Overall TLP of this document: TLP:RED

# Masquerade Monitor Report

TLP:AMBER

## VETERAN-THEMED MASQUERADE MONITORING - COMPREHENSIVE DETECTION

Generated: 2025-04-20 19:17:04

Generated by: **MalasadaTech**

TLP Level: TLP:RED

---

TLP:CLEAR Comprehensive monitoring for veteran-themed masquerades using multiple detection methods

Search query: `No query specified`

### Query Metadata

**Query Name:** military-themed-monitoring

**Notes:**

- TLP:GREEN This group combines multiple detection methods for a comprehensive view of VETERAN-THEMED masquerade attempts.
- TLP:AMBER The combined approach detects phishing sites through page titles, and logo hashes.

**Frequency:** Daily

**Priority:** High

**Tags:** financial usaa combined-monitoring military-themed

## Results (4)

## aafes-logo

TLP:CLEAR This shows one subset of phishing sites that masquerade as AAFES.

TLP:RED **Query:** `hash:32be958b45dfdfadd1c4184b8f75f04d8cdef0dea772a8f4f3b9a59cc9d9fc5f AND NOT task.domain:(www.shopmyexchange.com OR shopmyexchange.com)`

**Notes:**

- TLP:CLEAR This is a report of phishing sites that masquerade as AAFES.
- TLP:GREEN The query tracks the masqs by the AAFES logo hash.
- TLP:RED P0401.003 - HTTP: Shared Resources (32be958b45dfdfadd1c4184b8f75f04d8cdef0dea772a8f4f3b9a59cc9d9fc5f)

**References:**

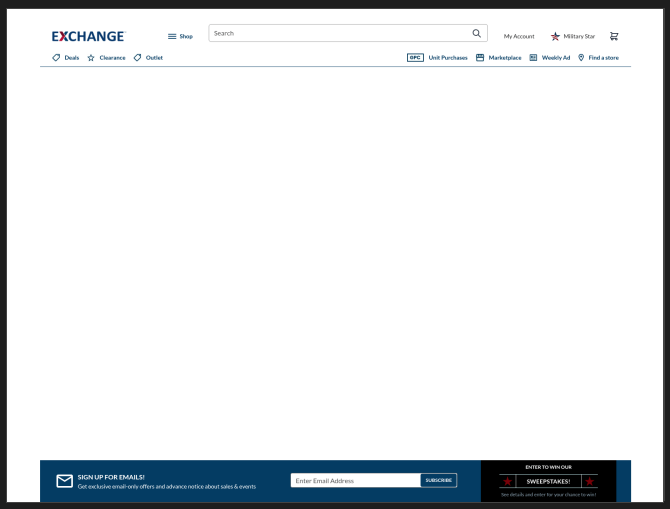
- TLP:GREEN https://malasada.tech/aafes-phishing-sites-observed/
- TLP:GREEN https://github.com/MalasadaTech/defenders-threatmesh-framework
- TLP:RED https://github.com/MalasadaTech/defenders-threatmesh-framework/blob/main/pivots/P0401.003.md

**Frequency:** TLP:GREEN Daily

**Priority:** TLP:GREEN High

**Tags:** TLP:GREEN phishing aafes

**Results:** 1




**Source Query:**
aafes-logo

**URL:**
hxxps://www[.]shopmyexchannge[.]com/

**Domain:**
www[.]shopmyexchannge[.]com

**Page Title:**
Exchange | Military Discount - Tax Free Shopping

**IP Address:**
172.67.221.227

**Scan Date:**
2025-04-21T05:16:14.150Z

**URLScan Link:**
View Full Scan

## usaa-title

TLP:CLEAR This report shows one subset of phishing sites that masquerade as USAA.

TLP:RED **Query:** `page.title:"Member Account Login | USAA" AND NOT task.domain:*.usaa.com AND NOT page.domain:*.usaa.com`

**Notes:**

- TLP:CLEAR This shows phishing sites that masquerade as USAA.
- TLP:GREEN The query tracks the masqs by the page title.
- TLP:RED P0401.001 - HTTP: Title ("Member Account Login | USAA")

