Analyzing Targeted Attacks through "Hiryu" – An IOC Management and Visualization Tool

Hiroshi Soeda
Incident Response Group,
JPCERT/Coordination Center

Agenda

1. Advanced attacks specifically targeting Japanese organizations
   - APT Campaigns
   - Getting IOC
   - Motivation to Develop a Tool

2. Development of the tool
   - Components
   - Structure

3. Introducing “Hiryu”
   - Web UI
   - Import/Export Data
   - Visualization

1. ADVANCED ATTACKS SPECIFICALLY TARGETING JAPANESE ORGANIZATIONS

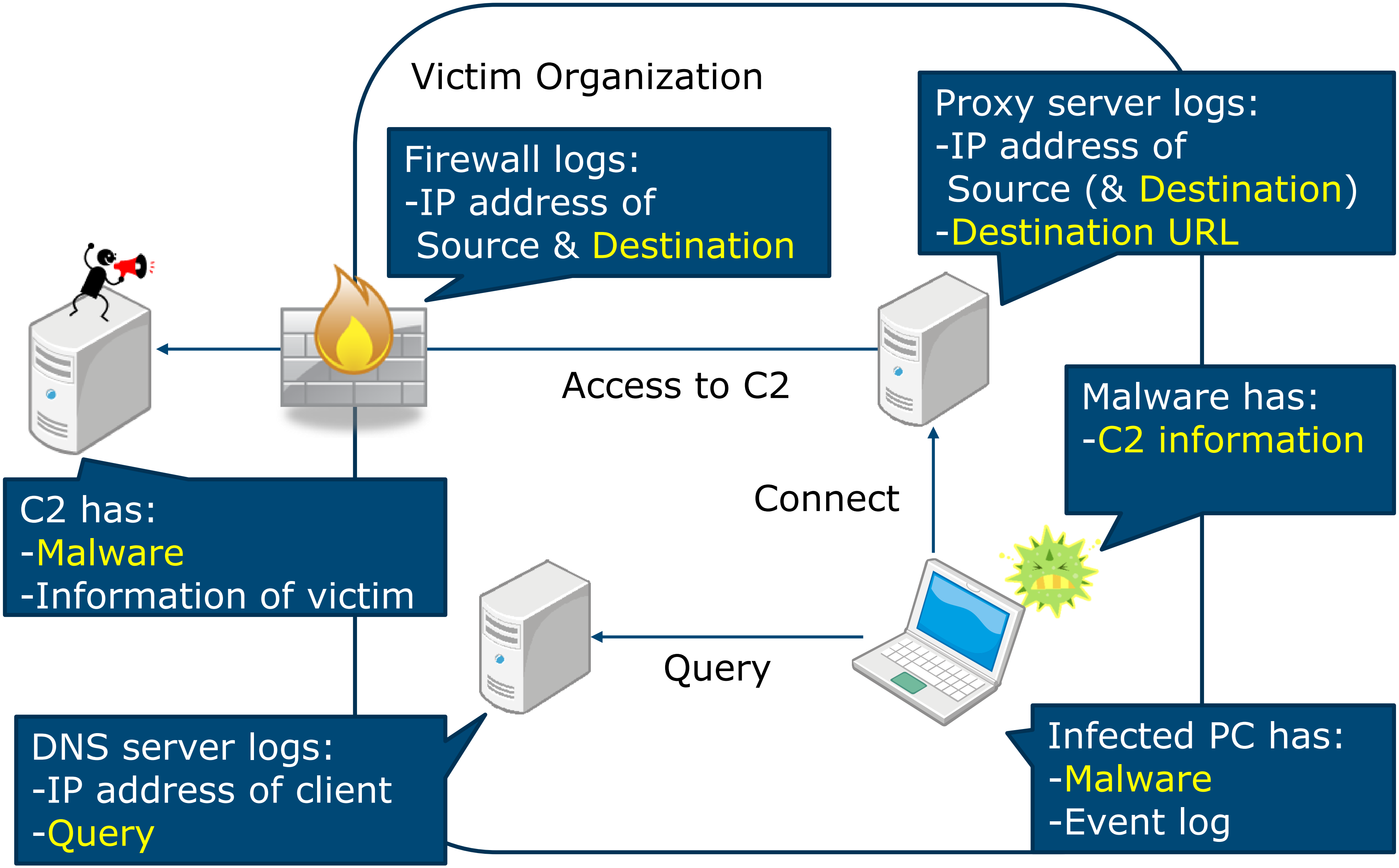
APT Campaign (1)

- Cloudy Omega (Symantec) / Blue Termite (Kaspersky)
  - Various targets
    - Government, Defence industry, Energy sector, Think tank, Media…
  - TTP
    - Before intrusion
      - Malware called “Emdivi” used
      - Malware attached emails disguising medical bill notifications
      - Drive-by download attacks
    - After intrusion
      - Steal domain administrator’s account
      - Active directory privilege escalation
        - Kerberos KDC vulnerability (MS14-068)
  - Behavior
    - Gather information from network
    - Exfiltration
      - Using password protected RAR file
      - Domain credentials, sensitive information

APT Campaign (2)

- Winnti (Kaspersky) / Axiom (Novetta)
  - Target
    - Online gaming company
    - Pharmaceutical industry
  - TTP
    - Use malware signed by legitimate code signing certificates
    - Register a task to install malware on the server
    - Create a service to activate the malware and execute
  - Behavior
    - Steal code signing certificates
    - Steal information

Getting IOC



Firewall logs:
-IP address of
Source & Destination

Proxy server logs:
-IP address of
Source (& Destination)
-Destination URL

Malware has:
-C2 information

C2 has:
-Malware
-Information of victim

DNS server logs:
-IP address of client
-Query

Infected PC has:
-Malware
-Event log

Motivation to Develop a Tool

- Organizing information
  - What types of malware are used in which attacks
  - Correlation among IOCs in different incidents
  - Overall picture of attack campaigns

