TLP:WHITE

Rethinking the Graph Visualization for Threat Reports

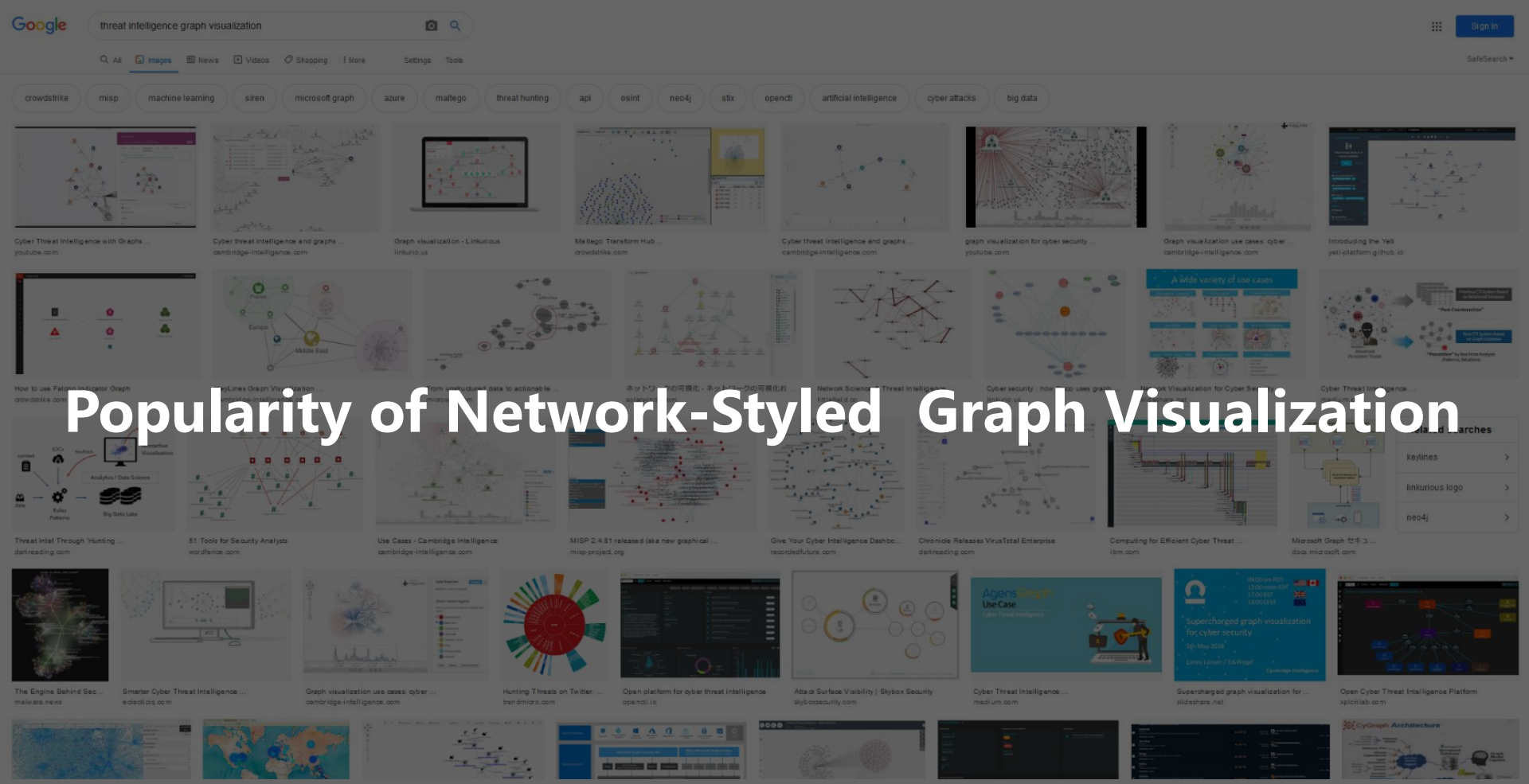
Mayo YAMASAKI, NTT-CERT

Outline

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

Outline

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

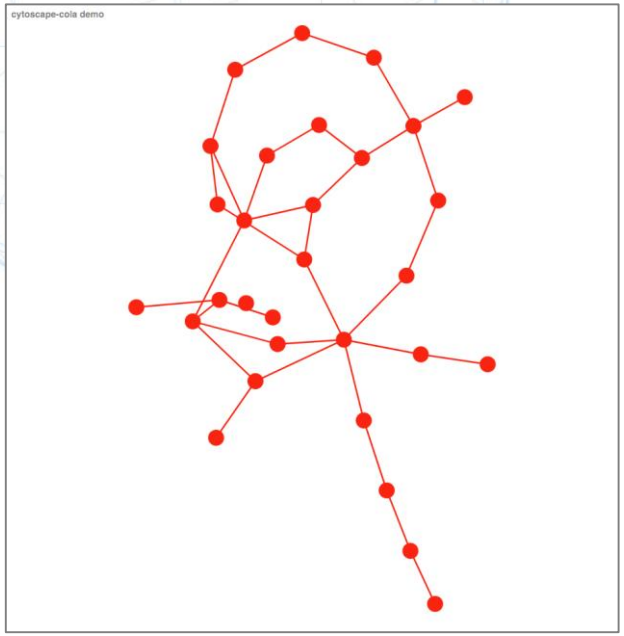


https://www.google.com/search?q=threat+intelligence+graph+visualization&tbm=isch

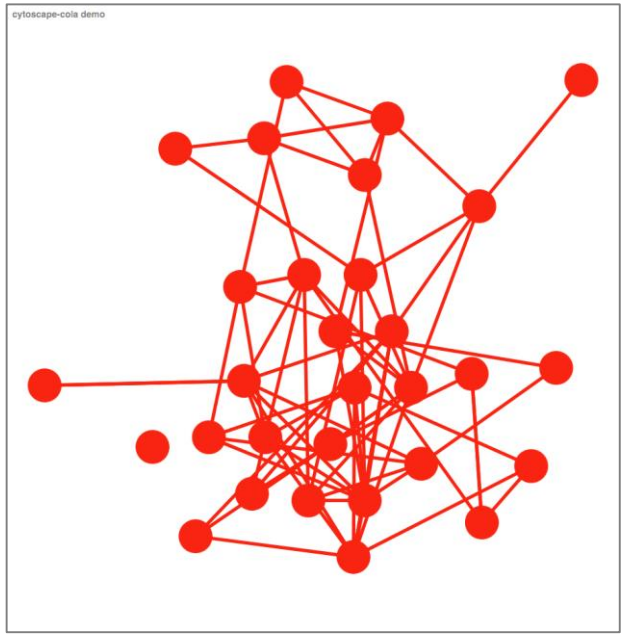
Problems with Dense Graph

NTT Confidential

density = 0.08



density = 0.16



density = 0.32

These graphs have 30 nodes, and edges are randomly created according to each density.
density = |Edge| / (|Node| * (| Node| - 1))

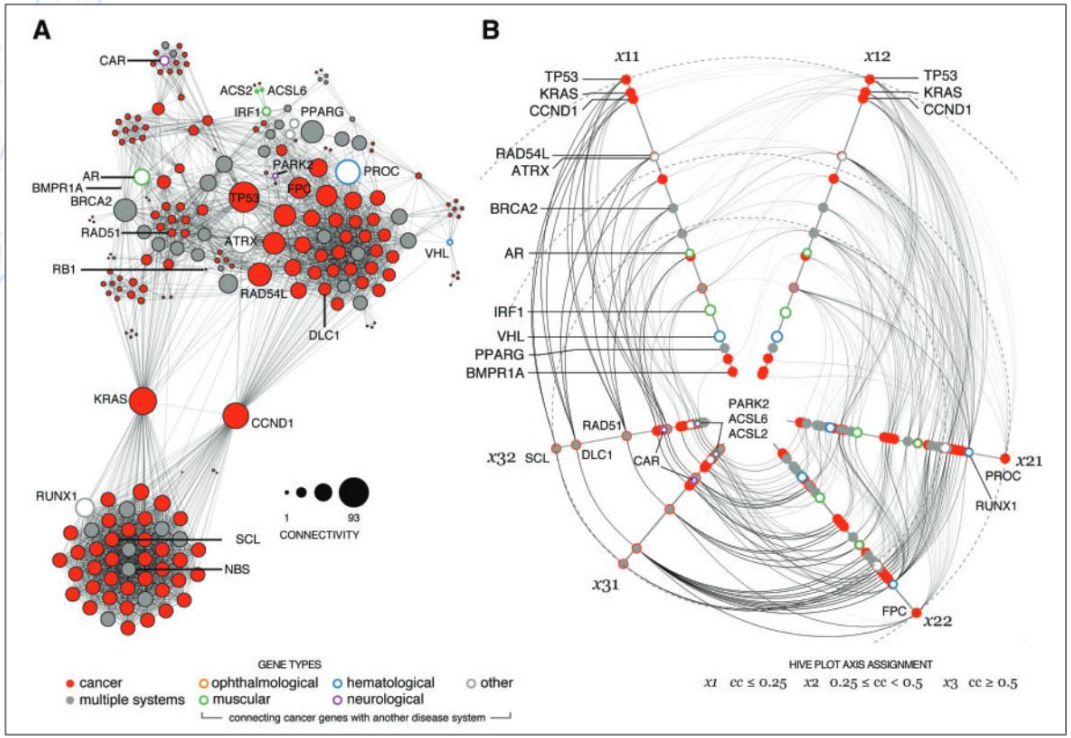
How to Improve Graph Visualization?

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

} **Impossible for Non-experts**

Brand New Way: Hive Plot

NTT Confidential



Briefings in Bioinformatics, Volume 13, Issue 5, September 2012, Pages 627–644, https://doi.org/10.1093/bib/bbr069

How to Improve Graph Visualization?

