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
Who we are

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

Sarah
MITRE, Fox-IT, NATO

Dhia
OpenDNS / Cisco
Threat Landscape
Categories of Hosting Providers

Good

Abused

Bulletproof
Threat Intelligence Cycle

- Requirements
- Collection
- Processing
- Dissemination
- Analysis
- Feedback
Threat Intel Ecosystem Focus Areas

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

1. Which hosting providers are serving toxic content?

1. How do bulletproof hosting providers carry out their operations?

1. How is this possible in NL with the existing legal infrastructure?
Our Stakeholders

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

Requirements → Collection → Processing

Feedback ← Dissemination ← Analysis
Umbrella Investigate Intel Production Cycle

**Feedback**
Protected customers, actionable use cases with Investigate

**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

**Dissemination**
Domains, IPs into block list
Investigate UI and API

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

**Processing**
Caching, indexing, enriching, summarizing data at scale
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

VPS
HOSTING - GUIDE

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
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
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
EK, malware, porn, pharma, fake sw

MPAA (movie) piracy

Adult and child porn

Dataclub.biz

Ferazko Holding.ru

Ecatel

165 credit card dump shops

197812

201; THE ROGERS OFFICE BUILDING; EDWIN WALLACE REY DRIVE; GGEORGE HILL; ANGUILLA B.W.I.

99 Albert Street; Belize City; Belize

Suite 1; Second Floor; Sound & Vision House; Francis Rachel Street; Victoria; Mahe; Seychelles
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
6. Handle abuse
7. Shut down, move elsewhere, repeat
Law enforcement: Cross Jurisdictional Business Model

Operators

Servers

Ukraine, Russia

Netherlands

Business

Belize, Panama, Seychelles

Information Sharing Agreements vary widely between nations
Law enforcement: Taking Down Bad Content

- Security community
  - Abuse complaint
  - Notify
- Hosting providers
  - NTD
  - Warrant
- NCSC NHTCU
  - Request for warrant
- Public prosecutor
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](https://www.youtube.com/watch?v=ep2gHQgjYTs&t=818s)
Additional Related Work

- SANS CTI Summit 2018
- Flocon 2018
- Defcon 2017 [https://www.youtube.com/watch?v=AbJCOVLQbjs](https://www.youtube.com/watch?v=AbJCOVLQbjs)
- Black Hat 2017
- Black Hat 2016 [https://www.youtube.com/watch?v=m9yqnwugdSk](https://www.youtube.com/watch?v=m9yqnwugdSk)
- RSA 2016 [https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker](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](https://www.youtube.com/watch?v=8edBgoHXnwg)
- Black Hat 2014 [https://www.youtube.com/watch?v=UG4ZUaWDXS](https://www.youtube.com/watch?v=UG4ZUaWDXS)
Thank you!

dhia@opendns.com
sarah@securitylinks.nl