RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-W03

Attacks on Critical Infrastructure: Insights from the "Big Board"

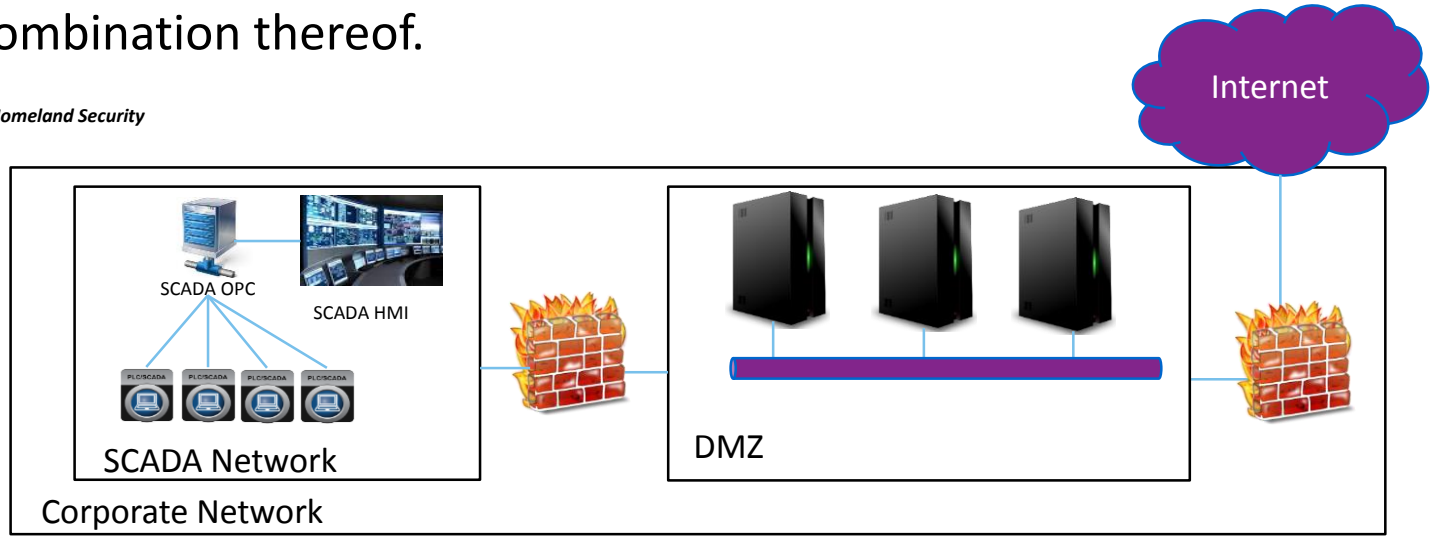
Daniel Cohen
Head of RSA FraudAction
RSA, The Security Division of EMC
@iFraudFighter

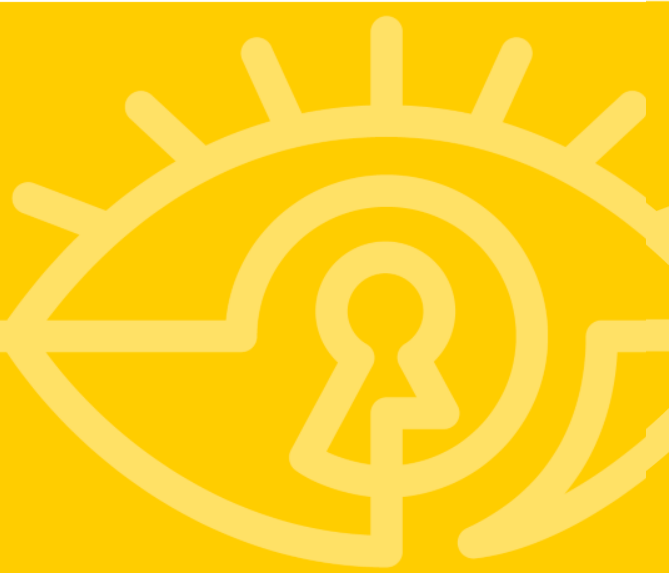
Bob Griffin
Chief Security Architect
RSA, the Security Division of EMC
@RobtWesGriffin

What is a critical infrastructure from attacker point of view? An opportunity!

Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

USA Department of Homeland Security





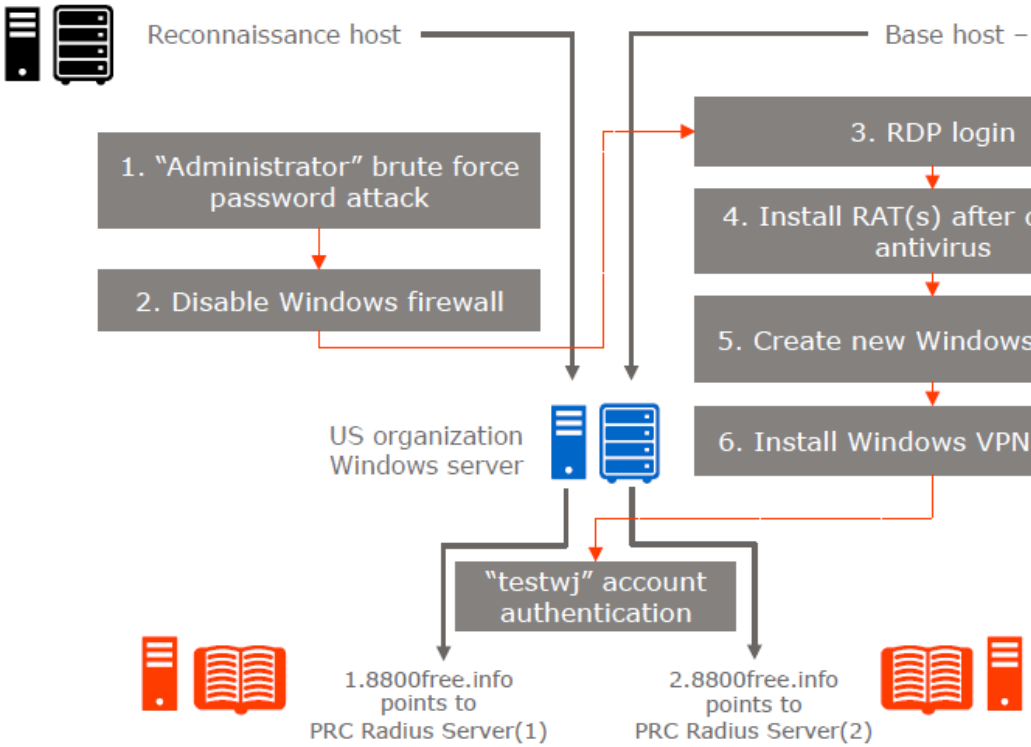
More Insights from the Dark Web: Terracotta and GlassRat

