

Technical Means to

Fight **Ph!sh!ng**



APTLD 84 Seoul

Ching Chiao
Senior Advisor APAC
WhoisXMLAPI



WhoisXMLAPI (WXA): What do we do ?

For over a decade, we have been **gathering, analyzing, and correlating domain, IP, and DNS data to make the Internet more transparent and secure.** Our comprehensive collection of cyber threat intelligence feeds have proven invaluable in augmenting the capabilities of commercial / governmental security platforms (SIEM, SOAR and TIP) and helping Security Operations Centers (SOCs) & Managed Security Service Providers (MSSPs) achieve superior network visibility.

Security Industry : Hot “ABC” Topics

- Attack Surface Management (ASM)
 - eASM
- Business Email Compromised (BEC)
/ Spear Phishing
- Cloud Security
 - “agentless” deployment in large scale



Extraordinary Attorney Woo 2022, Netflix



Topics

- Stats / Trends from WXA **Threat Intelligence** data
- Identify phishing domains : examples
- Proposal to APTLD community

From Moderator:

Q1 : what is your experience/statistics of phishing in your registry?

Q2 : what do you do for mitigating phishing in your registry?

Q3 : what do you plan to do for mitigating phishing in your registry?

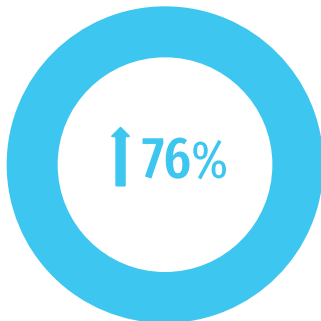
Q4 : what is your proposal to the APTLD community as a whole?

(if you provide solutions to registries/registrars, please read the above questions by replacing "in your registry" to "for your customer registries/registrars")

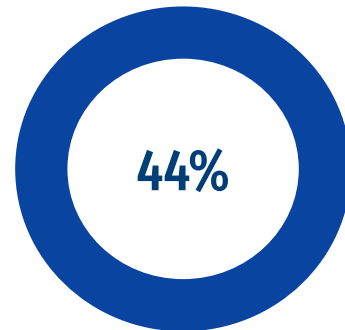
Phishing : Scope of the Problem



**Most prevalent
crime in the US**



**Direct financial losses
increase from successful
phishing attacks**



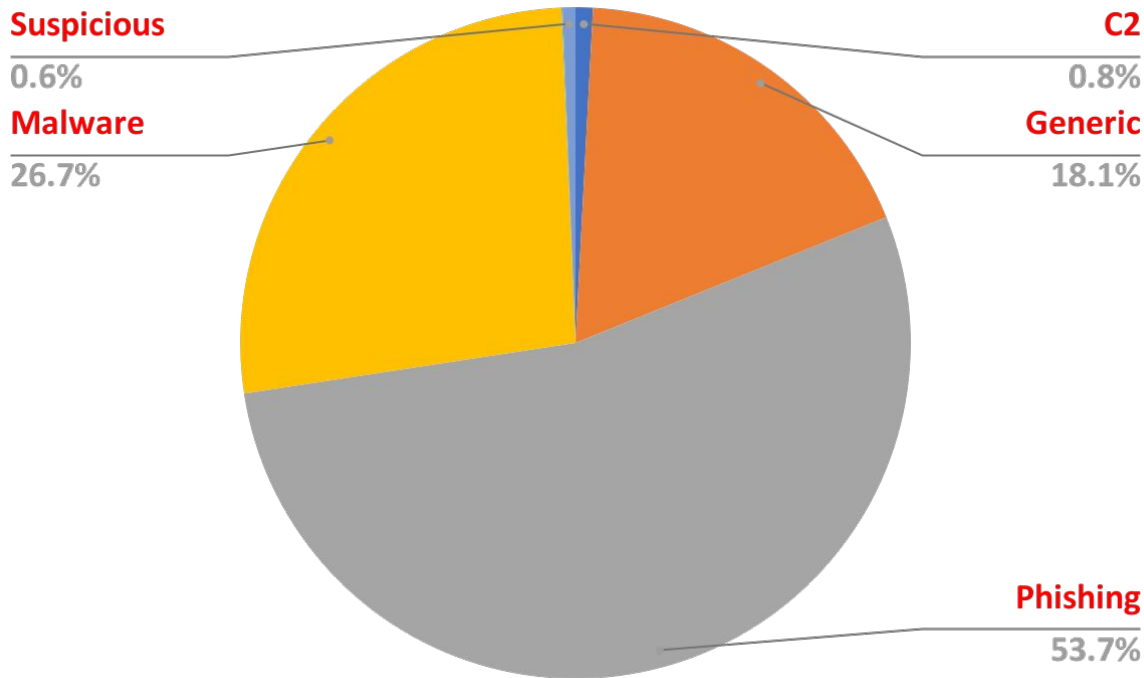
**Users unaware that a
familiar brand doesn't
guarantee the safety of
the email**