- Collecting public information
  - Need to organize IOCs published in blogs/reports by security vendors, as they sometimes link to the incidents
  - Need to sort out attack groups and campaigns that are named uniquely by different security vendors

2. DEVELOPMENT OF THE TOOL

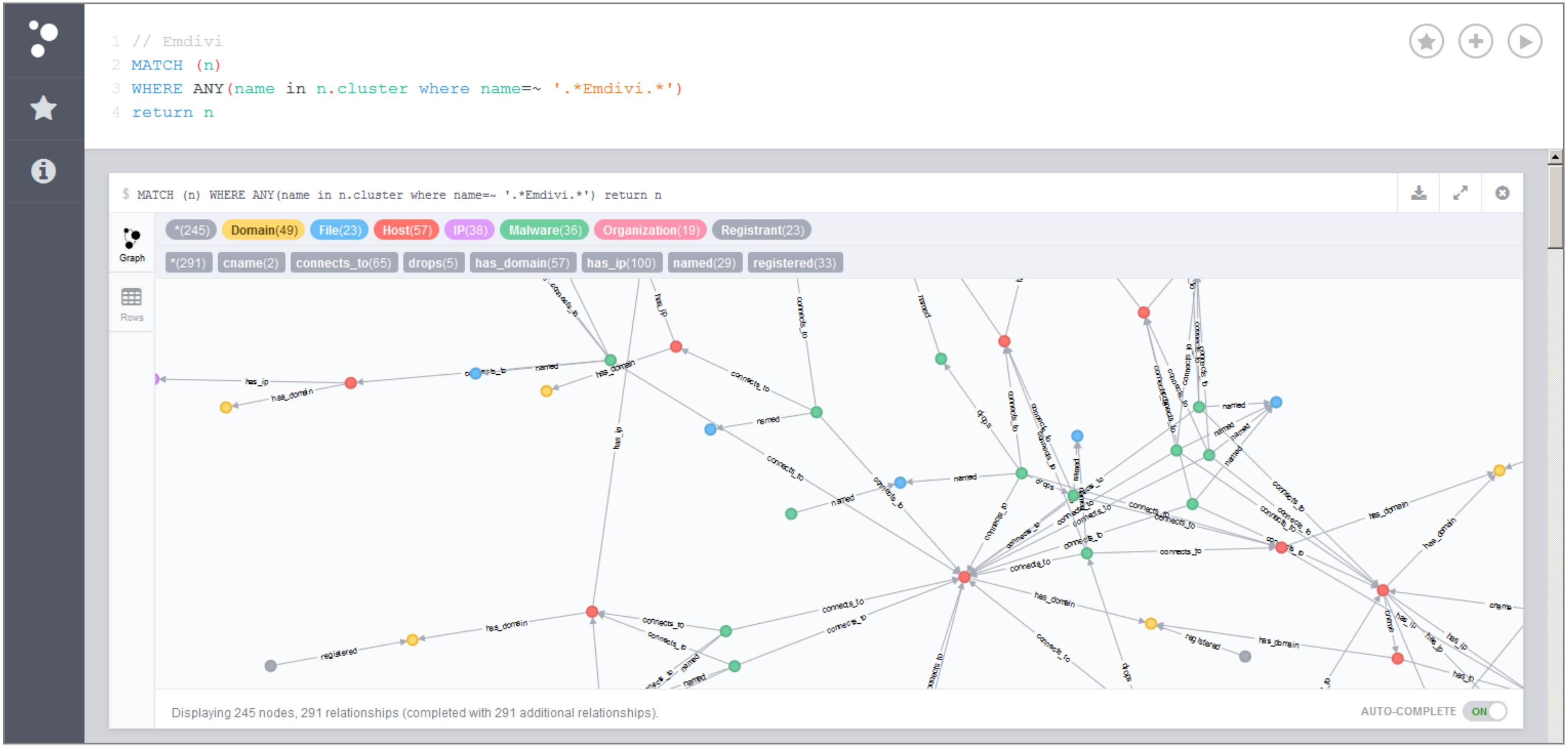
Components

- Django
  - Web application framework
- vis.js
  - Visualization library
- Neo4j (Optional)
  - Graph Database

- Python modules
  - pythonwhois
    - for domain whois
  - ipwhois
    - for ip whois
  - Py2neo
    - Neo4j client library
  - ioc_writer
    - export IOC as OpenIOC format
  - python-stix
    - export IOC as STIX format

Neo4j

- Graph DB stores Nodes and Relations
- Using Cypher query language



```
// Emdivi
MATCH (n)
WHERE ANY(name in n.cluster where name=~ '.*Emdivi.*')
return n
```

```
$ MATCH (n) WHERE ANY(name in n.cluster where name=~ '.*Emdivi.*') return n
```

*(245) Domain(49) File(23) Host(57) IP(38) Malware(36) Organization(19) Registrant(23)

*(291) cname(2) connects_to(65) drops(5) has_domain(57) has_ip(100) named(29) registered(33)

Displaying 245 nodes, 291 relationships (completed with 291 additional relationships).