Bob Griffin

Terracotta

https://blogs.rsa.com/terracotta-vpn-enabler-of-advanced-threat-anonymity/

Terracotta

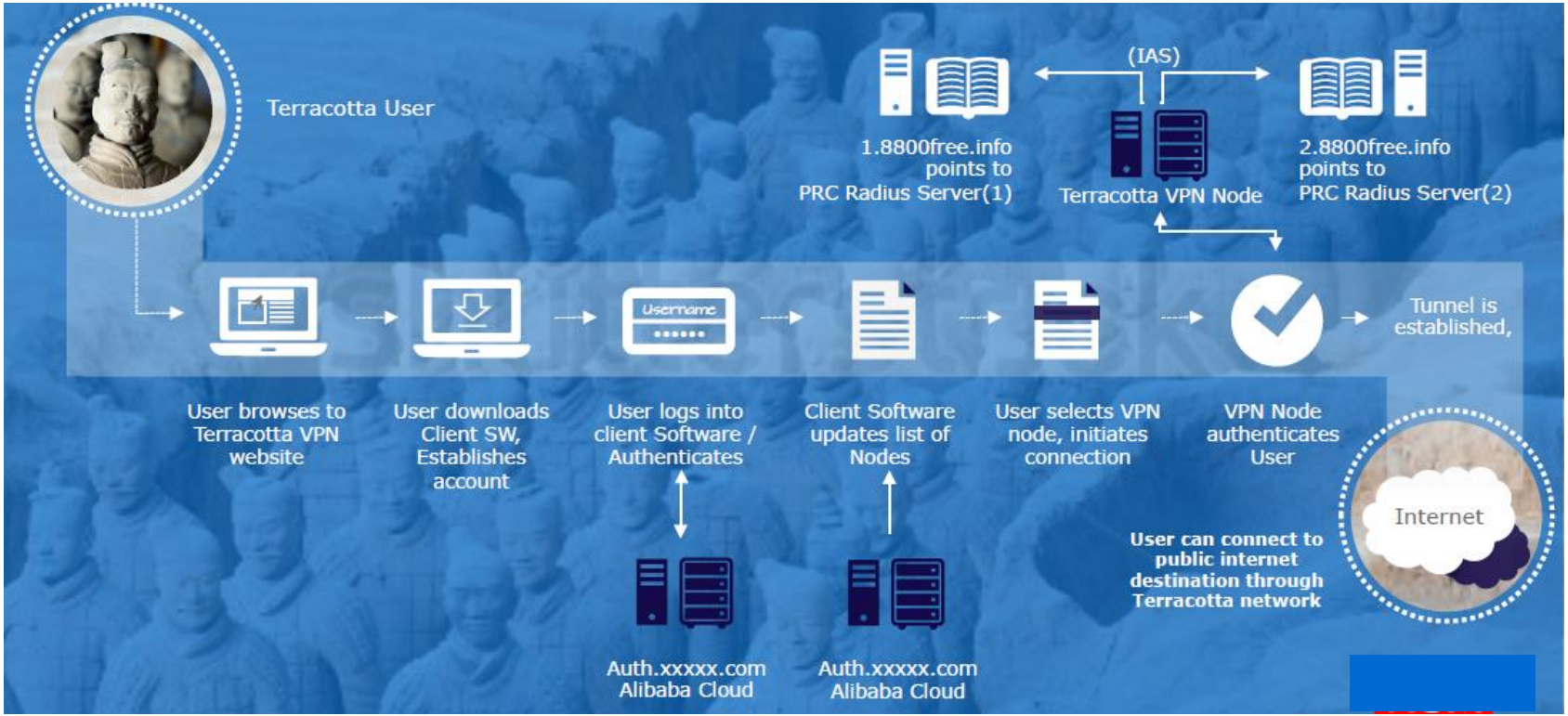


Wang Jia (testwj)
Dongguan

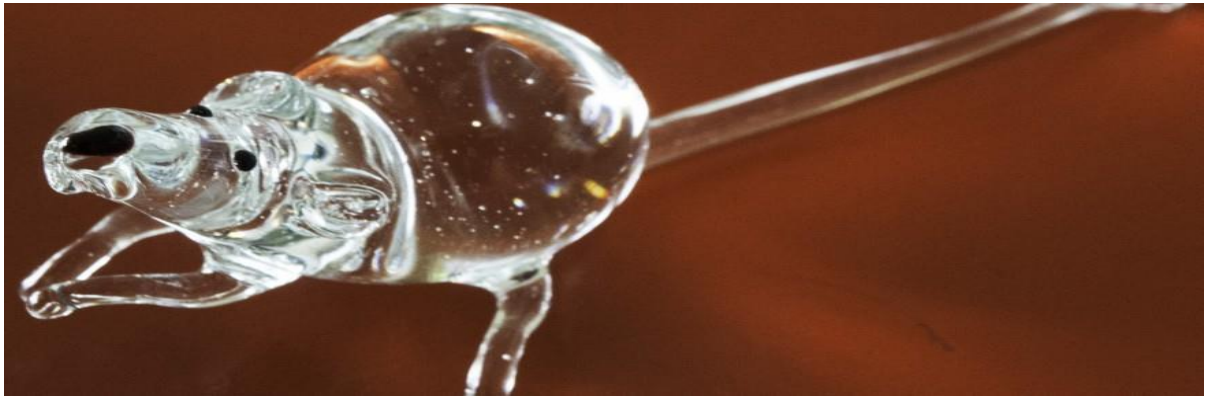
Victims all had Internet-exposed Windows servers without firewalls

