Rethinking the Graph Visualization for Threat Reports

Mayo YAMASAKI, NTT-CERT
Outline

1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
Popularity of Network-Styled Graph Visualization

https://www.google.com/search?q=threat+intelligence+graph+visualization&tbm=isch
Problems with Dense Graph

These graphs have 30 nodes, and edges are randomly created according to each density.

density = |Edge| / (|Node| * (| Node| - 1))
How to Improve Graph Visualization?

1. Brand New Way
2. Extract Subgraph
3. Interactive layout
4. Improve layout

Impossible for Non-experts
Brand New Way: Hive Plot

Briefings in Bioinformatics, Volume 13, Issue 5, September 2012,
Pages 627–644, https://doi.org/10.1093/bib/bbr069
How to Improve Graph Visualization?

1. Brand New Way
   Impossible for Non-experts

2. Extracting Subgraph
   De Facto Standard to Explore Data

3. Interactive layout
   Depend on Your Use Case

4. Improving layout

Let’s Rethink the STIX Visualization for Threat Reports
Outline

1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
Process of Study

- Collecting Threat Diagrams
- Classifying Diagrams
- Extracting Observations
Process of Study

1. Collecting Threat Diagrams
2. Classifying Diagrams
3. Extracting Observations
Visualization on Threat Reports

- Collecting **700** Images from **83** Reports on **8** Websites
- Only 37 Images which Describing Threat Structure

![Pie Chart]

- **616** Total Images
- **37** Screenshot
- **32** Threat Diagram
- **15** Statistics
- **Other**
Screenshots

Transform your face using Artificial Intelligence with just one tap

Source: https://research.checkpoint.com/2019/danabot-demands-a-ransom-payment/
https://www.welivesecurity.com/2019/07/19/faceapp-spotlight-scams-emerge/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/
Statistics

Source:

2008
- Wajam Internet Technologies Inc. is founded

2011
- Wajam is launched as a browser extension

2012-2014
- Google+, LinkedIn and Facebook can’t be linked to Wajam anymore

2016
- Complaint against Wajam from the Privacy Commissioner of Canada

2017
- All Wajam assets are transferred to a Hong Kong company called IMFL

Dropper Type Distribution

- Games: 12%
- Photo Utility: 7%
- System Utility: 1%
- Adult Entertainment: 1%
- Media Player: 74%
Process of Study

1. Collecting Threat Diagrams
2. Classifying Diagrams
3. Extracting Observations
Classification on Why and How

**Why?**
1. Attack Flow
2. C2 Infrastructure
3. Malware Behavior

**How?**
1. Attack Chain
2. Directory Structure
3. Flow Chart Diagram
4. Function Structure
5. Network Topology
6. Sequence Diagram
Attack Flow - Attack Chain

Source:
https://securelist.com/twas-the-night-before/91599/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

Disclosure to 2020 FIRST CTI Symposium. Copyright©2020 NTT Corp. All Rights Reserved.
C2 Infrastructure

Directory Structure

Network Topology

Source: https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/
https://blog.malwarebytes.com/cybercrime/2019/07/no-mans-land-how-a-magecart-group-is-running-a-web-skimming-operation-from-a-war-zone/
Malware Behavior

Attack Chain

Sequence Diagram

Flow Chart

Function Structure

Source:
https://securelist.com/platinum-is-back/91135/
https://research.checkpoint.com/danabot-demands-a-ransom-payment/
https://www.welivesecurity.com/2019/06/05/wajam-startup-massively-spread-adware/
Process of Study

Collecting Threat Diagrams → Classifying Diagrams → Extracting Observations
Visualization for Attack Flow

- **Attack Flow**: 17
- **C2 Infrastructure**: 0 1 0 0 3 0
- **Malware Behavior**: 3 0 2 9 0 2

The diagram shows the visualization of an attack flow with categories such as Attack Chain, Directory Structure, Flow Chart Diagram, Function Structure, Network Topology, and Sequence Diagram.
Observations

