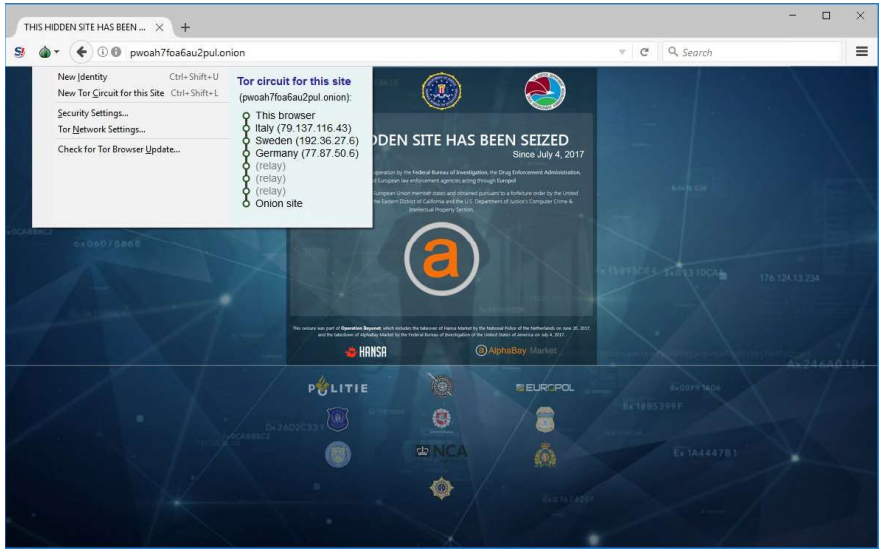
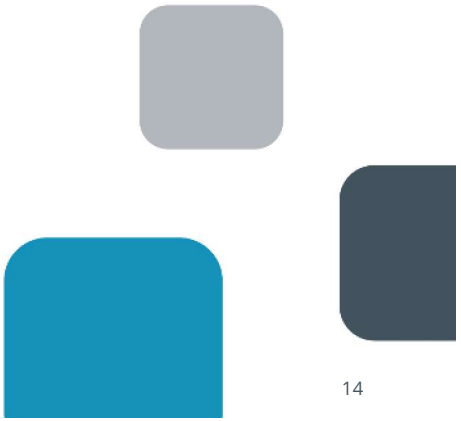
Threat Research Sources



- Counterintelligence
- Tactics, techniques, and procedures (TTPs)
- Threat research sources
  - Academic research
  - Analysis of attacks on customer systems
  - Honeypots/honeynets
  - Dark nets and the dark web

Threat Intelligence Providers

- Narrative analysis and commentary
- Reputation/threat data feeds—cyber threat intelligence (CTI)
- Platforms and feeds
  - Closed/proprietary
  - Vendor websites
  - Public/private information sharing centers
  - Open source intelligence (OSINT) threat data sources
- OSINT as reconnaissance and monitoring

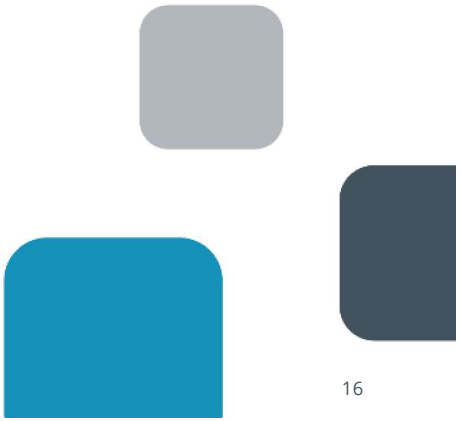


Other Threat Intelligence Research Sources

- Academic journals
- Conferences
- Request for Comments (RFC)
- Social media

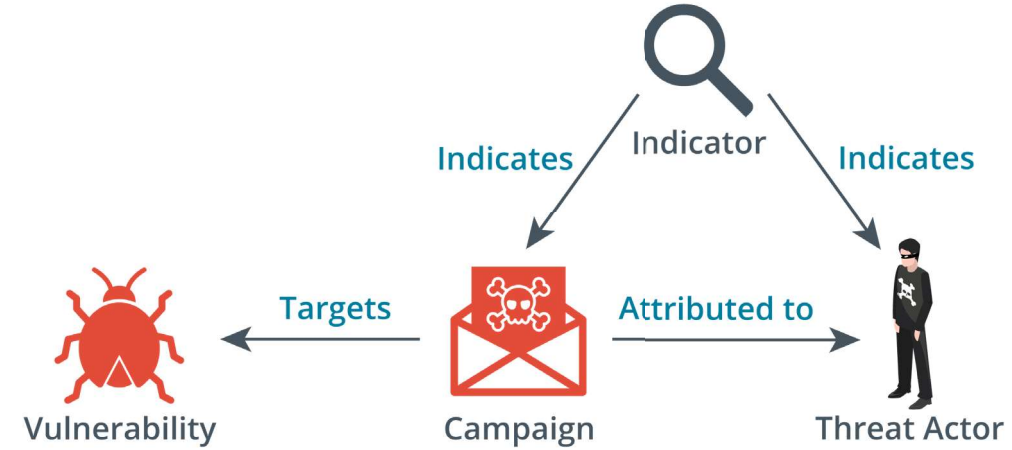
Tactics, Techniques, and Procedures and Indicators of Compromise

- Tactics, Techniques, and Procedures (TTPs)
  - Generalized statement of adversary behavior
  - Campaign strategy and approach (tactics)
  - Generalized attack vectors (techniques)
  - Specific intrusion tools and methods (procedures)
- Indicator of compromise (IoC)
  - Specific evidence of intrusion
  - Individual data points
  - Correlation of system and threat data
  - AI-backed analysis
  - Indicator of attack (IoA)



Threat Data Feeds

- Structured Threat Information exchange (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- Automated Indicator Sharing (AIS)
- Threat maps
- File/code repositories
- Vulnerability databases and feeds



Icon images © Copyright 2016 Bret Jordan. Licensed under the Creative Commons Attribution-ShareAlike (CC BY-SA) License, Version 4.0. (freetaxii.github.io/stix2-icons.html.)

Artificial Intelligence and Predictive Analysis

- Correlation between security intelligence/event monitoring and threat data
- Artificial intelligence (AI) and machine learning (ML)
  - Expert systems
  - Artificial neural networks (ANN)
    - Inputs, outputs, and feedback
    - Objectives and error states
- Predictive analysis
  - Threat forecasting
  - Monitor “chatter”