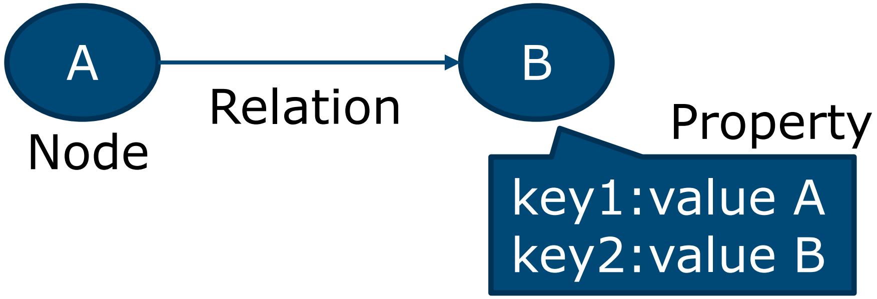
Structure (1)

- Node
  - Components include
    - Host name
    - Domain name
    - IP address
    - Organization
    - Malware (hash)
    - File name

    …
- Relation
  - Relation of Nodes
    - Host name tied to IP address
    - Organization tied to IP address
    - Host name tied to domain name
    - Malware connecting to IP address

    …

- Multiple Properties can be registered to Nodes/Relations
- Property
  - Combination of an arbitrary key and value
- e.g. Property of malware
  - md5:…
  - sha1:…
  - sha256:…
  - type: HTTP bot

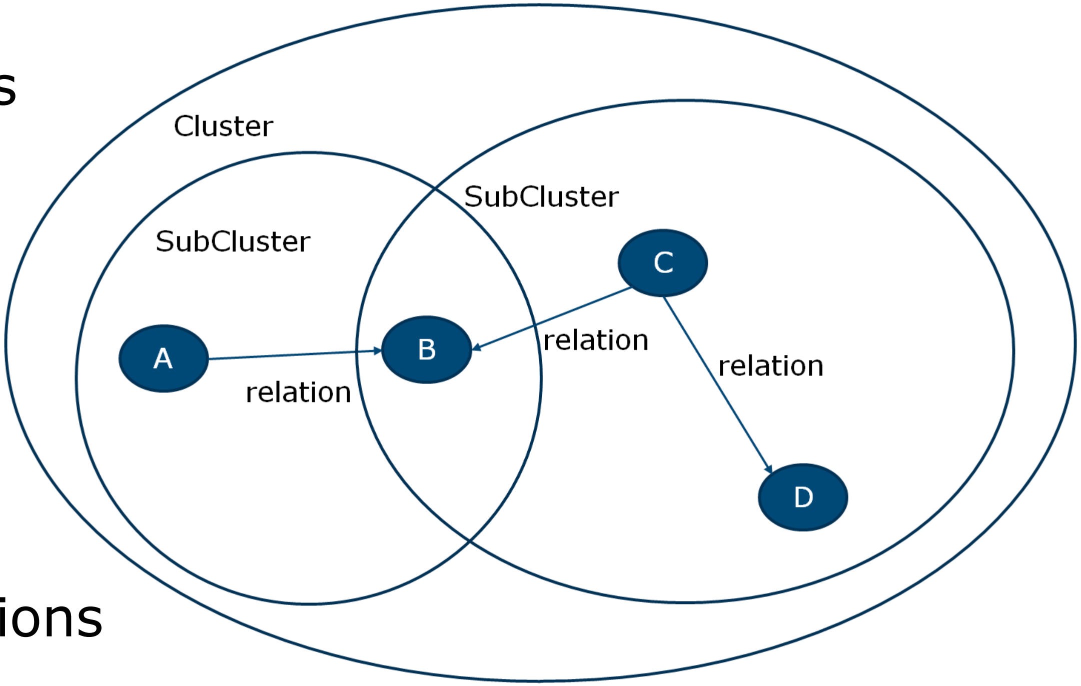


Structure (2)

- Cluster
  - Includes SubClusters
  - e.g.
    - Campaign name
      - APT-x
      - Operation X

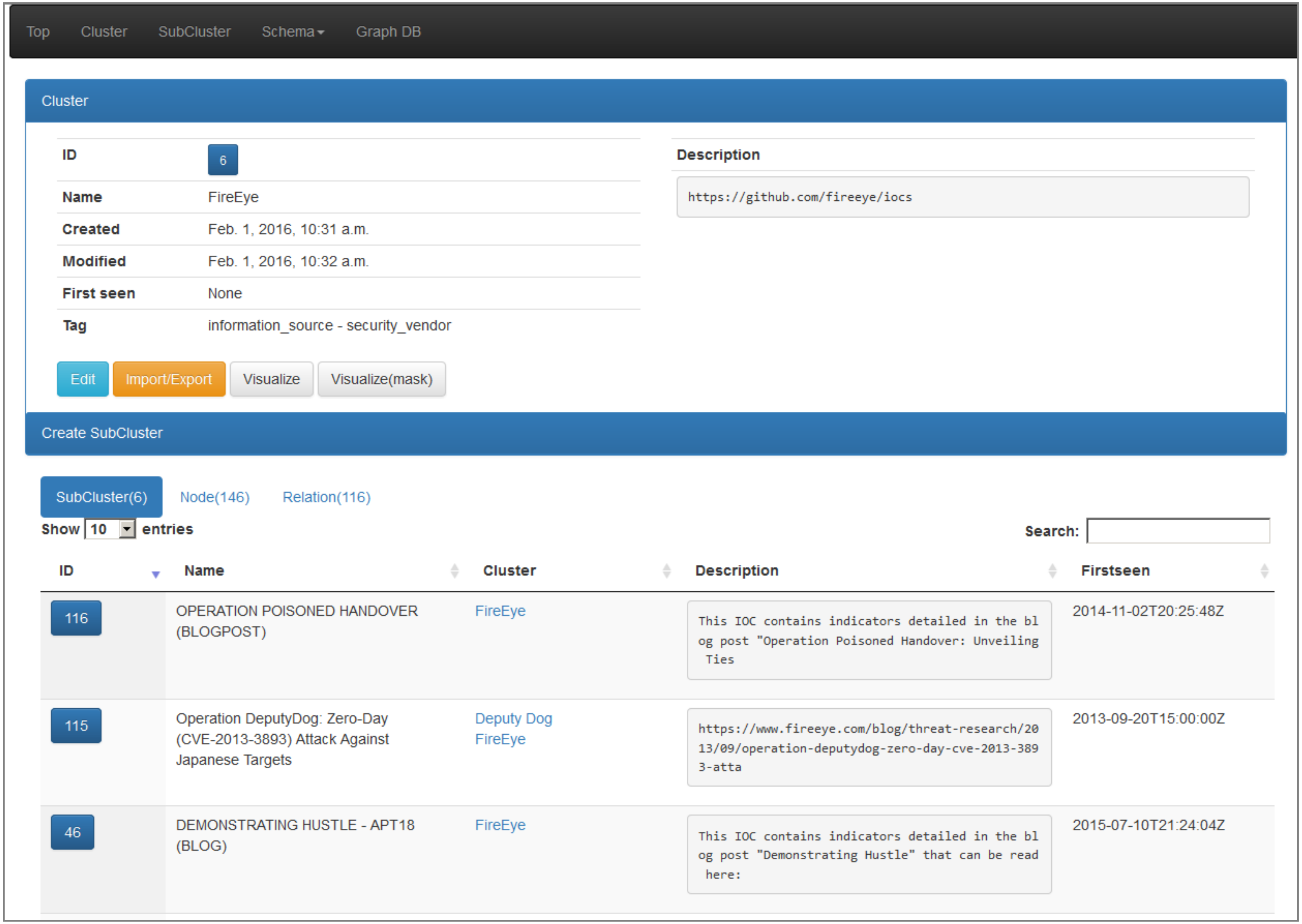
      …
    - Data source
- SubCluster
  - Include Nodes/Relations
  - e.g.
    - Incident
      - Communication with C2
      - Malware attached emails