The problematic **bulk-registered domains** have been used in different cyber attacks.

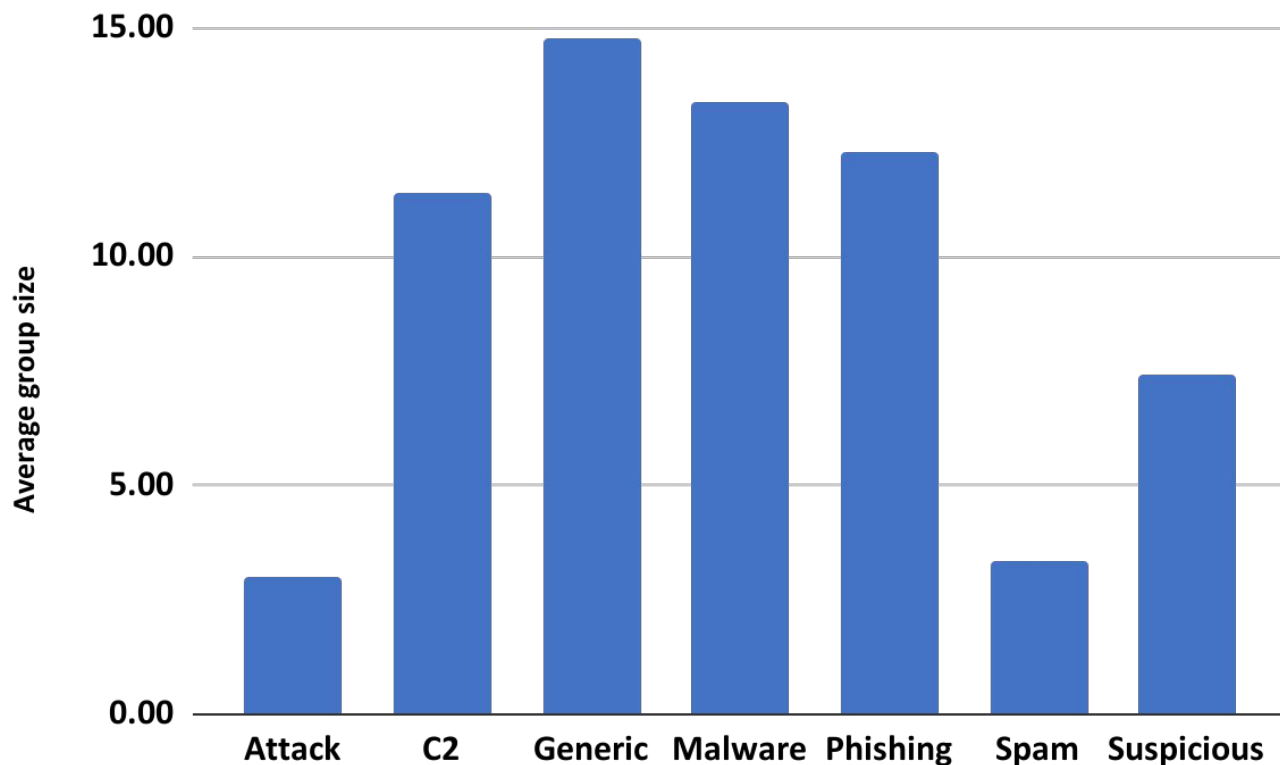
Total Typosquatting Domains:	4,678,815
Total # of hits on TIDF:	20,237
%	0.433



