DRAGOS

Threat Activity Groups

Your Hosts
Sergio Caltagirone @cnoanalysis
Joe Slowik @jfslowik

intel@dragos.com

DiamondModel.org

Industrial Threat Activity Groups

ALLANITE

CAPABILITIES
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

RASPITE

CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

MAGNALLIUM

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

CHRYSENE

CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

XENOTIME

CAPABILITIES
TRISIS, custom credential harvesting

VICTIMOLOGY
Oil & Gas, Middle East

ELECTRUM

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

DYMALLOY

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

COVELLITE

CAPABILITIES
Encoded binaries in documents, evasion techniques

VICTIMOLOGY
Electric Utilities, US

Is Activity Group Just a Fancy Name for Adversary?

DRAGOS

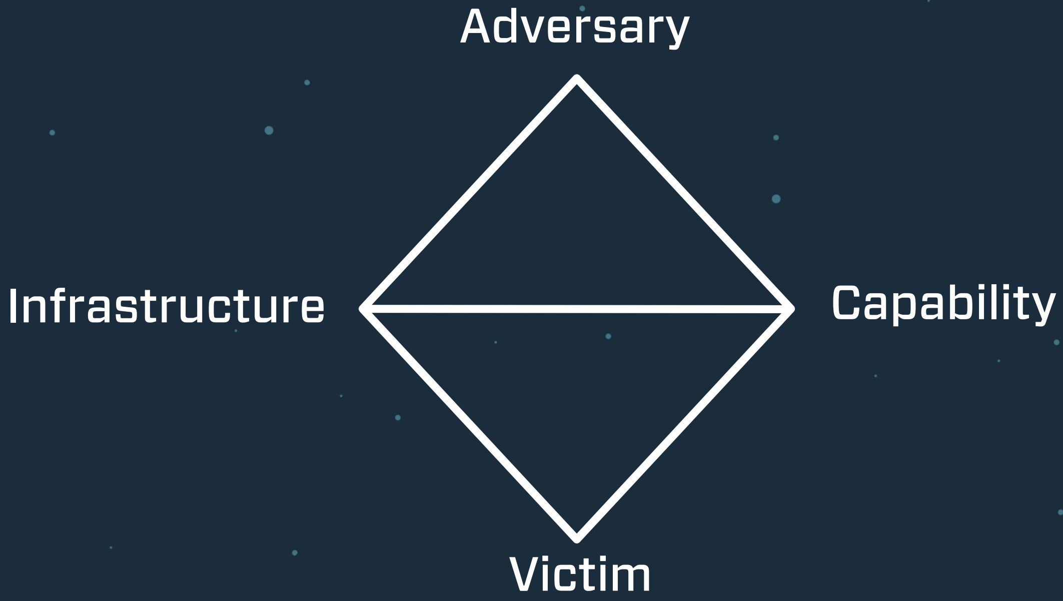
The Diamond Event

Axiom 1 For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.

Meta-Features

Timestamp
Phase
Result
Direction
Resources
Methodology
<your feature here>

Each edge can carry a confidence



DRAGOS

Activity Group

Activity Group An activity group is a set of Diamond events and activity threads associated by similarities in their features or processes and weighted by confidence

Two purposes of an activity group:

Framework to answer analytic questions requiring a breadth of activity knowledge

The development of mitigation strategies with an intended effect broader than activity threads

DRAGOS

Activity Groups – What You Hear is Not it All

What you normally see…

Analysts traditionally form activity groups to identify a common adversary behind events and threads usually using similarities in infrastructure and capabilities.

But, that’s not all…

But, the concept is inherently flexible and extends to include any grouping based on similarities to address a multitude of analytic and operational needs. The desired analytic or operational outcome determines the implementation and type of correlation (i.e., grouping function) used.

And they change…

Activity groups are not static – just as adversaries are not static. Activity groups must grow and change over time to absorb new knowledge of the adversary including changes in their needs and operations

Why Activity Groups? To Solve Analytic Problems

What is the Analytic Problem

- Activity grouping is used to solve a number of problems.
- These problems generally require deduction and inference based on a common set of features (i.e., feature vector).
- These problems are generally distinct enough to require a different feature vector for each problem.
- For instance, the feature vector which would group events and threads by likely adversary (e.g., attribution) would not always suffice to group events to discover common malware authors/developers.
- The analytic problem must first be defined.