      …
    - System’s ticket



3. INTRODUCING “HIRYU”

Cluster



Cluster

ID	6
Name	FireEye
Created	Feb. 1, 2016, 10:31 a.m.
Modified	Feb. 1, 2016, 10:32 a.m.
First seen	None
Tag	information_source - security_vendor

Description

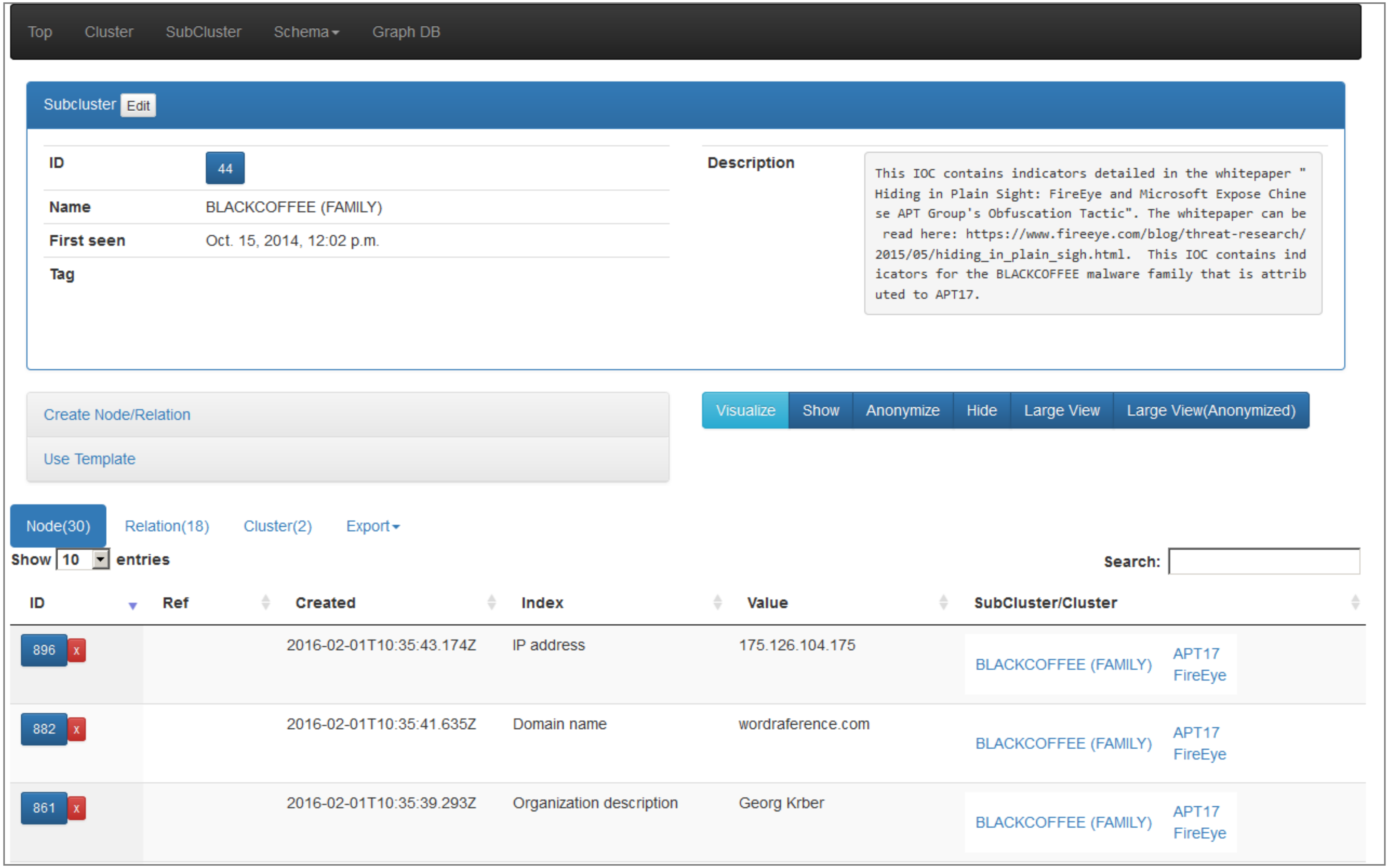
https://github.com/fireeye/iocs

Show 10 entries

Search:

ID	Name	Cluster	Description	Firstseen
116	OPERATION POISONED HANDOVER (BLOGPOST)	FireEye	This IOC contains indicators detailed in the blog post "Operation Poisoned Handover: Unveiling Ties	2014-11-02T20:25:48Z
115	Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets	Deputy Dog FireEye	https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-atta	2013-09-20T15:00:00Z
46	DEMONSTRATING HUSTLE - APT18 (BLOG)	FireEye	This IOC contains indicators detailed in the blog post "Demonstrating Hustle" that can be read here:	2015-07-10T21:24:04Z

SubCluster(1)



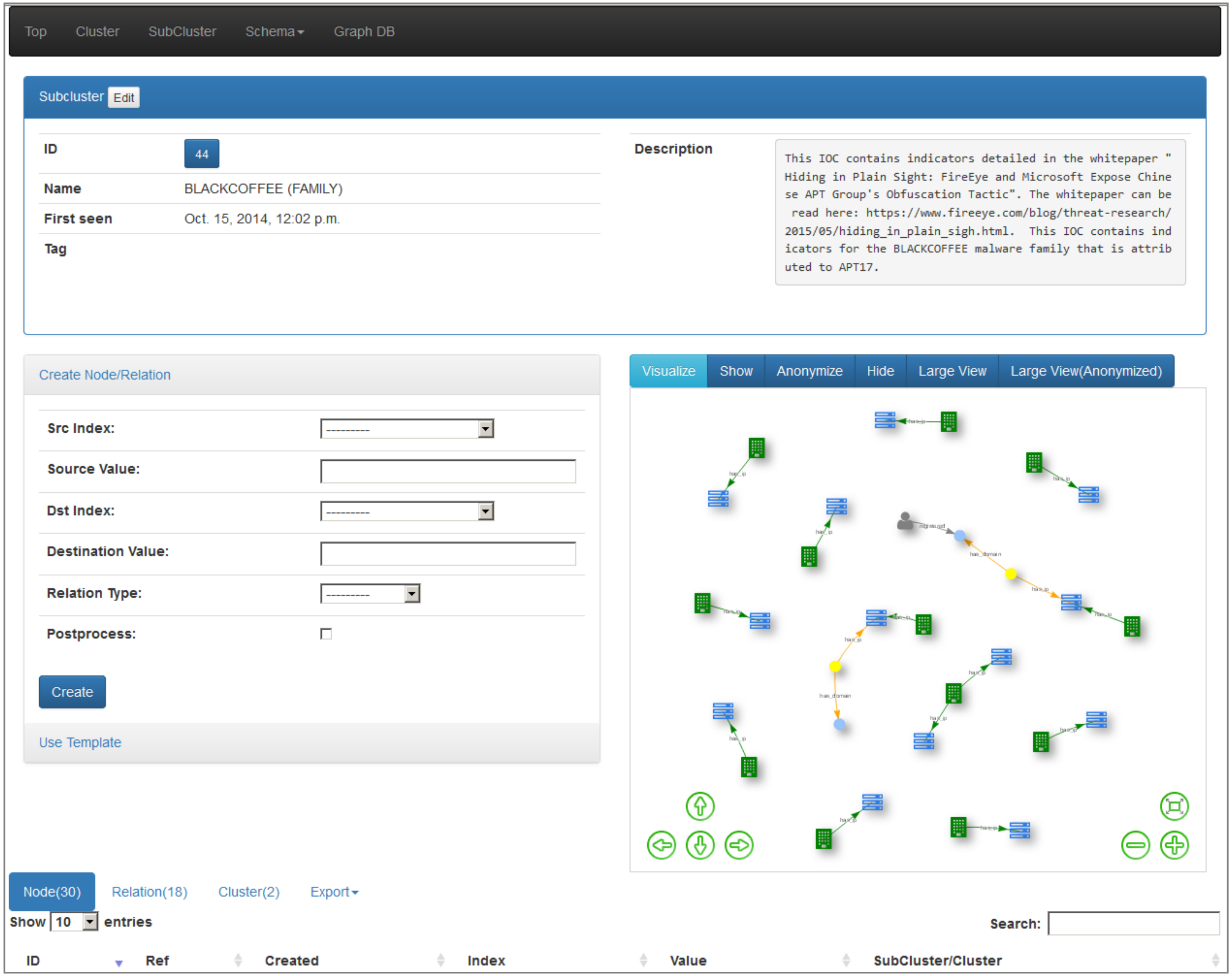
ID	44
Name	BLACKCOFFEE (FAMILY)
First seen	Oct. 15, 2014, 12:02 p.m.
Tag	

Description

This IOC contains indicators detailed in the whitepaper " Hiding in Plain Sight: FireEye and Microsoft Expose Chinese APT Group's Obfuscation Tactic". The whitepaper can be read here: https://www.fireeye.com/blog/threat-research/2015/05/hiding_in_plain_sigh.html. This IOC contains indicators for the BLACKCOFFEE malware family that is attributed to APT17.