Threat Intelligence Data Feed
(TIDF) dated 10 May 2023

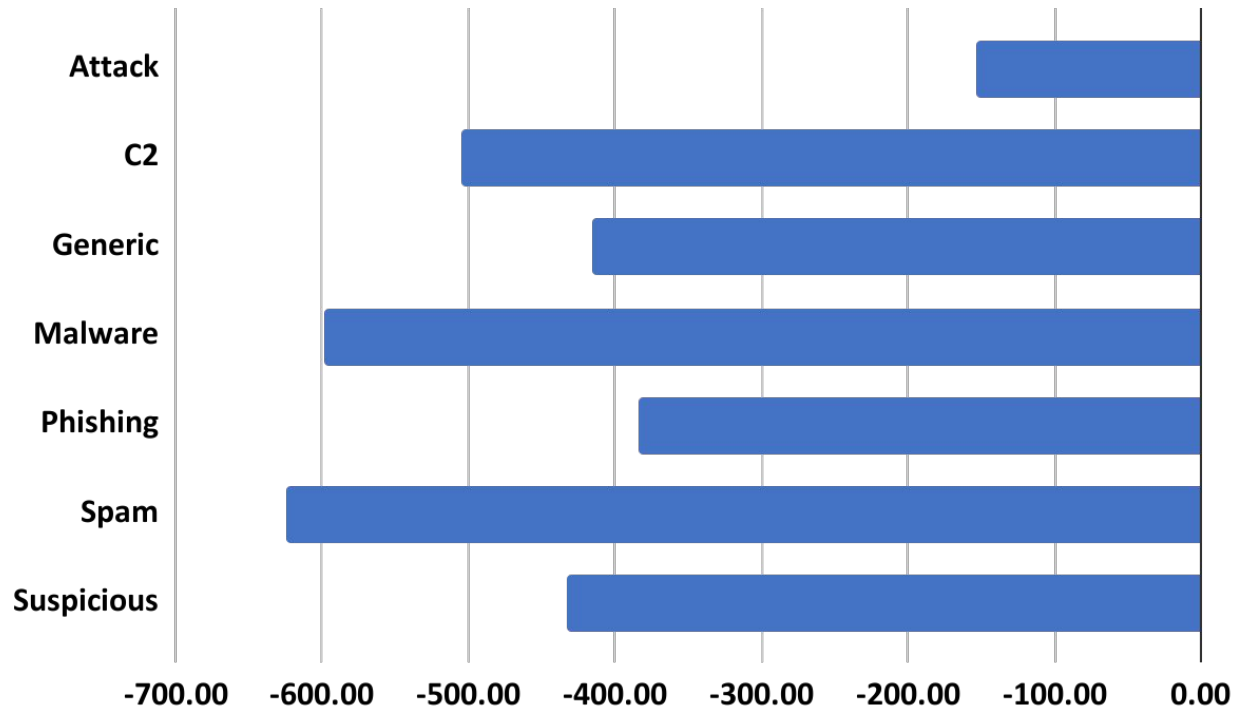


- We also determined the average group size of the problematic **bulk-registered domains**.
- Phishing is a top-3 problem!





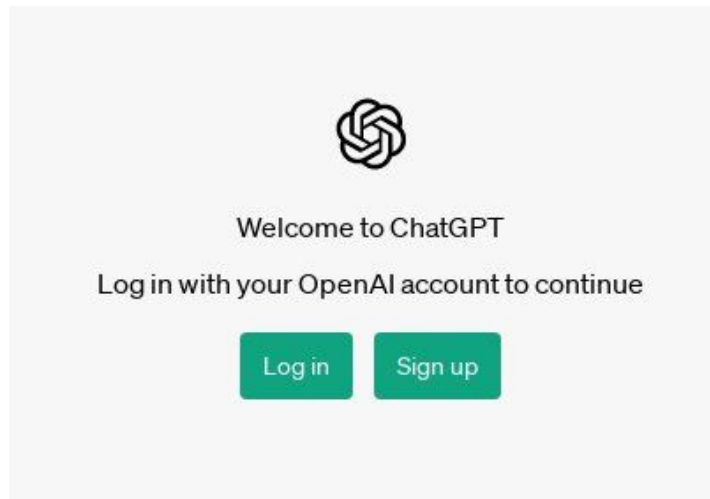
The average “deltaDays” is the gap between **Typosquatting Data Feed** detection and when problematic usage was last detected by TIDF. This value differs per attack type, with Spam having the longest gap of 624.11 days.



