Is AI the Answer to Reducing Cyberattack Risks?

Dhia Mahjoub, PhD.
Principal Engineer, Head of Security Research, Cisco Umbrella @DhiaLite
Jan 27th 2020

Barcelona | January 27-31, 2020

Who am I?

Dhia Mahjoub, Ph.D.

Principal Engineer & Head of Security Research, Cisco Umbrella

- First member of OpenDNS research team
- Threat and Cybercrime research at scale, Graph data analysis
- Supporting LEAs in fighting cybercrime
- International and keynote speaker: Black Hat, Defcon, FloCon, FIRST, KPMG i4 forum,
  FS-ISAC, RSA, Europol-INTERPOL conference, GartnerSEC UK, RIPE

@DhiaLite

Agenda

Agenda

- Global visibility, threat detection at scale, threat intel
- Classes of threat problems to solve with ML
- Various use cases: NLP, graph analysis, anomaly detection, clustering
- Takeaways
- Q&A

Introduction

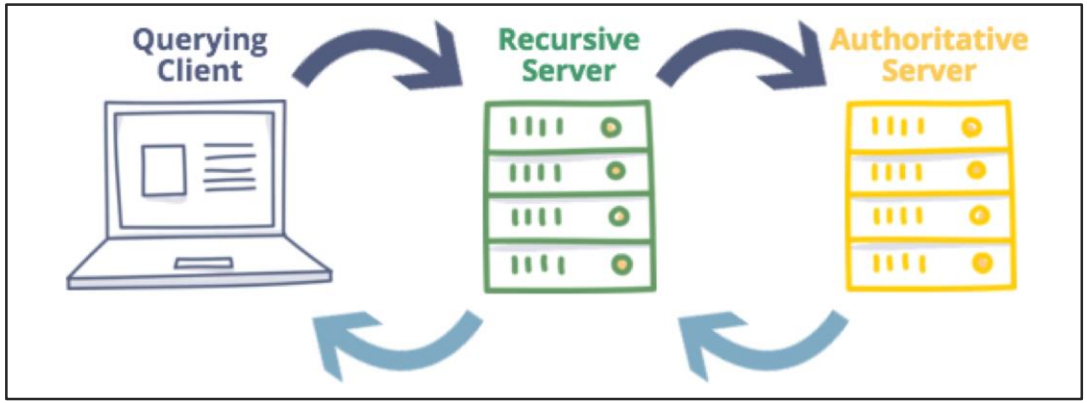
Data centers co-located at major IXPs

36 POPs – 11 in Europe

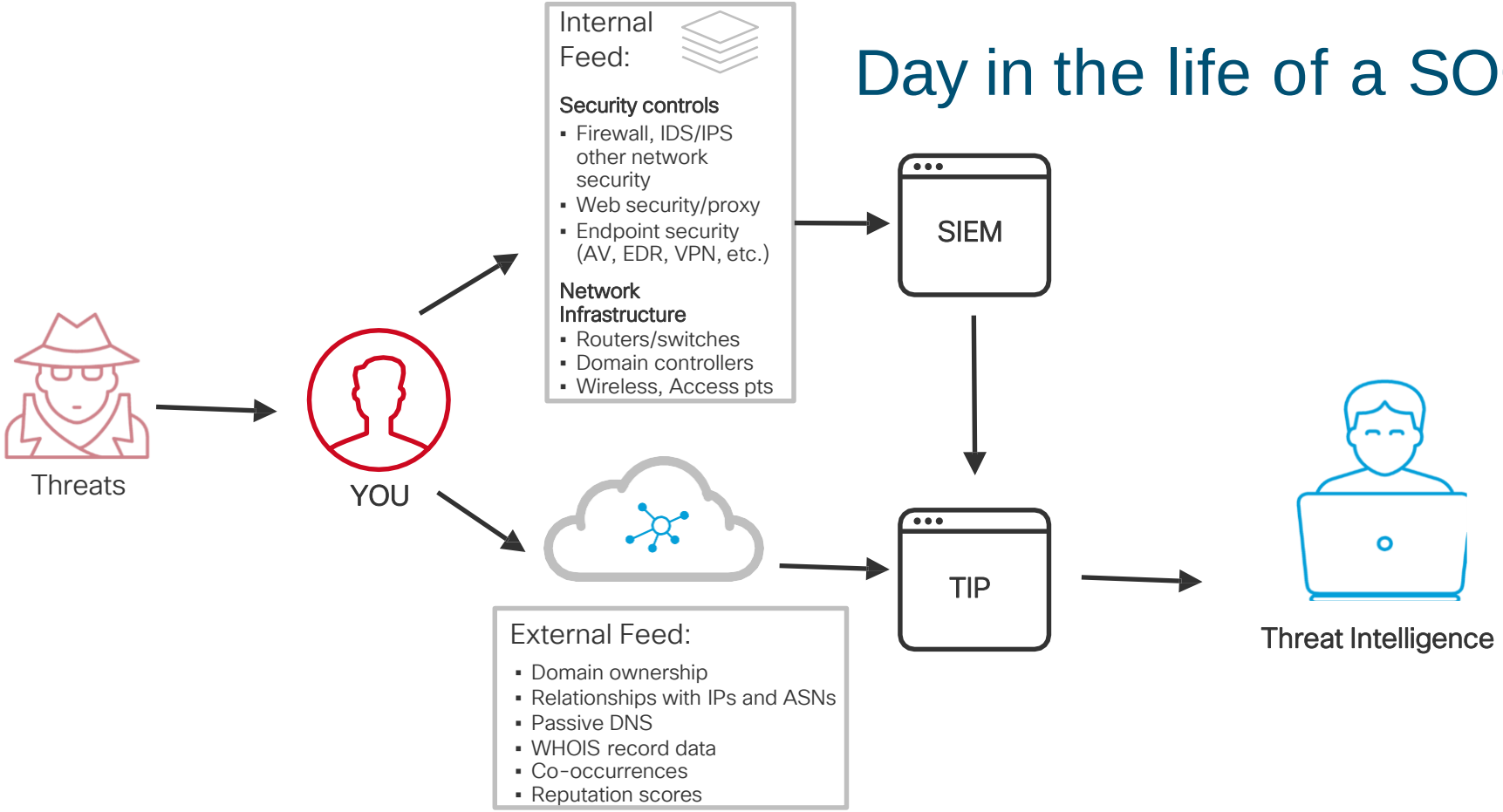
20 Countries

Online

Recursive and Authoritative DNS



Day in the life of a SOC



Our threat intel production cycle

Scale

Automation

Efficacy

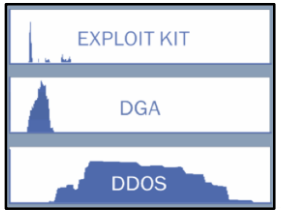
Context

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

Threat Detection at Scale

Raw data

0110
1101
1010

DNS
IP
BGP
SSL
WHOIS
HASH
WEB
ETC

DOMAIN
IP

Patterns and behaviors

Lexical

fgpxmvlsxpsp.me.uk
hsjnkhqxqiox.com

Live DGA prediction

Anomaly detection

Newly seen domains

Spike rank model

Predictive IP

Predictive IP space monitoring

Graph-based

Co-occurrence model

Threat types

Botnet

Crimeware

Exploit Kit

Phishing

Ransomware

Spam

Trojan

Cryptojacking

Deliverables

Enforcement

Intelligence

3 Classes of ML algos to solve threat detection

NLP/Clustering

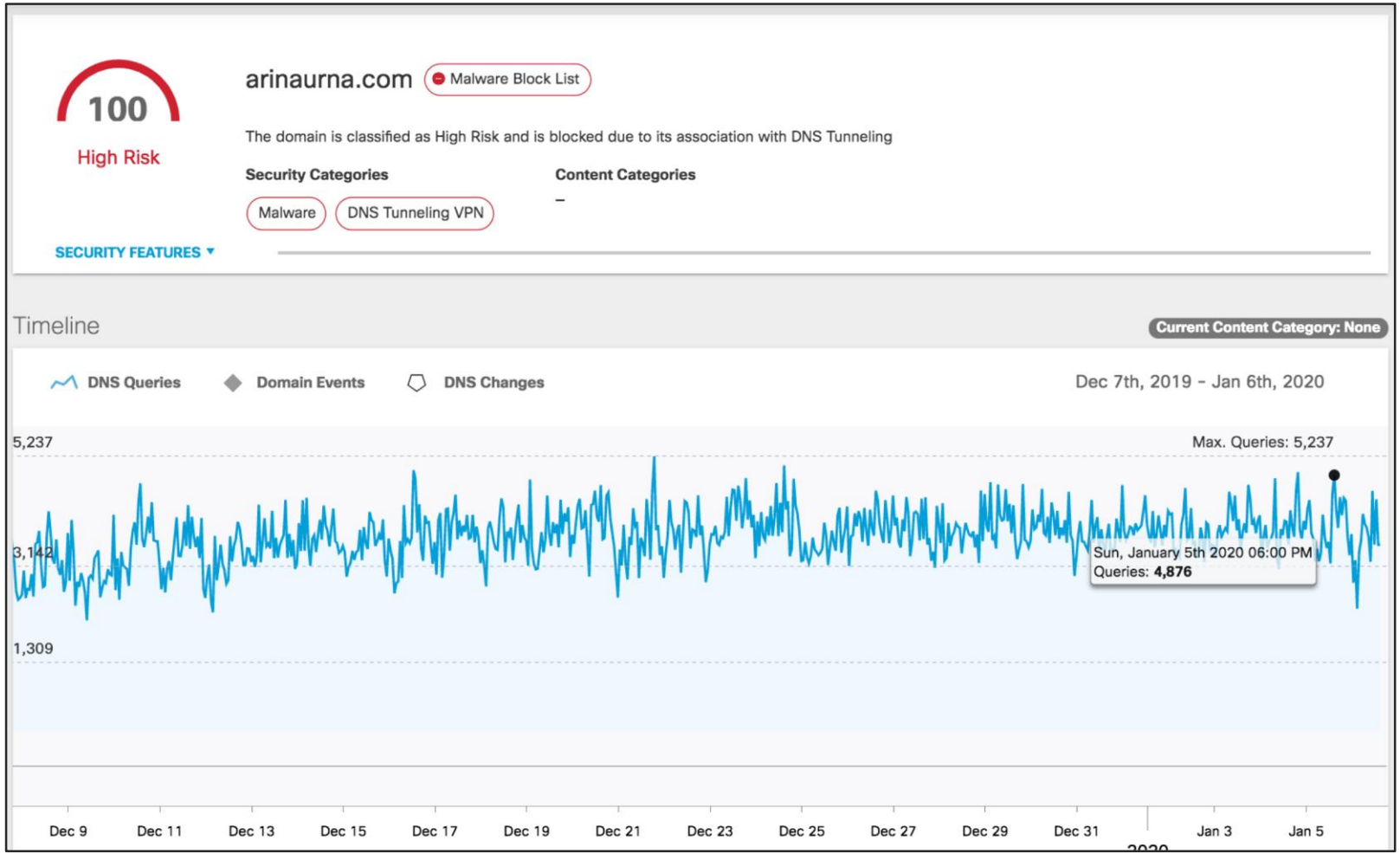
- DNS tunneling
- Malvertising
- Phishing

Graph analysis

- Cybercrime goods and services
- DGA botnets

Anomaly detection

- Cryptomining pools
- Crimeware



Subdomains

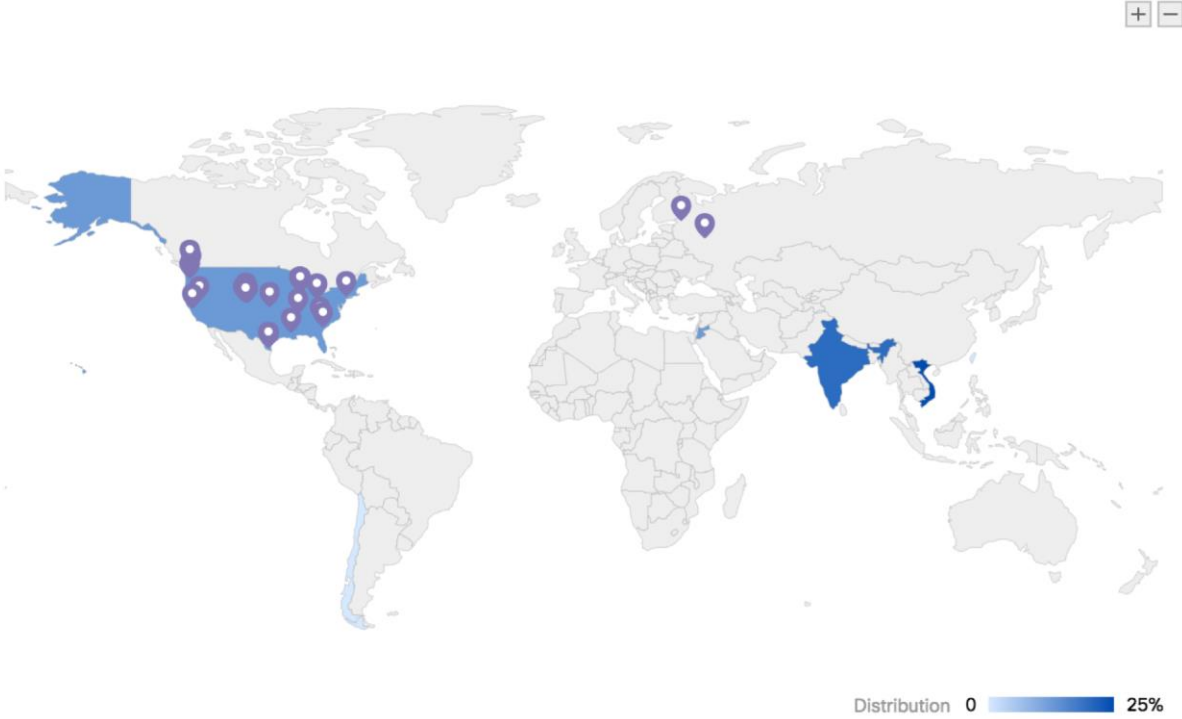
Name	First Seen	Umbrella Behavior
0.arinaurna.com	2019/06/24 19:20	Malware, DNS Tunneling VPN
0-pt09wmiulavzgb.arinaurna.com	2019/06/19 21:10	Malware, DNS Tunneling VPN
02j2dojivhbgqqhz.arinaurna.com	2019/06/24 02:52	Malware, DNS Tunneling VPN
02sdakp2jferyube.arinaurna.com	2019/04/22 20:30	Malware, DNS Tunneling VPN
02td34w3hbvcswqy.arinaurna.com	2019/07/10 23:47	Malware, DNS Tunneling VPN
03qknm6vctqscye4.arinaurna.com	2019/05/14 03:13	Malware, DNS Tunneling VPN
04ibxc3adsi4xx.arinaurna.com	2019/08/13 02:32	Malware, DNS Tunneling VPN
06iyemngbqrmxppt.arinaurna.com	2019/04/01 04:21	Malware, DNS Tunneling VPN
08hdrvfdh97buiwl.arinaurna.com	2019/05/13 01:52	Malware, DNS Tunneling VPN
0al9bo8646izpqkb.arinaurna.com	2019/06/26 22:40	Malware, DNS Tunneling VPN
0awsrz5cgrzyldis.arinaurna.com	2019/09/10 21:37	Malware, DNS Tunneling VPN
0bbwjslm3rgdnpdu.arinaurna.com	2019/05/17 06:24	Malware, DNS Tunneling VPN
0bohvzleab23gtzra8uo2qwbaulpqtpolxdatfr1...	2019/09/17 04:36	Malware, DNS Tunneling VPN

Host

IP Count	32
Registrant Country	US

Requester Distribution

COUNTRY	PERCENTAGE
Viet Nam	25.00%
India	18.75%
United States	12.50%
Singapore	12.50%
Jordan	12.50%



Data transfer direction

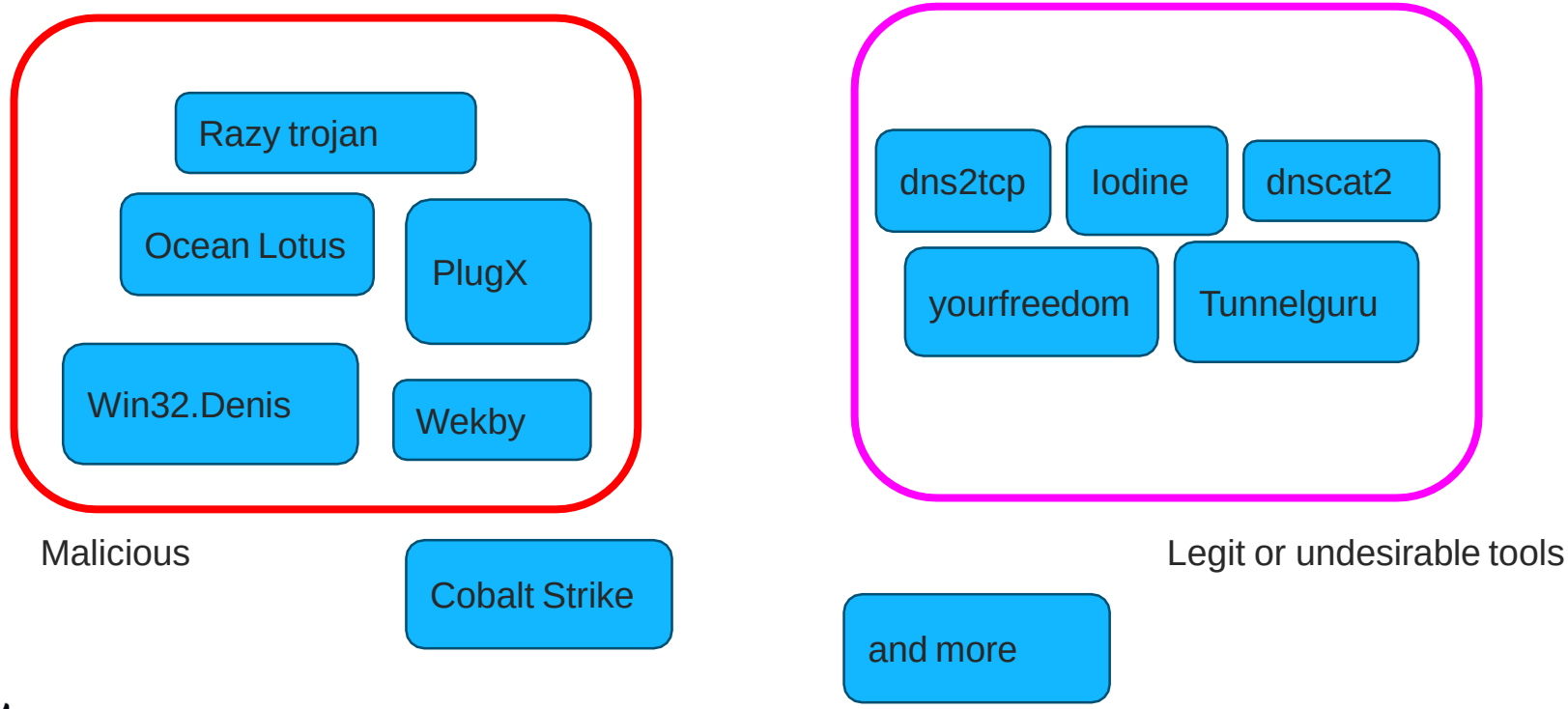
To attacker

From attacker

bidirectional

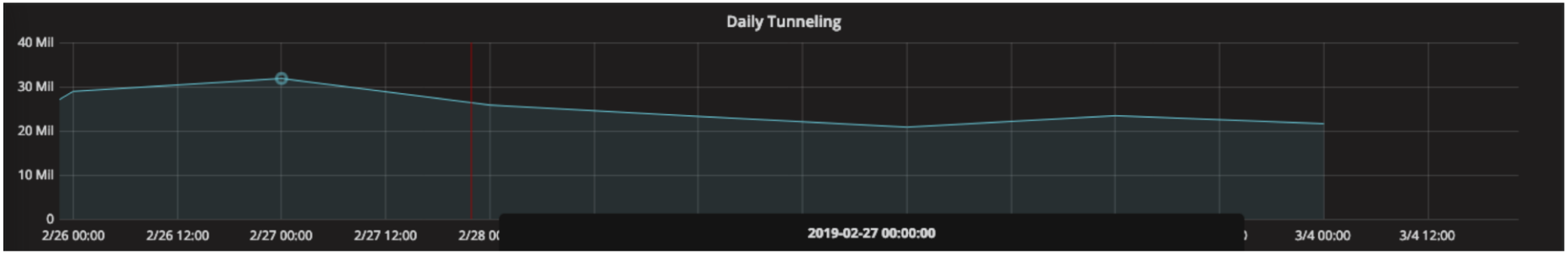
Attacker controls an authoritative name server

