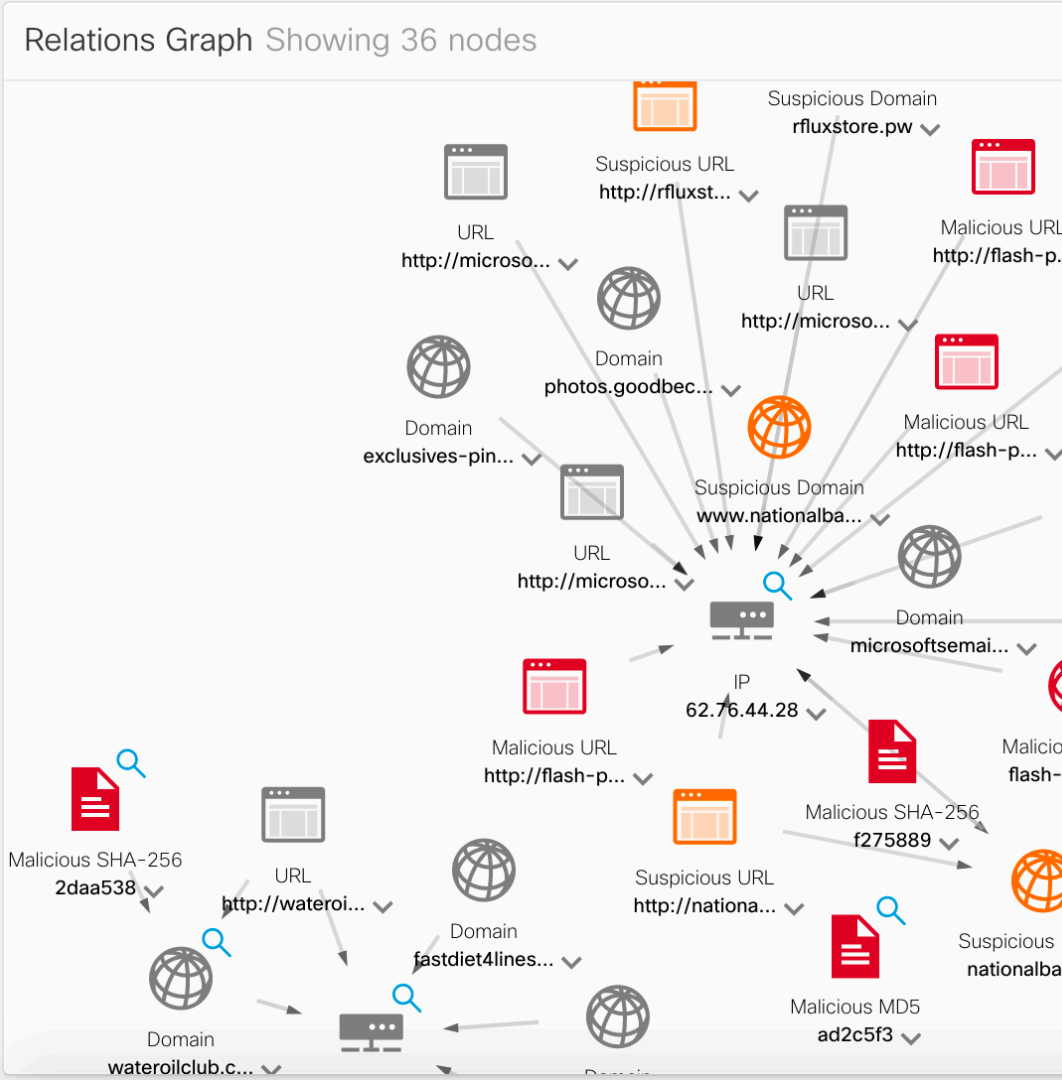
Типовые use case банковского SOC.

Что мы должны мониторить обязательно?

Руслан Иванов
Старший технический консультант по информационной безопасности
ruivanov@cisco.com

Типовые use case банковского SOC.

Что мы должны мониторить обязательно?



Use case для DNS-активности (пример)

1. Молодой (менее 7 дней) или недавно зарегистрированный домен
2. Имя не в списке Alexa
3. Странный или длинный домен второго уровня
4. Шестнадцатеричное имя домена
5. Энтропия символов в названии домена
6. Трафик к внешнему IP без запроса DNS
7. Запросы с длинными TXT записями
8. TXT без записи типа A
9. Запросы к динамическим DNS-провайдерам
10. Взаимодействие с вредоносными TLD

Типовые use case банковского SOC. Что мы должны мониторить обязательно?

Базовый уровень: сбор сведений об атакующих доменах:

- Собрать достаточно данных для принятия решения о блокировке или постановке под мониторинг;
- Данные должны проходить перекрёстную проверку для снижения вероятности блокировки или пропуска атаки из-за ошибок первого или второго рода;
- Данные можно использовать для ретроспективного анализа

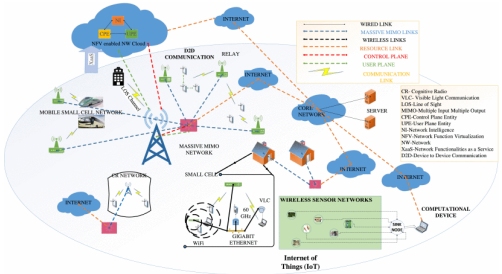
Сбор сведений об атакующих доменах

Данные из журналов прокси-серверов, межсетевых экранов, маршрутизаторов, почтовых шлюзов и серверов:

- Синхронизированная метка времени события
- Индикаторы, на основе которых можно будет создать индикаторы компрометации, такие как:
  - ASN
  - IP
  - Доменное имя/зонная информация
  - FQDN
  - URL
  - Перенаправления на другие ресурсы и т.д.