Trending and Hot Topics

ChatGPT and the popularity of AI tools

chat.openai.com



170 lookalike domain & subdomain compositions

chat.openai.be >	chat.openai.to >
chat.openai.id >	chat.openai.vn >
chat.openai.kg >	chat.openai.fo >
chat.openai.run >	chat.openai.com >
chat.openai8.me >	chat.openai.dad >
chat.openai.ngo >	chat.openaib.cn >
chat.openai.org.chat.openai.com >	chat.openai1.top >
chat.openaie.com >	chat.openaip.xyz >
chat.openai.bond >	chat.openai8.top >
chat.openai.tube >	chat.openaiw.com >



Trending and Hot Topics

ChatGPT and the popularity of AI tools

chat.openai.com

Domain age

Created Date: January 19, 2007 18:28:24 UTC

Updated Date: December 1, 2022 02:58:08 UTC

Expires Date: January 19, 2027 19:28:24 UTC

Estimated Domain Age: 6053 day(s)

Registrar Name

GANDI SAS >

Very different details found in WHOIS records!

domainName	createdDate	registrarName
openai-telegram.ru	2023-07-21T10:22:25Z	REGRU-RU
aiopenai.net	2023-07-04T09:34:29Z	Wild West Domains, LLC
nextopenai.cn	2023-03-31 23:31:14	阿里云计算有限公司 (万网)
openaiw.com	2023-01-20T02:10:30Z	GoDaddy.com, LLC
openai-gc.cn	2023-04-25 21:33:55	广州云讯信息科技有限公司
infoopenai.com	2023-03-21T09:23:13Z	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
askopenai.net	2023-03-12T11:28:50Z	Google LLC
foxopenai.com	2023-05-23T00:23:33Z	NAMECHEAP INC
hi-openai.com	2023-04-14T11:29:16Z	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
openai-link.cn	2023-04-28 23:00:29	阿里云计算有限公司 (万网)
openai-365pro.com	2023-07-05T21:09:40Z	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
openai-365.com	2023-04-28T13:38:45Z	NAMECHEAP INC

Source: WXA Domain Research Suite (DRS)

Trending and Hot Topics

Also regularly present in our predictive threat intel feeds are brand names

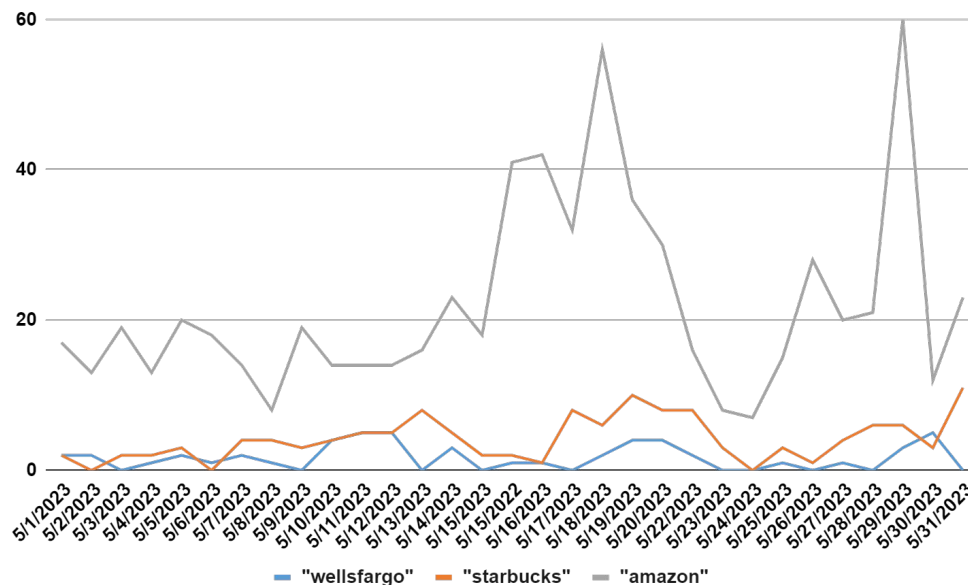
In May 2023, NRDs bearing the strings

“wellsfargo”

“starbucks”

“amazon”

were consistently found in the EWPF files.





