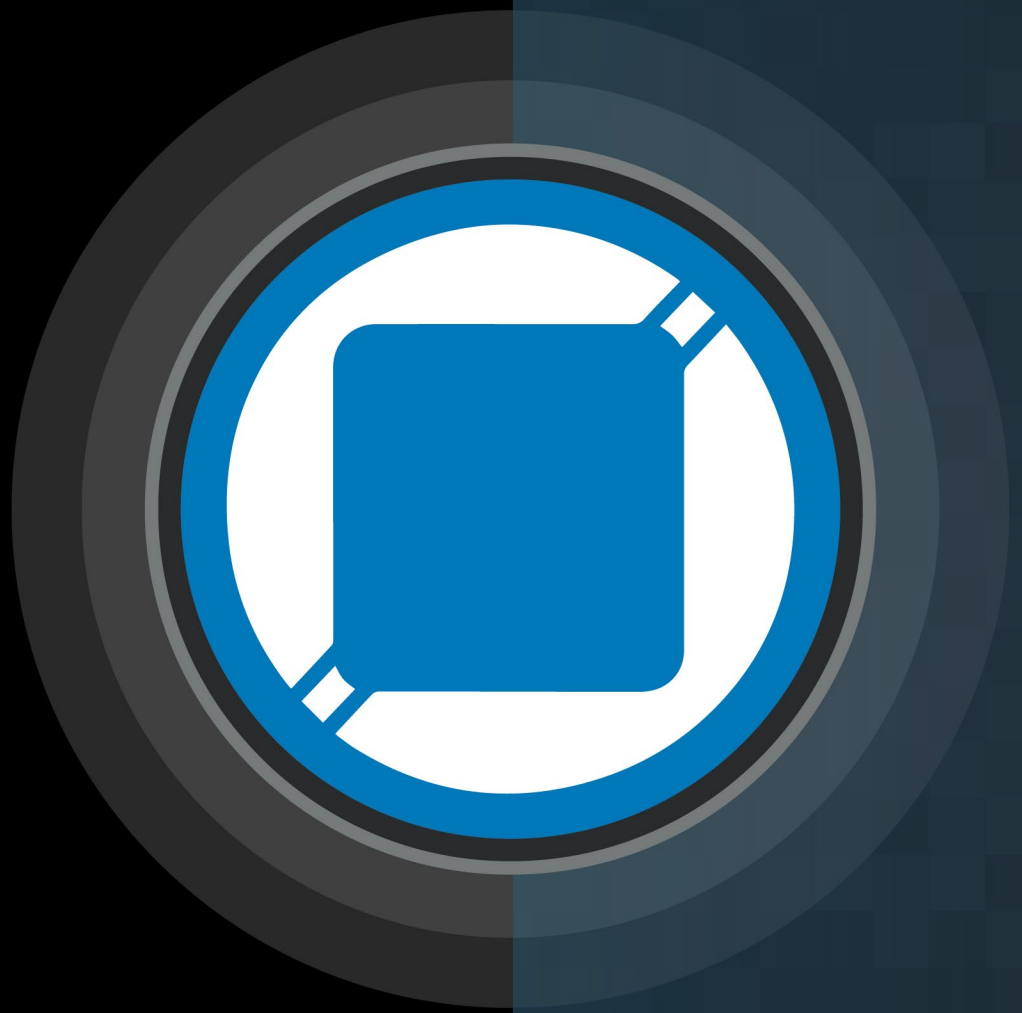


A Glimpse of the Future: Cyber Insecurity and Modern Conflict.

Martin LEE, Cisco Talos.

cisco | Talos

Active in Ukraine since 2016

Partnering with

- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

Assisting with

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

Current Ukraine Cyber Assistance

Free offer of Cisco Security products in Ukraine.

Dedicated threat hunting task unit.

660 people contributing to threat detection.

"Our teams of threat hunters have been around-the-clock hunting in the data since the invasion. They're stopping attacks from happening."