DNS основа критической инфраструктуры Интернет

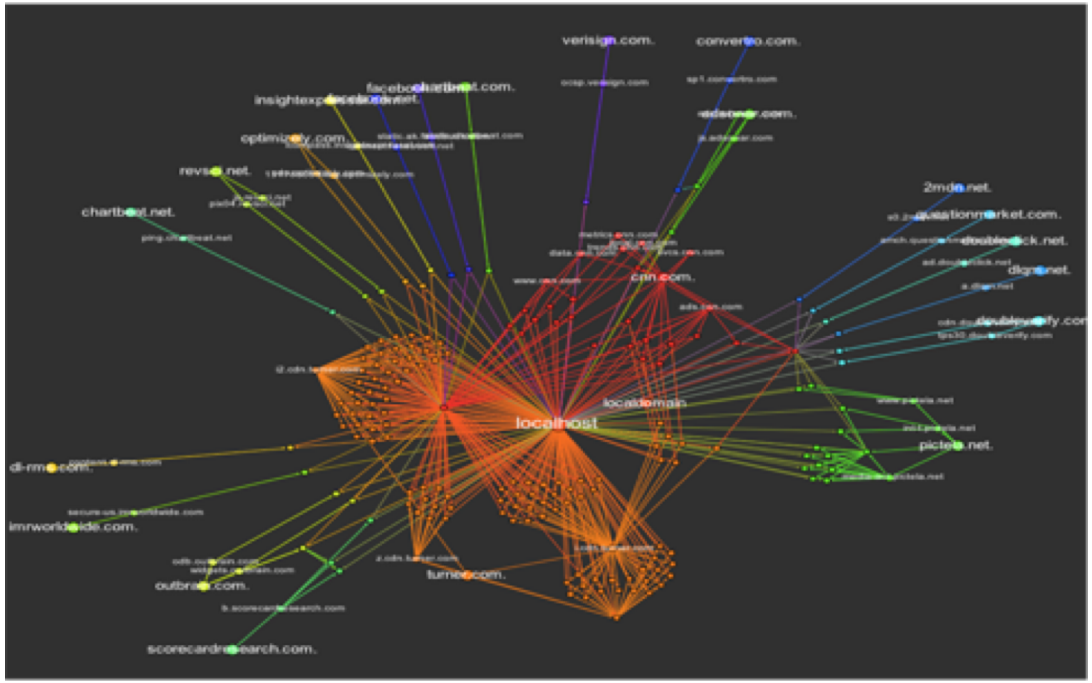
Все возможные устройства



Любые сетевые архитектуры

Все операционные системы

Что происходит, когда мы посещаем всего один сайт?



68%

организаций не мониторят DNS-запросы

Пример индикаторов из реальной фишинговой рассылки

- nationalbank[.]bz

Пример индикаторов из реальной фишинговой рассылки

Фишинг – nationalbank[.]bz

Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Ruslan Ivanov

New Investigation | Assign to Incident | Snapshots ... | Automatic Layout

Investigation 1 of 1 enrichments complete

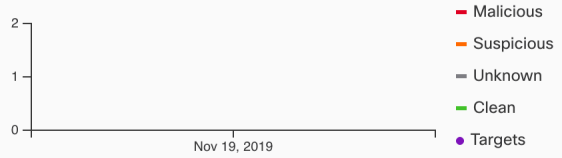
nationalbank[.]bz

Investigate | Clear | Reset | What can I search for?

