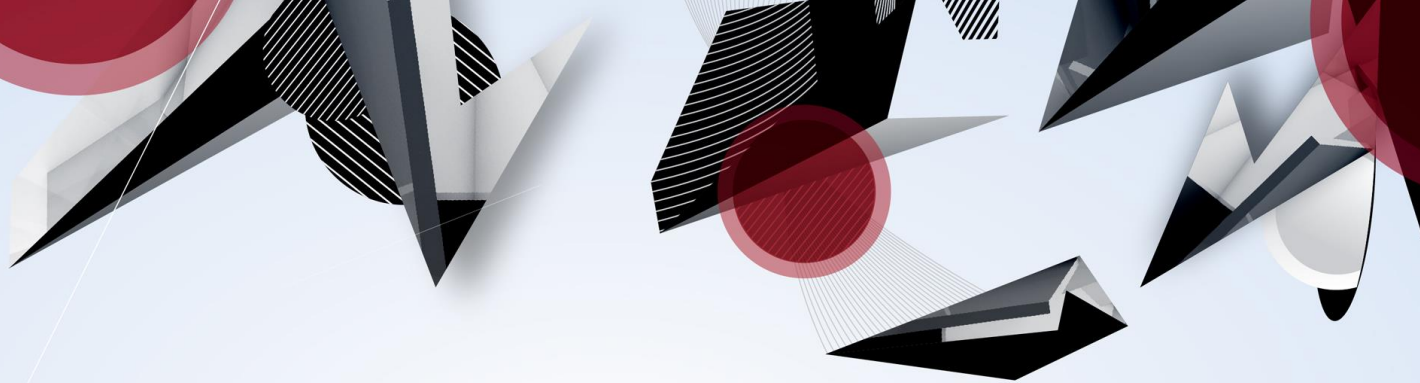


A Brief History of Attribution Mistakes

Sarah Jones

Principal Analyst at FireEye

whoami

- Principal Analyst at FireEye, 2018
- US Defense Industrial Base SOC, 2014-2018
- USG Legislative and Executive Branch SOCs, 2011-2014

- BA in International Relations, MA in Security Policy

- Disclaimer: personal opinions

whoami

- Principal Analyst at FireEye, 2018
- US Defense Industrial Base SOC, 20
- USG Legislative and Executive Bran

- BA in International Relations, MA in

whoami

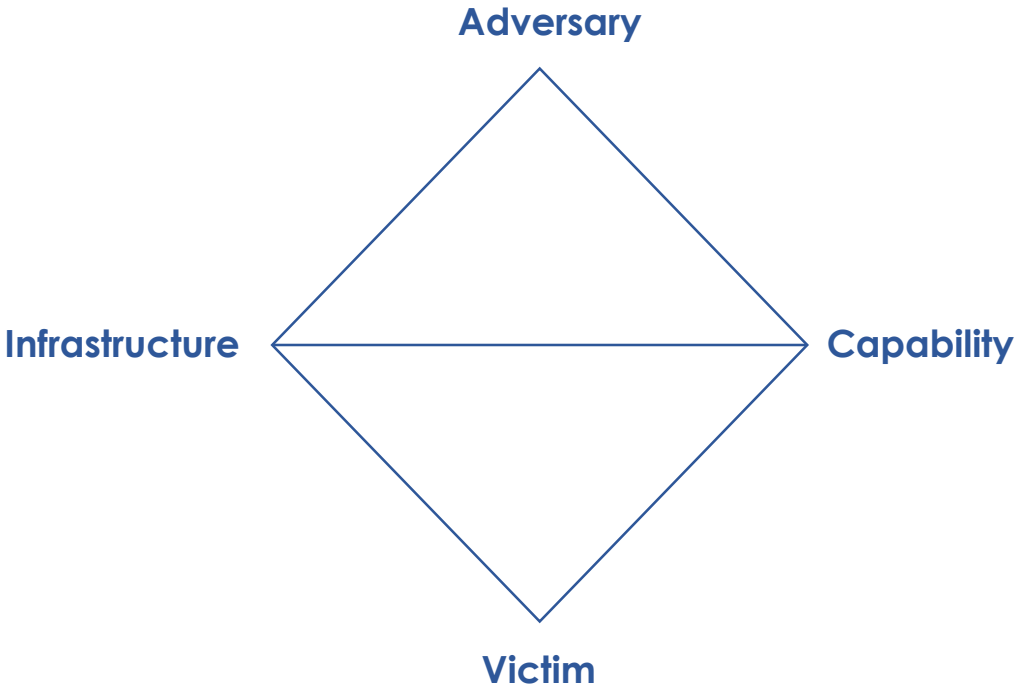
- Principal Analyst at FireEye, 2018
- US Defense Industrial Base SOC, 20
- USG Legislative and Executive Bran
- BA in International Relations, MA in

Goals

- Examine analytic mistakes
- Identify the root causes and cognitive biases
- Highlight successes
- Practical takeaways

