



Типовые use case банковского SOC.

Что мы должны мониторить обязательно?

Руслан Иванов

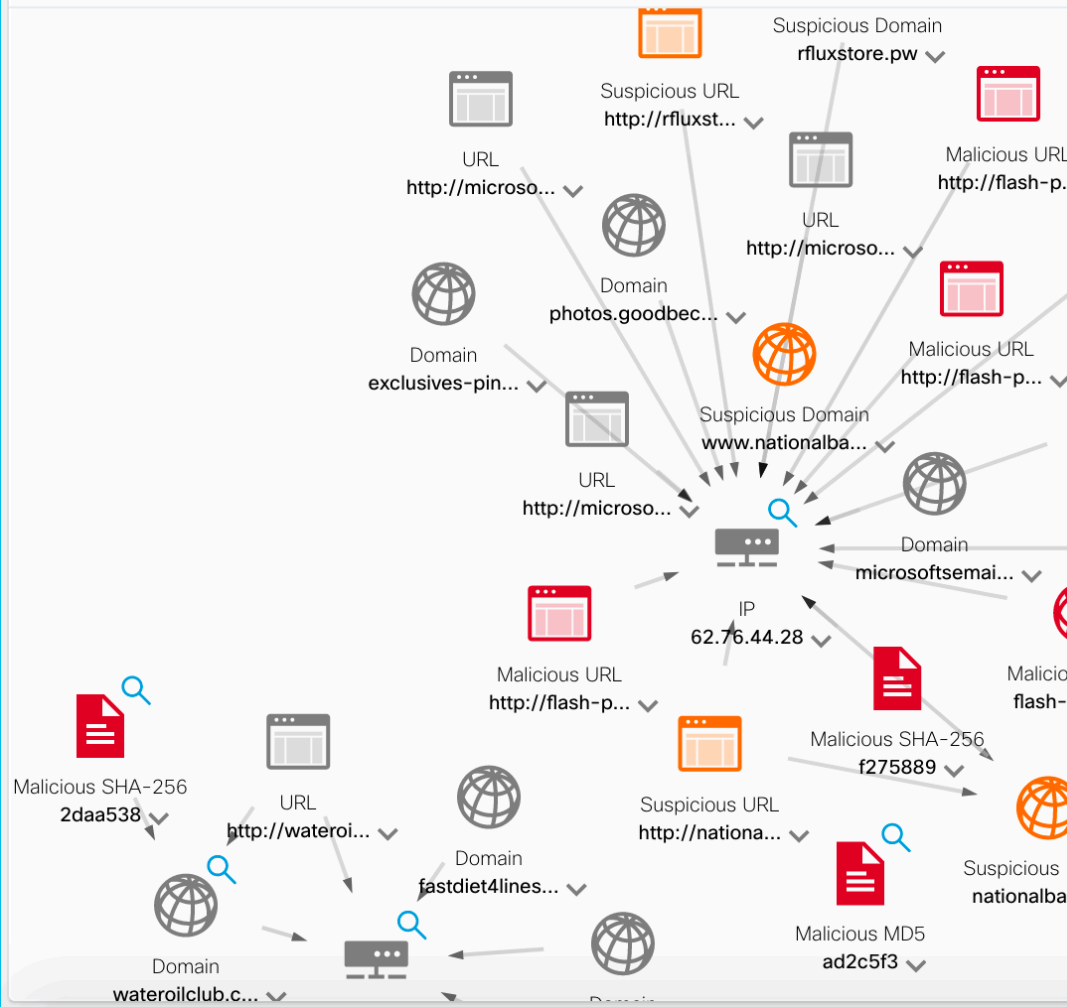
Старший технический консультант по информационной безопасности

ruivanov@cisco.com

Типовые use case банковского SOC.

Что мы должны мониторить
обязательно?