Trending and Hot Topics

Ukraine invasion

wedonateukraine.org >
donateukraine.world >
ukraine-donatee.com >
ukrainedonate.today >
ukrainedonation.com >
ukrainedonate.co.uk >
ukrainedonate.pp.ua >
donateukraine.today >
donatetoukraine.org >
donate-ukraine.name >

Covid / vaccine

buyvaccinecovid.ru >
covidvaccinece.org >
ndcovidvaccine.com >
covidvaccine.earth >
mdcovidvaccine.com >
ohcovidvaccine.com >
covid-19vaccine.eu >
covidvaccine.world >
covidvaccine.study >
covid-19vaccine.de >

2023 bank failures

bankcollapse.com >
svbankcollapse.com >
bigbankcollapse.com >
bankcollapse2023.com >
bankcollapselawyer.com >
deutschebankcollapse.fm >
bankcollapselawyers.com >
deutschebankcollapse.com >
bankingsystemcollapse.com >
whichbankcollapsedtoday.com >



Determining If Malicious Domains Remain Active

- We subjected the domains to a bulk IP geolocation lookup to determine if they still had A records.
- Many domains in the sample group had various A records, and therefore may still be resolving to IP addresses.

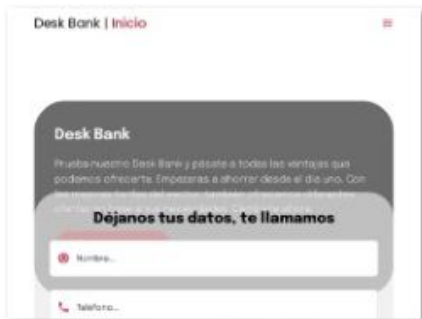


**Bulk IP Geolocation [Lookup](#) dated
13 June 2023**

Term	Resolved IP	Country	Region	City	Latitude	Longitude
banco-desk.site	51.91.153.25	FR	Grand Est	La Petite F	48.58053	7.74058
banco-desk.digital	51.91.153.25	FR	Grand Est	La Petite F	48.58053	7.74058
banco-desk.website	51.91.153.25	FR	Grand Est	La Petite F	48.58053	7.74058
banco-desk.online	51.91.153.25	FR	Grand Est	La Petite F	48.58053	7.74058
coinbasedex.vip	2606:4700:3031::6815:3f16	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.vip	2606:4700:3035::ac43:8e91	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.vip	104.21.63.22	US	California	South Bea	37.78298	-122.39
coinbasedex.vip	172.67.142.145	US	California	South Bea	37.78298	-122.39
coinbasedex.live	2606:4700:3032::ac43:ab0d	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.live	2606:4700:3033::6815:3fa1	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.live	172.67.171.13	US	California	South Bea	37.78298	-122.39
coinbasedex.live	104.21.63.161	US	California	South Bea	37.78298	-122.39
coinbasedex.top	2606:4700:3033::ac43:d1e7	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.top	2606:4700:3032::6815:5d81	CA	Ontario	Toronto	43.70011	-79.4163
coinbasedex.top	104.21.93.129	US	California	South Bea	37.78298	-122.39
coinbasedex.top	172.67.209.231	US	California	South Bea	37.78298	-122.39
hongkong-telegram.com	47.242.229.139	HK	Wong Tai	Wong Tai	22.35	114.1833
hongkong-telegram.site	47.242.229.139	HK	Wong Tai	Wong Tai	22.35	114.1833
hongkong-telegram.org	2606:4700:3034::6815:f6	CA	Ontario	Toronto	43.70011	-79.4163
hongkong-telegram.org	2606:4700:3031::ac43:977e	CA	Ontario	Toronto	43.70011	-79.4163
hongkong-telegram.org	172.67.151.126	US	California	South Bea	37.78298	-122.39
hongkong-telegram.org	104.21.0.246	US	California	South Bea	37.78298	-122.39
hongkong-telegram.xyz	47.242.229.139	HK	Wong Tai	Wong Tai	22.35	114.1833

Determining If Malicious Domains Remain Active

- To further verify the status of the malicious typosquatting groups, we retrieved their website screenshots.
- The content hosted on the sample domains hinted at impersonation, credential theft, and malware distribution.