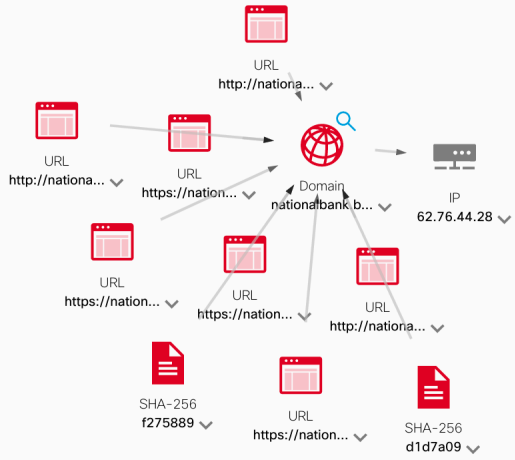
Sightings Timeline

My Environment | Global

0 Sightings in My Environment



Relations Graph Showing 11 nodes



Observables

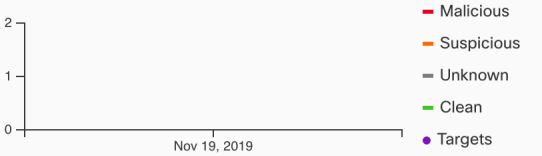
List View

nationalbank.bz

Malicious Domain

My Environment | Global

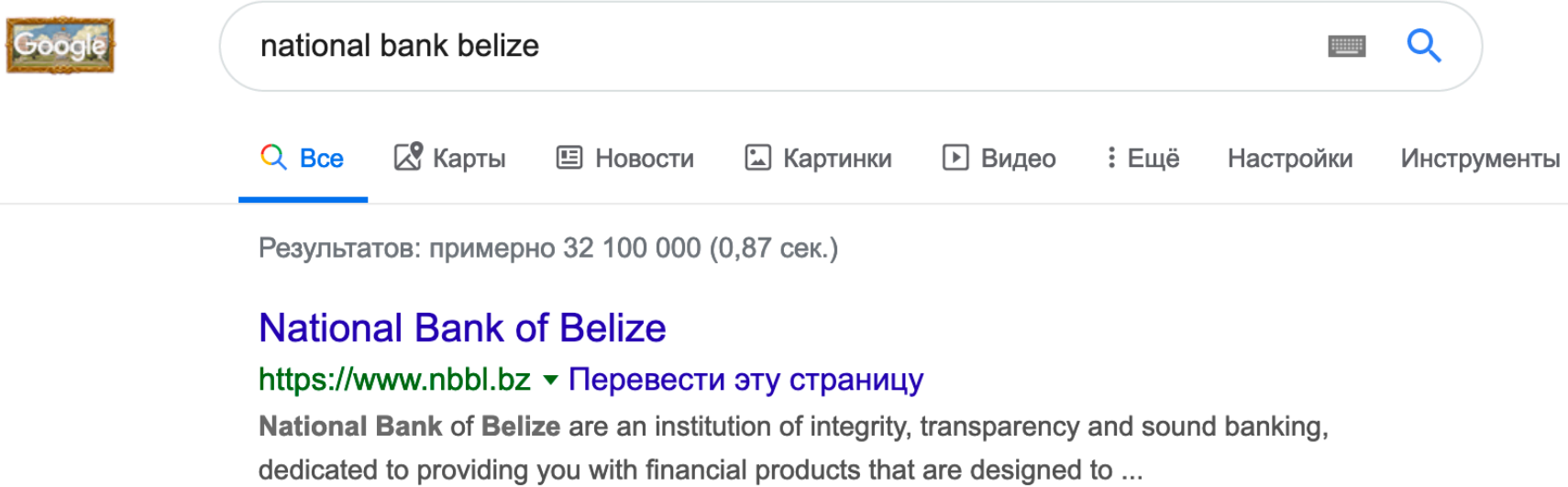
0 Sightings in My Environment



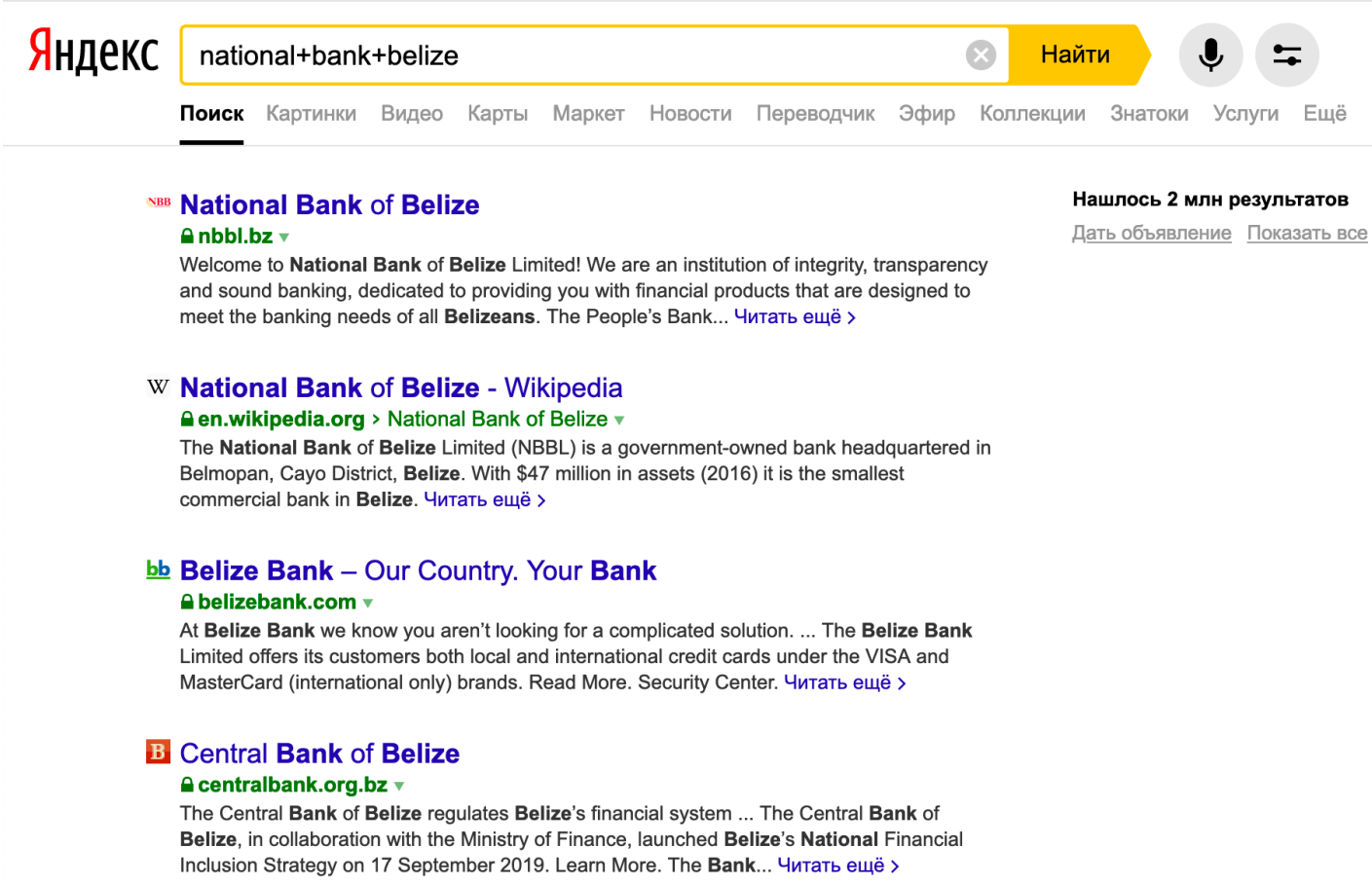
Judgements (2) | Verdicts (1) | Sightings (3)

Module	Observable	Disposition	Reason
Umbrella	DOMAIN: nationalbank.bz	Malicious	Poor Cisco Umbrella reputation sta
Talos Intelligence	DOMAIN: nationalbank.bz	Malicious	Poor Talos Intelligence reputation

Фишинг – nationalbank[.]bz



Фишинг – nationalbank[.]bz



Investigate

SEARCH PATTERN SEARCH

nationalbank.bz

INVESTIGATE

Google VirusTotal

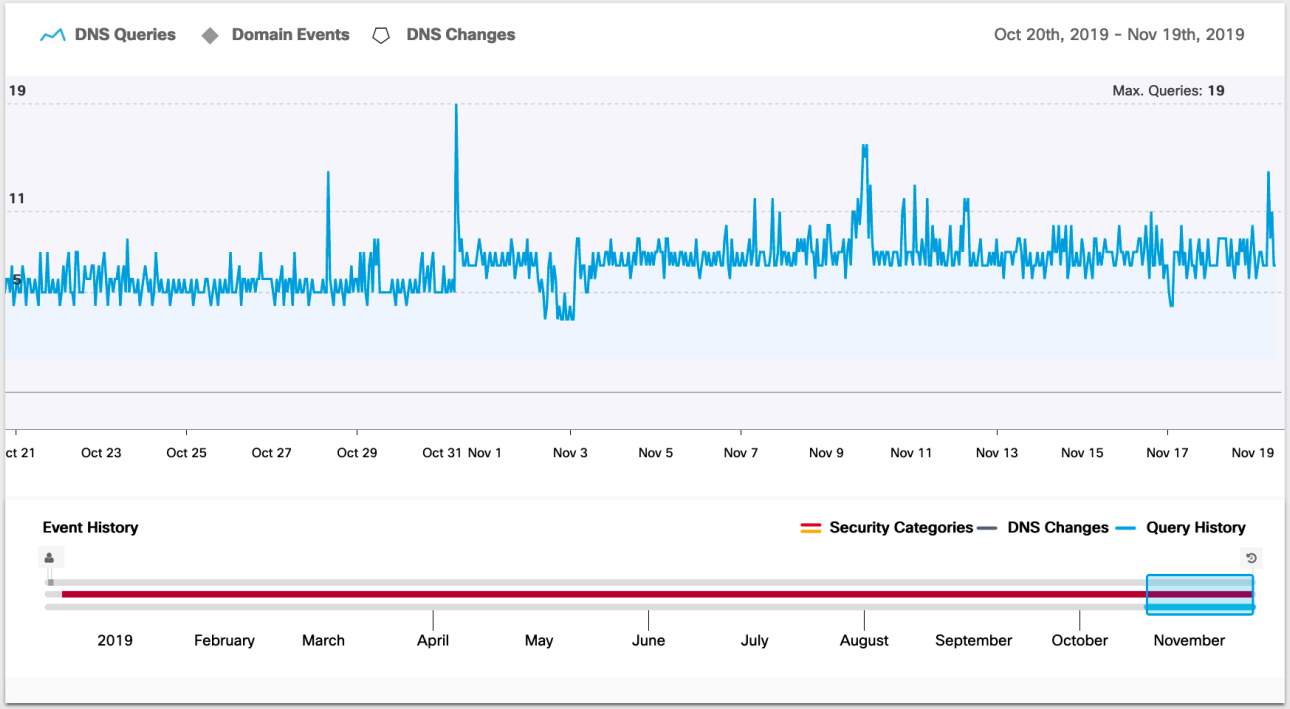
Details for nationalbank.bz

This domain is currently in the Umbrella block list.

