■ PROJECT SHADOWSCALES ■

11-Year Investigation Timeline: 2015-2026

11 YEARS	2,900+ EXHIBITS	47+ PARTICIPANTS	5 ATTACK PHASES

JULY - SEPTEMBER 2015

Campaign Initiation

Doxing and character assassination begins. Targeted dissemination of false information across multiple platforms.

■ *Investigation Start Point*

DECEMBER 2015

Business Interruptions Begin

Systematic interference with professional activities. Economic warfare tactics targeting income streams.

■ *Escalation Phase 1 • Economic targeting*

OCTOBER 2017

Death Threats Begin

Coordinated death threats documented. Escalation from harassment to direct threats of violence.

■ *Legal Context: 4 months after defamation filing*

MARCH 2018

Coordinated Cyberstalking Begins

Multi-vector cyber operations initiated. Technical sophistication indicates professional-grade tools.

■ *Legal Context: Hearing on death threats upcoming*

APRIL 2019

Kinetic Stalking First Noted

Physical surveillance documented. Coordination between cyber and physical operations.

■ *Critical Breach: Bank breach through Graduate Spa vector*

2021

Katie Baby Pictures Steganography

68KB encrypted data hidden in photos. Military-grade encryption (entropy 7.9/8.0). Chi-square proof.

■ *Technical Evidence: FBI CRRU submission recommended*

MARCH 2021

First Exchange-Box Access (Location 1)

Infrastructure-level access at telecommunications exchange box. Carrier-level compromise documented.

■ *Network infrastructure targeting*

DECEMBER 2021

Second Exchange-Box Access (Location 1)

Return to same infrastructure. Persistent compromise pattern established.

■ *Concurrent: Significant bank breach*

DECEMBER 27, 2021

Coordinated Email Server Attack

8 malicious IPs. Pavel K. identified. "Investigator pretext" signature documented.

■ *Legal Context: Davis pushing for trial date*

JANUARY 4 & 22, 2022

Continued Server Breach Activity

Sustained unauthorized access. Pattern matches December 2021 attack vectors.

■ *Persistent targeting*

FEBRUARY 2022

Third Exchange-Box Access (Location 1)

Third documented infrastructure access. Evidence submitted to federal authorities.

■ *Legal Context: Filed for dismissal (court date November)*

OCTOBER 2022

First Exchange-Box Access (Location 2)

Expansion to second geographic location. Multi-site surveillance network confirmed.

■ *Professional-grade operations*

DECEMBER 2024

Thorndal + Ichter-Davis Phishing

SharePoint zero-day. init_1_.js malware attributed to Kathy Scott DoxingTwitter.com.

■ *Legal Context: Just after Davis filed in Oglethorpe (Oct 1, 2024)*

JANUARY 2025

Second Exchange-Box Access (Location 2)

Return to second location. Confirms sustained multi-site capability over 3 years.

■ *Decade-long persistence proven*

PATTERN ANALYSIS

Every major escalation correlates with legal proceedings. Attack sophistic
Infrastructure access demonstrates carrier-level compromise. Multi-year pers
surveillance-as-a-service platform targeting litigation opp