DNS Tunneling in the wild



DNS Tunneling stats

Less than 1% of global traffic



Ocean Lotus

NULL_QTYPE_TUNNELING	
1198	nsquery.net
1198	jessicajoshua.com
1198	facebook-cdn.net
1197	phillippcliche.com
1193	thomaswaechter.com
1170	charlotteagnes.com
1168	poppyranken.com
1167	gl-appspot.org
1165	lotteagnesar.com
1153	tonholding.com
1150	teriava.com
875	tulationeva.com
486	5t2.be
406	notificeva.com
380	vieweva.com
41	getbring.de
35	shervin.org
31	89u.uk

TXT_QTYPE_NS_LABEL	
1000	yomiuri.us
1000	voanews.hk
1000	nowpublic.us
1000	microsofurl.com
1000	microsoftner.com
1000	micorsoff.com
995	micrrsoft.net
733	flashplayerget.com
520	facebookcdn.com
319	microselver.com

PlugX

100 UK orgs surveyed in 2017
21% impacted by data exfil via DNS tunneling*

*https://www.infosecurityeurope.com/__novadocuments/445880?v=636554279131430000

cisco Live!

DNS Tunneling and ATT&CK

- T1071 -> Standard Application Layer Protocol

Home > Techniques > Enterprise > Standard Application Layer Protocol

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

ID: T1071

Tactic: Command And Control

Platform: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

Version: 1.0

Enterprise	T1071	Standard Application Layer Protocol	Cobalt Group has used HTTPS and DNS tunneling for C2. The group has also used the Plink utility to create SSH tunnels.[1][3][4]

Enterprise	T1071	Standard Application Layer Protocol	OilRig has used HTTP and DNS for C2. The group has also used the Plink utility and other tools to create tunnels to C2 servers.[5][7]

DNS Tunneling and APT groups

Groups	Software	Abused DNS QTypes
Cobalt group	Cobalt Strike	NULL A AAAA TXT etc.
OceanLotus/APT32	Denis SOUNDBIT E Goopy	
OilRig	ISMDoor ISMAgent Helminth ALMA	
Multiple Chinese APT groups	PlugX	
Darkhydrus	RogueRobin	Google Drive

Lexical feature selection and Clustering

- Interested in lexical features of subdomains
  - Subdomains contain the ‘payload’ of the message
- Look at the following feature sets:
  - Number of subdomains
  - Length of subdomains
  - Number of consecutive numeric characters
  - Existence of particular trigrams
  - Frequency of switching between numbers and characters
  - Compressibility of feature sets

Cluster: Ocean Lotus/APT32

- A cluster containing many Ocean Lotus domains
- The payload contained in the 2nd level subdomain
- Not necessarily all malware

```
otakeaaaaaaaaaaaaaaaaaaaaaaaaaaah28.z.teriava.com.,5
ifh78qaaaaaaaaaaaaaaaaaaaaaaaaalle.z.nsquery.net.,5
mayohospital1-mail-onmicrosoft-com.mail.protection.outlook.com.,5
fenghuangshishicaipingtaixiazai.nsvpn-lvs-hosts.paypalcorp.com.,5
6wjdlcryvvlq673h3u4ehtbwpkohzfem._domainkey.concursolutions.com.,5
yciodgaaaaaaaaaaaaaaaaaaaaaaaaajyy.z.phillippcliche.com.,5
secure.wellsfargo.com-verify-your-account-information.yunkui.ru.,5
o0wc5aaaaaaaaaaaaaaaaaaaaaaaaaaah6p.z.tonholding.com.,5
personalresponsibilityselfreliant.wordpress.com.,5
mjlokdqcpbbbjbllpndcondcbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
aomenzuqiubocaiguanfangwangzhan.lvs-ns-mpls.paypalcorp.com.,5
luciazanetti-files-wordpress-com.cdn.ampproject.org.,5
memjloqcpbbbjbllqfdcqfdcbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
pujingxianshangyulechengfanshuiduoshao.lvs-sc-craz.paypalcorp.com.,5
lpkejjqcpbbbjbllqodcpodcbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
autometer1309tachometerspeedometered2.wordpress.com.,5
beqipnqcpbbbjbllnfdcmfdcbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
nhmmlbqcpbbbjbllppdcopdcbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
selector1-logicspedsrl-onmicrosoft-com._domainkey.logicspedsrl.onmicrosoft.com.,5
bgdlfqqcibbbjhjbhbbbqffbbbbbbbbbbbbbbbb.ns.micorsoff.com.,5
t1rtaqaaaaaaaaaaaaaaaaaaaaaaaaakgb.z.jessicajoshua.com.,5
xrn54qeh3ez3fn2ecfybtlcifcm67ayl._domainkey.bookinggroup.com.,5
willthegaymarriagerulingaffectme.com.dns.shodan.io.,5
91ncsgaaaaaaaaaaaaaaaaaaaaaaaaakaw.z.teriava.com.,5
zn2tvwvymmbpccqd6-alliancehealth.siteintercept.fanduel.com.,5
```

Cluster: PlugX and Benign Traffic

- Cluster contains malware and benign tunneling
  - PlugX
- Similar tunneling encoding structure
- Example of how clustering does not cleanly split into groups

```
cjboadobcenncdlapbognlmalfkkjpieijhogdfiendcchbmabpfoknpnemjlok.djiinhcghfmebdgclcabfakpoodnimnlckhjmibhghlgaffekdpcebjaopcohnm.mbmgllkajfikhpgefj.ns2.voanews.hk.,1
gifnfcoblcojidahcabfakpoodninnmclhkmjbighlgaffekepdecjboadphomn.bmgllkafjkiphegjfoeddicnbcbhampaofnkmplekjjoidiihngcfhemdbcgbl.aapepjoondmilnkcjh.ns2.voanews.hk.,1
lckhjmobknghgaagampaofnkmplekjjojdiihngcfhemdbcgblaapeojoondmil.nkcjhimhbggfleadfdkcpbeajpnocnhmmlbkgjliaifhkgpfeejdocdbianpbog.nlnamflkkpjeijhogd.ns2.voanews.hk.,1
lokdkiobmjnbbihchpgefjeoddcibnacpgolnamflkkpkejjiohdgifnecdhcmb.bagpkopnemjlokdjiinhcghfmfbegdlcabfakpoodnimnlckhjmibhgglfaefdk.cpbeajaopcohnmmblg.ns2.voanews.hk.,1
mclhkmobmnkfglkkbgalppoenjmoldkijnichhgmfbegdlcabfbkappdoinnmcl.hkmjbighlgaffekdpcebjaopcohnmmbmgllkajfikhpgefjeoddcibnacpgolna.mflkkpjeijhohdgifn.ns2.voanews.hk.,1
ngmllaobmbhimcjhichhgmfbegdlcabfakpopdoinnmclhkmjbighlgaffekdpc.ebjaopcohnmmblgllkajfikhpgefjeoddcibnacpgolnamflkkpjeijhohdgifn.ecdhcmbbagpkopnemj.ns2.voanews.hk.,1
```

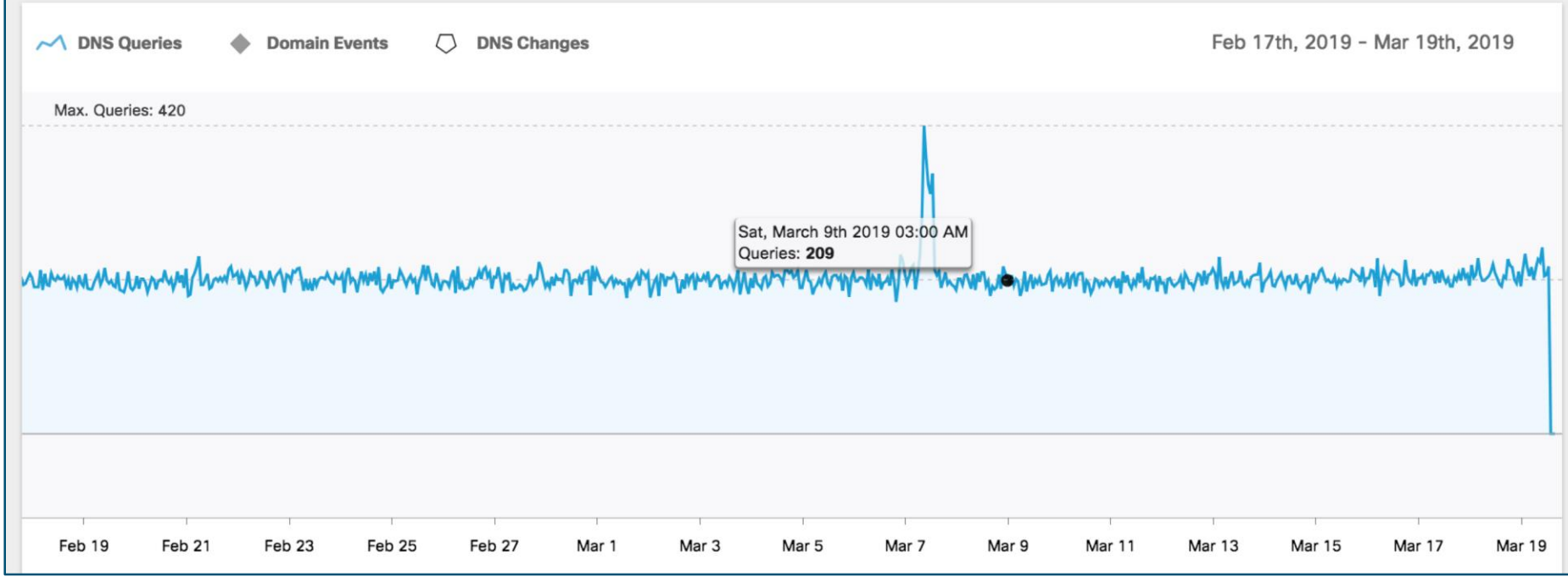
```
bl.ukctfyldvpcnk38qlumhjgas5jf7jpbh9fr8x1fd3x7jsskbcgyhdjgiuo9i8xy.rtojs7kcxb4wpq6ev5rkt0pjmzn790h29vm10n3ozxpfwryjr5fhgh30nds.s03.63z.de.,1
pxomnrxkmsooppjmltlyknjsywylxqwvvkvpuutjsostryqnpspxomnrmwmllqk.vjkjpytxywnwsvxumtrtwslrqqvqkppounjnomtlyknksjxyl.ns9.microsofurl.com.,1
bl.u0cftdgcb7mxah1okmfslolkz4tlftgkwlcuslmonesznkgfwswfkq1fz4dbuxy.r5hblw3szv2zibzxozbv0gwuintozn8tossc1qjjbrbabwhnu6bwae5ttnk.s17.8u6.de.,1
cb.usnms63bs36dvf2u1hajwgqrctgoh3no3s4obxq2kut1thvempwxiqnugpbauxy.umn50d9tradwpmurgqmjiypo0czaboqsyc1no9gm0eggo1faepscqj1pxbyaiwi.nmyvgxen3dag9cyi0wb.s33.8u6.de.,1
bl.ua9swwzb3kixmq3yem3kk6j70vwfslz8oygeousfexonaxrx74lp1sboknccouxy.r2o2tzfb08g5sf1m1ofase2dvtbqseyoaunq3zq1wow5rboqssixtdhv54t.s11.63z.de.,1
cb.usheucanf1dmh7sjrsfr3w6prznsnjkxmltkj4ekvql5bbrvre2xzfzecvomauxy.usn2qq6bx3npsnleovewh6kqehf7dqmfjiookq60wu42qrnvtbhhjsk7shkoz9h.nipk7dizfjlrjvzylud.s33.8u6.de.,1
cb.ux7cahe27n88kis5hgz3hzjc7hlsaqk2tl5eatpsbvmutkft88qsorwam0lauxy.uzeyi8ptazleftkcolyxaadul5wcqmoqckunfswvrfuh1a3b7dfkqgdhywb2hbv.n2aj04p8j9q36dc5vod.s14.8u6.de.,1
bv.uek21hkem9idr5o6jmrvpyqcxca1en2jti0vu7ipo1pdsiwnzpvrb420zeofxxy.b86pnoquwnnzuixnwxzkcgg44l62r92zxzjnp.s26.63z.de.,1
bp.u9yyixozon8de0mzjz1lcgdfqkleojqy6b5vnprsq4zo556v3wam6zmoxlomuxy.vwsc87nw04adzwyagw5qc72edqxrm.s24.63z.de.,1
bf.u2vrpbyswsloypctmqmhk46uwodxagmuq5cy3e4dvvryu4dvkpbxgpynh2gauxy.lrenxva4frohafoh0wlhpojzizdcpzmovouvlrk4k529aulmhud.s16.63z.de.,1
mt.9f005hrws8mliotmdqovnevimthj8zwri7rp06lut2r6vxk4rum6v1tb.gd7p9g02jxc.s23.8u6.de.,1
cb.u5av8odrudahplhjolfvq4exiye8mypnsmeucavlwjmek4mutx0w8prv8htg7xy.um53cvycr5rhaqbgbwcj0ntgdeb2pwms7cwhx3ew38zldzu1vohzye9blhfvzlq.n230bdfnzm1bot1dc5c.s25.8u6.de.,1
cb.umlslzjvqh54optjvkaqfj7njgjaftqoxpjp8fvkzk9sex4uk0xzfzecvomauxy.ufw5svpv51onapjw9eilzsajydy5ymxhzieksavpxw1jllaz7pbv9h33svejmee.nr8ya0z0pnvrxgsbmmd.s33.8u6.de.,1
cb.uijxgpszlge4xembsf7ctzjap5bxm0o2vr2tax4xebvcuvnd1fe7gwhqmabbuxy.u2r4smq08kopkyhebonqanvps8lt3kprolhxmgjrhig8ruasfo0mvj2esyzmfib.nnznhwzibayya5wjyhe.s25.63z.de.,1
```

Details for prosalar.com

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 53

Timeline (Beta)



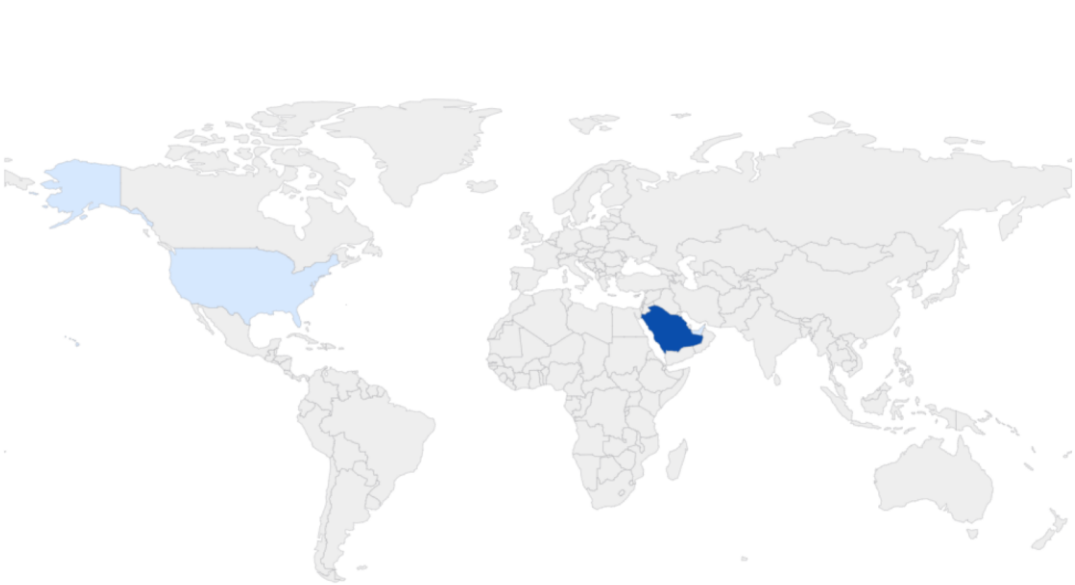
OilRIG group, ALMAcommunicator

Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km
Registrant Country	US

Requester Distribution

COUNTRY	PERCENTAGE
Saudi Arabia	40.00%
United States	20.00%
United Arab Emirates	20.00%
Bahrain	20.00%



Subdomains

Name	First Seen	Category
6190id4a5b753459-0-2d-2d.prosalar.com	2017/11/02 19:13	
2721id4a5b753489-0-2d-2d.prosalar.com	2017/11/02 19:13	
5310id4a5b753473-0-2d-2d.prosalar.com	2017/11/02 19:13	
6646id4a5b753455-0-2d-2d.prosalar.com	2017/11/02 19:13	
1138id0b25c0f5120-0-2d-2d.prosalar.com	2017/11/13 15:57	
3658id4a5b753493-0-2d-2d.prosalar.com	2017/11/02 19:13	
1190id4a5b753486-0-2d-2d.prosalar.com	2017/11/02 19:13	
9315id4a5b753446-0-2d-2d.prosalar.com	2017/11/02 19:13	
3025id4a5b753432-0-2d-2d.prosalar.com	2017/11/02 19:13	
7860id4a5b75348-0-2d-2d.prosalar.com	2017/11/02 19:13	
1393id4a5b753414-27-3a5265706561743a2045-5f446e73496e6974.prosalar.com	2017/11/02 19:15	
5076id4a5b753496-0-2d-2d.prosalar.com	2017/11/02 19:13	
7291id4a5b753457-0-2d-2d.prosalar.com	2017/11/02 19:13	