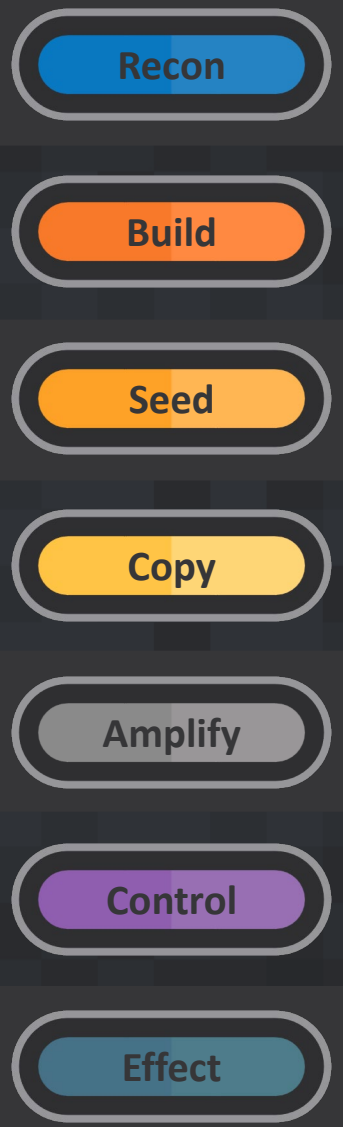
cisco | Talos

Future Conflict is…

Hybrid Threats

- Conflict in multiple domains
  - Disinformation & propaganda
  - Cyber disruption
- Cycle of abuse
  - Denial
  - Minimise
  - Blame victim

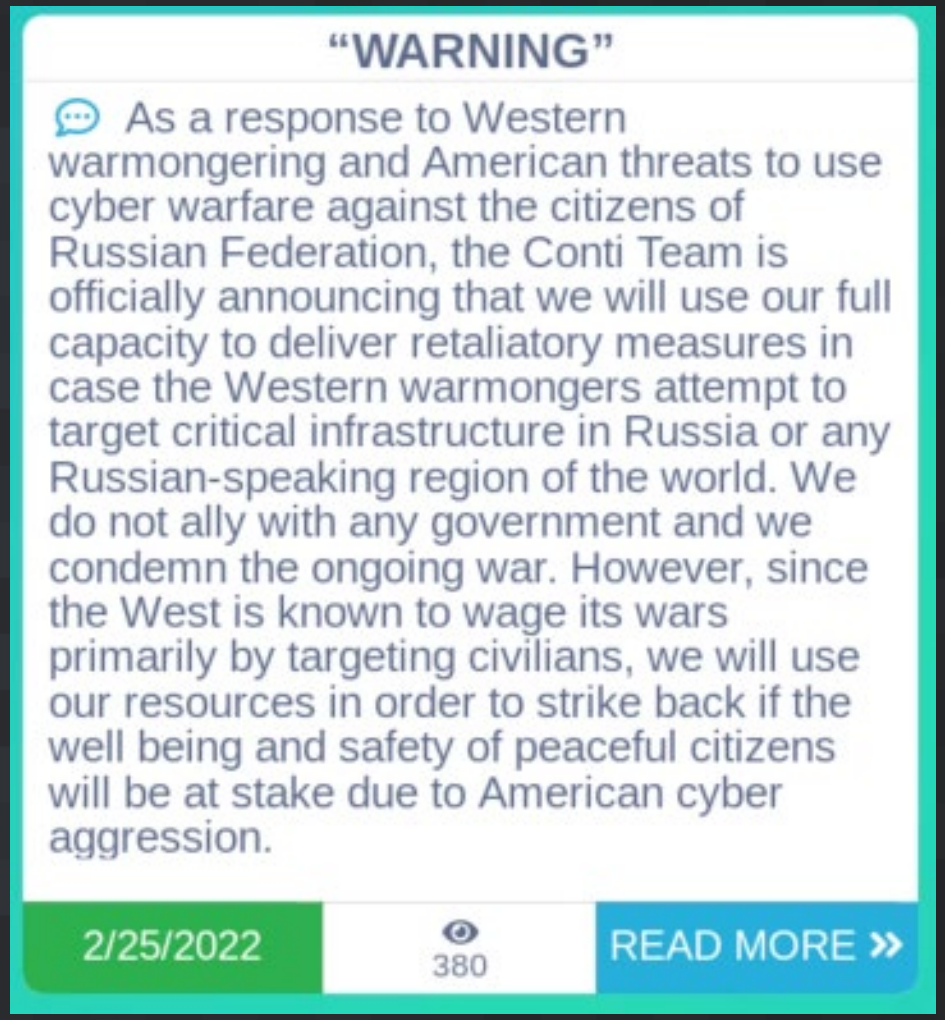
Disinformation Kill Chain



cisco | Talos

Proxy Agents

- Non-state actors
  - Act under state direction
  - Augment capability
- Provide
  - Plausible deniability
  - Action at arms length
  - Smoke screen for state actors



Hacktivist Actors

Crowd sourcing offensive cyber capability

Susceptible to shifting narratives

Who chooses targets?