NTT Confidential

1. Brand New Way
2. Extracting Subgraph
3. Interactive layout
4. Improving layout

Impossible for Non-experts

De Facto Standard to Explore Data

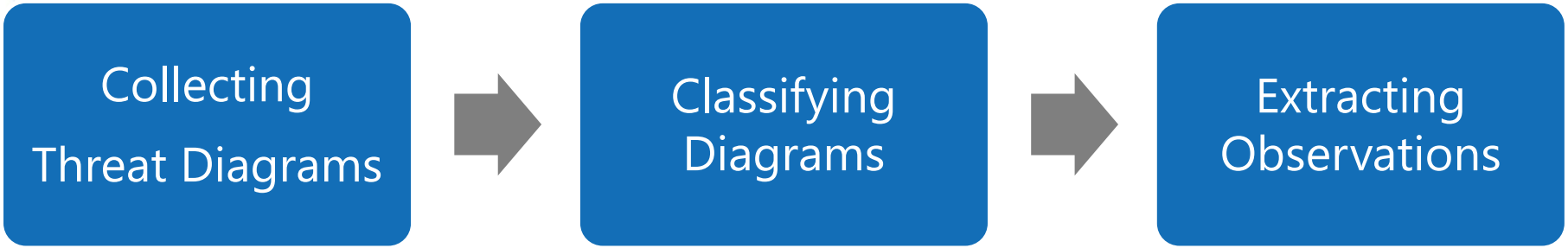
Depend on Your Use Case

Let's Rethink the STIX Visualization for Threat Reports

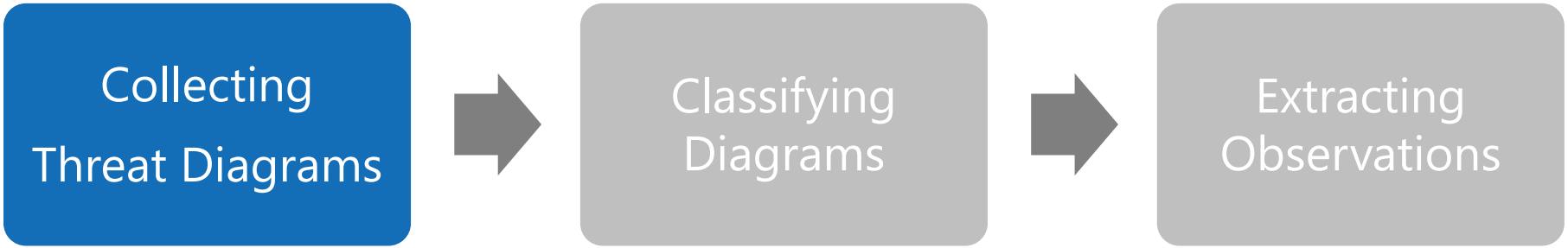
Outline

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

Process of Study

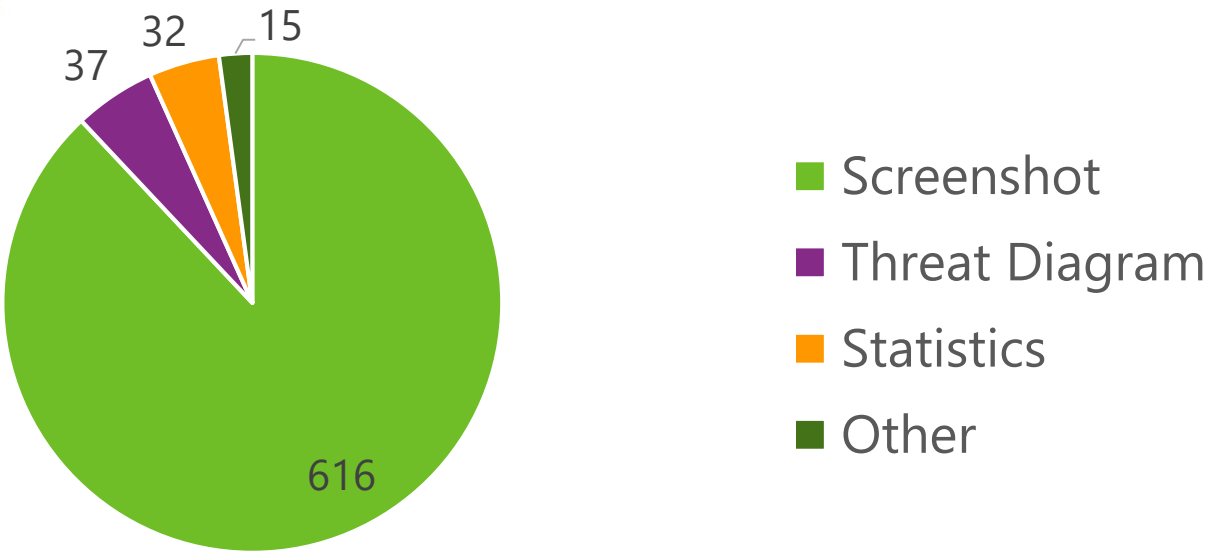


Process of Study

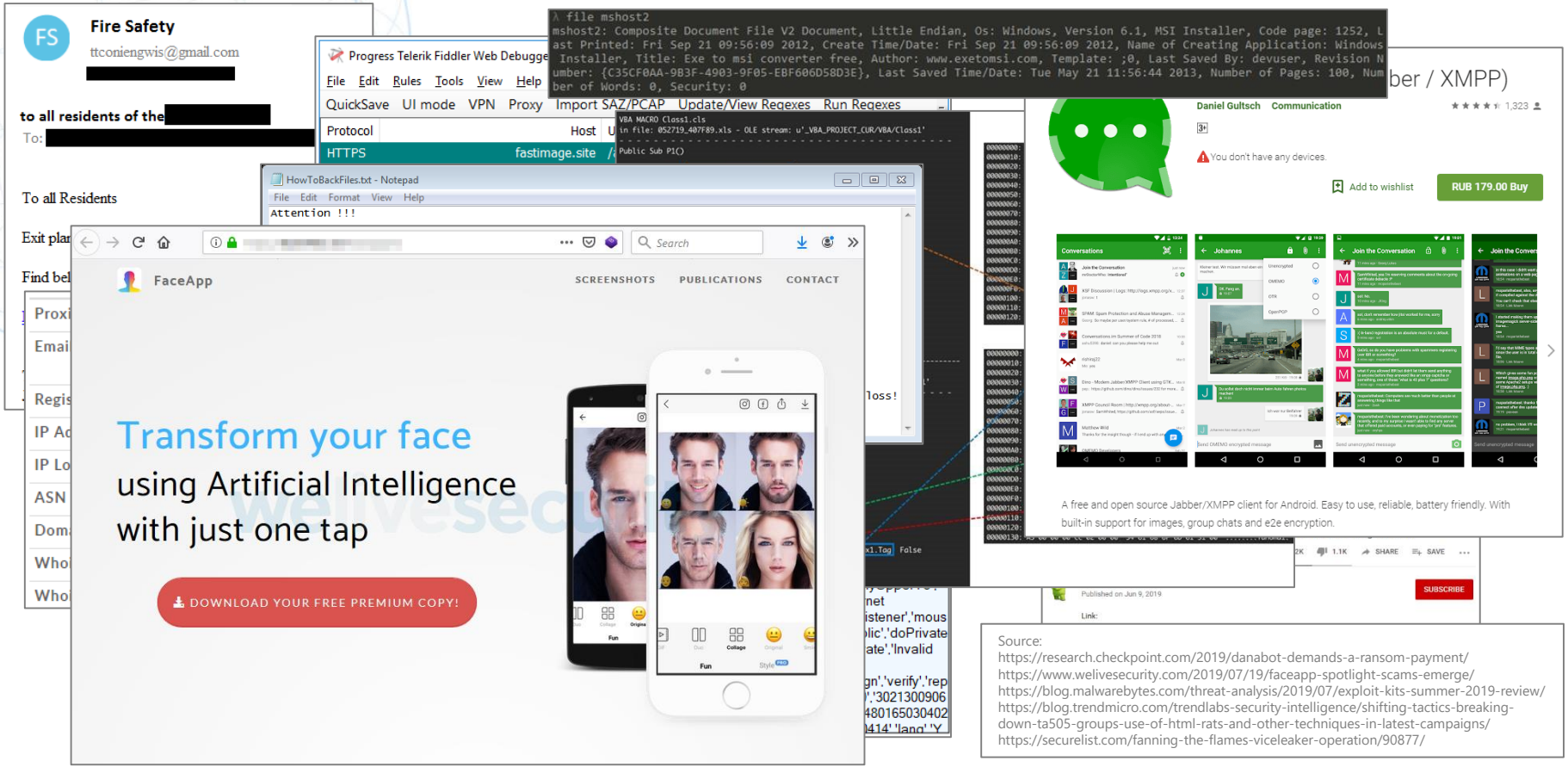


Visualization on Threat Reports

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

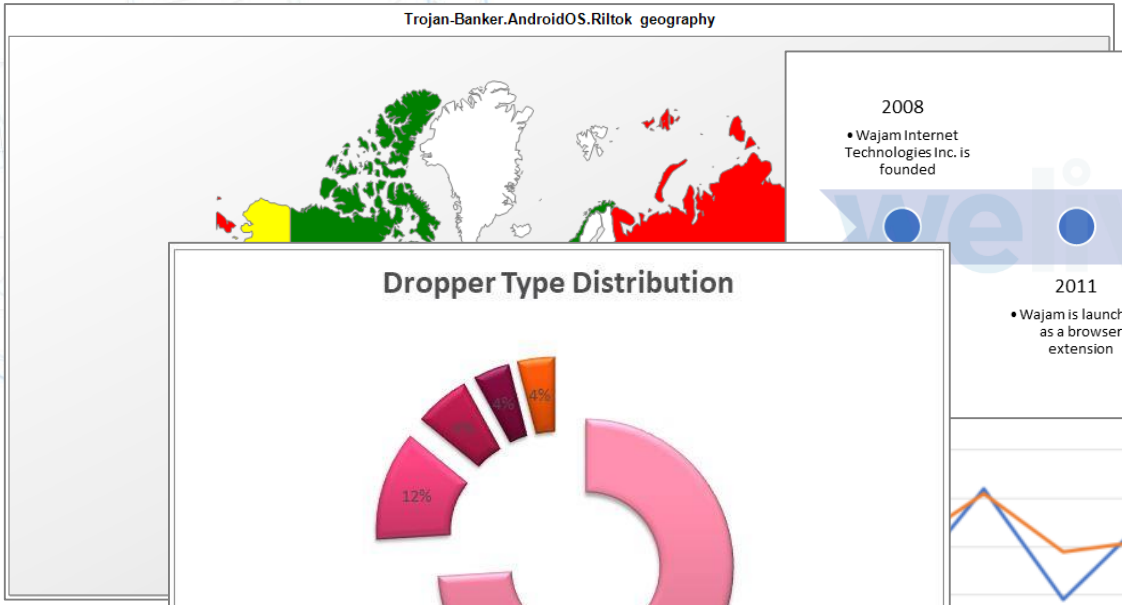


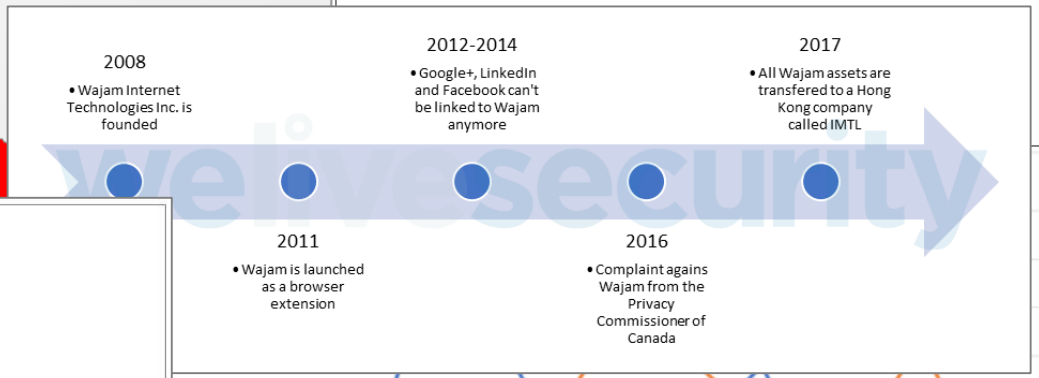
Screenshots



Source:
https://research.checkpoint.com/2019/danabot-demands-a-ransom-payment/
https://www.welivesecurity.com/2019/07/19/faceapp-spotlight-scams-emerge/
https://blog.malwarebytes.com/threat-analysis/2019/07/exploit-kits-summer-2019-review/
https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

