS30860 & AS208046

MX with Terrahost

Physical servers w/ Terrahost & VSYS

Volumetric defence by Terrahost & Cosmic

Home-grown PoW app-layer defence
Extreme hate speech & malware are alike. It looks like a duck, quacks like a duck, yet isn’t recognised as one.
Key problems in obtaining action

- Plausible deniability of off-forum coordination
- “In Minecraft” & other slang to avoid casual scrutiny
- Sensitive info hidden behind registration gates
- “Freedom of speech”
- “Section 230”
- “We don’t send unsolicited IP traffic”
- “Net neutrality”
- “There’s worse stuff elsewhere”
How does deplatforming work?
First, on the ethics

What Uses are Prohibited?

Unacceptable use includes, but is not limited to, any of the following:

1. Posting, transmission, re-transmission, or storing material on or through any of Cogent’s products or services, if in the sole judgment of Cogent such posting, transmission, re-transmission or storage is: (a) in violation of any local, state, federal, or non-United States law or regulation (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations); (b) threatening or abusive; (c) obscene; (d) indecent; or (e) defamatory. Each customer shall be responsible for determining what laws or regulations are applicable to his or her use of the products and services.

<table>
<thead>
<tr>
<th>Products &amp; Services</th>
<th>Solutions</th>
<th>Network</th>
<th>About Cogent</th>
<th>Support</th>
<th>Offices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hurricane Electric Acceptable Use Policy (AUP)</td>
<td>[Image of AUP policy]</td>
<td>[Image of Cogent products and services]</td>
<td>[Image of Cogent products and services]</td>
<td>[Image of Cogent products and services]</td>
<td>[Image of Cogent products and services]</td>
</tr>
</tbody>
</table>

Zayo also reserves the right to deny access to the services to any user or service that becomes a source or target of unsolicited mass e-mail (spamming), or consistently transmits large volumes of traffic of a type other than that authorized under the user agreement for the relevant service. In addition, users will not use the Services to conduct activities that may be harmful or offensive to other users or to the Services, such as sending e-mail that is unwanted or otherwise inappropriate. Users will not use the Services to conduct activities that may be harmful or offensive to other users or to the Services, such as sending e-mail that is unwanted or otherwise inappropriate. Users will not use the Services to conduct activities that may be harmful or offensive to other users or to the Services, such as sending e-mail that is unwanted or otherwise inappropriate.
Initially: Tweet storms. 

(but this stopped working)
Complain to origin

Yes, they will retaliate.

At best, with publishing the complaint.

At worst, with doubling down.
Then wait for response or non-response. :(  

#908447 - We Have Answered Your Ticket - Terrahost

Terrahost AS <noreply@terrahost.no>
To: You

Hello,

This is a notification to let you know that one of our support representatives has answered your ticket.

The message is:
Hello

Thank you for notifying us. We already know, and we do not care. Thank you!

Regards,
TH Support

To reply to this ticket, please log into ENIGMA.

Thank you for using Terrahost.
Go further up the chain

Use evidence of previous refusals down the chain.

Cite specific evidence & AUP clauses violated.

Wait longer and longer at each step, as providers are busier/more indifferent.
Wait multiple weeks per step in chain if no action.
Find escalation points

Email/LinkedIn & network to find individuals who will use internal escalation paths.

Liz Fong-Jones (She/Her) · 2:13 PM

Hi, we’ve never corresponded before but we both know [redacted] and [redacted].

I’m writing to you regarding one of GTT’s clients that is refusing to enforce any kind of terms of service upon its customers (and thus falling afoul of GTT’s own terms of service). Strangely enough, GTT has already banned the indirect customer causing the issues when they tried to use GTT services through a different direct client/routing path.

The direct client of GTT’s is Cosmic Global Networks (GameServerKings), and the offending traffic that Cosmic refuses to action is originating from Veilios LLC and “1776 Solutions” on 103.114.191.1, better known as Kiwi Farms (kiwifarms[,]net). Kiwi Farms engages in networked harassment against people they deem to be “lolcows”, including transgender people, neurodiverse people, and anyone who stands in their way (including employees of ISPs...
If all else fails, litigate.
This process is broken.
Our team has had more success, at a cost

- 12 volunteers
- 16 months of work & counting
- 42 providers dropped
- 1000s of hours spent
- 4 parallel legal teams in US, CA, AU, IE
- Approx 100,000 GBP spent on litigation, excluding pro bono assistance
Publicly observable effort != private efforts

Confounding factors (e.g. “new” users may be those that lost passwords and had to recreate)

Measuring a months/years-long process after 4 months is premature.

Talk to malware/cybercrime takedown experts.

Considerations on funding/biz model and whether KF/Moon are an exceptional case

Comparison of “cow” vs “social” subforums?
Thank you