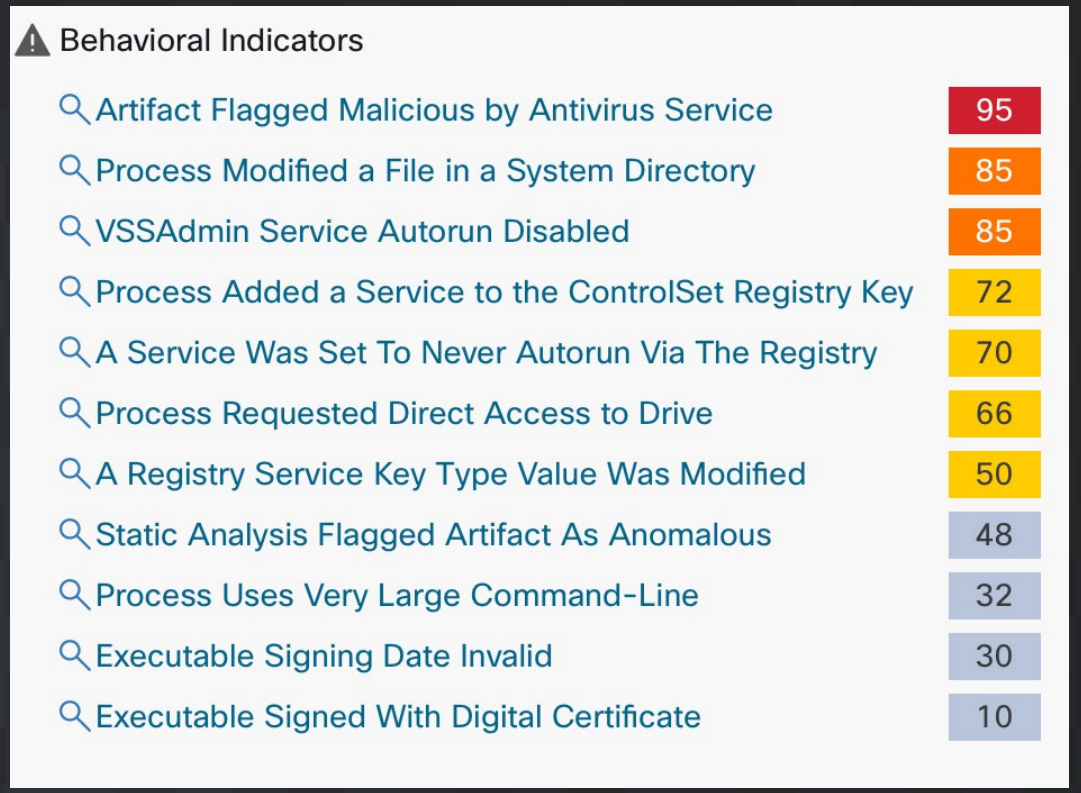
Varying levels of skill & engagement

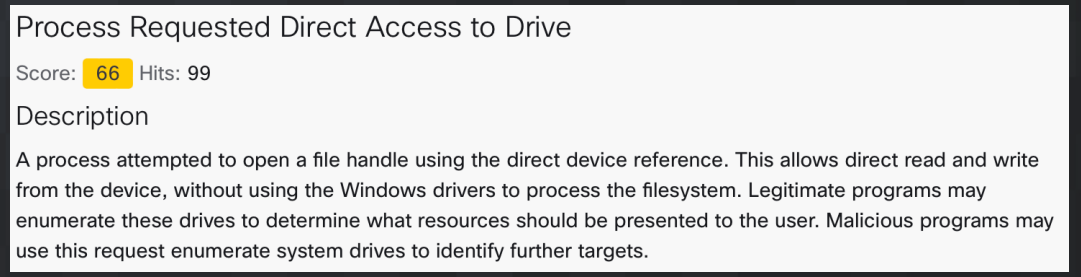
Post-conflict deradicalization

cisco | Talos

Disruptive Cyber Attacks

- Wiper malware
  - Malicious software written to destroy systems and data
- Denial of service attacks
  - Prevent access to services
- Disruption of society
- Reduces ability to respond
- Promote disinformation