ID	Ref	Created	Index	Value	SubCluster/Cluster
896 x		2016-02-01T10:35:43.174Z	IP address	175.126.104.175	BLACKCOFFEE (FAMILY) APT17 FireEye
882 x		2016-02-01T10:35:41.635Z	Domain name	wordraference.com	BLACKCOFFEE (FAMILY) APT17 FireEye
861 x		2016-02-01T10:35:39.293Z	Organization description	Georg Krber	BLACKCOFFEE (FAMILY) APT17 FireEye

SubCluster(2)



ID	44
Name	BLACKCOFFEE (FAMILY)
First seen	Oct. 15, 2014, 12:02 p.m.
Tag	

Description

```
This IOC contains indicators detailed in the whitepaper "
Hiding in Plain Sight: FireEye and Microsoft Expose Chine
se APT Group's Obfuscation Tactic". The whitepaper can be
 read here: https://www.fireeye.com/blog/threat-research/
2015/05/hiding_in_plain_sigh.html.  This IOC contains ind
icators for the BLACKCOFFEE malware family that is attrib
uted to APT17.
```

Create Node/Relation

Src Index:	---------
Source Value:	
Dst Index:	---------
Destination Value:	
Relation Type:	---------
Postprocess:	□

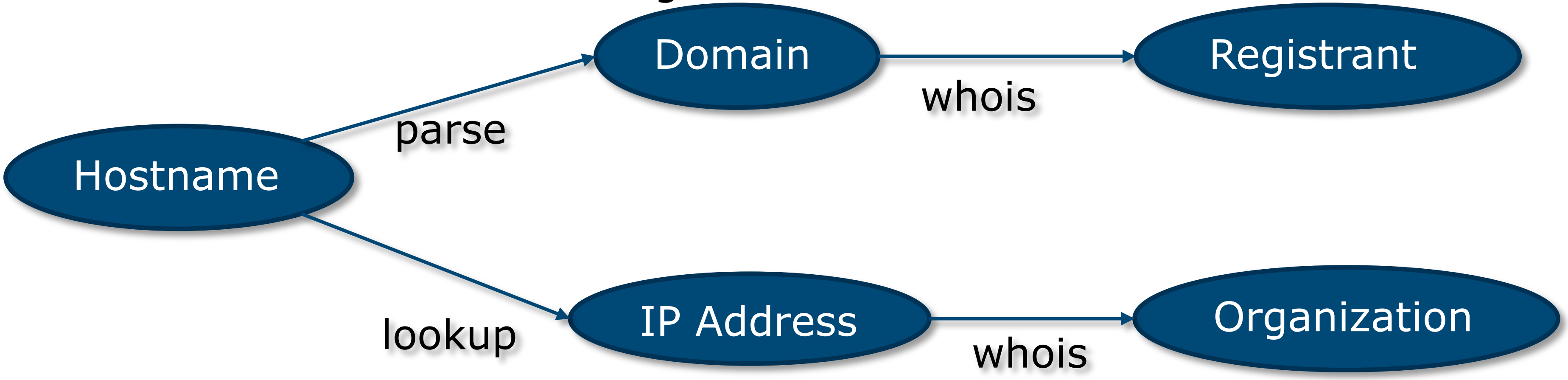
Show 10 entries

Search:

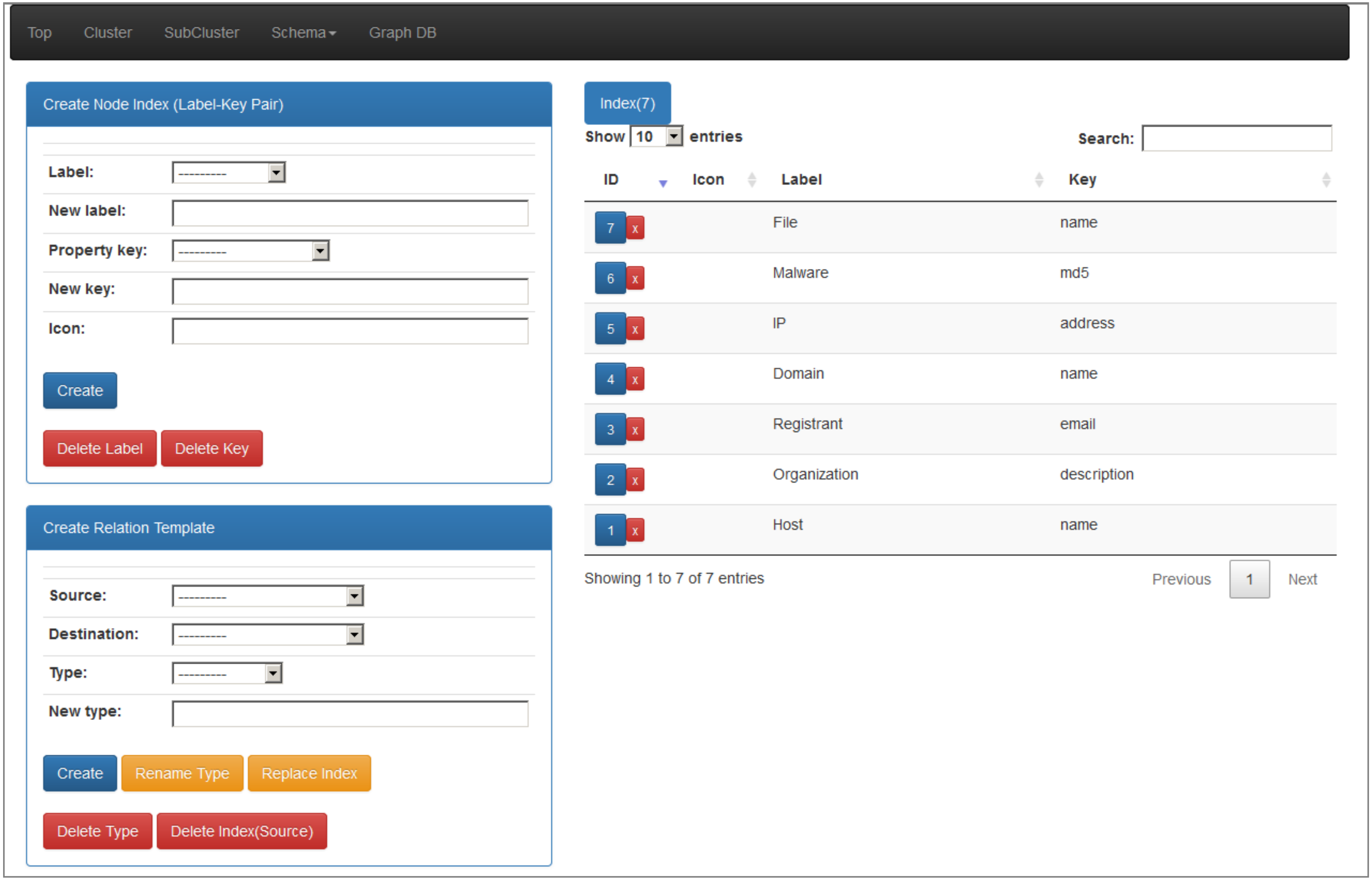
ID	Ref	Created	Index	Value	SubCluster/Cluster