Terracotta may target vulnerable Windows servers because this platform includes VPN services that can be configured in a matter of minutes

How Terracotta Works



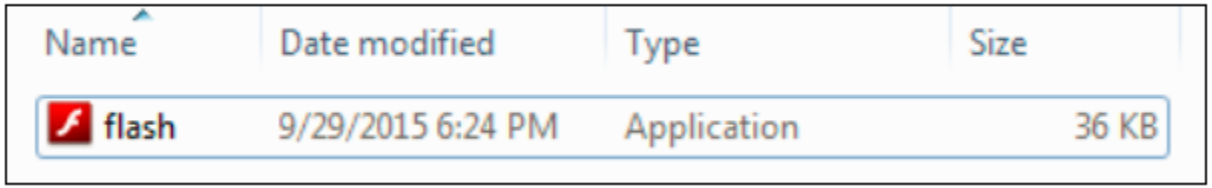
GlassRat



- Detected February 2015 but had been in the wild since 2012
- Linked to other campaigns such as Mirage (2012)
- Targets Chinese nationals in commercial enterprises world-wide

https://blogs.rsa.com/resource/peering-into-glassrat/

GlassRat Dropper (Installer)



Double clicking on the flash.exe files causes the dropper to launch.

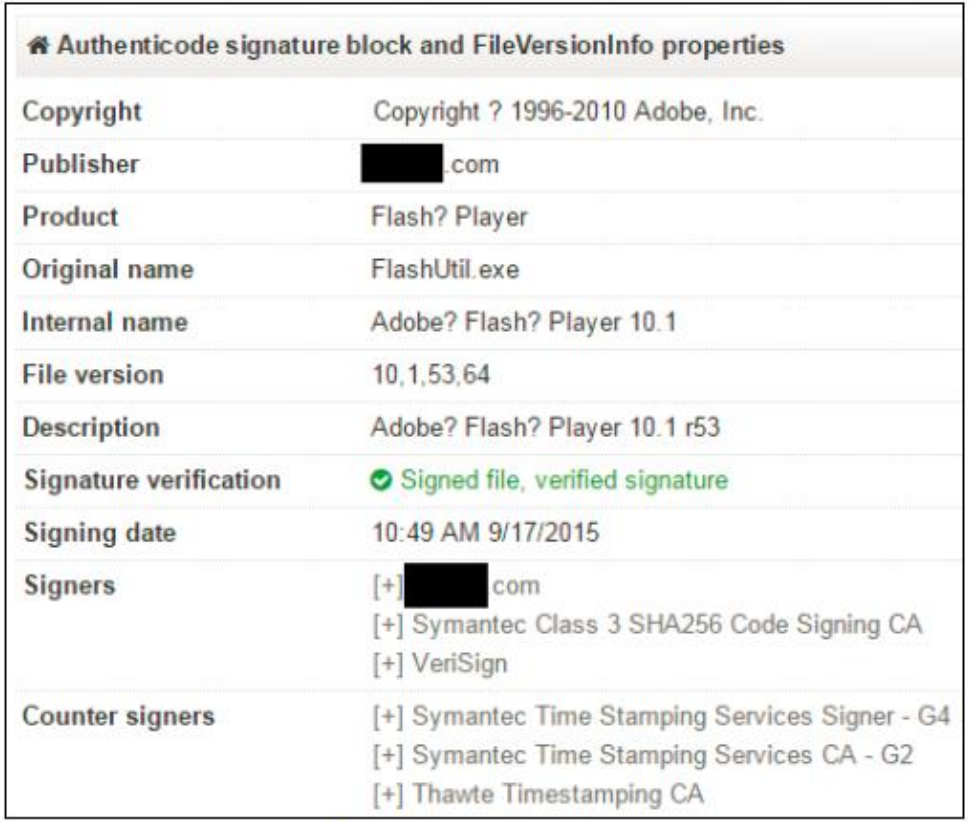
1. Dropper (flash.exe) writes the GlassRAT DLL to the ProgramData folder
2. 2. Dropper runs the DLL file using the built-in Windows utility rundll32.exe
3. 3. GlassRAT DLL file modifies the run key for logon persistence with user-level permissions with the following registry key.

   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run **Update**

4. 4. the dropper deletes itself with and embedded command:

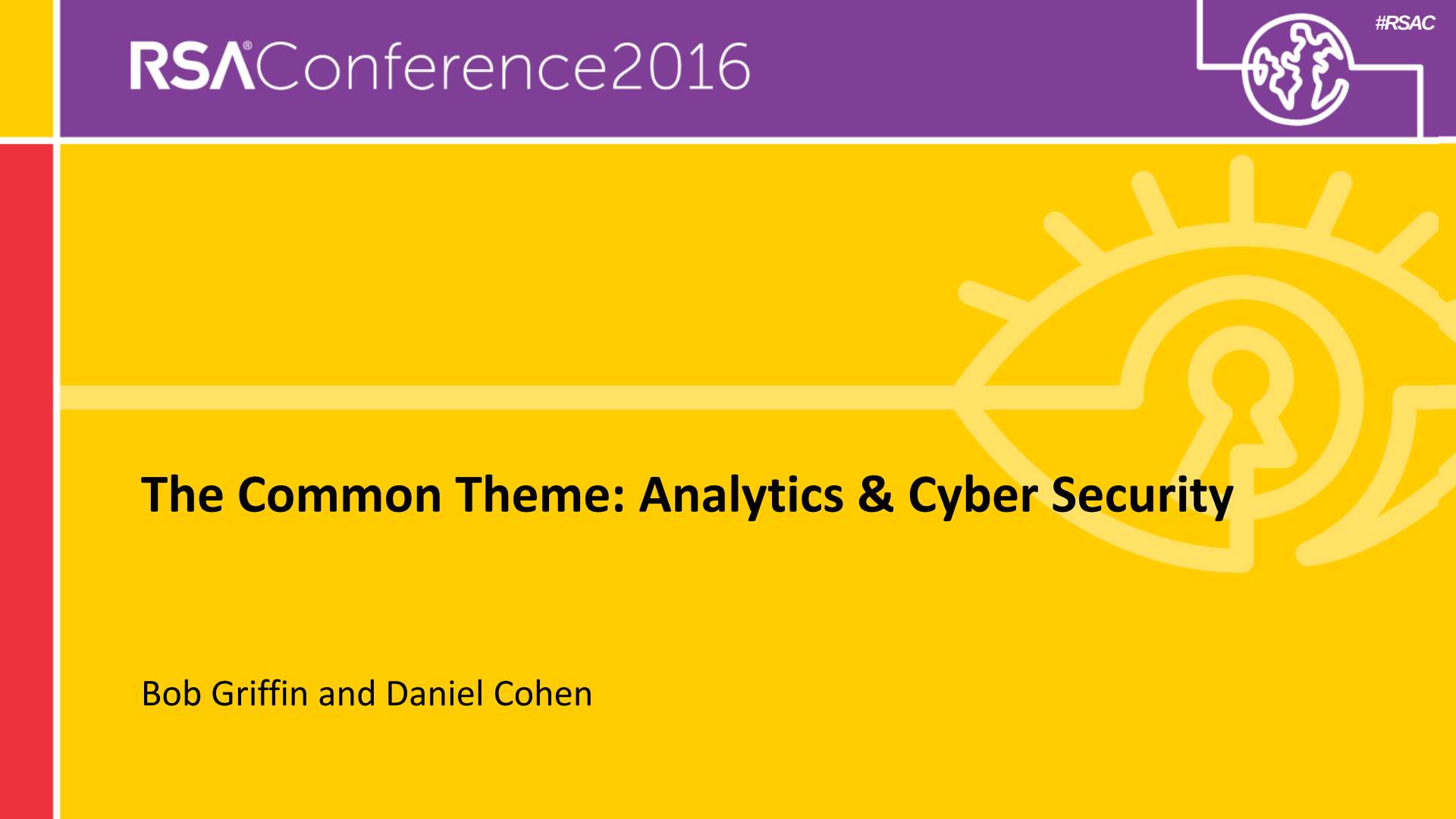
   “cmd.exe /c erase /F "%s",”

GlassRat Code Signing



Authenticode signature block and FileVersionInfo properties

Copyright	Copyright ? 1996-2010 Adobe, Inc.
Publisher	[redacted].com
Product	Flash? Player
Original name	FlashUtil.exe
Internal name	Adobe? Flash? Player 10.1
File version	10,1,53,64
Description	Adobe? Flash? Player 10.1 r53
Signature verification	Signed file, verified signature
Signing date	10:49 AM 9/17/2015
Signers	[+] [redacted].com [+] Symantec Class 3 SHA256 Code Signing CA [+] VeriSign
Counter signers	[+] Symantec Time Stamping Services Signer - G4 [+] Symantec Time Stamping Services CA - G2 [+] Thawte Timestamping CA



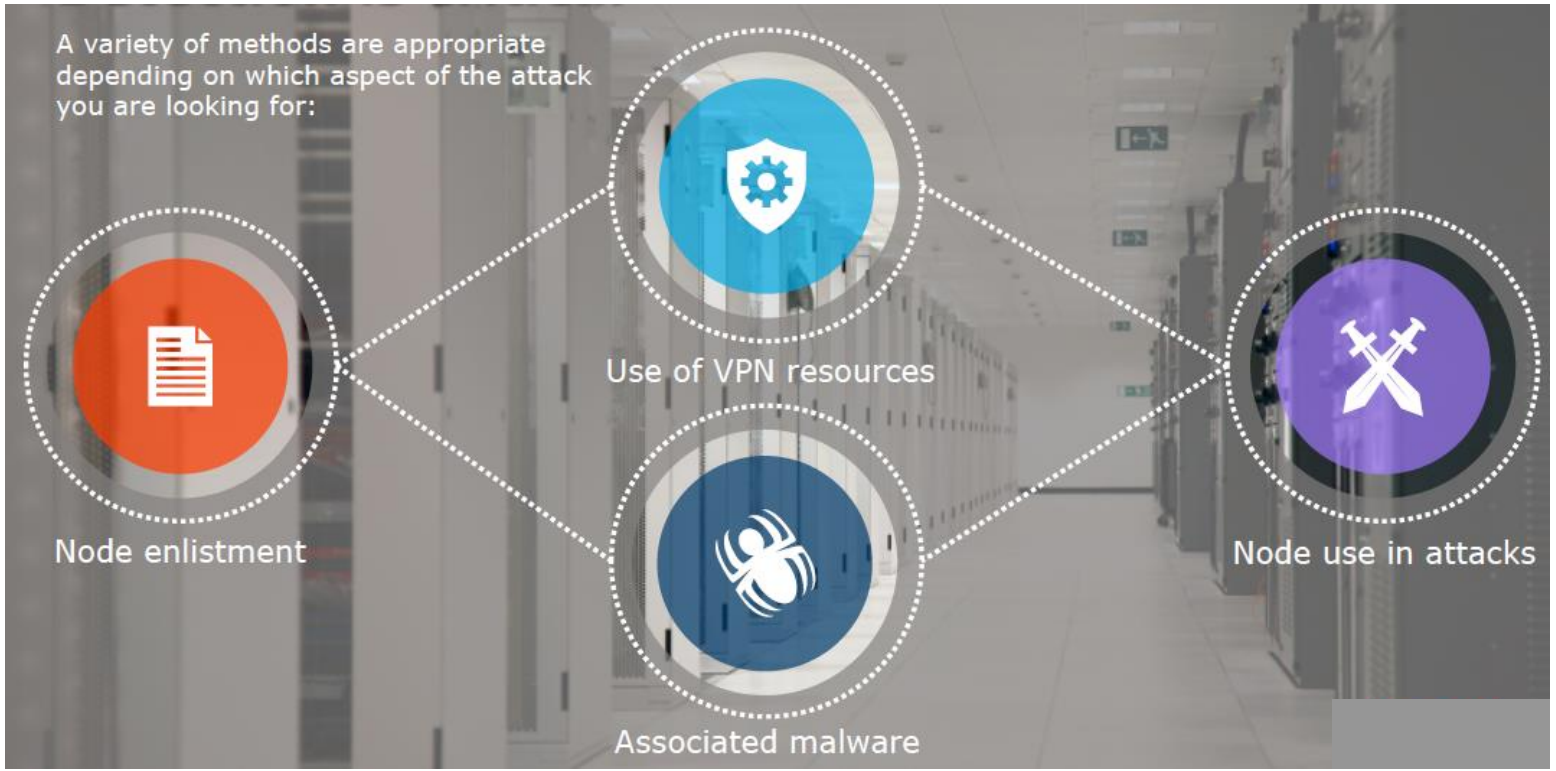
The Common Theme: Analytics & Cyber Security