3 Classes of ML algos to solve threat detection

NLP/Clustering

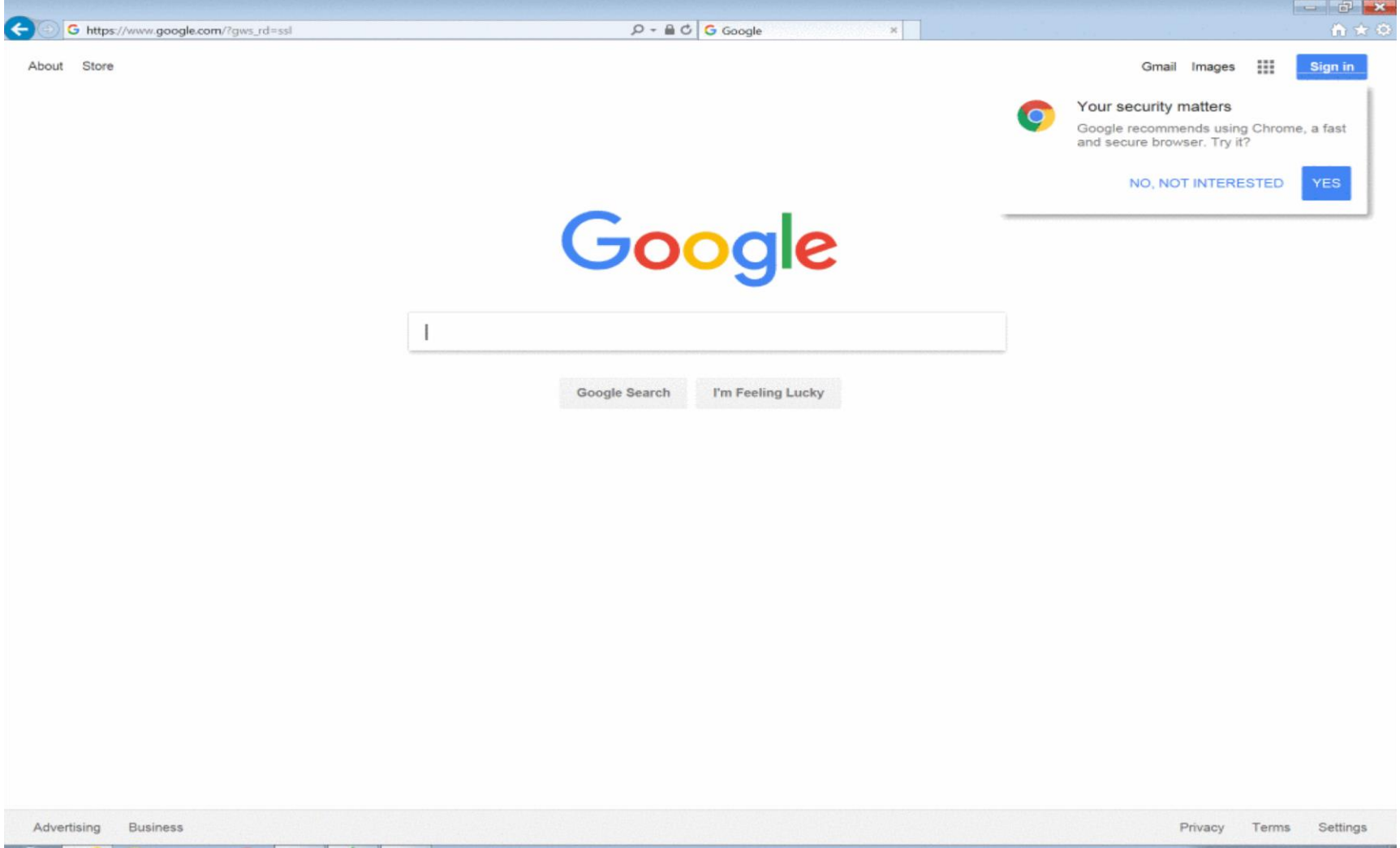
- DNS tunneling
- Malvertising
- Phishing

Graph analysis

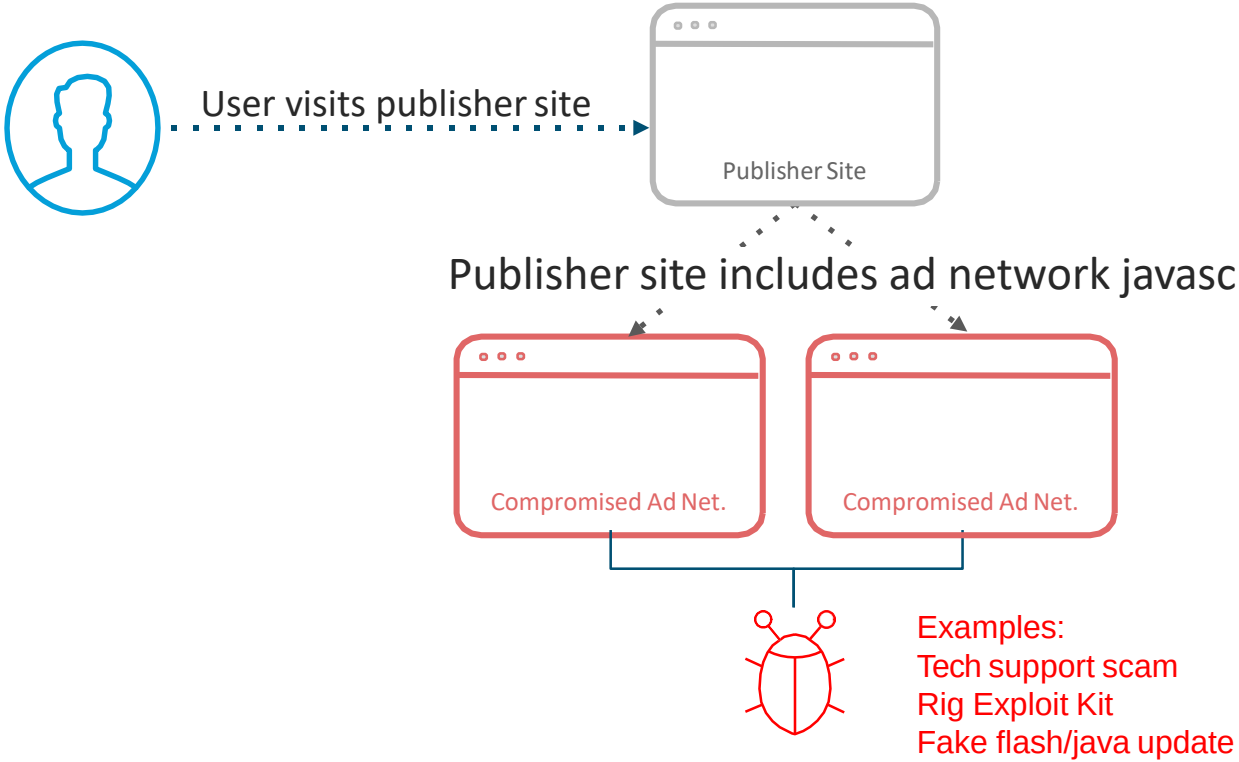
- Cybercrime goods and services
- DGA botnets

Anomaly detection

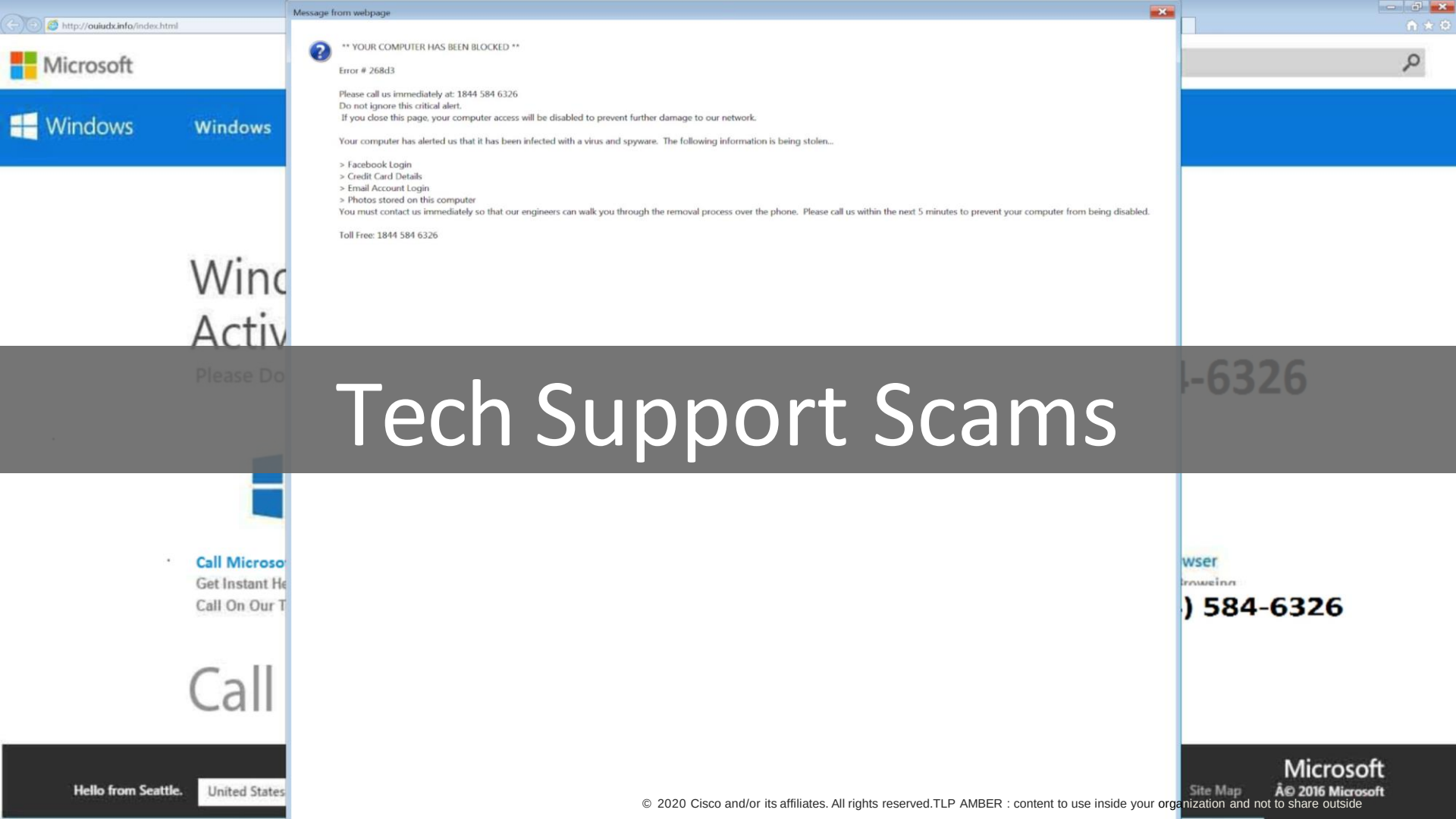
- Cryptomining pools
- Crimeware

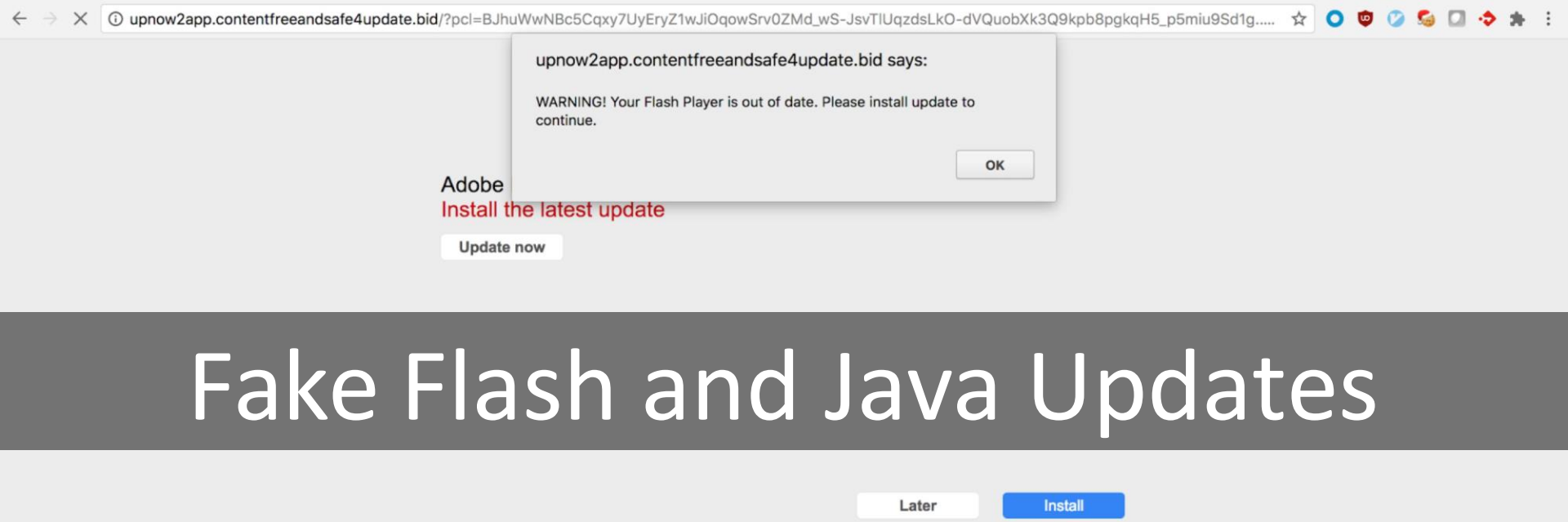


Ad campaign flow

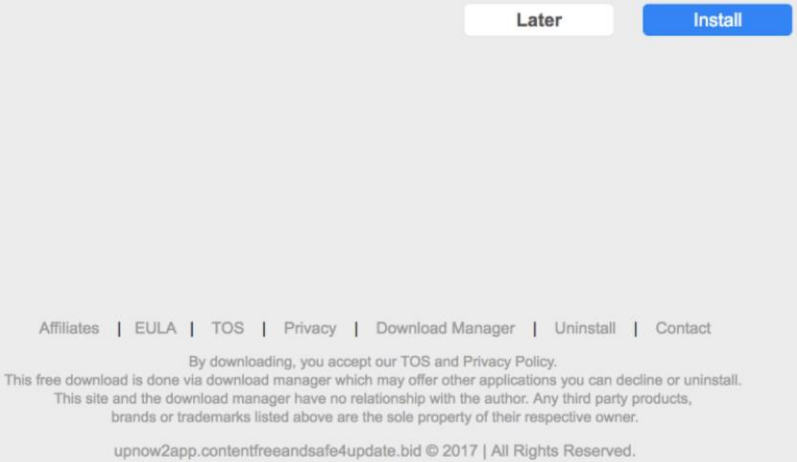


Tech Support Scams

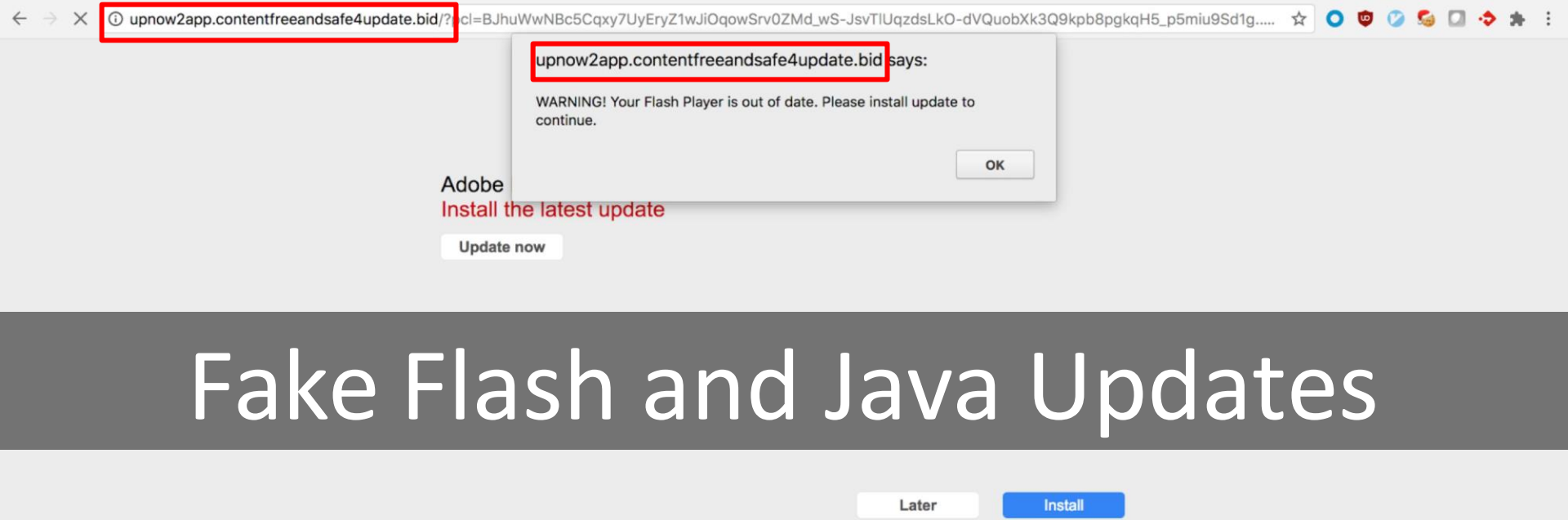




Fake Flash and Java Updates



Lexical Clustering



Fake Flash and Java Updates

Investigate

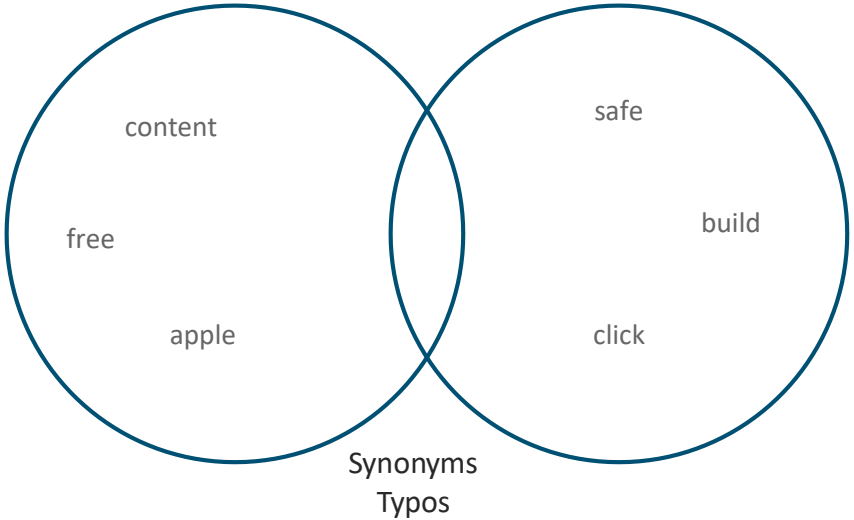
SEARCH PATTERN SEARCH BULK EDIT

contentfreeandsafe.* INVESTIGATE Constrain RegEx search to Last 30 days

Showing 460 results for **contentfreeandsafe.***

Domain Name	Security Categ...	First Seen
contentfreeandsafe2updating.stream	Newly Seen Do...	December 13, 2017, 3:17pm
contentfreeandsafetoupdating.review	Newly Seen Do...	December 13, 2017, 3:09pm
contentfreeandsafe4updating.date	Newly Seen Do...	December 13, 2017, 3:00pm
contentfreeandsafeupdatesgreat.win	Newly Seen Do...	December 13, 2017, 2:18pm
contentfreeandsafeupdatingnew.win		December 13, 2017, 11:27am
contentfreeandsafetoupgrade.stream		December 13, 2017, 11:16am
contentfreeandsafe4upgrading.download		December 13, 2017, 10:39am