Relations Graph Showing 36 nodes



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
- ... 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

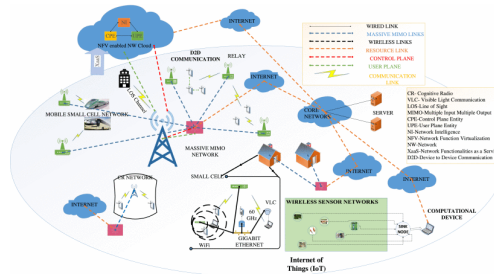
Данные из журналов прокси-серверов, межсетевых экранов, маршрутизаторов, почтовых шлюзов и серверов:

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

DNS основа критической инфраструктуры Интернет



Все возможные
устройства



Любые сетевые архитектуры



Все операционные
системы

Пример индикаторов из реальной фишинговой рассылки

- nationalbank[.]bz

Пример индикаторов из реальной фишинговой рассылки

[New Investigation](#) [Assign to Incident](#) [Snapshots ... ▾](#)

Automatic Layout ▾

Investigation 1 of 1 enrichments complete

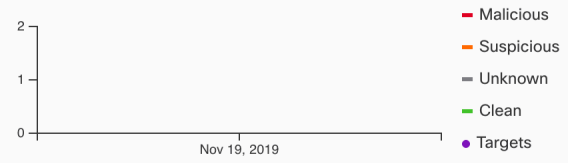
nationalbank[.]bz

[Investigate](#) [Clear](#) [Reset](#) [What can I search for?](#)

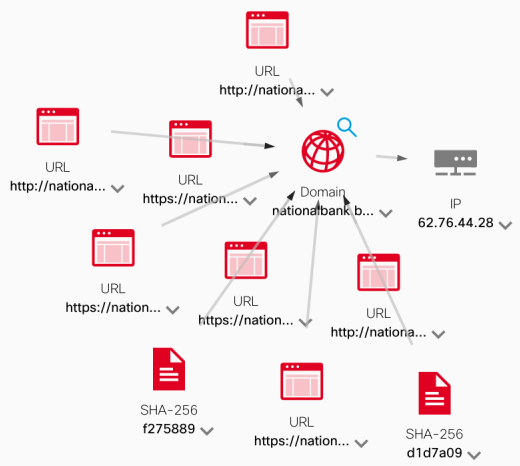
Sightings Timeline

My Environment Global

0 Sightings in My Environment



Relations Graph Showing 11 nodes



Observables

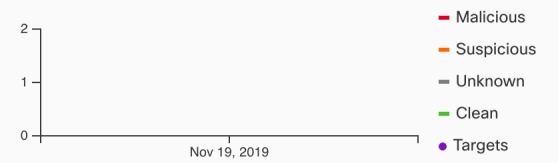
List View ▾

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 st
Talos Intelligence	DOMAIN: nationalbank.bz	Malicious	Poor Talos Intelligence reputat



Фишинг – nationalbank[.]bz



national bank belize



Все

Карты

Новости

Картинки

Видео

Ещё

Настройки

Инструменты

Результатов: примерно 32 100 000 (0,87 сек.)

National Bank of Belize

<https://www.nbbi.bz> ▼ [Перевести эту страницу](#)

National Bank of Belize are an institution of integrity, transparency and sound banking, dedicated to providing you with financial products that are designed to ...

Фишинг – nationalbank[.]bz

Яндекс

national+bank+belize



Найти



Поиск Картинки Видео Карты Маркет Новости Переводчик Эфир Коллекции Знатоки Услуги Ещё

National Bank of Belize

nbbi.bz

Welcome to **National Bank of Belize** Limited! We are an institution of integrity, transparency and sound banking, dedicated to providing you with financial products that are designed to meet the banking needs of all **Belizeans**. The People's Bank... [Читать ещё >](#)

National Bank of Belize - Wikipedia

en.wikipedia.org > National Bank of Belize

The **National Bank of Belize** Limited (NBBL) is a government-owned bank headquartered in Belmopan, Cayo District, **Belize**. With \$47 million in assets (2016) it is the smallest commercial bank in **Belize**. [Читать ещё >](#)

Belize Bank – Our Country. Your Bank

belizebank.com

At **Belize Bank** we know you aren't looking for a complicated solution. ... The **Belize Bank** Limited offers its customers both local and international credit cards under the VISA and MasterCard (international only) brands. Read More. Security Center. [Читать ещё >](#)

