

# Rethinking the Graph Visualization for Threat Reports

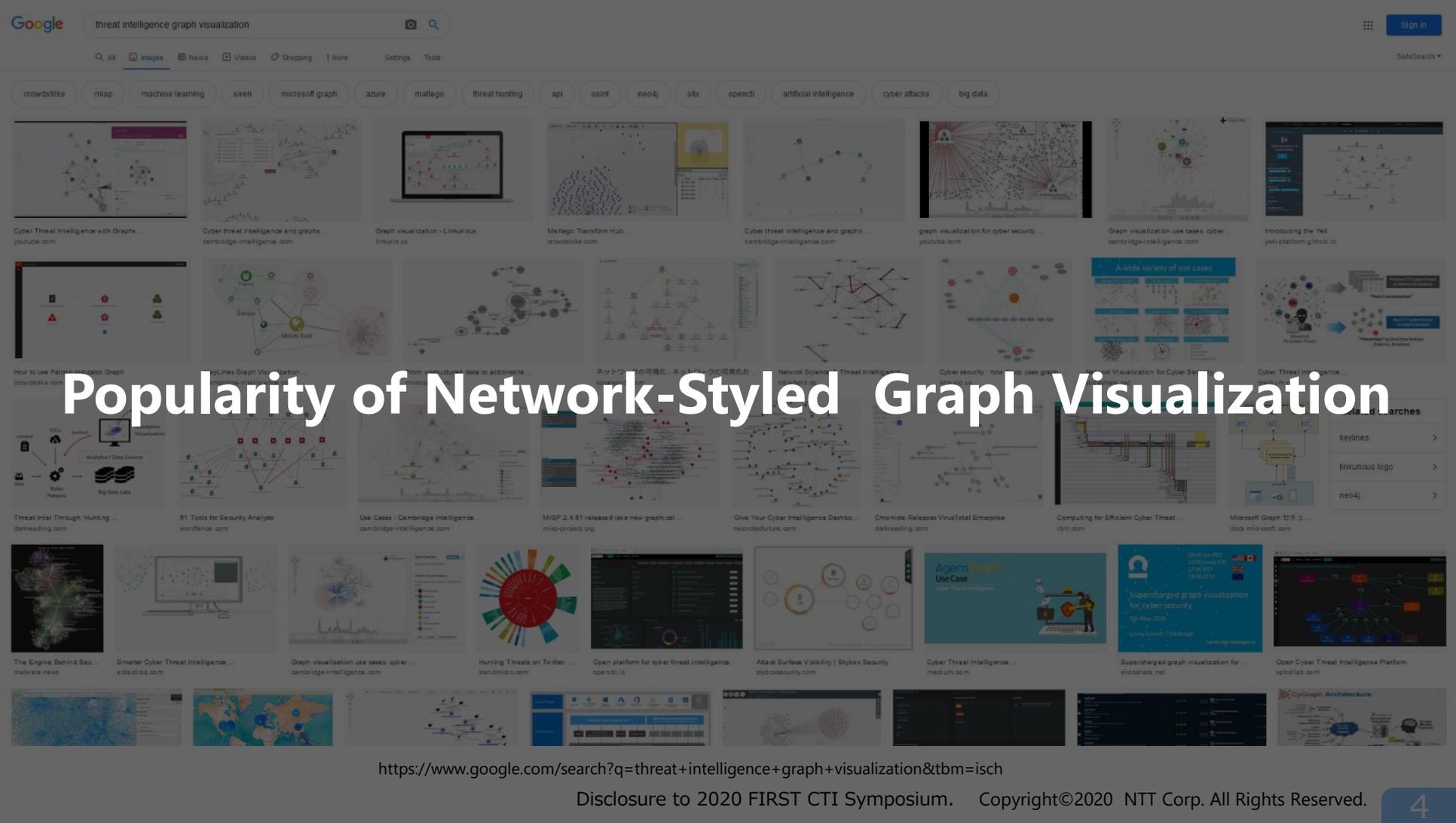
Mayo YAMASAKI, NTT-CERT

# 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



crowdstrike misp machine learning siren microsoft graph azure maltego threat hunting apt osint neo4j stix opend1 artificial intelligence cyber attacks big data

Cyber Threat Intelligence with Graphs ... youtube.com

Cyber threat intelligence and graphs ... cambridge-intelligence.com

Graph visualization - Linkurious linkurious.us

Maltego Transform Hub ... rowsswisse.com

Cyber threat intelligence and graphs ... cambridge-intelligence.com

graph visualization for cyber security ... youtube.com

Graph visualization use cases: cyber ... cambridge-intelligence.com

Introducing the Yell yell-platform.github.io

How to use Palo Alto Networks Graph ... rowsswisse.com

Lines Graph Visualization ... cambridge-intelligence.com

From structured data to actionable ... cambridge-intelligence.com

ネットワークの可視化 - ネットワークの可視化 ... cambridge-intelligence.com

Network Science Threat Intelligence ... cambridge-intelligence.com

Cyber security - how to use graph ... cambridge-intelligence.com

A wide variety of use cases ... cambridge-intelligence.com

Cyber Threat Intelligence ... cambridge-intelligence.com

Threat Intel Through 'Hunting' ... darkreading.com

51 Tools for Security Analysts ... wordfence.com

Use Cases - Cambridge Intelligence ... cambridge-intelligence.com

MISP 2.4.81 released (aka new graphical ... misp-project.org

Give Your Cyber Intelligence Dashbo ... reordofuture.com

Chronicle Releases VirusTotal Enterprise ... darkreading.com

Computing for Efficient Cyber Threat ... ibm.com

Microsoft Graph 72年 ... docs.microsoft.com

The Engine Behind Sec ... malware.news

Smarter Cyber Threat Intelligence ... sileadici.com

Graph visualization use cases: cyber ... cambridge-intelligence.com

Hunting Threats on Twitter ... trendmicro.com

Open platform for cyber threat intelligence ... opend1.io

Atak Surface Visibility | Skybox Security skyboxsecurity.com

Cyber Threat Intelligence ... medium.com

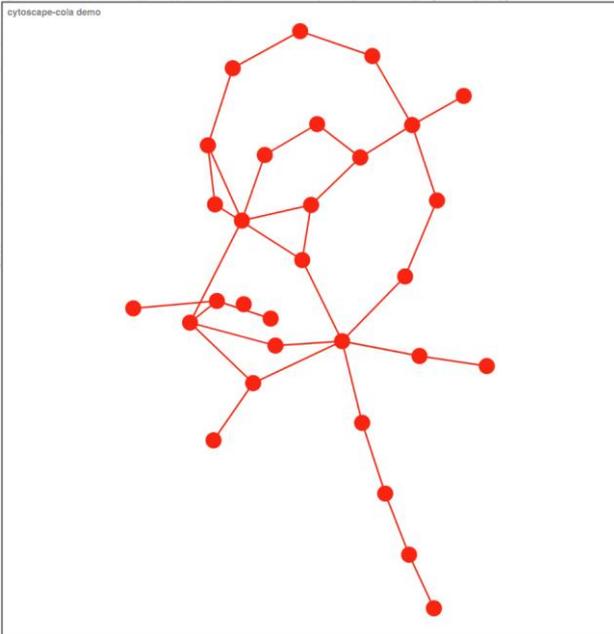
Supercharged graph visualization for ... slideshare.net

Open Cyber Threat Intelligence Platform xploitlab.com

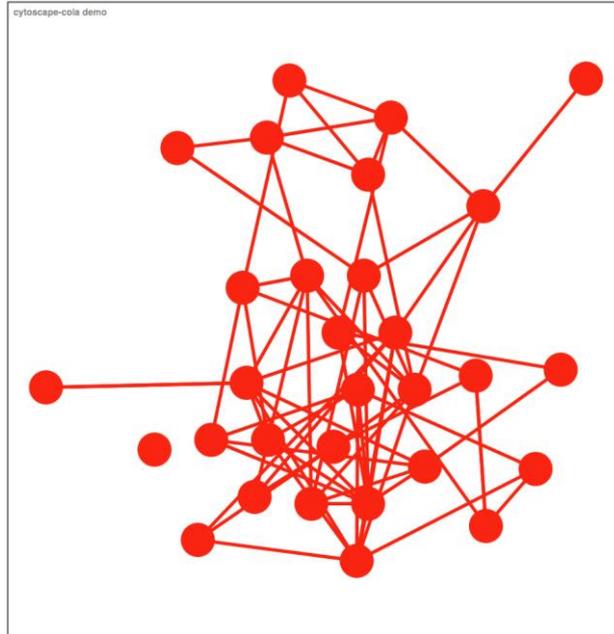
# Popularity of Network-Styled Graph Visualization

# Problems with Dense Graph

**density = 0.08**



**density = 0.16**



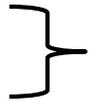
**density = 0.32**



These graphs have 30 nodes, and edges are randomly created according to each density.  
$$\text{density} = \frac{|\text{Edge}|}{(|\text{Node}| * (|\text{Node}| - 1))}$$

