



Cisco ETA

Encrypted Traffic Analytics, Introduction

Michal Svoboda

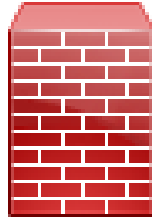
Cognitive Team Architect

Nov 28 2019



- Network Security
- Data Analytics
- Cognitive Team

What's inside your network?



Line of defense

Blocks **known** threats

*How do we reliably detect
malicious activity in the network?*

... without inspecting the content?

Website classification quiz

Legitimate OR malicious?

<https://statetraveling.com/go/u/0/r/1581>

Travel Worldwide With Us!

[Busta Rhymes Island in Shrewsbury, Massachusetts](#)

Search... Search

October 26, 2014 9:30 pm | Published by [Kevin](#) | [Leave a comment](#)

Busta Rhymes Island There is a small piece of land sticking out of a Shrewsbury, Massachusetts pond that doesn't seem to belong to anyone in particular, but, as 99% Invisible has reported, one local man is crusading to name the spot Busta Rhymes Island. The tiny, 40x40 outcropping has no official name, but Shrewsbury resident Kevin [...]

Recent Posts

- [Busta Rhymes Island in Shrewsbury, Massachusetts](#)
- [Old Muskego Church in Saint Paul, Minnesota](#)
- [The Forgotten Entrance to Clinton Hall in](#)

It depends

<https://statetraveling.com/go/u/0/r/1581>

- Click fraud activity (earning money through fake paid clicks)
- Fake site with bogus content
- Works selectively depending on the user

Which of these encrypted requests is malware?

<https://136.243.4.68>

<https://64.233.162.83>

Which of these encrypted requests is malware...

<https://136.243.4.68>

- Malware c&c and exfiltration (encrypted)

<https://64.233.162.83>

- Google Mail (encrypted)

Which of these is more legitimate?

<https://google.com>

<https://llanfairpwllgwyngyllgogerychwyrndrobwlllantysilioogogoch.co.uk>

Which of these is more legitimate...

<https://google.com>

- Used commonly by malware – connectivity check

<https://llanfairpwllgwyngyllgogerychwyrndrobwlllantysiliogogogoch.co.uk>

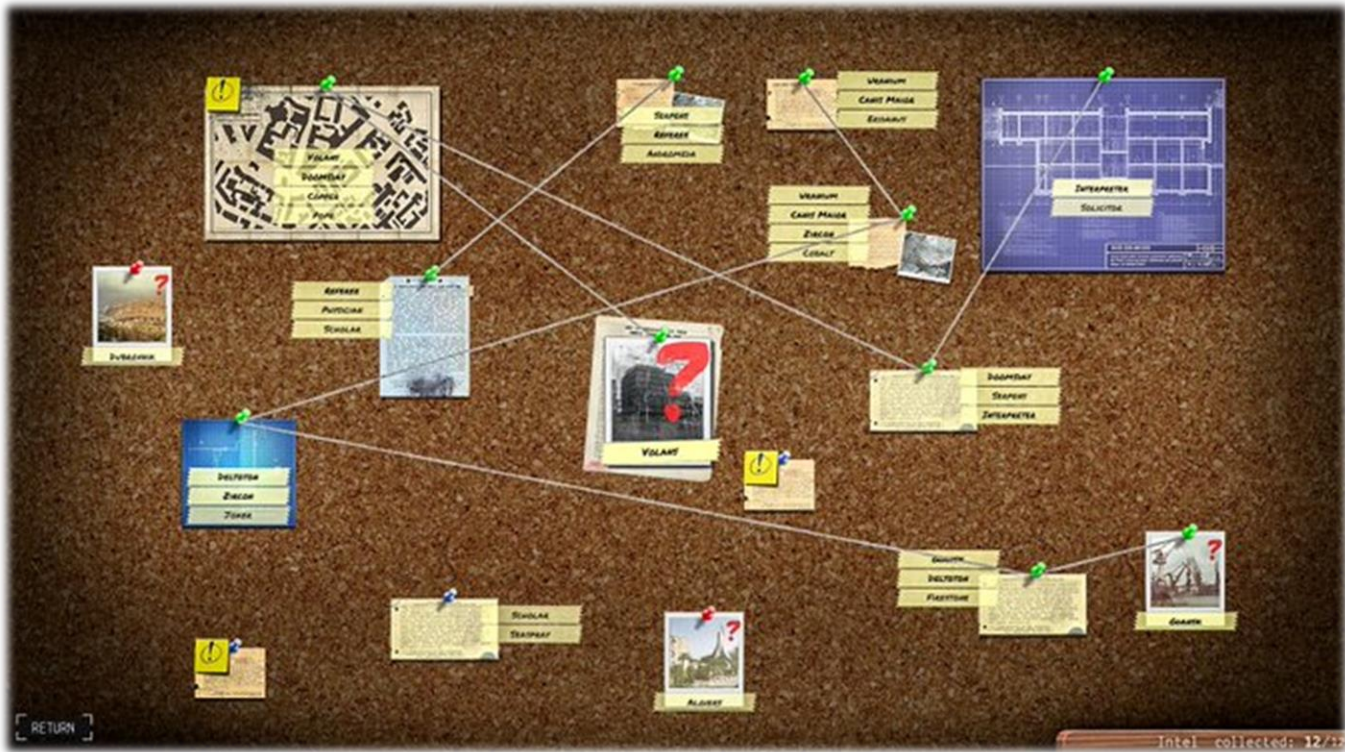
- Welsh village with the *longest* name in Britain

