Applying Key Threat Intelligence Practices to Fight Cybercrime

Dhia Mahjoub, PhD., Head of Security Research, Cisco Umbrella (OpenDNS)

Sarah Brown, Independent Researcher, Security Links

Dec 6th, 2017

Security Links

cisco Cisco Umbrella

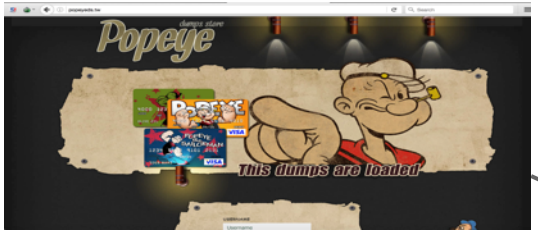
Who we are

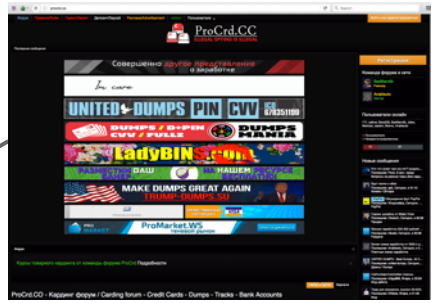
Sarah
MITRE, Fox-IT, NATO

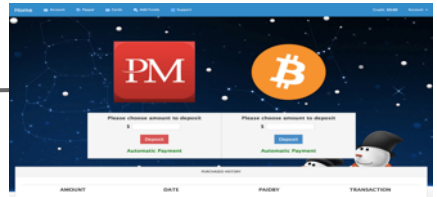
Bringing together tactical and strategic cyber threat intel from different locations, perspectives

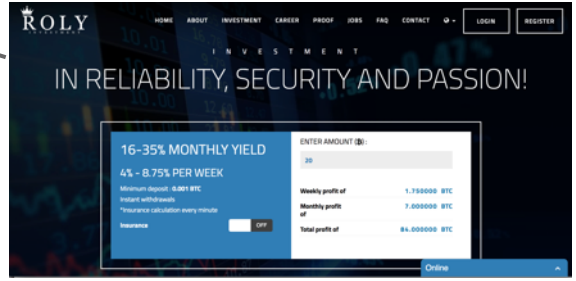
Dhia
OpenDNS / Cisco

Threat Landscape





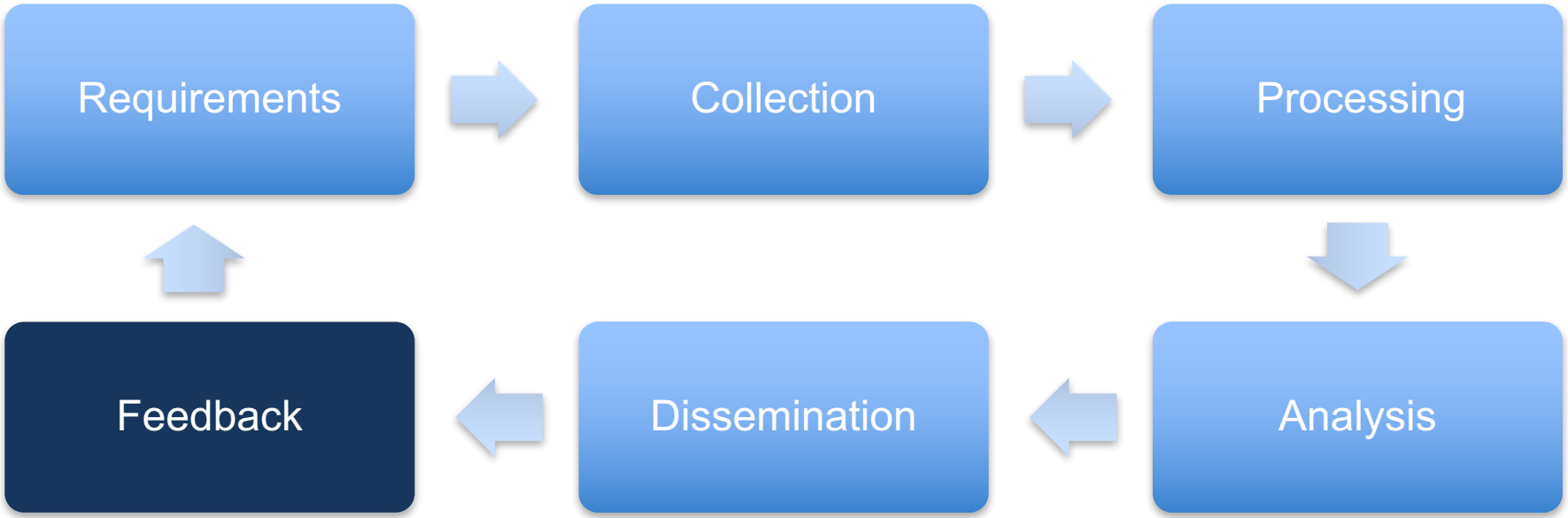




Categories of Hosting Providers

Good Abused Bulletproof

Threat Intelligence Cycle



Threat Intel Ecosystem Focus Areas

Investigations	Data analysis and processing	Strategic reports and/or tactical feeds	Actor-centric intelligence	Technical IOC-based intelligence

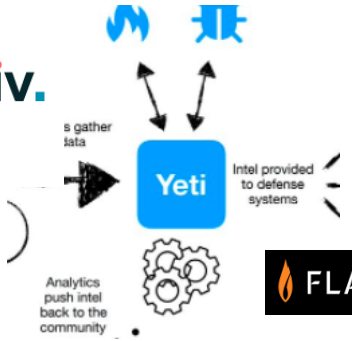
INTEL471

eclectic iq
INTELLIGENCE POWERED DEFENSE

MISP
Threat Sharing

ANOMALI

Blueliv.



