CYBER THREAT INTELLIGENCE

2019-02-04

Siri Bromander
mnemonic & UiO

mnemonic

A STEP BACK

Digital Fortress

«Defender's Dilemma»

«The defenders trying to secure our computer networks have to close off every possible vulnerability. They have to get everything right, every time. The attackers just have to find one mistake.»

http://www.abc.net.au/radionational/programs/futuretense/what-makes-hacking-so-easy-and-security-so-hard/6990902

Digital Resilience

SO WHAT IS THREAT INTELLIGENCE?

Threat Intelligence – Definition

Threat intelligence is ***evidence-based knowledge***, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging ***menace or hazard*** to assets that can be used to ***inform decisions*** regarding the subject's response to that menace or hazard.

- Gartner (2013)

Example: WannaCry

www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

THE ORIGINS OF THREAT INTELLIGENCE

The Morris Worm (1988)

From: rsk@mace.cc.purdue.edu (Rich Kulawiec)
To: phage
Date: Fri 14:32:27 04/11/1988 EST
Subject: Steps in the virus, as best we know them (and fixes)

I don't claim that all of this is definitive, or accurate; it's the best I know right now after working on this for quite a while. Please don't flame me if I'm wrong about something; I'm simply trying to help.

1. Virus arrives via shell script using sendmail. Uses debug mode of sendmail to extract itself into temporary file in /usr/tmp, named something like x1234567,l1.c. This temporary file is a small C program, sort of like a second-stage bootstrap.

(Telltale sign is a line like this:
sed "1,/^$/d" | sh
in your sendmail log, on a message originating from /dev/null.)

Fix: disable "debug" mode of sendmail This was sent out by Keith Bostic of Berkeley yesterday.

2. The second stage boot compiles small (40 line) C driver and executes it with arguments giving the Internet originating point of the virus. This then sucks over the x1234567,vax.o and x1234567,sun3.o files. It compiles them into the file /usr/tmp/sh.

(Telltale sign: files with names like those given above in /usr/tmp.)

Fix: Create /usr/tmp/sh as a directory. This works because the script that creates /usr/tmp/sh from one of the .o files checks to see if /usr/tmp/sh exists, but not to see if it's a directory. Locally, we call this fix "the condom".

http://securitydigest.org/phage/archive/035

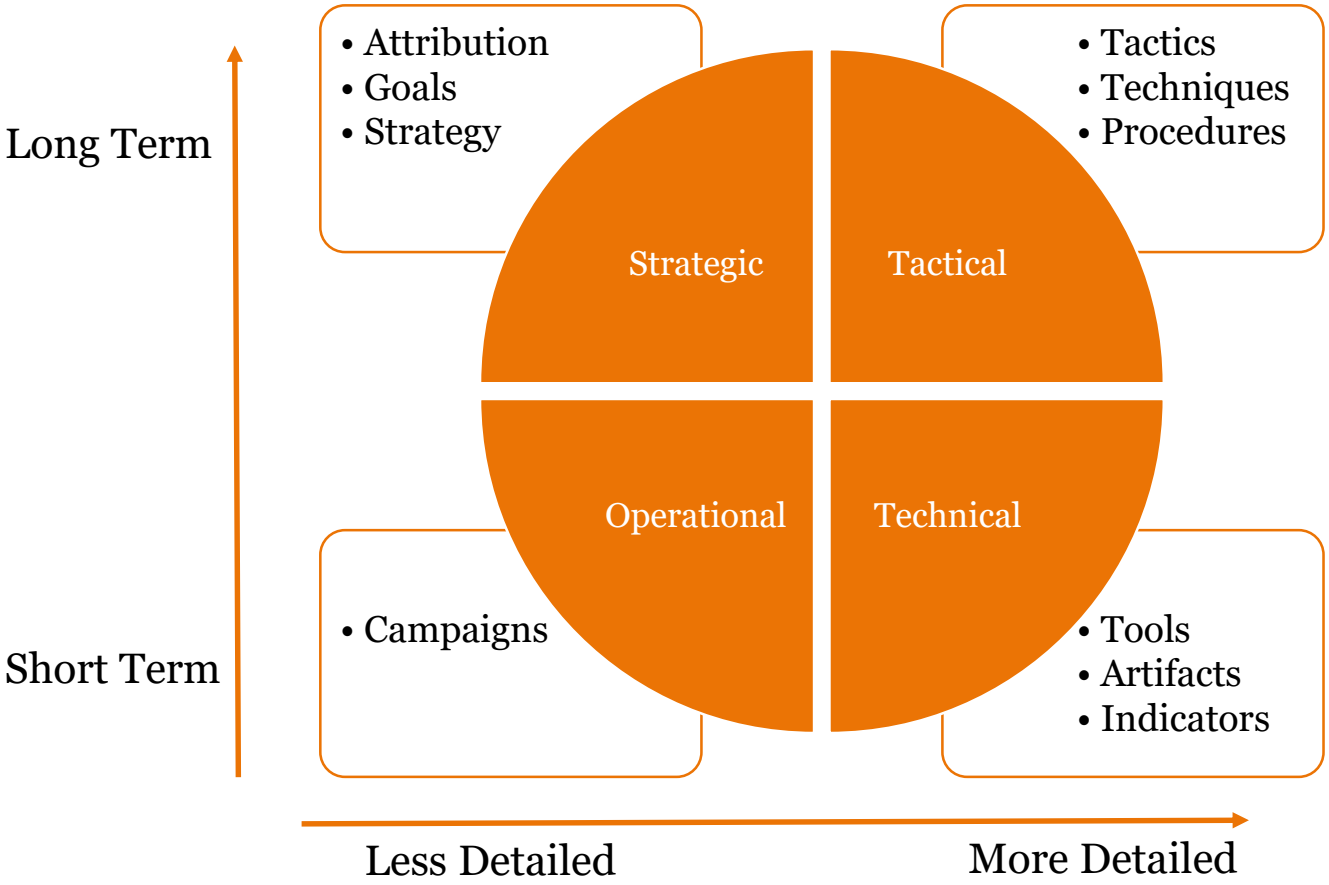
What is different today?