Regular expressions



Known Keywords

UnKnown Keywords

Regular expressions

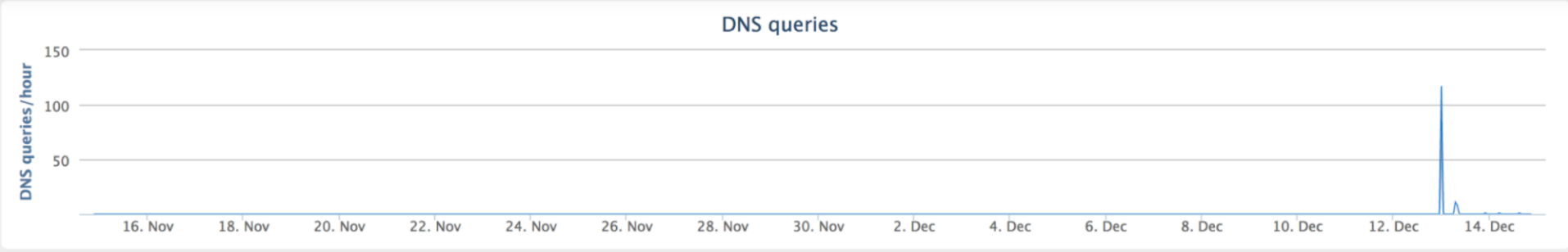
~~grep "* fake.*"~~

Traffic patterns

contentfreeandsafe4update.bid

INVESTIGATE

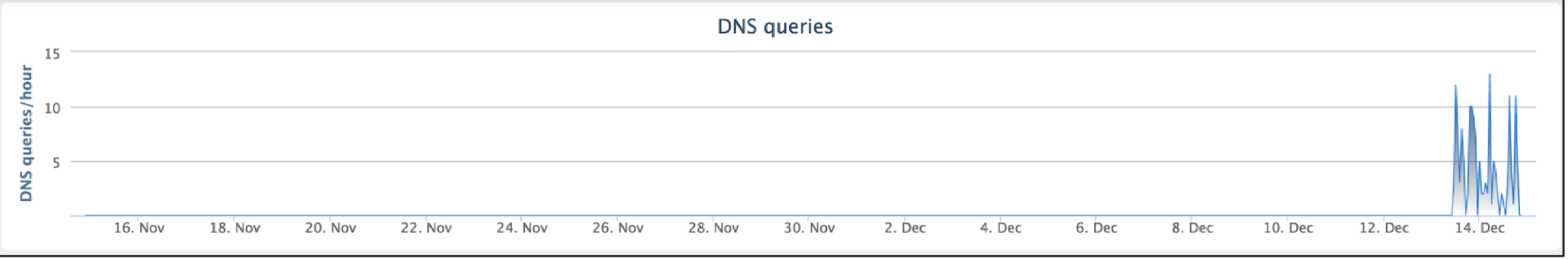
BACK TO TOP



contentfreeandsafe2update.date

INVESTIGATE

BACK TO TOP



Traffic patterns

~~Look for burst in traffic~~

Shingling Fake Java and Flash Updates

Trigram host name

contentfreeandsafe4update

{‘con’, ‘ont’, ‘nte’, ‘ten’, ‘ent’, …, ‘ate’}

Shingling Fake Java and Flash Updates

Trigram host name

↓

contentfreeandsafe4update

↓

{‘con’, ‘ont’, ‘nte’, ‘ten’, ‘ent’, …, ‘ate’}

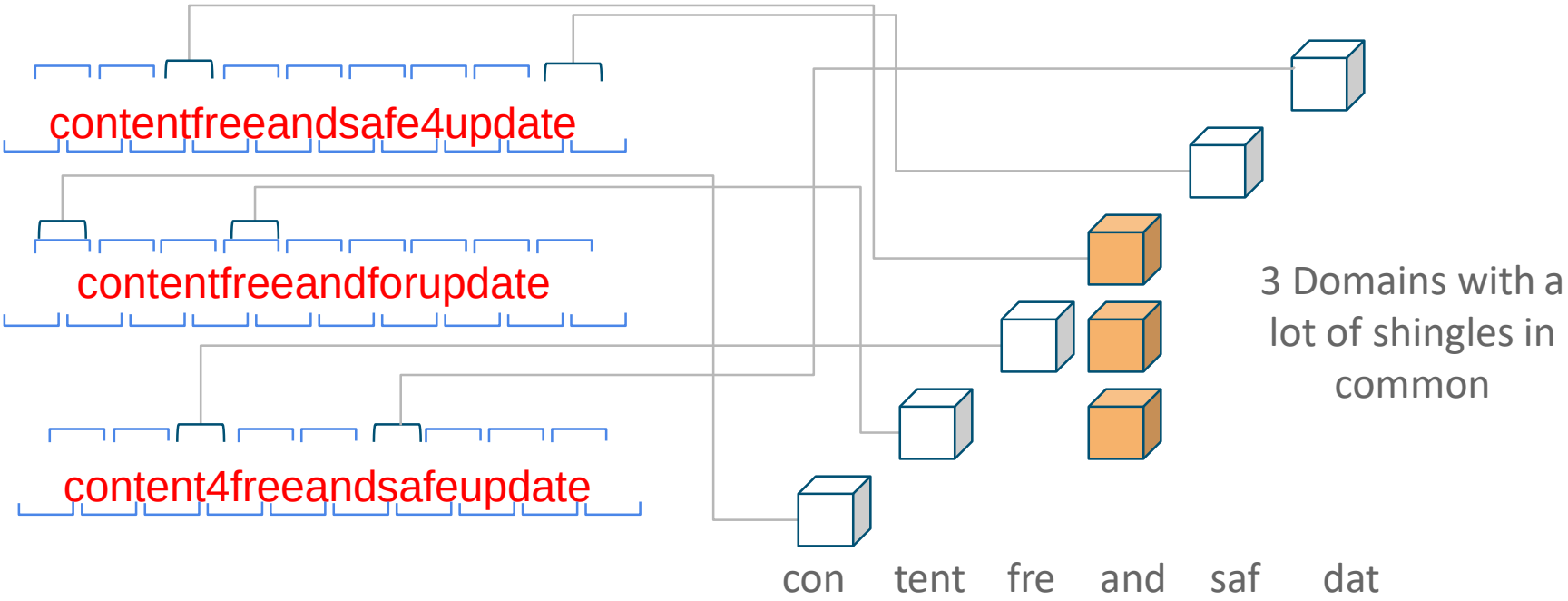
↓

MinHash

↓

LSH

Locality Sensitive Hashing Fake Flash



Results

Fake Flash and Java Update lexical clustering

cluster_1:
goodnewcontentssafe.download
goodnewfreecontentsload.date
goodnewfreecontentall.trade
...

cluster_2:
call-mlcrosoftnw-err81711102.win
call-mlcrosoftnw-err99817109.win
call-mlcrosoftnw-err81711101.win
...

cluster_3:
artificialintelligencesweden.se
artificialintelligencechip.com
artificialintelligence.net.cm
...

cluster_4:
mkto-sj220048.com
mkto-sj220146.com
mkto-sj220162.com
...

Tagging dashboard


```
30
31          for j, domain in enumerate(entry['domains']):
32              entry['domains'][j] = {'domain': domain, 'timestamp': entry['ti
33
34          entry.pop('timestamps')
35
36      for i, idx in enumerate(date_changes):
37          n = date_changes[i+1] if i < len(date_changes) - 1 else None
38          r[idx:n] = sorted(r[idx:n], key=lambda x: x['c_num'])
39
40  @app.route("/clusters/attribution", methods=['POST'])
41  def attribution():
42      if not request.json:
43          return "Error!"
44      resp = {}
45      for cluster_id in request.json:
46          attr = request.json[cluster_id]
47          ret = add_attribution(cluster_id, attr)
48          resp[cluster_id] = ret
49
50          if ret == 'success' and BLOCKING:
51              domains = m.get_cluster_domains(cluster_id)['domains']
52              block_description = "Domain showed similarities to {0} malverti
53              print "Blocking domains: {0}".format(", ".join(domains))
54              block(domains, block_description=block_description)
55
56      return jsonify(resp)
57
58  @app.route("/clusters/attribution/<string:cluster_id>")
59  def get_attribution(cluster_id):
60      return jsonify(m.get_attribution(cluster_id))
61
62  @app.route("/clusters/uncategorized")
63  def get_uncategorized():
64      r = [entry for entry in m.get_uncategorized()]
65
66      if not r or len(r) == 1:
67          return jsonify(results=r)
```

3 Classes of ML algos to solve threat detection

NLP/Clustering

- DNS tunneling
- Malvertising
- Phishing

Graph analysis

- Cybercrime goods and services
- DGA botnets

Anomaly detection

- Cryptomining pools
- Crimeware

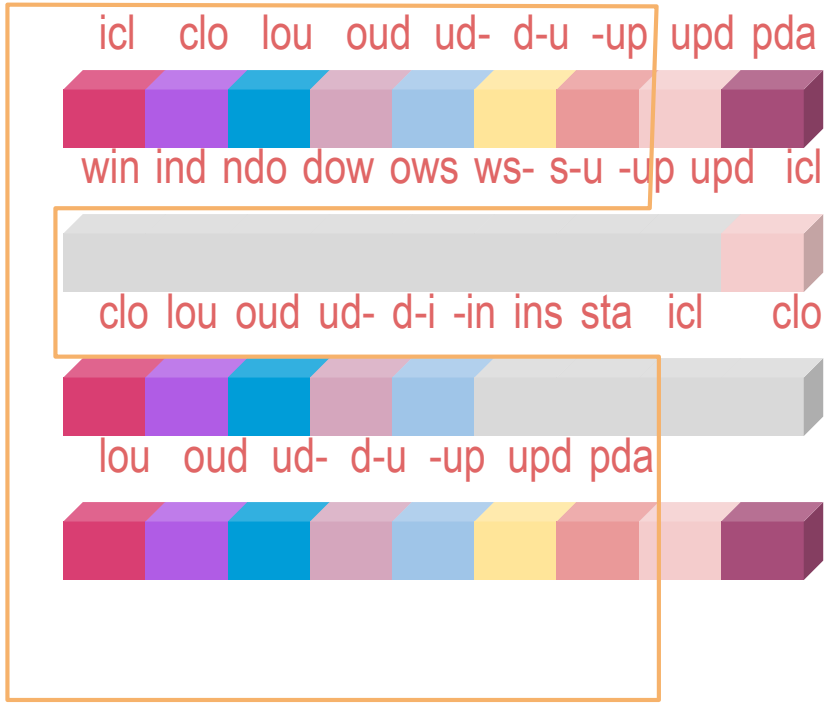
Newly seen domains - Lexical clustering w/ LSH

icloud-update-usa.com

windows-update-usa.com

icloud-install-usa.com

icloud-update-now.com



Investigate

SEARCH PATTERN SEARCH

appleid.* INVESTIGATE Constrain RegEx search to Last 7 days

Showing 349 results for appleid.*

Domain Name	Security Categories	First Seen
appleid.apple.com-283mawj29sj.labloco.com	Newly Seen Domains	September 22, 2018, 07:25pm
appleid-reset.com.authsids-sign.in		September 22, 2018, 06:53pm
appleid.apple.com.com-page-manage-purchase-cancel.com	Malware	September 22, 2018, 06:53pm
appleid-apple-icloudaccountrecovery.flu.cc	Malware, Phishing	September 22, 2018, 06:53pm
appleid.apple.com.manage.accounte.support.siliti.xyz	Malware	September 22, 2018, 06:53pm
appleid.com.verifyiing-locked-account.tk		September 22, 2018, 06:53pm
appleid.apple.com.accountverification.sampaimodar.com		September 22, 2018, 06:53pm
appleid.apple.com.unlocked-accountcc.serveirc.com		September 22, 2018, 06:53pm
appleid-centre-unblock.com	Newly Seen Domains	September 22, 2018, 06:26pm
appleid.apple.com.signin-6dc5hbed6e3e4af795g72c62d952a2c4.com	Newly Seen Domains	September 22, 2018, 06:15pm
appleid-support.manage-verificationaboutservice.com	Newly Seen Domains	September 22, 2018, 05:52pm
appleid-unlock.apple.idapps-assistance.info	Newly Seen Domains	September 22, 2018, 05:37pm
appleid.apple.com.tuyulgauls.com	Newly Seen Domains	September 22, 2018, 05:18pm
appleid-login-apple.us	Newly Seen Domains	September 22, 2018, 05:06pm
appleid.siignin.us	Newly Seen Domains	September 22, 2018, 04:56pm
appleid-apple.com.toyolgauls.com	Newly Seen Domains	September 22, 2018, 04:26pm
appleid.mil.ph	Newly Seen Domains	September 22, 2018, 03:21pm
appleid.apple.com.aldyjembut.co.uk	Newly Seen Domains	September 22, 2018, 02:02pm
appleid.verified-unlocked-account-information.com	Newly Seen Domains	September 22, 2018, 01:18pm
appleid-account-cancel-purchase-apple.com		September 22, 2018, 12:35pm
appleid-appleca.com	Newly Seen Domains	September 22, 2018, 12:35pm
appleid-cancel-purchase-apple.com		September 22, 2018, 12:35pm
appleid.rdsapple.com	Newly Seen Domains	September 22, 2018, 11:31am
appleid-apple-icloudaccountverify.nut.cc	Malware	September 22, 2018, 10:52am

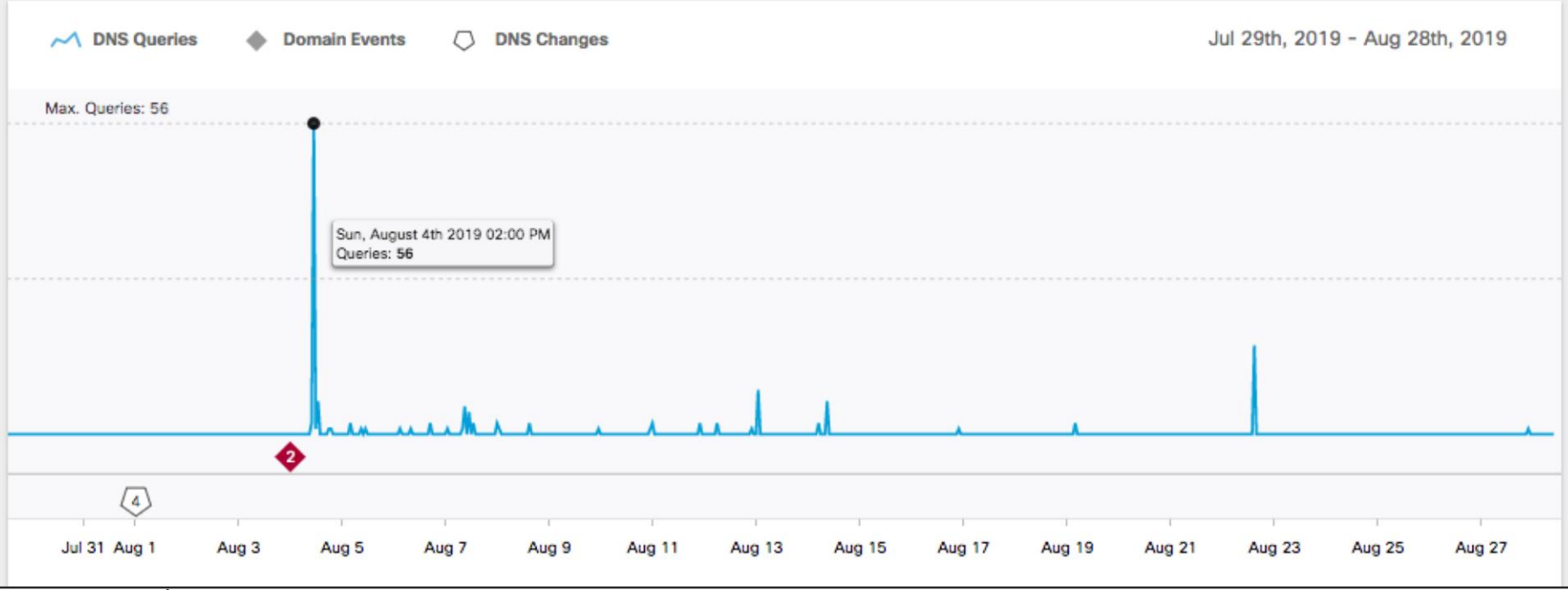
Details for securekonto-santander.com

Classifier prediction: Medium

Umbrella Investigate Risk Score: 64

Timeline (Beta)

Current Content Category: None



Lexically Similar Domains (Experimental)

Name	Distance
inmo-santander.com	0.3333333432674408
piso-santander.com	0.3333333432674408
b-santander.com	0.3333333432674408
grupo-santander.com	0.3499999940395355
santandersecure.com	0.3499999940395355
pb-santander.com	0.3513513505458832
seesantander.com	0.3513513505458832
bp-santander.com	0.3513513505458832
rcmsantander.com	0.3513513505458832
santander.com	0.3529411852359772
cruesantander.com	0.3684210479259491
ola-santander.com	0.3684210479259491
notisantander.com	0.3684210479259491
nunusantander.com	0.3684210479259491
dsantander.com	0.37142857909202576
msantander.com	0.37142857909202576
vsantander.com	0.37142857909202576
bsantander.com	0.37142857909202576
elhostelco-santander.com	0.3777777850627899
danzasantander.com	0.38461539149284363