CRITS

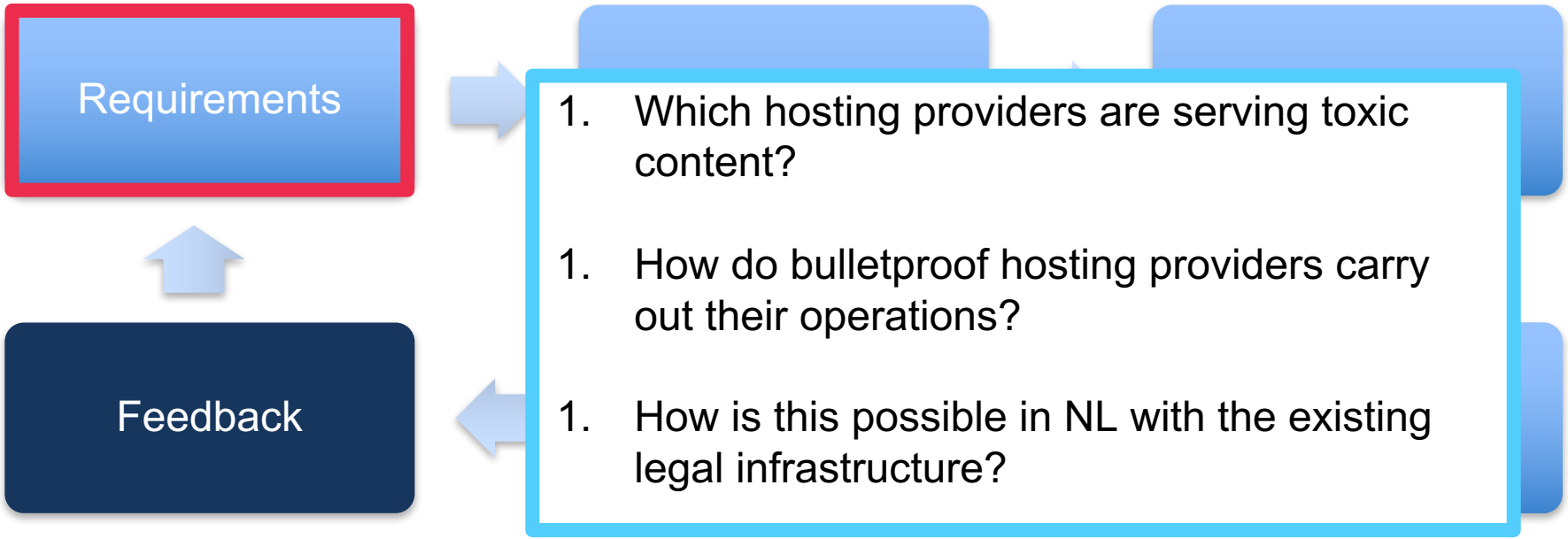
FOX IT
part of nccgroup

cisco Cisco Umbrella

Recorded
Future

FLASHPOINT

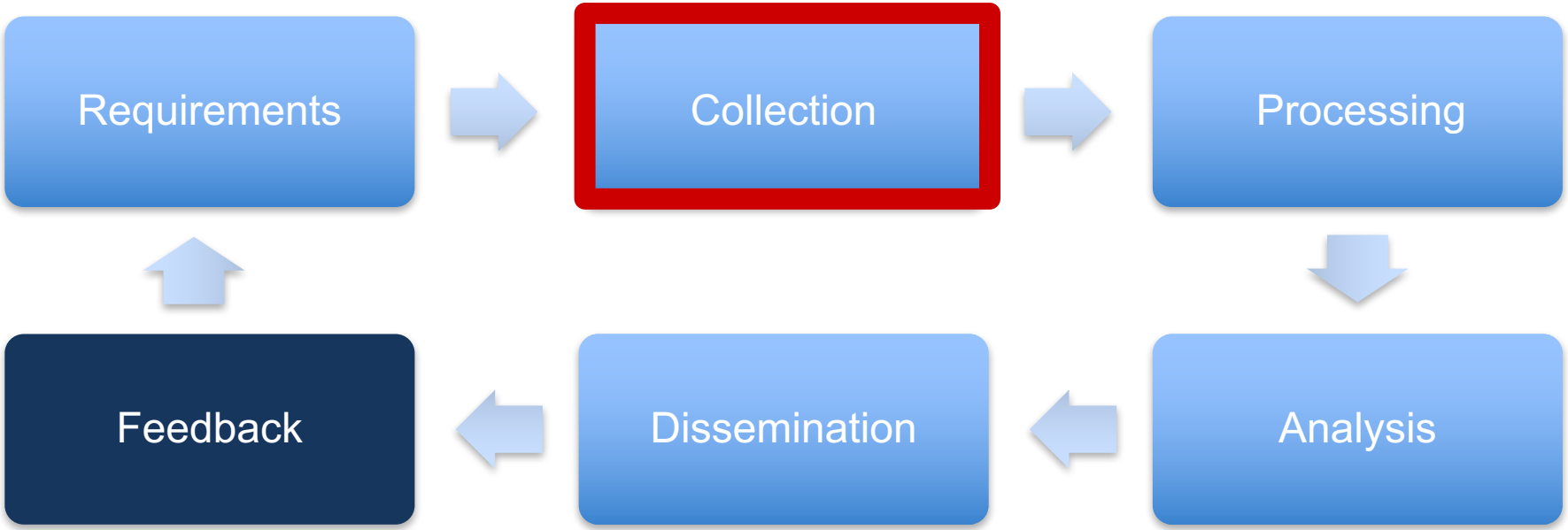
Requirements



Our Stakeholders

- Threat intel teams
- ISPs and hosters
- Law enforcement
- Policy makers

Collection


Requirements
Collection
Processing
Analysis
Dissemination
Feedback

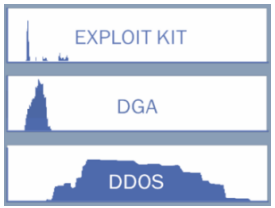
Umbrella Investigate Intel Production Cycle