Lesson learned?

Cannot apply this type of thinking...



More like this...










ETA

Stealthwatch

Cognitive

What can we see on the network?

-  IP address
-  Data size
-  Time duration
-  Domain
-  Encryption parameters
-  URL
-  Content



What can we infer?



Do you visit this site often?



When do you work/sleep?



...



How many users go to this site?



When was it registered?



Who owns it?



...

Cognitive intelligence



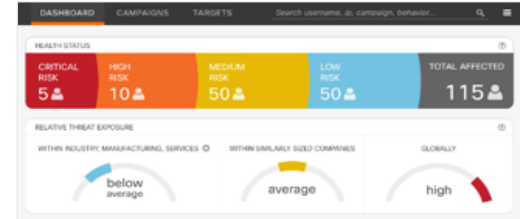
Network activity



Data points

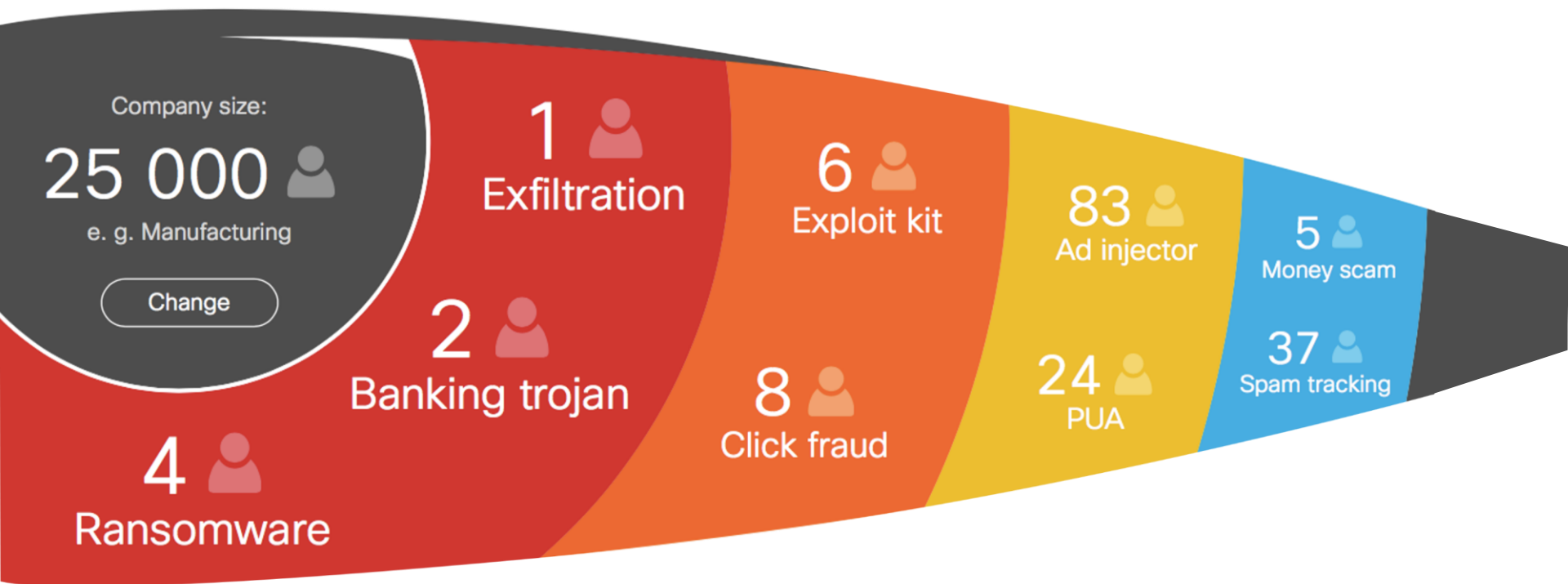


Automation



Intelligence + Alerts

Sample threat report



Further learning