Additional Processing of Nodes

- Additional processing is performed when registering a specific type of Node
  - Register host name
    - Extracts domain names
      - Searches whois for the domain name
        - Extracts registrant's email address from whois results
    - DNS lookup for IP address
      - Searches whois for the IP address
        - Extracts organization name from whois results



Schema



Create Node Index (Label-Key Pair)

Label:	---------
New label:	
Property key:	---------
New key:	
Icon:	

Create Relation Template

Source:	---------
Destination:	---------
Type:	---------
New type:	

Index(7)

Show 10 entries Search:

ID	Icon	Label	Key
7 x		File	name
6 x		Malware	md5
5 x		IP	address
4 x		Domain	name
3 x		Registrant	email
2 x		Organization	description
1 x		Host	name

Showing 1 to 7 of 7 entries

Import/Export Data

- CSV
  - Able to import/export Node, Relation, Cluster, SubCluster

- Neo4j
  - Able to push/pull
  - Need to register an Index (a combination of the Node’s label and main key) to import data

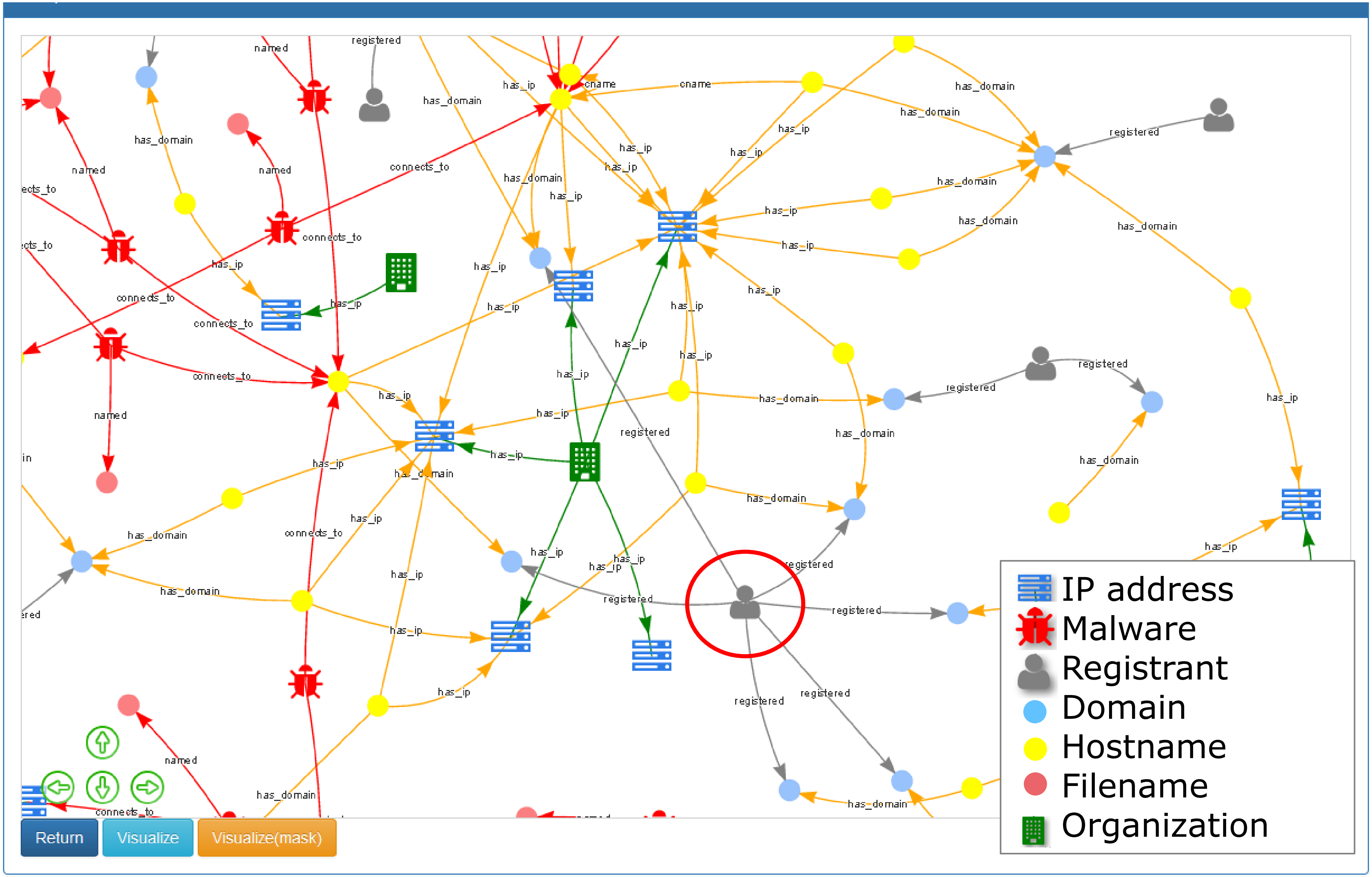
- OpenIOC
  - Need a table of how OpenIOC terms and Index correspond