Requirements
Detect and block domains/IPs to protect customers and provide insight and context around domains/IPs

Collection
Retrieve raw DNS, IP, BGP, SSL, whois, hash, crawled web data, etc. at scale

Processing
Caching, indexing, enriching, summarizing data at scale

Analysis
Threat detection and reputation scores using ML & graph models, human domain expertise

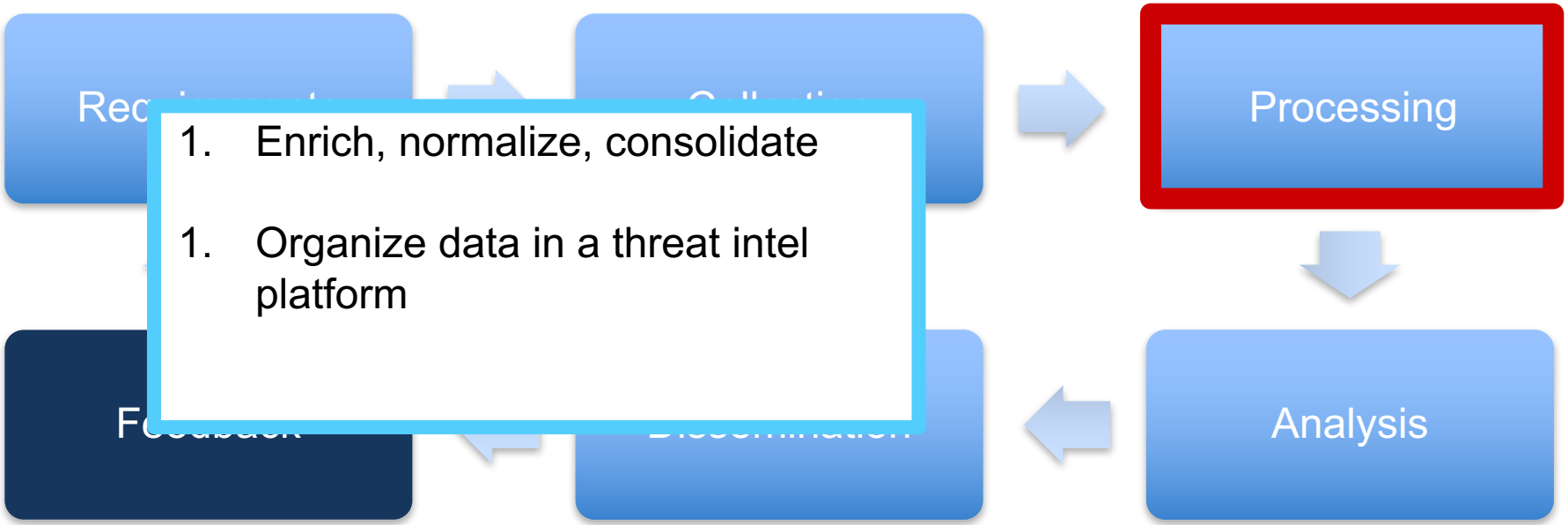


Dissemination
Domains, IPs into block list

Investigate UI and API

Feedback
Protected customers, actionable use cases with Investigate

Processing

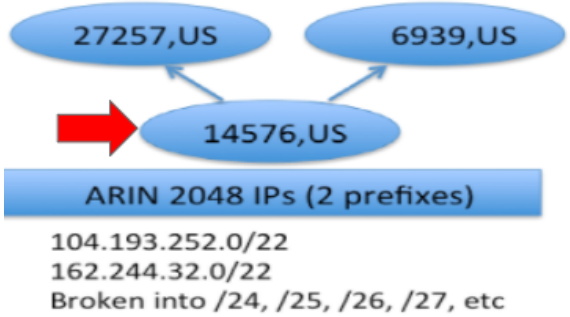


1. Enrich, normalize, consolidate

1. Organize data in a threat intel platform

Enrich with context across various attributes

Business registration

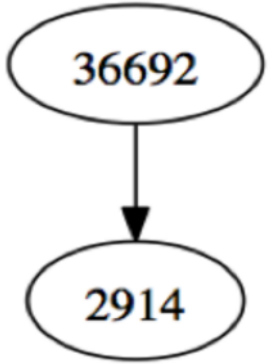


Helping the customer preserve bad content