# How to Improve Graph Visualization?

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



**Impossible for Non-experts**



# How to Improve Graph Visualization?

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

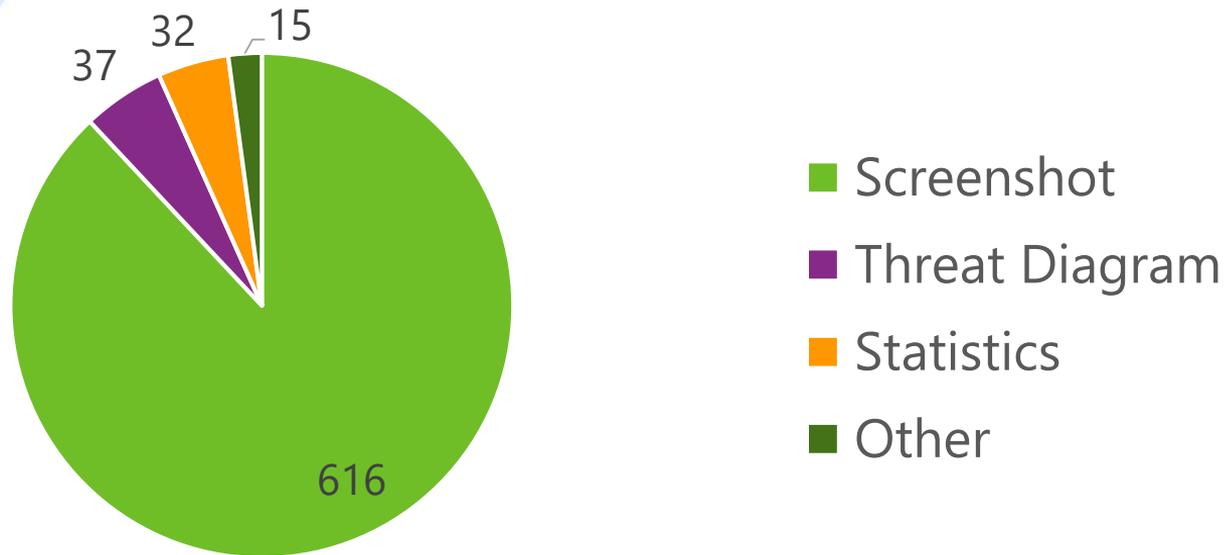


# Process of Study

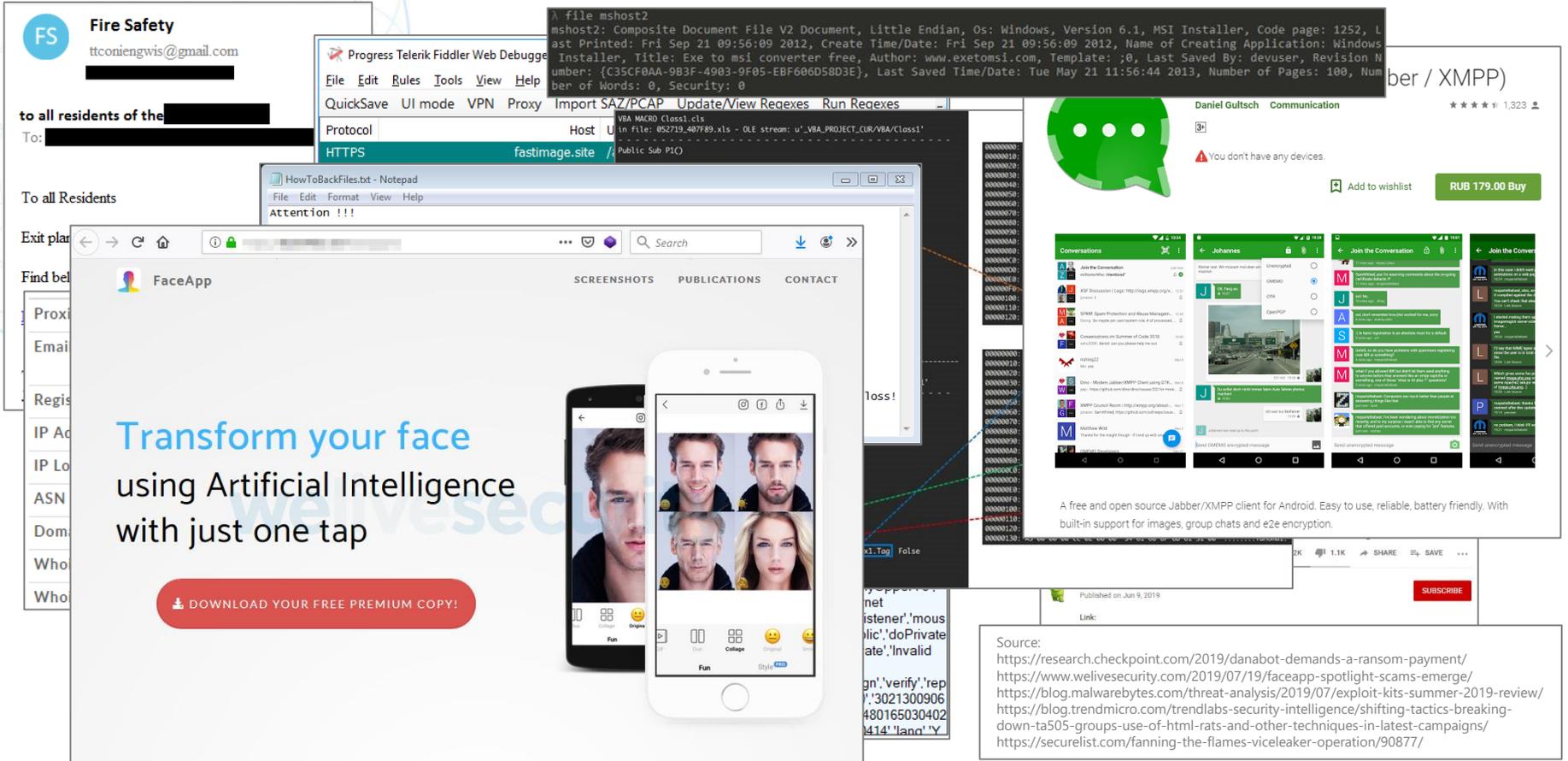


# Visualization on Threat Reports

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



# Screenshots



**Fire Safety**  
ttconienewis@gmail.com

to all residents of the [redacted]

To all Residents

Exit plan

Find be

Proxi

Email

Regis

IP Ac

IP Lo

ASN

Dom

Who

Who

**Transform your face using Artificial Intelligence with just one tap**

DOWNLOAD YOUR FREE PREMIUM COPY!

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

QuickSave UI mode VPN Proxy Import SAZ/PCAP Update/View Regexes Run Regexes

Protocol Host U

HTTPS fastimage.site / Public Sub P10

VBA MACRO Class1.cls

In file: 852719\_40789.xls - OLE stream: u'\\\_VBA\_PROJECT\_CUR/VBA/Class1'

Attention !!!

SCREENSHOTS PUBLICATIONS CONTACT

FaceApp

net listener 'mouse', doPrivate, 'Invalid

gn', verify', rep', '3021300906', 480165030402', '414'land', Y

A file mshost2

mshost2: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, MSI Installer, Code page: 1252, Last Printed: Fri Sep 21 09:56:09 2012, Create Time/Date: Fri Sep 21 09:56:09 2012, Name of Creating Application: Windows Installer, Title: Exe to msi converter free, Author: www.exetomsi.com, Template: ;0, Last Saved By: devuser, Revision Number: {C35CF0AA-9B3F-4983-9F05-EBF606D58D3E}, Last Saved Time/Date: Tue May 21 11:56:44 2013, Number of Pages: 100, Number of Words: 0, Security: 0

Daniel Gultsch Communication

★ ★ ★ ★ 1,323

⚠ You don't have any devices.

Add to wishlist RUB 179.00 Buy

Conversations

Join the Conversation

Join the Conversation

Join the Conversation

Join the Conversation

A free and open source Jabber/XMPP client for Android. Easy to use, reliable, battery friendly. With built-in support for images, group chats and e2e encryption.

Published on Jun 9, 2019

Link:

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/>

Trojan-Banker.AndroidOS.Riltok geography



**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

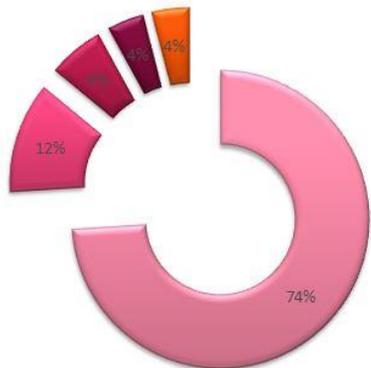
**2016**

- Complaint against Wajam from the Privacy Commissioner of Canada

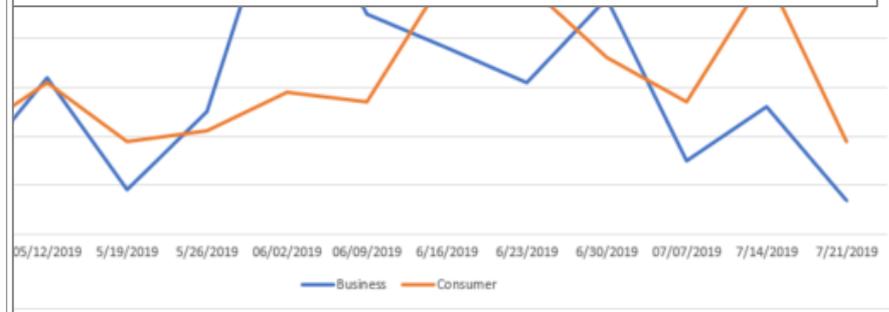
**2017**

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

Dropper Type Distribution



■ Games 
 ■ Photo Utility 
 ■ System Utility 
 ■ Adult Entertainment 
 ■ Media Player



