Mar 06 2024

NETMANAGEIT

Intelligence Report

On-Device Fraud on the rise: exposing a recent fraud campaign

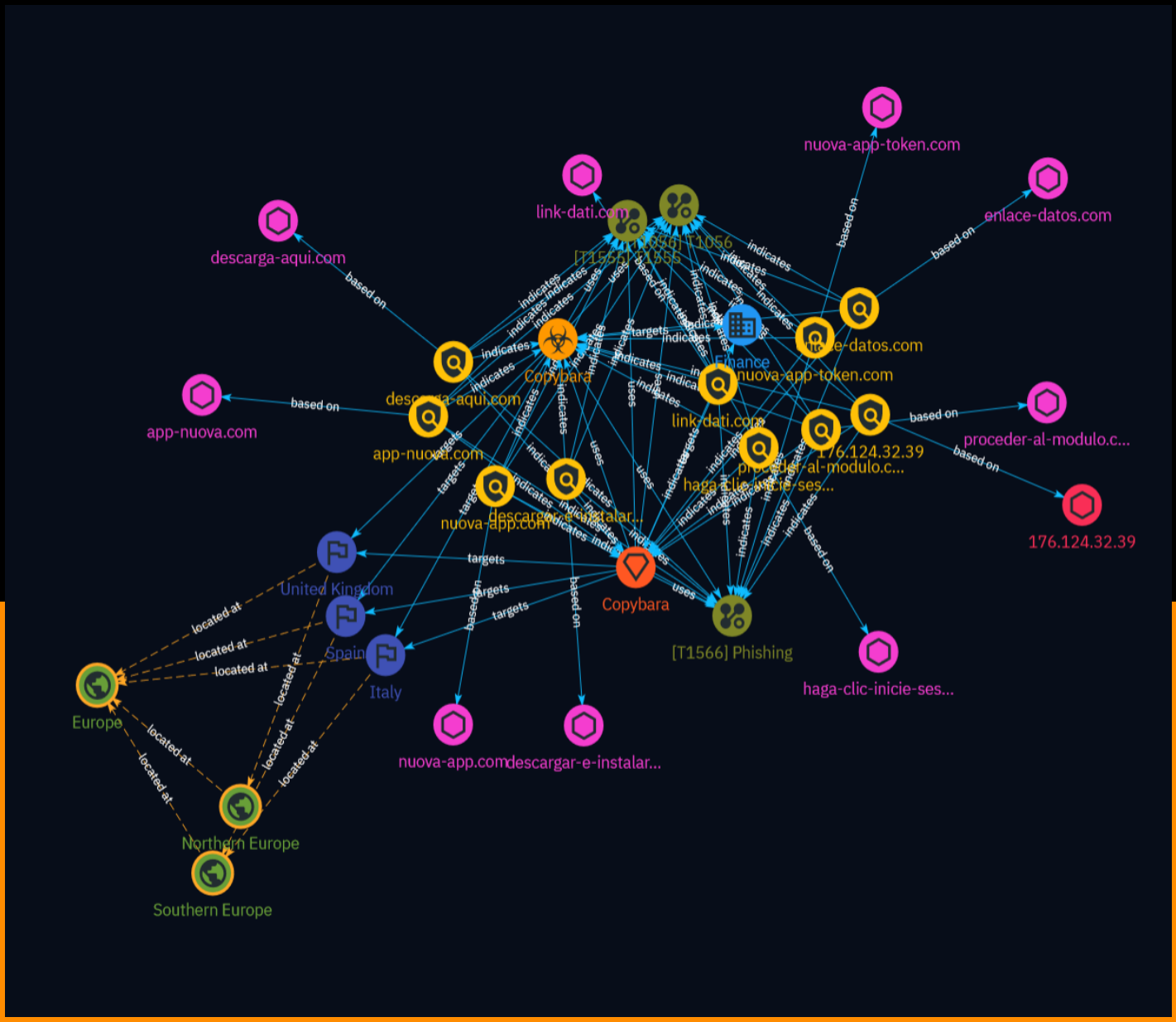

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A recent investigation uncovered an ongoing fraud campaign abusing the Copybara Android banking trojan to perform unauthorized bank transfers via instant payments. Threat actors exploited social engineering and remote access capabilities to infect devices and orchestrate on-device fraud undetected.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

proceder-al-modulo.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1703759408, 'iso': '2023-12-28T05:30:08-05:00'} - **IPQS: Domain:** proceder-al-modulo.com - **IPQS: IP Address:** 172.67.199.21