Payment methods

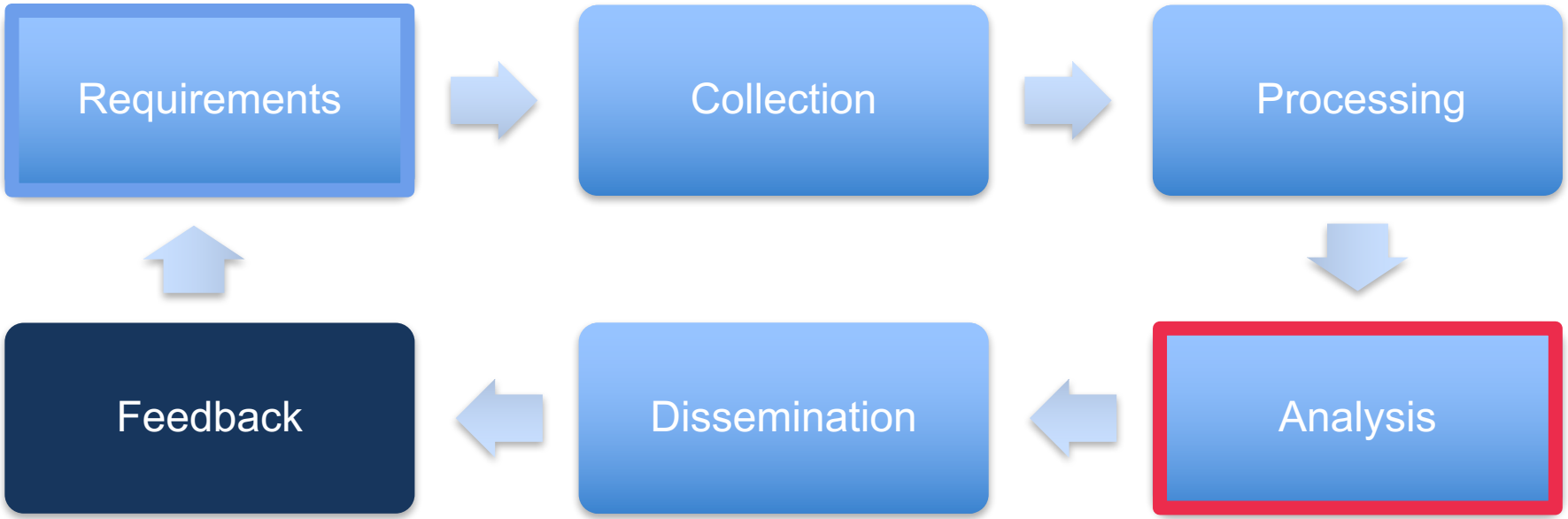
Autonomous System Number (ASN)

- Footprint of hosting provider in network view
- Unique identifier of a business' IP space
- An ASN can be an ISP, or a hosting provider
- Routers exchange IP ranges (BGP prefixes) and AS paths



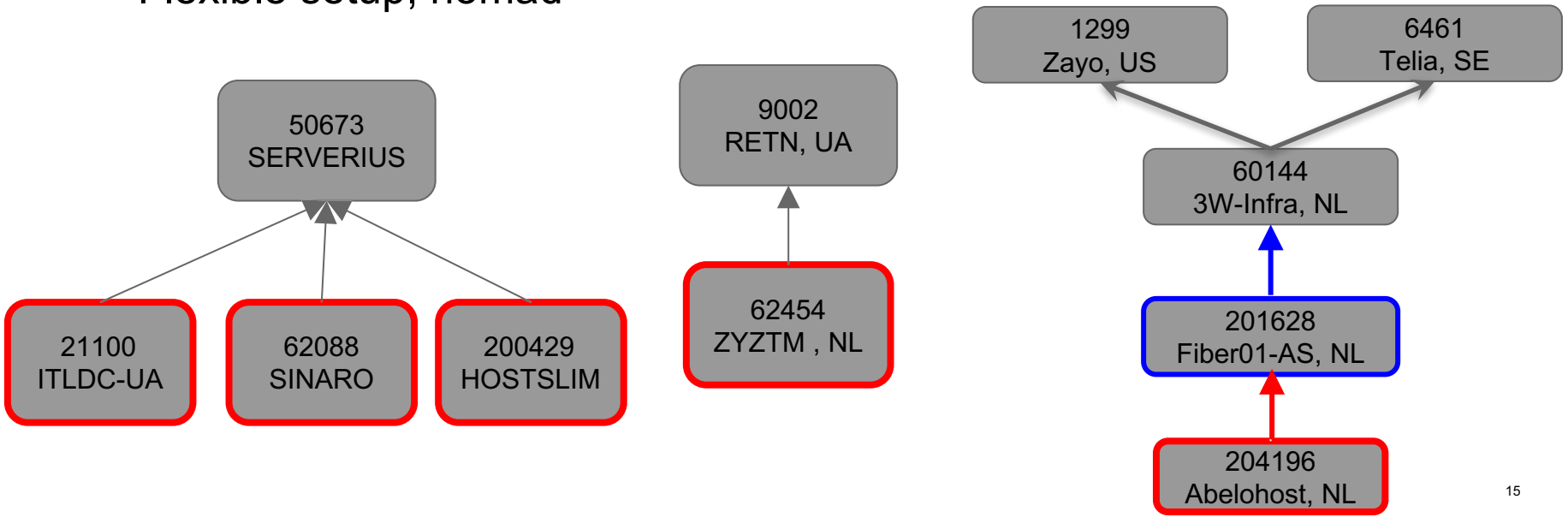
|67.215.94.0/24|11686 4436 2914 36692|

Analysis


Requirements
Collection
Processing
Analysis
Dissemination
Feedback

Leaf (Stub) ASN or leaf ASNs chain

- Have only upstream peers, no downstream
- Frequent pattern for questionable/bulletproof hosters
- Flexible setup, nomad



Indicator: Offshore Business Registration

Minimal taxation
Financial secrecy
Shareholder Secrecy

- UAE (10)
- Panama (13)
- BVI (21)
- Belize (60)
- Anguilla (63)
- Seychelles (72)
- Dominica (89)