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



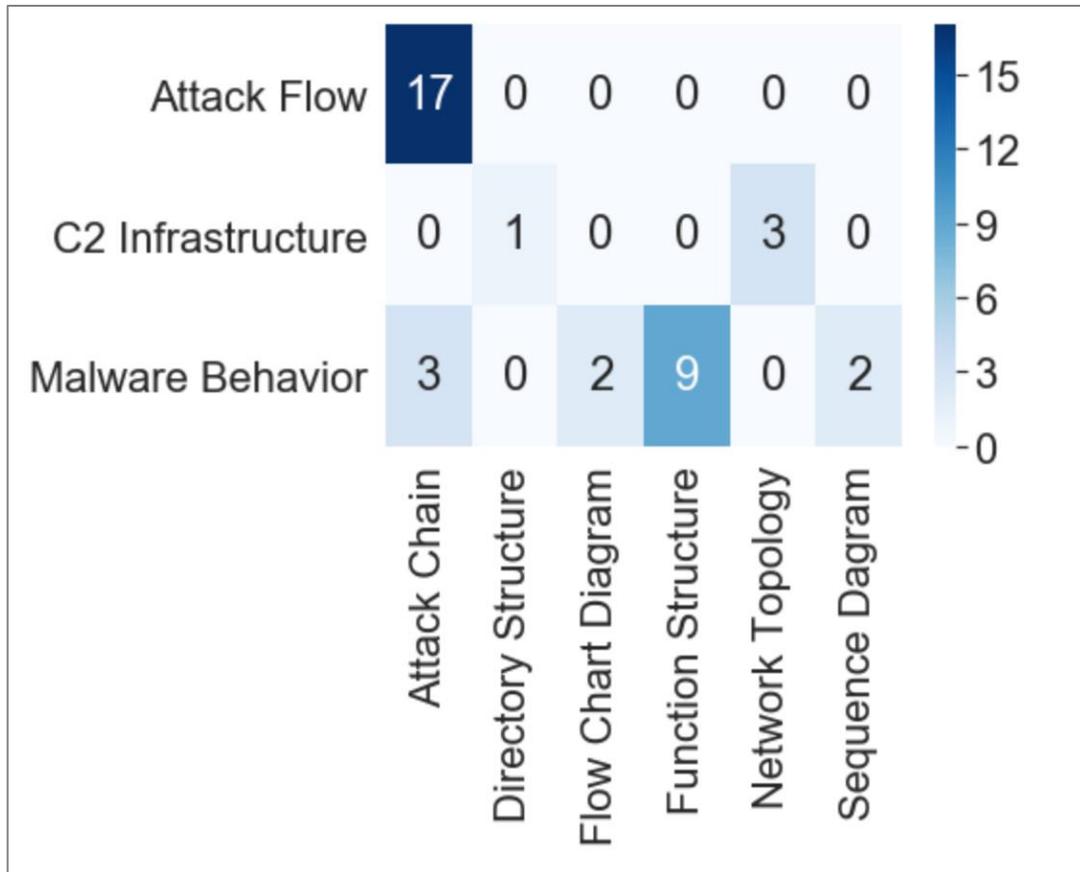
# Classification on Why and How

## ■ Why?

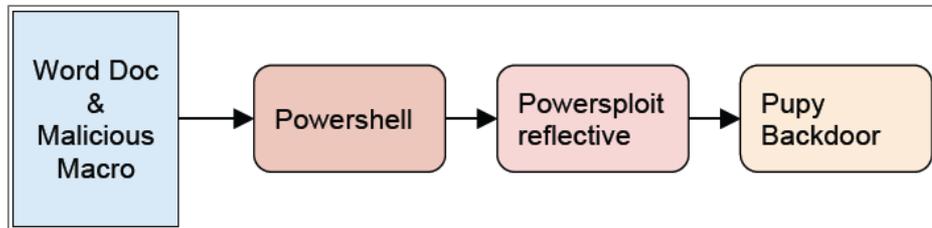
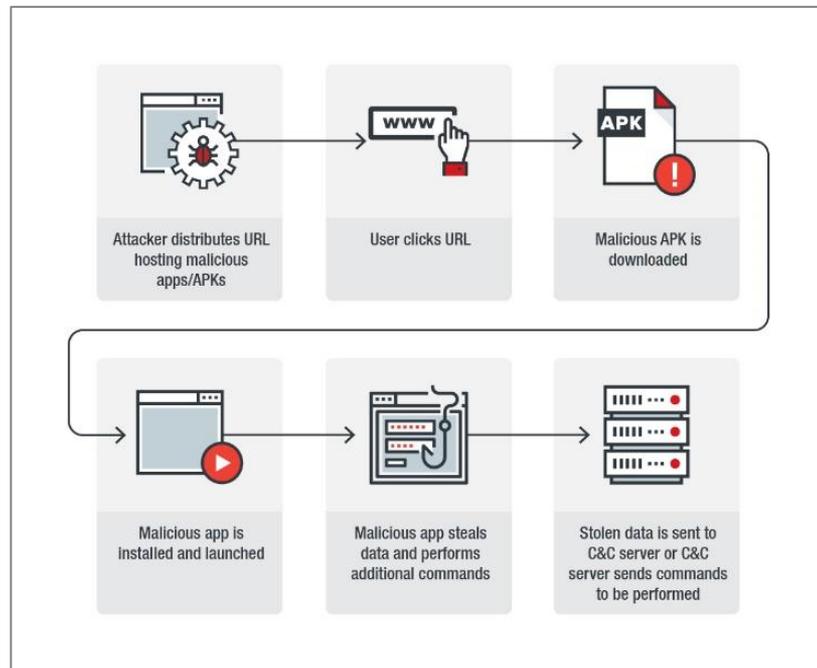
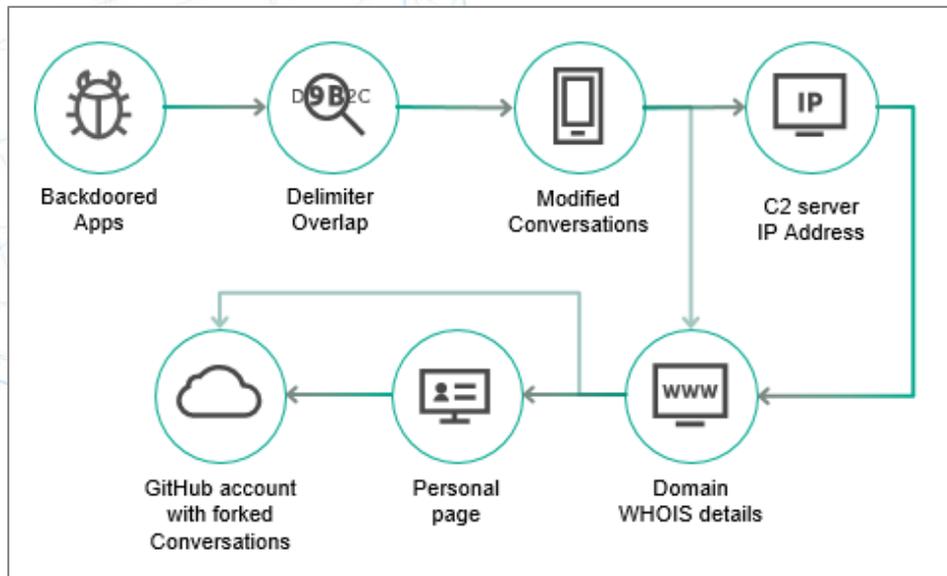
1. Attack Flow
2. C2 Infrastructure
3. Malware Behavior

## ■ How?

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

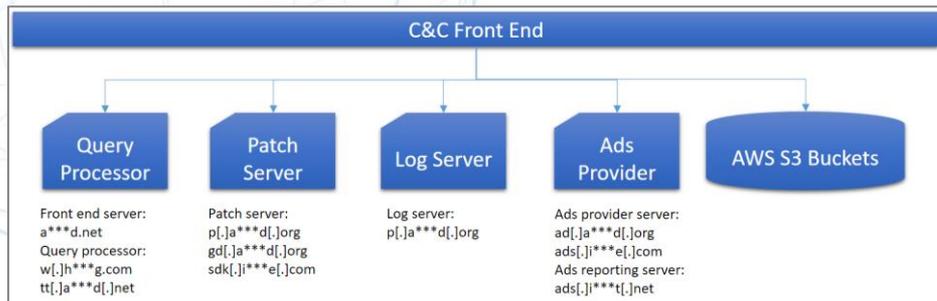


# Attack Flow - Attack Chain

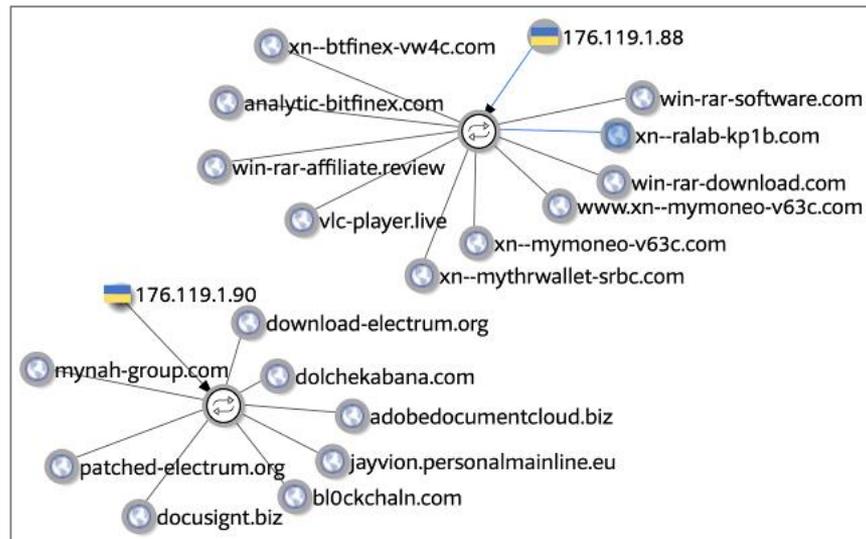


Source:  
<https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/>  
<https://securelist.com/twas-the-night-before/91599/>  
<https://securelist.com/fanning-the-flames-viceleaker-operation/90877/>

## Directory Structure



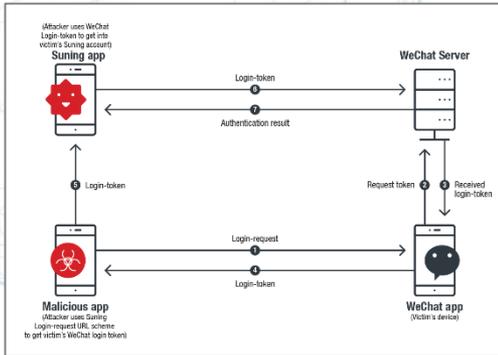
## Network Topology



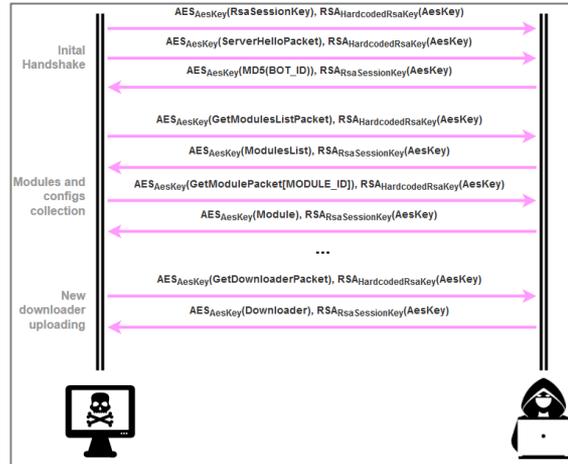
Source:  
<https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/>  
<https://blog.malwarebytes.com/cybercrime/2019/07/no-mans-land-how-a-magecart-group-is-running-a-web-skimming-operation-from-a-war-zone/>

# Malware Behavior

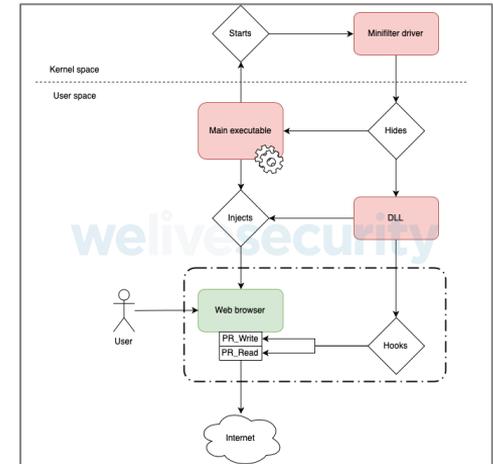
## Attack Chain



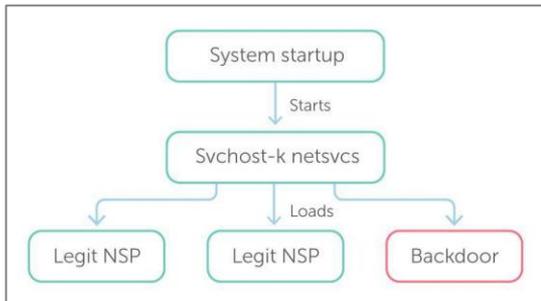
## Sequence Diagram



## Flow Chart



## Function Structure

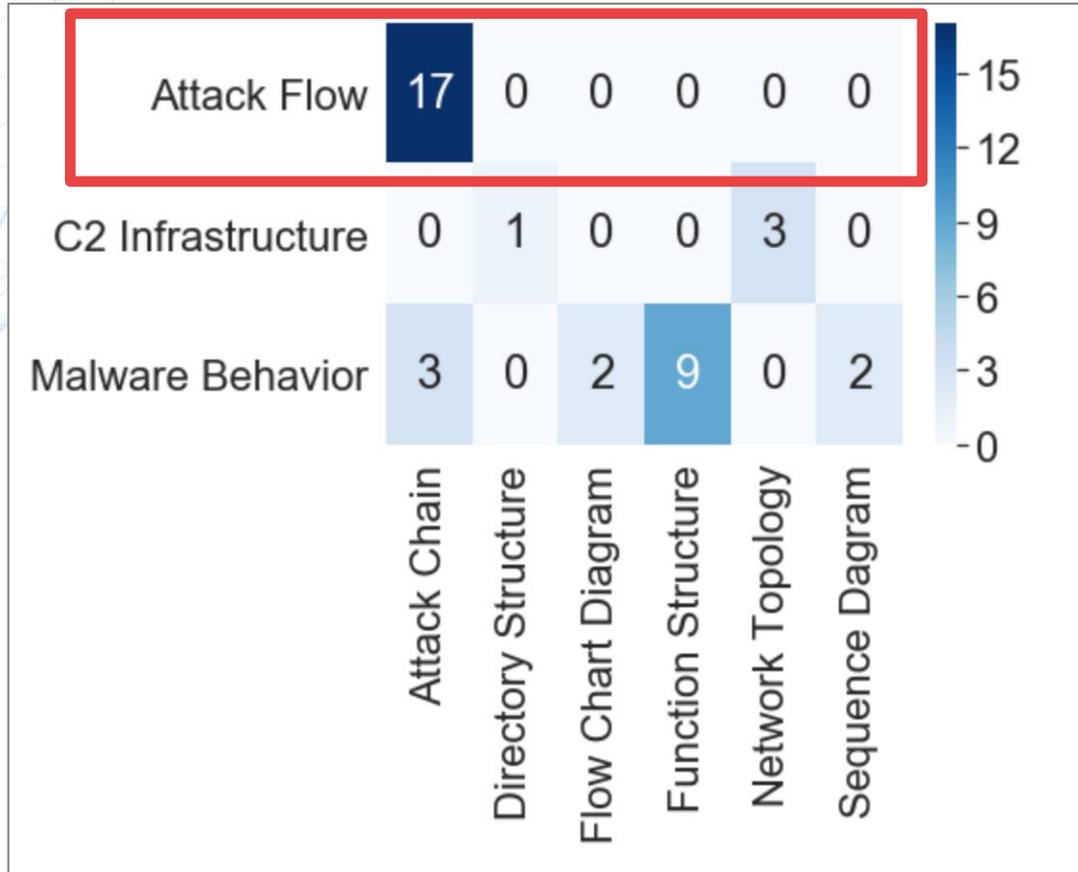


Source:  
<https://securelist.com/platinum-is-back/91135/>  
<https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/>  
<https://research.checkpoint.com/danabot-demands-a-ransom-payment/>  
<https://www.welivesecurity.com/2019/06/05/wajam-startup-massively-spread-adware/>