Central Bank of Belize

centralbank.org.bz

The Central **Bank of Belize** regulates **Belize's** financial system ... The Central **Bank of Belize**, in collaboration with the Ministry of Finance, launched **Belize's National** Financial Inclusion Strategy on 17 September 2019. Learn More. The **Bank**... [Читать ещё >](#)

Нашлось 2 млн результатов

[Дать объявление](#) [Показать все](#)

SEARCH PATTERN SEARCH

nationalbank.bz

INVESTIGATE

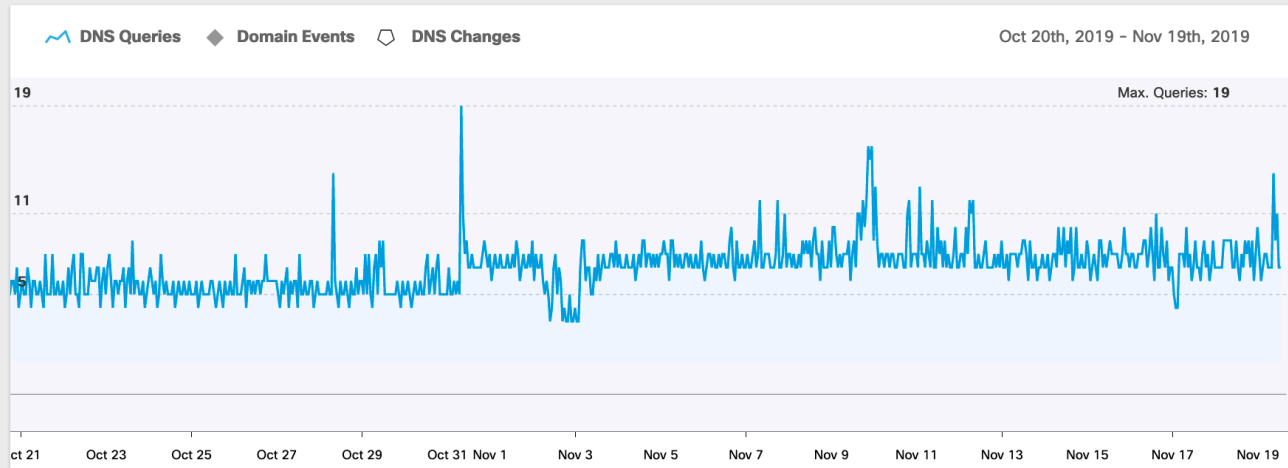


Details for nationalbank.bz

This domain is currently in the Umbrella block list. Umbrella Investigate Risk Score: 100

