ThreatConnect

Incident Report

20210329A: Gmail and Yahoo Spoofing Domains Registered Through Njalla on 3/25/21

Type
Incident

Owner
Common Community

Event Date
03/29/2021

Date Added
03/29/2021

Description

ThreatConnect Research identified Gmail and Yahoo spoofing domains admin-gmall-na-reset.click and yahoousersecurity.com, which were registered at essentially the same time through Njalla on 3/25/21. The admin-gmall-na-reset.click previously resolved to a dedicated server at 207.148.10.117, while yahoousersecurity.com hasn't resolved. Both domains are set up to use Protonmail mail servers, suggesting their use in phishing activity.

Security Labels

TLP:GREEN

Tags

Dedicated Server | Phishing | Spoofed | Suspicious Name Server Use

Attributes

Threat Level
Medium
Source Date Time
03-29-2021 00:00 UTC
Date of Discovery
03-29-2021
Source
ThreatConnect Enrichment

20210329A: Gmail and Yahoo Spoofing Domains Registered Through Njalla on 3/25/21

Incident Report

Associated Signatures

20210329A: Gmail and Yahoo Spoofing Domains Registered Through Njalla on 3/25/21.rules

Type
Signature

Description
Snort signature to detect network indicators associated with Incident 20210329A: Gmail and Yahoo Spoofing Domains Registered Through Njalla on 3/25/21

Associated Indicators

207.148.10.117

Type
Address

Date Added
03/29/2021

Description
IP address previously hosted possible phishing domain admin-gmall-na-reset.click.

Source
ThreatConnect Enrichment

Rating
Low
(2/5)

Confidence
Unknown

20210329A: Gmail and Yahoo Spoofing Domains Registered Through Njalla on 3/25/21

Incident Report

yahoousersecurity.com

Type
Host

Date Added
03/29/2021
Description
Spoofed domain registered through Njalla on 3/25/21 and possibly used for phishing.
Source
ThreatConnect Enrichment

Rating
Low
(2/5)
Confidence
Improbable
(9/100)

admin-gmall-na-reset.click

Type
Host

Date Added
03/29/2021
Description
Spoofed domain registered through Njalla on 3/25/21 and possibly used for phishing.
Source
ThreatConnect Enrichment

Rating
Low
(2/5)
Confidence
Improbable
(9/100)