3 Classes of ML algos to solve threat detection

NLP/Clustering

- DNS tunneling
- Malvertising
- Phishing

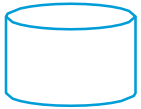
Graph analysis

- Cybercrime goods and services
- DGA botnets

Anomaly detection

- Cryptomining pools
- Crimeware

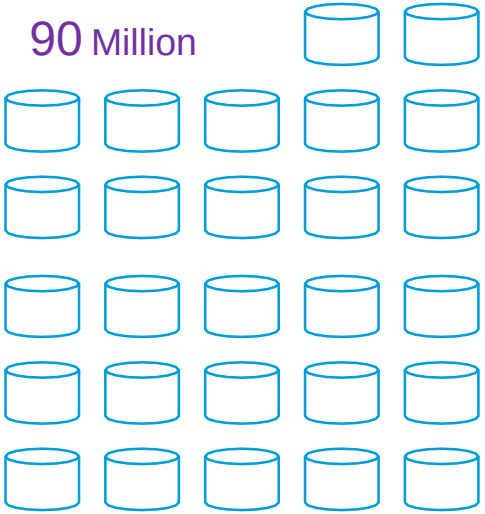
Graph Partitions/Propagation



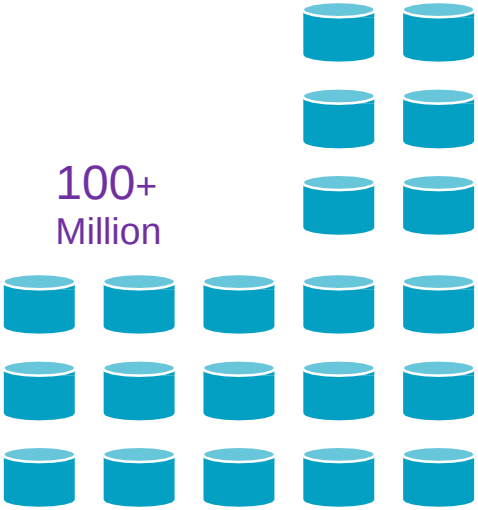
Client IP

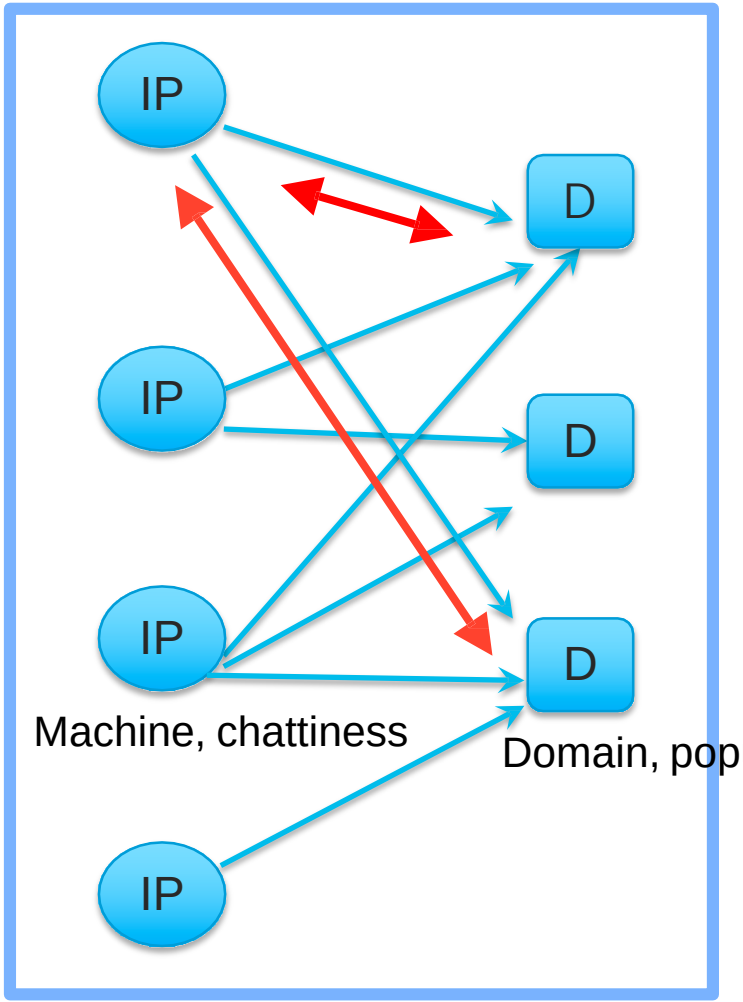
Hosting IP

90 Million



100+ Million





Amplifying signals through seeds

For every 1 hour of traffic, we define:

- Chattiness: # unique domains a machine queries
- Popularity: # unique machines that queried the domain

- amplify domain/ip chattiness/popularity nbdayspast
- Pivot through domains and machines by keeping a threshold of chattiness and popularity

Cybercrime , Fraud Management & Cybercrime , PCI Standards

Joker's Stash Advertises More Stolen Payment Card Data

Carder Forum Listing Appears Tied to Breaches at Four Restaurant Chains

Scott Ferguson (@Ferguson_Writes) • November 27, 2019

Twitter Facebook LinkedIn Credit Eligible Get Permission

jstash-bazar.store

Joker's Stash

Moving To .bazar

Joker's Stash has moved into blockchain-based domain name system.

Because it's decentralized and has no central authority, it's resistant to domain locks and other abuse.

Access Joker's Stash using this link:

http://jstash.bazar/

To surf **.bazar** domains install one of these browser extensions:

- **Blockchain-DNS** is the preferred choice, available for Chrome and Firefox
- **friGate CDN** - an alternative
- **PeerName** - another alternative

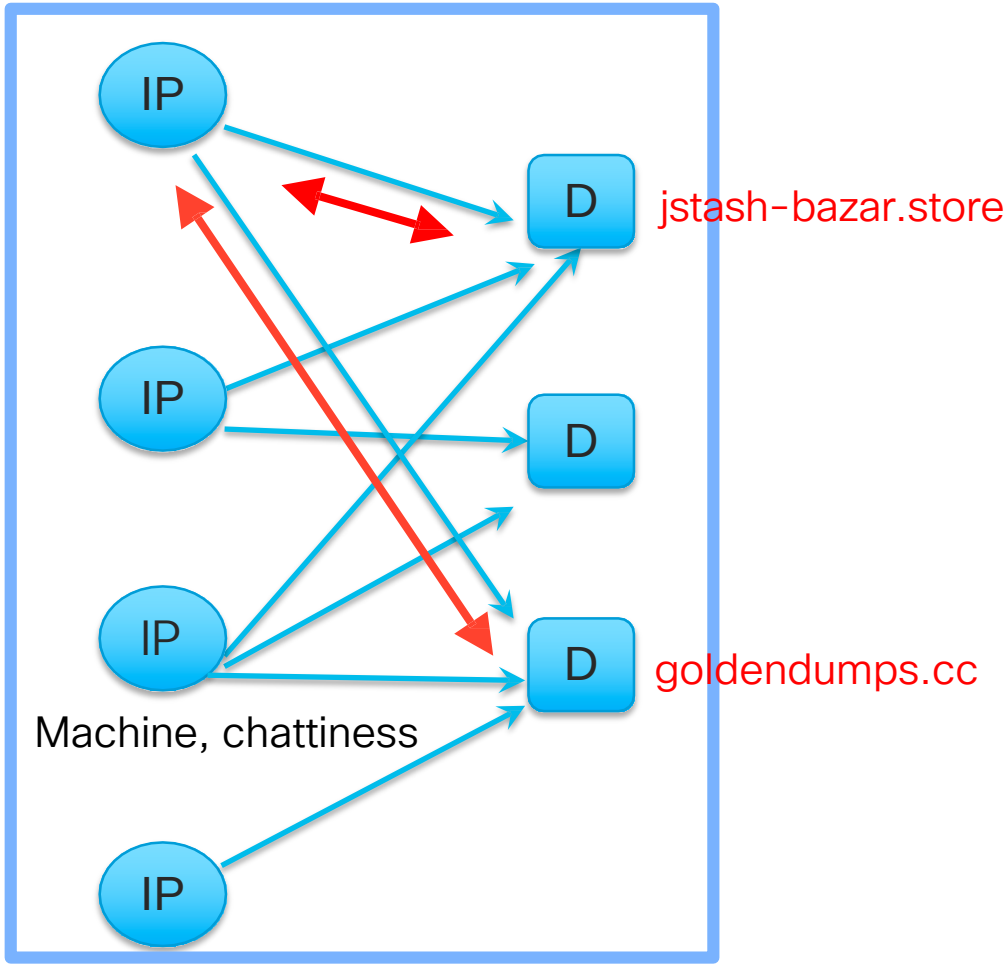
Do not enter just "jstash.bazar" into the address bar! This will trigger browser search operation. Instead, enter either:

- **jstash.bazar/** (with a slash at the end), or
- **http://jstash.bazar/**

© Joker's Stash

Machine, chattiness

Domain, popularity



GOLDEN DUMPS

Counsomed
$ 0.00

HOME | NEWS | DUMPS | CVV | NO CVV | PACKS | BILLING | ORDERS | TUTORIAL | SUPPORT

Support ● offline 00[00] - 19[00]

Hot news

Best cvv shop online ♦ cc shop ♦ cvv shop
TODAY 1/6/20 NEW GOOD UPPY in our shop:

CVV SECTION
- New updare from supplier SEOMI, MIX_JAN_5 [FULLZ][1/6/20] / Dark Market_191 [SSN+DOB][1/6/20] ready
- New update from supplier DOTA, Backhunter_93 [SSN+DOB][1/6/20] ready

whats a cvv on a credit card

buy cc full

cvv or cvv

best cc shop

credit card track 2 numbers generator

USERS ONLINE
562

Admin
User Liberia101 was banned by admin
Admin
User morrison112 was banned by admin
Admin
User Zoehova050 was banned by admin
Admin

Your message...

Amplifying signals through seeds

Pivot from jstash-bazar.store, jstashbazar.link, jstash-bazar.link, jstash03.link -> other cybercrime sites

amplify.sh dom jstash_list 100 10 [degree = 100, 10 days]

-Carding/dump shops: gocvv.biz, mastercvv.ru, cardmafia.cc, cardmafia.pw, cardmafia.ws, cardx.biz, cardx.ws, dumpswithpin.ru, goldendumps.cc, realdumppin.biz, trump-dump.bz, trump-dump.ru

-Cybercrime forums: gofuckbiz.com, bhf.io

-Anonymous vpn, proxy, socks: anonymous-vpn.biz, dblvpn.net, doublevpn.com, 5socks.net, isocks.pro, luxsocks.ru, rsocks.net, proxy6.net

Our main TOR mirror (All external resources and analytics Disabled): http://aprovpnacgvqwh76.onion

Your IP: 104.244.72.221 | Server time - 1, 7, 2020, 10:19

Sign In | Sign Up

Anonymous-VPN

Home Pricing Setup Help Blog en

PROFESSIONAL VPN SERVICE

- Guaranteed confidentiality
- 100% secure
- Without logs

BUY VPN

Protecting your personal data from government, police and ISP

ABOUT ANONYMOUS VPN

We - a unique VPN service that provides a truly anonymous and maximally safe access to the Internet, with us always easy and just stay in the shadow of the state supervisory bodies and other third parties, as well as being in full confidence that your personal data is safe .

PAYMENTS SYSTEMS

RECENT POSTS

How to fix dns leaks in Ubuntu 18, Debian 9, Kali Linux 2018
Posted 11 September 2018

How to fix DNSleak in Ubuntu 17
Posted 14 January 2018

CONTACT US

Anonymous VPN Technologies LTD
Tel: +507-833-6291
Address: New Horizon Building, Ground Floor, 3 1/2 Miles Philip S.W. Goldson Highway, Belize City, Belize
Email: support@anonymous-vpn.biz

Privacy Policy
Terms Of Use

FOLLOW US:

Copyright © 2020 Anonymous VPN All rights reserved.

Home | Blog | VPN

VIRUSCHECKMATE
Fastest comprehensive analysis

Check API Videos Tariffs Affiliate Sign in Sign up!

Be sure, check your files here

This is a place where you can check content for quick detection of viruses, worms, trojans, and all kinds of malware.
Also you can scan web-pages and domain. Check out our video tours if you have any questions!

Fastest analysis

High speed get partial and full results the scan. Special superfast methods for server-side usage.

Usable report

Most informative results page, both antivirus and for each of the objects to be scanned.

Smart auto scans

No runs by cron! Rescan immediately after antivirus was updated. Complete statistics for all time watching an object.

Full anonymity

All cloud services are disabled manually. All scanned objects are removed immediately.

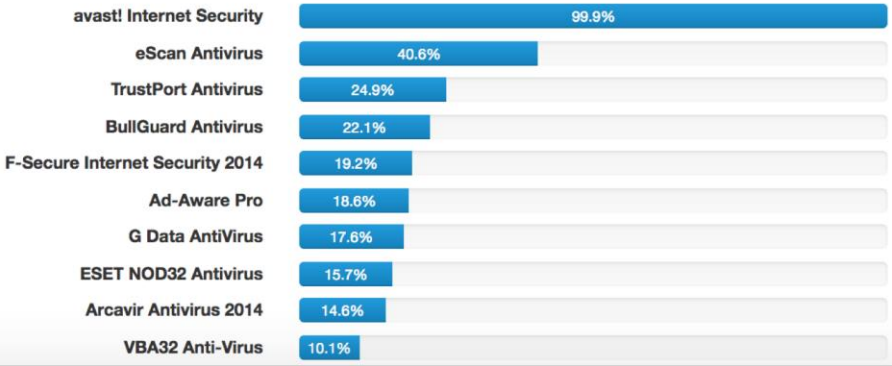
Clever API

Crafted API, giving wide scope when using server-side checks. More info..

Many great apps

Variety of clients, from simple CLI module, ending DLL library and plugin for OllyDBG.

TOP 10 Ranking Antiviruses



Amplifying signals through seeds

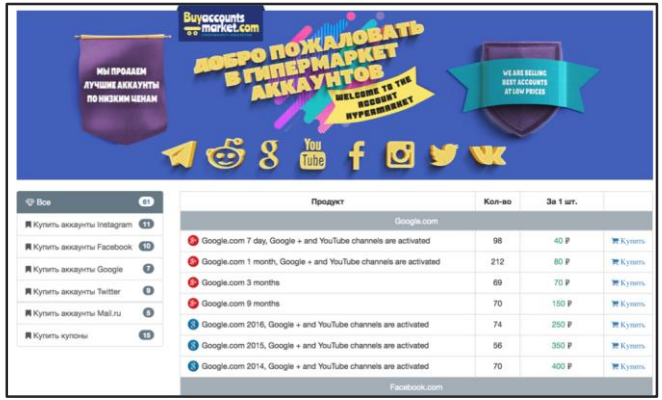
Pivot from viruscheckmate.com -> other crimeware sites

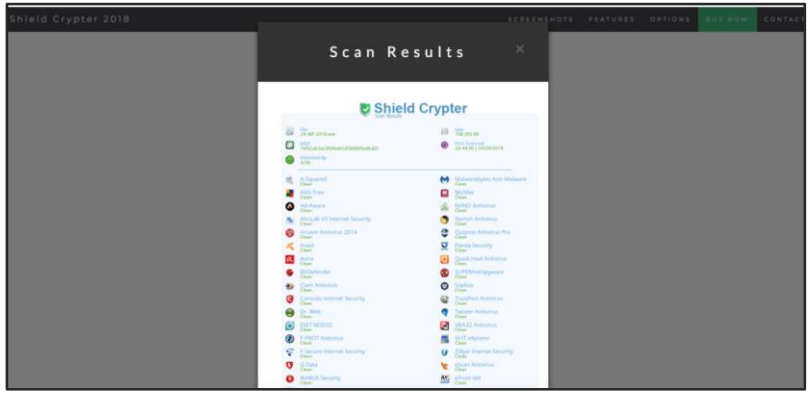
amplify.sh dom viruscheckmate 100 10 [degree = 100, 10 days]

ifud.ws

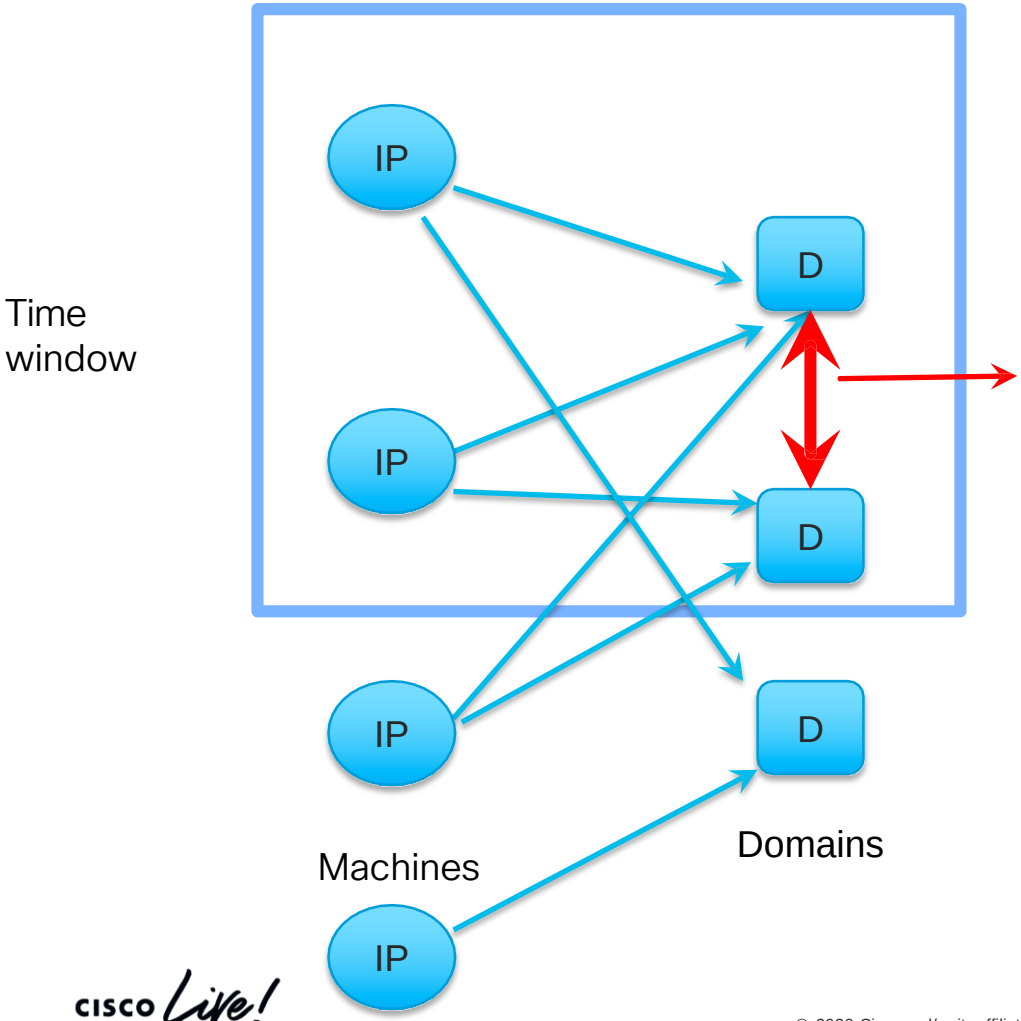
vkpro.biz
valid-vk.ru
hackway.s
u
buyaccs.or
g
mybot.su
buyaccounts-
market.com b-p.sale

shieldcrypter.com





Co-occurrences



- The closer in time, the higher the co-occurrence score
- The more clients exhibiting this behavior, the higher the score

Patended

Co-occurrences

- Domains having similar topic, e.g. security sites, hacking, carding sites
  - Visited by users with related interest
- Example: first.org

Co-occurrences

nakedsecurity.sophos.com (92.14) www.bleepingcomputer.com (7.86)

- Botnet CnC domains, e.g. DGAs
- Infection chains: compromised sites -> Exploit kit landing domains

Co-occurrences

- carderland.com – carding site
- izzvbczwk.info
- cashback.bazar

в связи с личными обстоятельствами.Предложения в лс админу

g3mz Dump Shop
Quality Dumps for cheap price!

registration | reference | Users | The calendar | Search | Messages for the day | All sections read | All sections read | Forum Guide

Members panel

Carding forum

Name Имя Remember?
Password Login Now!

