Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis (NECOMA Project)

Director : Youki Kadobayashi
Nara Institute of Science and Technology

Presentator : Yuji Sekiya
The University of Tokyo
Consortium Members

Hervé Debar (EU lead)

Youki Kadobayashi (Japan lead)

Dawid Machnicki

Kenjiro Cho

Sotiris Ioannidis

Akira Kato

Piotr Kijewski

Romain Fontugne

Jouni Viinikka

Yuji Sekiya
# The Goals of NECOMA Project

## Existing Research

<table>
<thead>
<tr>
<th>Description</th>
<th>NECOMA</th>
<th>Expected Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focused to data collection and threat detection.</td>
<td>Focused to threat mitigation and resilience of system.</td>
<td>Actionable Information</td>
</tr>
<tr>
<td>Focused to detection of the particular threats.</td>
<td>Detection threats as mixture of incidents. Multilayer Analysis</td>
<td>Advanced defense mechanism.</td>
</tr>
<tr>
<td>No tight relations among data collection, analysis, and defense.</td>
<td>Pipeline and Automation.</td>
<td>Pipeline from data collection to mitigation.</td>
</tr>
</tbody>
</table>
Multi-layer Threat Analysis

Threat analysis (detection) across multiple datasources

Analysis 1

Analysis 2

Analysis 3

Victim side action
Filtering
Load balancing
Isolation

Countermeasure for Attackers
Report to ISP
Announce to users
Filtering at ISP level
Configuration to servers

Threat Information Share
Among organizations
Announce to public

Data collection at
Multiple layers/locations

Analysis Platform

Network device

Servers

Users Device
Security Information Pipeline

- Making pipeline through divert activities
  - Data collection (Traffic, User behavior, etc)
  - Threat Analysis
  - Human decision
  - Protection (Enforcement)
NECOMA Eco-System

- Operators can consider and decide the appropriate action based on the information posted to NECOMAter
  - Automatic defense based on posts
  - Manual defense by posting
- Defense modules watch the posted information and take actions in multi-places

- MATATABI collects datasets and accommodates analysis modules
- Analysis modules post the information to NECOMAter
- Operator can perform more analysis on MATATABI using the posted information on NECOMAter
- The posts are shared between operators and modules

---

www.necoma-project.eu  6th Japan-EU Symposium on ICT Research and Innovation
NECOMA Work Packages

WP1
Network
Cloud
Client PC
End-user

Knowledge Management Framework
External source
Data exchange format for cyber threats

Threat Analysis Platform
Data aggregation and analysis algorithms
Automated rating and classification mechanisms

WP4
Test platform

WP3
Resilient Cyberdefense System
leverage on available policy enforcement points

WP2

DEMONSTRATION
Major Achievements

- **WP1**
  - MATATABI : Data Collection and Threat Analysis System

- **WP2**
  - NECOMAtter : Threat Information Exchange and Pipeline System

- **WP3**
  - SDN-IX : Cyber-Threat Defense at the Internet Core
  - Hashdoop : Anomaly Detection Mechanism based on Network Traffic Behavior
  - Cloud Defense : Threat Detection and Defense Mechanism for Public and Private Cloud
  - Endpoint Defense : Mitigation Mechanism in Wireless Access Point
  - Human Behavior : Software Plugins to Protect Users from Phishing

- **WP4**
  - Demonstration Videos for Use Cases on youtube
  - Liaison meetings with Operators and Companies
  - Summer School for Students
  - RAID2015, BADGERS 2015 : International Conference
WP1 : MATATABI

Switch

NetFlow

Router

sFlow

DNS

querylog pcap

syslog

Firewall

SPAM Sender

URL

Phishing Site

External Information

text URL

SPAM

External Information

SPAM Sender

URL
# WP2 : Analysis

<table>
<thead>
<tr>
<th>Name</th>
<th>Datasets</th>
<th>Frequency</th>
<th>LoC (#lines)</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZeuS DGA detector</td>
<td>DNS pcap, netflow</td>
<td>daily</td>
<td>25</td>
<td>hadoop-pcap</td>
</tr>
<tr>
<td>UDP fragmentation detector</td>
<td>sflow</td>
<td>daily</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>Phishing likelihood calculator</td>
<td>Phishing URLs, Phishing content</td>
<td>1-shot</td>
<td>–</td>
<td>Mahout (RandomForest)</td>
</tr>
<tr>
<td>NTP amplifier detector</td>
<td>netflow, sflow</td>
<td>daily</td>
<td>143</td>
<td>pyhive, Maxmind GeoIP</td>
</tr>
<tr>
<td></td>
<td>sflow</td>
<td>daily</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>DNS amplifier detector</td>
<td>sflow, open resolver [19]</td>
<td>daily</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Anomalous heavy-hitter detector</td>
<td>netflow, sflow</td>
<td>daily</td>
<td>106</td>
<td>pyhive</td>
</tr>
<tr>
<td>DNS anomaly detection</td>
<td>DNS pcap, whois, malicious/legitimate domain list</td>
<td>daily</td>
<td>57</td>
<td>hadoop-pcap, Mahout (RandomForest)</td>
</tr>
<tr>
<td>SSL scan detector</td>
<td>sflow</td>
<td>1-shot</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>DNS failure graph analysis</td>
<td>DNS pcap</td>
<td>daily</td>
<td>159</td>
<td>pyhive</td>
</tr>
</tbody>
</table>
WP2: Visualization of Zeus DGA and Botnet

