Investigation Log

Case Information

Case ID: 2025-09-10-001

Date & Time: 2025-09-10, 11:00 – 13:00

Analyst: Oluwaniyi Damilare Enoch

Escalation Level: Tier 1 – Tier 2

Initial Alert

Time and date detected: 2025-09-10, 11:05

URL received: hxxps[://]sites[.]google[.]com/view/xksl/home

Suspicion: Possible phishing attempt.

Artifact 001:

Actions Taken

11:12 – First Analysis

Opened in URL2PNG

Artifact 002:

Homepage displayed **GMX branding** (possible impersonation).

Visible button text: *KLICKEN SIE HIER* (“Click Here” in German).

11: 20 - Page Content Analysis

Opened in Wanna Browser

Suspicious link extracted (from <a> tags)

Defanged Link:
hxxps[://]www[.]google[.]com/url?q=hxxps%3A%2F%2Fwonderful-ganache-327ff8[.]netlify[.]app%2F&sa=D&sntz=1&usg=AOvVaw3TU1W7ZzQGpdsh2YKdStjv

11:40 – Redirect Chain Analysis

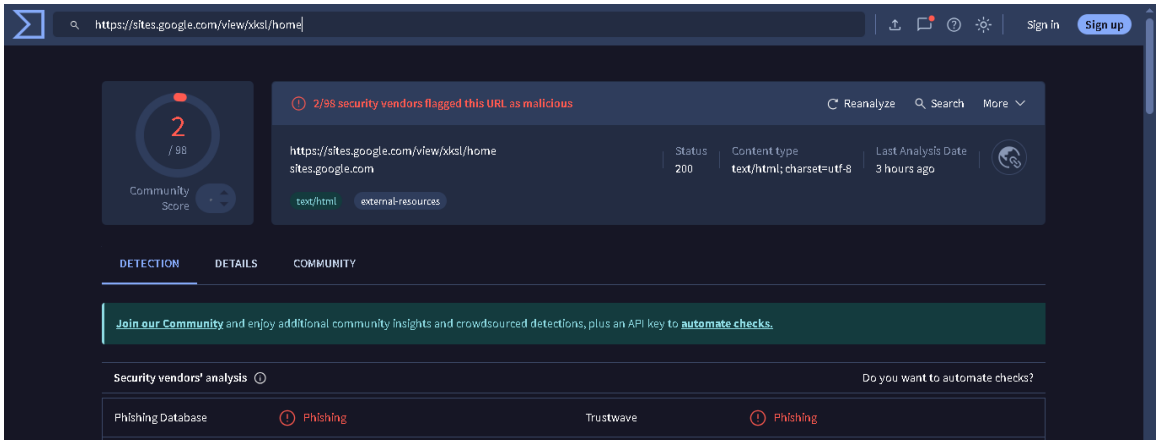
Observed 3 stages(all URLS were Defanged):

1. Initial page → hxxps[://]sites[.]google[.]com/view/xksl/home
2. Redirect → hxxps[://]www[.]google[.]com/url?q=hxxps%3A%2F%2Fwonderful-ganache-327ff8[.]netlify[.]app%2F&sa=D&sntz=1&usg=AOvVaw3TU1W7ZzQGpdsh2YKdStjv
3. Final destination → hxxps[://]wonderful-ganache-327ff8[.]netlify[.]app

11:50 – VirusTotal Analysis

1. hxxps[://]sites[.]google[.]com/view/xksl/home → flagged (phishing).

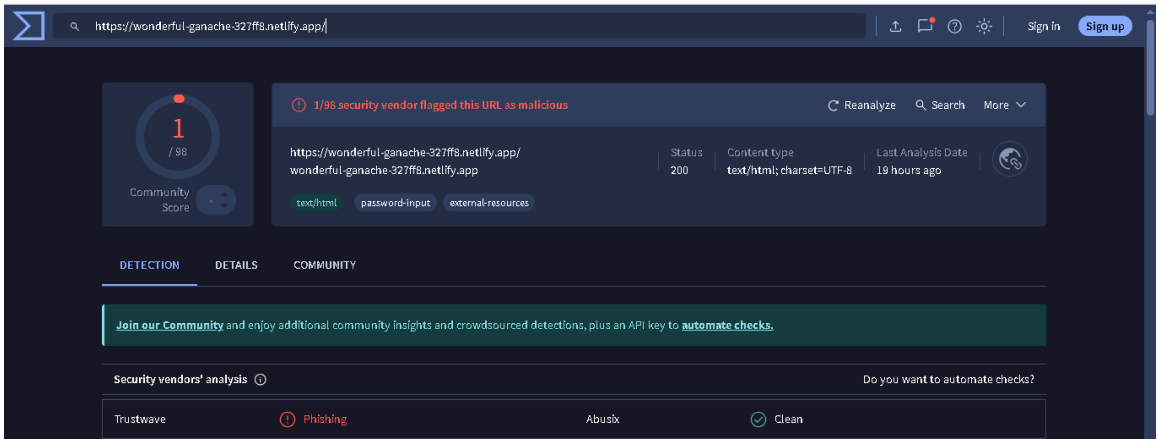
Artifact 003:



Body SHA-256:
5d0d18c0f01903de67441a0dbb5a366b9c66b949069a6789821827f340401d2a

2. hxxps[://]wonderful-ganache-327ff8[.]netlify[.]app → flagged by multiple vendors as phishing.

Artifact 004:



Body SHA-256:
d62c53f8272758e99e35ca2e1c51b3cca79d9fdcaf60db16b6a15091de54e4da

12:05 – Background Behavior Concern

- Final page returned “Site not found” on Netlify.
- Possible that content was removed OR taken down after reporting.
- Cannot rule out hidden background requests (data exfil, beaconing).
- No active payload downloaded during test.

12:20 – Contextual Research

- GMX = two popular domains:
  - gmx.com (European email provider).
  - gmx.io (crypto exchange).
- Fake site may have attempted credential harvesting for either/both.

12:35 - MITRE ATT&CK Mapping

- Observed Technique(s):
  - T1566.002 – Phishing: Spearphishing via Link

- Potential/Intended Technique(s):
  - T1105 – Ingress Tool Transfer (if a payload were delivered)
- Follow-on Technique(s) (possible future use):
  - T1078 – Valid Accounts (if credentials harvested are later used)

13:00 – Escalation

- Recommended for Tier 2:
  - Run in sandbox with full network traffic capture**.**
  - Analyze for hidden background requests.
  - Attempt recovery of phishing form (if Netlify page restored).
- **Artifacts Submitted to Case Folder:**
  - Screenshots (Artifacts 001–004).
  - VirusTotal raw JSON reports for these two urls below are attached to the case folder:

    hxxps[://]sites[.]google[.]com/view/xksl/home (virustotal_report.json)

    hxxps[://]wonderful-ganache-327ff8[.]netlify[.]app (virustotal_report1.json)

  - HTML snippet extraction is attached below

 KLICKEN SIE HIER

Summary Section:

- Summary: Phishing attempt impersonating GMX via Google Sites which redirects to another site hosted on Netlify. Site taken down mid-investigation. No payload observed, but credential harvesting suspected.
- Impact: Medium – risk of stolen email or crypto credentials.
- Status: Escalated to Tier 2 for deeper investigation