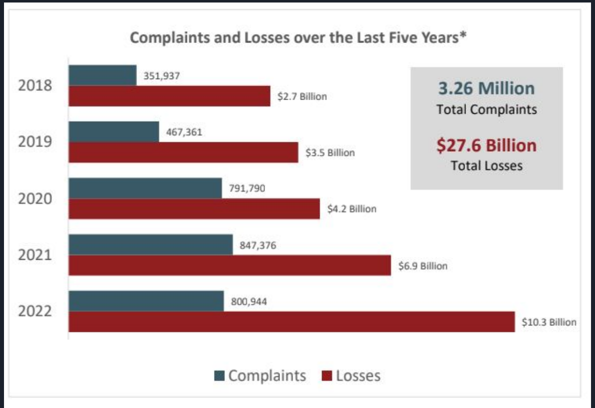
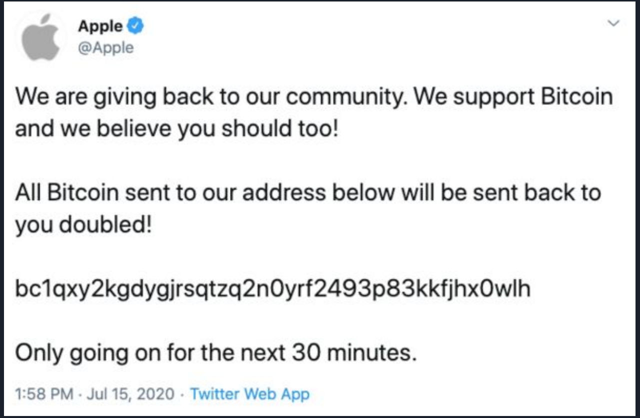
Phishing

Why learn Phishing?

- Phishing is the most common kind of attack, and surprisingly effective
- Used even in high profile attacks
- The 2020 twitter hack used common phishing tactics, which was “the worst hack of a major social media platform yet.”




Apple
@Apple

We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

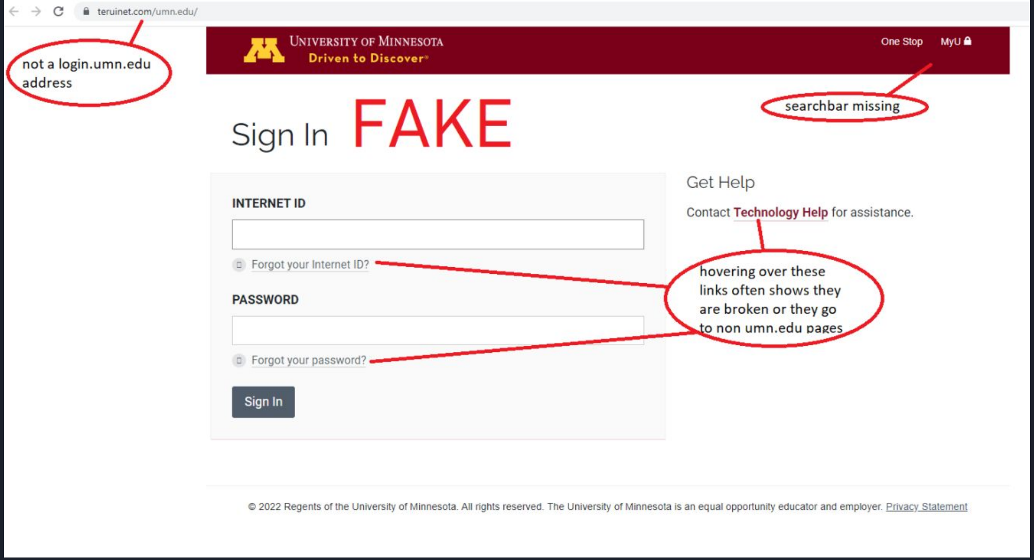
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for the next 30 minutes.

1:58 PM · Jul 15, 2020 · Twitter Web App

Common Techniques for Phishing

- Impersonation
- Fake login pages (links)
- Obfuscation of identity
- Botting



teruinet.com/umn.edu/

not a login.umn.edu address

searchbar missing

Sign In FAKE

INTERNET ID

Forgot your Internet ID?

PASSWORD

Forgot your password?

