Actionable Threat Intelligence:
The Intelligence Life Cycle

(plus some thoughts on Wannacry / Petya)

Adrian Culley
Consulting Engineer
Threat Intelligence and Malware
Palo Alto Networks

Actionable Threat Intelligence

- *Intelligence that not only **can**, but also **should**, be acted upon.*

The Intelligence Life Cycle Concepts:

Ignorance	We know nothing
Data	We know something
Information	We know something about what we know
Knowledge	What we know is useful
Intelligence	What we know is actionable
Wisdom	What we know is actionable in the future

("Joint Publication 2-0, Joint Intelligence" (PDF). *Defense Technical Information Center (DTIC)*. Department of Defense. 22 June 2007.)

CONTEXT CORROBORATION ANALYSIS

Targeted attack challenges

VOLUME

Increased attack volume from automated adversaries

ALERTS

Too many alerts from too many sources without context

COMPLEXITY

Highly manual response with complex workflows

Increased Attack Volume

Too Many Alerts, No Context: Data is useless without context

Three Key Concepts:

1. Context
2. Corroboration
3. Complexity (increases Vulnerability, increases Exploits)

Intelligence Life Cycle expanded…..

Analysis

Ignorance
Data
Information
Knowledge
Intelligence
Wisdom

Context

Grading and Weighting

Mathematics: Probability, Statistics, Data Mining, Data Modelling, Predictive Analytics.

Tacit Knowledge

CORROBORATION

CAUTION!! ATTRIBUTION IS HARD

Metrics for success

TIME TO IDENTIFICATION

Decrease time to identify new, targeted attack

TIME TO ERADICATION

Speed mitigation without adding specialized staff

Threat Intelligence Layers: Context and Corroboration

Threat Actors

Threat Campaigns

Threat Techniques

Individual Breaches (Specific Binaries, Exploit Kits)

Responsiveness is Key

Malware Analysis: A very quick, exhaustive guide

Static (Automatic)

Dynamic (Automatic)

Bare Metal (Automatic and Manual)

Artificial Intelligence

Machine Learning

Predictive Analytics (future)

Data Mining (past)

“There are no silver Bullets”

Why?

Prevent (Known)

Detect (Unknown)

Prevent (Known)

You can buy many things, you cannot buy more time.

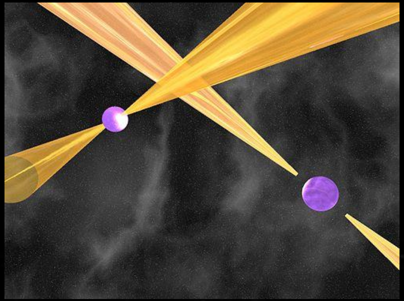
Wannacry and Petya Attacks: Some Thoughts

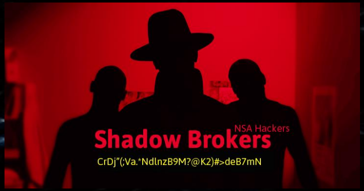
Smoke (Ransomware)

&

Fire (Exploits)

DOUBLEPULSAR
ETERNALBLUE





PSR J0737-3039

Thank you

谢谢