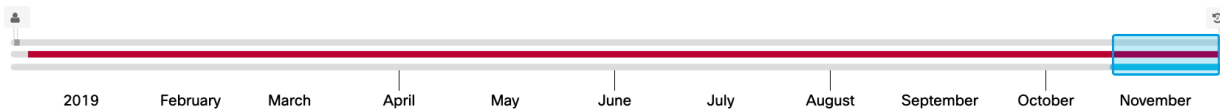
Timeline

Current Content Category: None



Event History

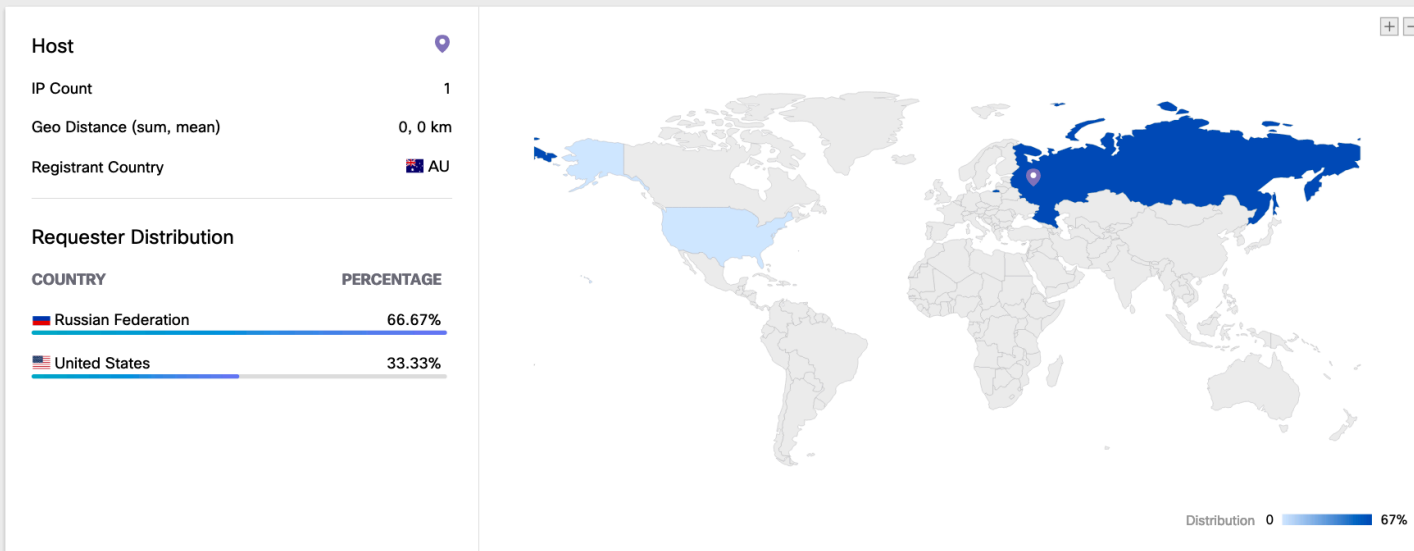
Security Categories DNS Changes Query History



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 ▾



Associated Samples

POWERED BY **CISCO AMP THREAT GRID**

Threat Score	SHA256 Signature	AV Result
81	fe5135ce1928f613e2b0500eadbd588e9ead84feb5fd377e4b03284f9515c31a	

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

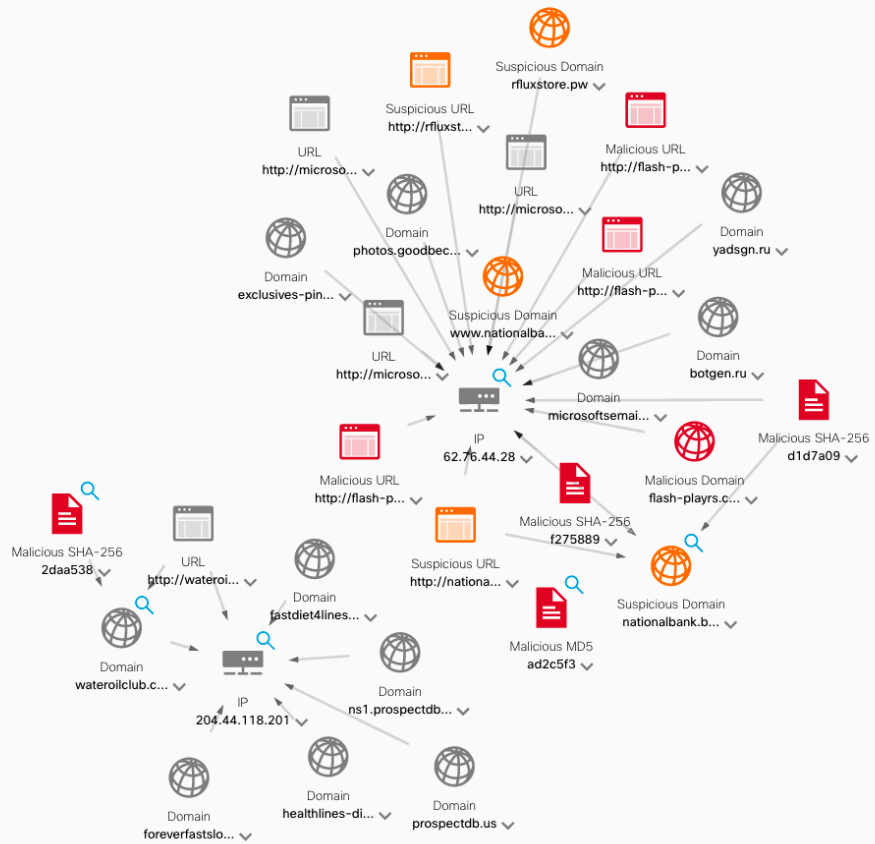
- средний уровень: раскрытие инфраструктуры злоумышленника (с одного домена или по e-mail владельца) для проактивного внесения в черные списки и мониторинга того, что еще может произойти в будущем:

Выявленные индикаторы из фишинговой рассылки

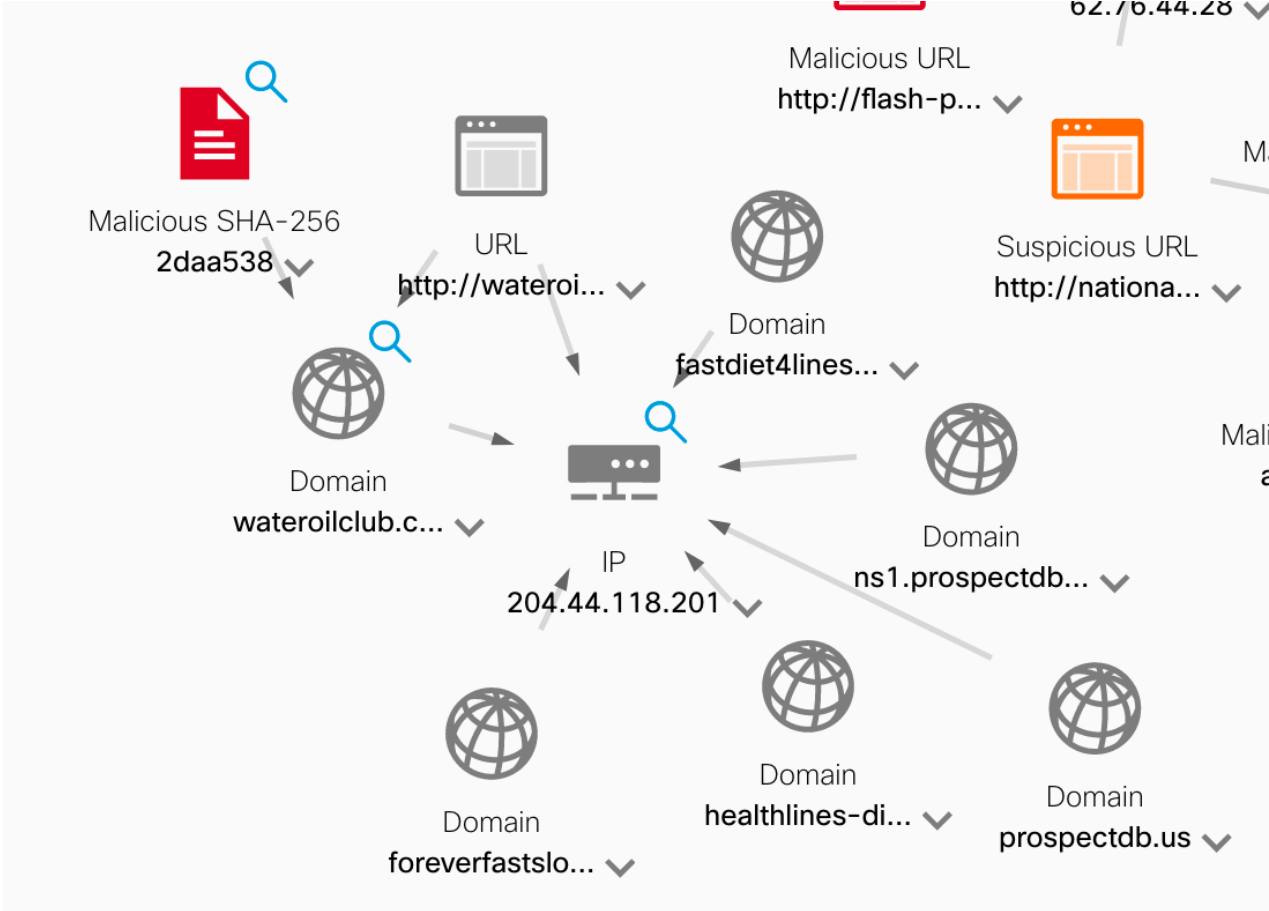
- nationalbank[.]bz
- 62.76.44[.]28
- ad2c5f31e65b8710c8230067a22e8206
- C:\Users\[username]\AppData\Local\Temp\vuwl\
- wateroilclub[.]com
- 204.44.118[.]201
- 150039308d5385b8170a01307864b761
- Formixing[.]com
- 185.244.149[.]78 и т.д.

