Cyber Threat Researcher at Okta

DANIEL LÓPEZ

Threat intelligence / Phishing / Identity attacks

Currently at Okta, focused on researching identity-based threats, tracking threat actors and campaigns, and turning threat intelligence into actionable detections and protections. I also build open threat feeds now included in MISP, YETI and OpenCTI.

hi@daniel.tools linkedin.com/in/0xDanielLopez github.com/0xDanielLopez x.com/0xDanielLopez

Now	**Cyber Threat Researcher, Okta** Identity Threat Research team
Building	**TweetFeed and phishunt** Open threat intelligence feeds
Experience	**In cybersecurity since 2017** Security operations, incident response, threat research
Research	**Okta Threat Intelligence blog** Phishing, PhaaS and infostealer campaigns
Open source	**Feeds in MISP, YETI and OpenCTI** Available as default feeds, lookup modules and connectors
Education	**Master's Degree in Telecommunications Engineering** Universidad de Sevilla

Experience

I am a **Cyber Threat Researcher** with a background spanning identity threat research, phishing investigations, incident response, threat hunting and security operations. Since 2017, I have helped international organizations in a wide range of sectors investigate, contain and remediate threats across diverse environments.

Jun. 2024 - Present
2 yrs 5 mos

Current role

Okta

Cyber Threat Researcher

okta.com

Part of Okta's **Identity Threat Research** team, researching identity-focused threats and attacker tactics, techniques and procedures.

A few pieces of research published on the Okta Threat Intelligence blog.

See the 6 posts in Research ↓

Oct. 2020 - Jun. 2024
3 yrs 9 mos

Citrix

Cloud Software Group

Sr. Security Engineer

cloud.com

Worked in the global Security Operations Center of Cloud Software Group, the parent company of Citrix, handling 24/7 incident response, threat hunting and detection tuning.

- **Analyzed, contained and remediated** malware, malicious email campaigns, fraud and abuse, insider threats and data-loss incidents
- **Hunted threats** and researched malware and phishing campaigns, translating findings into concrete mitigations
- Partnered with SIEM and Detection Engineering to tune alerts, reduce noise and improve detection performance

Aug. 2018 - Oct. 2020
2 yrs 3 mos

Banco Santander

Global SOC Security Analyst

bancosantander.es

Worked in Banco Santander's Global SOC, providing 24/7 monitoring and an on-call service to the bank's entities worldwide.

- Performed **in-depth investigation and mitigation** of security incidents
- Monitored web traffic and **critical SWIFT assets**, investigating malware, phishing, DDoS and brute-force activity
- Supported **fraud prevention** across phishing, suspicious email, compromised cards, mule accounts, data leaks and impersonation

Aug. 2017 - Aug. 2018
1 yr 1 mo

Deloitte

CyberSOC Security Analyst

deloitte.com

Worked in Deloitte's CyberSOC, delivering managed security services for national and international clients.

- Conducted **initial triage** of SIEM alerts to identify potential threats
- Applied playbooks and immediate containment or remediation measures when required
- Escalated potential incidents with the context and evidence needed for further investigation

Tools I've built

I also build **open security tools**. I enjoy turning noisy data into practical intelligence with **AI**, cloud services and APIs.

TweetFeed

Open IOC feed

Indicators shared by the security community, collected in one place

TweetFeed collects and organizes **indicators of compromise** posted on X. It focuses on URLs, domains, IP addresses and file hashes, and publishes them as an open feed.

694 stars on GitHub

tweetfeed.live ↗ GitHub ↗

phishunt

Open phishing feed

Suspicious phishing sites, captured and enriched

phishunt identifies and monitors **suspicious phishing sites**. It captures them, enriches them with hosting, certificate and network context, and publishes the results as an open feed.

286 stars on its phishing kits archive

phishunt.io ↗ Kits archive ↗

Research

A few pieces of research published on the Okta Threat Intelligence blog.

Aug. 23, 2026

First on the scene of the (cyber)crime

Okta Threat Intelligence sent its 10,000th suspicious domain notification to a customer. Most of the indicators in those notifications were not flagged by other providers at the time.

May 2, 2026

Tycoon 2FA phishing actors disperse, branch into new attacks

Changes in the Tycoon 2FA phishing operation after law enforcement disrupted it in March 2026.

Dec. 19, 2025

Jobseekers exploited in fake recruiter phishing campaigns

Phishing campaigns that impersonate recruitment sites of well-known companies to steal the credentials of jobseekers.

Sep. 30, 2025

EvilProxy phishing campaign leverages convincing impersonations of enterprise applications

A campaign that uses the EvilProxy phishing-as-a-service toolkit for real-time phishing against users of popular enterprise apps.

Aug. 28, 2025

Attackers target hotelier accounts in malvertising and phishing campaign

A large-scale phishing campaign that impersonates service providers for hotels and vacation rentals.

Jun. 19, 2025

How this ClickFix campaign leads to Redline Stealer

Deceptive CAPTCHA pages that distribute a range of malicious payloads, including Redline Stealer.

Open source contributions

Pull requests I wrote so that TweetFeed and phishunt work inside open source threat intelligence platforms.

7 merged pull requests **4** repositories

MISP

`MISP/MISP`

Added TweetFeed and phishunt to the MISP default feed list.

For #11111 #11150

misp-modules

`MISP/misp-modules`

Added TweetFeed and phishunt lookup modules (expansion and hover).

For #898 #926

YETI

`yeti-platform/yeti`

Added the phishunt feed and moved the TweetFeed feed out of the deprecated feeds.

For #1401 #1366

OpenCTI connectors

`OpenCTI-Platform/connectors`

There is a TweetFeed connector for OpenCTI.