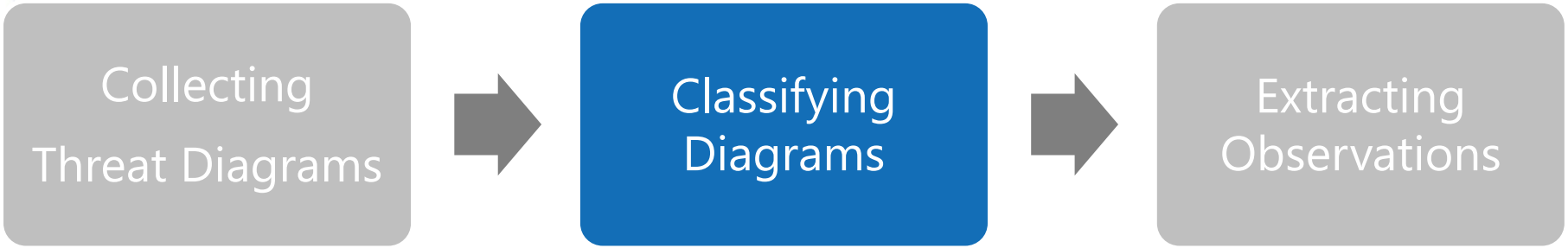
Statistics





Source:
https://securelist.com/mobile-banker-riltok/91374/
https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/
https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/
https://www.welivesecurity.com/2019/06/05/wajam-startup-massively-spread-adware/

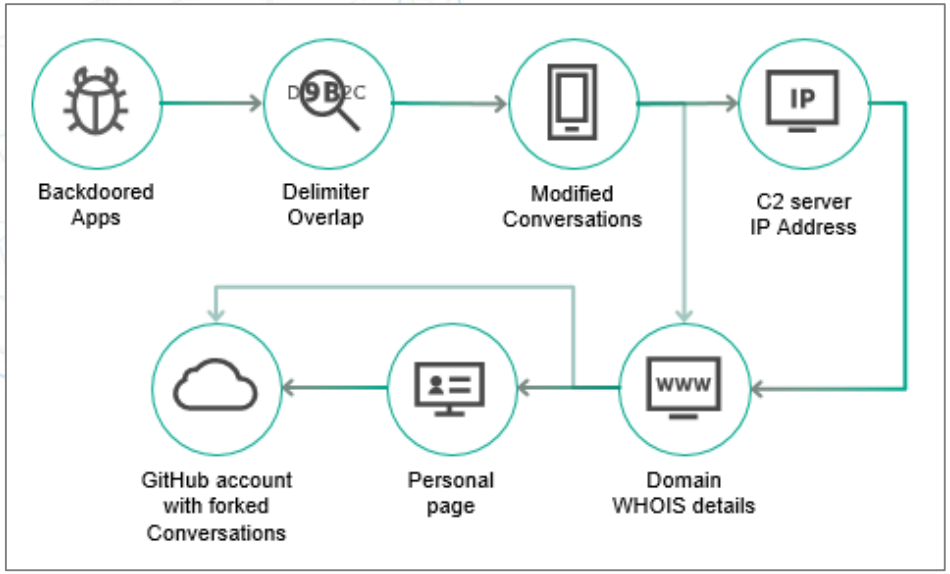
Process of Study

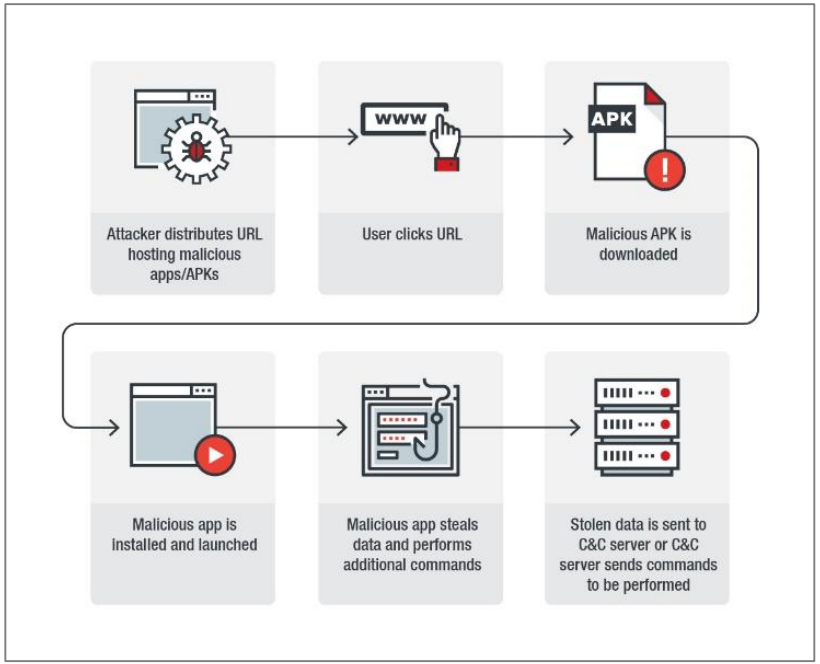


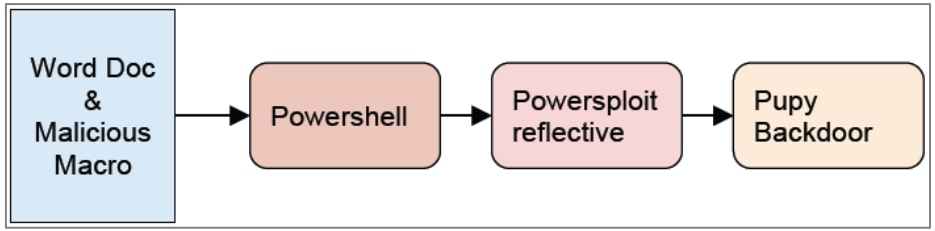
Classification on Why and How

- 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





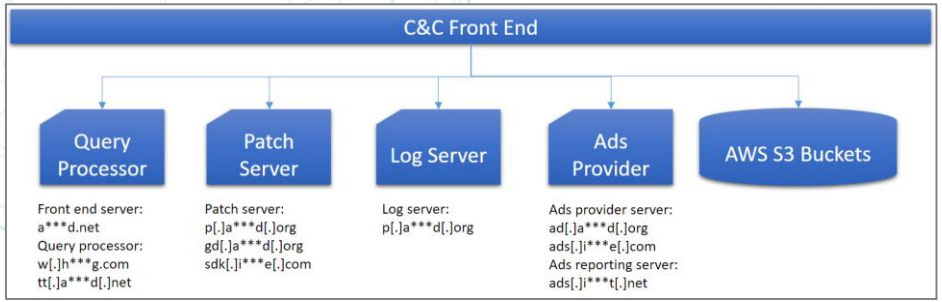


Source:
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/
https://securelist.com/twas-the-night-before/91599/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

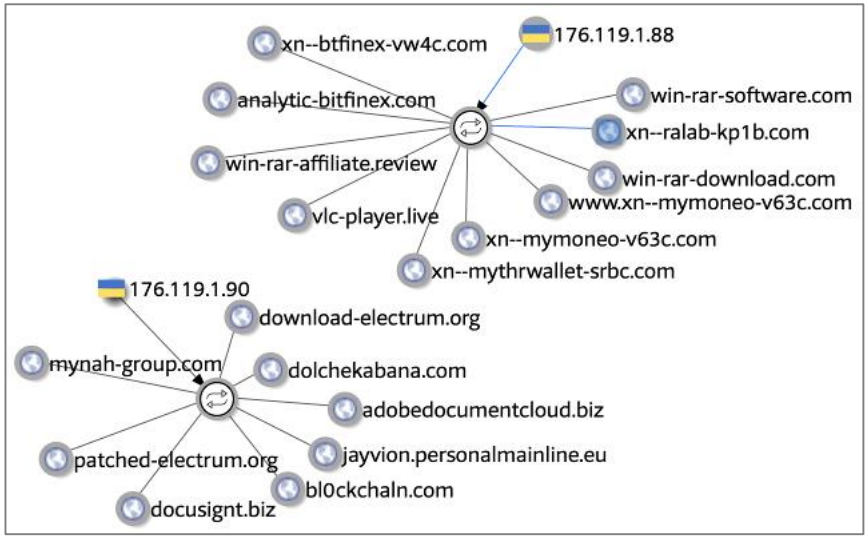
C2 Infrastructure

NTT Confidential

Directory Structure



Network Topology

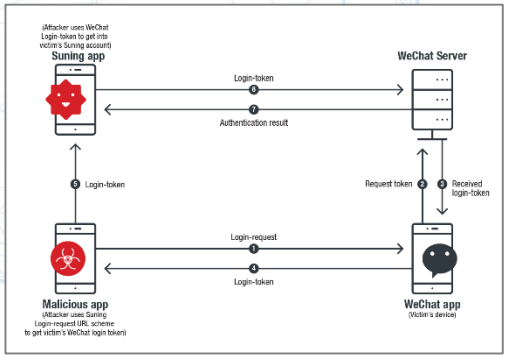


Source:
https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/
https://blog.malwarebytes.com/cybercrime/2019/07/no-mans-land-how-a-magecart-group-is-running-a-web-skimming-operation-from-a-war-zone/

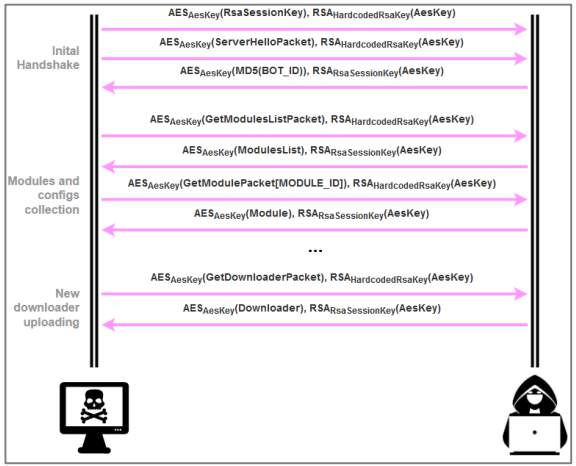
Malware Behavior

NTT Confidential

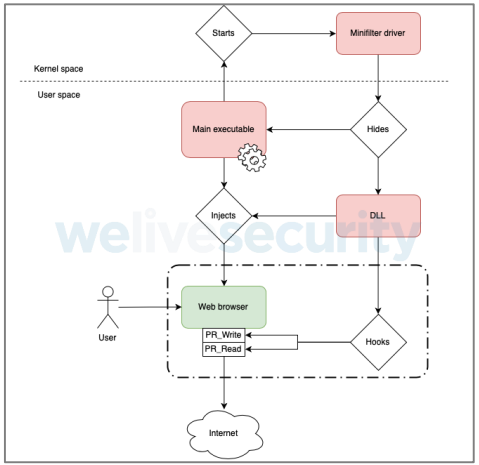
Attack Chain



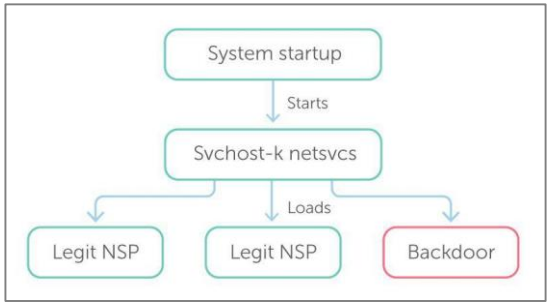
Sequence Diagram



Flow Chart

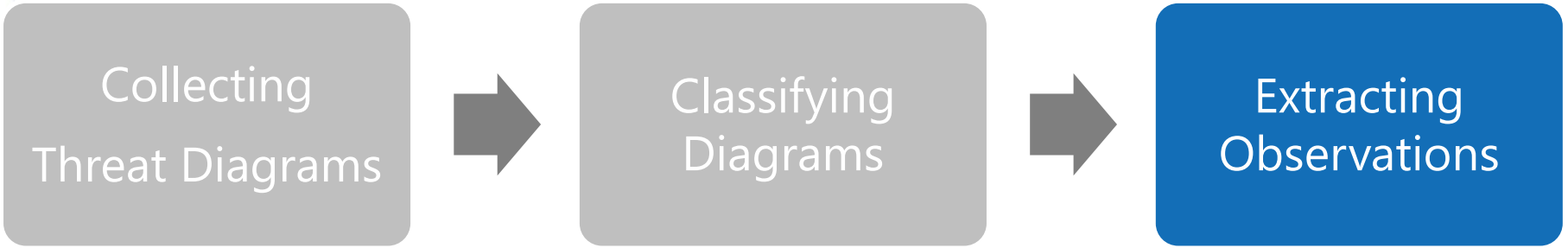


Function Structure



Source:
https://securelist.com/platinum-is-back/91135/
https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/
https://research.checkpoint.com/danabot-demands-a-ransom-payment/
https://www.welivesecurity.com/2019/06/05/wajam-startup-massively-spread-adware/