# Process of Study



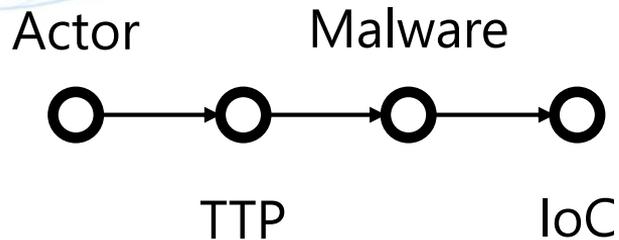
# Visualization for Attack Flow



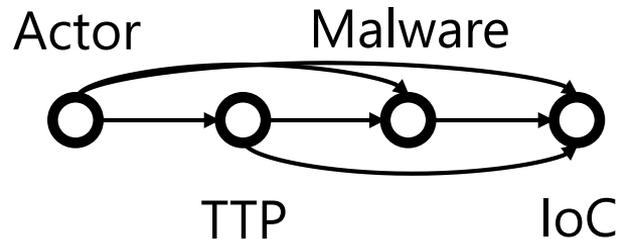
# Observations

## 1. DAG Network with Edges between Adjacent Layers

### Threat Diagram



### STIX Data

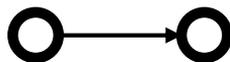


# Observations

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

## Threat Diagram

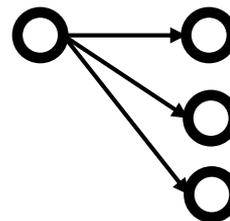
Malware



IoCs

## STIX Data

Malware



IoCs

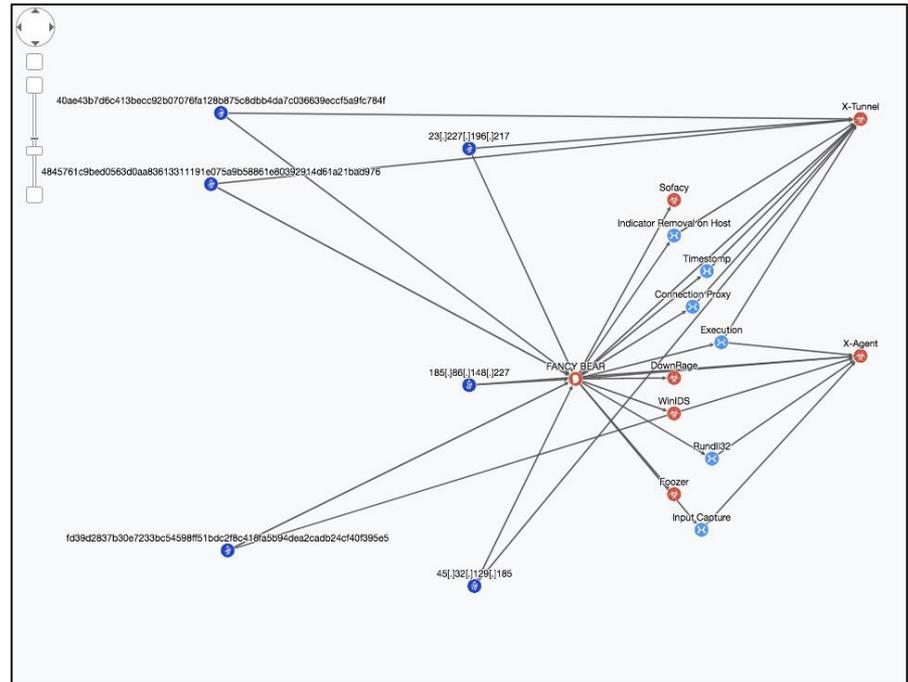
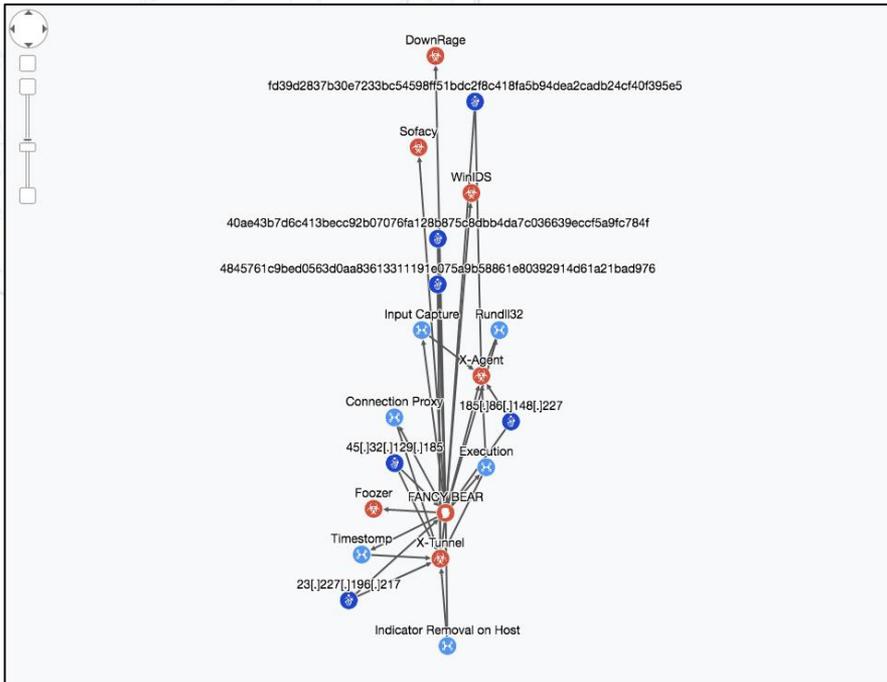
# Observations

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

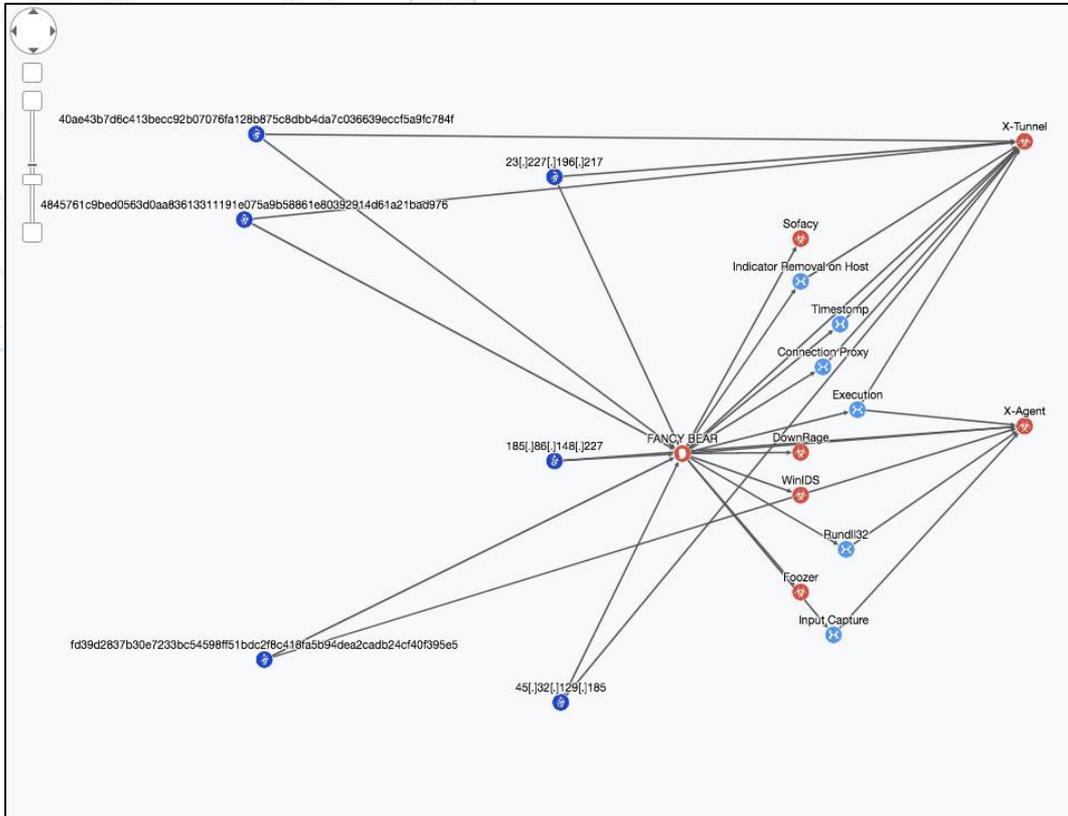
# Outline

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)