For #7526

Education

2015 - 2019

Universidad de Sevilla

Master's Degree in Telecommunications Engineering

Advanced study of **telecommunications networks and systems**, including network architecture, signal processing, wireless communications and network security.

2011 - 2015

Universidad de Sevilla

Bachelor's Degree in Telecommunications Engineering

Foundations in telecommunications engineering, computer science and **software development**.

Certifications and courses

- GIAC Security Essentials (GSEC) / SANS SEC401 — Badge
- MITRE ATT&CK Defender™ - Cyber Threat Intelligence Certification Training — Badge
- CrowdStrike FHT 201: Intermediate Falcon Platform for Responders
- Splunk 7.x Fundamentals
- Claude Code 101 (Anthropic) — Badge
- Security Engineering on AWS
- AWS Technical Essentials
- Python for Offensive PenTest (Udemy)
- MITRE ATT&CK Defender™ - Fundamentals Badge Training — Badge
- MITRE ATT&CK Defender™ - SOC Assessments Certification Training — Badge
- CrowdStrike FHT 202: Intermediate Falcon Platform for Hunters
- Claude Code in Action (Anthropic) — Badge
- Introduction to agent skills (Anthropic) — Badge
- Architecting on AWS - Accelerator
- Penetration Testing and Ethical Hacking (Cybrary)
- ITIL Foundation — Badge

In the News

TV3 midday news

Telenotícies migdia

Two appearances on the midday news of TV3.

Apr. 12, 2023

Fake SMS from the Spanish Tax Agency during the income tax campaign. I explained that these campaigns are massive, the fake site copies the Agency's website and the stolen data goes to the attacker through Telegram.

Jun. 2, 2023

Fake Booking.com messages that asked travelers for their card details. I explained that attackers who compromise Booking's partners can reach customer data, including card numbers.

Watch from 32:15 ↗ Watch from 27:48 ↗

Se ofrece ciberataque gratis en Telegram: el nuevo anzuelo de los robos 'online'

In an interview, I explained how Telegram phishing services work, with paid anti-blocking extras and ready-made target lists. I linked a Spanish Tax Agency SMS scam to the kit used against delivery firms.

elconfidencial.com ↗

Siguen las campañas de phishing suplantando a la Agencia Tributaria, ahora también por SMS

My tweet is the source for this post, which uses my SMS sample and code screenshot. I also noted that low-skill criminals can easily get the ready-made kits, which use Telegram.

ESET blog ↗

Están suplantando la web de Correos con kits vendidos en Telegram que usan sus bots para recopilar contraseñas. Y hay muchos kits así

The story starts from my tracking of dozens of fake Correos parcel-tracking sites. Their code shows that several share one kit that sends stolen credentials to Telegram bots, and the article uses my screenshots.

genbeta.com ↗

Así pueden estafarte con la declaración de la Renta

This guide to tax-season scams cites my warning about fake tax-refund SMS. It also embeds my tweet on new fake Spanish Tax Agency sites, one of which sends stolen data through Telegram.

elcorreo.com ↗

Telegram abre paso a la venta de kits para suplantar webs como la de Correos a través de bots

Based on my Twitter thread, the article shows how fake Correos sites share one phishing kit. It embeds my tweets and ends with the list of fake domains I collected.

mundodeportivo.com ↗

phishunt.io, cazando phishings

This post presents phishunt.io, the site I built to find and monitor suspected phishing websites, and its three sections: suspicious sites, new domain registrations and phishing kits.

derechodelared.com ↗

Suplantan la identidad de tenistas como Rafa Nadal para incentivar la descarga de vídeos con malware

On Twitter, I reported that scammers used the live chats of Wimbledon interview videos on YouTube to spread malware and crypto-scam links. The article cites and embeds my tweet.

20minutos.es ↗

El ciberataque vía Youtube que ha suplantado a Nadal o a Djokovic durante Wimbledon

I uncovered this campaign on Jul. 9, 2022, and the article embeds my two tweets about it. Another researcher replied to my finding and linked the malware to Raccoon Stealer v2.

escudodigital.com ↗

Continúan los SMS con falsos envíos de FedEx: cómo identificarlos y eliminar esta amenaza

As the person behind phishunt.io, I am cited for showing how criminals kept adding hacked websites to host a fake FedEx app. The app was an Android banking trojan spread through SMS links.

ESET blog ↗

Los timos con criptomonedas que usan imágenes de famosos continúan muy activos

The post follows a crypto scam from a spam email to a fake investment platform. It names me among the researchers who had warned for weeks about fake celebrity arrest ads, and links my tweet.

ESET blog ↗

Aplicación maliciosa para Android se hace pasar por una versión de la cartera de criptomonedas MetaMask

From Apr. 9, 2023, I tracked fake versions of the MetaMask app for Android, and the post links my tweet. My details show that the criminals copied the official website almost exactly.

ESET blog ↗

FedexBanker: El nuevo troyano bancario para Android que utiliza tus paquetes para robarte las credenciales

According to the post, I was the first to warn on Twitter about this SMS campaign, which sent users to a fake FedEx site. It embeds my tweet of Feb. 11, 2021.

hispasec.com ↗

How does a modded crypto wallet steal credentials of an user?

The author reverse-engineers a fake Android MetaMask app that sends the wallet recovery phrase to the attackers. The post says I first identified the app, and links my tweet.

@themalwarebug - medium.com ↗

Best Cyber Threat Intelligence Feeds

TweetFeed, my open feed, is one of the open-source threat feeds benchmarked in this post. Both TweetFeed lists were first to report over 90% of their indicators, and only about a quarter overlapped with other feeds.

silentpush.com ↗

A little more about me

- Enneagram Type 5
- Member of the Curated Intelligence Trust Group
- Enjoy lifting weights and riding my bike to avoid burnout