Welcome to the Carding Forum.

If this is your first visit, be sure to check out the FAQ by clicking the link above. To post your messages you need to register . To start viewing messages, select the section.

Services - all about hosting, dumps, plastic cards and withdrawals.

Section	Last message	By	Posts
Sell CC + CVV (view: 4) Sell CC's + CVV only	Reload this Page & Luxe CC ... from Regedit 06:41 PM 18:41	19	20
Enroll, Accounts, Shops, SSN (browsing: 1) Enroll (COBs, Full info). Sell & Buy Accounts: Banks, PP, MB and more. Search SSN, DOB.	Having broken through Dob / SSN 700k + online from dobblack 06:24 PM 18:24	9	10
CashOut Services & Drops for Stuff (viewed: 2) ATM Any cashout. Exchange, purchase, electronic currency. Drops for stuff.	de and tr bank drop by avalanche 12:57 PM 12:57	17	18
Only dumps (Viewing: 1) Selling and cashout dumps only.	credit card copies with ... by skimmer 04:15 PM 16:15	1	12
Other services (browsing: 4) Credit card fraud for sale topical working order. Selling online stores for online carding.	Are You looking for easy way ... from R0yalCard3rs 10:41 AM 10:41	8	fifteen

carderland.com

INVESTIGATE

BACK TO TOP

Details for carderland.com

Classifier prediction: Severe

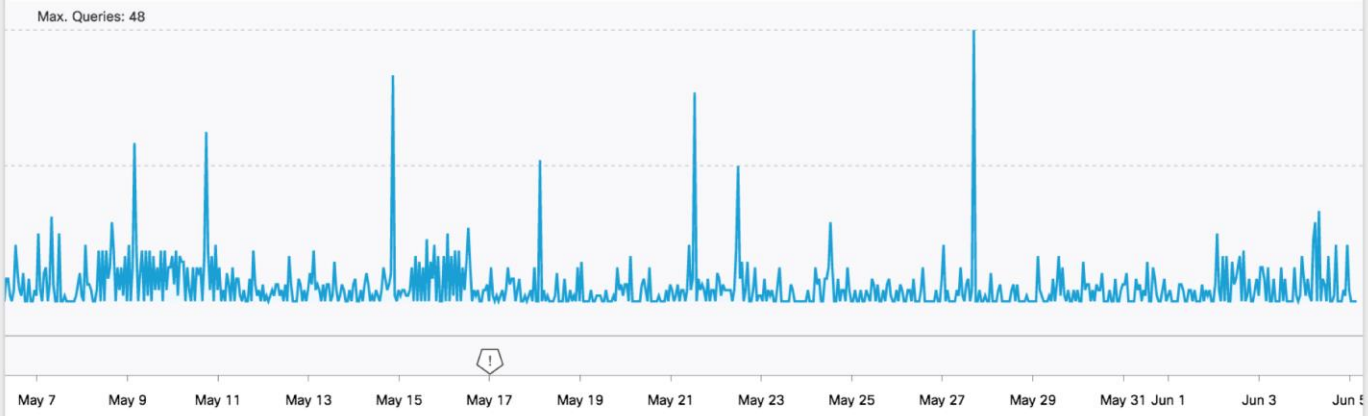
Umbrella Investigate Risk Score: 86

Timeline (Beta)

Current Content Category: None

DNS Queries | Domain Events | DNS Changes

May 6th, 2019 - Jun 5th, 2019



Event History

Security Categories | DNS Changes | Query History

Co-occurrences

darkmarket.li (67.62) blackforum.cc (32.38)

DarkMarket
теневой рынок

ВОССТАНОВЛЕНИЕ СИМ-КАРТ

Форумы | Что нового? | Гарант | ₽ Реклама | Арбитраж | Аттестация продавцов | Вход | Регистрация

Новые сообщения

Сейчас Ваши права ограничены!
Авторизуйтесь или зарегистрируйтесь, чтобы стать полноценным участником форума.

Запомните и не теряйте доступ к форуму.
Tor зеркало: DARKMARKETRITFZF.ONION

Co-occurrences

- carderland.com
- **izzvbczwk.info – Pykspa malware**
- cashback.bazar

izzvbczwk.info

INVESTIGATE

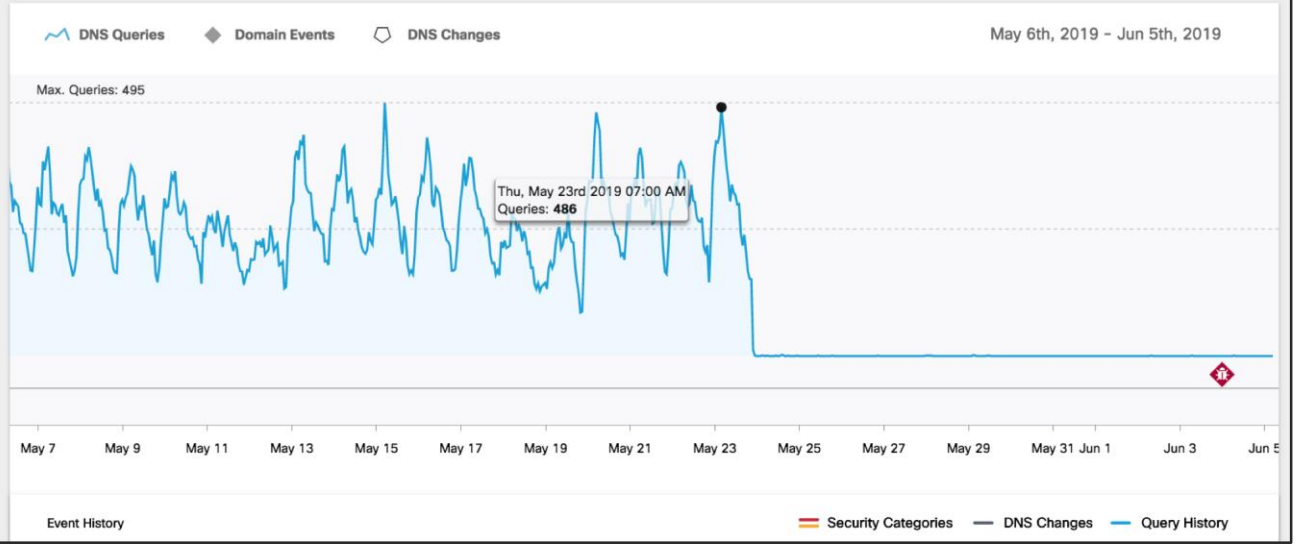
BACK TO TOP

Details for izzvbczwk.info

This domain may have been created using a domain generation algorithm (DGA).

Timeline (Beta)

Current Content Category: None



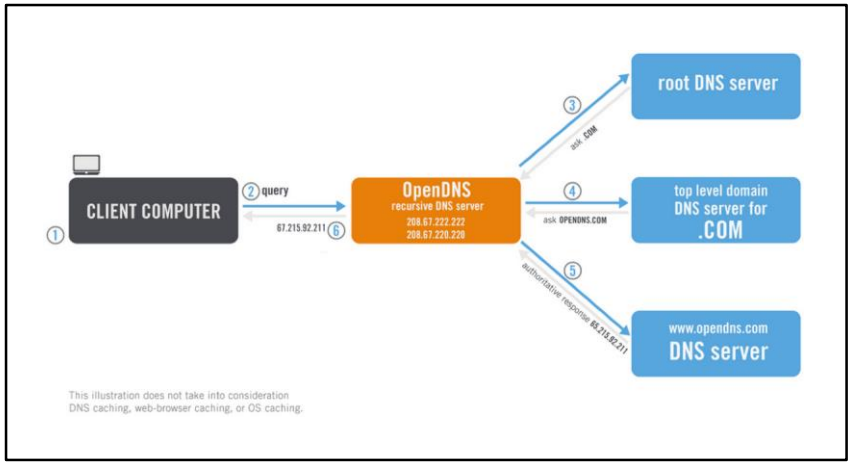
Co-occurrences

qjnsfustt.net (17) myjvxutyh.info (7) csmoggsiwq.com (5) lpfaxbnidlu.net (5) pwdcrccrp.net (5) exvphacahza.net (5) gogciiaoqk.org (4) jomougvg.net (4) rtmmielec.net (4) ruewwab.net (4) viuhdvad.net (4) vpbuasip.info (4) vwhytdhh.net (4) vwqtdpf.org (4) yssaauywyc.org (4) jxbcnouwlp.net (3) buqoisjet.org (3) cikxqa.net (3) dubkqfacwx.info (3) hgdpoyxyxwr.org (3) hjnqkq.info (3) leqpsol.info (3) pzydhzjjxyvn.info (3) zwegtahrnwj.info (3)

Co-occurrences

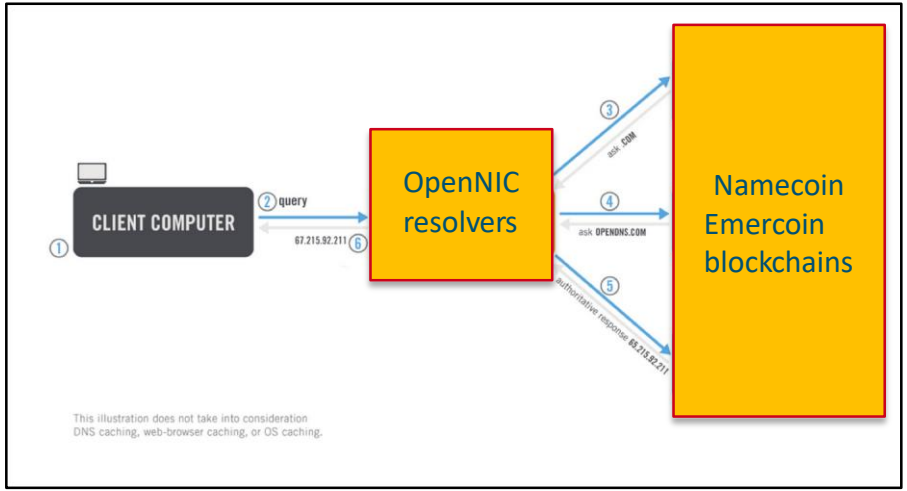
- carderland.com
- izzvbczwk.info
- cashback.bazar – carding site

Blockchain and DNS



- Blockchain DNS is even more decentralized than current DNS
- Does not depend on registrars, registries, root DNS servers, regular DNS hierarchy
- Namecoin and emercoin blockchains
- DNS managed by the p2p network of the underlying blockchain

- Mapping domain->hosting IPs is tamper-proof
- Countering censorship and domain take down



Namecoin (Symbol: N or **NMC**) is a cryptocurrency originally forked from bitcoin software. It is based on the code of bitcoin and uses the same proof-of-work algorithm. Like bitcoin, it is limited to 21 million coins.[2]

Unlike bitcoin, Namecoin can store data within its own blockchain transaction database. The original proposal for Namecoin called for Namecoin to insert data into bitcoin's blockchain directly. Anticipating scaling difficulties with this approach, a shared proof-of-work (POW) system was proposed to secure new cryptocurrencies with different use cases.

Namecoin's flagship use case is the censorship-resistant top level domain `.bit`, which is functionally similar to `.com` or `.net` domains but is independent of ICANN, the main governing body for domain names.[3]

Namecoin	
namecoin	
Denominations	
Plural	namecoins
Symbol	N
Ticker symbol	NMC
Subunits	
1/1000	millinamecoin

.bit

.bazar
.coin
.emc
.lib

OpenNIC Public Servers

Search

Tier1 | Tier2 | Ok: 75 | Err: 6 | Total: 81 | Log in

<ALL> AT AU CA CZ DE EC FI FR GB IN IT JP MD MX NL PT RO RU SE UK US

Anonymized logs
No logs kept
DNScrypt
Whitelisting
Blocklist

Hostname (Click for details)	IPv4	IPv6	Owner(s)	Added	Status
ns1.any.dns.opennic.glue	185.121.177.177	2a05:dfc7:5::53	Fusl	2016-May-24	Pass
ns3.any.dns.opennic.glue	169.239.202.202	2a05:dfc7:5353::53	Fusl	2016-May-30	Pass
ns1.vie.at.dns.opennic.glue	5.132.191.104	2a03:3180:f:7::dfc6:cfb7	user42	2017-Dec-07	Pass
ns1.au.dns.opennic.glue *Sponsored by Parrot Linux*	13.239.157.177	2400:6180:100:d0::842:4001	palinuro	2019-Jan-31	Pass
ns5.nsw.au.dns.opennic.glue	207.148.83.241	2001:19f0:5801:11:5400:ff:fe2d:7724	connorw600 lchimp	2016-Jul-18	Pass
ns1.ca.dns.opennic.glue *Sponsored by Parrot Linux*	165.227.40.43	2604:a880:cad:d0::5ed:5001	palinuro	2019-Feb-02	Pass
ns3.ca.dns.opennic.glue	142.4.204.111	2607:5300:120:a8a:142:4:204:111	luggs	2014-Mar-08	Pass
ns4.ca.dns.opennic.glue	142.4.205.47	2607:5300:120:a8a:142:4:205:47	luggs	2014-Mar-08	Pass

dig @185.121.177.177 1pass.bazar

Co-occurrences

- carderland.com
- izzvbczwk.info
- cashback.bazar

Co-occurrences

cashb3ozrhhumfby.onion (100.00)

CashBack | Inscription

cashb3ozrhhumfby.onion/inscription

Search

CASHBACK v2.0

Accèdez a des milliers de cartes bancaire et de logs en tout genre.

Connexion **Inscription**

Nom d'utilisateur

Mot de passe

Jabber e-mail

8 + 5 =

Valider

TOR LINK **http://cashb3ozrhhumfby.onion**

3 Classes of ML algos to solve threat detection

NLP/Clustering

- DNS tunneling
- Malvertising
- Phishing

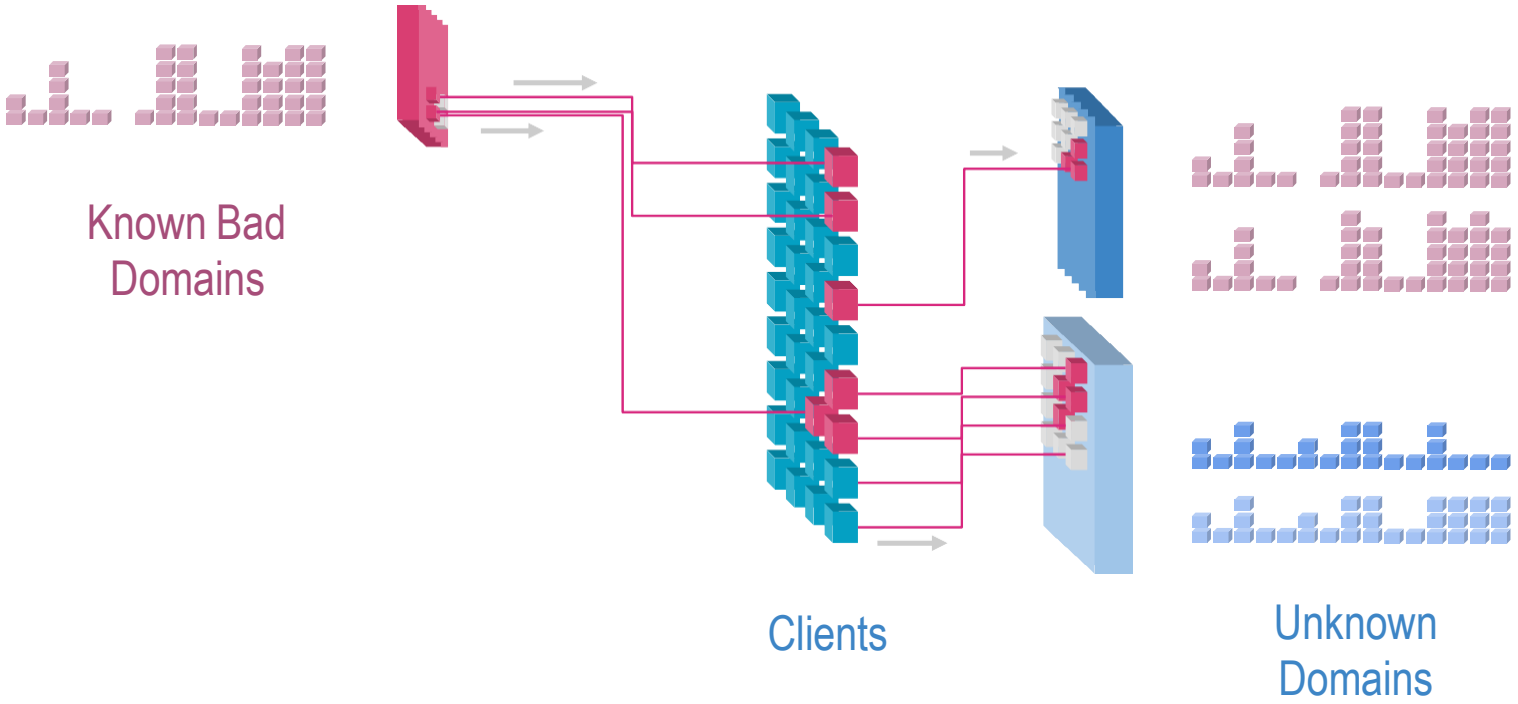
Graph analysis

- Cybercrime goods and services
- DGA botnets

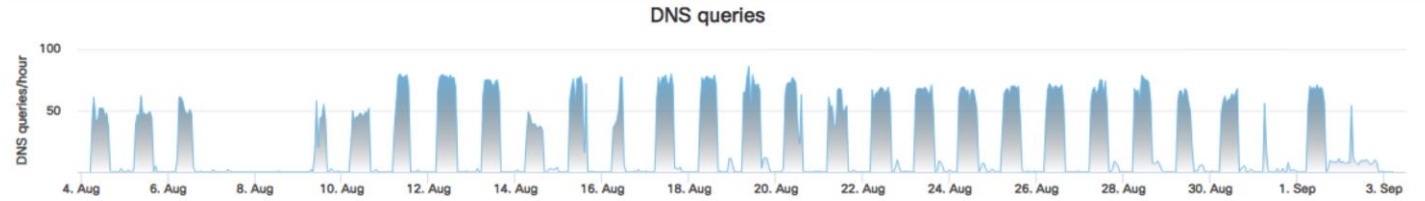
Anomaly detection

- Cryptomining pools
- Crimeware

Bipartite Graph – subgraph clustering of query volume using LSH



Details for gatyzyw.com



Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km

Requester Distribution

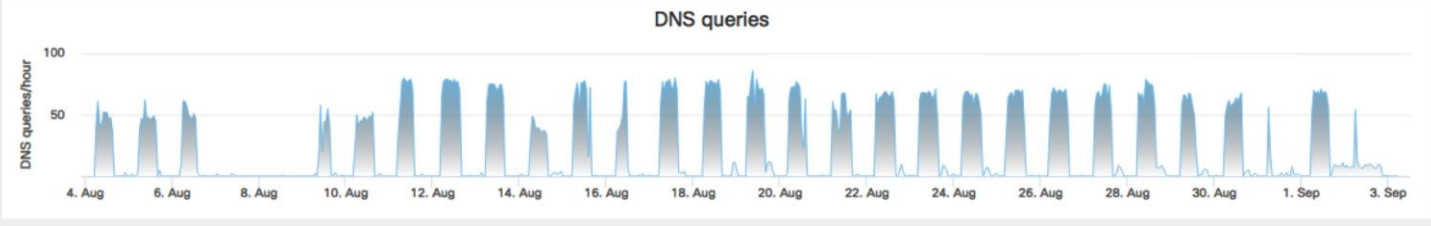
COUNTRY	PERCENTAGE
Spain	50.00%
Russian Federation	50.00%

