Threat Report Preview

2025 Tax-Themed Threats: New Insights You Can't Miss

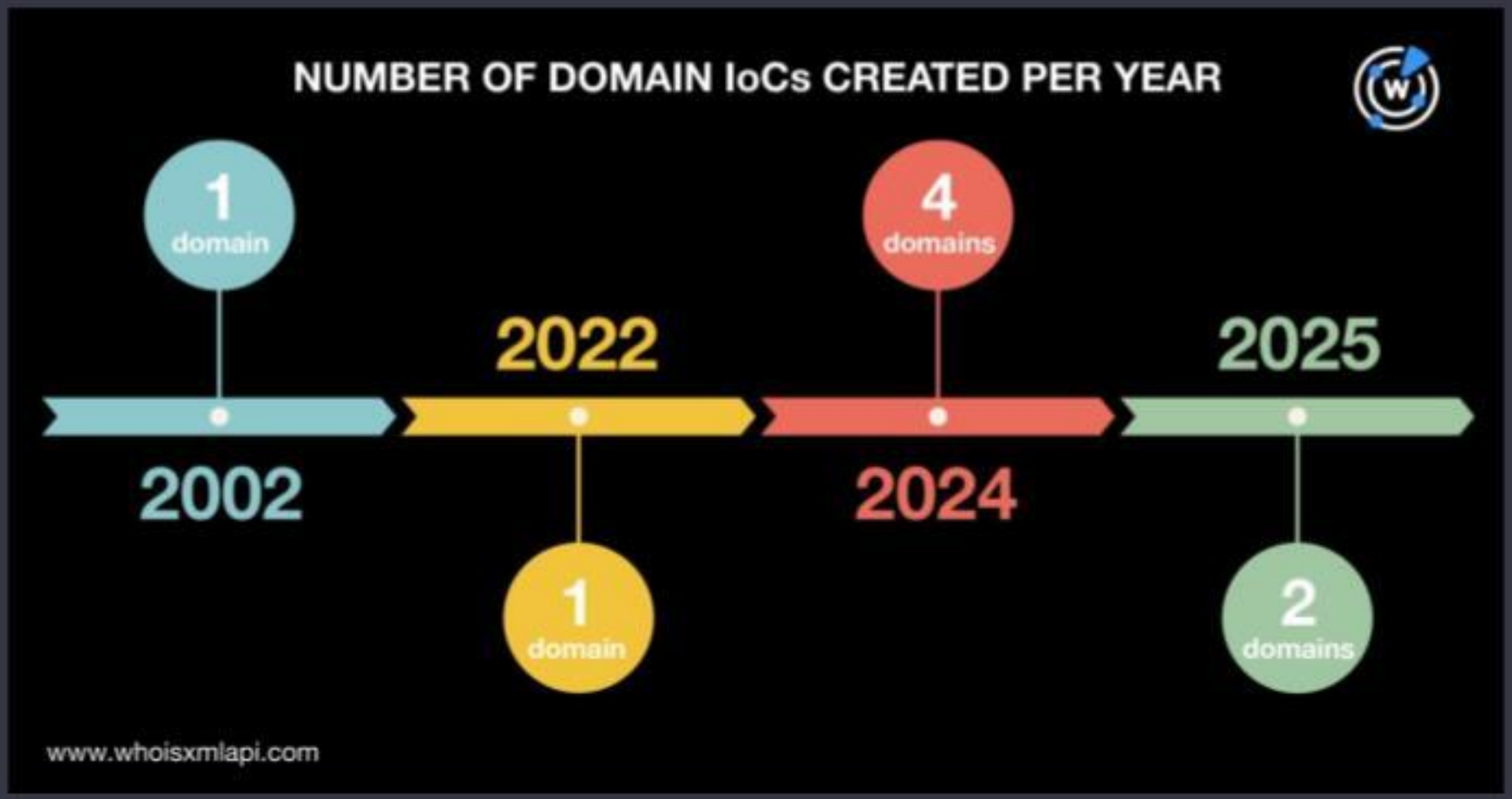
SWIPE

WhoisXMLAPI

whoisxmlapi.com

What Do We Know So Far?