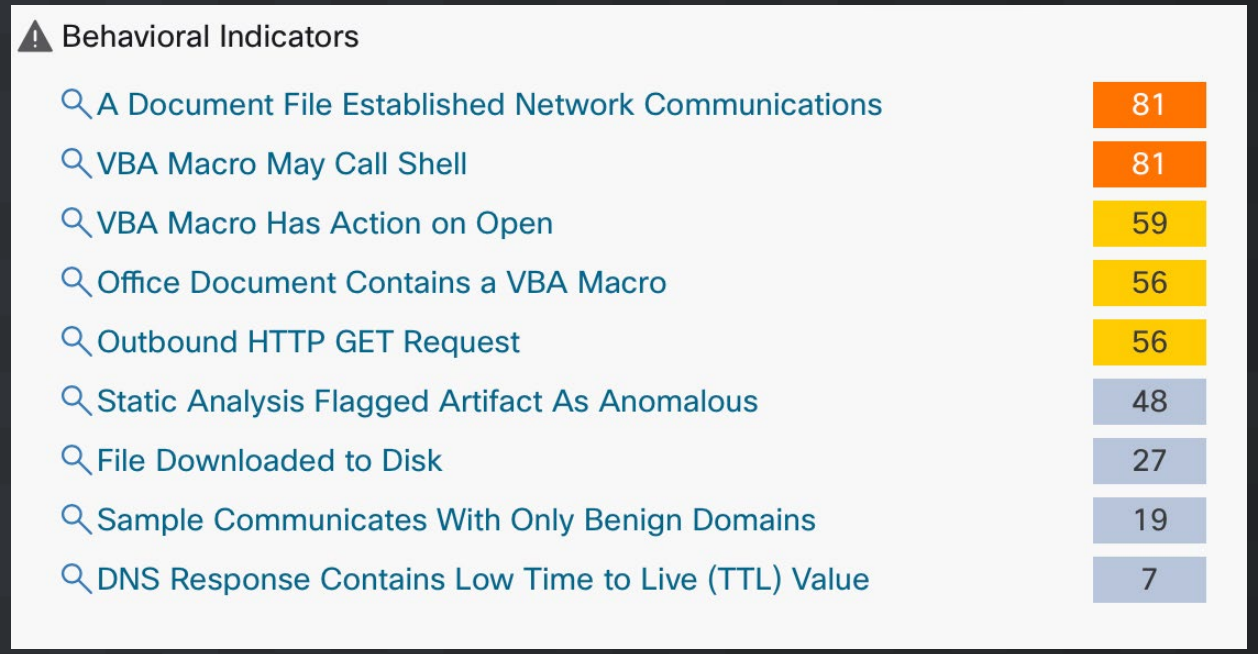




cisco | TALOS

Information Stealers

- Malicious software
  - Conduct espionage
  - Steal credentials
  - Profile targets
  - Social engineering
  - Disinformation



Infrastructure as a Target

Disrupt critical national infrastructure

Disrupt communications

April 12, 2022
3:32 PM GMT+1
Last Updated a month ago

Europe

Ukraine says it thwarted Russian cyberattack on electricity grid

By James Pearson

2 minute read

Building Resilient Societies

Prepare

Awareness

- Threat actors will target you
  (even if you think that you are insignificant)
- Disinformation campaigns
- Denial of service attacks
- Defacement of website
- Wiper malware
- Supply chain attacks

Media Literacy

- Identify disinformation

cisco | TALOS

Prepare

Prevention

- Identify & manage risks
- Aggressively harden systems

Detection

- Protection everywhere
- Visibility & vigilance
- Proactive threat hunting

Response

- Plan in advance
- Redundant systems & fail over
- Test & rehearse

cisco | TALOS

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

cisco | Talos

Thank you!

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity


CISCO
TALOS
TALOSINTELLIGENCE.COM