RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: AIR-R11

Cyber Threat Alliance: Could 7.4Bn+ Collaborate Together against the Bad Minority?

MODERATOR: **Greg Day**
VP & Chief Security Officer, EMEA. Palo Alto Networks
@GregDaySecurity

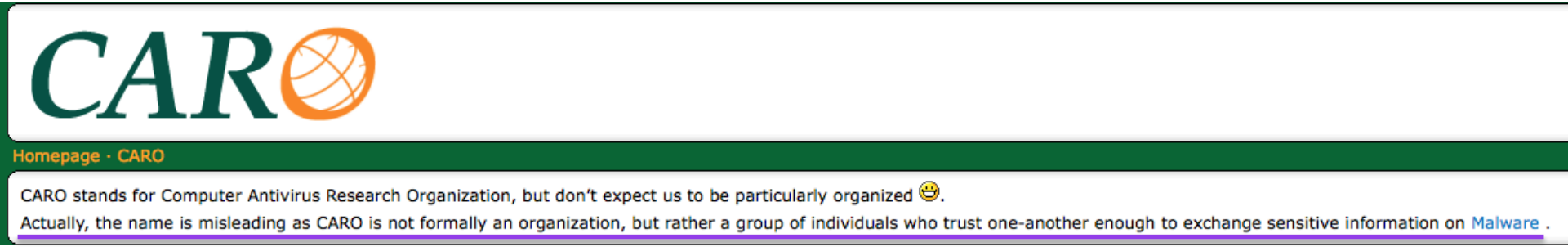
PANELISTS: **Derek Manky**
Global Security Strategist
Fortinet
/in/derekmanky

John Hultquist
Director, Cyber Espionage Analysis
iSIGHT Partners/FireEye
@johnhultquist

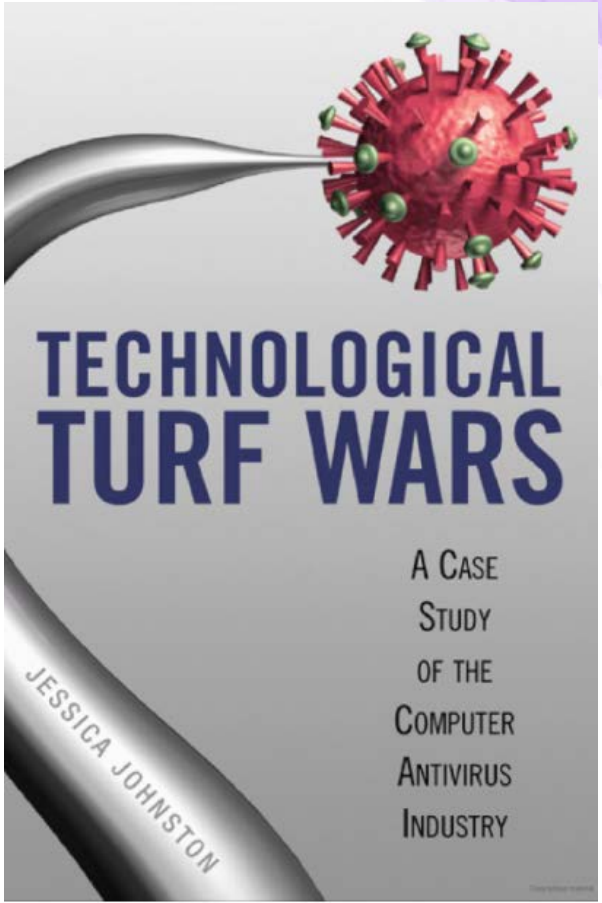
Freddy Dezeure
Head of EU-CERT
@certeu

Not a new idea…

- CARO



- REVS – Rapid Exchange of Virus Samples (1999) – antivirus vendors sharing samples and reports on attacks during an emergency to react
- virustotal Advanced features & tools VirusTotal Community
- CiSP A CATALYST FOR COLLABORATION - joint industry/gov scheme based in CERT-UK.
  - online tool, enables its members to exchange information on threats/vulns in real time.



Bedtime reading?

Cyber Threat Alliance

Founding Members:

paloalto NETWORKS

Symantec

FORTINET

intel Security

Purpose: *The Cyber Threat Alliance is a group of cyber security practitioners that have chosen to share threat information with each other for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers.*

Founding CEOs

Mark McLaughlin

Greg Clark

Ken Xie

Chris Young

Contributing Members:

BARRACUDA NETWORKS

REVERSING LABS

Telefónica

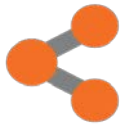
zscaler
Secure. Everywhere.

Membership: Open to any organization that can share a minimum volume of threat intelligence designed by the Alliance.

The CTA's Guiding Principles

The CTA Mission

Work together in good faith to equitably share **campaign based** cyber threat intelligence to defend against cyber adversaries and improve our customers' security



FOR THE GREATER GOOD

Share intel to strengthen critical infrastructure and protect our customers.