Фишинг – nationalbank[.]bz

Relations Graph Showing 36 nodes



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
centurnationalbankcom.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:

SEARCH PATTERN SEARCH

.[*nationalbank.*](#)



INVESTIGATE

Constrain RegEx search to [Last 30 days](#)

Showing 500 results for [.*nationalbank.*](#)

Search maxed out at 500 results. For complete results please narrow your search.

Domain Name	Security Categories	First Seen
postmaster.ehnationalbank.com	Newly Seen Domains	November 19, 2019, 04:11pm
mxs.accessnationalbank.com	Newly Seen Domains	November 19, 2019, 01:14pm
ftp.accessnationalbank.com	Newly Seen Domains	November 19, 2019, 11:42am
mbox.internationalbanking.eu	Newly Seen Domains	November 19, 2019, 09:04am
centurnationalbankcom.plastbut.pl	Newly Seen Domains	November 19, 2019, 06:22am
asalaccounting.alainnationalbank.com	Newly Seen Domains	November 19, 2019, 04:54am
firstrnationalbankafton.biz.at	Newly Seen Domains	November 18, 2019, 08:57pm
ww1.wwwparknationalbank.com		November 18, 2019, 05:09pm

Поиск сайтов-клонов:

SEARCH PATTERN SEARCH

?