Bob Griffin and Daniel Cohen

Analytics at the RSA AFCC

http://australia.emc.com/video-collateral/demos/microsites/mediaplayer-video/glimpse-rsa-anti-fraud-command-center.htm

Detecting Terracotta



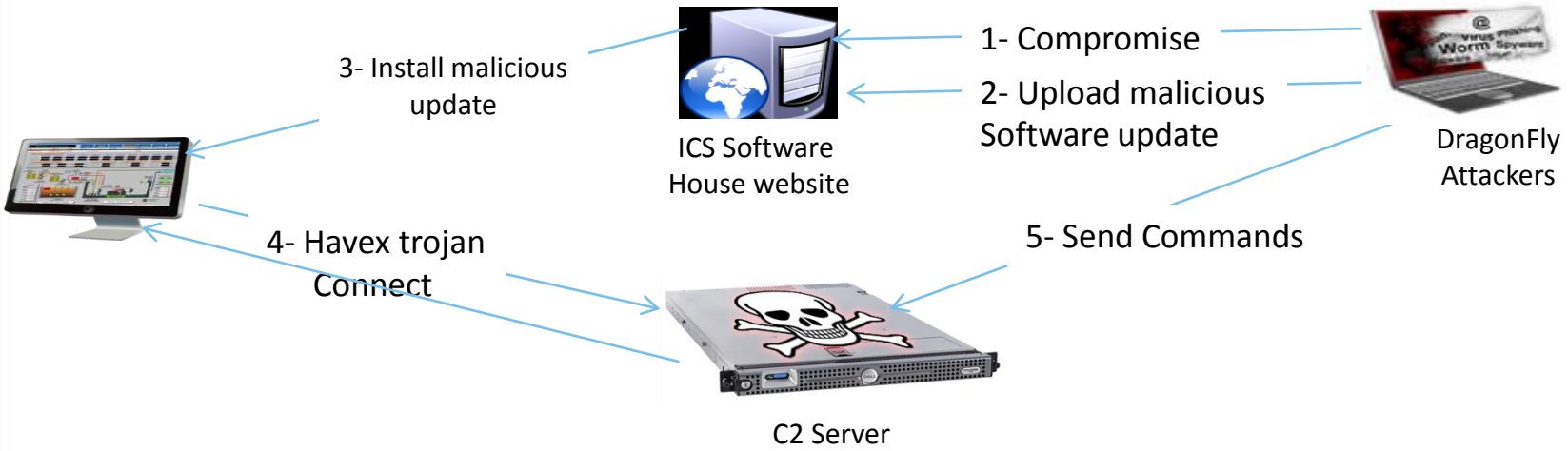
https://blogs.rsa.com/wp-content/uploads/2015/08/Terracotta-VPN-Report-Final-8-3.pdf