Source: Grant Thornton

Anonymous Payment Methods

WESTERN UNION MONEY TRANSFER

MoneyGram International Money Transfer

EGOPAY

MasterCard VISA SOLID TRUST PAY

pecunix money refined

Skrill moneybookers

Perfect Money Just perfect

Liberty Reserve

PayPal

Payza

OKPAY

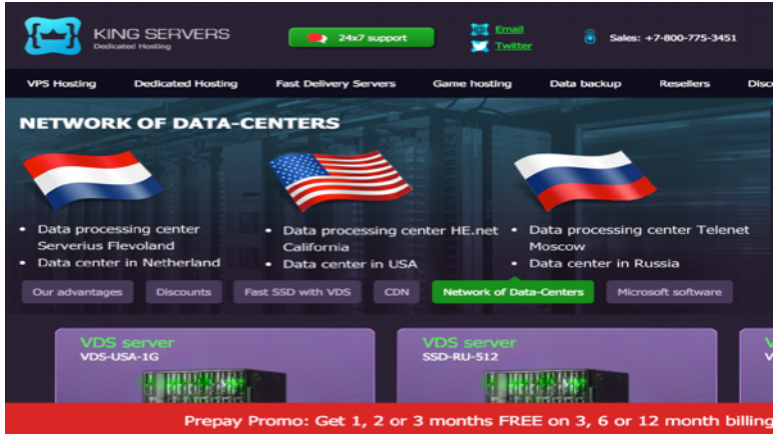
WebMoney

Helping customers to maintain operations

- **bob bob** i need to install doorway and mass mailer. is that good?
- **David** Once you purchase dedicated servers you will get root access on server. Then ***you can install anything what you want.***
- **bob bob** ***do u ignore dmca*** ?
- **David** For this please read our DMCA policy as below
- The actions we take with DMCA complaints depends on the criteria of the complaint, sometimes they don't apply to us in Panama Law, but if it's a copyrighted content we will ask you to remove the specific content they are complaining about, but ***we can handle them and keep your service alive.***

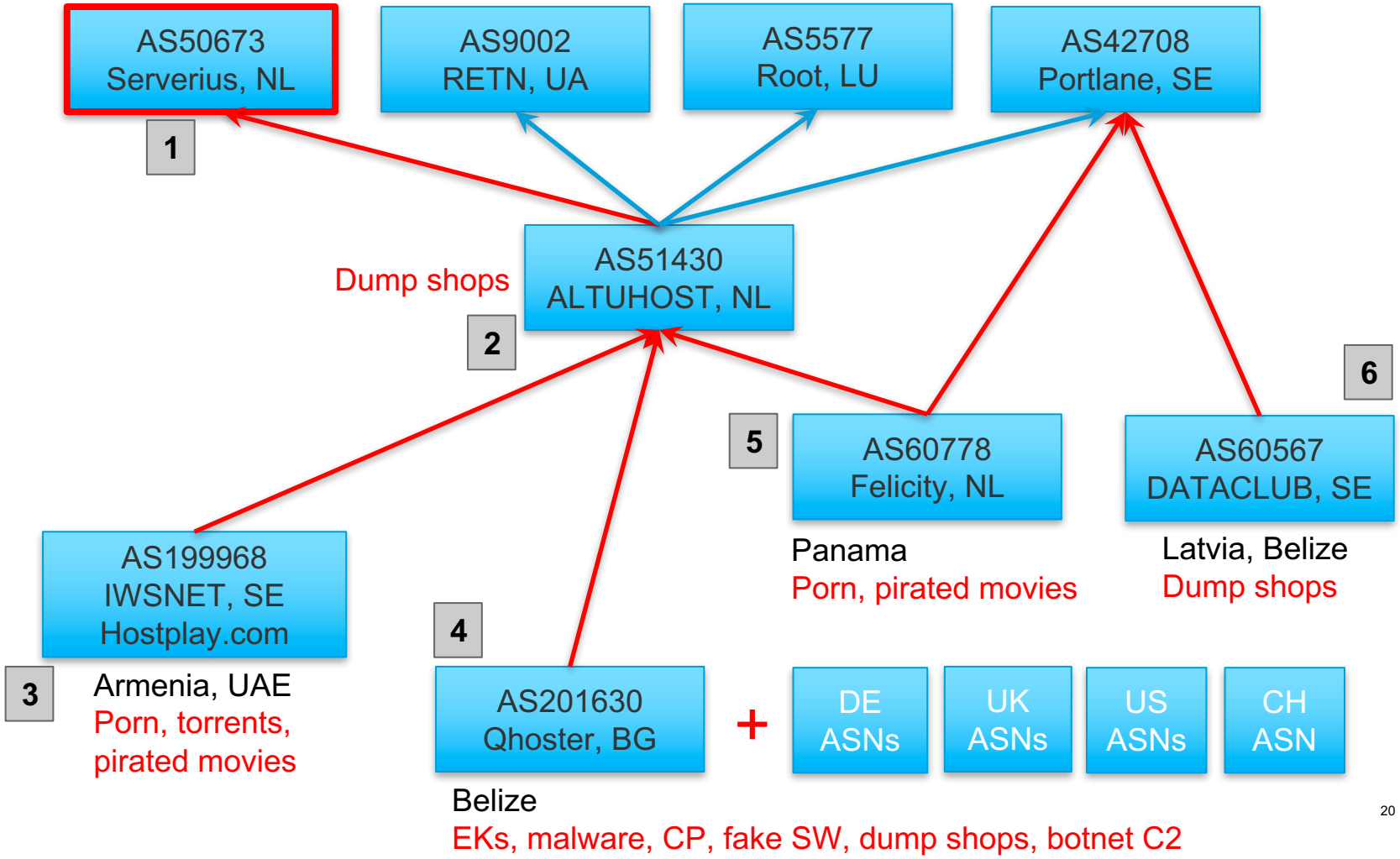
Sample Rogue Hosters with a Dutch footprint (as of Oct 2017)

