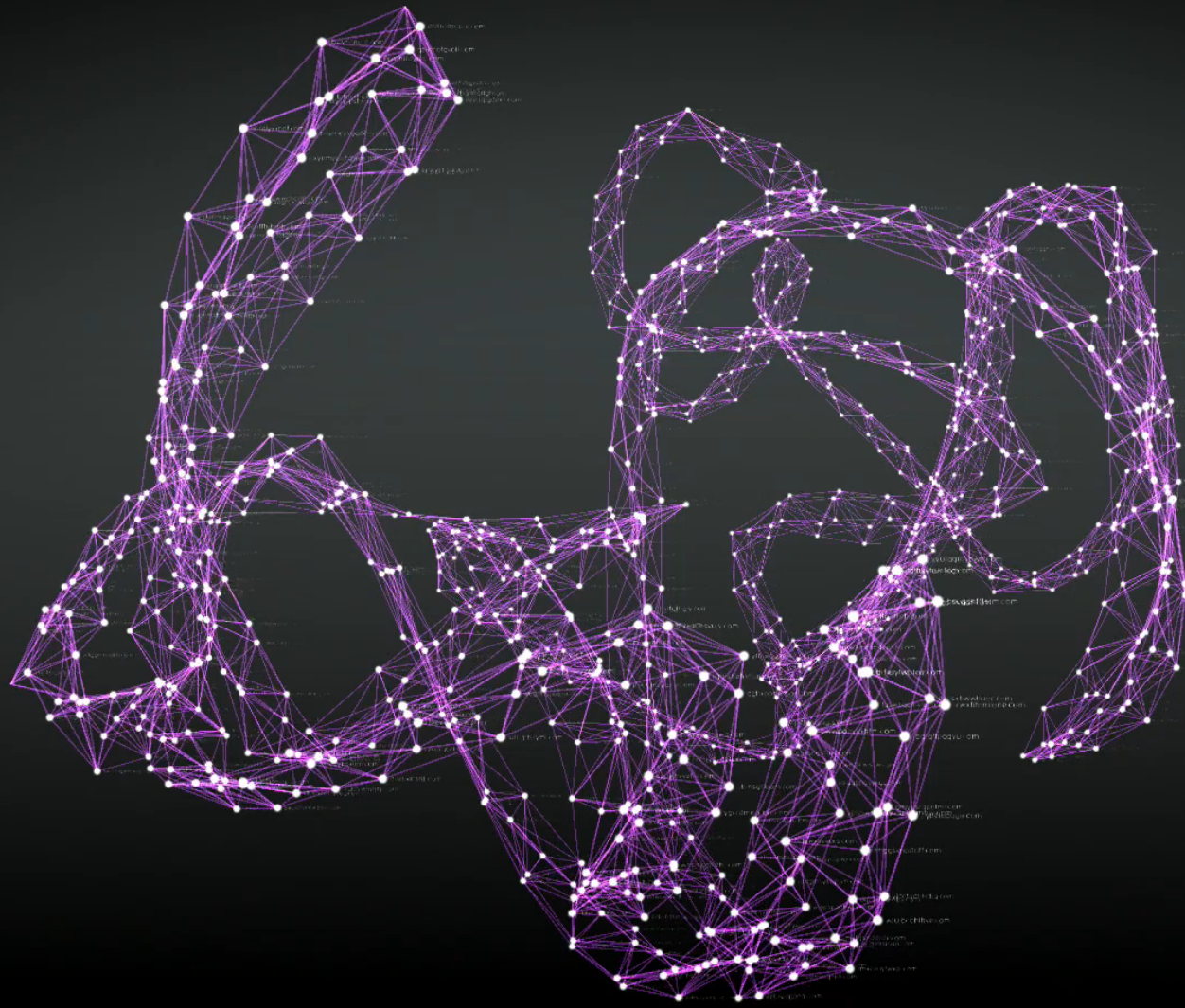


# Как ловить кибермафию с помощью DNS

И попутно повышать доверие к Президенту России

08 сентября 2020



# www.cisco.com

Домен  
третьего  
уровня

Домен  
второго  
уровня

Домен  
верхнего  
уровня

FQDN

# Что можно вытащить из DNS-трафика: уровень I


Тип записи	Значение
A или AAAA	IP-адрес (IPv4 или IPv6)
NS	Отвечающий за домен сервер имен
TXT	Описание домена
MX	Почтовый обменник
CNAME	Альтернативное имя для ресурса (для перенаправления на другое имя)
SOA	Ключевые данные о зоне (например, TTL или контакты владельца)