Get Help

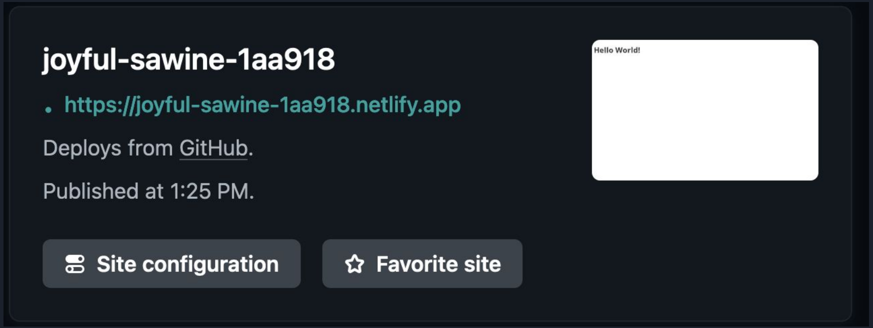
Contact Technology Help for assistance.

hovering over these links often shows they are broken or they go to non umn.edu pages

© 2022 Regents of the University of Minnesota. All rights reserved. The University of Minnesota is an equal opportunity educator and employer. Privacy Statement

QR Code Demo

- This is more of a bad link example
- But bad links can be anywhere!

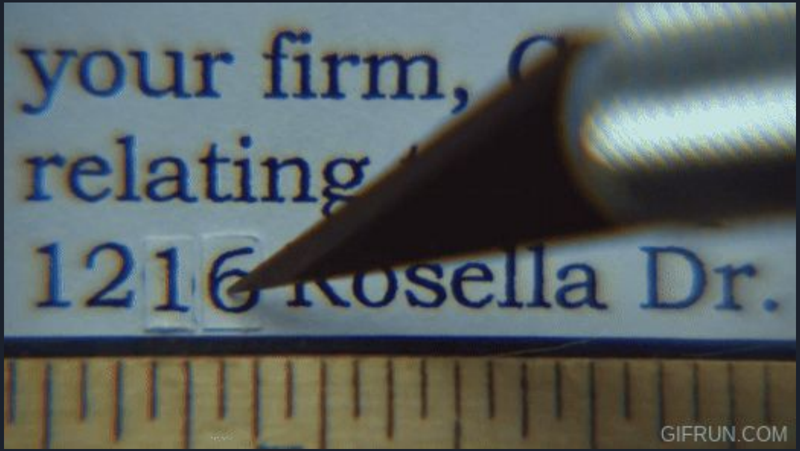


joyful-sawine-1aa918

https://joyful-sawine-1aa918.netlify.app

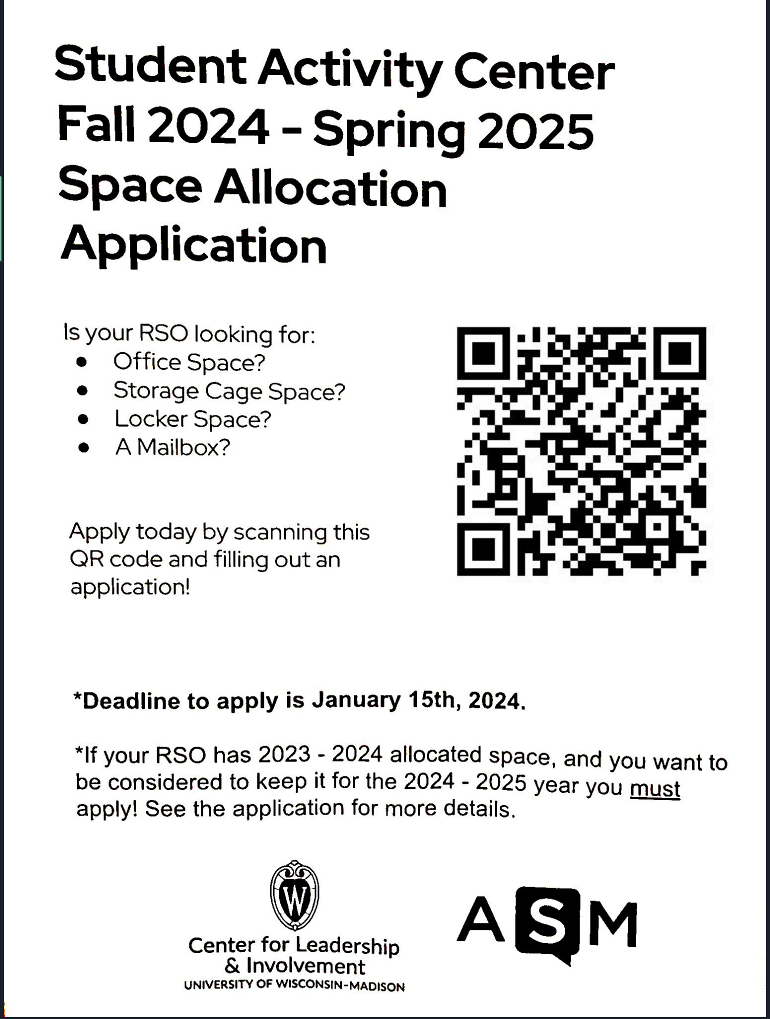
Deploys from GitHub.