bancodeskdigital



bancodeskwebsite



coinbasedexvip



hongkongtelegramcom



Screenshot **Lookup** dated 13 June 2023



Leveraging Trusted Infrastructure

Many free services can be leveraged to execute phishing campaigns

Site builders - e.g., WordPress

chatgpttech.wordpress.com >
chatgptplus.files.wordpress.com >
chatgptglobalnews.files.wordpress.com >

chatgptopen.wordpress.com >
chatgptfinance.files.wordpress.com >

SaaS companies- e.g., Zendesk

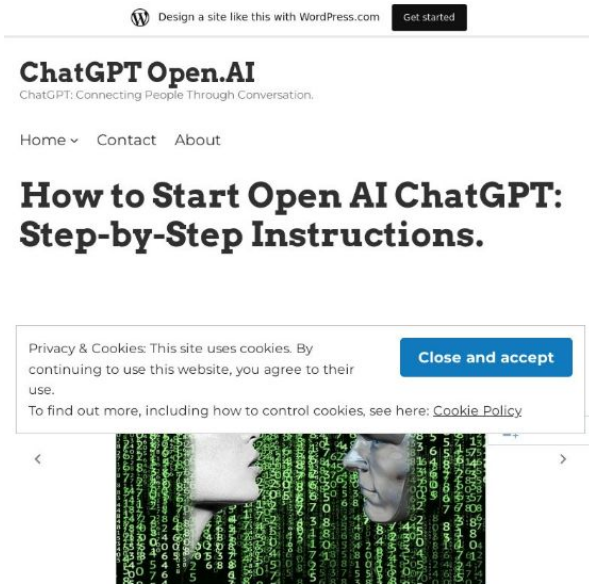
chatgpt.zendesk.com >
chatgpt9659.zendesk.com >
chatgpt3137.zendesk.com >
chatgpt4143.zendesk.com >
chatgpt960.zendesk.com >
chatgpthelp.zendesk.com >
chatgpt8653.zendesk.com >
chatgpt9940.zendesk.com >



Leveraging Trusted Infrastructure

Yet it's not easy to determine what's indeed badness

chatgpttech.wordpress[.]com




chatgptloginncom.files.wordpress[.]com



ChatGPT Login

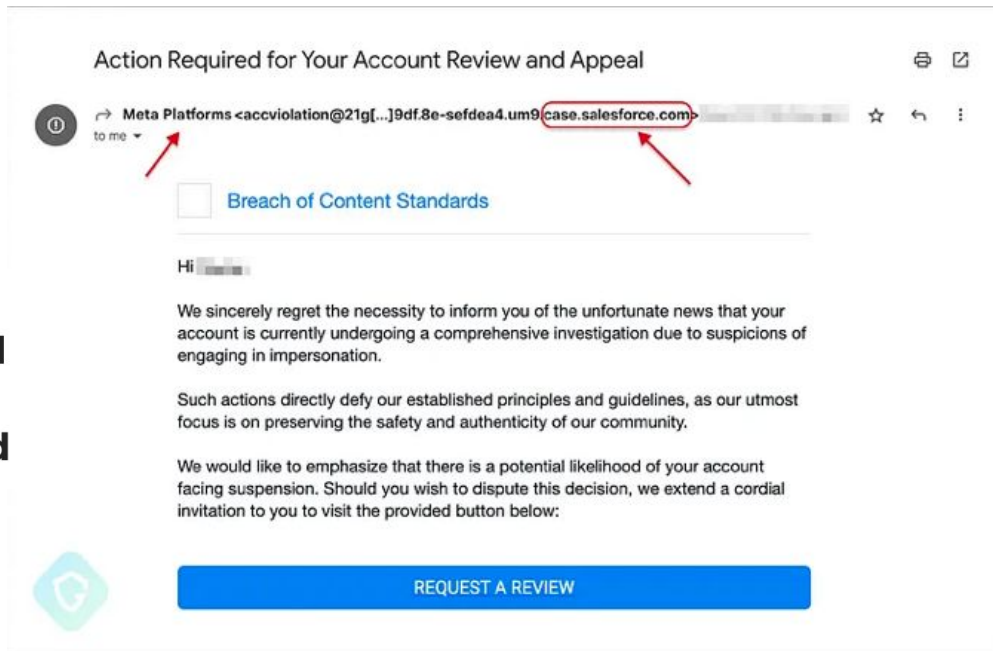
Welcome to the ChatGPT login page! Here, you can easily log in to your account and access all the features of our platform.