TIME IS OF THE ESSENCE

Prevent and circumvent attacks by sharing timely, actionable intel.

CONTEXT IS KING

Prioritize the sharing contextual, accurate intel tied to specific campaigns.

RADICAL TRANSPARENCY

All intel is attributed, and intel sharing rules will always be published and clear.

NO PAY TO PLAY

All members must share intel to extract intel from the CTA.

CTA's Value Proposition

The CTA's intelligence sharing improves the security, availability, integrity, and efficiency of information systems through the sharing of **verified, actionable, near real-time indicators of compromise**

Intelligence Sharing: Inputs versus outputs

WHAT YOU SUBMIT

You must submit a minimum value of threat intelligence consisting of:

- ***Observables***
  - – Based on STIX package
- ***Context***
  - – Campaign, Threat Actor, etc.

WHAT YOU RECIEVE

You choose what intelligence you extract from the CTA by applying the below filters:

- *Which member submitted the data*
- *Affiliation with a particular threat actor*
- *Date of data submission or detection*
- *Verification/validation by other members*
- *Data type (e.g. malware, domain)*

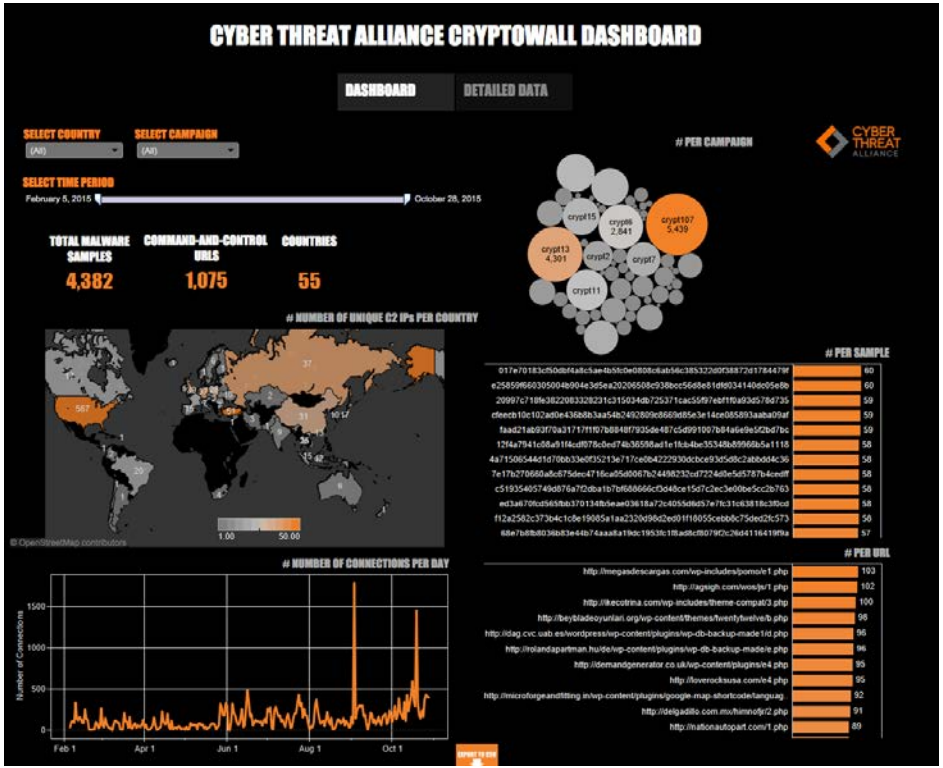
What Happens in Between?

- **A value based algorithm will analyze all intelligence submitted to the CTA**
  - — Information will be assigned points at the time of submission
  - — Submitted data will be correlated with other member data for mutual validation

Long Term Intent

The point value of data you submit will eventually determine the amount of data you can extract from the CTA.

Proving value…



CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

$325M in estimated damages across the globe

839 command and control URLs

5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples

Working committee

Rick Howard Ryan Olson

Joe Chen

Derek Manky

Vincent Weafer Jeannette Jarvis

Where next….

- Adversary Playbooks
- Intelligence Marketplace
- Crossing the Last Mile
- Systematic Orchestration

Want to become a member?

Why Join Now?

- Help shape the CTA's initial intelligence sharing value **algorithm**
- Influence new **member recruitment** and selection of the CTA's first **President**
- Participate in the **inaugural board meeting** after January incorporation
- Collaborate with the **Founding Member CEOs** in their role as CTA Directors in Year 1

How to Join

1. Contact Kathi Haley for more details on technical requirements for the CTA Platform
2. Confirm your decision to join pre-RSA by January 1, 2017

We're happy to meet with your company 1:1 to answer any additional questions

For more information, contact **Kathi Haley** of Palo Alto Networks
khaley@paloaltonetworks.com or (571) 266-5694

Meet todays panel…

Derek
Manky
Fortinet
(CTA member)

John
Hultquist
iSIGHT/FireEye

Freddy
Dezeure
EU-CERT