



Client Outcome

3 Hours to Attribution

How Nisos expediently unmasked an adversary that was leaking a Client's trade secrets on social media

At 5:00pm, a Nisos Adversary Insights RetainerSM Client requested attribution of a Twitter handle after public comments posted leaked sensitive trade secrets. The unidentified individual claimed to have “anonymous sources inside of the Client's factory with inside access to sensitive trade secrets.”

At 5:15, queries were sent to internal Nisos Intelligence Databases (NID) to identify results related to a Twitter handle within breach data, PII, password resets, and dark web data sources. **By 5:20,** automated keyword searches revealed usable clues to unmask the unidentified individual.

Attribution Clues Gathered:



Leaker reveals they acquired the information from a source during a conversation at redacted fast food restaurant on date



Posts using same handle on a different online forum



Male located in redacted city



Ancestors were French who settled in redacted and belonged to redacted political party



Approximate age: 40



Oldest son was in 7th grade in 1991, giving approximate birth year



Married for over 20 years



Father had 4 sisters and 1 brother



Retired from Federal Government



Provides care for wife with redacted health condition



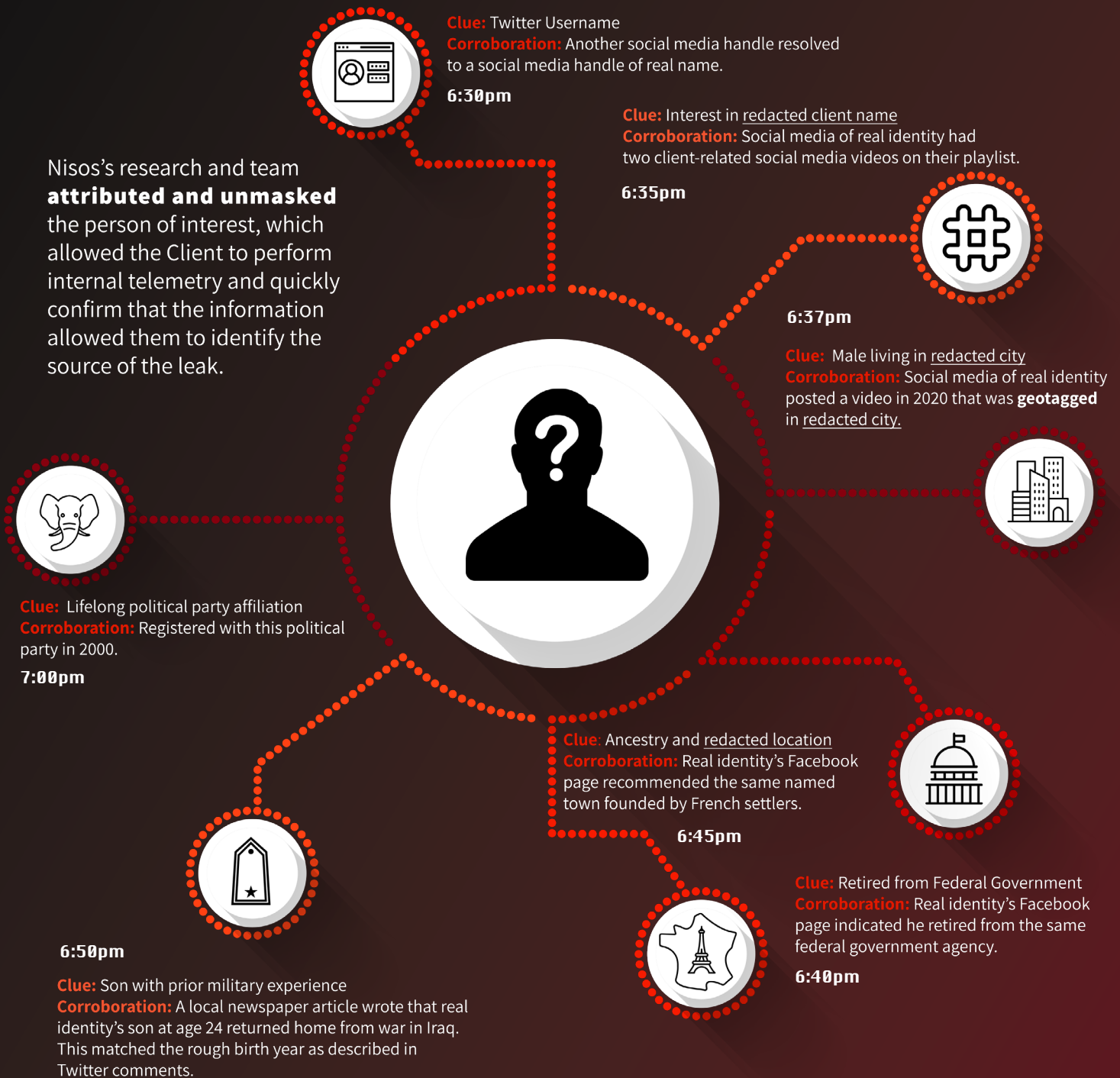
Son worked at redacted Client company and has prior military experience

At 6:00, manual analysis returned additional clues which were investigated using subscription PII databases and a variety of technical tools. Research and analysis from six different Nisos analysts confirmed the real identity of the Twitter handle.

- The last 2 digits of the Twitter handle's phone number
- An additional social media account with the same handle using the real name of the person of interest

From 6:30-7:00, extensive research corroborated information on the real identity of the man.

CLIENT OUTCOME: 3 HOURS TO ATTRIBUTION



By 7:20, exclusive mobile data available to Nisos confirms the person of interest was located at redacted fast food restaurant on the day of the tweet. **At 7:25**, reporting and delivery starts. Within an hour, Nisos executives review team's report for the Client.

At 8:30, just 3 hours after research began, Nisos provides a probable attribution report to the Client who performs internal telemetry analysis, confirms information provided, and identifies the source of the leak.

Learn more about Nisos - The Managed IntelligenceSM company by visiting www.nisos.com.

If you need immediate help, contact us: info@nisos.com or 703-382-8400.