Examples

- **Trending**: How has an adversary's activity changed over time and what is the current vector to infer future change?
- **Intent Deduction**: What is the intent of the adversary?
- **Attribution Deduction**: Which events and threads are likely conducted by the same adversary?
- **Adversary Capabilities and Infrastructure**: What is the complete set of observed capabilities and infrastructure of the adversary?
- **Cross-Capability Identification**: Which capabilities have been used by multiple adversaries?
- **Adversary Campaign Knowledge Gap Identification**: What are the organization's knowledge gaps across an adversary's campaign?

DRAGOS

The Activity Group Process

1 Analytic Problem

The particular analytic problem to be solved through grouping

2 Feature Selection

The event features and adversary processes used to form the basis of classification and clustering are selected

3 Creation

Activity groups are created from the set of events and threads

4 Growth

As new events flow into the model, they are classified into the Activity Groups

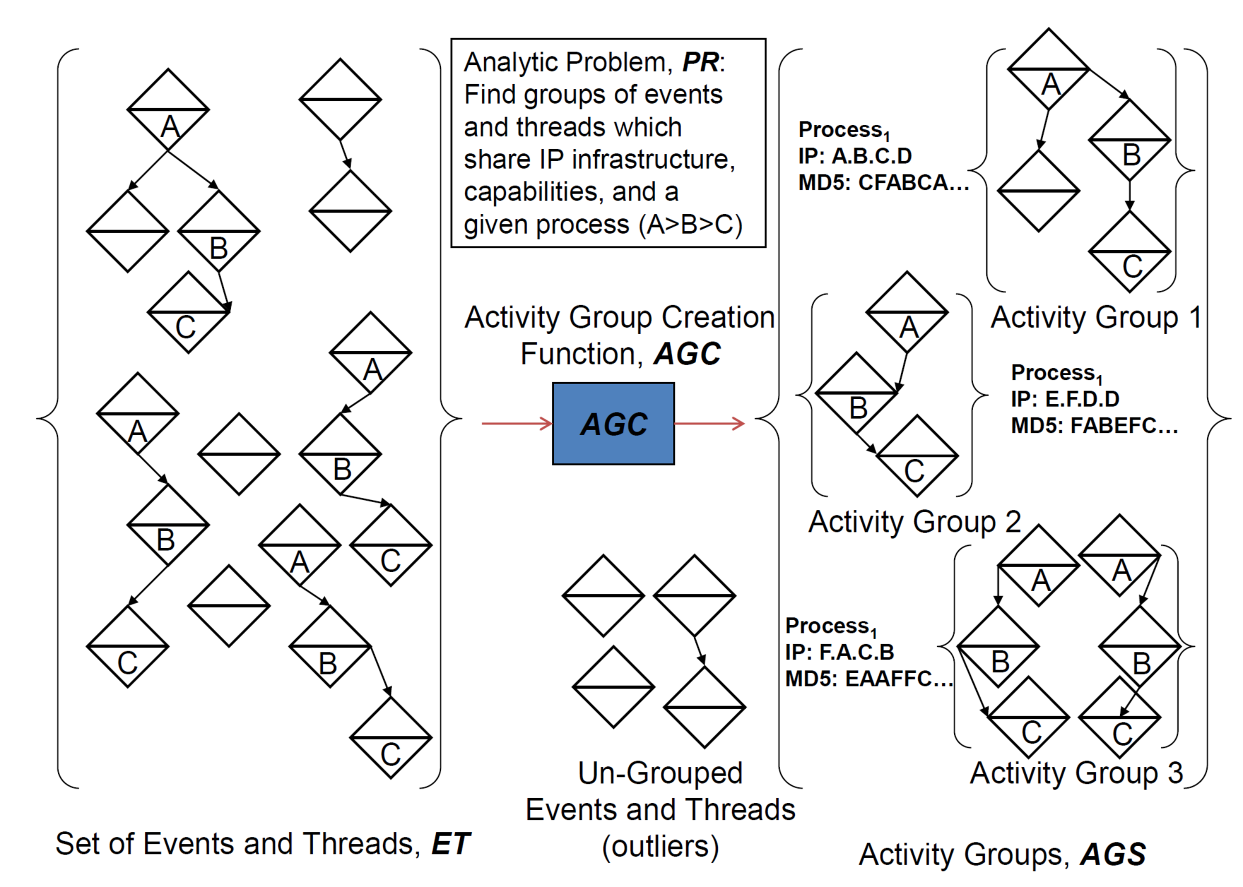
5 Analysis

Activity groups are analyzed to address the analytic problem(s) defined

6 Redefinition

Activity groups need to be redefined from time-to-time to maintain their accuracy