Published at 1:25 PM.



https://joyful-sawine-1aa918.netlify.app/netlify/functions/log →

Left is evil, Right is original



Student Activity Center Fall 2024 - Spring 2025 Space Allocation Application

Is your RSO looking for:

- Office Space?
- Storage Cage Space?
- Locker Space?
- A Mailbox?

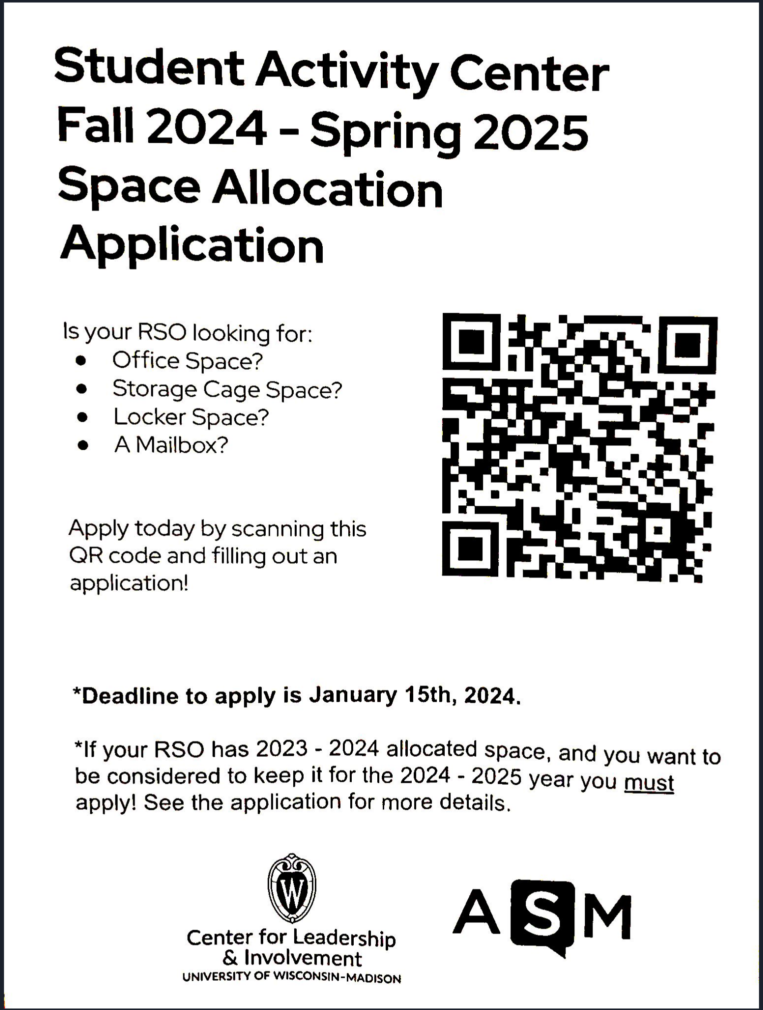
Apply today by scanning this QR code and filling out an application!

***Deadline to apply is January 15th, 2024.**

*If your RSO has 2023 - 2024 allocated space, and you want to be considered to keep it for the 2024 - 2025 year you must apply! See the application for more details.

Center for Leadership & Involvement
UNIVERSITY OF WISCONSIN-MADISON

ASM



Student Activity Center Fall 2024 - Spring 2025 Space Allocation Application

Is your RSO looking for:

- Office Space?
- Storage Cage Space?
- Locker Space?
- A Mailbox?