Pattern Type

stix

Pattern

[domain-name:value = 'proceder-al-modulo.com']

Name

nuova-app.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Phishing - **Domain Age:** {'human':

'2 months ago', 'timestamp': 1704723293, 'iso': '2024-01-08T09:14:53-05:00'} - **IPQS: Domain:** nuova-app.com - **IPQS: IP Address:** 172.67.159.113

Pattern Type

stix

Pattern

[domain-name:value = 'nuova-app.com']

Name

nuova-app-token.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 months ago', 'timestamp': 1704887890, 'iso': '2024-01-10T06:58:10-05:00'} - **IPQS: Domain:** nuova-app-token.com - **IPQS: IP Address:** 104.21.66.121

Pattern Type

stix

Pattern

[domain-name:value = 'nuova-app-token.com']

Name

link-dati.com

Pattern Type

stix

Pattern

[domain-name:value = 'link-dati.com']

Name

haga-clic-inicie-sesion.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1704454694, 'iso': '2024-01-05T06:38:14-05:00'} - **IPQS: Domain:** haga-clic-inicie-sesion.com - **IPQS: IP Address:** 104.21.23.47

Pattern Type

stix

Pattern

[domain-name:value = 'haga-clic-inicie-sesion.com']

Name

enlace-datos.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2

months ago', 'timestamp': 1704892513, 'iso': '2024-01-10T08:15:13-05:00'} - **IPQS: Domain:** enlace-datos.com - **IPQS: IP Address:** 104.21.88.23

Pattern Type

stix

Pattern

[domain-name:value = 'enlace-datos.com']

Name

descargar-e-instalar.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1704454919, 'iso': '2024-01-05T06:41:59-05:00'} - **IPQS: Domain:** descargar-e-instalar.com - **IPQS: IP Address:** 172.67.202.17

Pattern Type

stix

Pattern

[domain-name:value = 'descargar-e-instalar.com']

Name

descarga-aqui.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 months ago', 'timestamp': 1704800918, 'iso': '2024-01-09T06:48:38-05:00'} - **IPQS: Domain:** descarga-aqui.com - **IPQS: IP Address:** 104.21.66.224

Pattern Type

stix

Pattern

[domain-name:value = 'descarga-aqui.com']

Name

176.124.32.39

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Europe/Tallinn - **Mobile:** False - **Host:** 176.124.32.39 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** EE - **Region:** Harjumaa - **City:** Tallinn - **Latitude:** 59.44 - **Longitude:** 24.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.124.32.39']

Name

app-nuova.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 months ago', 'timestamp': 1704801324, 'iso': '2024-01-09T06:55:24-05:00'} - **IPQS: Domain:** app-nuova.com - **IPQS: IP Address:** 104.21.1.242

Pattern Type

stix

Pattern

[domain-name:value = 'app-nuova.com']

Malware

Name
Copybara

Intrusion-Set

Name
Copybara

Attack-Pattern

Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
Phishing
ID
T1566
Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1555

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Country

Name
Spain
Name
Italy
Name
United Kingdom

Region

Name
Southern Europe
Name
Northern Europe
Name
Europe

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Domain-Name

Value
proceder-al-modulo.com
nuova-app.com
nuova-app-token.com
haga-clic-inicie-sesion.com
link-dati.com
enlace-datos.com
descargar-e-instalar.com
descarga-aqui.com
app-nuova.com

IPv4-Addr

Value
176.124.32.39

External References

- https://www.cleafy.com/cleafy-labs/on-device-fraud-on-the-rise-exposing-a-recent-copybara-fraud-campaign
- https://otx.alienvault.com/pulse/65e88d9fdd767d276ae35f0d