**References:**

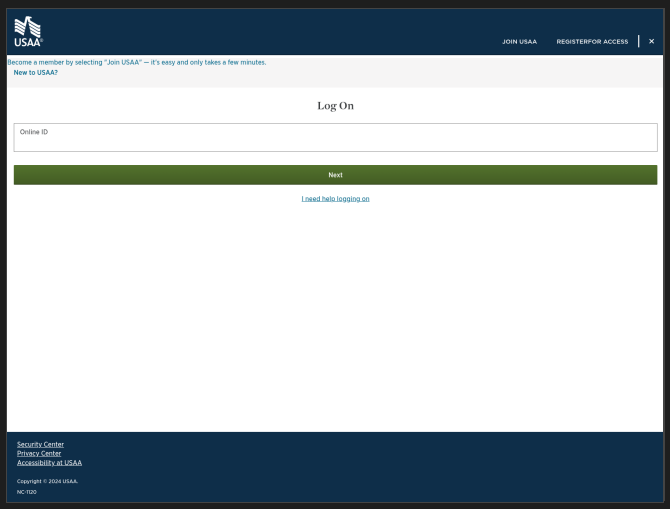
- TLP:GREEN https://malasada.tech/usaa-masquerades-found/
- TLP:GREEN https://github.com/MalasadaTech/defenders-threatmesh-framework
- TLP:RED https://github.com/MalasadaTech/defenders-threatmesh-framework/blob/main/pivots/P0401.001.md

**Frequency:** TLP:GREEN Daily

**Priority:** TLP:GREEN High

**Tags:** TLP:GREEN phishing banking

**Results:** 3




**Source Query:**
usaa-title

**URL:**
hxxps://hospitable-ethereal-horn[.]glitch[.]me/public/style.html

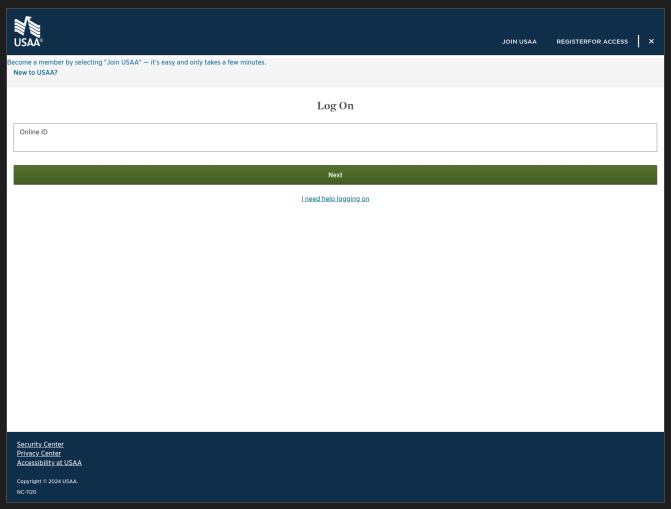
**Domain:**
hospitable-ethereal-horn[.]glitch[.]me

**Page Title:**
Member Account Login | USAA

**IP Address:**
151.101.194.59

**Scan Date:**
2025-04-21T05:15:26.516Z

**URLScan Link:**
View Full Scan




**Source Query:**
usaa-title

**URL:**
hxxps://hospitable-ethereal-horn[.]glitch[.]me/public/style.html

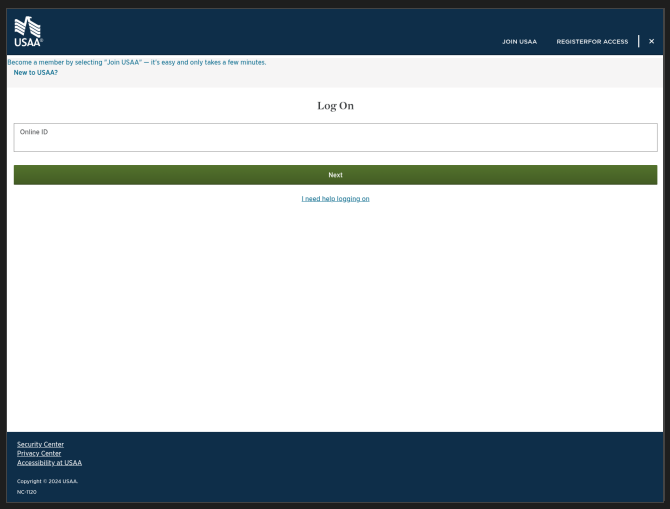
**Domain:**
hospitable-ethereal-horn[.]glitch[.]me

**Page Title:**
Member Account Login | USAA

**IP Address:**
2a04:4e42::571

**Scan Date:**
2025-04-15T23:25:06.068Z

**URLScan Link:**
View Full Scan




**Source Query:**
usaa-title

**URL:**
hxxps://hospitable-ethereal-horn[.]glitch[.]me/public/style.html

**Domain:**
hospitable-ethereal-horn[.]glitch[.]me

**Page Title:**
Member Account Login | USAA

**IP Address:**
2a04:4e42:200::571

**Scan Date:**
2025-04-15T17:05:20.277Z

**URLScan Link:**
View Full Scan

---

Overall TLP of this document: **TLP:RED**

Generated with Masquerade Monitor on 2025-04-20 19:17:04

GitHub Project | by MalasadaTech