- STIX
  - Able to import/export the following data
    - Host name, Domain name, IP address

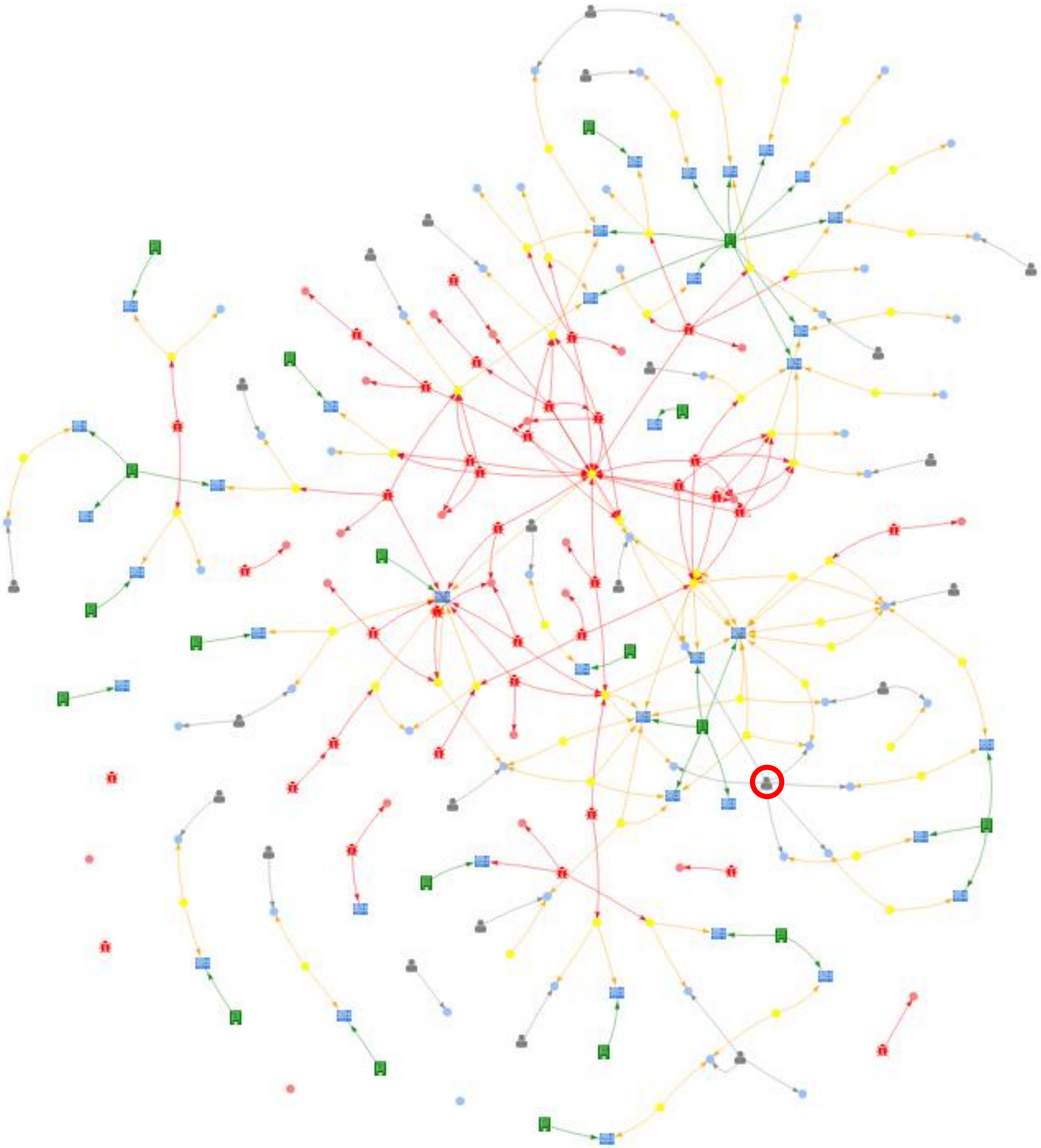
OpenIOC/STIX Correspondence Table

Hiryu		OpenIOC	STIX & CybOX
SubCluster		metadata	report:Header
name		short_description	Title
description		description	Description
Node Index		term	Cybox:Object
Label	Key		
IP	address	PortItem/remoteIP	AddressObj
Host	name	DnsEntryItem/Host	HostnameObj
Domain	name	-	DomainNameObj

Visualization



Visualization



ToDo

- Improve import/export of OpenIOC, STIX
  - Currently, only limited data can be imported from STIX
  - Import/Export is irreversible

- Implement a new feature on incident response timeline
  - Record date/time and events
    - A suspicious file created on the server
    - A suspicious communication performed from the server
  - May be achieved to a certain extent by adding time information to the Relations field
  - Some events may be difficult to fit in Relations
    - Received a malware sample from victim organization
    - Reported analysis results to victim organization

Thank you for your attention

- My email address
  - hiroshi.soeda@jpcert.or.jp
- Repository of Hiryu
  - https://github.com/S03D4-164/Hiryu
- Incident report notifications
  - info@jpcert.or.jp