Detecting GlassRat

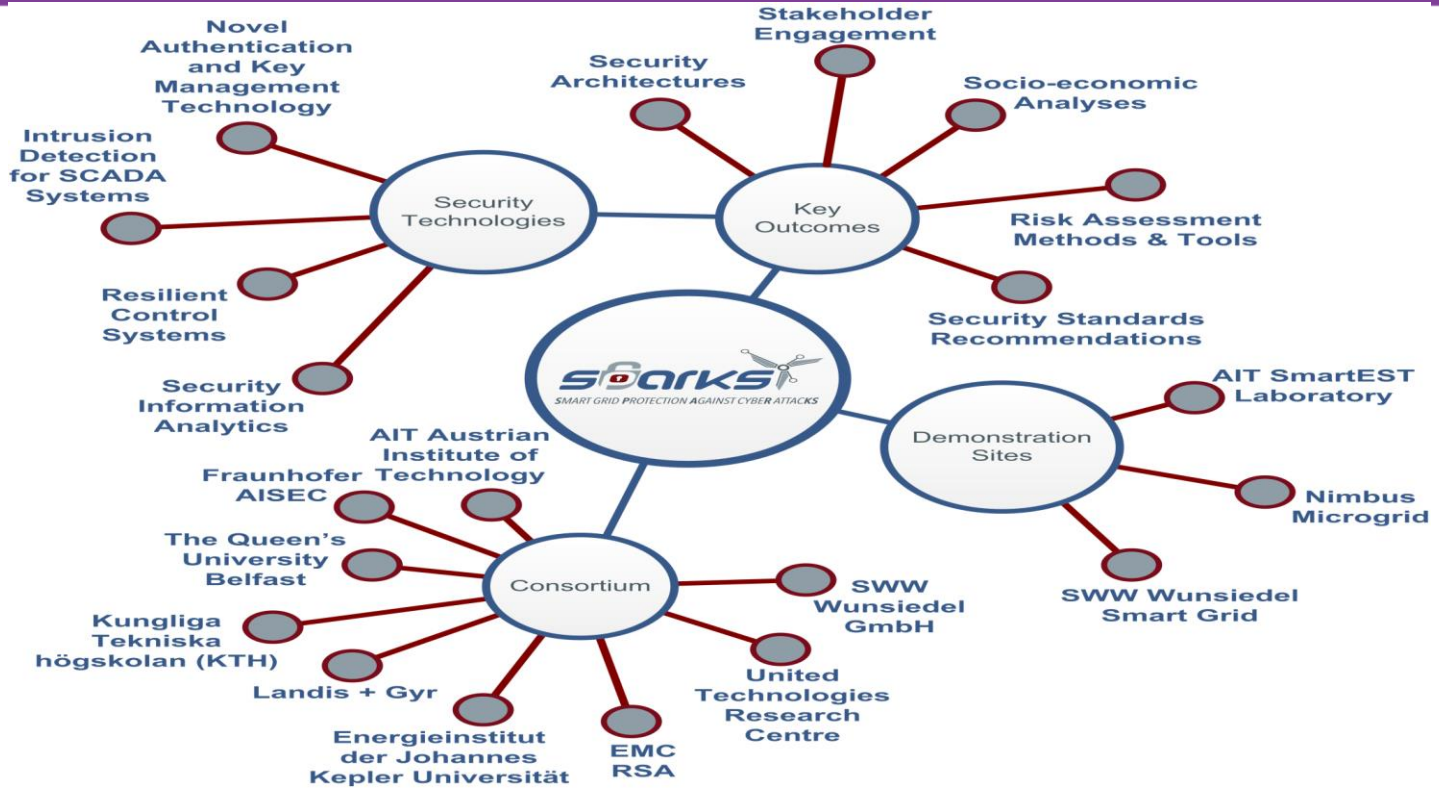
http://charge.rsa.com/wp-content/uploads/2015/09/Finding-The-R.A.T-With-ECAT.pdf

Attacks on the Smart Grid

The recent DragonFly campaign showed how the attackers could use malware to take control of SCADA systems



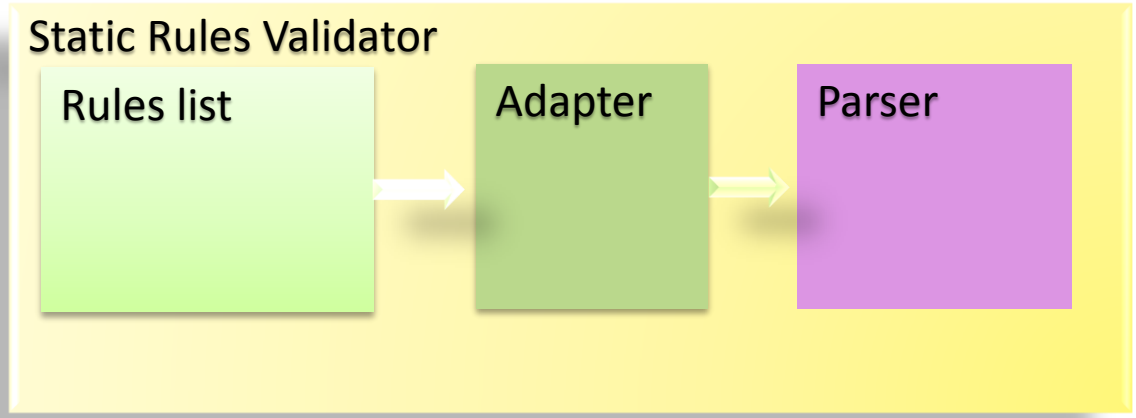
SPARKS Project Consortium



Analysis using Static Rules Validator

This component searches for systems' asserts violations

- *Rules List* contains the assertions to verify
- *Adapter* translate the rules in common language
- *Parser* get the rules and search for negative or positive outliers



Static Rules: Variable outlier

- Outliers against a predefined bound
  - E.g. Voltages should not fluctuate very much
- Examine voltages and frequency only

Static Rules: Rule Outlier

- Calculate physical relationships between variables
- 18 separate equations

$$\cos^{-1}\frac{V_A^{\,2}+V_B^{\,2}-V_{AB}^{\,2}}{2V_A\,V_B}+\cos^{-1}\frac{V_B^{\,2}+V_C^{\,2}-V_{BC}^{\,2}}{2V_B\,V_C}+\cos^{-1}\frac{V_C^{\,2}+V_A^{\,2}-V_{CA}^{\,2}}{2V_C\,V_A}=360°$$

- Measurement is asynchronous
  - Use difference between RHS and LHS (*error*)
- Determine probability of error from historical data
- Flag when below some threshold