 Examples	 Capabilities	 Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally  Follow harmful instructions or biased



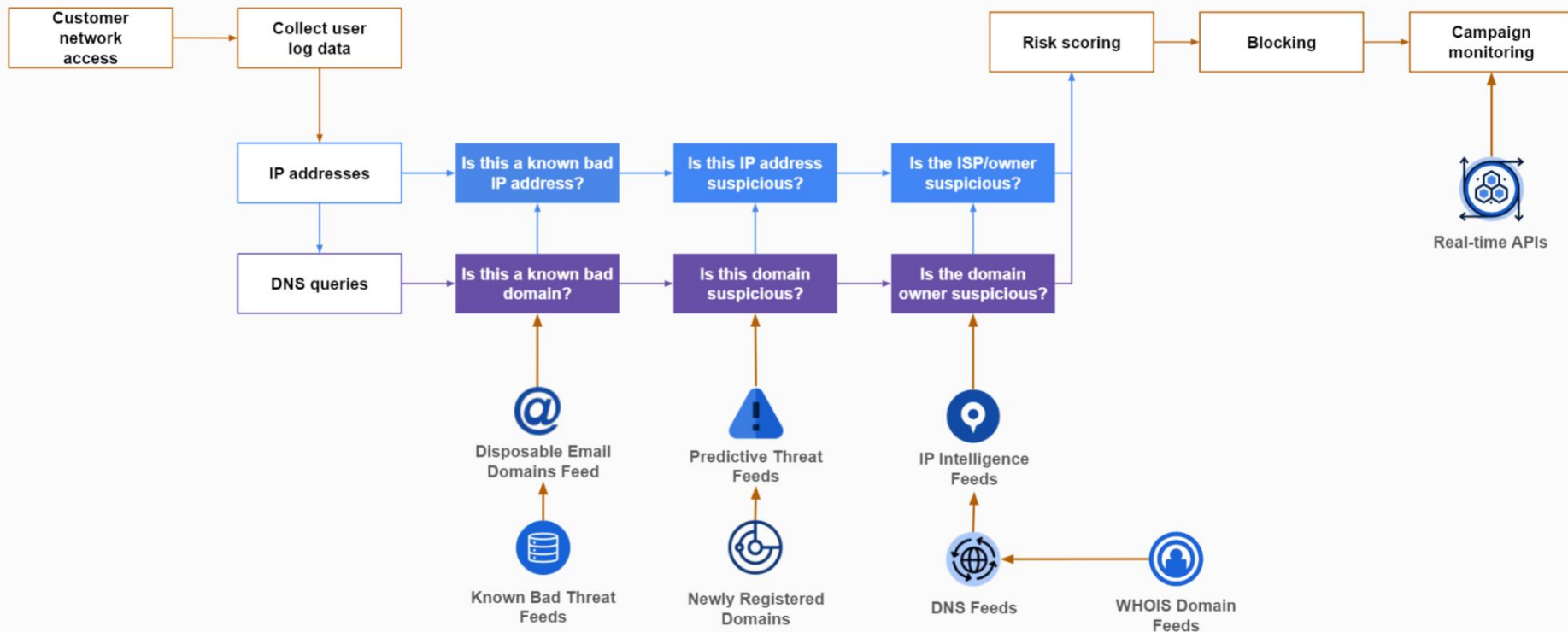
Leveraging Trusted Infrastructure

“PhishForce” — Vulnerability Uncovered in Salesforce’s Email Services Exploited for Phishing Facebook Accounts In-The-Wild



<https://labs.guard.io/phishforce-vulnerability-uncovered-in-salesforces-email-services-exploited-for-phishing-32024ad4b5fa>

DNS & IP Threat Filtering Workflow





Proposal to APTLD

- A Threat Intelligence Hub for APTLD Members
- Regular registry's security / CISO training
- Complimentary access to Domain Research Suite (DRS) for APTLD Members

The background of the slide is a blue geometric pattern composed of various triangles and polygons. The left half of the slide features a darker blue background, while the right half is a lighter blue. The text is positioned on the left side.

Thank you

ching.chiao@whoisxmlapi.com