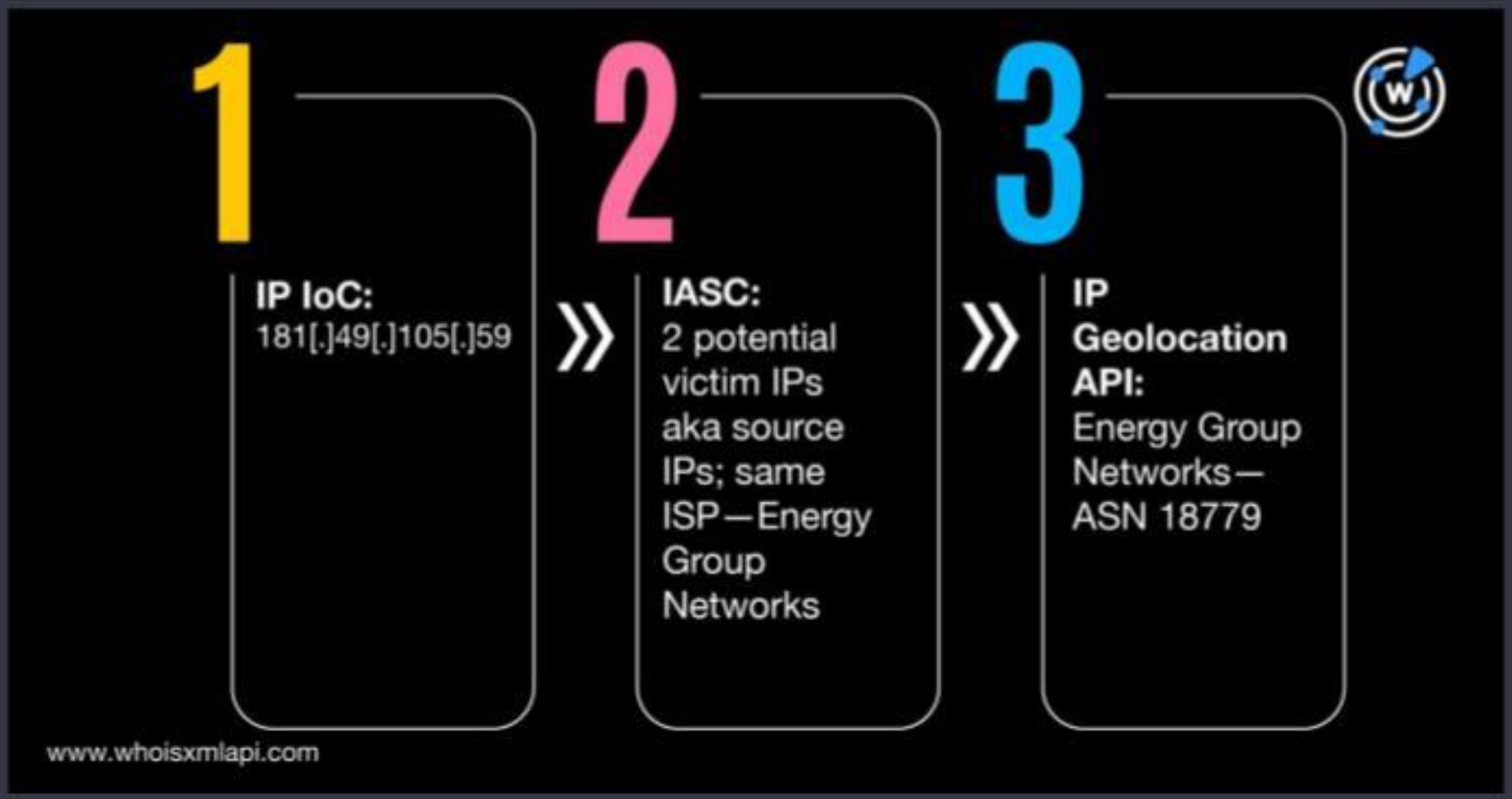
Microsoft identified 11 domains as IoCs in “Threat Actors Leverage Tax Season to Deploy Tax-Themed Phishing Campaigns.” Eight had current WHOIS records and were created between 2002 and 2025.



What about the sole IP address tagged as IoC?

What Do We Know about the IP IoC?

Using sample netflow data from the Internet Abuse Signal Collective (IASC), we further analyzed 181[.]49[.]105[.]59, a C&C IP address. Threat actors used it to send commands and retrieve stolen screenshots.



Can DNS intelligence give us more artifacts?