- 2015/07/01 – 2015/07/05
  - The number of the most active DGA query is 23
  - Related traffic flows from netflow datasets.

ZeuS DGA detector
WP3 : Resilient Defense in Public Cloud

SNMP (virtsnmmpd / cacti) from Hypervisor
sFlow (neutron-sflow) from Virtual Switch
NetFlow / sFlow (agurim) from Physical Switch
Syslog from Hypervisor and switches

Detector
(agerim, cacti, virtsnmpd, neuron-sflow, NECOMAtter BoT)

Post

MATATABI

Detecting malicious behaviors by agurim + NECOMAtter BoT
Posting malicious behaviors to NECOMAtter

Recording information of SNMP, sFlow, NetFlow, and syslog

Monitoring the posts

Mitigator
(NECOMAtter BoT)

Based on NECOMAtter timeline, controlling switches and mitigation mechanisms by OpenFlow, ovsdb, and restful API.

Decision by Human Operator

Monitoring NECOMAtter timeline and launch the mitigation mechanisms
- flow redirection rules in switches
- d4c
- Filtering ACL
WP3 : Defense Mechanism at the Internet Core

- SDN IX (PIX-IE)
  - Programmable IX in Edo : PIX-IE
  - Mitigating and filtering suspicious flows at IX
- IX is a public space in the Internet
  - Before link saturation, an ISP operator can stop DDoS flows

The operator has to contact to each ISP, and ask to filter the DDoS packets ...
WP4 : Liason Meeting
WP4 : RAID 2015, BADGERS 2015 in Kyoto

The 18th International Symposium on Research in Attacks, Intrusions and Defenses,
Kyoto, Japan | November 2-4, 2015

Conference dates November 2-4.
The 18th International Symposium on Research in Attacks, Intrusions and Defenses, previously known as Recent Advances in Intrusion Detection, will be held in Kyoto, Japan.

This symposium brings together leading researchers and practitioners from academia, government, and industry to discuss novel security problems, solutions and technologies related to intrusion detection, attacks and defenses.

Committees

Organizing Committee

- General Chair: Youki Kodobeyashi, NAIST
- Local Arrangement Chair: Kazuya Okada, NAIST
- PC Chair: Herbert Bos, Vrije Universiteit/VU University Amsterdam
- PC Co-Chair: Fabian Monrose, University of North Carolina at Chapel Hill
- Publication Chair: Gregory Blonder, Telecom SudParis
- Publicity Chair: Giorgos Vasilakis, FORTH

Program Committee

- Manos Antonakakis Georgia Tech
- Elias Athanasopoulos FORTH
- Herbert Bos Vrije Universiteit / VU University Amsterdam
- Gabriela Ciocarlie SRI International
- Lucas Devi Intel CPI-SG at TU Darmstadt
- Tudor Dumitrasc University of Maryland
- Petros Efstathioupolous Symantec Research Labs
- William Enck North Carolina State University
- Bryan Ford EPFL
- Aurelien Francillon Eurecom
- Alex Garde University of Birmingham
- Chris Karich University of Illinois at Chicago
- Christopher Kruegel UC Santa Barbara
- Andrea Lanzi U. di Milan
- Corrado Leita Lastline, Inc.
- Brian Levine UMass Amherst
- Fabian Monrose University of North Carolina at Chapel Hill
- Zachary Peterson Cal Poly, San Luis Obispo
- Georgios Portokalidis Stevens Institute of Technology
- Niel Provos Google
- Konrad Rieck University of Göttingen
- William Robertson Northeastern University
- Christian Rossoo Swarm University
- Andrei Sabelfeld Chalmers
- Stelios Sidiroglou-Douskos MIT
- Patrick Traynor U. of Florida
- XiaoFeng Wang Indiana University
- Dongyan Xu Purdue University

www.necoma-project.eu 6th Japan-EU Symposium on ICT Research and Innovation
Summary

With tremendous success, NECOMA seeks new horizon