ATT&CK Sightings

John Wunder
@jwunder

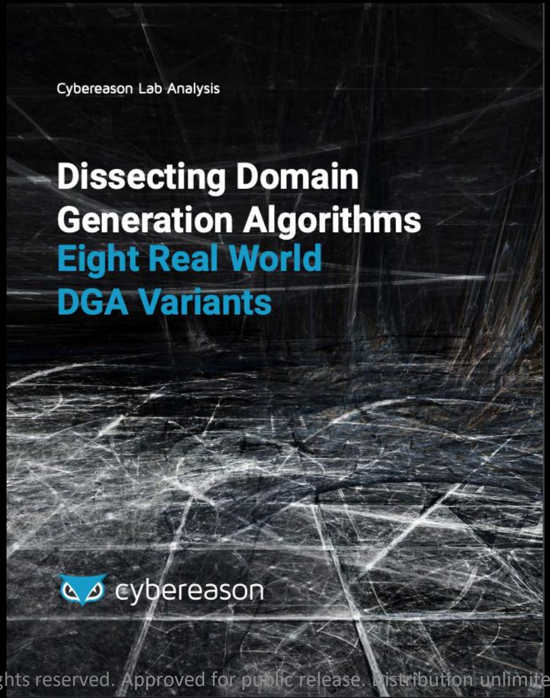
@MITREattack

#ATTACKcon

Threat intelligence reports are great!

They tell you about…

New, interesting techniques.


Cybereason Lab Analysis

Dissecting Domain Generation Algorithms Eight Real World DGA Variants

http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf

New tools.

ADWIND — A CROSS-PLATFORM RAT

REPORT ON THE INVESTIGATION INTO THE MALWARE-AS-A-SERVICE PLATFORM AND ITS TARGETED ATTACKS

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf

What a threat group is up to.

FIN7 Evolution and the Phishing LNK

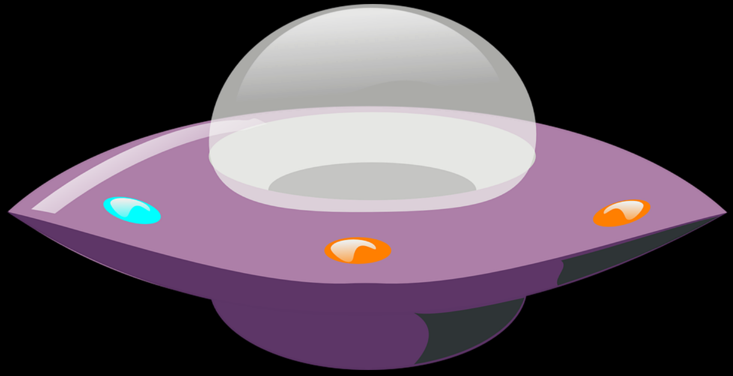
April 24, 2017 | by Nick Carr, Saravanan Mohankumar, Yogesh Londhe, Barry Vengerik, Dominik Weber

https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

But they don’t answer all of our questions

- Which techniques are more or less common?
- How do techniques tend to be used together (or not)?
- How has usage changed over time?
- Does prevalence differ by sector or geographic area?