How to Create an Activity Group



Analytic Problem, ***PR***: Find groups of events and threads which share IP infrastructure, capabilities, and a given process (A>B>C)

Activity Group Creation Function, ***AGC***

AGC

Process$_1$
IP: A.B.C.D
MD5: CFABCA…

Activity Group 1

Process$_1$
IP: E.F.D.D
MD5: FABEFC…

Activity Group 2

Process$_1$
IP: F.A.C.B
MD5: EAAFFC…

Activity Group 3

Set of Events and Threads, ***ET***

Un-Grouped Events and Threads (outliers)

Activity Groups, ***AGS***

Industrial Threat Activity Groups

ALLANITE

CAPABILITIES
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

RASPITE

CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

MAGNALLIUM

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

CHRYSENE

CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

XENOTIME

CAPABILITIES
TRISIS, custom credential harvesting

VICTIMOLOGY
Oil & Gas, Middle East

ELECTRUM

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

DYMALLOY

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

COVELLITE

CAPABILITIES
Encoded binaries in documents, evasion techniques

VICTIMOLOGY
Electric Utilities, US

Let me know if you've heard this one…

TG-3390

CROWDSTRIKE

APT29

FireEye

Symantec

FANCY BEAR

PLATINUM

Microsoft

KASPERSKY lab

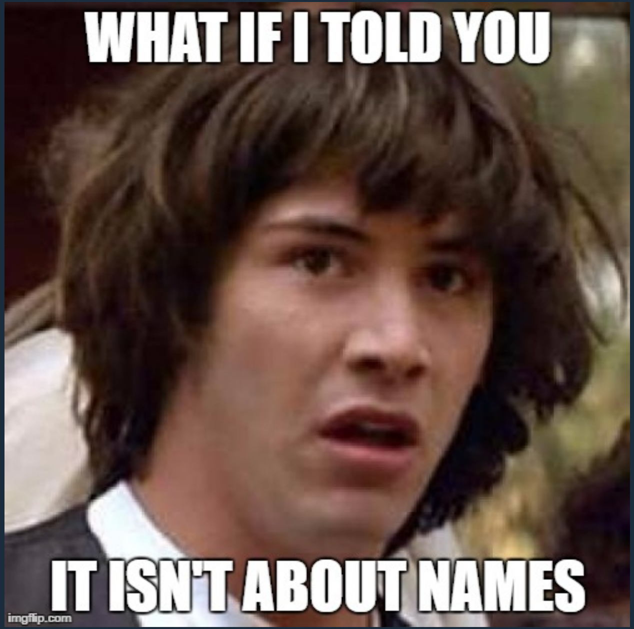
Names, names everywhere!

DRAGOS

Why can’t we all just agree on one name?!