- Ecatel
- Hostsailor
- Webzilla
- Hostkey
- QHoster
- Hostzealot
- King Servers



- Koddos/Amarutu
- Abelohost/Elkupi
- Deltahost
- Dataclub.biz
- Blazingfast.io
- Altuhost

GENIUS-SECURITY-LTD
HOSTSLIM
Some downstreams of Serverius
Some downstreams of NFORCE


AS50673
Serverius, NL
1
AS9002
RETN, UA
AS5577
Root, LU
AS42708
Portlane, SE
Dump shops
AS51430
ALTUHOST, NL
2
6
5
AS60778
Felicity, NL
AS60567
DATACLUB, SE
Panama
Porn, pirated movies
Latvia, Belize
Dump shops
AS199968
IWSNET, SE
Hostplay.com
4
3
Armenia, UAE
Porn, torrents,
pirated movies
AS201630
Qhoster, BG
+
DE
ASNs
UK
ASNs
US
ASNs
CH
ASN
Belize
EKs, malware, CP, fake SW, dump shops, botnet C2

Kings-servers Hosting-Solutions

50673 14576 44596

Upstream

50673 6939 174

AS32338, AS202951 Hostiserver

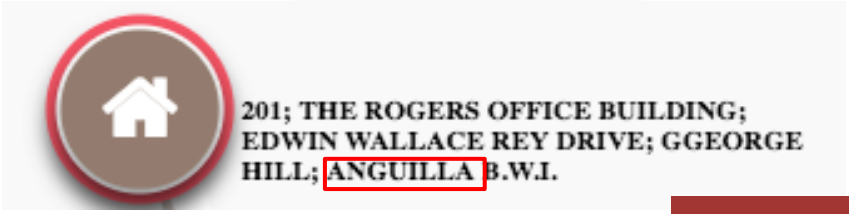
Adult and child porn

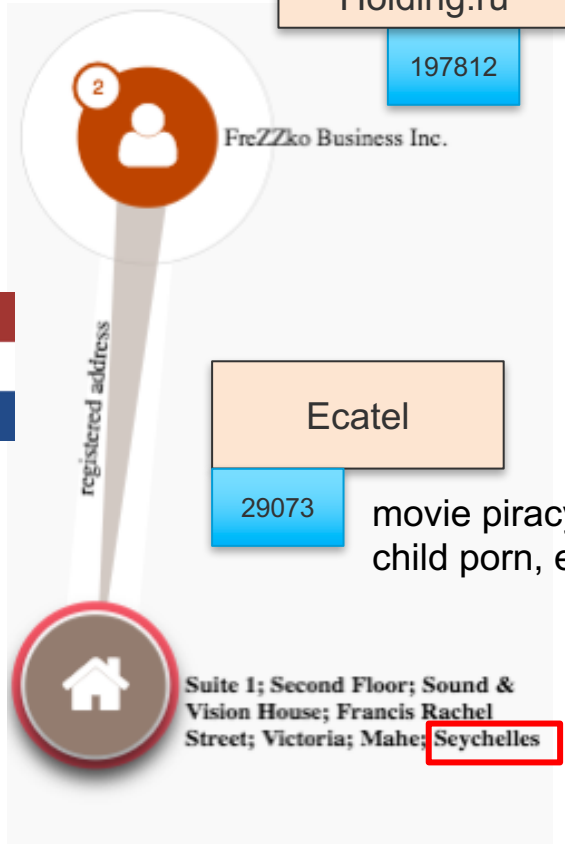
MPAA (movie) piracy

Ferazko Holding.ru

197812

EK, malware, porn, pharma, fake sw





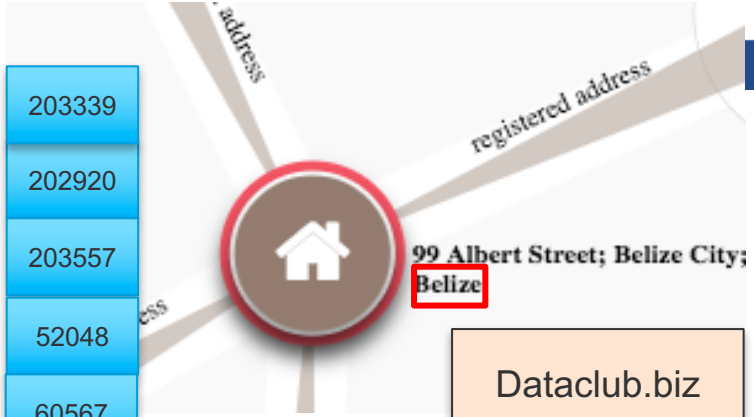
Ecatel

29073

movie piracy, child porn, etc

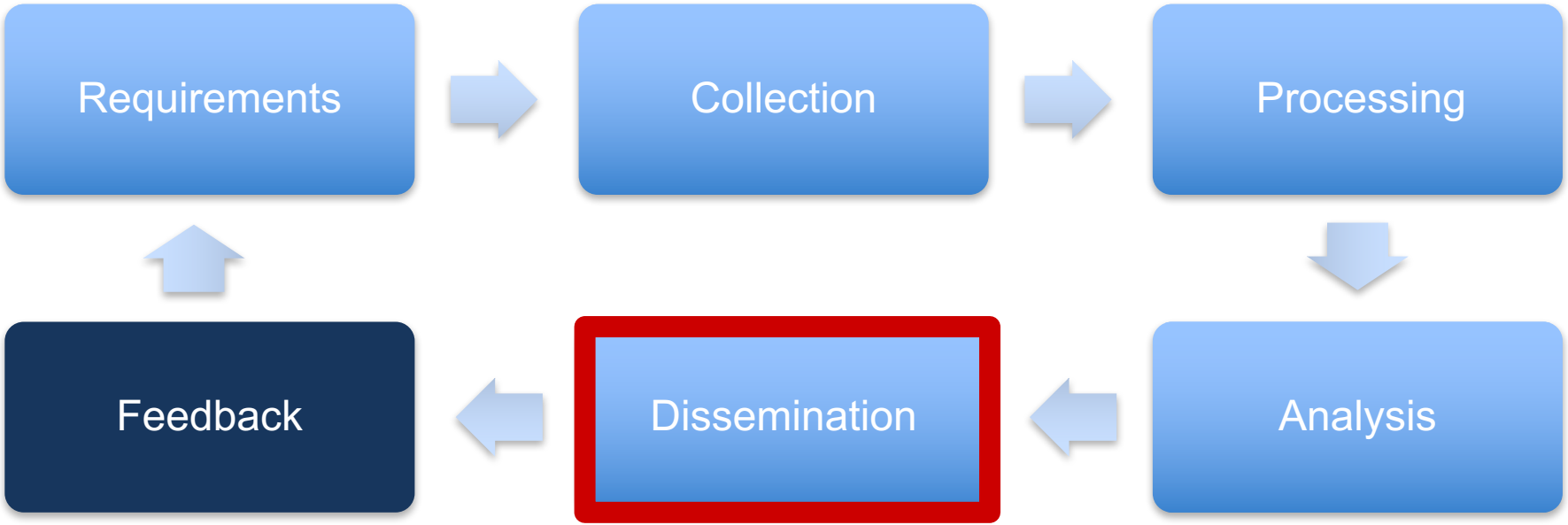
165 credit card dump shops

203339
202920
203557
52048
60567



Dataclub.biz

Dissemination

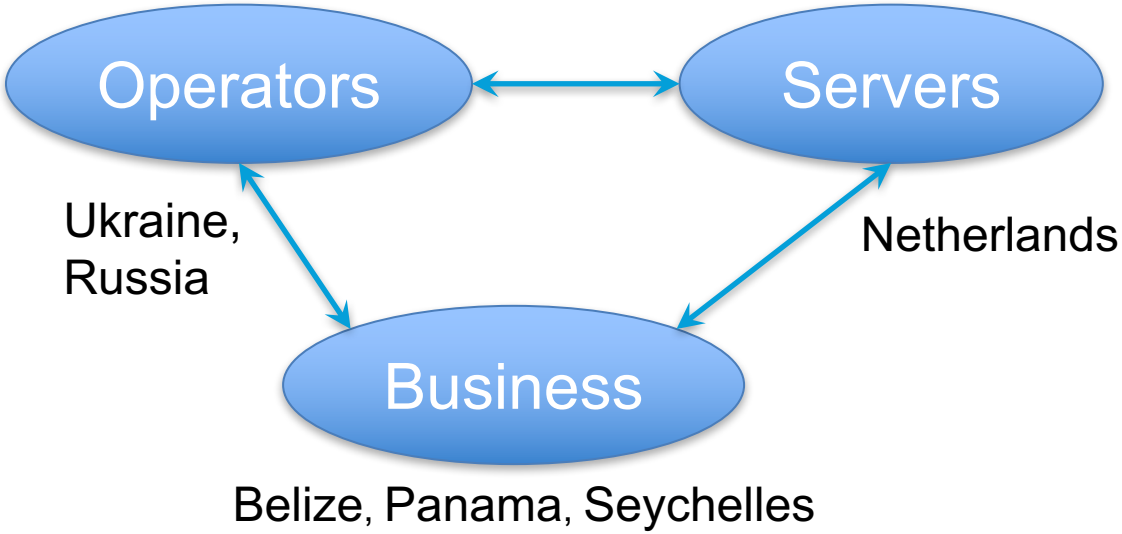


Rogue Hoster Recipe

Low barrier of entry (Approx <$2K)