Apply today by scanning this QR code and filling out an application!

*Deadline to apply is January 15th, 2024.

*If your RSO has 2023 - 2024 allocated space, and you want to be considered to keep it for the 2024 - 2025 year you must apply! See the application for more details.

Center for Leadership & Involvement
UNIVERSITY OF WISCONSIN-MADISON

ASM

Email Spoofing

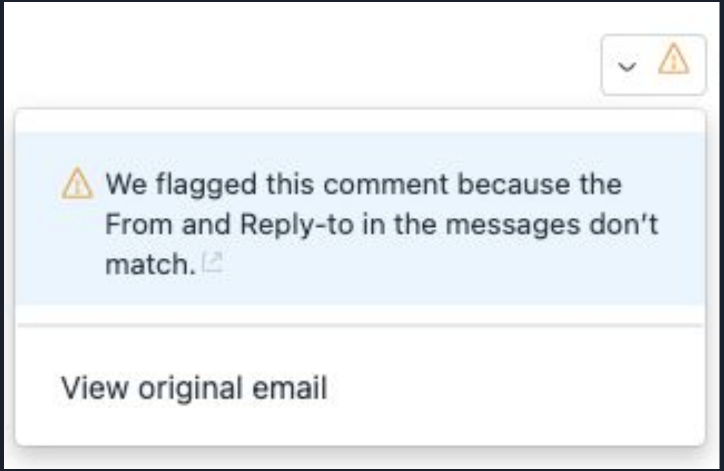
In addition to techniques used earlier, there are techniques specific to email.

Emails are sent using a protocol called Simple Mail Transfer Protocol (SMTP).

Because of the nature of SMTP, fields in the header can be set to anything, meaning the “From” and “Reply-To” fields can be set to any value.

As a result, you can have a message that looks like it was sent from a certain email, but all replies are sent back to the sender.

```
From: legitimate-account@example.com
Reply-to: malicious-actor@example.com
```



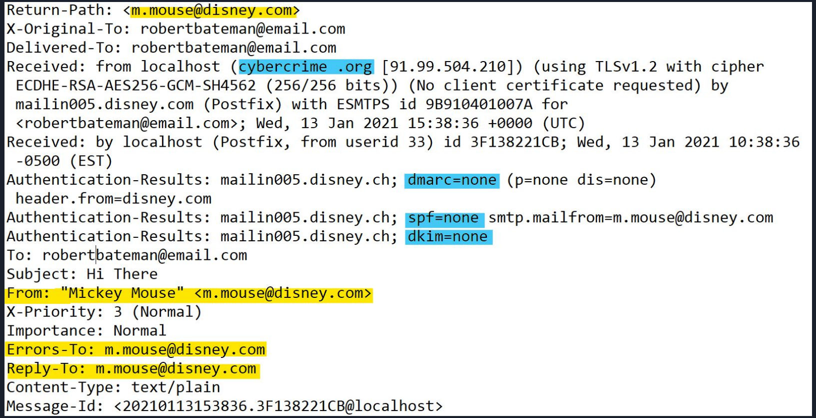
⚠ We flagged this comment because the From and Reply-to in the messages don't match.