Static Rules: Kullback Leibler

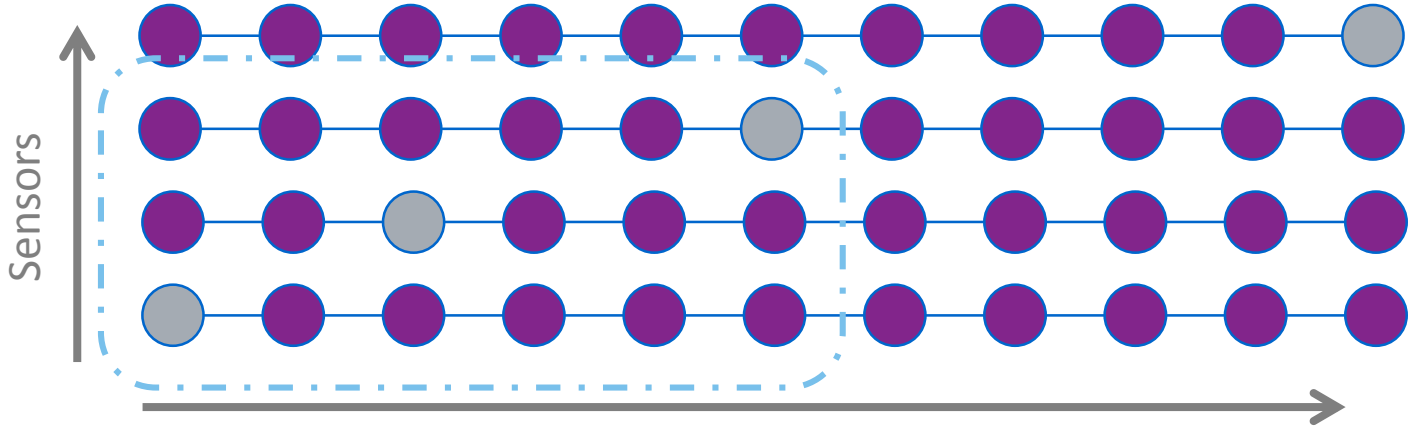
- Symmetrized KL distance on rule errors
  - Symmetrisation due to Kullback & Leibler

$$D_{KL} = d_{KL}(j,i) - d_{KL}(i,j)$$

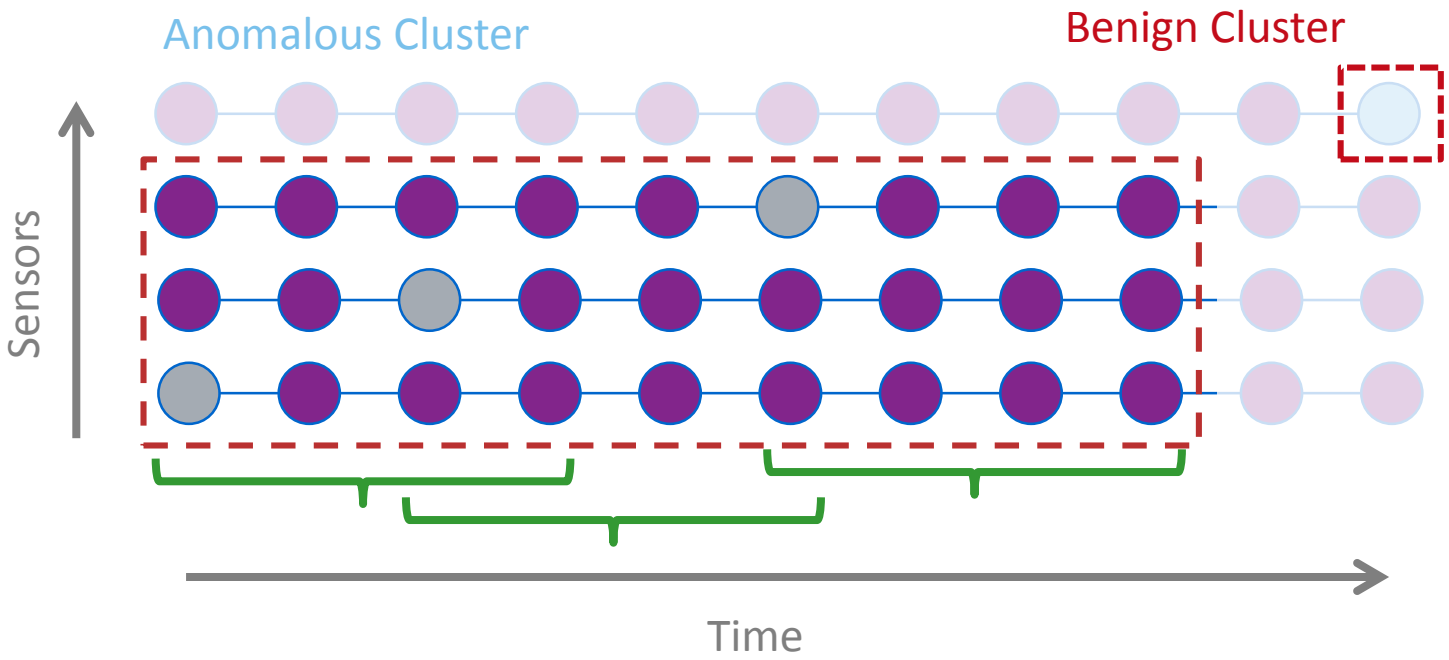
- Historical data (baseline) vs Current measurement
- Anomaly when value above some threshold

Static Rules: Dead Sensor Clustering

- Cluster sensors that stop recording in time
- User configurable time window
- Anomalous when cluster size > threshold



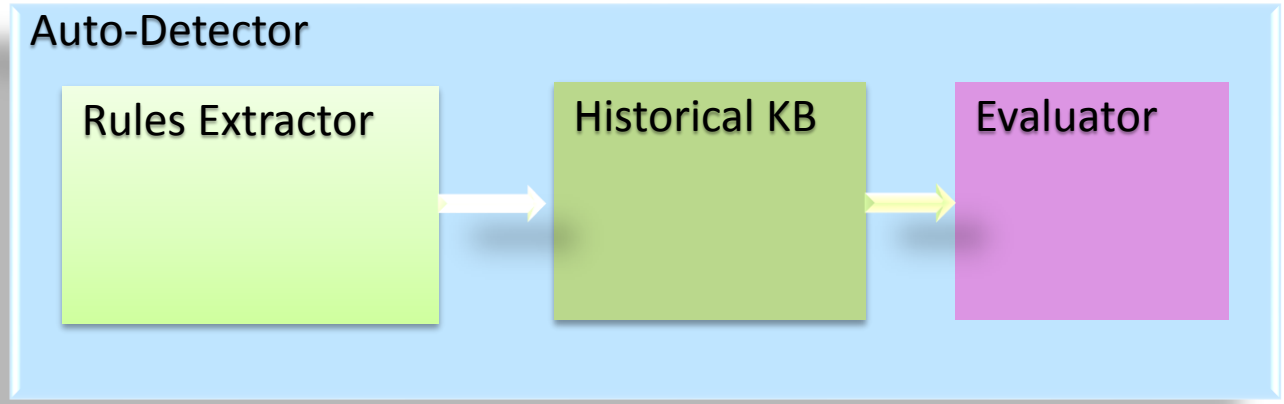
Static Rules: Dead Sensor Clustering



Analysis using Dynamic Detection

This component uses machine learning techniques to evaluate the entire system state