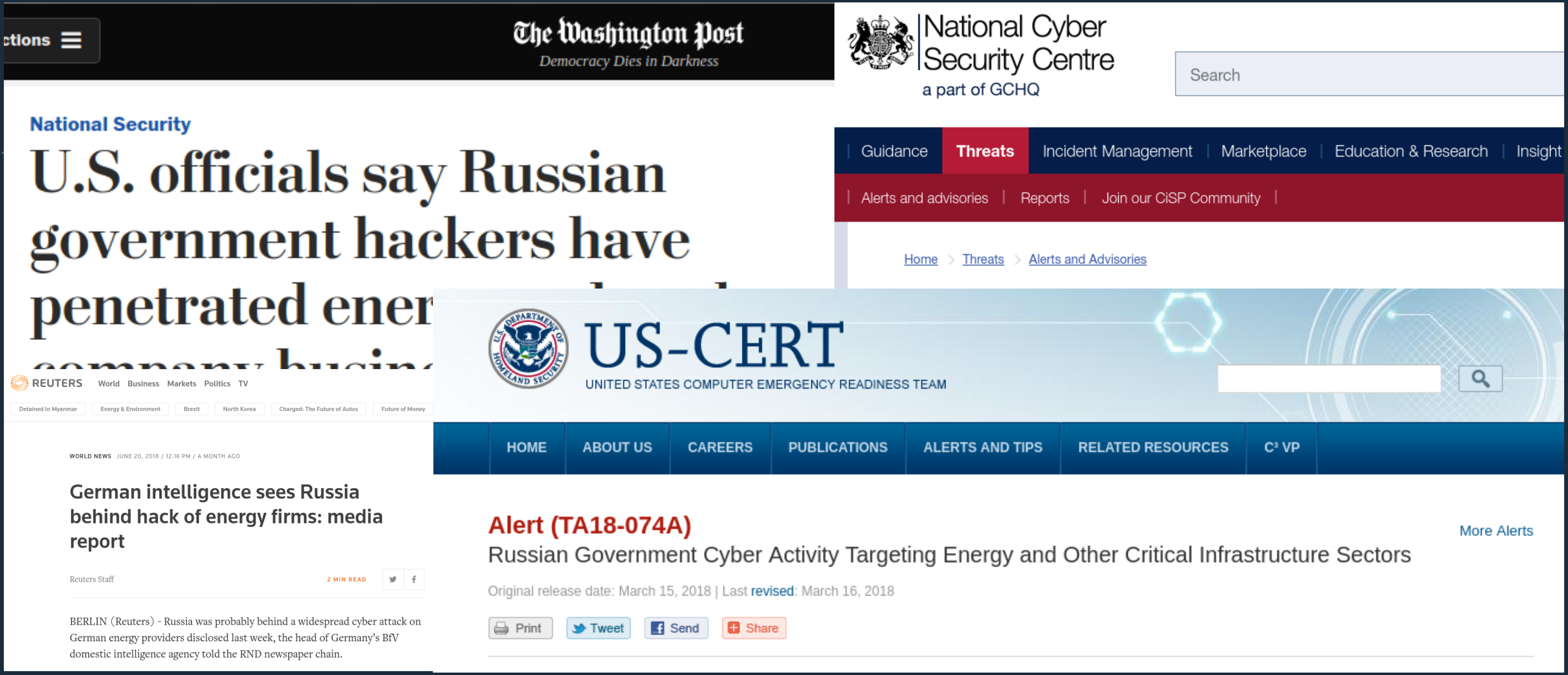
The simple answer: it’s hard enough to correlate activity consistently within a 10 person team let alone across a variety of organizations.

The complex answer: correlation and classification is a complex analytic problem which requires us to share the same grouping function and feature vector.