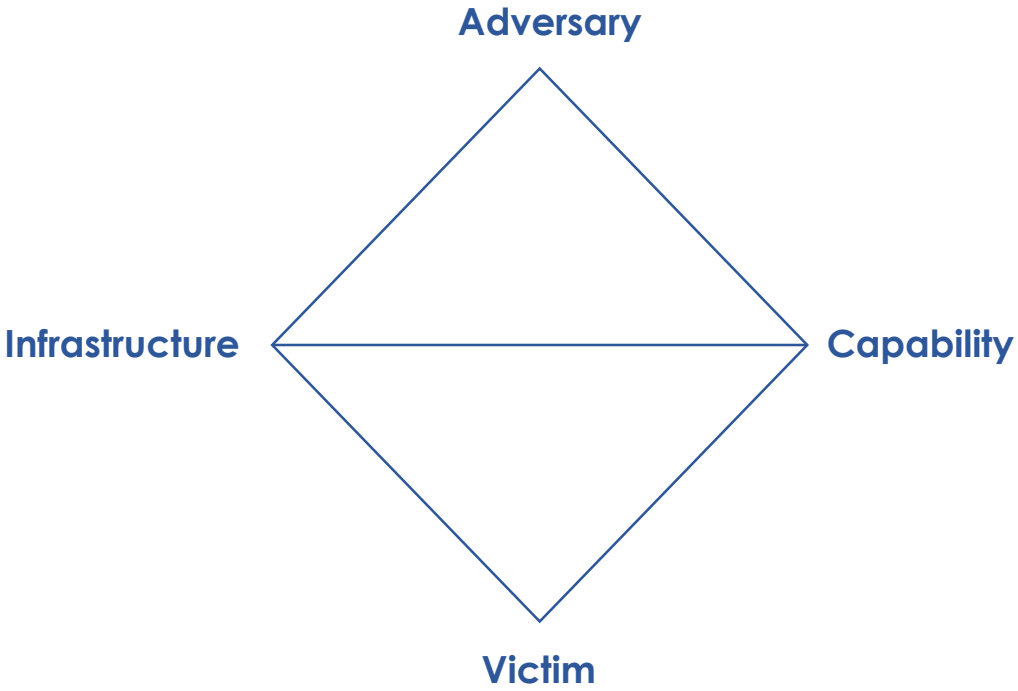
- Not: Naming and shaming

Using the Diamond Model



Using the Diamond Model

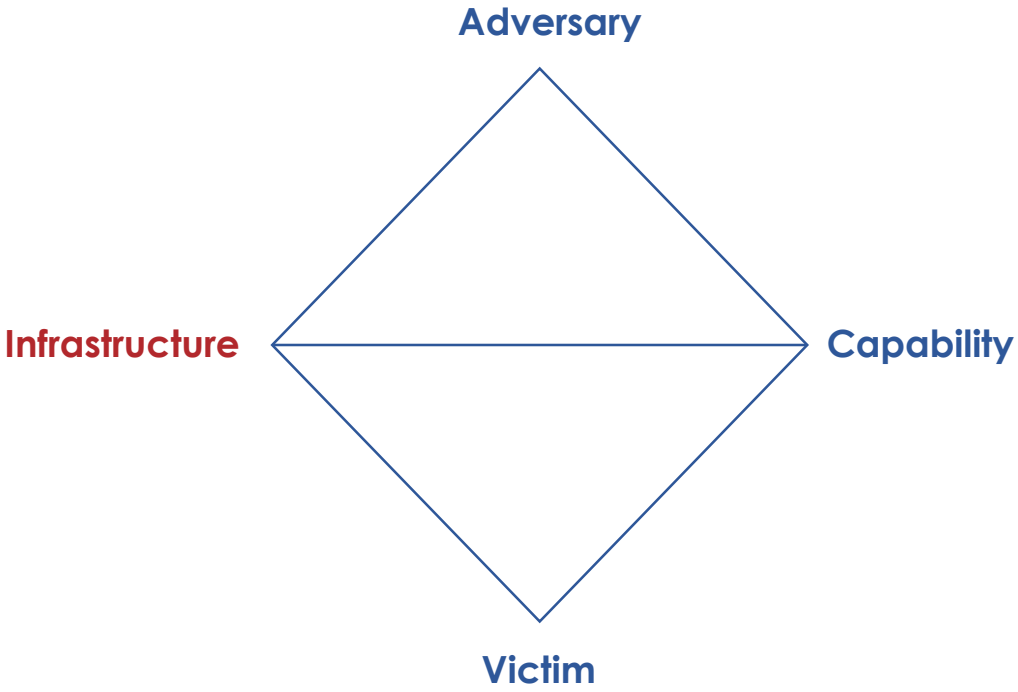
- Overreliance on
  - Infrastructure Centric Analysis
  - Capability Centric Analysis
  - Victim Centric Analysis
- Cognitive biases in
  - Adversary Analysis
- Lessons Learned



Infrastructure Centric Analysis

Correctly Interpreting Data

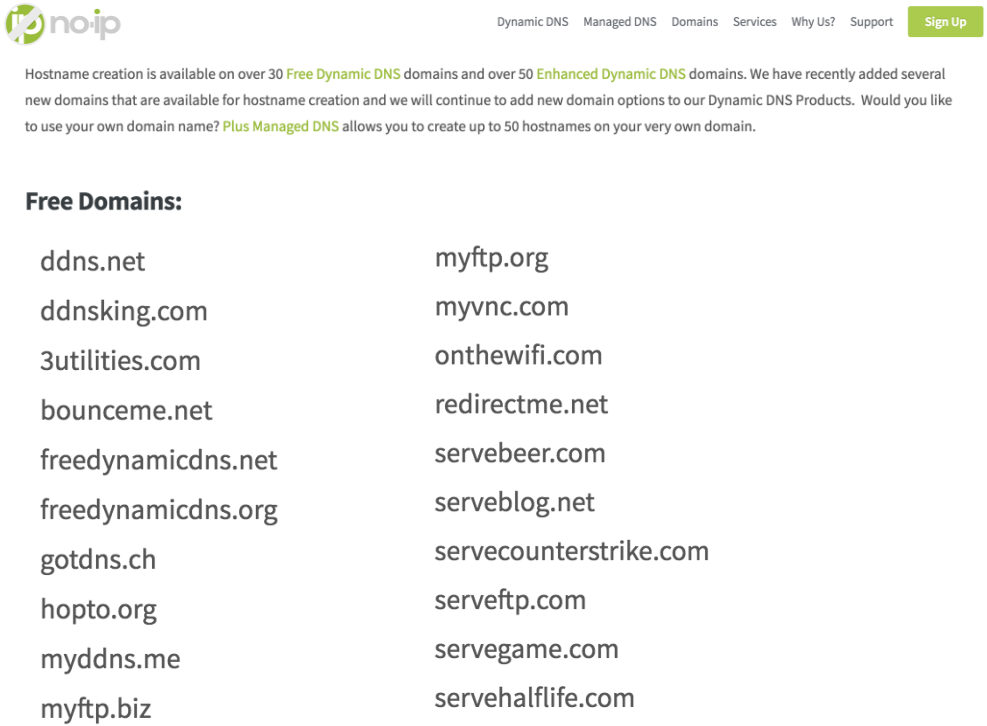
- Basic Research Mistakes



Infrastructure Centric Analysis

Correctly Interpreting Data

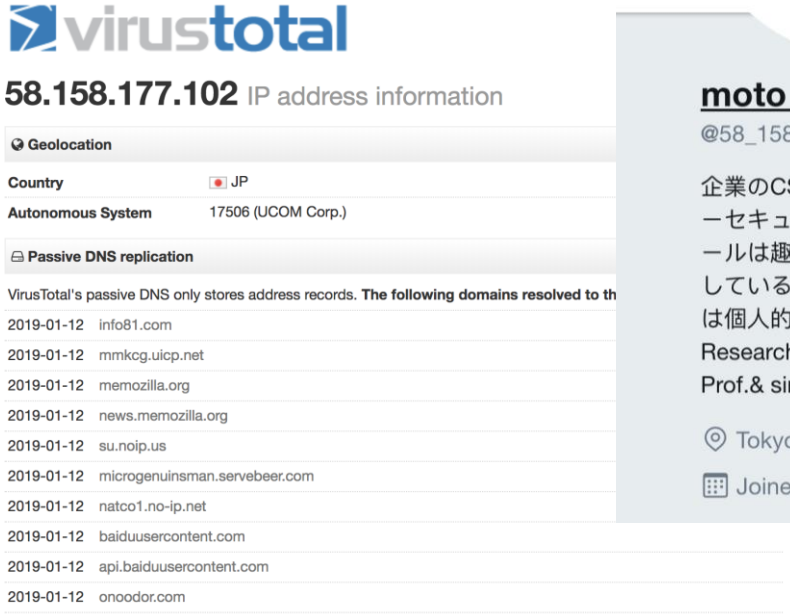
- Basic Research Mistakes
  - Dynamic DNS