Process of Study

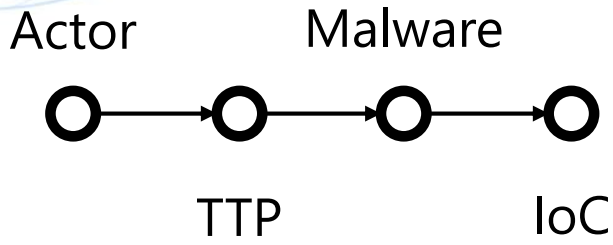


Visualization for Attack Flow

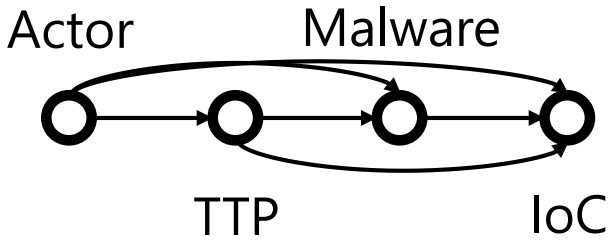
Observations

1. DAG Network with Edges between Adjacent Layers

Threat Diagram



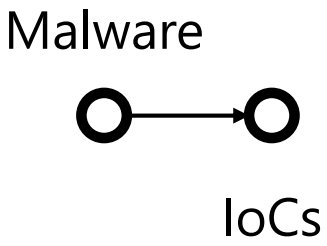
STIX Data



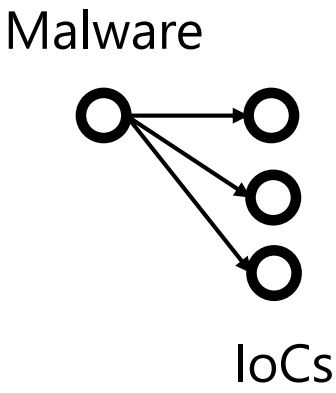
Observations

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

Threat Diagram



STIX Data



Observations

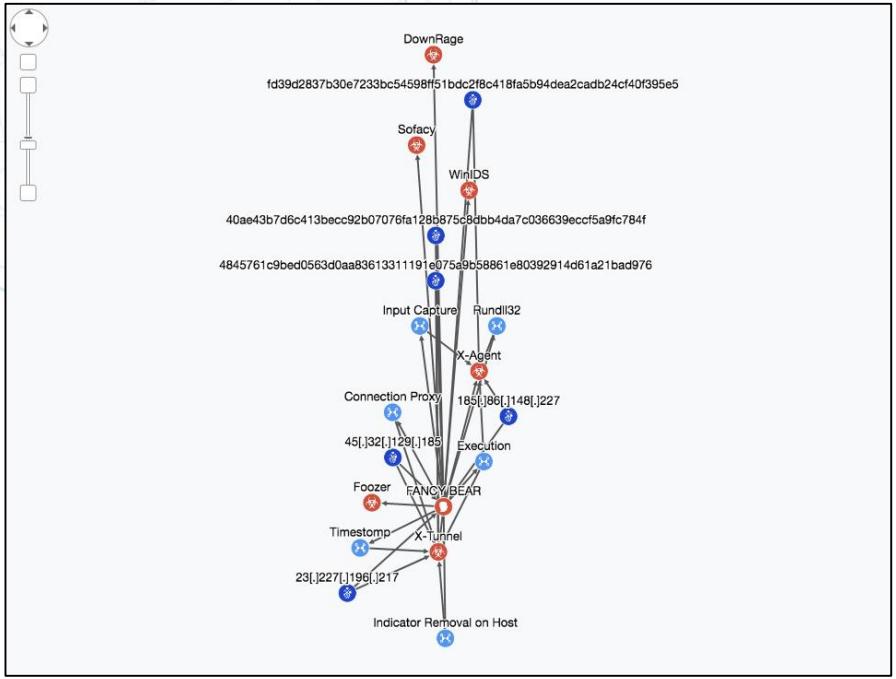
1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
3. Extracting Differences from Existing Intelligence
   - New Vulnerability
   - Same IoC
   - New Malware Component

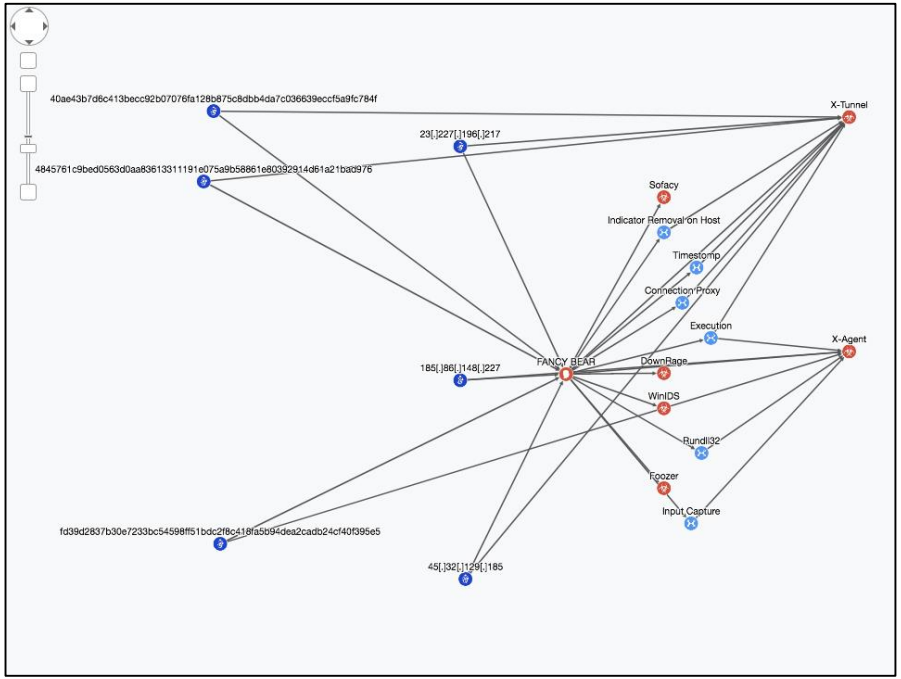
Outline

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

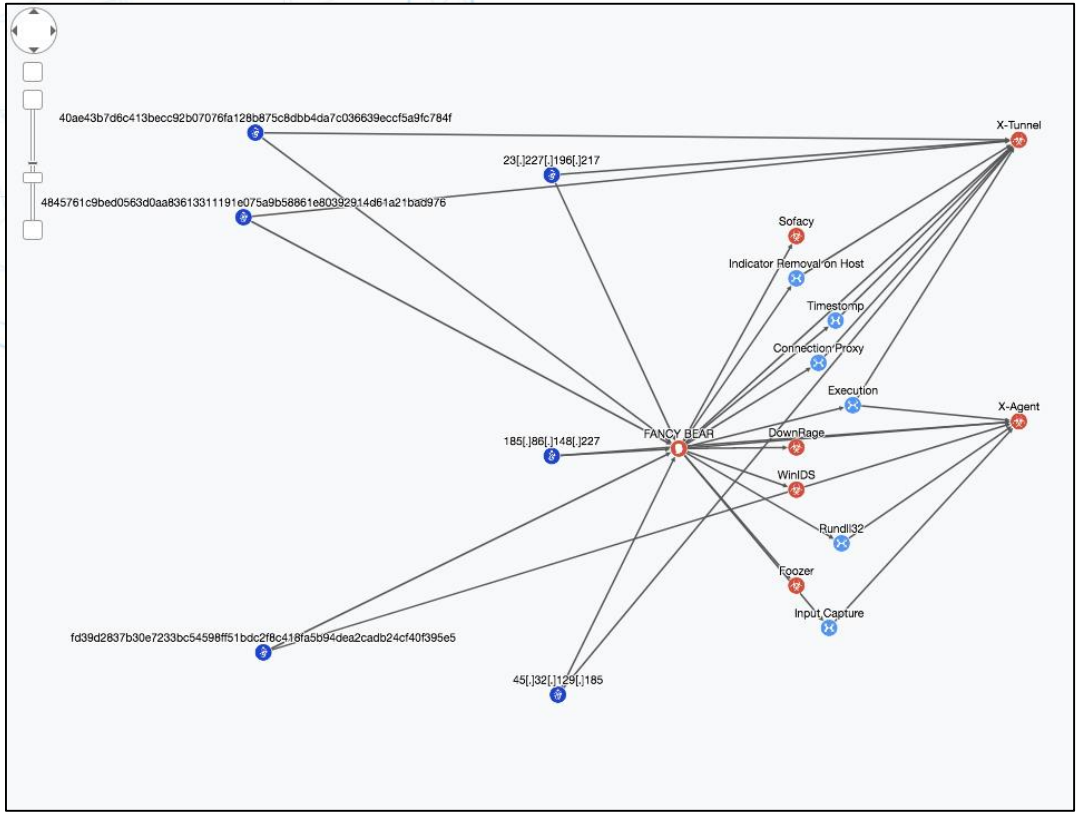
Layout for DAG (Directed Acyclic Graph)