INVESTIGATE

Constrain RegEx search to ▾

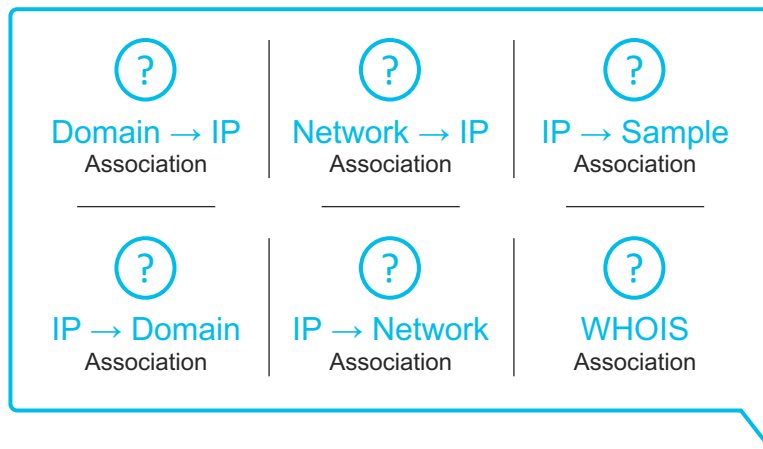
Showing 157 results for .*centralbank.*

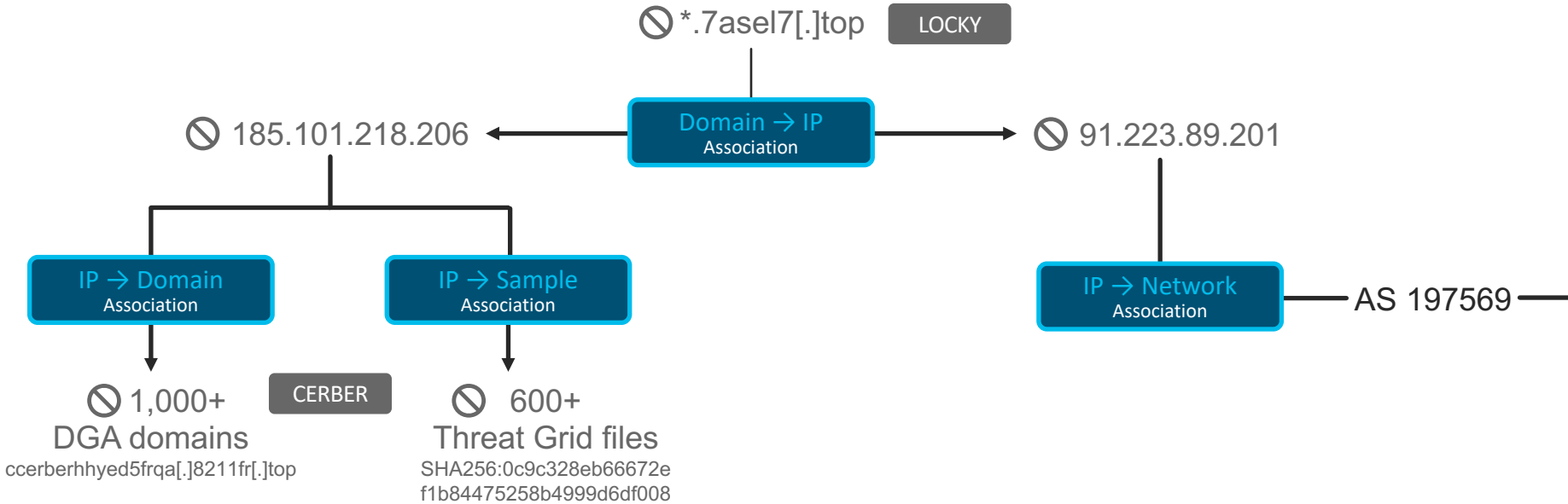
Domain Name	Security Categories	First Seen
mx1.advantagecentralbank.com	Newly Seen Domains	November 19, 2019, 03:51pm
ns2.advantagecentralbank.com	Newly Seen Domains	November 19, 2019, 01:51pm
gateway.advantagecentralbank.com	Newly Seen Domains	November 19, 2019, 01:50pm
mailer.advantagecentralbank.com	Newly Seen Domains	November 19, 2019, 12:36pm
mail7.centralbankng.ng.tn	Newly Seen Domains	November 19, 2019, 01:36am
news.centralbanking.co.uk		November 18, 2019, 05:16pm
m1.centralbanking.co.uk		November 18, 2019, 05:16pm
directory.centralbanking.co.uk		November 18, 2019, 05:16pm
mail4.advantagecentralbank.com		November 18, 2019, 05:04pm
mx5.advancescentralbank.com		November 18, 2019, 05:02pm

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

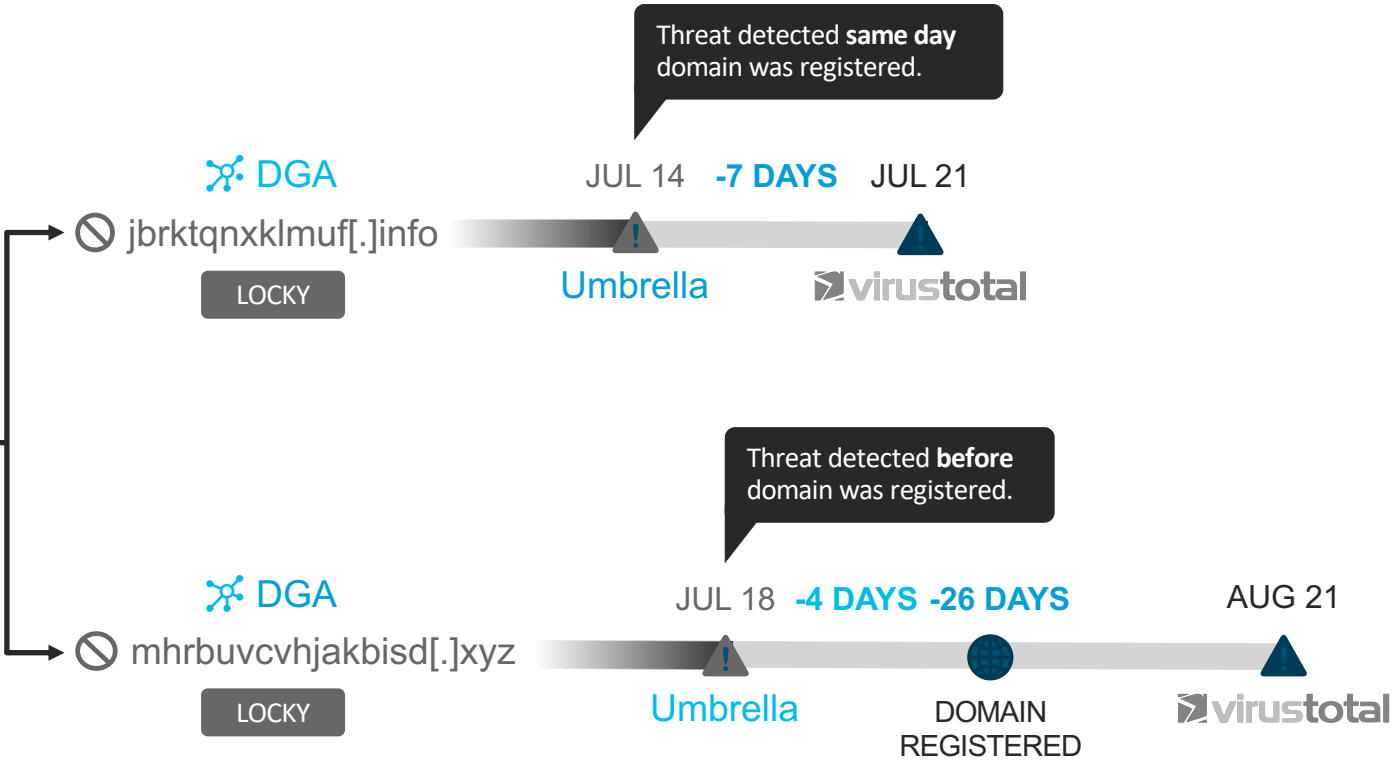
- средний уровень: проведения расследования киберкриминальной инфраструктуры (форумы, VPN-хостинги и т.п.):

Шифровальщик Locky – пример выявления инфраструктуры





Network → Domain Association



Alex BPH harvests a variety of toxic content



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

Insight into the IP network

INVESTIGATE

IP Addresses

First seen	Last seen	IPs
9/14/17	9/14/17	184.168.221.49 (TTL:)
8/31/17	9/13/17	184.168.221.49 (TTL: 600)
8/30/17	8/30/17	52.14.244.225 (TTL: 600)

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

[agentsellingtips.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

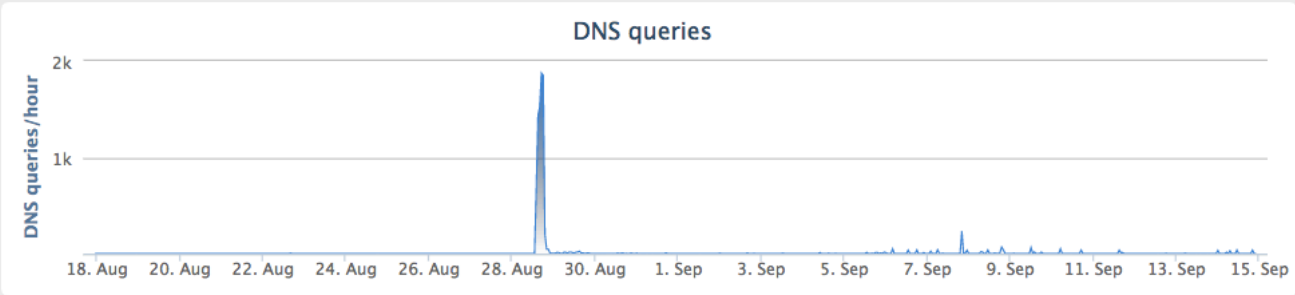
[BACK TO TOP](#)

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