Login Page Demo

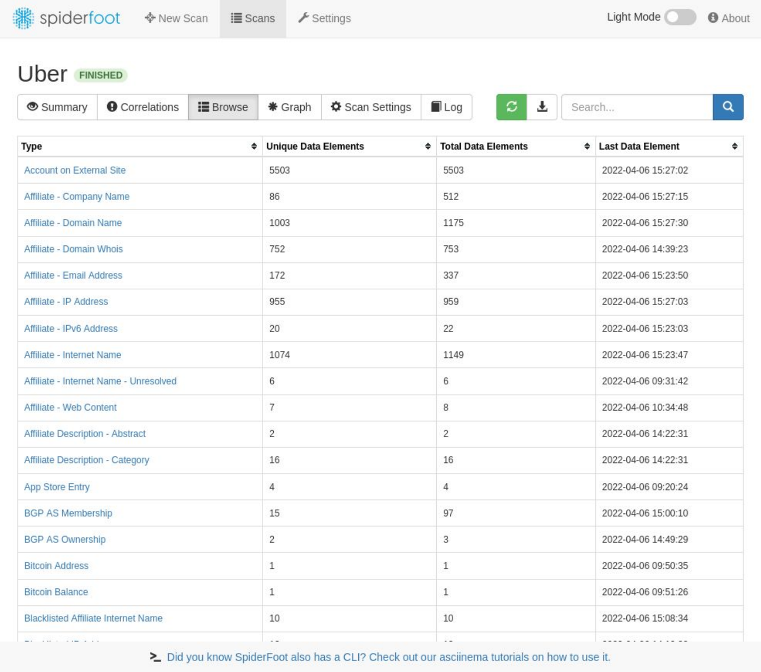
- Transition time

Advanced Techniques for SE

- SMS/Email spoofing
- Spearphishing (OSINT)
- LLM Spearphishing



```
Return-Path: <m.mouse@disney.com>
X-Original-To: robertbateman@email.com
Delivered-To: robertbateman@email.com
Received: from localhost (cybercrime .org [91.99.504.210]) (using TLSv1.2 with cipher
 ECDHE-RSA-AES256-GCM-SH4562 (256/256 bits)) (No client certificate requested) by
 mailin005.disney.com (Postfix) with ESMTPS id 9B910401007A for
 <robertbateman@email.com>; Wed, 13 Jan 2021 15:38:36 +0000 (UTC)
Received: by localhost (Postfix, from userid 33) id 3F138221CB; Wed, 13 Jan 2021 10:38:36
 -0500 (EST)
Authentication-Results: mailin005.disney.ch; dmarc=none (p=none dis=none)
 header.from=disney.com
Authentication-Results: mailin005.disney.ch; spf=none smtp.mailfrom=m.mouse@disney.com
Authentication-Results: mailin005.disney.ch; dkim=none
To: robertbateman@email.com
Subject: Hi There
From: "Mickey Mouse" <m.mouse@disney.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: m.mouse@disney.com
Reply-To: m.mouse@disney.com
Content-Type: text/plain
Message-Id: <20210113153836.3F138221CB@localhost>
```



Uber FINISHED

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	5503	5503	2022-04-06 15:27:02
Affiliate - Company Name	86	512	2022-04-06 15:27:15
Affiliate - Domain Name	1003	1175	2022-04-06 15:27:30
Affiliate - Domain Whois	752	753	2022-04-06 14:39:23
Affiliate - Email Address	172	337	2022-04-06 15:23:50
Affiliate - IP Address	955	959	2022-04-06 15:27:03
Affiliate - IPv6 Address	20	22	2022-04-06 15:23:03
Affiliate - Internet Name	1074	1149	2022-04-06 15:23:47
Affiliate - Internet Name - Unresolved	6	6	2022-04-06 09:31:42
Affiliate - Web Content	7	8	2022-04-06 10:34:48
Affiliate Description - Abstract	2	2	2022-04-06 14:22:31
Affiliate Description - Category	16	16	2022-04-06 14:22:31
App Store Entry	4	4	2022-04-06 09:20:24
BGP AS Membership	15	97	2022-04-06 15:00:10
BGP AS Ownership	2	3	2022-04-06 14:49:29
Bitcoin Address	1	1	2022-04-06 09:50:35
Bitcoin Balance	1	1	2022-04-06 09:51:26
Blacklisted Affiliate Internet Name	10	10	2022-04-06 15:08:34

Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.