DRAGOS

Example: 2017-Present Electric Utility Intrusions



National Security

U.S. officials say Russian government hackers have penetrated ener

WORLD NEWS JUNE 20, 2018 / 12:16 PM / A MONTH AGO

German intelligence sees Russia behind hack of energy firms: media report

Reuters Staff 2 MIN READ

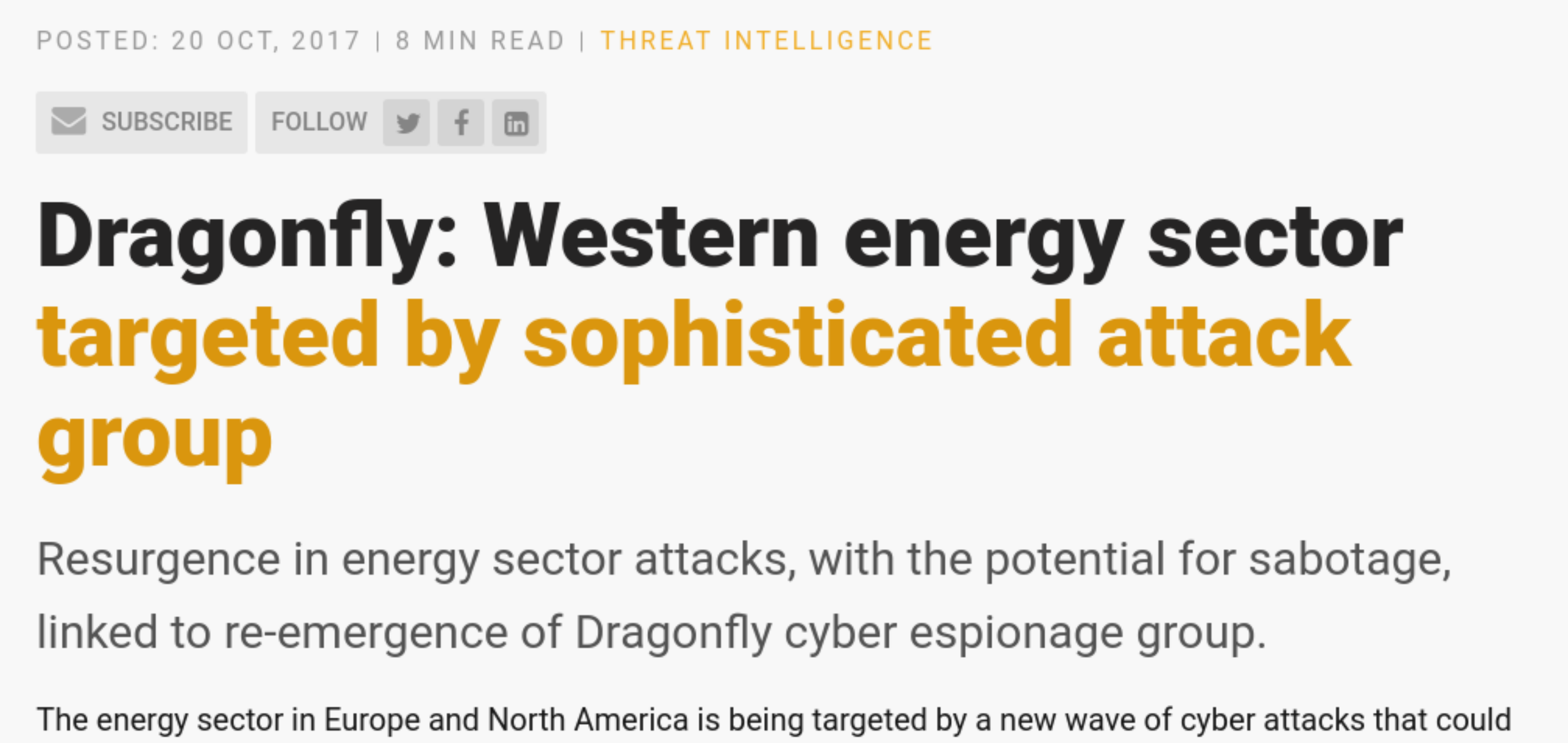
BERLIN (Reuters) - Russia was probably behind a widespread cyber attack on German energy providers disclosed last week, the head of Germany's BfV domestic intelligence agency told the RND newspaper chain.

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Initial Analysis: Dragonfly 2.0



POSTED: 20 OCT, 2017 | 8 MIN READ | THREAT INTELLIGENCE

Dragonfly: Western energy sector targeted by sophisticated attack group

Resurgence in energy sector attacks, with the potential for sabotage, linked to re-emergence of Dragonfly cyber espionage group.

The energy sector in Europe and North America is being targeted by a new wave of cyber attacks that could

Behavioral Analysis Yields Distinctions

	DRAGONFLY	DYMALLOY	ALLANITE
Active	2013-2014	Late 2015 – ?	Mid 2017 - ?
Target Geography	Europe North America	Turkey Europe North America	USA UK Germany
Infection Vector	Phishing w/PDF, Watering Hole, Trojanized Softare	Phishing w/Doc	Phishing w/Doc, Watering Hole
Persistence Mechanism	KARAGANY Malware	Various Malware and Backdoors	Create User Accounts, Credential Harvesting
ICS Impact	OPC-focused Malware Family	Survey and Screenshots via Malware	Survey and Screenshots vis System Tools

DRAGOS

Industrial Threat Activity Groups

ALLANITE

CAPABILITIES
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

RASPITE

CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

MAGNALLIUM

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

CHRYSENE

CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

XENOTIME

CAPABILITIES
TRISIS, custom credential harvesting

VICTIMOLOGY
Oil & Gas, Middle East

ELECTRUM

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

DYMALLOY

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

COVELLITE

CAPABILITIES
Encoded binaries in documents, evasion techniques

VICTIMOLOGY
Electric Utilities, US

Final Points

Activity Groups are an analytic concept driven by analysis problems

Activity Groups have varying degrees of confidence – as the grouping gets larger the confidence tends weaker

Activity Groups are not equivalent to attribution but, they can be used that way

Activity Groups are useful for analysts and defenders to group similar activity together to understand broader implications and take more strategic action

Activity Groups use stupid names

DRAGOS

Thank you

DiamondModel.org

Sergio Caltagirone	@cnoanalysis
Joe Slowik	@jfslowik

intel@dragos.com

DRAGOS