

Email samples and screenshots in this analysis are from Phishing Pot by Peixoto, licensed under CC BY-NC 4.0. The original sample analysed in this report can be found below:

Phishing Pot: https://github.com/rf-peixoto/phishing_pot

Peixoto: <https://github.com/rf-peixoto>

License: https://github.com/rf-peixoto/phishing_pot/blob/main/LICENSE

Source file: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-1050.eml

Executive Summary

=====

This report analyzes a phishing email impersonating Apple, sent from an Otto Newsletter email address. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of restoring their iCloud storage and getting 50 GB of free storage. Indicators of compromise include urgency tactics, failure of DKIM authentication, and the use of a malicious Webflow-hosted URL. Although the phishing page has since been removed, the email demonstrates typical characteristics of credential and credit card harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers

=====

Date: Mon, 31 Jul 2023 23:23:26

Subject: phishing@pot, Ihr iCloud-Speicher ist voll

To: phishing@pot

From: otto-newsletter@newsletter.otto.de

Reply-To: reply_to@winner-win.art

Return-Path: return@winner-win.art

Sender IP: 80.96.157.86

Resolve Host: qktxzqsjmhytguijbkrjxkzhstbswa.whstt5

Message-ID: <tybiCBw.50937.068+=phishing@pot@winner-win.art>

URLs

=====

hxxps[://]t[.]co/gDHura2rGc

hxxp[://]bsq2[.]firiri[.]shop/dGVQSnprazRvQzk4dkhsbkwyGVGNDdBZm41TE9NWTIRc2dRMFk0WkdFcTkyS2V4VHZldGpmbDNQa3FtUmJSL1RtYzloOFgzdlMwaFdUKy9WYkNSY2c9PQ__

hxxp[://]bsq2[.]firiri[.]shop/dGtKanBhZjJSSVE3K3MwNVU1VStTSlDnMTNwRS93ZE9MZ242NE9nM2RYaFg0N1IPak1IRGRFM0pLenZxT3QxOTRtV1dPL2dCMDNYeitjNXNUTW1ucFE9PQ__

hxxp[://]bsq2[.]firiri[.]shop/YIRmclFmUmJ1SHVMVFRGNjJRQU1QbVdtL2ZSS09CMVdXTkJGc2Z3cWFXMkVmT3NUN3BrdTfKZGJMQi84eVdJNG5hQ29NTzlzcS9hVTFvRnhudFdsUHc9PQ__

Description

=====

It is a German email, claiming to be related to Apple/iCloud, warning that the storage limit has been reached, and that they can get a free 50 GB upgrade by just clicking a prominent button in the email.

The email gives a sense of urgency, as it claims their data will be deleted if they do not increase their iCloud storage.

In small font, there is a disclaimer saying that they will need to enter credit card details, but that there will be no charge.

The Apple logo in the email is just a cartoon picture of an Apple, and not the correct logo. When looking at the eml file, it seems to just be the apple emoji.

The grammar uses the overly friendly version of 'you' (du) instead of the more formal 'you' (Sie) how customers would normally be addressed with.

Artifact Analysis

=====

Sender Analysis:

The From address uses the newsletter[.]jotto[.]de Domain, which is not related to Apple or iCloud.

The Return-to and Return-Path email addresses use the winner-win[.]art domain, which is not related to Apple or iCloud in any way. The winner-win[.]art domain is considered a phishing domain by 7 out of 95 security vendors on VirusTotal.

SPF, DKIM and DMARC authentication all fail.

URL Analysis:

hxxps[://]t[.]co/gDHura2rGc is a shortened URL that does not lead anywhere and looks to be expired. However, when looking up the URL on VirusTotal, it says that one security vendor reported the URL for phishing.

The hxxp[://]firiri[.]shop domain is considered malicious by 10 out of 97 security vendors on VirusTotal. When looking on Google, there do not seem to be any legitimate companies called

Firiri that use that domain. MxToolbox says that the URL cannot be resolved, so it looks like the attacker abandoned using this domain.