Infrastructure Centric Analysis

Correctly Interpreting Data

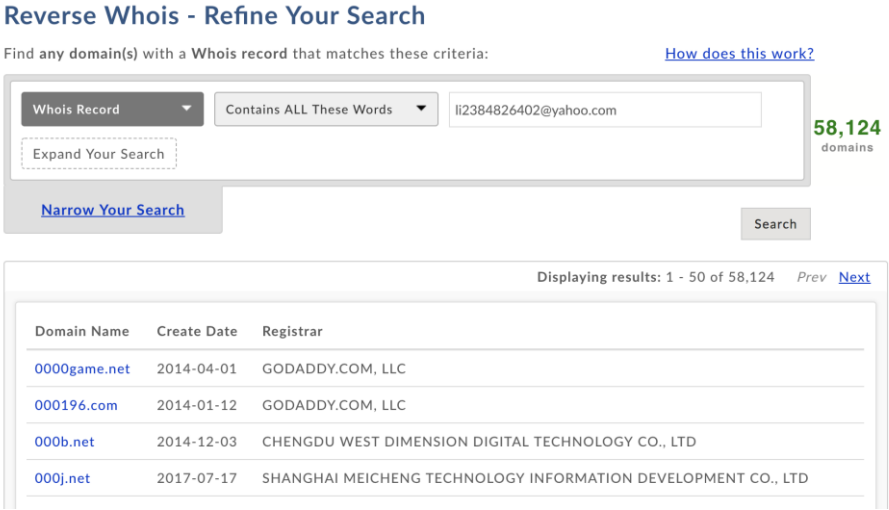
- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes



Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers



Leveraging ThreatConnect's WHOIS function, we identified the malware's hardcoded command and control domain adobesys[.]com was registered by the Chinese domain reseller and mass registrant, li2384826402[@]yahoo[.]com. This email address is infamous for registering domains used in the DEEP PANDA-attributed Anthem and OPM attacks in 2015, and provides additional evidence tying this HttpBrowser activity to Chinese APT actors.

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space

Bloomberg BusinessWeek: Portrait of a Chinese Hacker

Some of the addresses had also figured in Chinese espionage campaigns documented by other researchers. They were part of a block of about 2,000 addresses belonging to China Unicom, one of the country's largest Internet service providers. Trails of hacks had led Stewart to this cluster of addresses again and again, and he believes they are used by one of China's top two digital spying teams, which he calls the Beijing Group. This is about as far as Stewart and his fellow detectives usually get—to a place and a probable group, but not to individual hackers. But he got a lucky break over the next few months.

phoned home to a command node at AlexaUp.info. The billing name used in the registration: Zhang Changhe. Stewart says Zhang is affiliated with the Beijing Group, which probably involves dozens of people, from programmers to those handling the infrastructure of command centers to those who translate stolen documents and data. As Stewart discusses this, his voice is flat. He's realistic. Outing one person involved in the hacking teams won't stop computer intrusions from China. Zhang's a cog in a much larger machine and, given how large China's operations have become, finding more Zhangs may

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps

Disobedient Media
Truth has no bias

Front Page | Global Chess | American Affairs | Media & Tech

December 26, 2017 Adam Carter

Anomalies Discovered In Malware Found By CrowdStrike Merit Further Inspection

It's amazing what people retain and how they pick up on conflicts of information and inconsistencies. I've been impressed by a lot of people I've come to know through Twitter and one great example is Stephen McIntyre *(of Climate Audit – a blog that has an interesting history of its own in relation to the ClimateGate hack of 2009).*

Over recent months McIntyre has given some attention to the topic of the alleged hacking of the DNC in 2016 and his findings have been particularly interesting, at least, to anyone interested in unraveling digital deception.

As always, some of the background helps for context, if you're familiar with CrowdStrike's activity at the DNC, their background and the dates of their activities, feel free to skip the next couple of paragraphs.

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps

Disobedient Media
Truth has no bias

Front Page | Global Chess | American Affairs | Media & Tech

December 26, 2017 Adam Carter

Anomalies Discovered In Malware Found By CrowdStrike Merit Further Inspection

It's amazing what people retain and how they pick up on conflicts of information and inconsistencies. I've been impressed by a lot of people I've come to know through Twitter and one great example is Stephen McIntyre *(of Climate Audit – a blog that has an interesting history of its own in relation to the ClimateGate hack of 2009).*

Over recent months McIntyre has given some attention to the topic of the alleged hacking of the DNC in 2016 and his findings have been particularly interesting, at least, to anyone interested in unraveling digital deception.

Some of the sources of ITW dates errors are:

* When a user uploads the file on www.virustotal.com there is some javascript to check the creation time on the computer, if the date is wrong the wrong time gets set
* There are some 3rd party utilities that send file creation timestamps eg sysinternals that also might have the date wrong.

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps

Disobedient Media
Truth has no bias

Front Page | Global Chess | American Affairs | Media & Tech

December 26, 2017 Adam Carter

Anomalies Discovered In Malware Found By CrowdStrike Merit Further Inspection

Nick Carr @ItsReallyNick · 31 May 2018

Replying to @pat_r10t @QW5kcmV3 and 3 others

One interesting takeaway for me, while maybe not applicable for this file, is that @virustotal seemingly runs client-side javascript to identify file creation times from uploaded files.

Some of the sources of ITW dates errors are:

* When a user uploads the file on www.virustotal.com there is some javascript to check the creation time on the computer, if the date is wrong the wrong time gets set
* There are some 3rd party utilities that send file creation timestamps eg sysinternals that also might have the date wrong.

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps
  - Name Servers and Registrars

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps
  - Name Servers and Registrars

May 10, 2015 root9B: The Threat Defiance Report

APT28 TARGETS FINANCIAL MARKETS

ROOT9B RELEASES ZERO DAY HASHES

Evidence of intrusion within client networks pointed to a specific server, CARBON2U.COM, that had been previously linked to malicious activity and identified by other security firms as part of the infrastructure utilized by the Sofacy group. Analysts studied the remaining domains registered on that server, and initially noted that one in particular, CBIUAEBANK.

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps
  - Name Servers and Registrars
  - Scans are not attacks

Infrastructure Centric Analysis

Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps
  - Name Servers and Registrars
  - Scans are not attacks

THE GROWING CYBERTHREAT FROM IRAN

THE INITIAL REPORT OF PROJECT PISTACHIO HARVEST

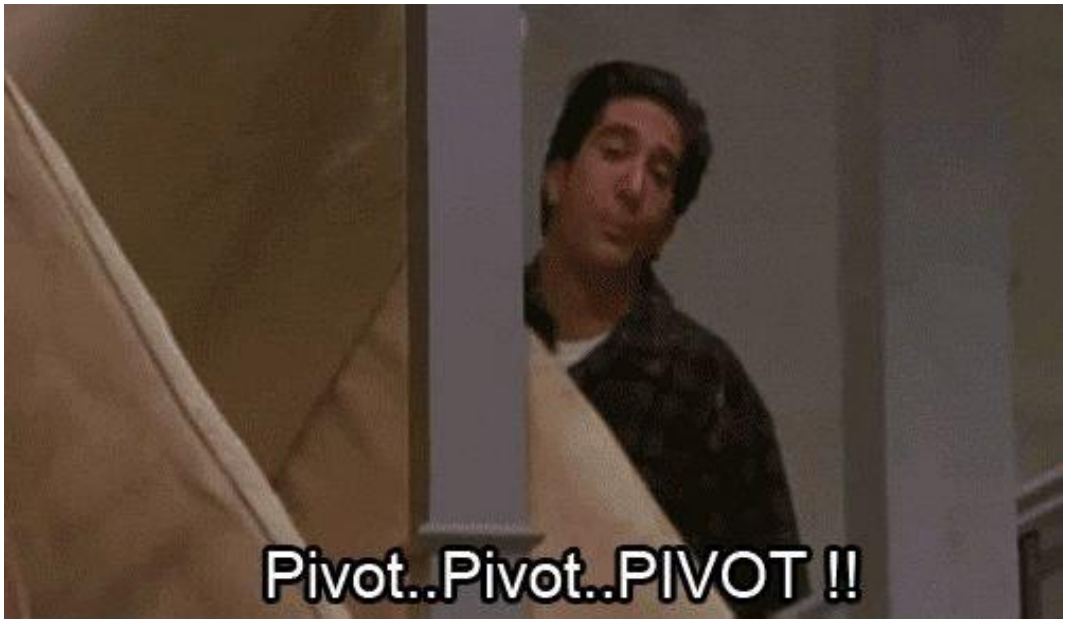
NORSE LIVE ATTACK MAP DEMONSTRATES ATTACKS DETECTED AGAINST 8 MILLION SENSORS

Note: Image captured on April 5, 2015.

Infrastructure Centric Analysis

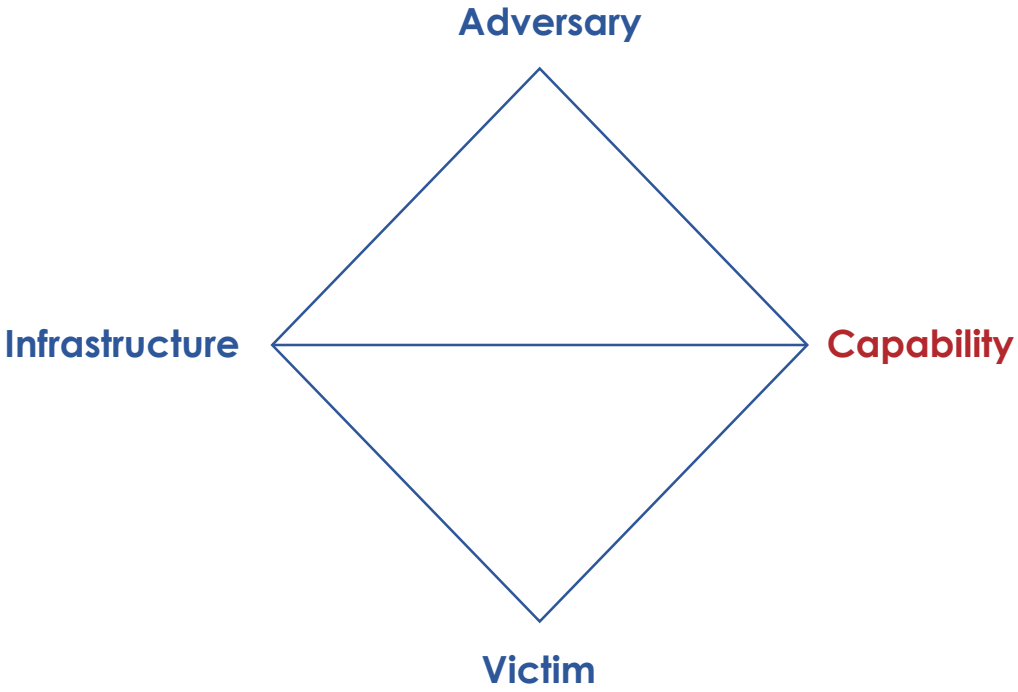
Correctly Interpreting Data

- Basic Research Mistakes
  - Dynamic DNS
  - Sinkholes
  - Domain resellers
  - IP Egress Space
  - VT timestamps
  - Name Servers and Registrars
  - Scans are not attacks



Capability Centric Analysis

Overestimating Uniqueness



Capability Centric Analysis

Overestimating Uniqueness

Capability Centric Analysis

Overestimating Uniqueness

Capability Centric Analysis

Overestimating Uniqueness

- Malware

Capability Centric Analysis

Overestimating Uniqueness

- Malware

SUPPLY CHAIN ANALYSIS:

From Quartermaster to SunshopFireEye

Shared development and logistics

Examining the 11 APT campaigns revealed a shared development and logistics operation used to support several APT actors in distinct but overlapping campaigns. This development and logistics operation is best described as a "digital quartermaster." Its mission: supply and maintain malware tools and weapons to support cyber espionage. This digital quartermaster also might be a cyber arms dealer of sorts, a common supplier of tools used to conduct attacks and establish footholds in targeted systems.

Capability Centric Analysis

Overestimating Uniqueness

- Malware
- Builders

Shared Builders

These observed shared characteristics across these malware samples are likely the result of a set of common "builders" developed by a shared development and logistics infrastructure.

Builders are tools used by malicious actors to quickly and easily create different variants of the same malware. In a typical scenario, a skilled developer creates a builder and shares it with an operator more skilled in intrusion operations than in code development. This separation of tasks is more efficient and supports a faster tempo of offensive operations. A typical builder provides a graphical user interface that enables a threat actor to configure elements such as the location of the CnC server.

To recap, these shared characteristics, as discussed in previous sections, include the following:

- The Sunshop and DTL PE resources
- Common import tables
- Six different digital certificates
- Common compile times
- Common malware families

Capability Centric Analysis

Overestimating Uniqueness

- Malware
- Builders
- Exploits

Capability Centric Analysis

Overestimating Uniqueness

- Malware
- Builders
- Exploits

The Italian Connection:

An analysis of exploit supply chains and digital quartermasters

In this paper we will focus on two exploits which at the time of discovery in the Hacking Team archives were unpatched. The two 0-days in question targeted Adobe Flash and were subsequently labeled CVE-2015-5119[1] and CVE-2015-5122[2].

The goal of this research is to demonstrate how quickly these exploits spread and were used by multiple independent cyber espionage operators.[3] Via the evidence presented within this paper we will demonstrate that at least two different exploit kits, or generators, were constructed by an unknown entity and shared amongst multiple operators believed to be located in China. We believe the following is a clear example of yet another 'digital quartermaster' of cyber espionage tools.

	One Quartermaster	Shared Generators	Shared Code
HT_Exploit	valid explanation	valid explanation	invalid explanation
flash_exploit_002	valid explanation	valid explanation	invalid explanation
exp1_fla	invalid explanation	invalid explanation	valid explanation
exp2_fla	invalid explanation	invalid explanation	valid explanation
movie_fla	invalid explanation	invalid explanation	valid explanation

Table 15: Competing Hypotheses

Capability Centric Analysis

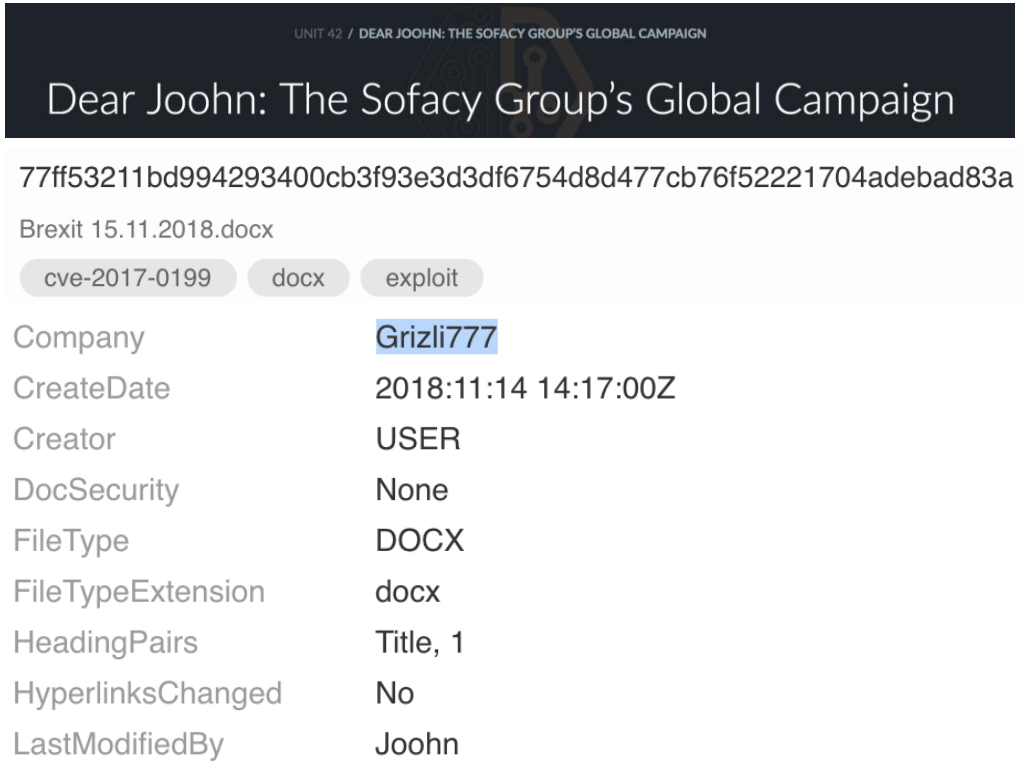
Overestimating Uniqueness

- Malware
- Builders
- Exploits
- Build Environments

Capability Centric Analysis

Overestimating Uniqueness

- Malware
- Builders
- Exploits
- Build Environments



Capability Centric Analysis

Overestimating Uniqueness

- Malware
- Builders
- Exploits
- Build Environments

UNIT 42 / DEAR JOOHN: THE SOFACY GROUP'S GLOBAL CAMPAIGN

Dear Joohn: The Sofacy Group's Global Campaign

77ff53211bd994293400cb3f93e3d3df6754d8d477cb76f52221704adebad83a

Brexit 15.11.2018.docx

cve-2017-0199 docx exploit

Company	Grizli777

Members
37 posts

Posted 16 July 2012 - 08:09 PM

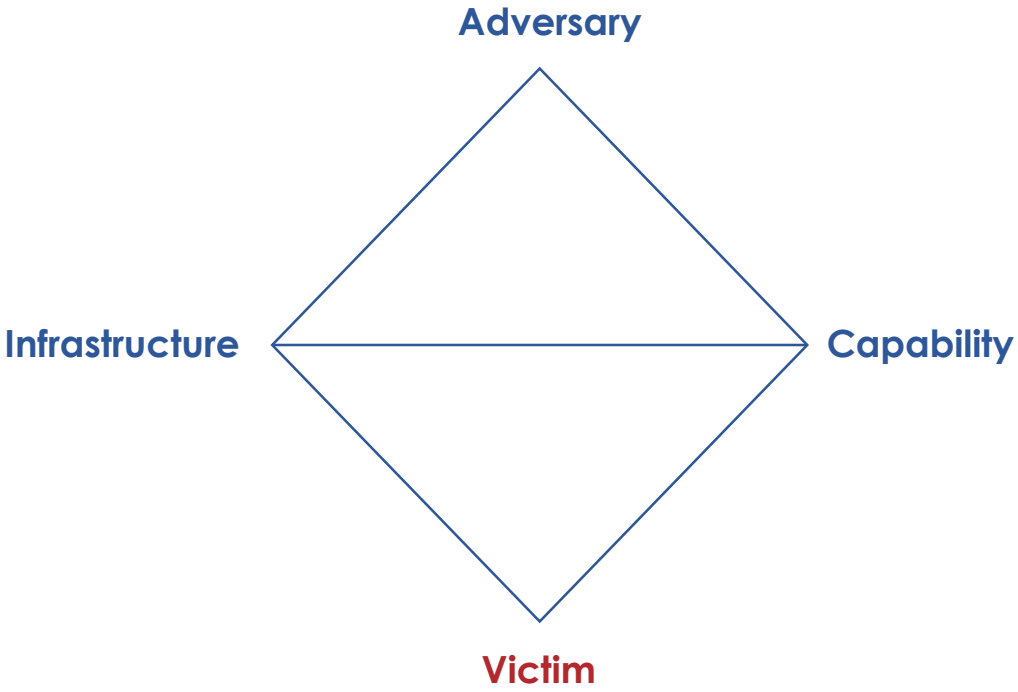
I bought a copy of Office 2007 about a year ago on eBay, and am starting to suspect that it is not a legitimate copy. I noticed today that the company name for all the documents I've created since last year is Grizli777, which apparently is one potential indication of a pirated copy. My questions are:

1.) Is there a way to confirm for certain that my copy of Office 2007 is counterfeit? I don't have the CD or packaging on hand, unfortunately.
2.) If I were to buy a genuine copy of Office and uninstall what I have now, would there then be any issue opening the documents that I've created in the last year using the (supposedly) pirated copy?

FileTypeExtension	docx
HeadingPairs	Title, 1
HyperlinksChanged	No
LastModifiedBy	Joohn

Victim Centric Analysis

Cognitive Traps



Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry

Victim Centric Analysis

Cognitive Traps

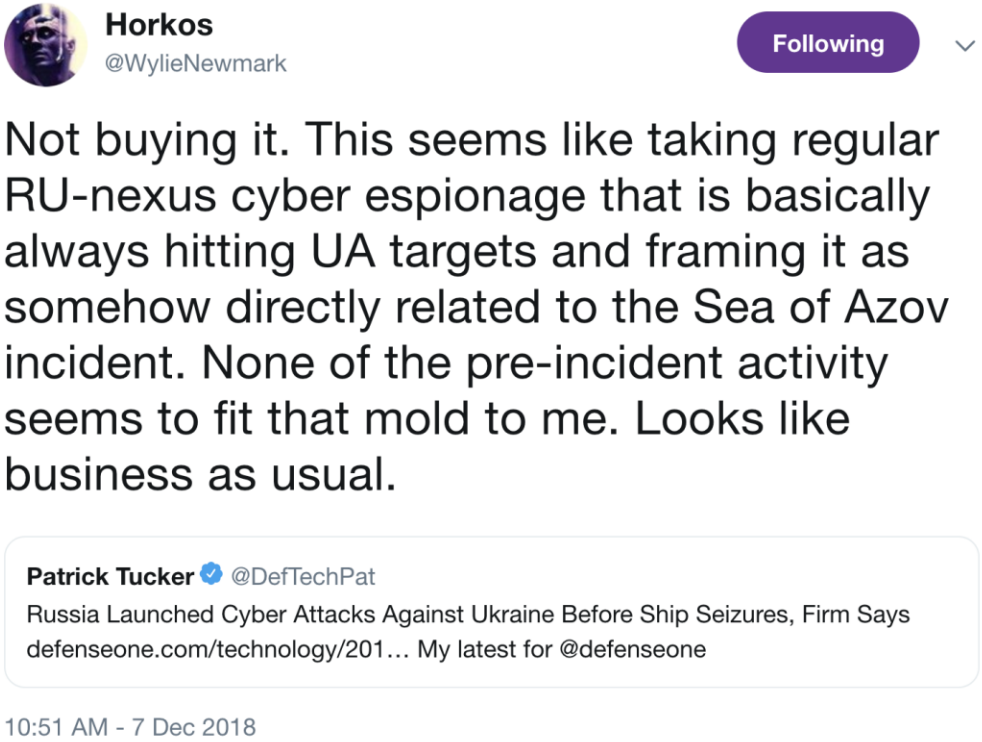
- Collection Bias
  - Telemetry

Taidoor malware, detected by Trend Micro as BKDR_SIMBOT variants, have been historically documented for their use in targeted attacks. Using techniques developed to match the network traffic Taidoor malware generate when communicating with a command-and-control (C&C) server, we were able to identify victims that these appeared to have compromised. All of the compromise victims we discovered were from Taiwan, the majority of which were government organizations.

Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc



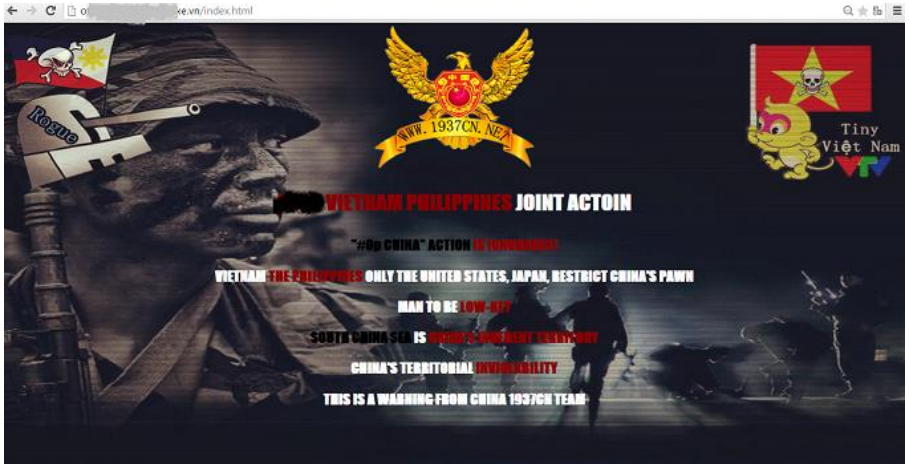
Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc
  - Cum hoc ergo propter hoc

China 1937CN Team hackers attack airports in Vietnam

July 31, 2016 By Pierluigi Paganini



Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc
  - Cum hoc ergo propter hoc

China 1937CN Team hackers attack airports in Vietnam

The campaign was uncovered when two malicious documents exploiting CVE-2012-0158 were submitted to Virus Total in early August. After following the breadcrumbs, researchers uncovered more than a dozen malicious domains being used for C&C activities. Some of them, such as dcsvn[.]org (a spoof of the website of the Vietnam Communist Party), have been active since 2015.

It's this same website that provides the link to 1937CN. In 2016, Vietnam's flagship airline was the victim of a coordinated attack in which malware was installed on the administrator's machine for espionage and remote access. The airline's website was defaced and its homepage replaced with a message from the 1937CN group, and data for more than 400,000 frequent flier enrollees to its Golden Lotus program was leaked online. At the same time, audio and screen systems at Tan Son Nhat and Noi Bai, the two biggest airports in Vietnam, were modified to spread political messages.

Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc
  - Cum hoc ergo propter hoc
- Anchoring
  - Primary vs Secondary Targets

Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc
  - Cum hoc ergo propter hoc
- Anchoring
  - Primary vs Secondary Targets

Privileges and Credentials: Phished at the Request of Counsel

June 06, 2017 | by Ian Ahl

Summary

In May and June 2017, FireEye observed a phishing campaign targeting at least seven global law and investment firms. We have associated this campaign with APT19, a group that we assess is composed of freelancers, with some degree of sponsorship by the Chinese government.

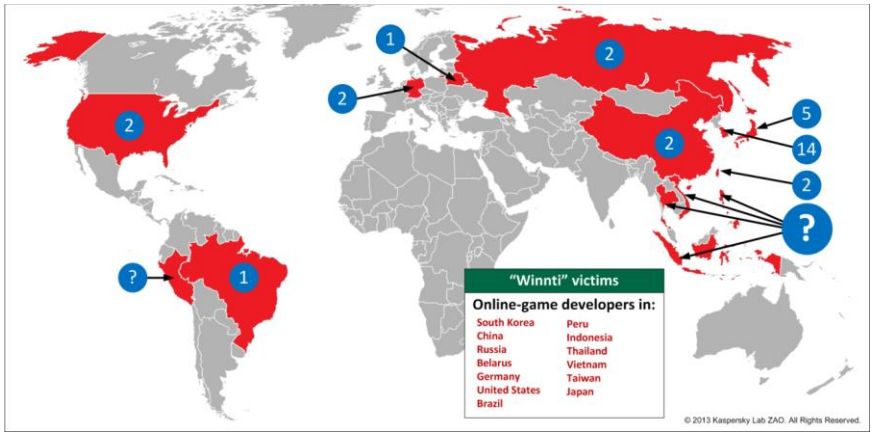
Victim Centric Analysis

Cognitive Traps

- Collection Bias
  - Telemetry
- Correlation != Causation
  - Post hoc ergo propter hoc
  - Cum hoc ergo propter hoc
- Anchoring
  - Primary vs Secondary Targets

Winnti. More than just a game

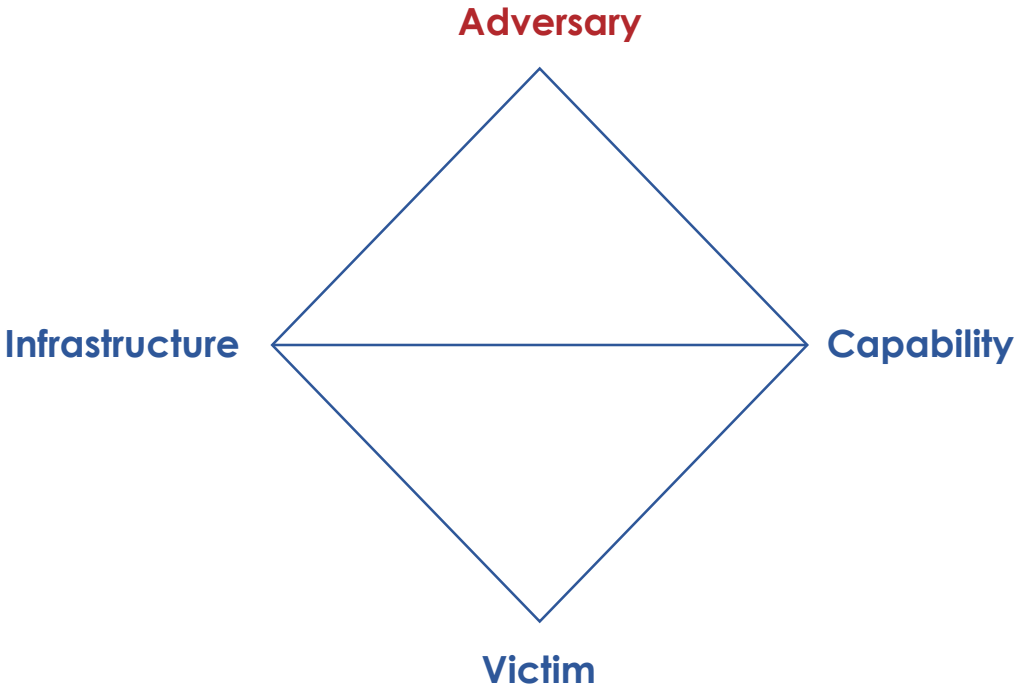
By GReAT on April 11, 2013. 5:00 pm



Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias



Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

27 MAR 2017

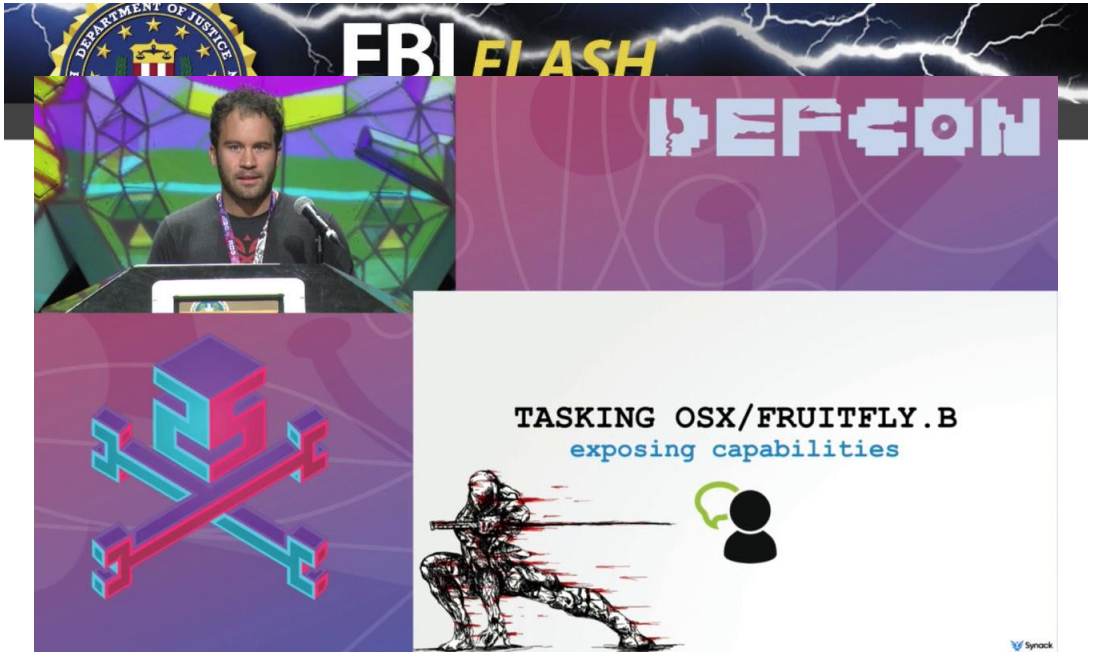
Alert Number

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly



Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly

Wardle said based on the target victims, the malware is less likely run by a nation state attacker, and more likely operated by a single hacker "with the goal to spy on people for perverse reasons." He wouldn't say how many were affected by the malware, but suggested it wasn't widespread like other forms of malware.

Adversary Centric Analysis

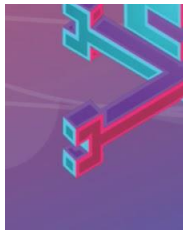
Cognitive Traps

- Anchoring Bias
  - FruitFly

The road from computer whiz to creepy hacker: North Royalton man accused of spying on thousands

Updated Feb 27, 2018; Posted Feb 26, 2018

Wardle said based on the tar
attacker, and more likely ope
perverse reasons." He would
it wasn't widespread like othe
sted



Feds say North Royalton hacker attacked Mac computers

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea

Adversary Centric Analysis

Cognitive Traps

- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea

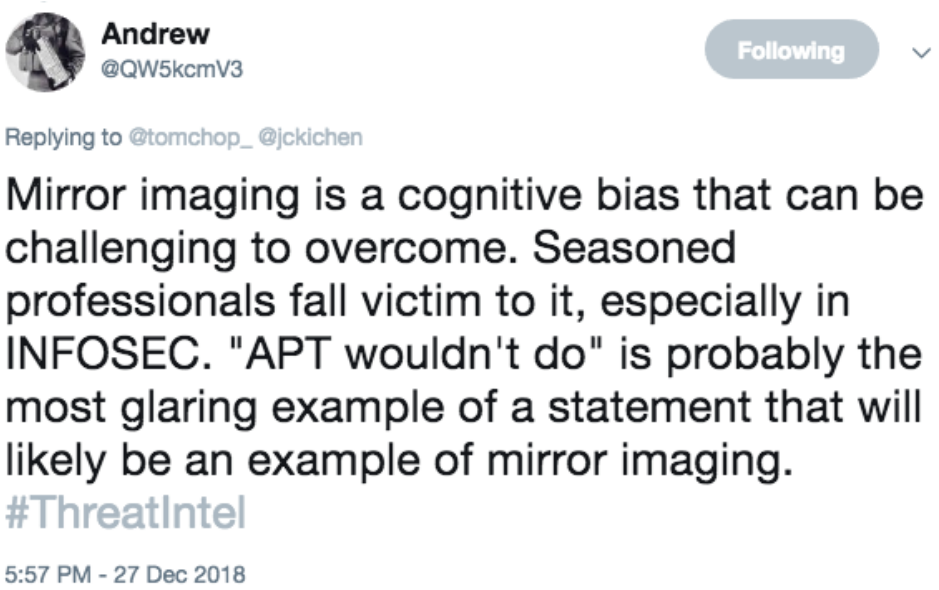
DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male

Adversary Centric Analysis

Cognitive Traps

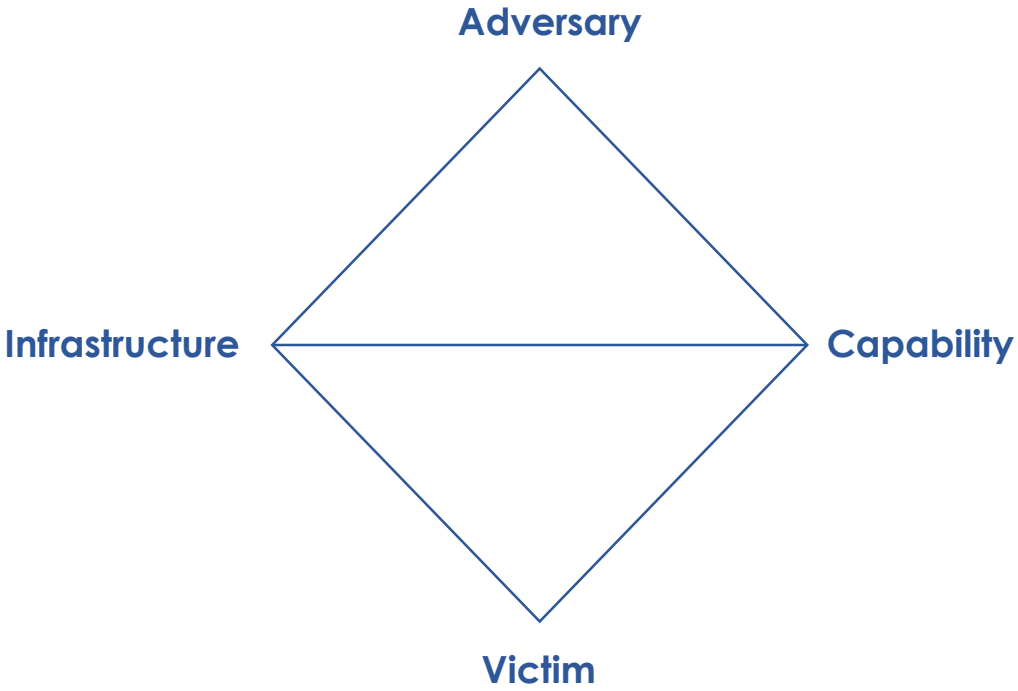
- Anchoring Bias
  - FruitFly
- Mirror Imaging
  - North Korea



Conclusions

Lessons Learned

- Acknowledge limitations of data
- Acknowledge preexisting ideas
- Correct for analytic biases by gathering context about adversaries



FireEye

Thank You