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	4c3e964ba22e333412b54c2b5b791e2b0a71c99880f5cb9febc21bf6b89da440	Win.Trojan.Banker
100	ab9353bc3a3bc1a2f6fd9c3eb781b46232e84b09c61e1093f66d5c23c3b4172e	Win.Trojan.Banker
100	68a4f805565b98bf0ba681ed8082baed15f32ec07aea4ad8020589272873f52a	Win.Trojan.Banker

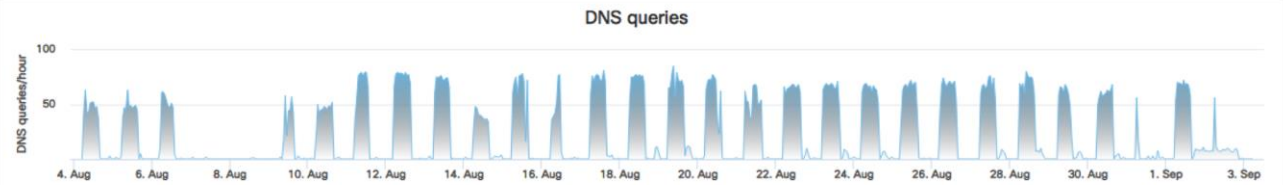
Details for gatyzyw.com



Co-occurrences

qedysol.com (64.11) pumyleg.com (13.01) lymylen.com (12.38) galynus.com (10.50)

Details for qedysol.com

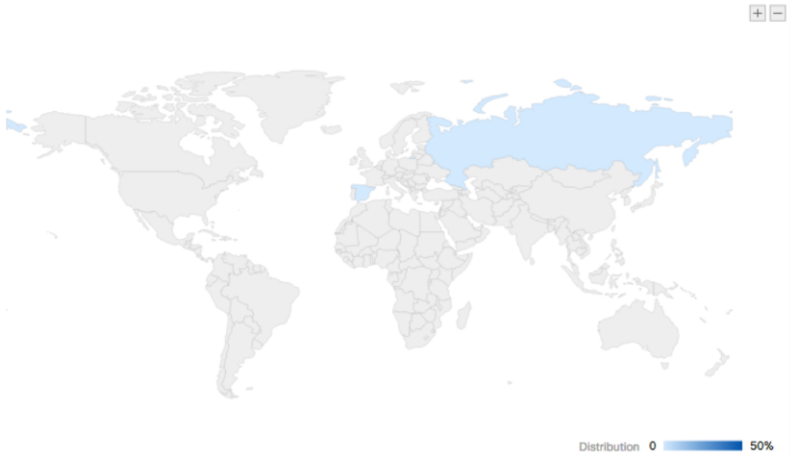


Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km

Requester Distribution

COUNTRY	PERCENTAGE
Spain	50.00%
Russian Federation	50.00%

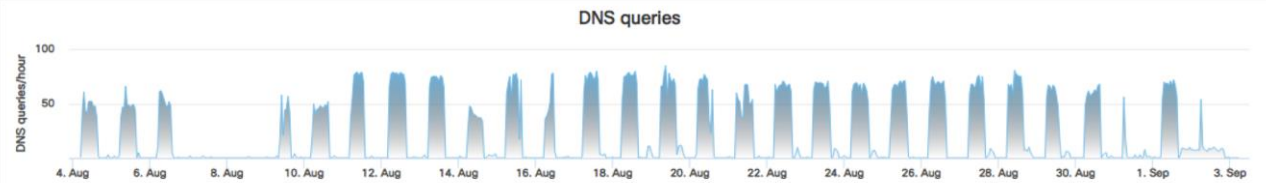


Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	4c3e964ba22e333412b54c2b5b791e2b0a71c99880f5cb9febc21bf6b89da440	Win.Trojan.Banker
100	ab9353bc3a3bc1a2f6fd9c3eb781b46232e84b09c61e1093f66d5c23c3b4172e	Win.Trojan.Banker
100	68a4f805565b98bf0ba681ed8082baed15f32ec07aea4ad8020589272873f52a	Win.Trojan.Banker

Details for pumyleg.com

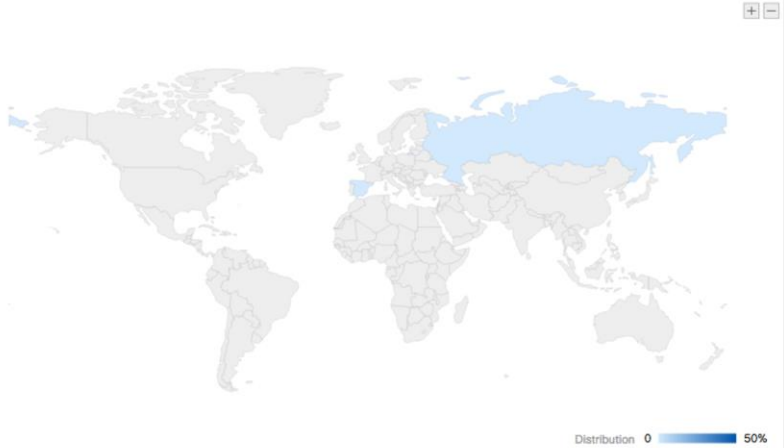


Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km

Requester Distribution

COUNTRY	PERCENTAGE
Spain	50.00%
Russian Federation	50.00%

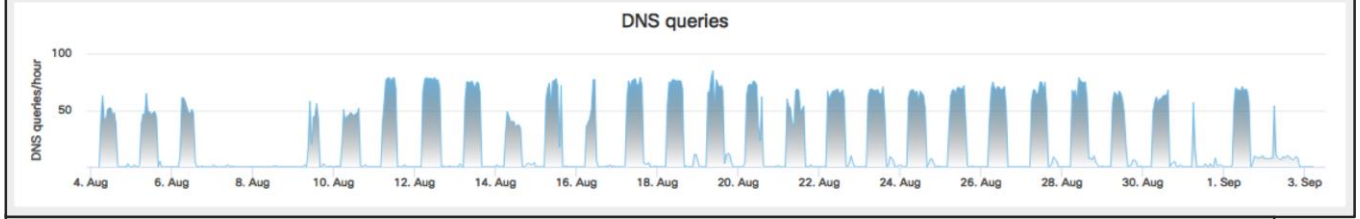


Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	4c3e964ba22e333412b54c2b5b791e2b0a71c99880f5cb9febc21bf6b89da440	Win.Trojan.Banker
100	ab9353bc3a3bc1a2f6fd9c3eb781b46232e84b09c61e1093f66d5c23c3b4172e	Win.Trojan.Banker
100	68a4f805565b98bf0ba681ed8082baed15f32ec07aea4ad8020589272873f52a	Win.Trojan.Banker

Details for lymylen.com



Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km

Requester Distribution

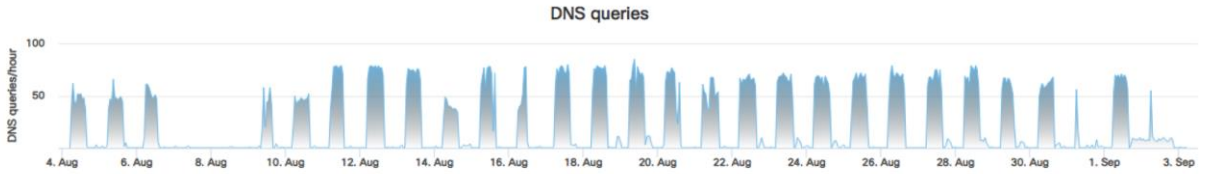
COUNTRY	PERCENTAGE
Russian Federation	100.00%

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	4c3e964ba22e333412b54c2b5b791e2b0a71c99880f5cb9febc21bf6b89da440	Win.Trojan.Banker
100	ab9353bc3a3bc1a2f6fd9c3eb781b46232e84b09c61e1093f66d5c23c3b4172e	Win.Trojan.Banker
100	68a4f805565b98bf0ba681ed8082baed15f32ec07aea4ad8020589272873f52a	Win.Trojan.Banker

Details for galynus.com



Host

IP Count	0
Geo Distance (sum, mean)	0, 0 km

Requester Distribution

COUNTRY	PERCENTAGE
Russian Federation	66.67%
Spain	33.33%

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	4c3e964ba22e333412b54c2b5b791e2b0a71c99880f5cb9febc21bf6b89da440	Win.Trojan.Banker
100	ab9353bc3a3bc1a2f6fd9c3eb781b46232e84b09c61e1093f66d5c23c3b4172e	Win.Trojan.Banker
100	68a4f805565b98bf0ba681ed8082baed15f32ec07aea4ad8020589272873f52a	Win.Trojan.Banker

3 Classes of ML algos to solve threat detection

NLP/Clustering

- DNS tunneling
- Malvertising
- Phishing

Graph analysis

- Cybercrime goods and services
- DGA botnets

Anomaly detection

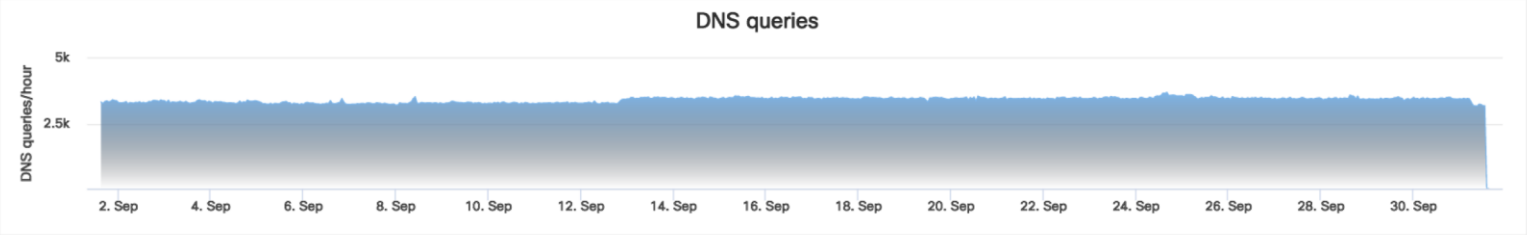
- Cryptomining pools
- Crimeware

SEARCH PATTERN SEARCH

moneromineers.net

INVESTIGATE

Google VirusTotal

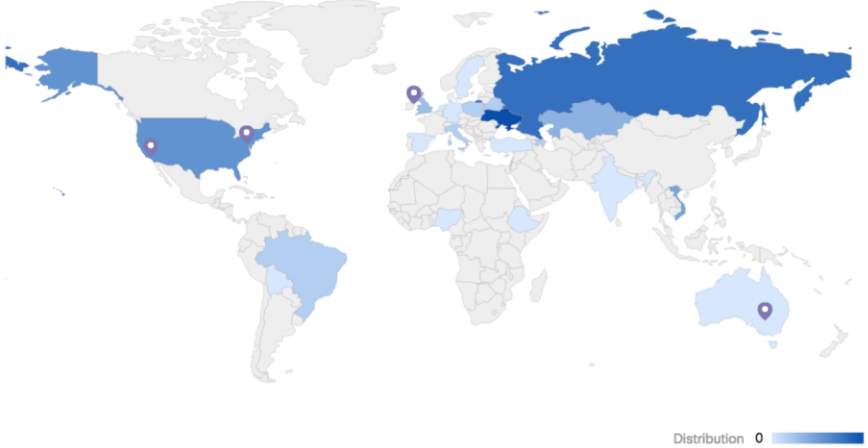


Host

IP Count	4
Geo Distance (sum, mean)	24670, 6167 km
Registrant Country	SC

Requester Distribution

COUNTRY	PERCENTAGE
Ukraine	44.63%
Russian Federation	18.18%
United States of America	7.44%
Viet Nam	4.96%
Kazakhstan	3.31%



Anomaly detection with global traffic analysis

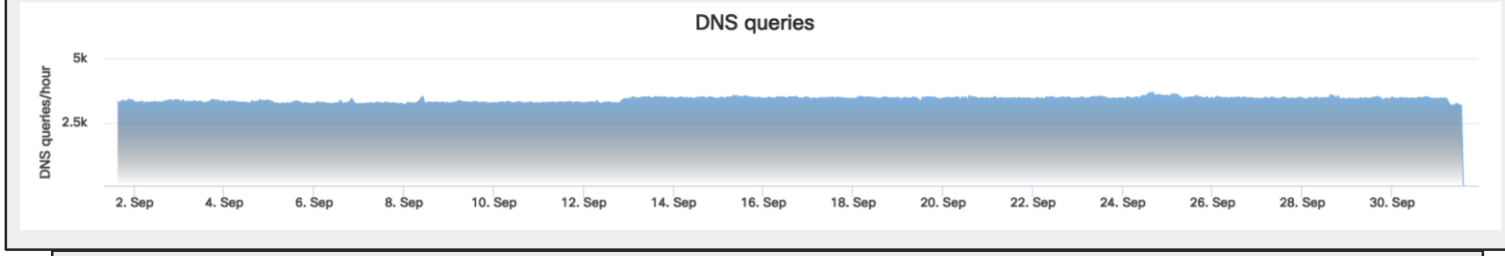
- Track domains with consistent high volume traffic
- Coefficient of variation: standard deviation / mean
- Track when it’s close to zero

SEARCH PATTERN SEARCH

moneromineers.net

INVESTIGATE

Google VirusTotal

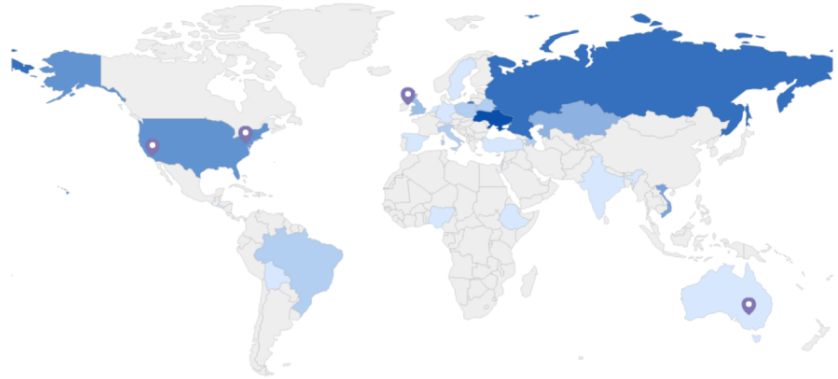


Host

IP Count	4
Geo Distance (sum, mean)	24670, 6167 km
Registrant Country	SC

Requester Distribution

COUNTRY	PERCENTAGE
Ukraine	44.63%
Russian Federation	18.18%
United States of America	7.44%
Viet Nam	4.96%
Kazakhstan	3.31%



Associated malware samples and co-occurrences

Associated Samples

POWERED BY CISCO AMP THREAT GRID

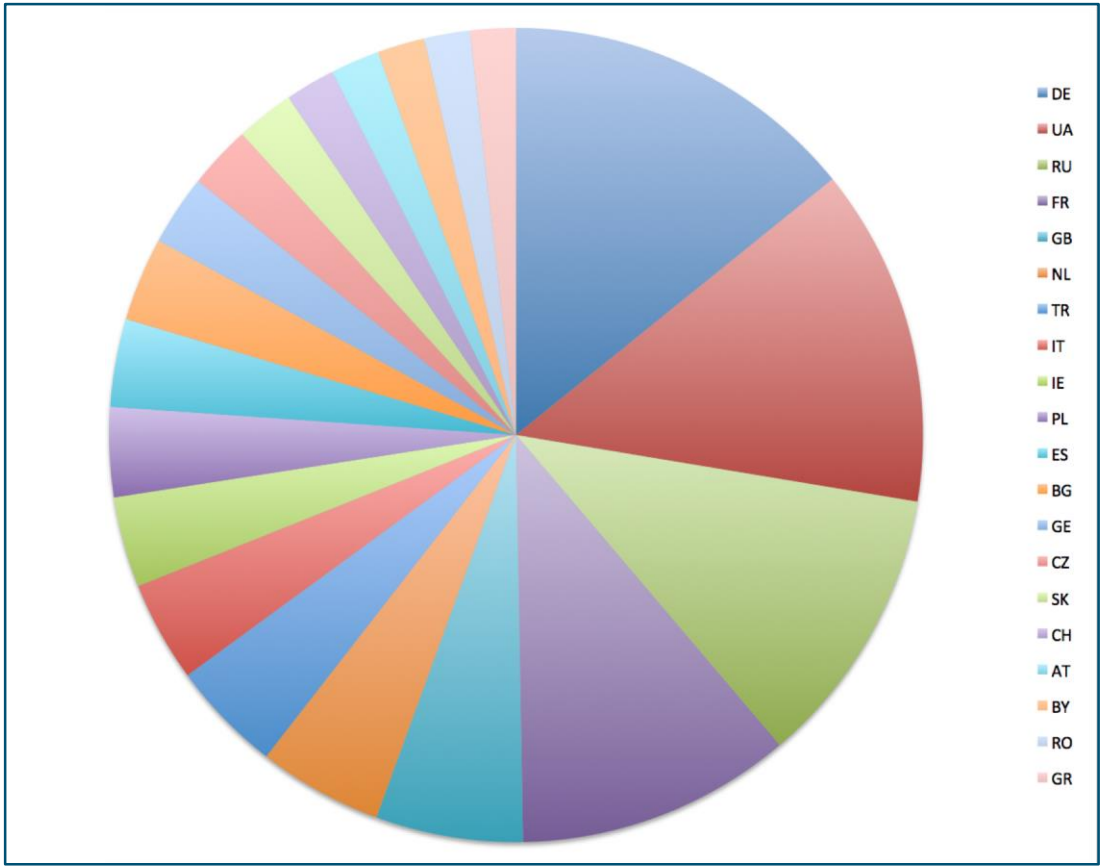
Threat Score	SHA256 Signature	AV Result
95	ebc2f05c63f6f176fdcb1d050bdf3c52feb3dc894f5cf4dc808d25eff36ac56b	
95	8c5a7371a81c08222fc81fc8ea0744eee9a317f9ce1c785d2bf9439f9ab5bcdf	
95	d6dcb53f95497e2062023a6c60c731d7dd417e7ac2f995b1cfbaf2c294d2f63d	
95	2046cccfa89592d4e8b22957ad865ccc28da7eaee8ef22bc51a57036d862e929	
95	16c1e2f7f04dd7ac7e4cc9ddfce9f23cd1109e1c72a1f684ec546618b84594af	
95	6c375b9779f8b8747c2db50b0c60360f6ff16f955594fba01f1a194e71c2dc01	