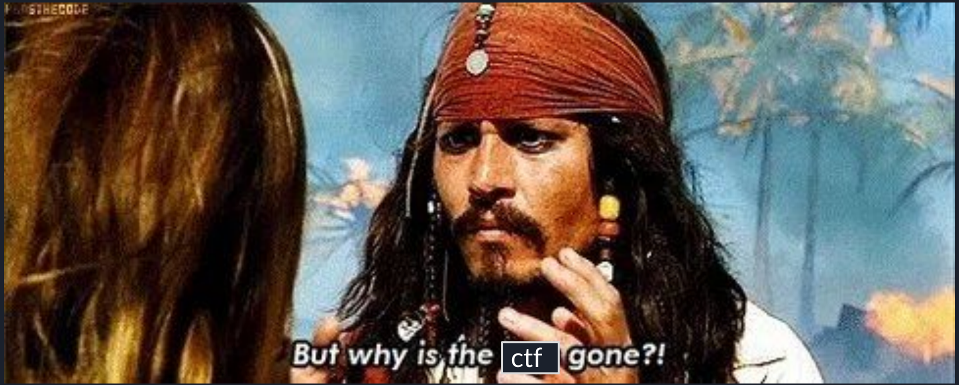
DNS Spoofing Demo

Paul will give this demo

Interactivity

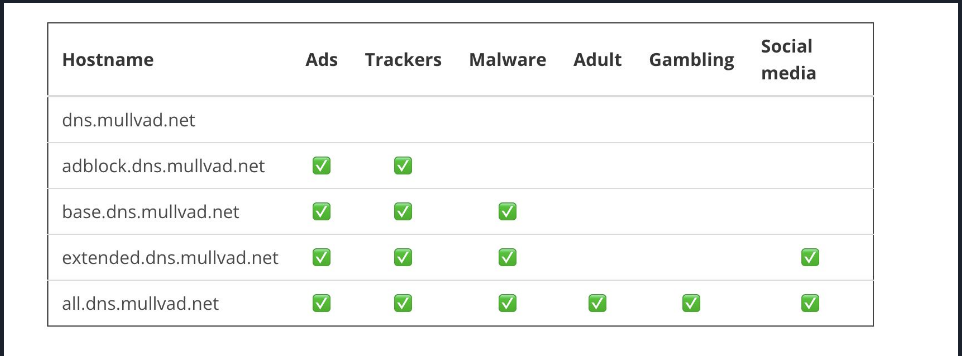
- But where's the CTF??
- Phishing is dangerous business, just ask this guy →

(plugwalkjoe)

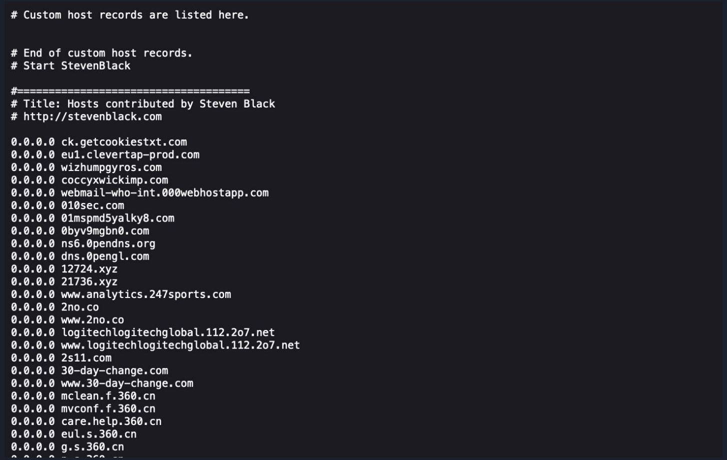


Interactivity

- What more protection can we have other than just “don’t click the link”
- Most of the work can be done in DNS settings!
- Post-click protection
- https://github.com/Ultimate-Hosts-Blacklist/Ultimate.Hosts.Blacklist
- https://github.com/StevenBlack/hosts



Hostname	Ads	Trackers	Malware	Adult	Gambling	Social media
dns.mullvad.net						
adblock.dns.mullvad.net	✅	✅				
base.dns.mullvad.net	✅	✅	✅			
extended.dns.mullvad.net	✅	✅	✅			✅
all.dns.mullvad.net	✅	✅	✅	✅	✅	✅



```
# Custom host records are listed here.


# End of custom host records.
# Start StevenBlack

#=====================================
# Title: Hosts contributed by Steven Black
# http://stevenblack.com

0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eu1.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
0.0.0.0 12724.xyz
0.0.0.0 21736.xyz
0.0.0.0 www.analytics.247sports.com
0.0.0.0 2no.co
0.0.0.0 www.2no.co
0.0.0.0 logitechlogitechglobal.112.2o7.net
0.0.0.0 www.logitechlogitechglobal.112.2o7.net
0.0.0.0 2s11.com
0.0.0.0 30-day-change.com
0.0.0.0 www.30-day-change.com
0.0.0.0 mclean.f.360.cn
0.0.0.0 mvconf.f.360.cn
0.0.0.0 care.help.360.cn
0.0.0.0 eul.s.360.cn
0.0.0.0 g.s.360.cn
```

(+ 160,000 lines more…)