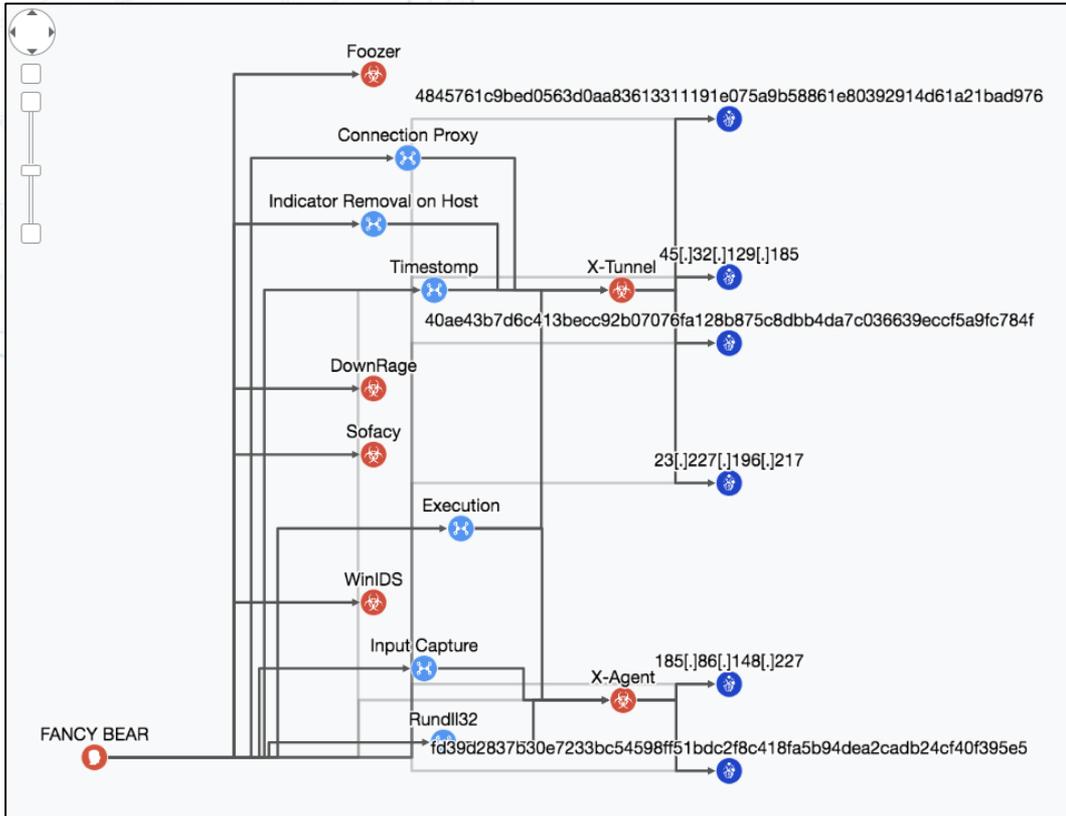


# DAG Layout: Problems



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

# DAG Layout++

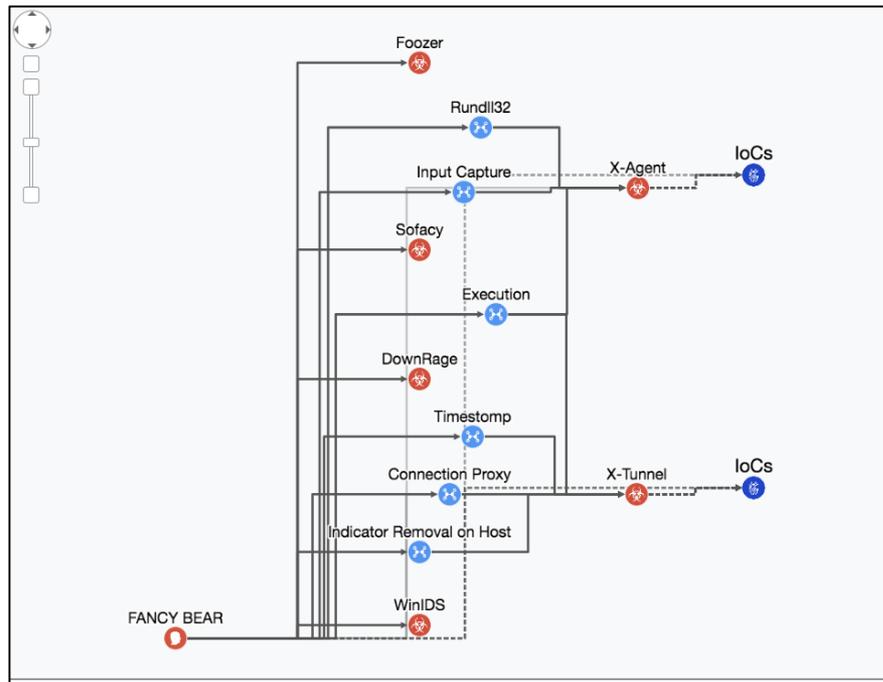
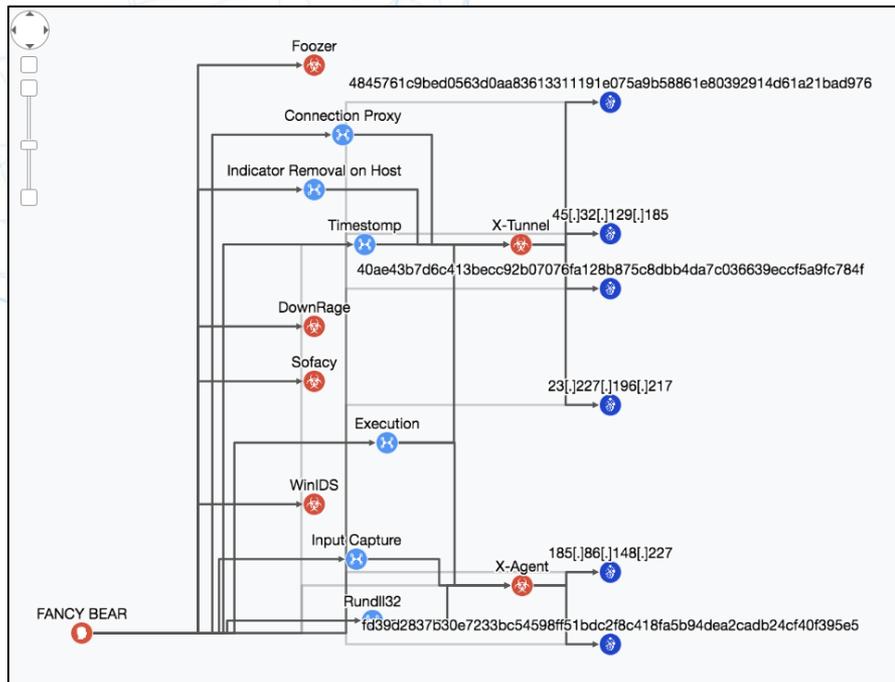


- Re-Mapping Edges
  - Remapping *indicates* Directions to Fit Intuition

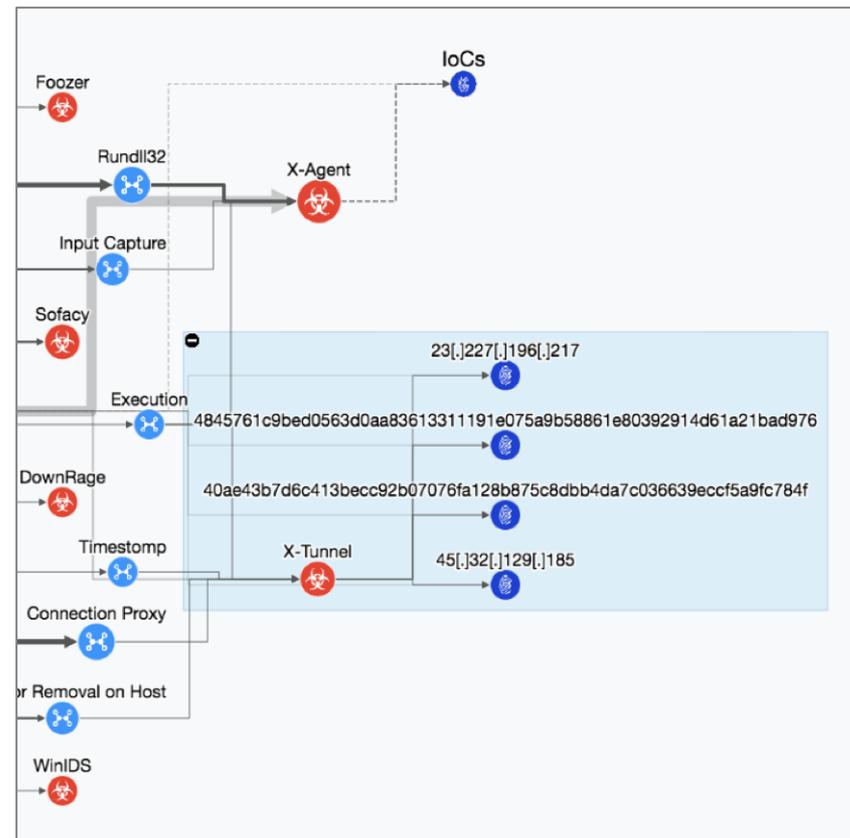
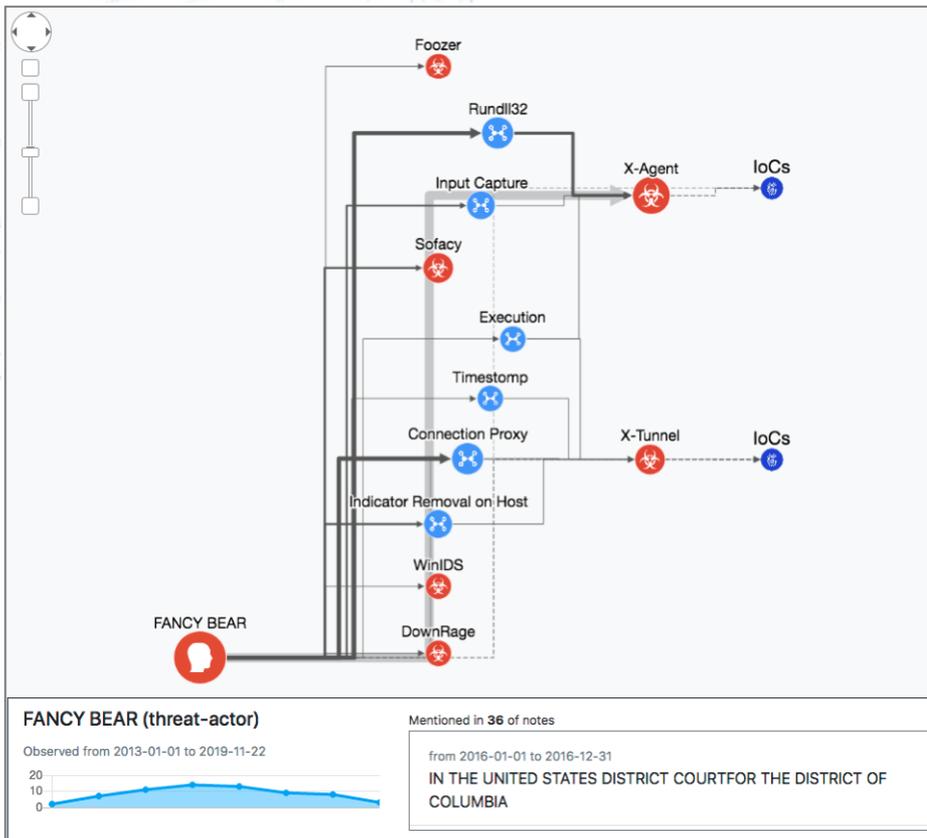
- Orthogonal Routing
  - Eliminating cross edges

- De-Emphasize Edges on Non-Adjective Layers
  - Bellman Ford Method for Longest Path Problem with Negative Weights