Umbrella Investigate Risk Score: 100

Timeline

Current Content Category: None



nationalbank.bz

INVESTIGATE

BACK TO TOP

Nameserver	Associated Domains	Last Observed
ns1.suspended-domain.com	Greater than 500 Total - At least 75 malicious	Current
ns2.suspended-domain.com	Greater than 500 Total - At least 75 malicious	Current

Showing 2 of 2 Results

Show more WHOIS data

Host

IP Count	1
Geo Distance (sum, mean)	0, 0 km
Registrant Country	AU

Requester Distribution

COUNTRY	PERCENTAGE
Russian Federation	66.67%
United States	33.33%

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
81	fe5135ce1928f613e2b0500eadbd588e9ead84feb5fd377e4b03284f9515c31a	

1 - 1 of 1

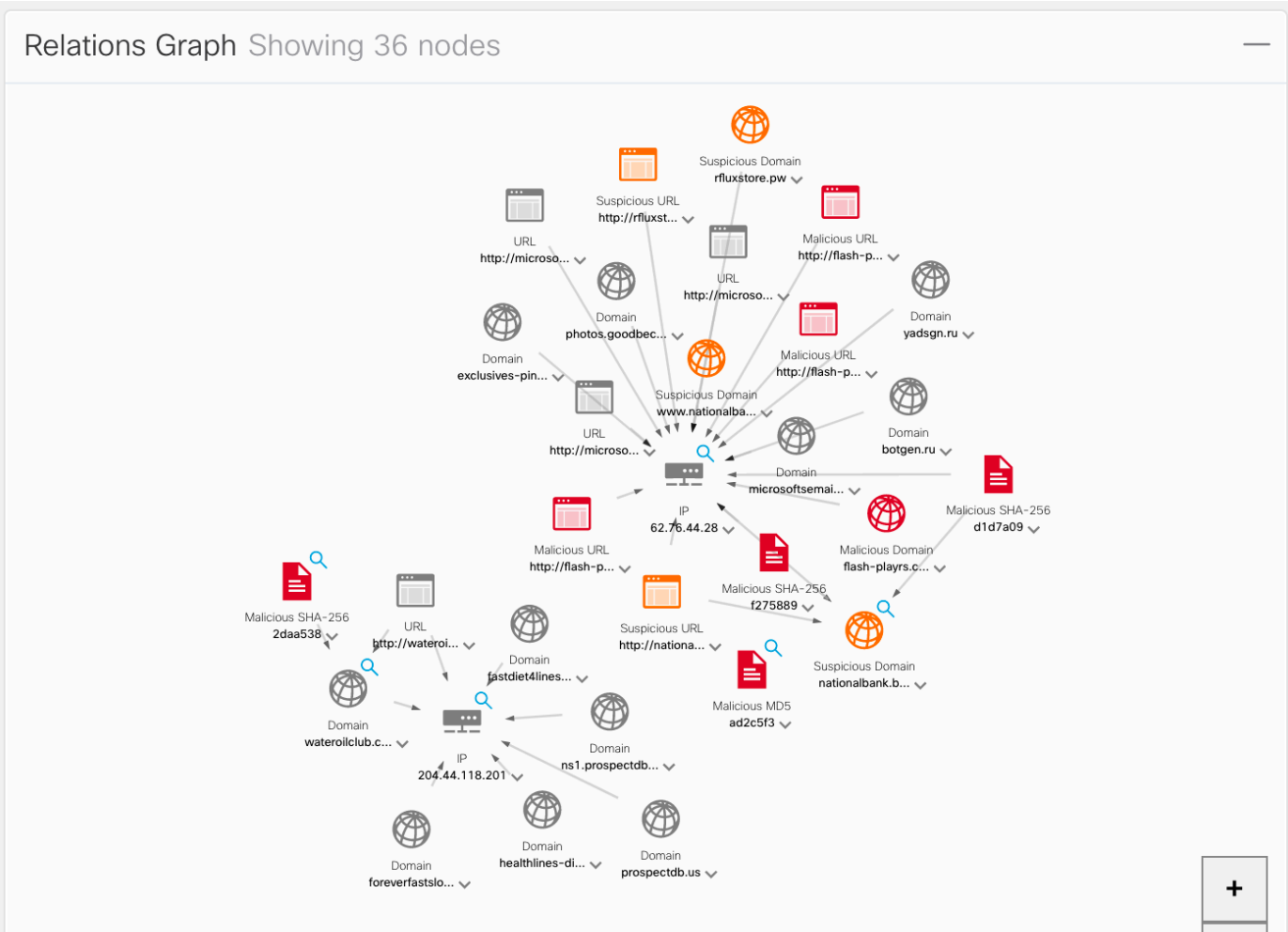
Типовые use case банковского SOC. Что вы должны мониторить обязательно?

- средний уровень: раскрытие инфраструктуры злоумышленника (с одного домена или по e-mail владельца) для проактивного внесения в черные списки и мониторинга того, что еще может произойти в будущем:

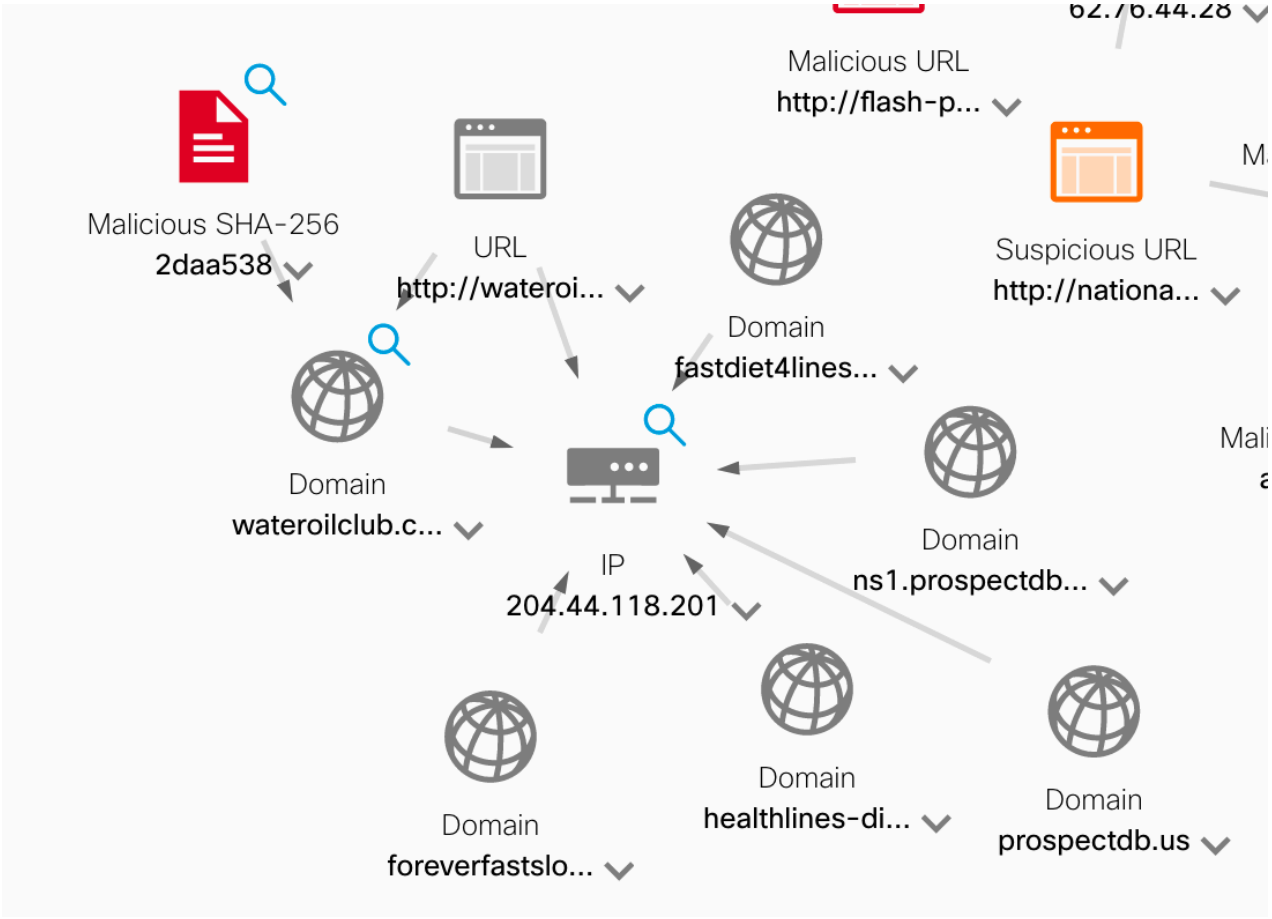
Выявленные индикаторы из фишинговой рассылки

- nationalbank[.]bz
- 62.76.44[.]28
- ad2c5f31e65b8710c8230067a22e8206
- C:\Users\[username]\AppData\Local\Temp\vuwln\
- wateroilclub[.]com
- 204.44.118[.]201
- 150039308d5385b8170a01307864b761
- Formixing[.]com
- 185.244.149[.]78 и т.д.

Фишинг – nationalbank[.]bz



Фишинг – nationalbank[.]bz



Типовые use case банковского SOC. Что вы должны мониторить обязательно?

- средний уровень: регулярный поиск сайтов-клонов (с помощью скриптов и с помощью GUI):
- https://github.com/brad-anton/brand_watch

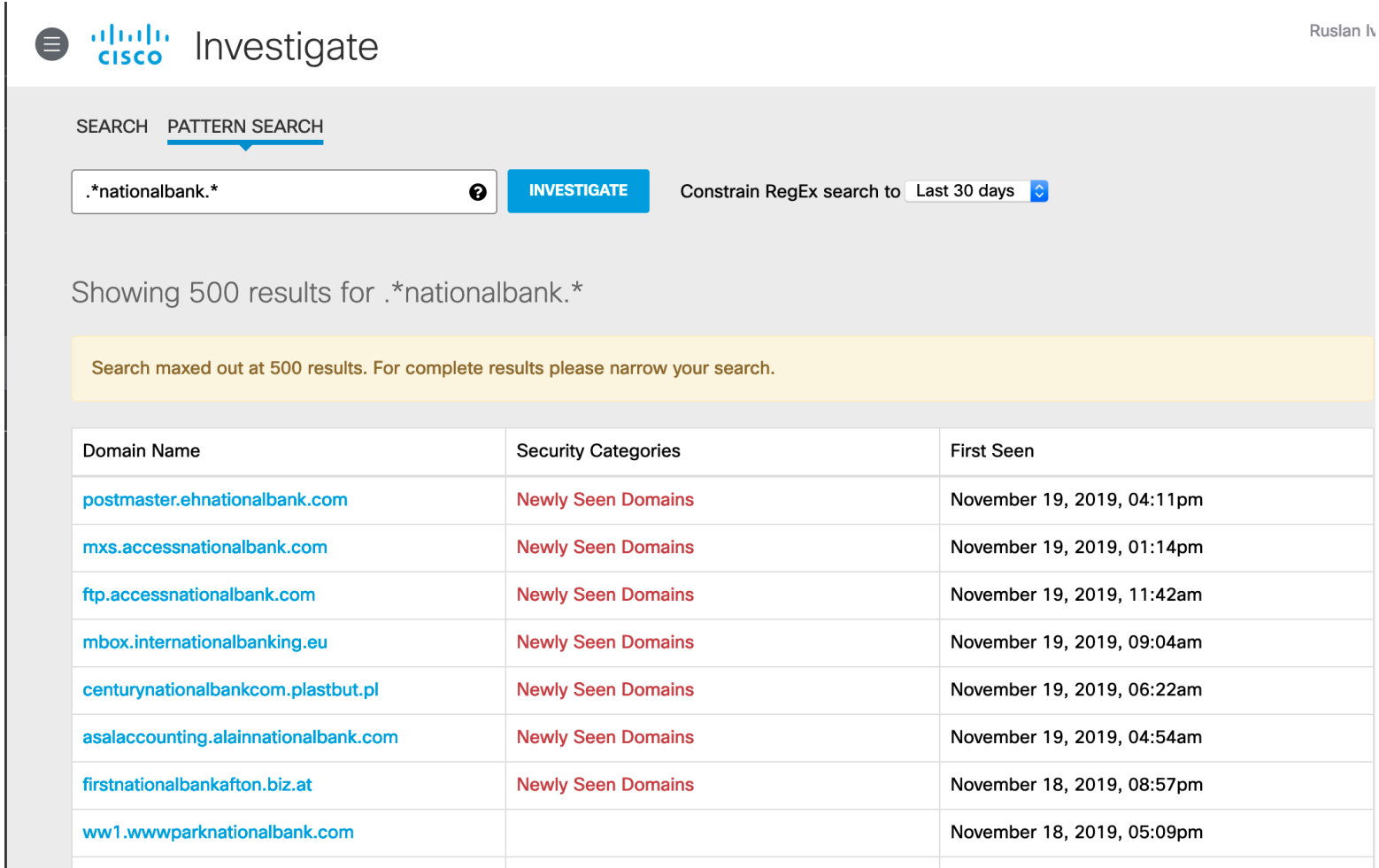
Поиск сайтов-клонов:

```
(py2-venv) [redacted]:brand_watch ruivanov$ python brand_watch.py nationalbank
ftp.accessnationalbank.com
ww1.wwwparknationalbank.com
asalaccounting.alainnationalbank.com
firstnationalbankafton.biz.at
mbox.internationalbanking.eu
centurynationalbankcom.plastbut.pl
postmaster.ehnationalbank.com
mxs.accessnationalbank.com
mail.nobleinternationalbank.com
(py2-venv) [redacted]:brand_watch ruivanov$
```

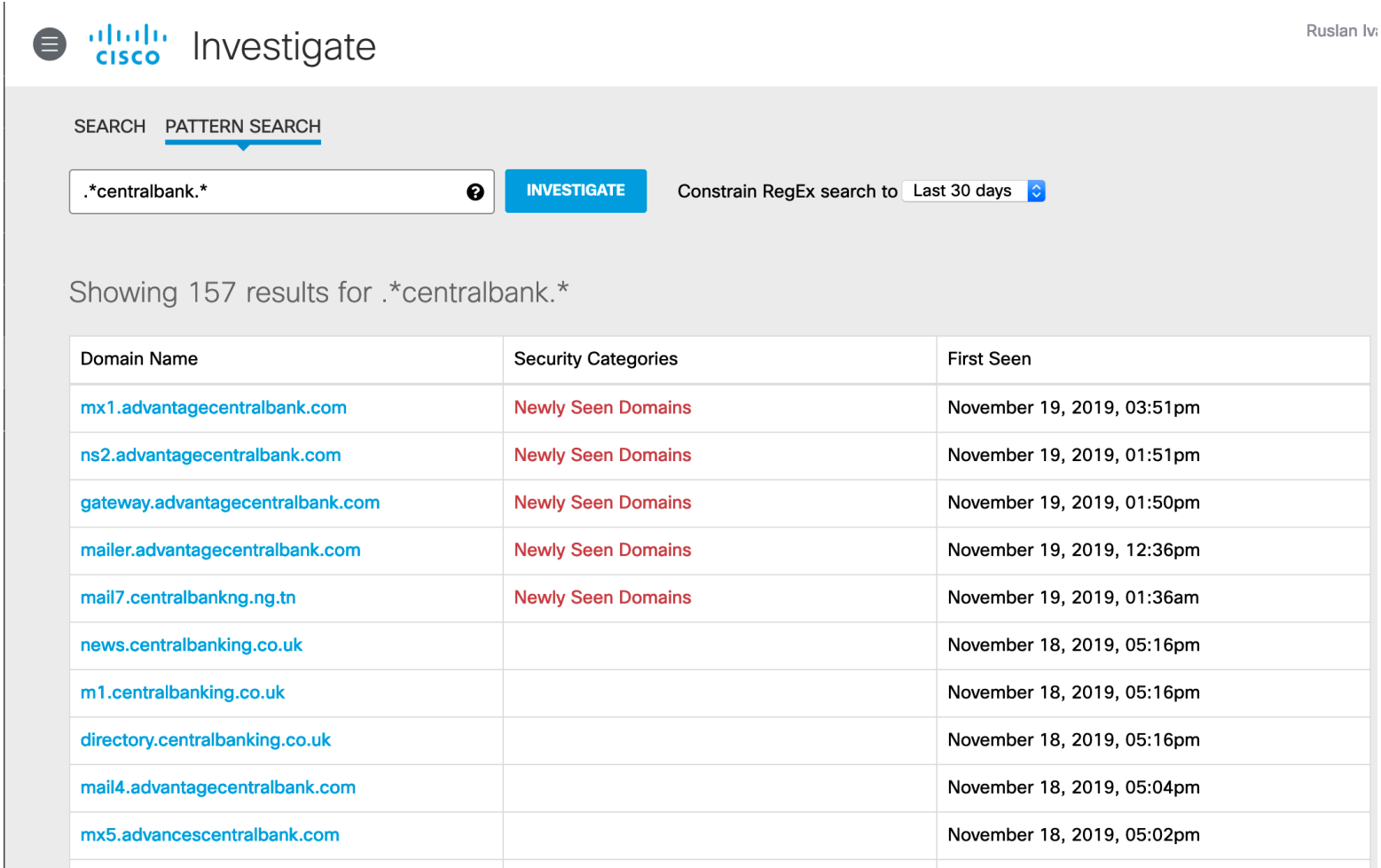
Поиск сайтов-клонов:

```
(py2-venv) [redacted]:brand_watch ruivanov$ python brand_watch.py centralbank
news.centralbanking.co.uk
mail7.centralbankng.ng.tn
gateway.advantagecentralbank.com
m1.centralbanking.co.uk
mx5.advancescentralbank.com
mail4.advantagecentralbank.com
mailer.advantagecentralbank.com
ns2.advantagecentralbank.com
directory.centralbanking.co.uk
mx1.advantagecentralbank.com
(py2-venv) [redacted]:brand_watch ruivanov$
```

Поиск сайтов-клонов:



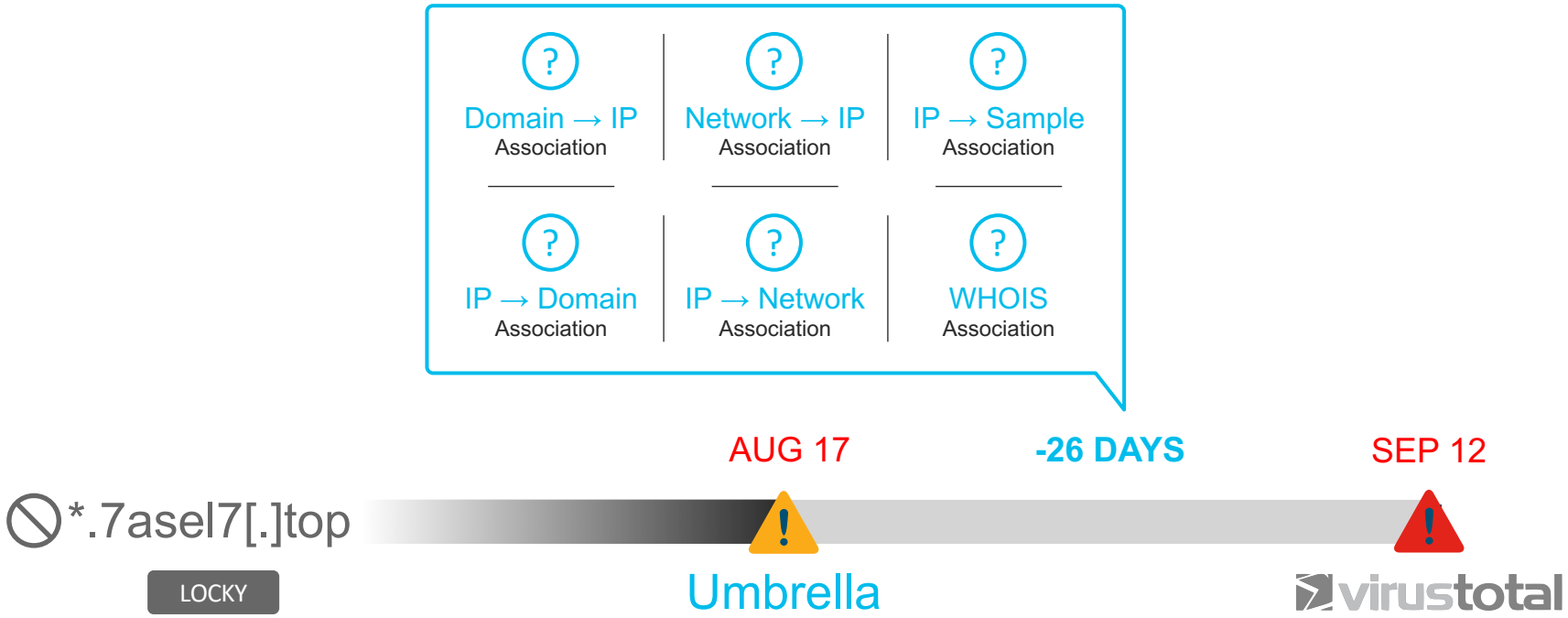
Поиск сайтов-клонов:

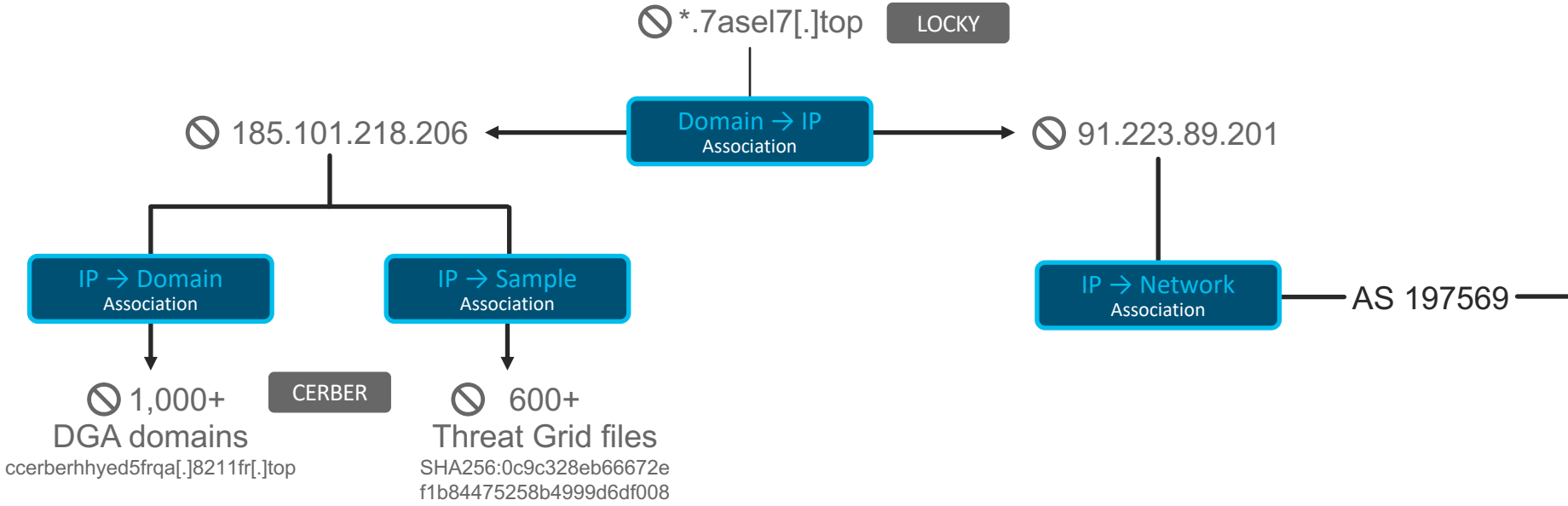


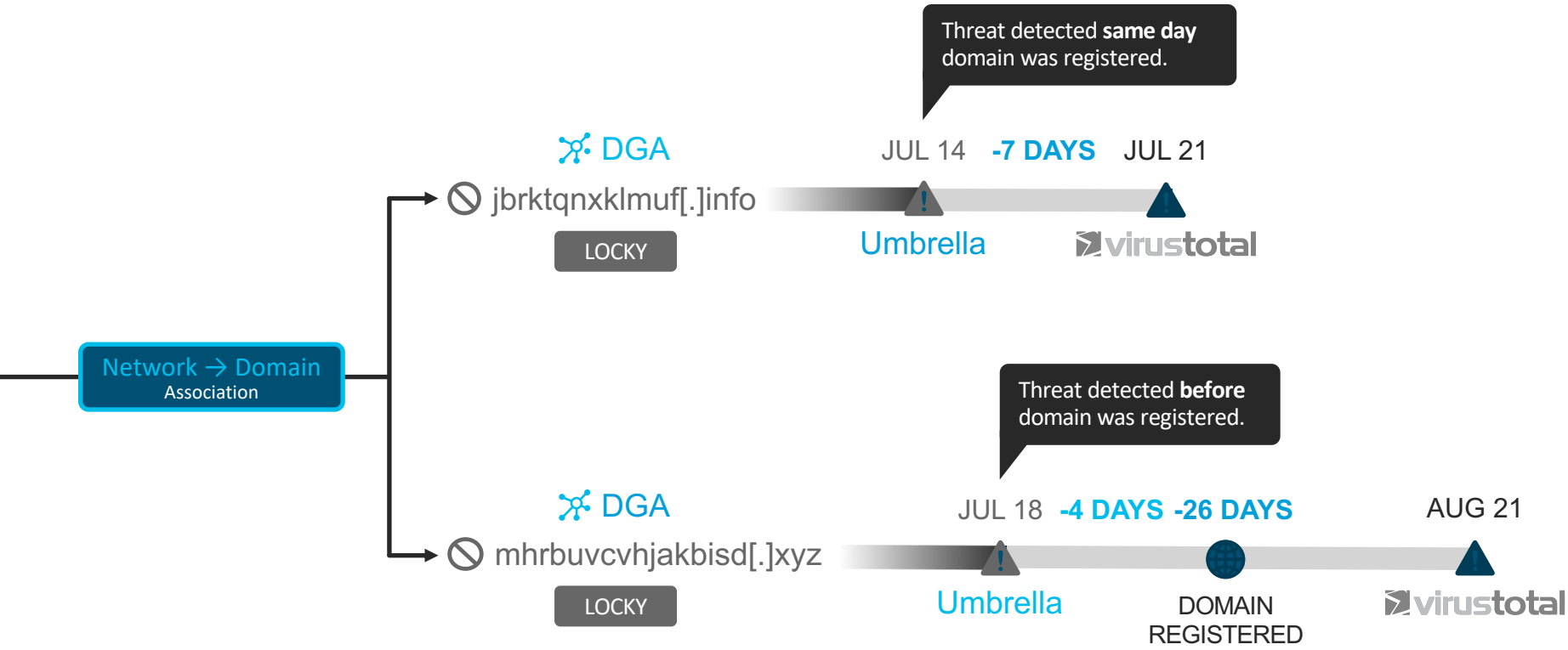
Типовые use case банковского SOC. Что вы должны мониторить обязательно?

- средний уровень: проведения расследования киберкриминальной инфраструктуры (форумы, BPH-хостинги и т.п.):

Шифровальщик Locky – пример выявления инфраструктуры



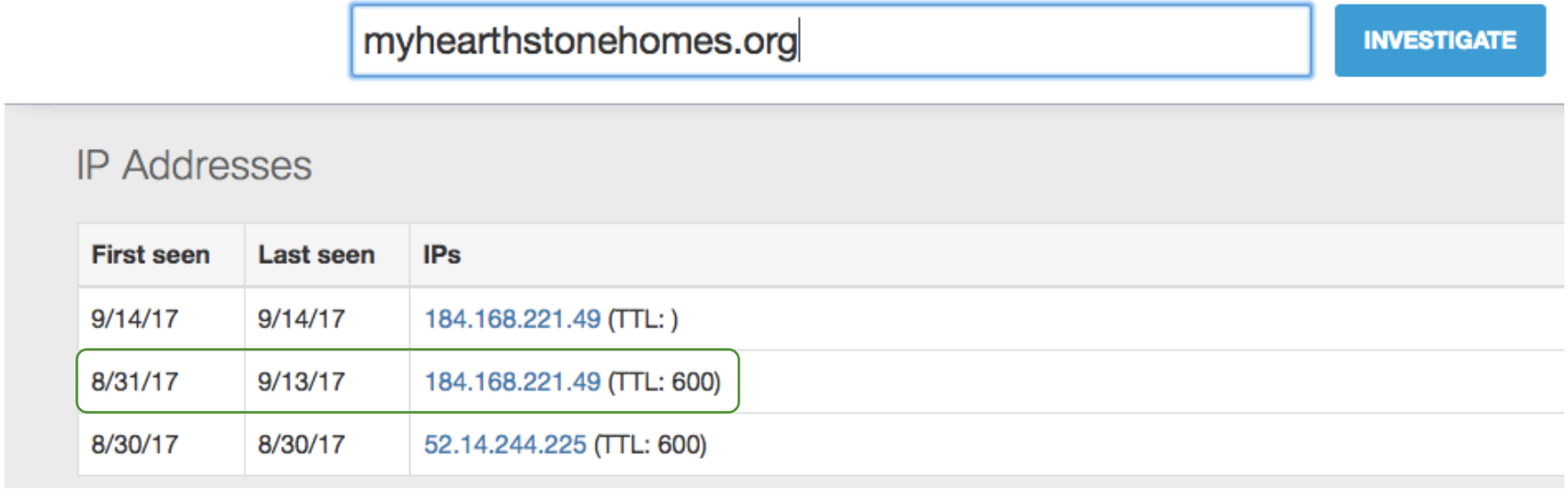




Alex BPH harvests a variety of toxic content

- Malware
- Ransomware
- Phishing
- Crimeware forums
- Credit card dump shops

Insight into the IP network



Details for 52.14.244.225

Hosting 0 malicious domains for 1 week

This IP is currently in the Umbrella block list as malware

Security Categories: Malware

Threat Types: Bulletproof Hosting

An AWS IP abused by Alex' BPH and offered to criminal customers to host malspam attack domains

AS

Prefix	ASN	Network Owner Description
52.14.0.0/16	AS 16509	AMAZON-02 - Amazon.com, Inc., US 86400

Known malicious domains on the same IP

Known domains hosted by 52.14.244.225

agentssellingtips.info antoineandmuse.com apadriana.com brookestonehousevalue.info centralflhousevalue.info
heymamaradio.com imap.antoineandmuse.com imap.centralflhousevalue.info imap.vetstuff.com myoutdoorchild.com
rexahunter.com susannahope.com thechristianblog.com verumpharmaceuticals.com whymovenow.info writerbloggers.com
www.heymamaradio.com www.zashealth.com zaspharma.com zassys.com accuratewindermerehousevalue.info
greathomesellingtips.info newwestorangehomes.info package2china.com realestatetruth.info vetstuff.com
wgopodcastbooking.com writerblogger.com www.agentssellingtips.info zasbiopharmaceuticals.com zasproperties.com
zasbiopharm.com zashealthsystems.com zasholdings.com zashealth.com lovelyflrealestate.com ourrealtyguy.org
protectorsuperhero.com www.lovelyflrealestate.com www.realestatetruth.info www.zasholdings.com www.zasproperties.com
myhearthstonehomes.info myhearthstonehomes.net myhearthstonehomes.org ourrealtyguy.info ourrealtyguy.net
ourrealtyguy.us www.myhearthstonehomes.info www.ourrealtyguy.org

heymamaradio.com

INVESTIGATE

BACK TO TOP

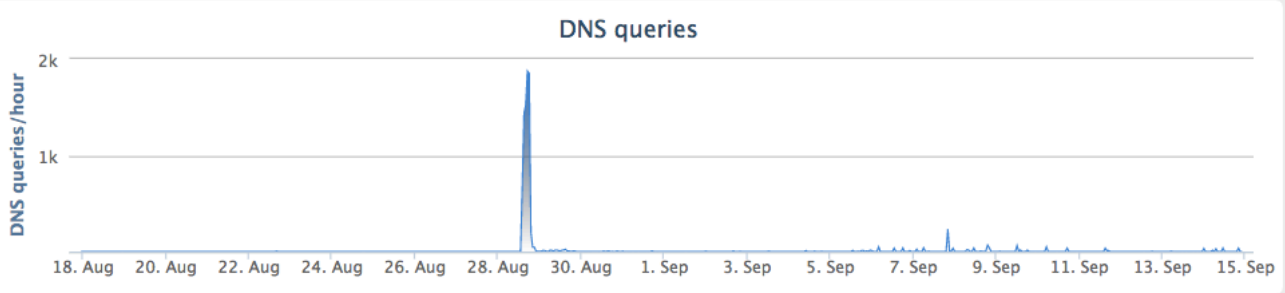
This domain is associated with the following attack: Hancitor Dropper

This domain has a suspicious prefix score

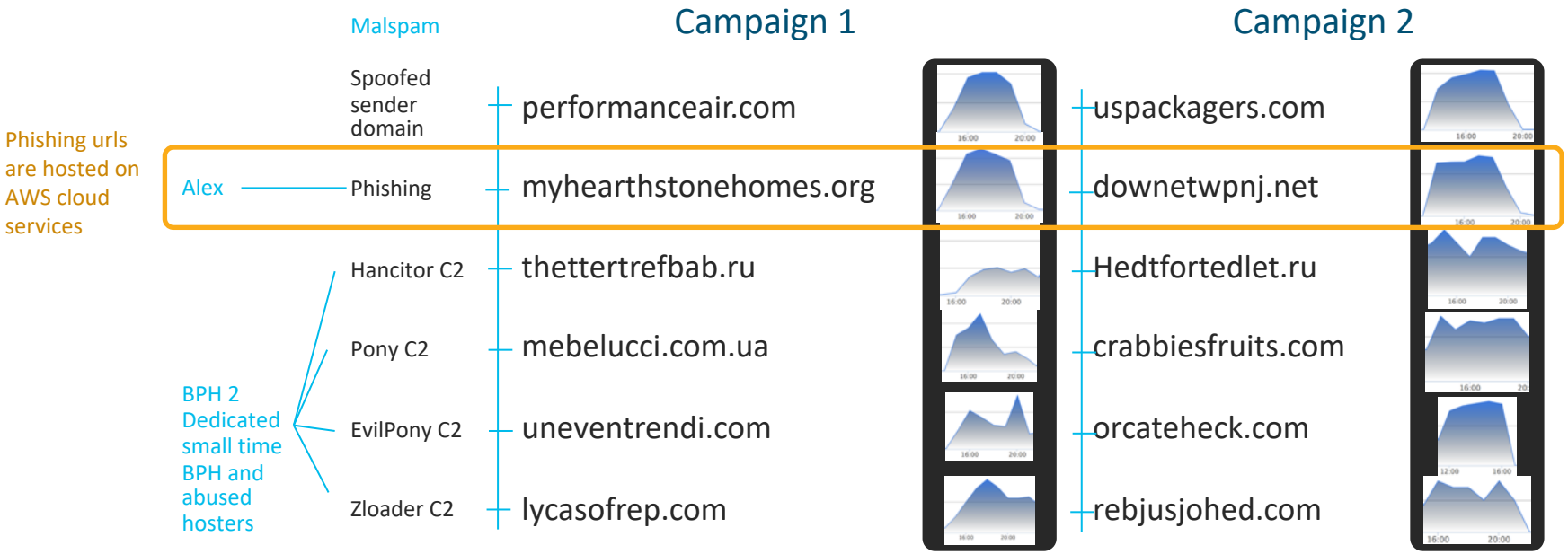
This domain has a suspicious RIP score

Classifier prediction: suspicious

Umbrella risk score: -83



Overarching patterns across a dozen malspam campaigns




CISCO