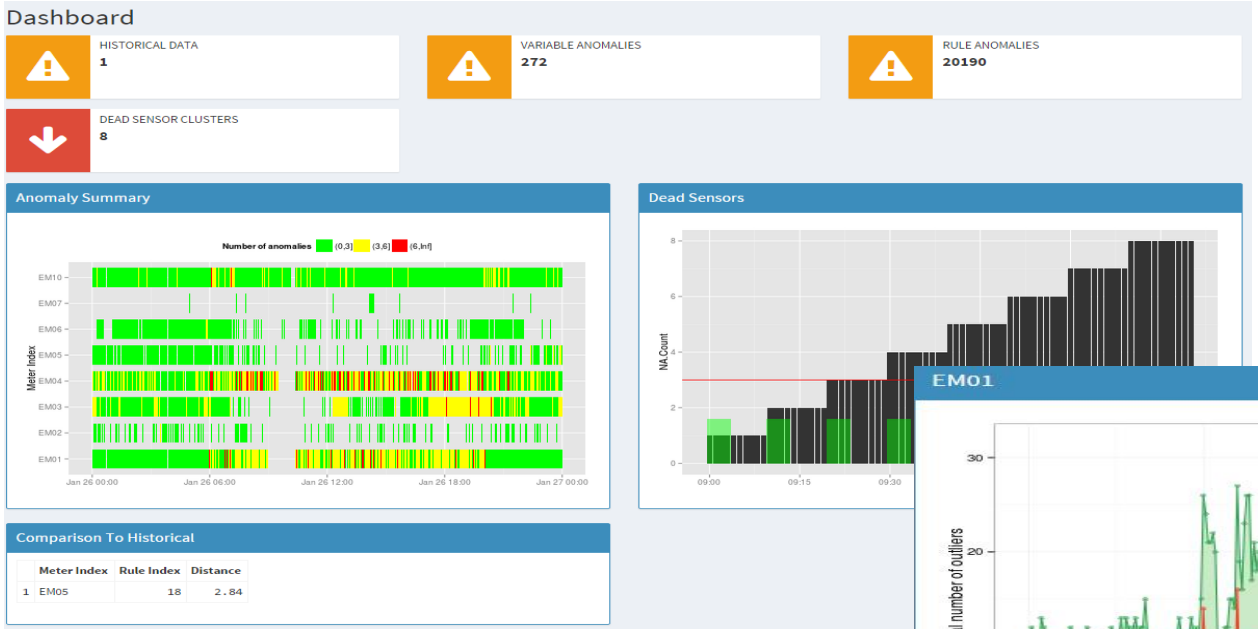
- *Rules Extractor* get data from last readings
- *Historical KB* compare the new feature with system history
- *Evaluator* use tolerance to reduce FP and noise

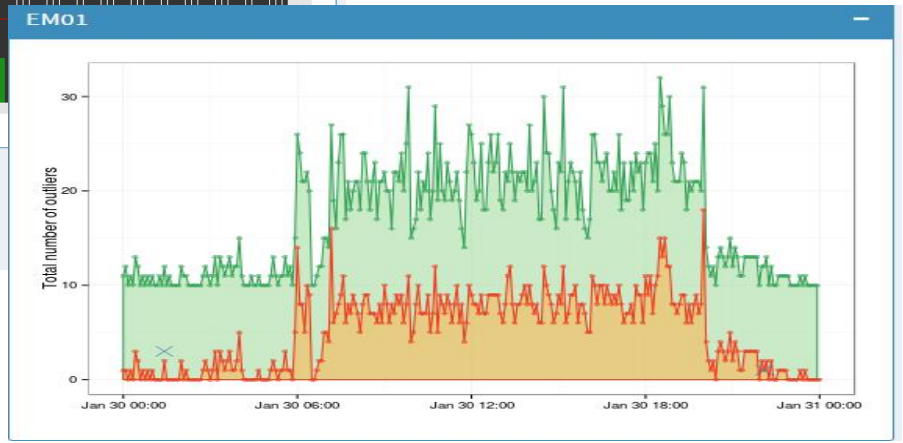


Dynamic Detection: ML Outliers

- Abundance of *normal* data. Little to no *outlier* data
- Train a one-class SVM using only normal data
- Group similar sensors and train a model for each sensor using only
- Early studies show good performance but modelling needs more work

Some Screenshots of SPARKS' Dashboard





Applying this Session

- Evaluate your current approach to responding to cyber threats in the light of the kinds of attacks we've discussed
- Identify an area in which security analytics could improve your ability to detect and respond to cyber attacks
  - Identify compromised end-user devices (eg, anomalies in behavior)?
  - Identify compromised servers (eg, evidence of beaconing)?
  - Identify lateral movement across your network (eg, anomalies in network traffic)?
- Prototype or pilot security analytics in that area

Thank you!

daniel.t.cohen@rsa.com
@iFraudFighter
www.linkedin.com/in/danieltcohen

robert.griffin@rsa.com
blogs.rsa.com/author/griffin
project-sparks.eu/blog/
@RobtWesGriffin
www.linkedin.com/pub/robert-griffin/0/4a1/608