1. DAG Network with Edges between Adjacent Layers

**Threat Diagram**
- Actor
- Malware
- TTP
- IoC

**STIX Data**
- Actor
- Malware
- TTP
- IoC
Observations

1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
Observations

1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
3. Extracting Differences from Existing Intelligence
   - New Vulnerability
   - Same IoC
   - New Malware Component
Outline

1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
Layout for DAG (Directed Acyclic Graph)
DAG Layout: Problems

- **Hierarchical Order**
  - Different order between STIX Edge and Diagrams

- **Cross Layered Edges**
  - Many Edges on Non-Adjective Layers
- Re-Mapping Edges
  - Remapping indicates Directions to Fit Intuition

- Orthogonal Routing
  - Eliminating cross edges

- De-Emphasize Edges on Non-Adjective Layers
  - Bellman Ford Method for Longest Path Problem with Negative Weights
Clustering IoCs based on Relationships
Emphasizing Differences

FANCY BEAR (threat-actor)

Mentioned in 36 of notes

Observed from 2013-01-01 to 2019-11-22

from 2015-01-01 to 2016-12-31

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Emphasizing Differences

FANCY BEAR (threat-actor)

Mentioned in 36 of notes

Observed from 2013-01-01 to 2019-11-22

from 2015-01-01 to 2016-12-31
IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
New Visualization based on Observations

1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
3. Extracting Differences from Existing Intelligence
Outline
1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
Example: An New Zebrocy Campaign

- Zebrocy Trojan used by APT28
  - Written in C++, Delphi, AutoIt, C#, VB.
- New Campaign since Sep 2019
  - Phishing with Malicious Word File
  - Usage of Dropbox for Hosting

Source: https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/
Example: An New Zebrocy Campaign
Example: An New Zebrocy Campaign

Observed from 2019-08-20 to 2019-08-20
No summer vacations for Zebrocy
Example: An New Zebrocy Campaign

Sednit uses Spearphishing Attachment

- Sednit
- Standard Cryptographic Protocol
- Spearphishing Attachment
- Data Encrypted
- Data Encoding
- Scripting

Disclosure to 2020 FIRST CTI Symposium. Copyright©2020 NTT Corp. All Rights Reserved.
Example: An New Zebrocy Campaign

[Diagram of the Spearphishing Attachment using Zebrocy]

- Sednir
- Standard Cryptographic Protocol
- Spearphishing Attachment
- Data Encrypted
- Data Encoding
- Scripting

Spearphishing Attachment uses Zebrocy

[Graph showing data mentions from 2017-01-01 to 2017-12-31 and 2018-10-01 to 2018-11-30]

Disclosure to 2020 FIRST CTI Symposium. Copyright©2020 NTT Corp. All Rights Reserved.
Example: An New Zebrocy Campaign
Example: An New Zebrocy Campaign
Example: An New Zebrocy Campaign

Not Found
Example: An New Zebrocy Campaign

ESET said,

As predicted by other fellow researchers, the Sednit group added a new development language in their toolset — more precisely, for their downloader: the Nim language. However, their developers were also busy improving their Golang downloader, as well as rewriting their backdoor from Delphi into Golang.

The Nim downloader fetches its dynamic-link library (DLL) payload, named ospsvc.dll, to C:\ProgramData\Java\Oracle, and executes it as a service via regsvr32 /s.
1. Backgrounds
2. Study of Diagrams on Threat Reports
3. Visualization for Threat Graph
4. Examples
5. Discussions & Conclusions
Discussions

• How to Capture Malware Behaviors?
  – Necessity to Build a Data Structure for Malware Behaviors
  – STIX 2.1 May Solve This Problem

• How to Fill Kill Chain Phases?
  – Shortage of Attack Phrase on Actually Shared Intelligence
  – Without Phrases, Difficulty to Reflect How IoCs are Used into Layouts

• To Make It Better
  – New Observations & Layout methods
  – Other Purposes for Visualization
  – Etc.
Conclusions

• Not The Only Way to Visualize Threat Intelligence
• Possibility to Improve Visualization for a Use Case
• Necessity to Rethink Your Purpose & Method of Visualization