NTT Confidential



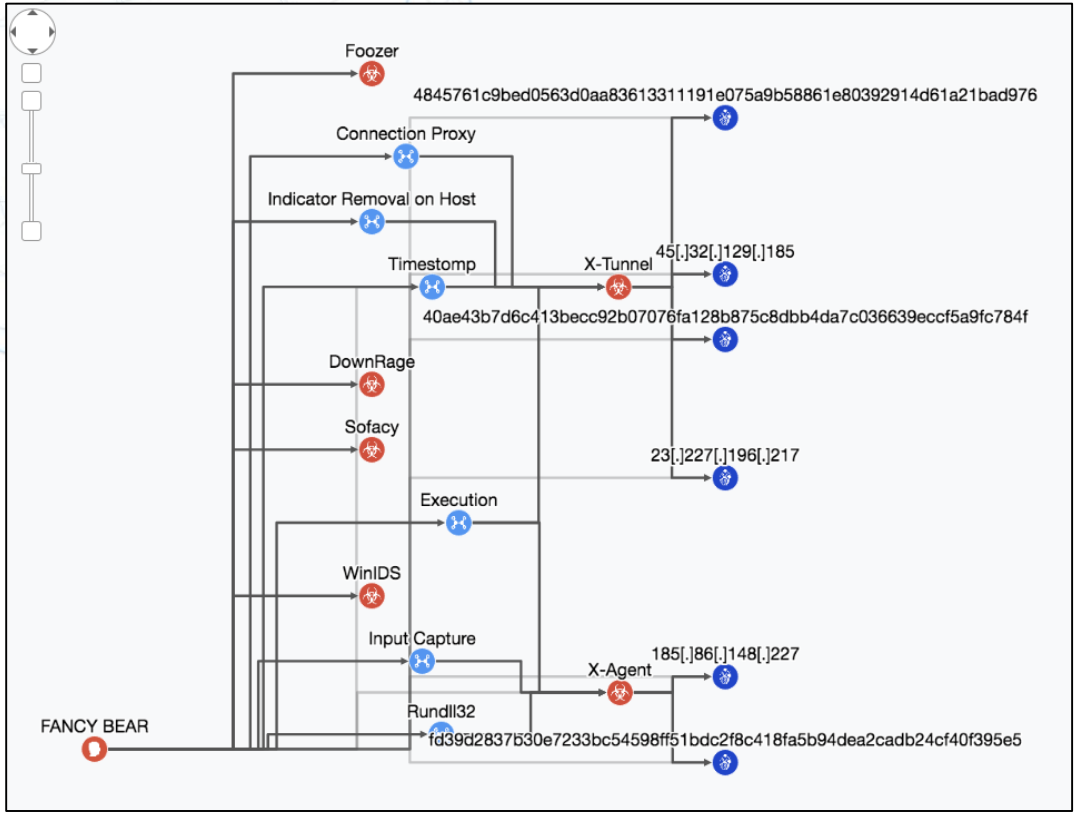


DAG Layout: Problems



- Hierarchical Order
  - Different order between STIX Edge and Diagrams
- Cross Layered Edges
  - Many Edges on Non-Adjective Layers

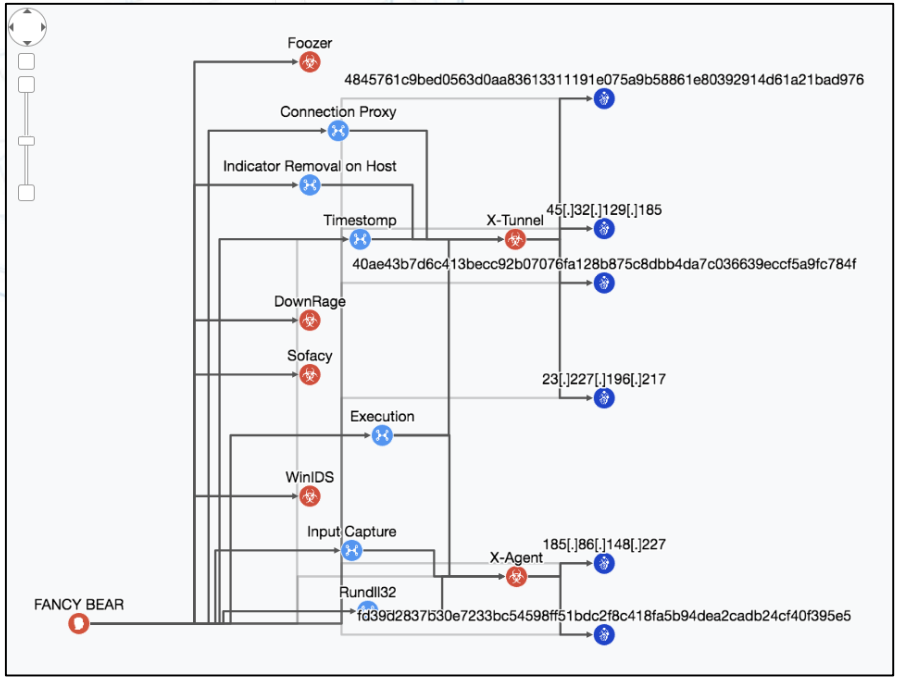
DAG Layout++

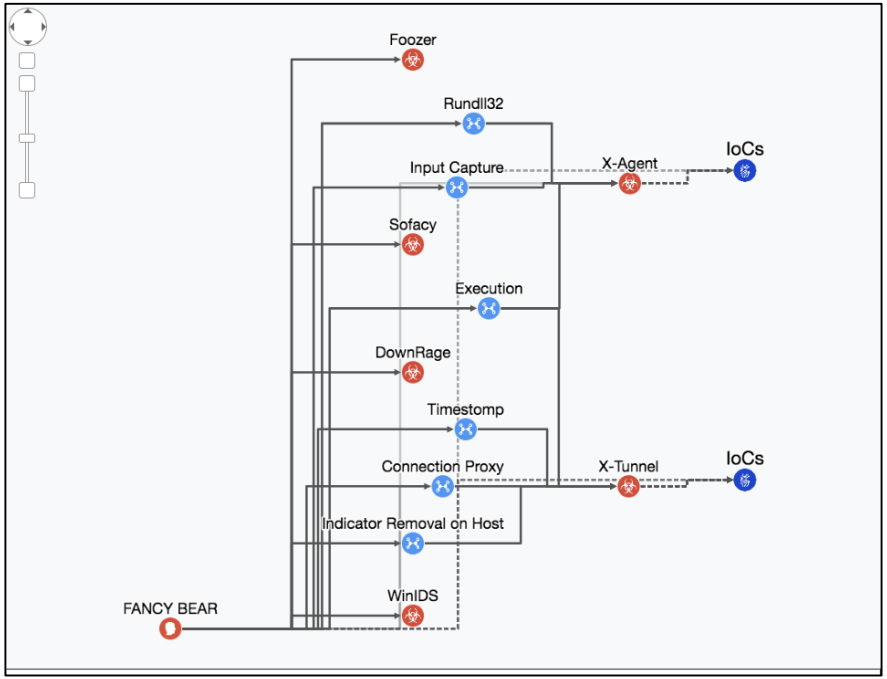


- Re-Mapping Edges
  - Remapping *indicates* Directions to Fit Intuition
- Orthogonal Routing
  - Eliminating cross edges
- De-Emphasize Edges on Non-Adjective Layers
  - Bellman Ford Method for Longest Path Problem with Negative Weights