https://pixabay.com/vectors/spaceship-ufo-cartoon-retro-art-304073/



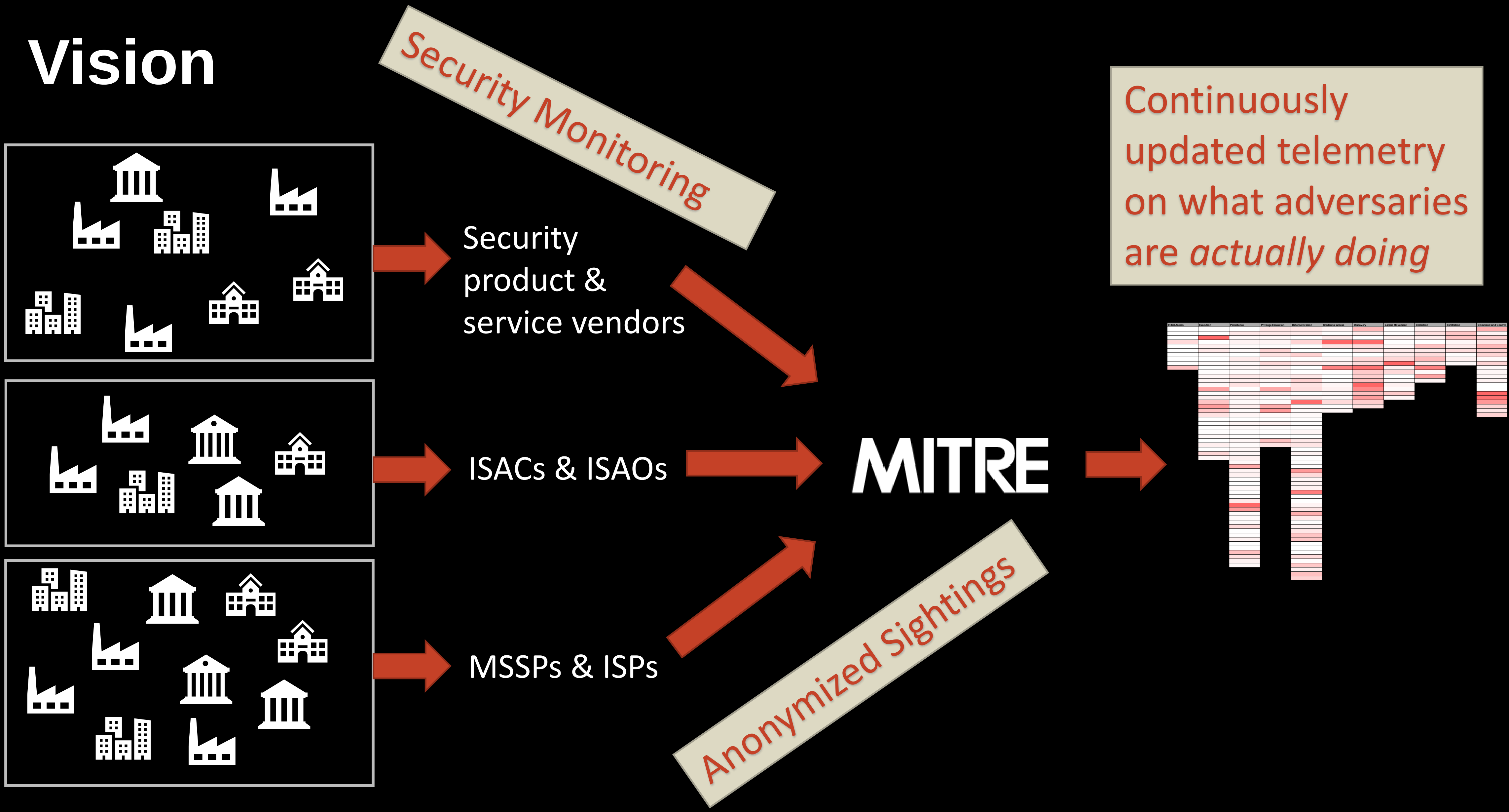
ATT&CK Sightings

ATT&CK Sighting*: Observation that provides evidence an ATT&CK technique is in use.*

- **Three types of sightings:**
  - **Direct Technique Sighting**
  - **Direct Software Sighting**
  - **Indirect Software Sighting**

- **Proposed Operating Model**
  - MITRE collects sightings from multiple organizations
  - Sightings are anonymized and aggregated
  - MITRE publishes insights and (potentially) data sets

Vision



Security Monitoring

Security product & service vendors

ISACs & ISAOs

MSSPs & ISPs

MITRE

Anonymized Sightings

Continuously updated telemetry on what adversaries are *actually doing*

Contributors

- Are able to easily and safely contribute.
- Are protected from disclosing too much information.
- Are acknowledged for providing data of value.

Defenders

- Can prioritize actions.
- Can understand and communicate the value of their work.
- Can see where they need to adapt based on changing tides.

Researchers

- Develop defensive approaches based on technique interdependencies.
- Develop an understanding of how usage differs by sector, actor type, or geography.
- Develop things we can’t even think of.

How to contribute

1. Email us at attack@mitre.org.

2. Generate data.

Directly

Data format is published at our sightings page. Generate JSON that conforms.

Via MISP

MISP developed a plugin to generate our sightings format via the API.

Other

Want to contribute via STIX? CSV? Morse Code?

3. Send us data.

Related Work

Red Canary Threat Detection Report

https://redcanary.com/resources/guides/threat-detection-report/

FIRST EDITION | 2019

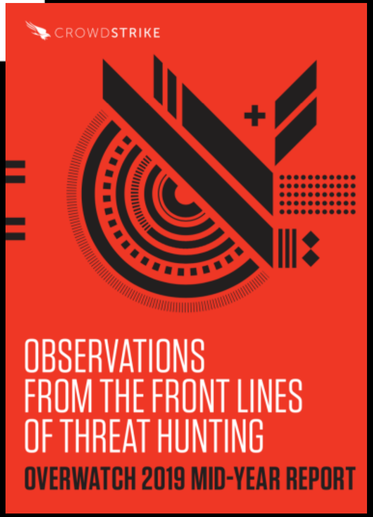
red canary

Threat Detection Report

An in-depth look at the most prevalent ATT&CK™ techniques according to Red Canary's historical detection dataset

CrowdStrike OverWatch Reports

https://www.crowdstrike.com/resources/reports/observations-from-the-front-lines-of-threat-hunting-2019/



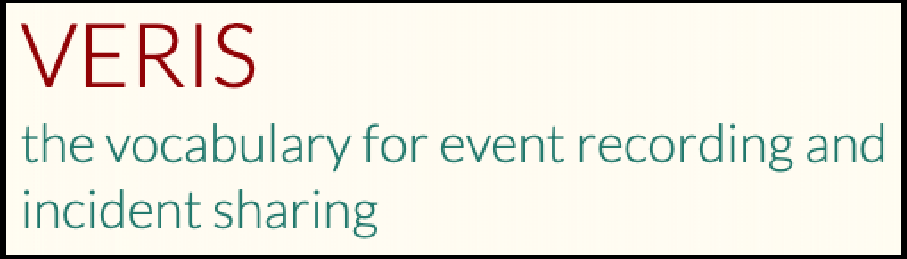
CROWDSTRIKE

OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING

OVERWATCH 2019 MID-YEAR REPORT

- **VERIS Community Database**

https://veriscommunity.net



VERIS

the vocabulary for event recording and incident sharing

Current status

- Have begun soliciting and collecting sightings under NDA

- Goal is to receive contributions from a few more organizations before moving forward

Get Involved

https://attack.mitre.org/resources/sightings

John Wunder

@jwunder

ATT&CK™

attack@mitre.org

@MITREattack

#ATTACKcon