- Vocabularies
- Models
- Processes
- Tools
- Standards

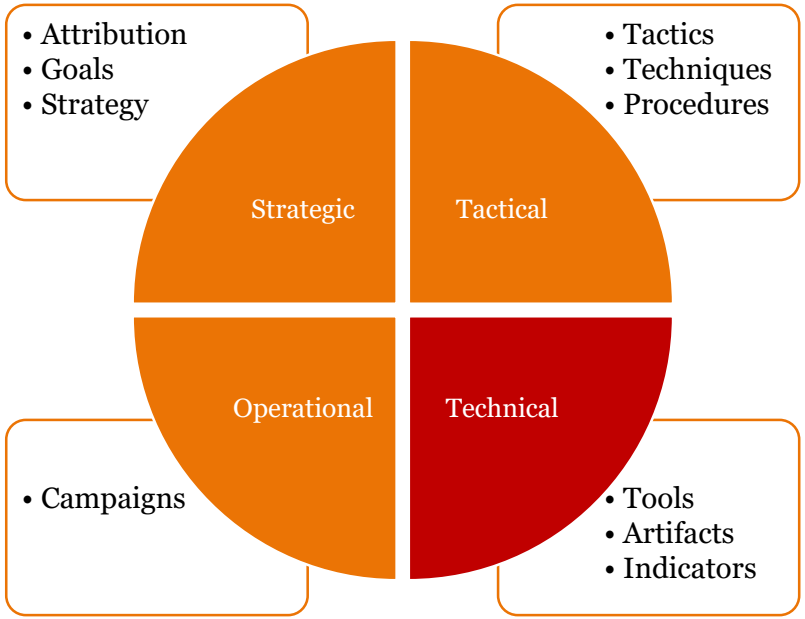
ANALOGY AND MODELS

Threat Intelligence – an Analogy

Threat Intelligence Categories



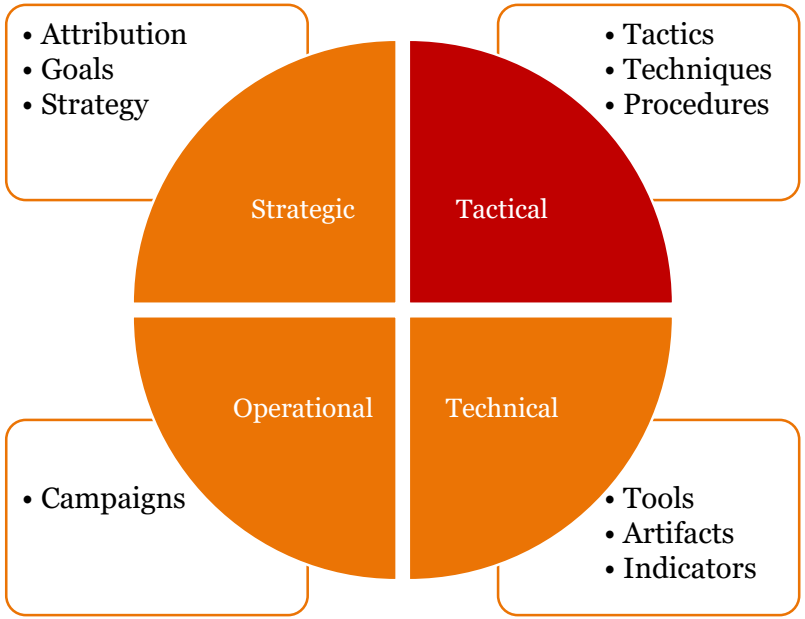
Technical Threat Intelligence



By Olavsplates (Own work) [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

www.example.com

Tactical Threat Intelligence

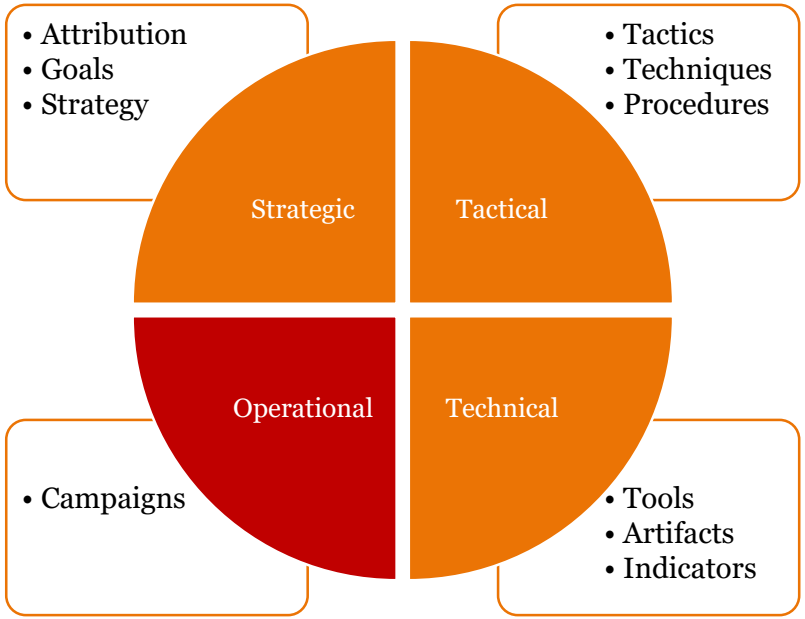


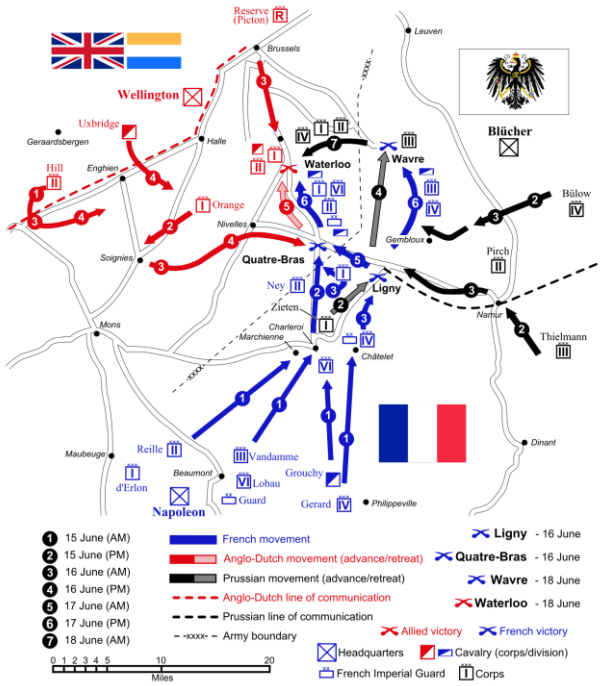
By High Contrast (Self-photographed) [CC BY 3.0 de (http://creativecommons.org/licenses/by/3.0/de/deed.en)], via Wikimedia Commons

Environment: Windows cmd.exe command line

1. ping -n 1 HOSTNAME
2. net use \\HOSTNAME\c$ "PASSWORD" /user:"DOMAIN\USERNAME"

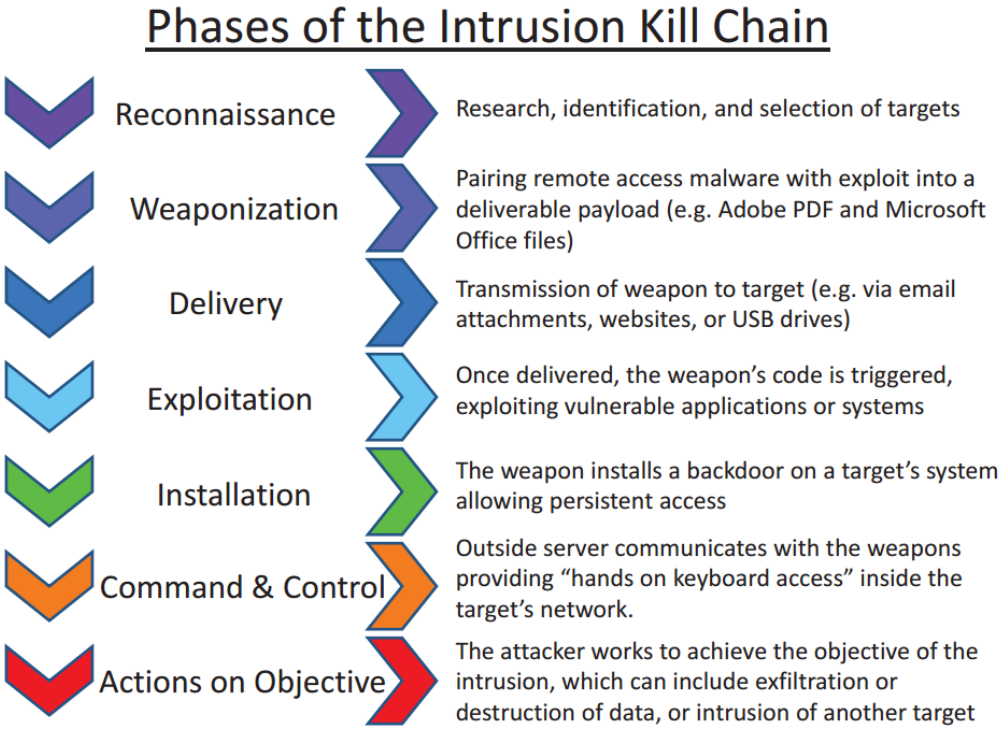
Operational Threat Intelligence





Strategic Threat Intelligence

Cyber Kill Chain



http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

CURRENT CHALLENGES AND RESEARCH

Some Research Challenges

- Analytics
- Enrichment Techniques
- Formal Representations of Tactics, Techniques and Procedures
- Natural Language Processing
- Taxonomies and Ontologies

Research Projects

- Semi-Automated Cyber Threat Intelligence (ACT)
  - Open Source Threat Intelligence Platform
  - https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
  - https://github.com/mnemonic-no/act-platform

- Threat Ontologies for CyberSecurity Analytics (TOCSA)
  - Ontologies
  - Siri Bromander's PhD Project
  - https://www.mnemonic.no/no/research-and-development/threat-ontologies-for-cybersecurity-analytics/
  - http://www.mn.uio.no/ifi/english/research/projects/tocsa/

- Operable Subjective Logic Analysis Technology for Intelligence in Cybersecurity (Oslo Analytics)
  - Project Lead: Professor Audun Jøsang, UiO
  - Analytics
  - Subjective Logic (Quantifying Uncertainty)
  - Trust Networks
  - http://www.mn.uio.no/ifi/english/research/projects/oslo-analytics/

Questions?