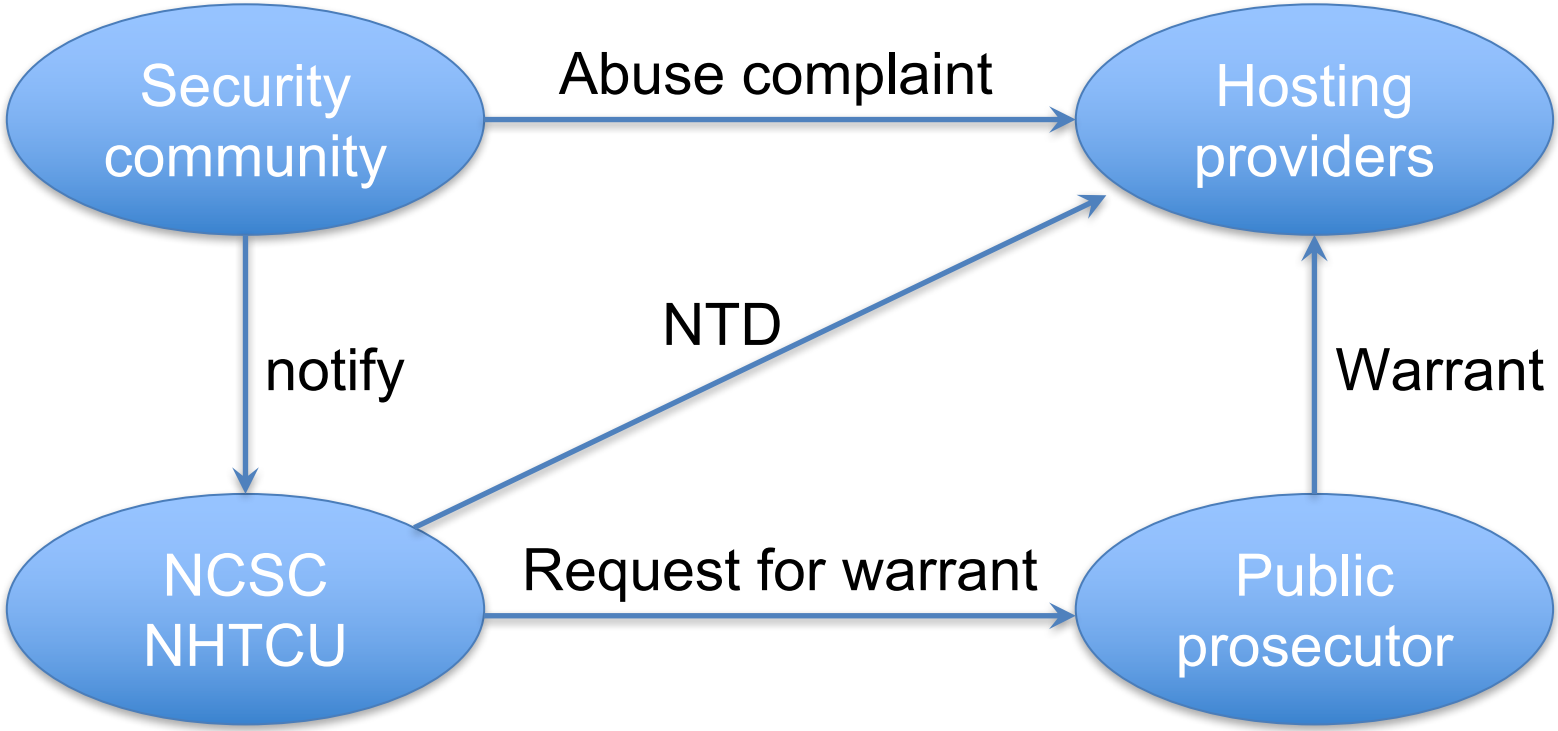
1. Register business offshore
2. Register own ASN and lease IP space
3. Setup website(s) or stay underground
4. Drive customers – forums (open, closed), social media
5. Generate revenue through hosting or sending traffic
7. Handle abuse
8. Shut down, move elsewhere, repeat

Law enforcement: Cross Jurisdictional Business Model



Information Sharing Agreements vary widely between nations

Law enforcement: Taking Down Bad Content



Law Enforcement Recommendations

1. Closer cooperation between LE teams in different countries

More scrutiny, liability for

1. Facilitators of cyber crime
2. Money laundering and currency exchange services

Security Community Recommendations

1. Think beyond reactive collection and blocking of IOCs
2. Understand and expose TTPs of rogue hosting providers
3. Share intel (e.g., evidence of intent) with security community/LE, monitor and take early action

Policy Makers: Operational Challenges with taking down a bad hoster

- Repeat offenses doesn't equal guilt
- Advertising as a bulletproof hoster not enough
- Criminal Exclusion Ground
- Incentive is profit and not to fight abuse

Policy Makers: Recommendations

- Rank hosters at a consumer agency (e.g., Consumentenbond)
  - Aids LE, businesses
  - Hosters care about their reputation

Hosting Community Recommendations

1. Urge datacenters to scrutinize peering and/or co-location requests more closely

2. Self-regulation to establish a Code of Conduct
   a. Acceptable Use Policy to check customer content
   b. Collecting personal details of customers
   c. When to support investigations and remove dodgy customers

3. Ask registries to scrutinize ASN requests more closely

Summary

- Leveraged the threat intel cycle to investigate criminal hosting space in the Netherlands
- Combined machine-based and human based collection and analysis
- Exposed business models and operations of criminal hosters
- Offered recommendations for four stakeholder groups

References

- Holland Strikes Back 2017
- NCSC One Conference 2017
- Australian Cyber Security Conference 2017
- Enigma 2017 https://www.youtube.com/watch?v=ep2gHQgjYTs&t=818s

Additional Related Work

- SANS CTI Summit 2018
- Flocon 2018
- Virus Bulletin 2017 https://www.virusbulletin.com/blog/2017/11/vb2017-paper-beyond-lexical-and-pdns-using-signals-graphs-uncover-online-threats-scale/
- Defcon 2017 https://www.youtube.com/watch?v=AbJCOVLQbjs
- Black Hat 2017
- Black Hat 2016 https://www.youtube.com/watch?v=m9yqnwuqdSk
- RSA 2016 https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker
- BruCon 2015 https://www.youtube.com/watch?v=8edBgoHXnwg
- Virus Bulletin 2014 https://www.virusbtn.com/conference/vb2014/abstracts/Mahjoub.xml
- Black Hat 2014 https://www.youtube.com/watch?v=UG4ZUaWDXS

Thank you!

dhia@opendns.com
sarah@securitylinks.nl