Exploring the High-Risk Connected IPs

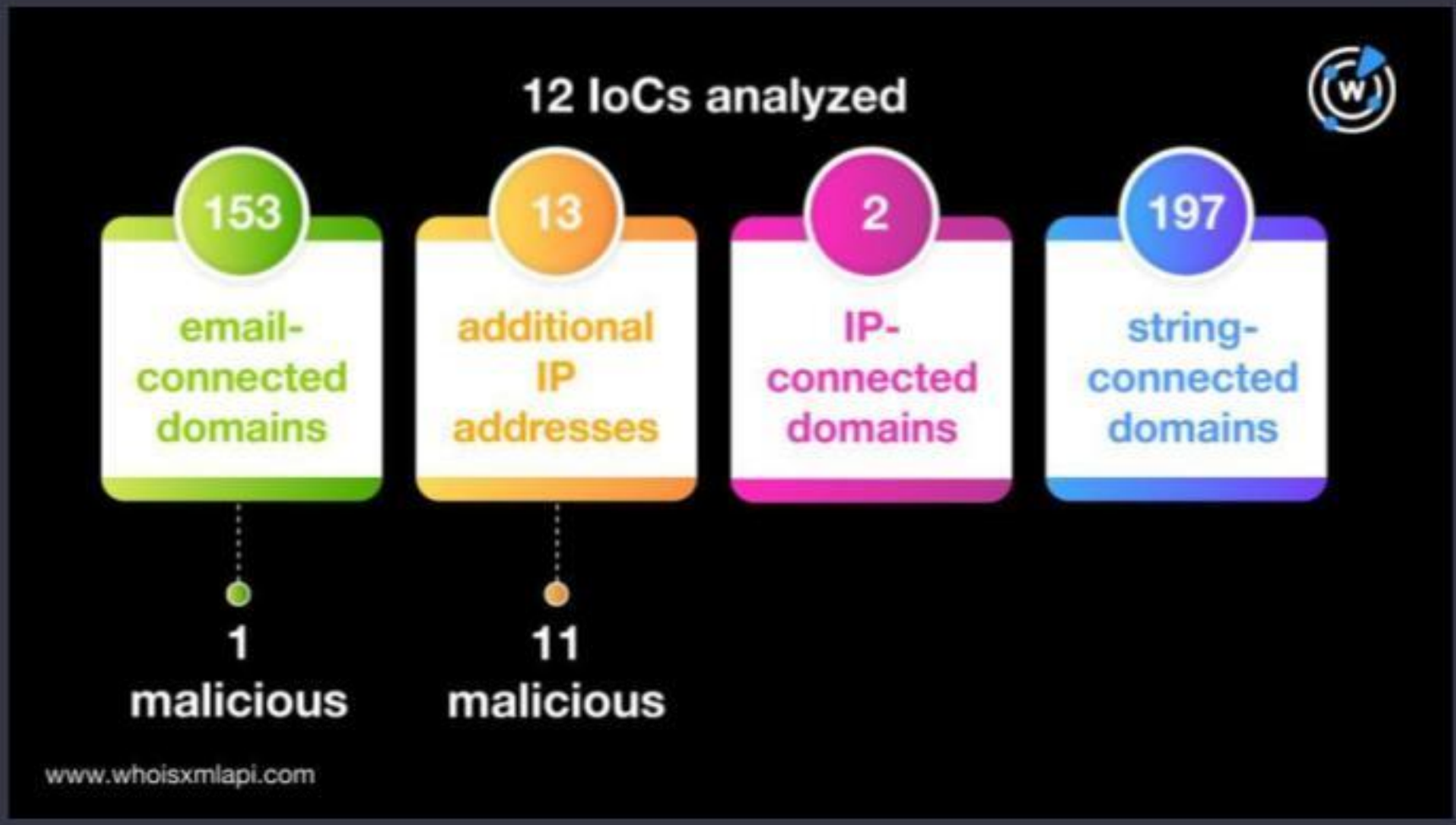
Six of the 11 domains identified as IoCs resolved to 13 additional IP addresses, 11 of which turned out to be malicious.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]16[.]1	Attack C&C Generic threat Malware distribution Phishing Spamming Suspicious activity
87[.]251[.]67[.]203	C&C
94[.]232[.]40[.]48	C&C

How many artifacts did we find in all?

Summing Up Our Expansion Analysis

Through various expansion and pivoting techniques applied to our diverse intelligence sources, we identified hundreds of connected artifacts that may require the attention of security teams.



We uncovered a total of 360+ connected artifacts.

Want to dive deeper into the 2025 tax-themed threats?

Download our full report for our in-depth analysis or talk to us about this research.

www.whoisxmlapi.com


WHOIS Database Download


DNS Database Download


Subdomains Database Download

WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence