Automated cyber-security intelligence (ASI)

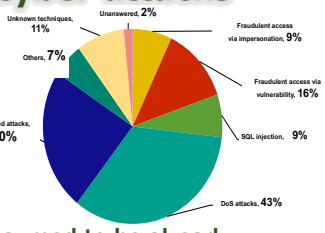
Faculty of Engineering and Design, Kagawa University. Association Prof. KIDA KOJI
Email: kida.koji@kagawa-u.ac.jp

Introduction

No approach can 100% prevent cyber attacks

Increasingly sophisticated cyber attacks

Insufficient security patch application that handles basic cyberattacks only



Malware should be assumed to be already in your system.

Concept

Change the game

Lack of capability to uncover the whole picture of attacks

Attacking techniques evolve continuously, it is hard for defenders to overtake attackers.

e.g.)
- Pattern match
- Behavioral analysis
- Sandbox test

We will "know" our system completely for finding different status than usual in order to detect enemies indirectly.

孫子

知彼知己，百戦不殆

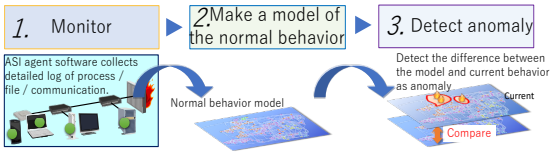
"knowing the enemy and yourself will get you unscathed through a hundred battles "

Technology

Data-mining for anomaly detection

Detect unknown attacks by understanding system and analyzing changes and isolate attacked area automatically

- Automatically make a model of the normal behavior of the system by learning the system behavior from detailed logs collected from endpoints
- No need for manual settings or domain knowledge
- Compare the model and current system behavior and detect abnormal behavior, which could lead to cyber attack detection



Malware detection evaluation

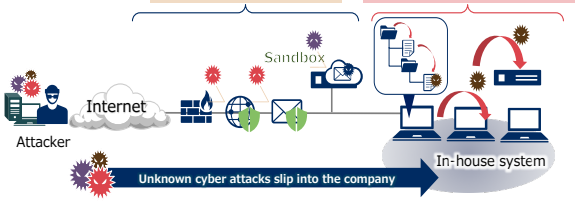
unknown malware			Conventional AV-software		AI based AV-Software	
Malware	拡張子	Our system	Product S	Product D	Product C	Product F
Specimen-1	exe	NG	NG	NG	✓	NG
Specimen-2	lnk	✓	NG	NG	NG	NG
Specimen-3	exe	✓	NG	NG	✓	NG
Specimen-4	exe	NG	NG	NG	NG	NG
Specimen-5	xls	✓	NG	NG	NG	NG
Specimen-6	exe	✓	NG	NG	✓	NG
Specimen-7	doc	✓	NG	NG	NG	✓
Specimen-8	doc	✓	NG	NG	NG	NG
Specimen-9	exe	✓	NG	NG	✓	NG
Specimen-10	lnk	✓	NG	NG	NG	NG
Total		80%	0 %	0%	40%	10%

Operation

Change of operation

Conventional manner
Prevention of infection
(EPP: Endpoint Protection)

Our manner
Detect attack activities inside the system
(EDR: Endpoint Detection and Response)



Case studies

Reduce time to analyze an alert

5 days -> 1.5 hrs

Finding evidences of malware execution in endpoints, infection routes, impacts

Analyst — **Before** No idea where the needle is in a haystack (Big Data)

ASI — **After** Just start with something different from normal

Unknow attack detection

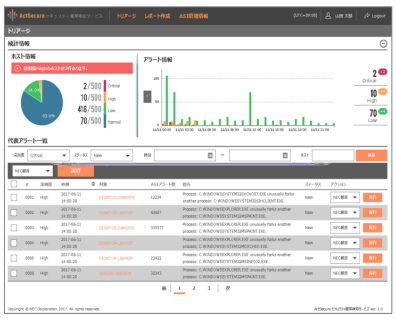
100% detection

Directly detected 80% of the malware and the rest was found as abnormal behavior of the system.

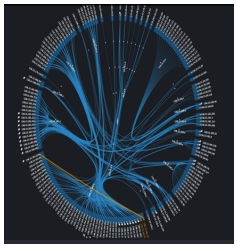
Traditional Anti-virus — **Before** Signatures no longer works against APT malware.

ASI — **After** Detect something different probably caused by an attack

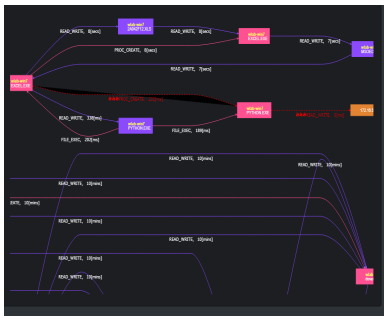
Screen Shots



Dashboard



System blueprint



Analyzing tool