Clustering IoCs based on Relationships

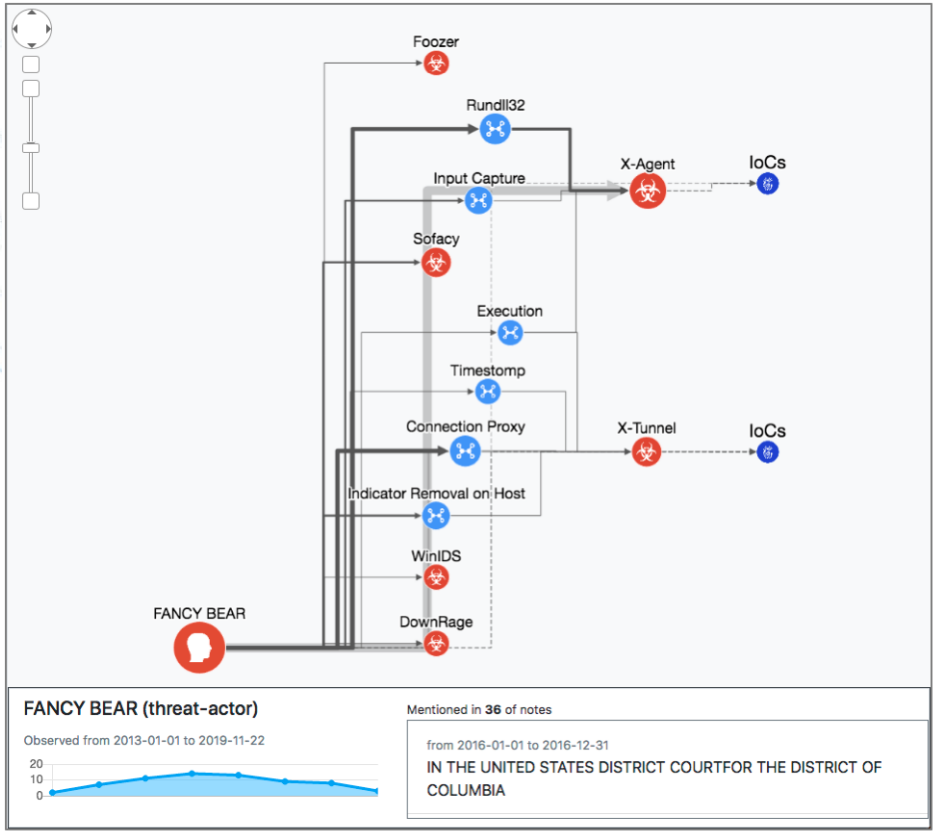
NTT Confidential

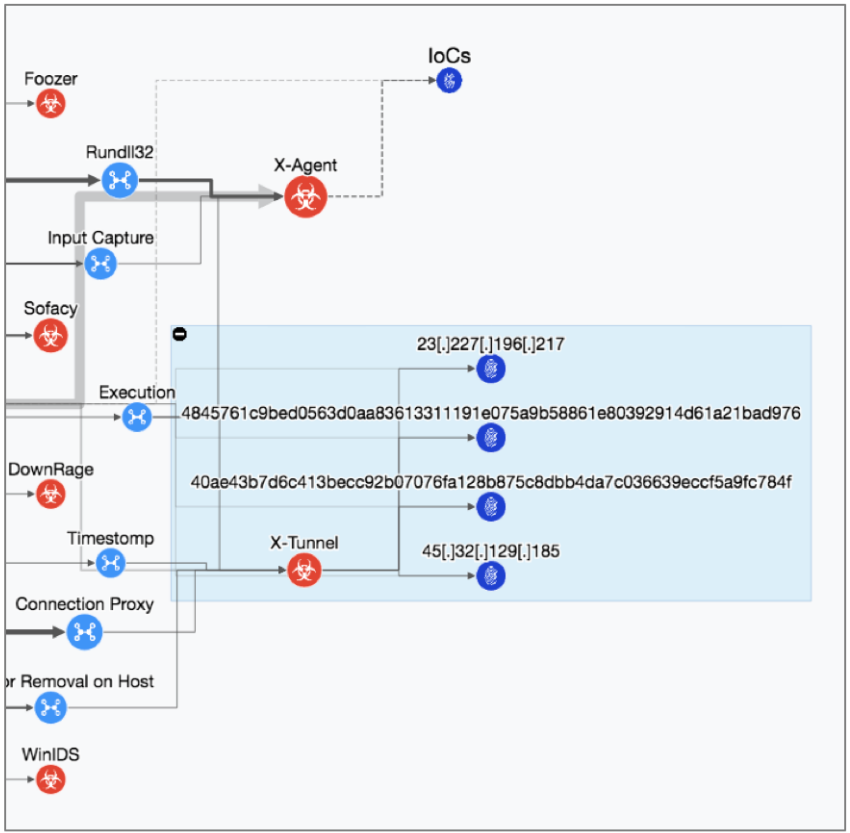




Emphasizing Differences

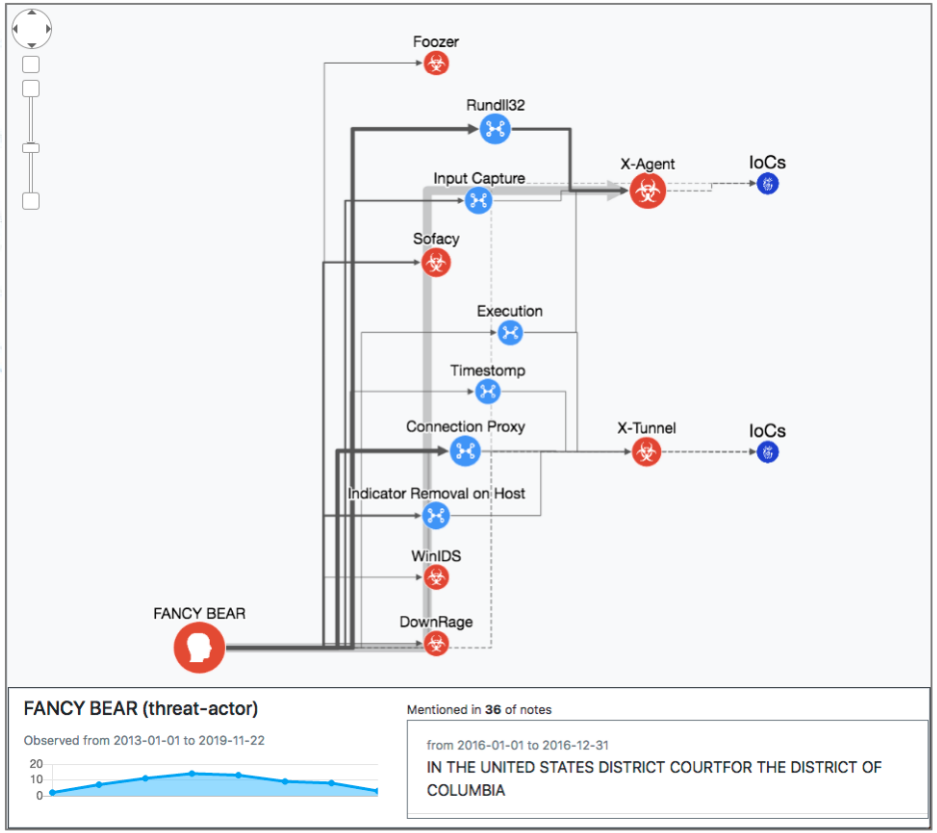
NTT Confidential

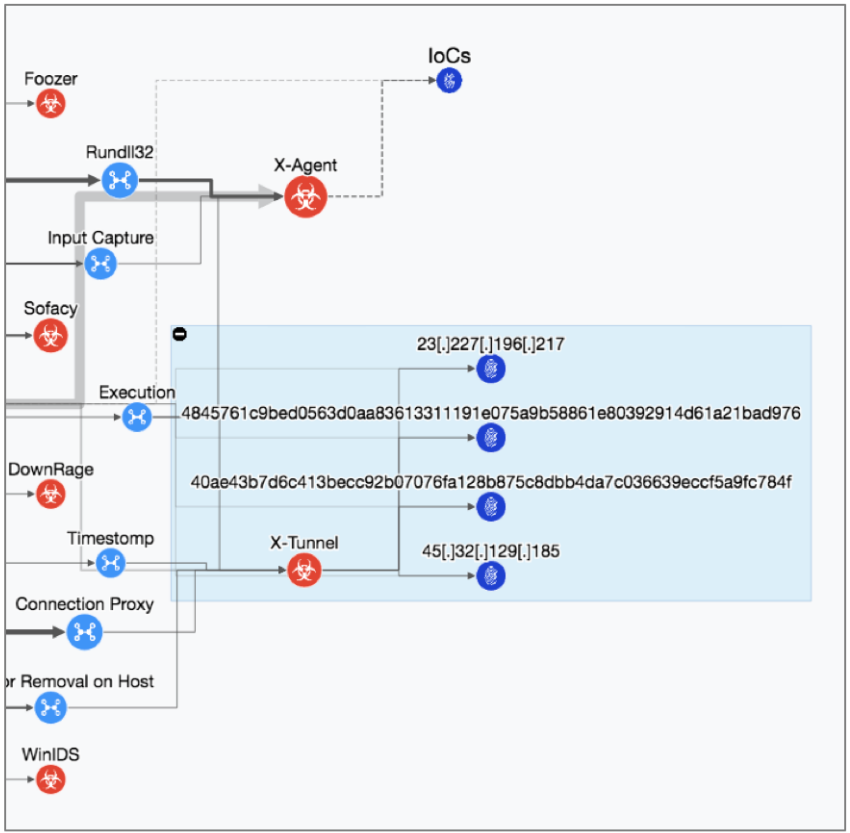




Emphasizing Differences

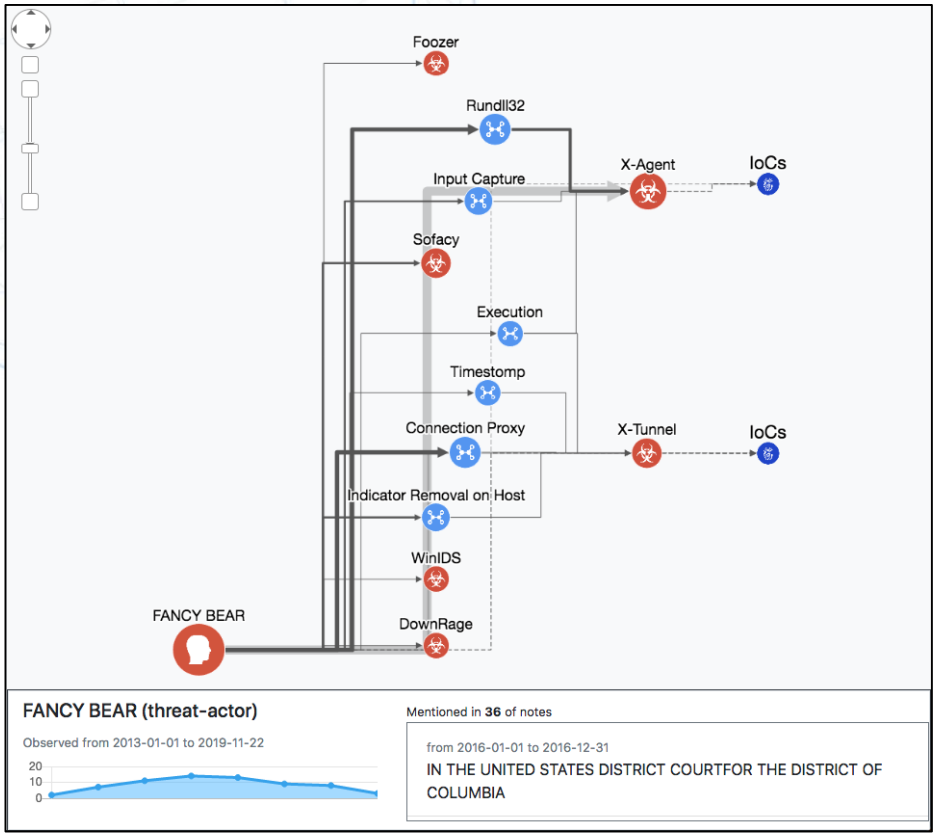
NTT Confidential





New Visualization based on Observations

NTT Confidential

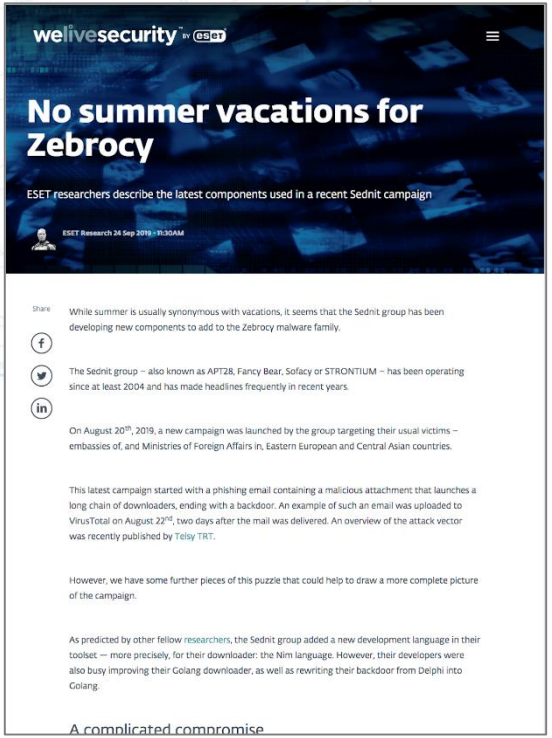


1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
3. Extracting Differences from Existing Intelligence

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



welivesecurity by eset

No summer vacations for Zebrocy

ESET researchers describe the latest components used in a recent Sednit campaign

ESET Research 24 Sep 2019 - 11:30AM

Share

While summer is usually synonymous with vacations, it seems that the Sednit group has been developing new components to add to the Zebrocy malware family.

The Sednit group – also known as APT28, Fancy Bear, Sofacy or STRONTIUM – has been operating since at least 2004 and has made headlines frequently in recent years.

On August 20th, 2019, a new campaign was launched by the group targeting their usual victims – embassies of, and Ministries of Foreign Affairs in, Eastern European and Central Asian countries.

This latest campaign started with a phishing email containing a malicious attachment that launches a long chain of downloaders, ending with a backdoor. An example of such an email was uploaded to VirusTotal on August 22nd, two days after the mail was delivered. An overview of the attack vector was recently published by Telsy TRT.

However, we have some further pieces of this puzzle that could help to draw a more complete picture of the campaign.

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.