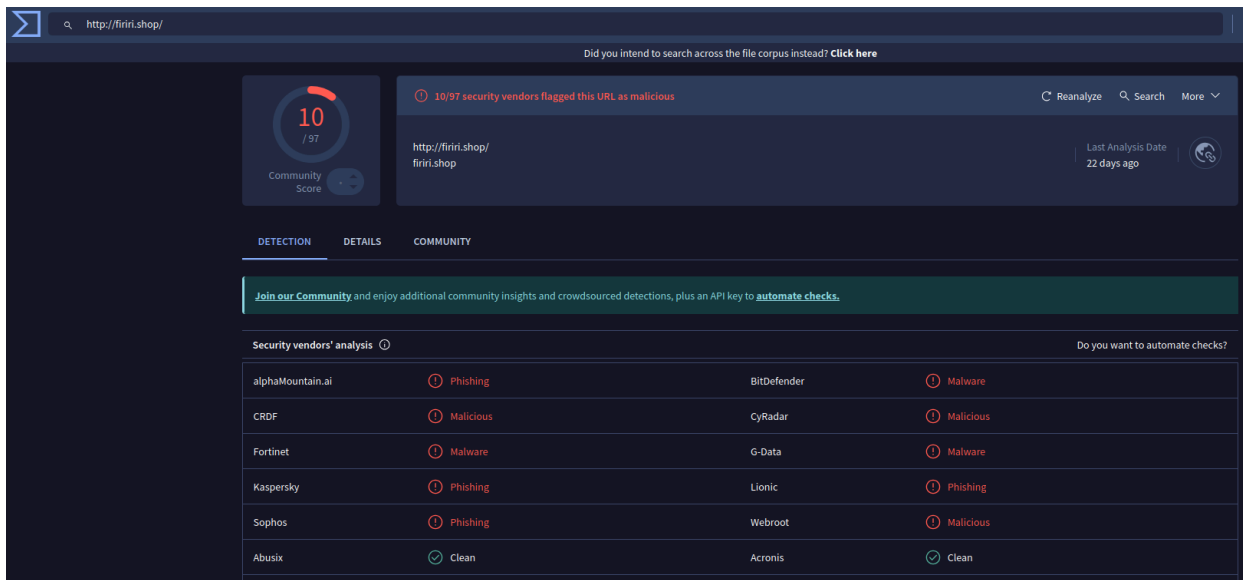
Verdict

=====

Due to the sender not being affiliated with Apple and not using the proper logo, this is a clear spoofing attempt.

Additionally, after analyzing the URL contained in the email's call to action, it was flagged on VirusTotal to be malicious.

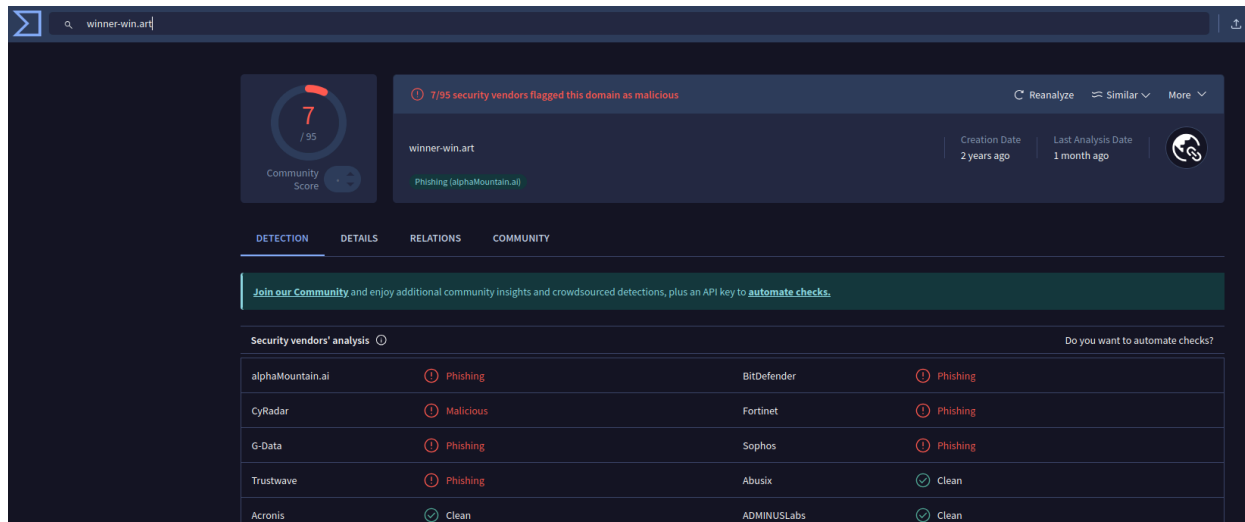
hxxp[:]firiri[.]shop on VirusTotal:



The screenshot shows the VirusTotal interface for the URL `http://firiri.shop/`. The Community Score is 10/97. A warning states that 10/97 security vendors flagged this URL as malicious. The last analysis date was 22 days ago. Below the tabs, a banner encourages joining the community. The 'Security vendors' analysis' table shows the following results:

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Phishing	BitDefender	Malware
CRDF	Malicious	CyRadar	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Phishing	Lionic	Phishing
Sophos	Phishing	Webroot	Malicious
Abusix	Clean	Acronis	Clean

Winner-win[.]art on VirusTotal:



As a result of the analysis, this email has been determined to be malicious.

Defense Actions

=====

After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the “winner-win[.]art” email domain on the email gateway. The winner-win[.]art domain does not seem to be related to any actual legitimate companies or services.

To ensure users are unable to access this malicious URL or domain, I have blocked “firiri[.]shop” on the EDR and on the Web Proxy. While the website seems to have been removed, it is unlikely that a legitimate service will use that domain in the future.

The otto.de domain seems to be a legitimate German retailer, and has therefore not been blocked. Likewise, the URL shortening service is a legitimate service that seems to have been used by a malicious actor.