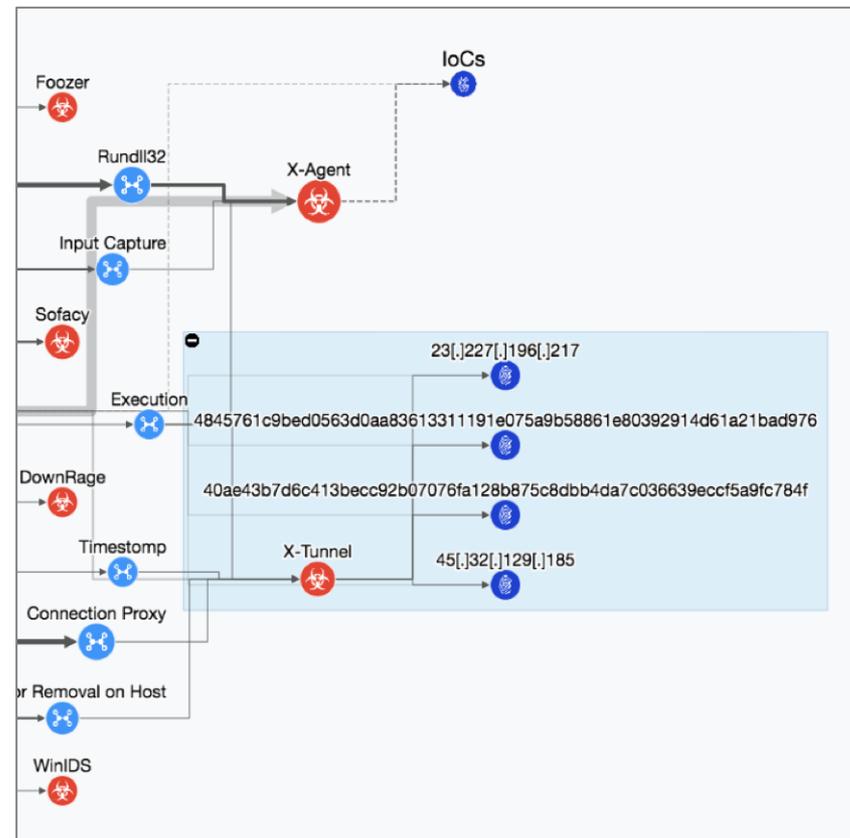
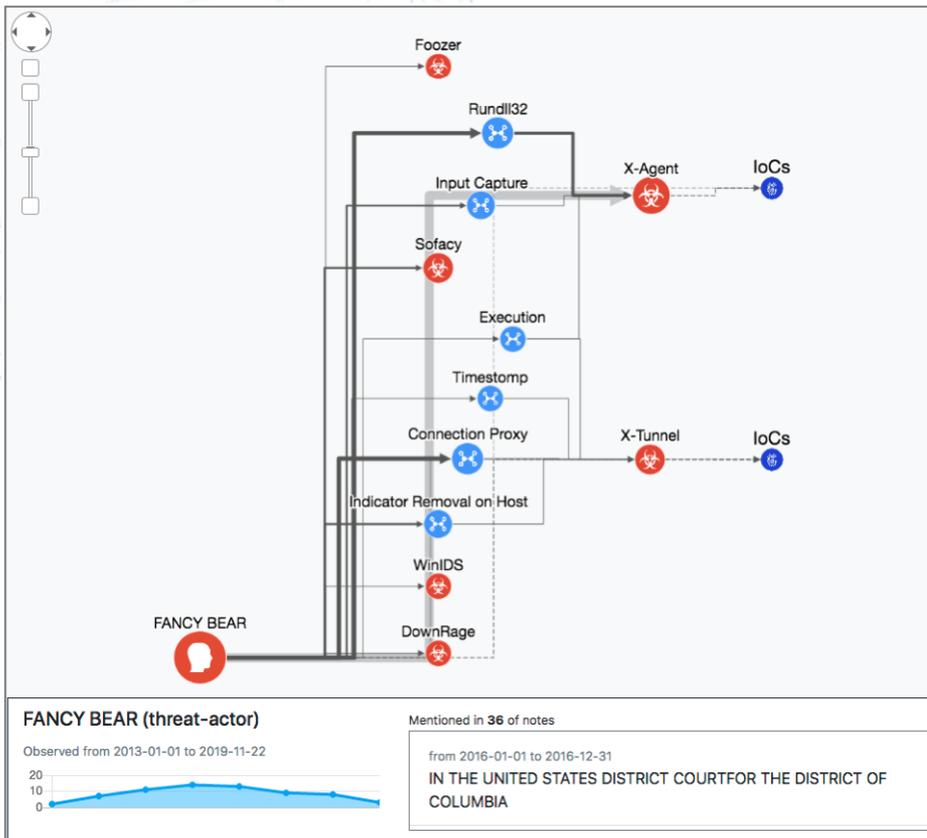
# Clustering IoCs based on Relationships



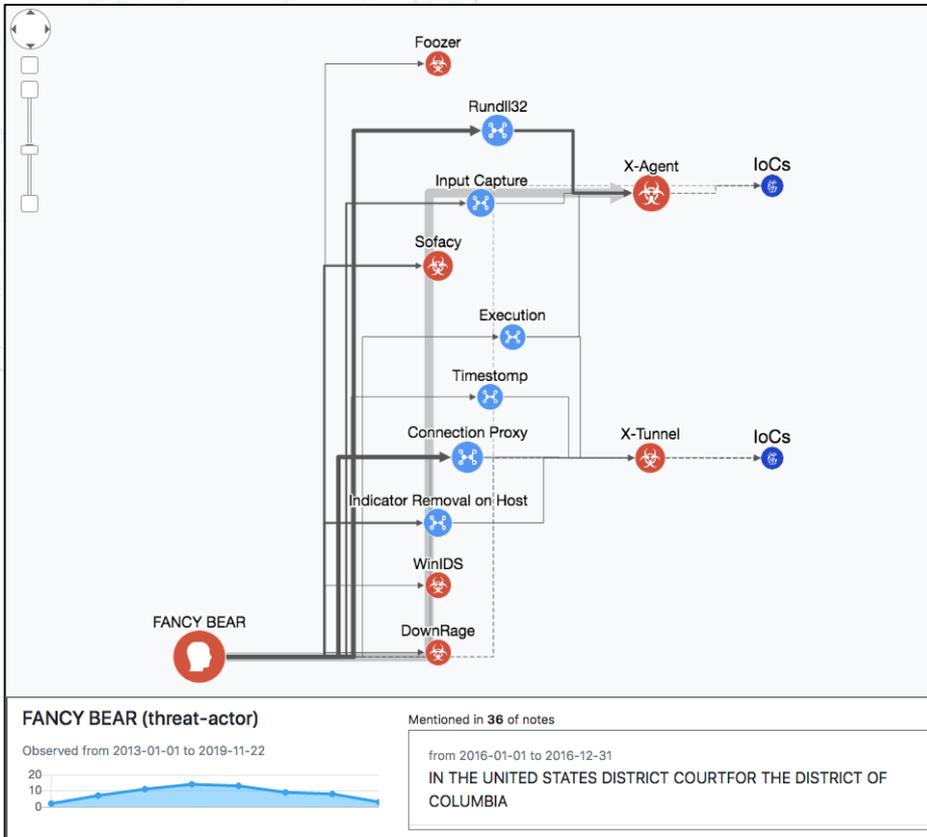
# Emphasizing Differences



# Emphasizing Differences



# New Visualization based on Observations

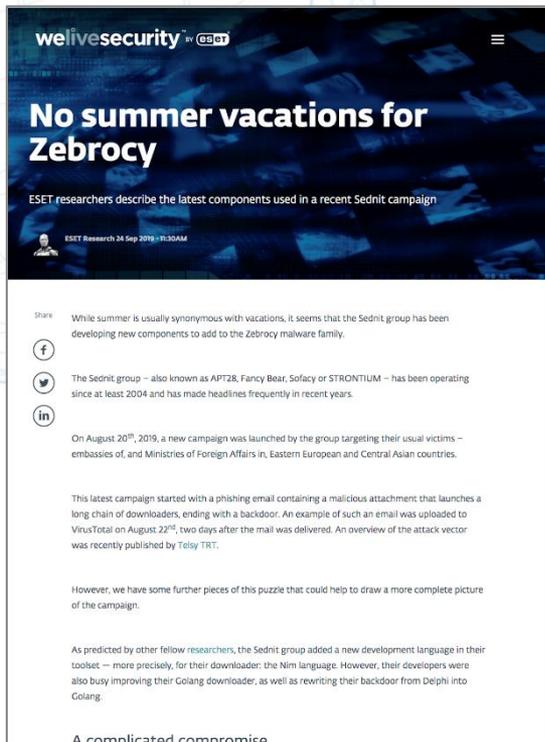


1. DAG Network with Edges between Adjacent Layers
2. Focusing on Relationship between IoCs and Other Entities
3. Extracting Differences from Existing Intelligence

# 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

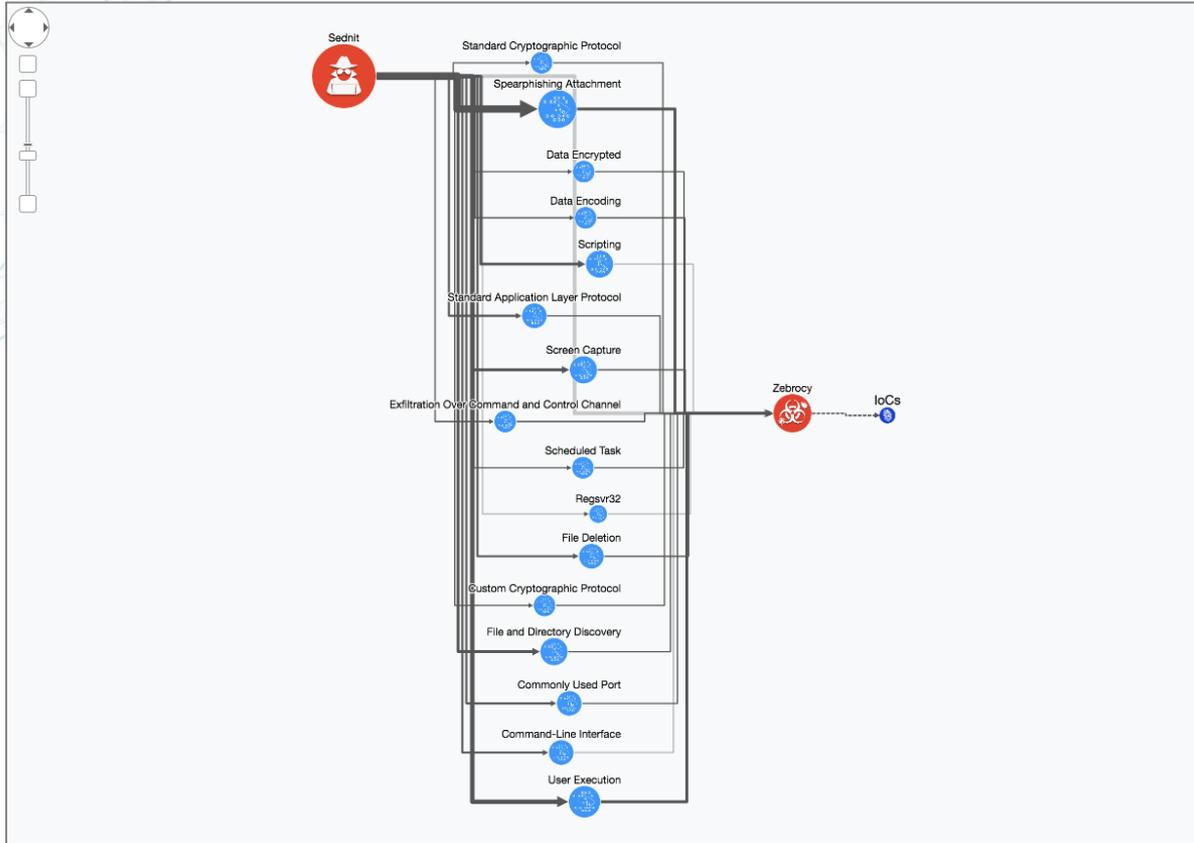


The screenshot shows a news article from WeLiveSecurity. The title is "No summer vacations for Zebrocy". The sub-headline reads "ESET researchers describe the latest components used in a recent Sednit campaign". The article text discusses the Sednit group's activities, mentioning their use of various languages like Nim and Delphi, and their focus on phishing and malware distribution. It also mentions the use of Dropbox for hosting. The article is dated "ESET Research 24 Sep 2019 - 11:30AM".