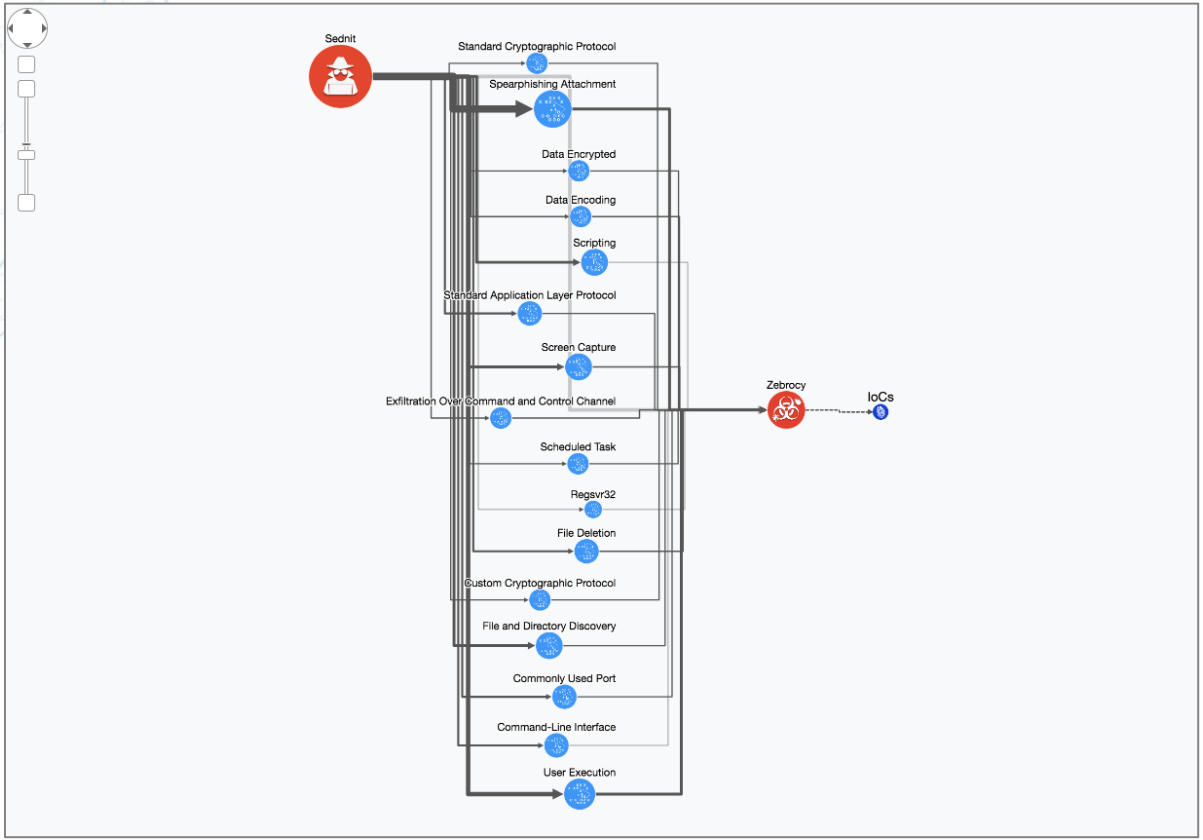
A complicated compromise

- 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/

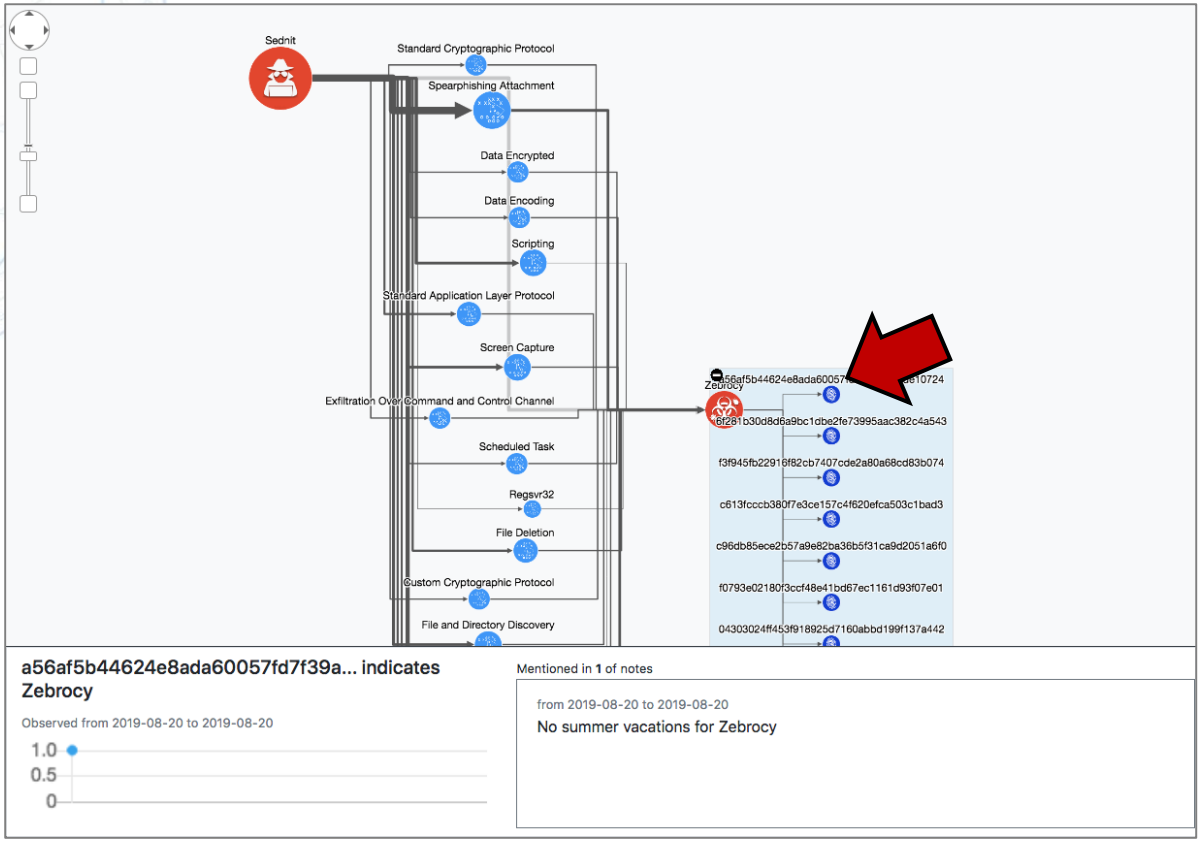
Example: An New Zebrocy Campaign

NTT Confidential



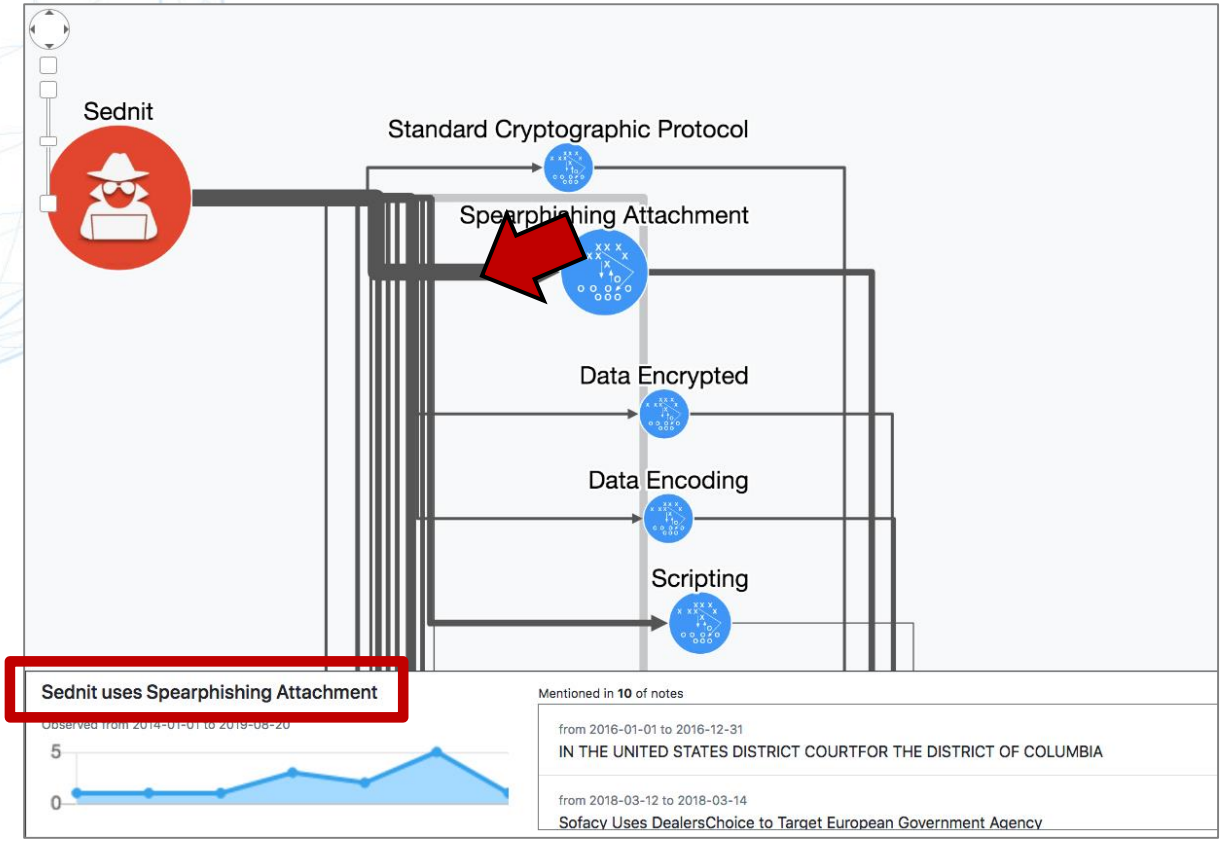
Example: An New Zebrocy Campaign

NTT Confidential



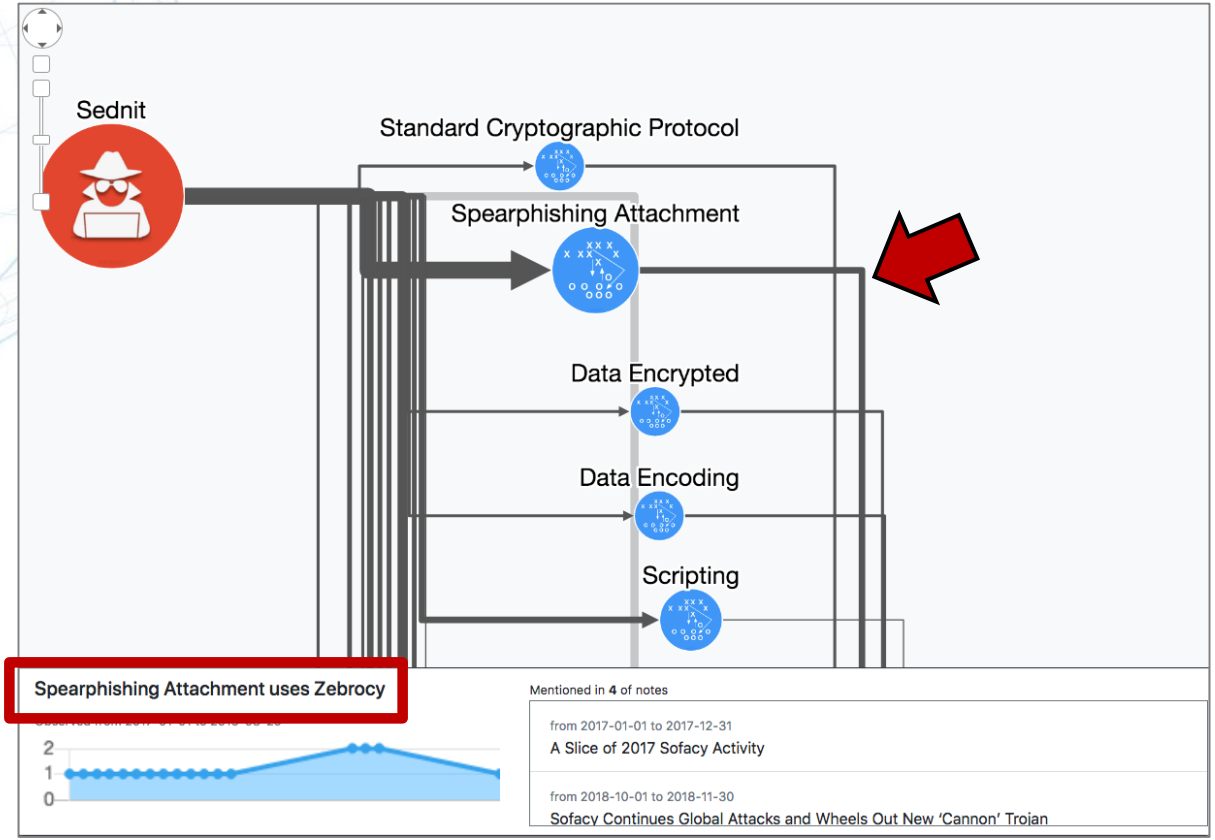
Example: An New Zebrocy Campaign

NTT Confidential



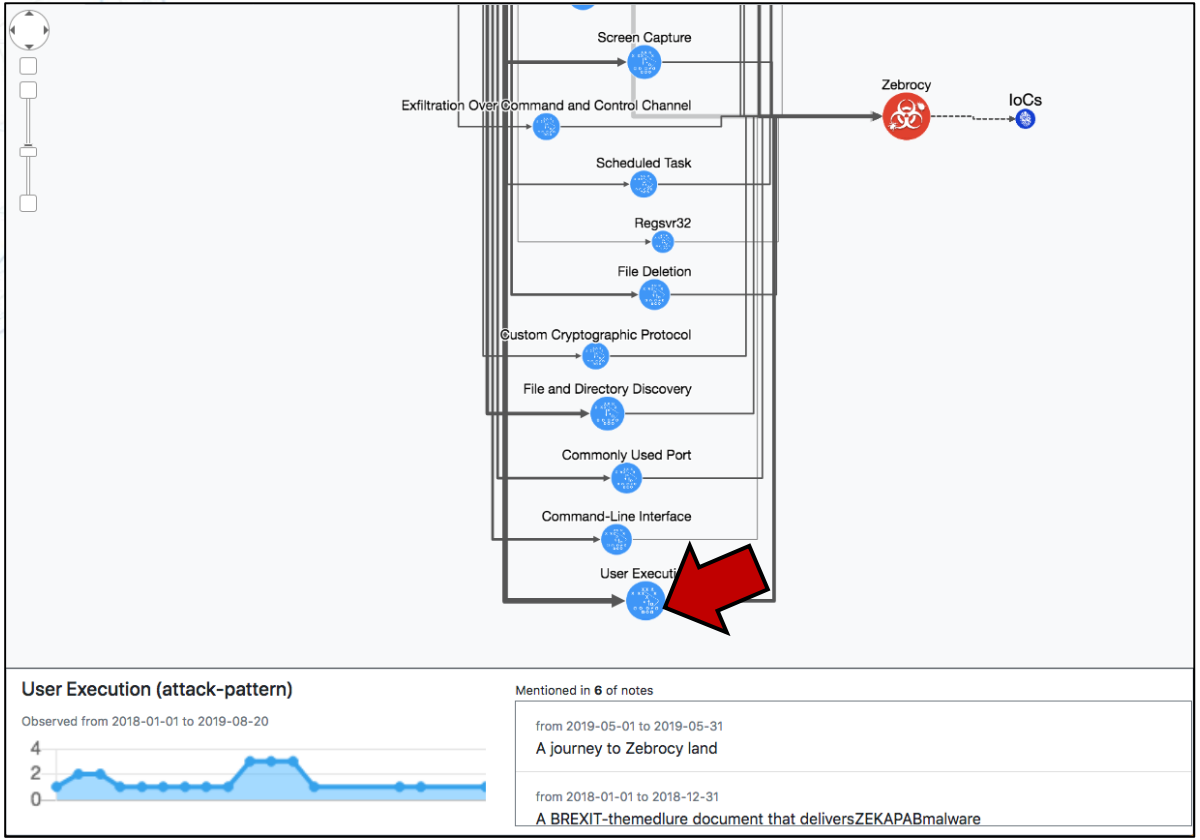
Example: An New Zebrocy Campaign

NTT Confidential