1 - 6 of 6

Co-occurrences

cryptonotepool.org.uk (8) pool.cryptoescrow.eu (5) monero.crypto-pool.fr (4) xmr.coinmine.pl (4) mine.moneropool.org (3) monero.farm (3) pool.minexmr.com (3) xmr.farm (3)

- Top European countries communicating with cryptomining pools



3 Classes of ML algos to solve threat detection

NLP/Clustering

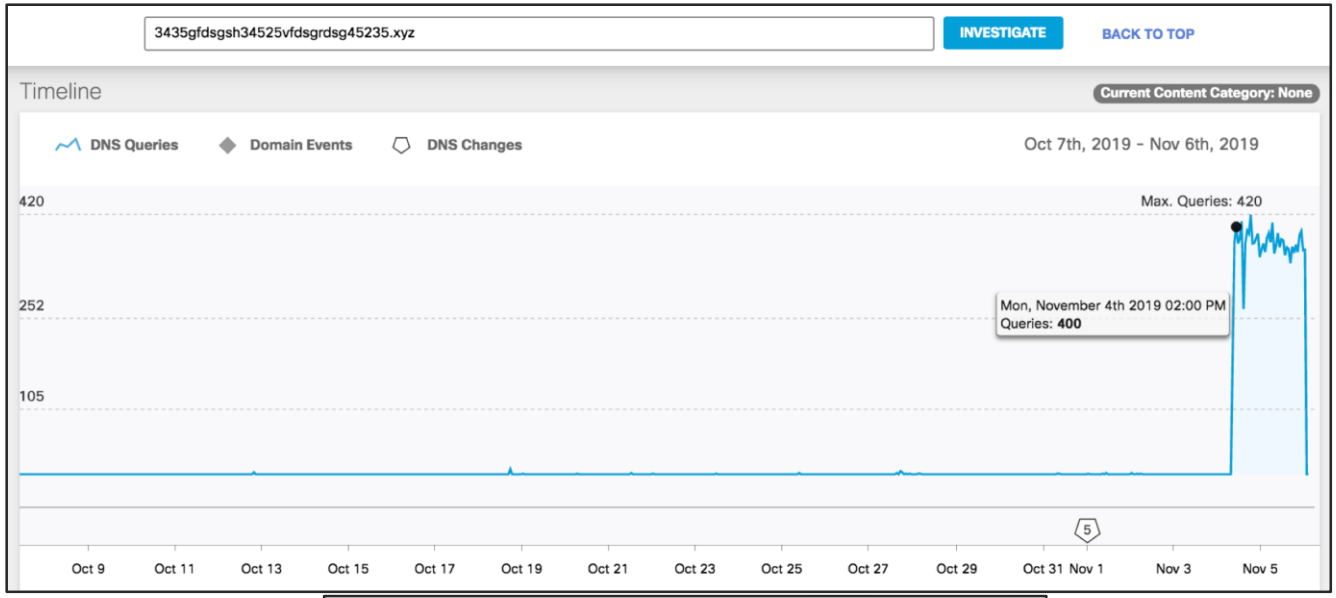
- DNS tunneling
- Malvertising
- Phishing

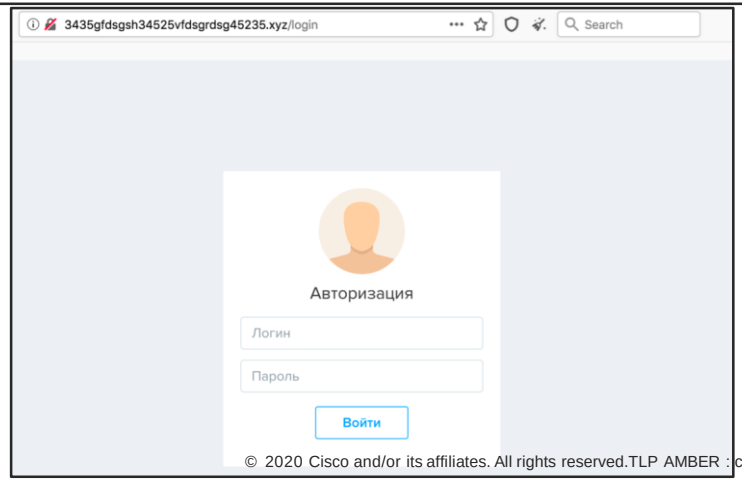
Graph analysis

- Cybercrime goods and services
- DGA botnets

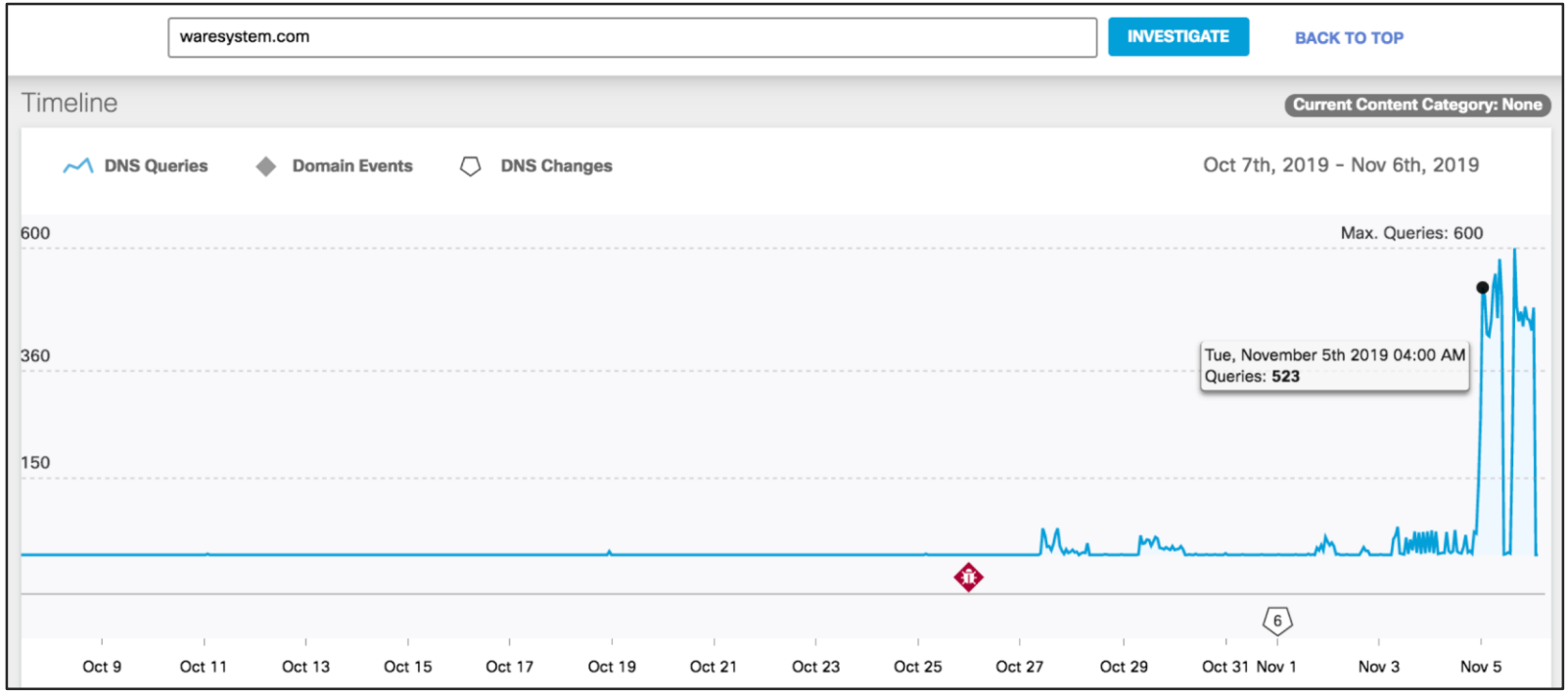
Anomaly detection

- Cryptomining pools
- Crimeware

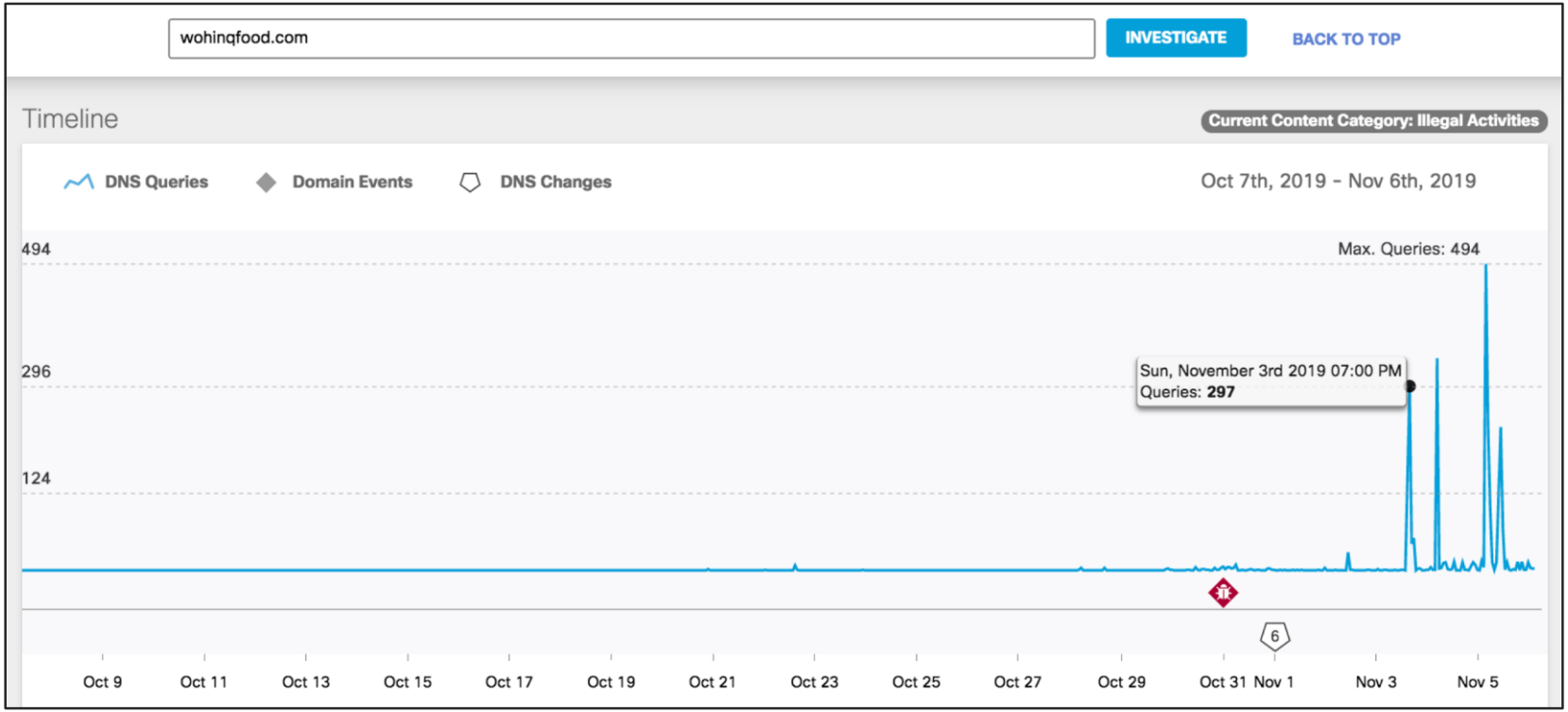




Predator the Thief



AZORult



Lokibot

Anomaly detection with global traffic analysis

- Identify threats such as malware panels, malware C2s, ransomware, malspam, phishing domains from recursive DNS traffic
- Observation: these threat domains always show a spike in traffic
- Examine traffic logs for possible signals

Recursive DNS features

Domain	QTYPE	RCODE	Resolvers	# of unique IPs
	1 – A 15 – MX 28 – AAAA 16 – TXT 99 – SPF 255 – ANY	0 Resolving	List of resolvers	

Taxonomy of DNS features

Assigned

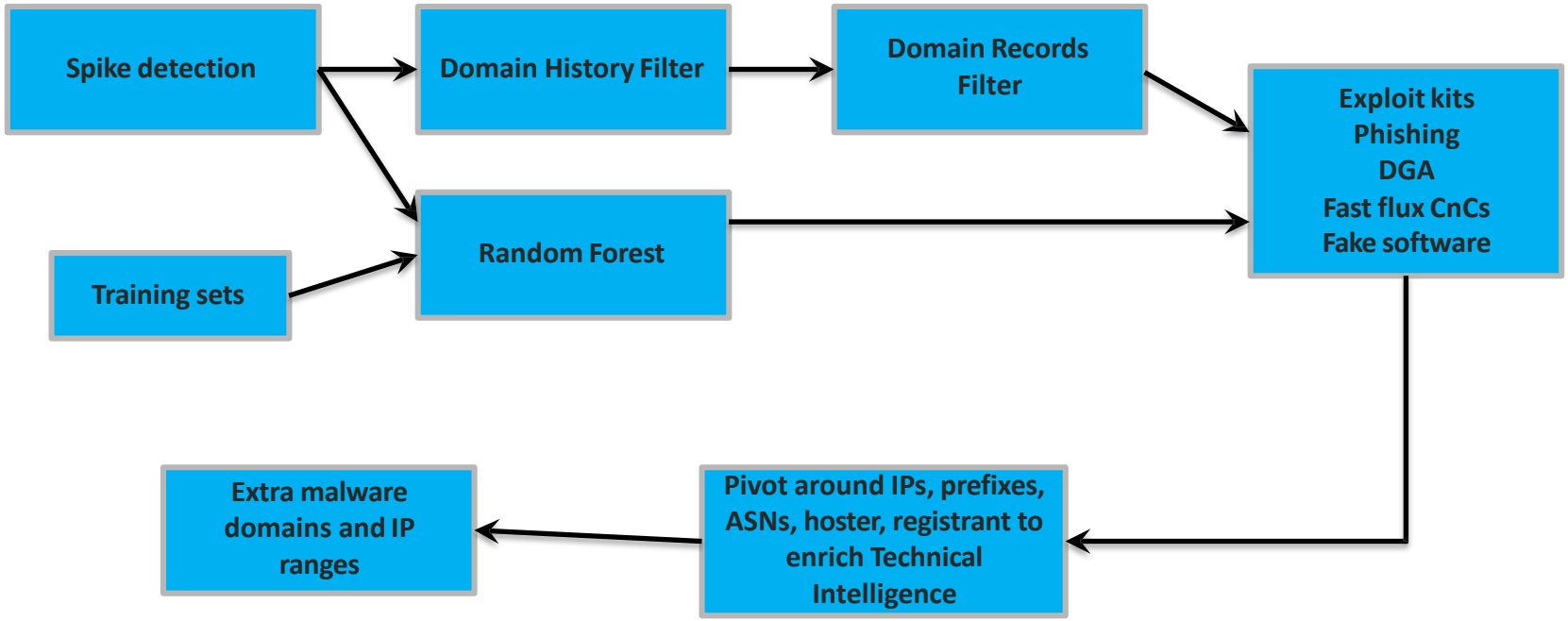
- Lexical
- DGA setup
- Hosting
- Registration

Inherent

- DNS query trends
- Diversity of clients across geography and IP space
- DNS query volume
- Query types
- Number of querying IPs
- Distribution of queries across resolvers

Harder to obfuscate and change by actors at global scale

Spike Detection Pipeline



Patended

Detected Threats

Exploit kits

DGA

Phishing

Malware C2s

Ransomware

Takeaways

Dealing with large scale threat intel problems, you need to:

- Know your requirements: what are you looking for?
- Know what to collect
- Know how to store and process the data at scale
- Know what analysis to apply: human or machine based at scale or a combination
- Before applying AI/ML, know your data, problem and features
- What is your final product: discrete IOCs, or trends and TTPs

Our Related Work

- FIRST 2018 https://www.first.org/resources/papers/conf2018/Mahjoub-Dhia_FIRST_20180712.pdf
- Hack in the Box 2018 https://youtu.be/co2cvi_5Flc
- SANS CTI Summit 2018 https://www.sans.org/summit-archives/file/summit-archive-1517343456.pdf
- Flocon 2018 https://schd.ws/hosted_files/flocon2018/d7/2.%20FloCon%202018_.pdf
- https://schd.ws/hosted_files/flocon2018/16/2.%20Flocon_2018_Thomas_Dhia_Jan_10.pdf
- Virus Bulletin 2017 https://www.youtube.com/watch?v=sbzvZ8ChTiU
- Defcon 2017 https://www.youtube.com/watch?v=AbJCOVLQbjs
- Black Hat 2017 https://www.youtube.com/watch?v=PGTTRN6Vs-Y&feature=youtu.be
- Usenix Enigma 2017 https://www.youtube.com/watch?v=ep2gHQgjYTs&t=818s
- 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=UG4ZUaWDXSs

Thank you

Dhia Mahjoub, dmahjoub@cisco.com,
@DhiaLite

Acknowledgements

David Rodriguez
Thomas Mathew
Matt Foley
Scott Sitar
Jingchuan Chen

CISCO

You make **possible**