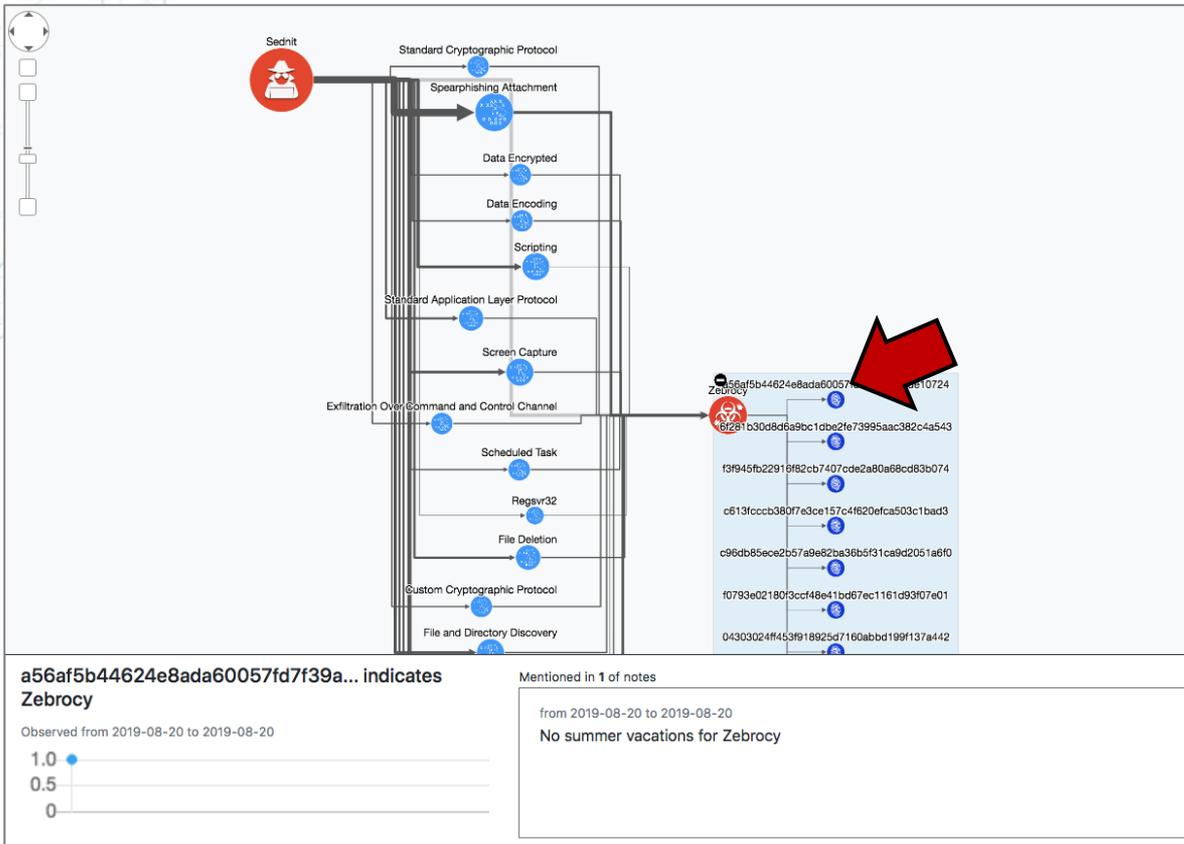
- Zebrocy Trojan used by APT28
  - Written in C++, Delphi, AutoIt, C#, VB.
- New Campaign since Sep 2019
  - Phishing with Malicious Word File
  - Usage of Dropbox for Hosting