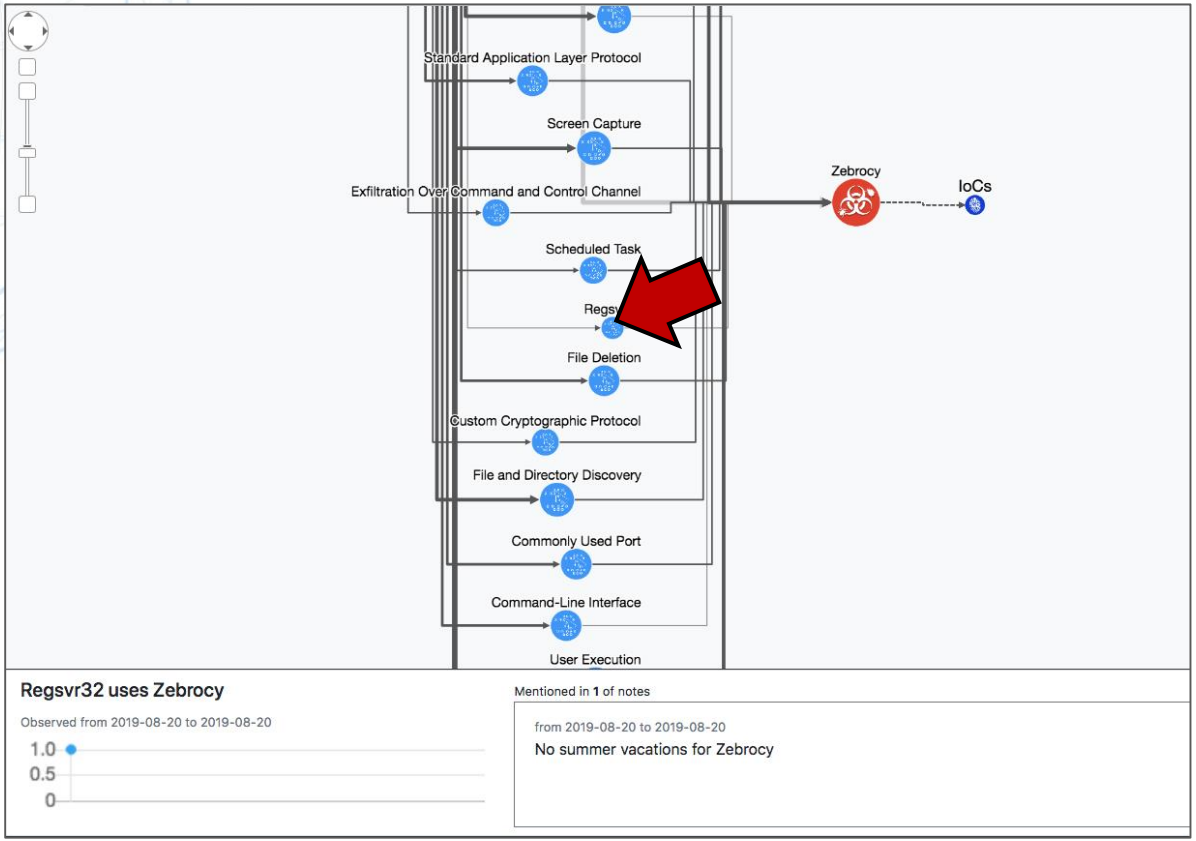
Example: An New Zebrocy Campaign

NTT Confidential



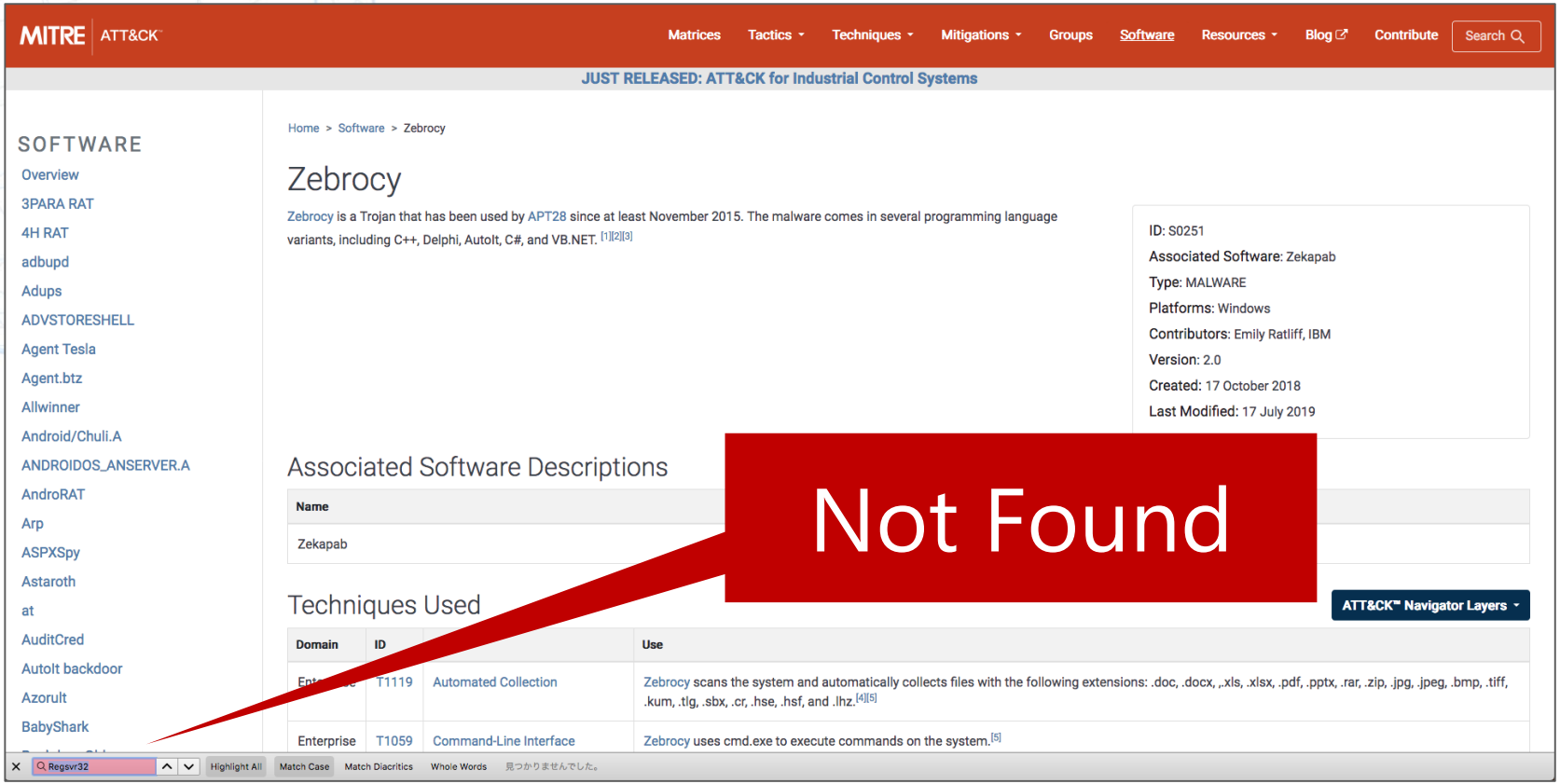
Example: An New Zebrocy Campaign

NTT Confidential



Example: An New Zebrocy Campaign

NTT Confidential



Example: An New Zebrocy Campaign

NTT Confidential

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`.

Outline

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

NTT Confidential

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