Source:  
<https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/>

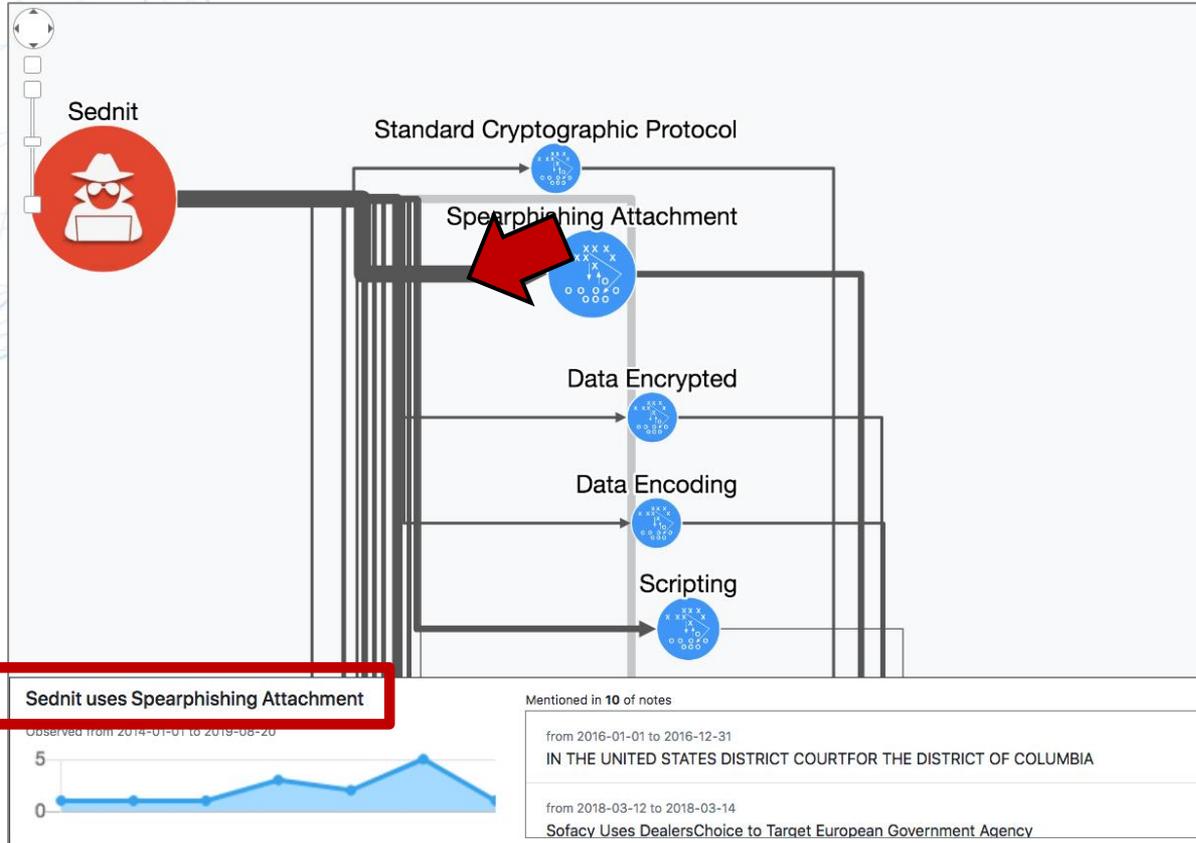
# Example: An New Zebrocy Campaign



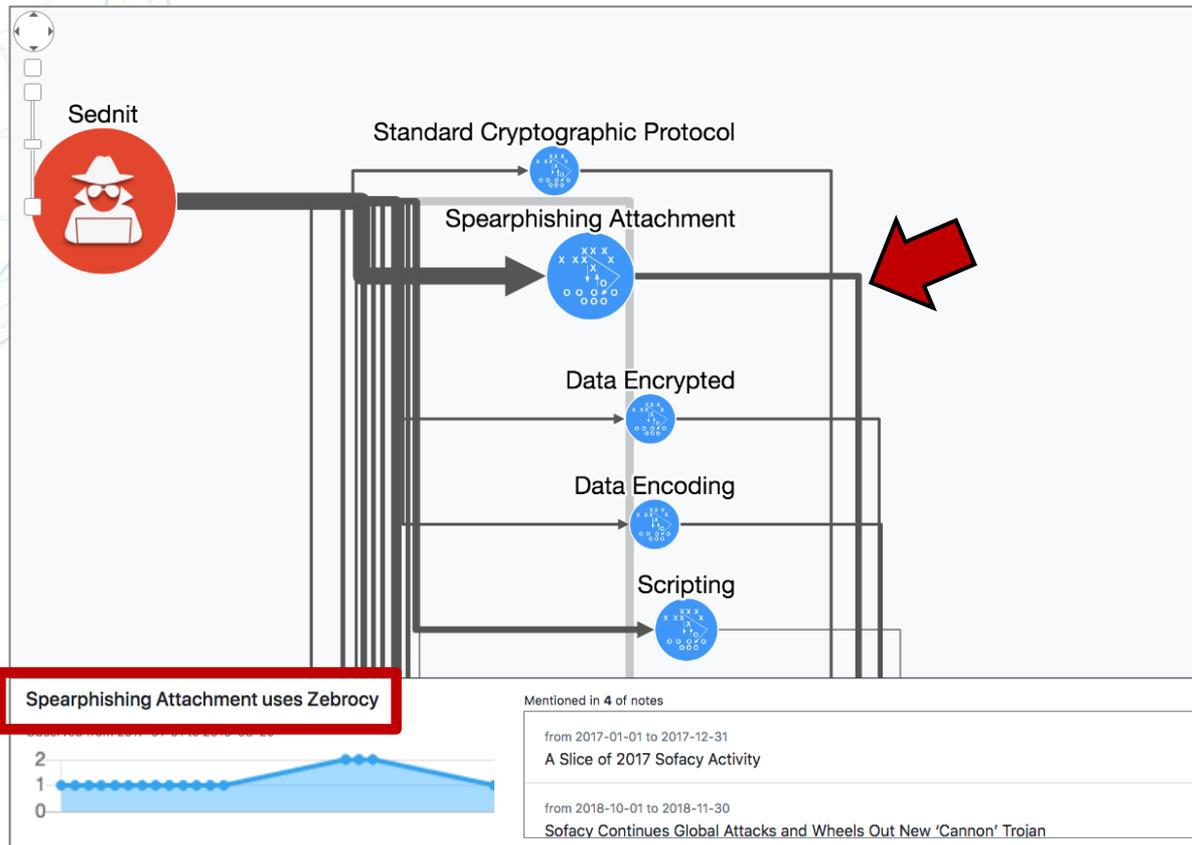
# Example: An New Zebrocy Campaign



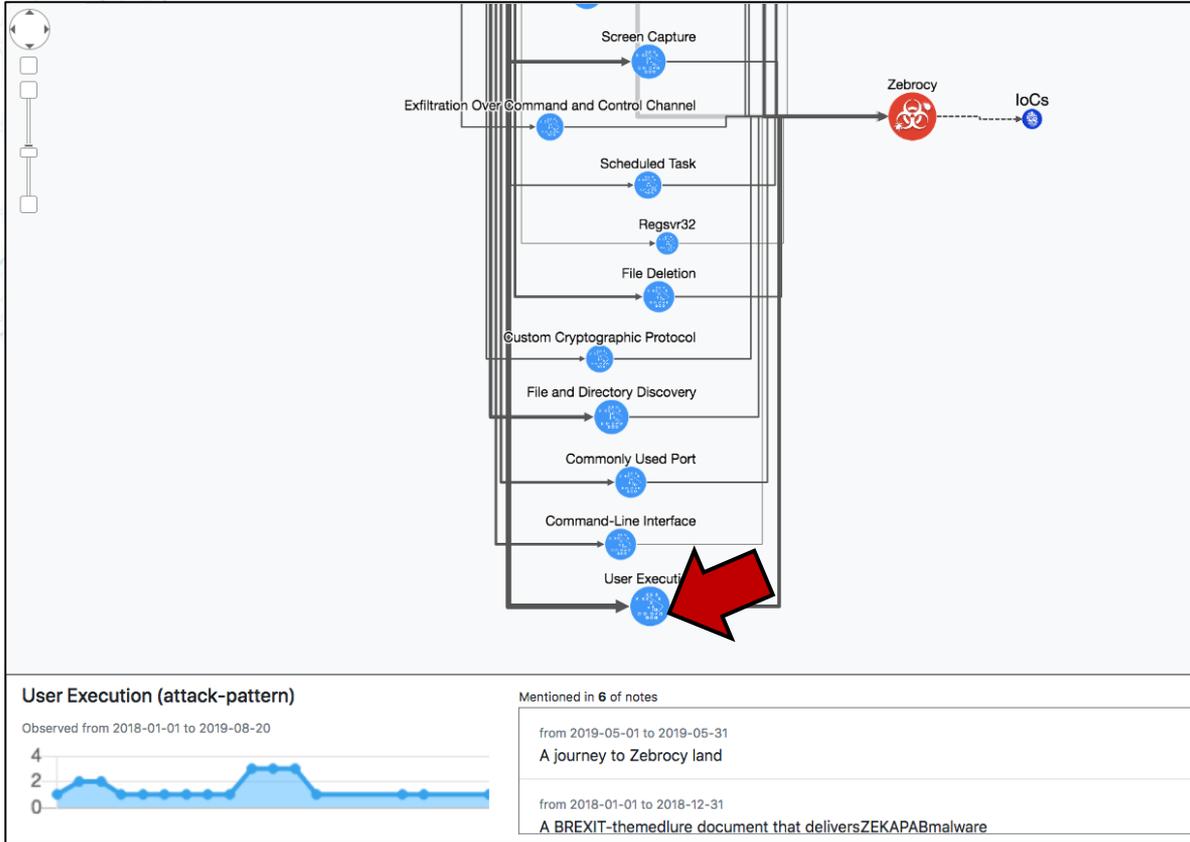
# Example: An New Zebrocy Campaign



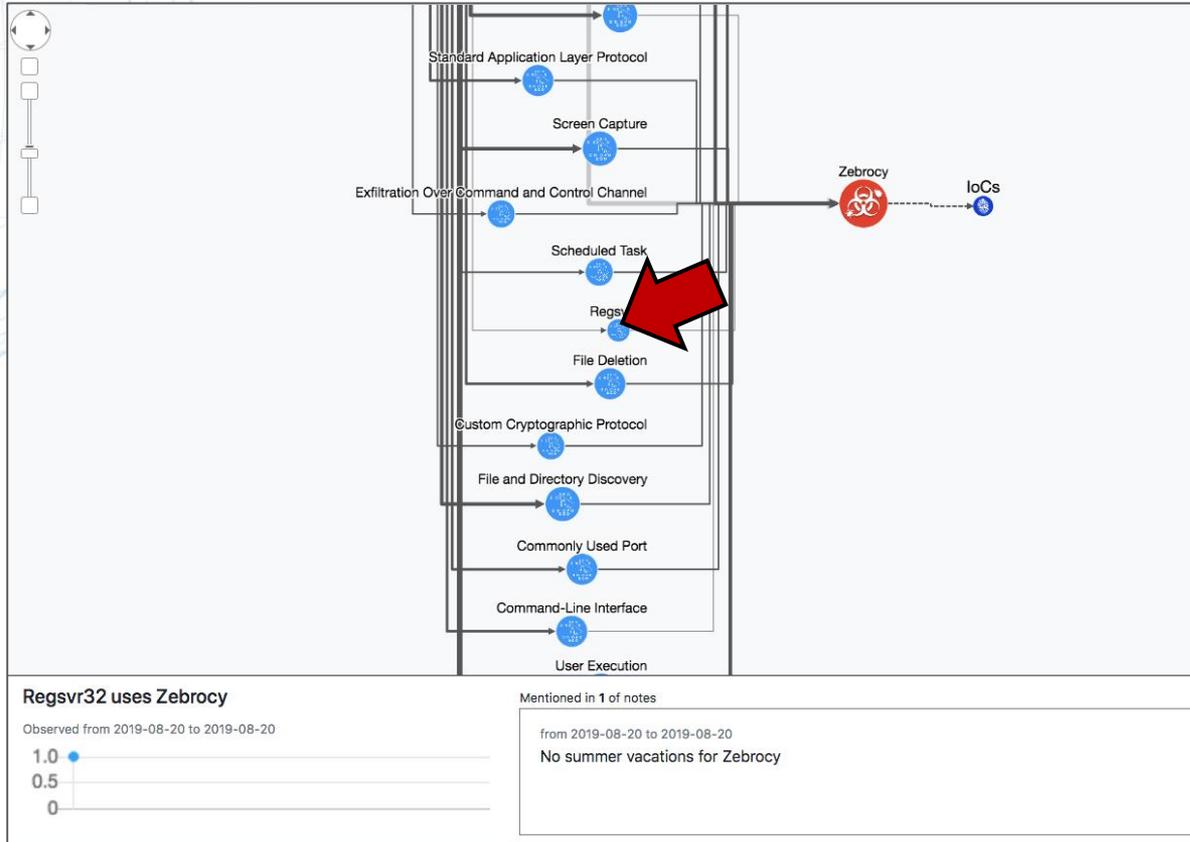
# Example: An New Zebrocy Campaign



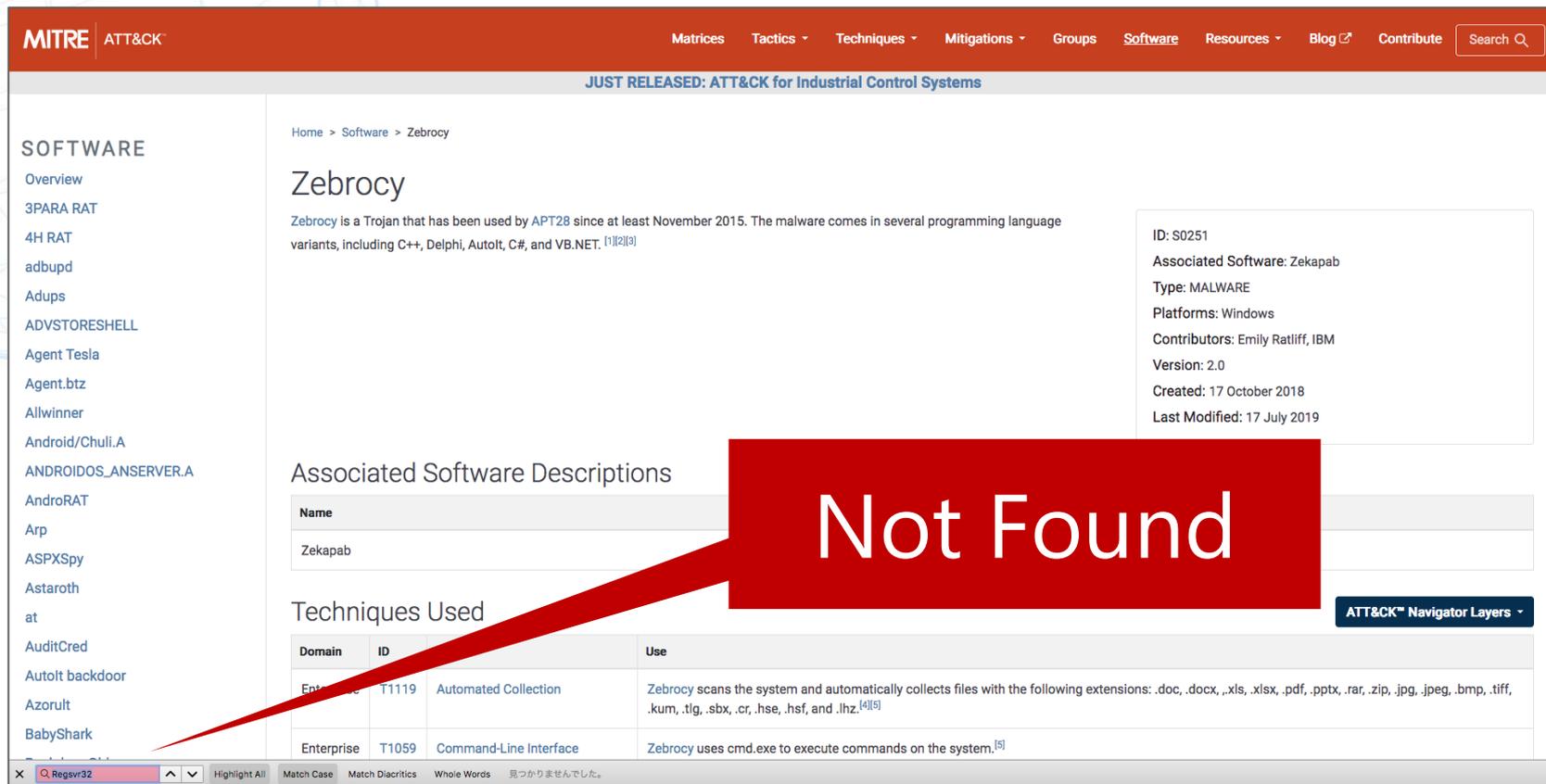
# Example: An New Zebrocy Campaign



# Example: An New Zebrocy Campaign



# Example: An New Zebrocy Campaign



**MITRE ATT&CK** Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

JUST RELEASED: ATT&CK for Industrial Control Systems

Home > Software > Zebrocy

## Zebrocy

Zebrocy is a Trojan that has been used by APT28 since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, and VB.NET. [1][2][3]

ID: S0251  
Associated Software: Zekapab  
Type: MALWARE  
Platforms: Windows  
Contributors: Emily Ratliff, IBM  
Version: 2.0  
Created: 17 October 2018  
Last Modified: 17 July 2019

### Associated Software Descriptions

Name
Zekapab

### Techniques Used

Domain	ID	Use
Enterprise	T1119	Automated Collection Zebrocy scans the system and automatically collects files with the following extensions: .doc, .docx, .xls, .xlsx, .pdf, .pptx, .rar, .zip, .jpg, .jpeg, .bmp, .tiff, .kum, .tlg, .sbx, .cr, .hse, .hsf, and .lhz. [4][5]
Enterprise	T1059	Command-Line Interface Zebrocy uses cmd.exe to execute commands on the system. [5]

ATT&CK™ Navigator Layers

Regsvr32 Highlight All Match Case Match Diacritics Whole Words 見つかりませんでした。

# 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`.

# 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

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