# Что можно вытащить из DNS-трафика: уровень II

Протокол DNS		IP/Сеть		Регистрация домена	
Длина FQDN	Лексические данные FQDN	IP-адреса	ASN	Контакты: регистратор и владелец	Дата создания
Длина домена 2-го/n-го уровня	Лексические данные доменов 2-го/n-го уровня	Запаркованные домены	CNAME, NS, SOA, MX	Дата окончания	Последнее обновление
Значения TTL	Коды ответов			Страна / геолокация	
Временная информация					

# Обнаружение алгоритмов генерации доменов DGA

**“N-gram” анализ**  
Соответствуют ли  
наборы рядом  
стоящих символов  
языковому шаблону?



yfrscsddkddl.com  
qgmcgoqeasgomme.org  
iyyxtyxdeypk.com  
diiqngijkpop.ru

**Анализ энтропии**  
Не выглядит ли  
распределение  
символов случайным?

# Что можно вытащить из DNS-трафика: уровень III

- Энтропия / распределение символов в FQDN
- Взаимосвязи между доменами / IP-адресами / e-mail владельцев / автономными системами (ASN)
- Вредоносная активность, связанная с доменом / IP / e-mail владельцев / автономными системами (ASN)

Кто нас атакует?



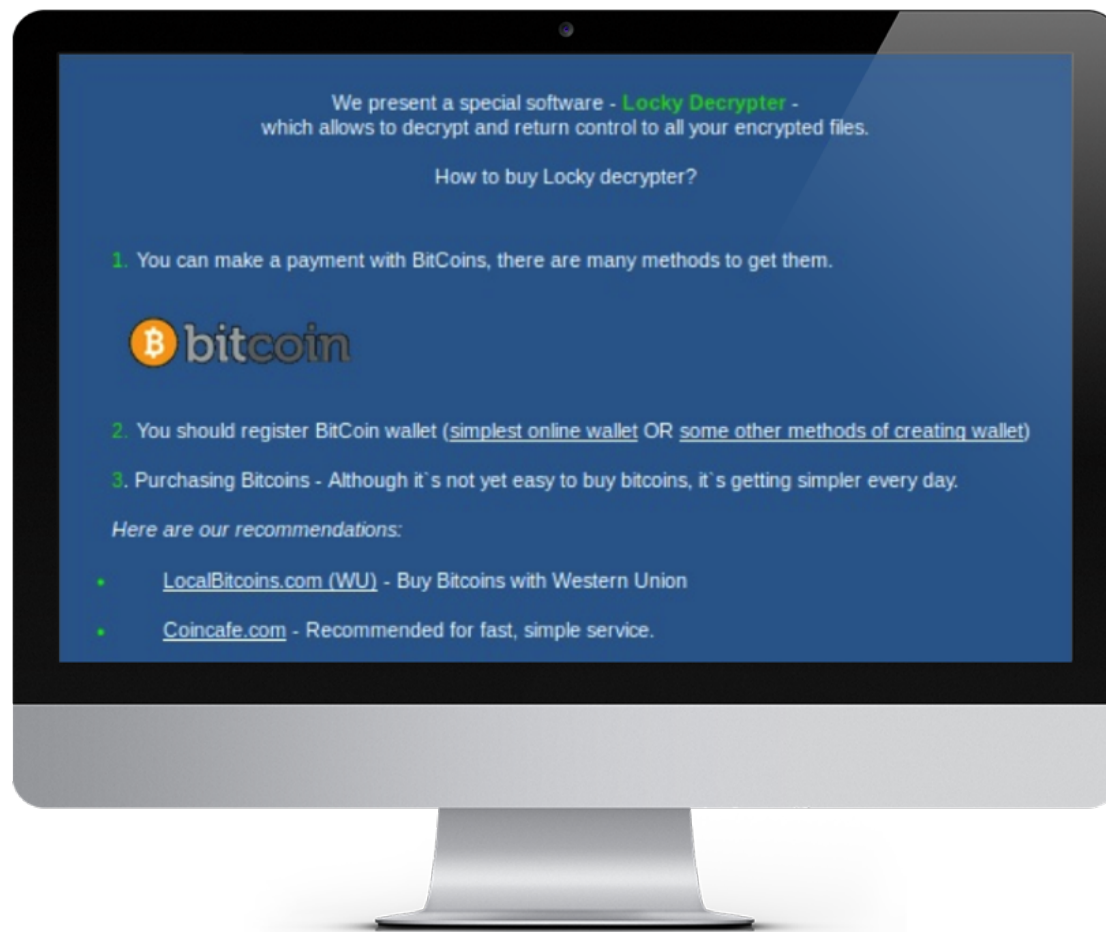
Какова инфраструктура нападающих?



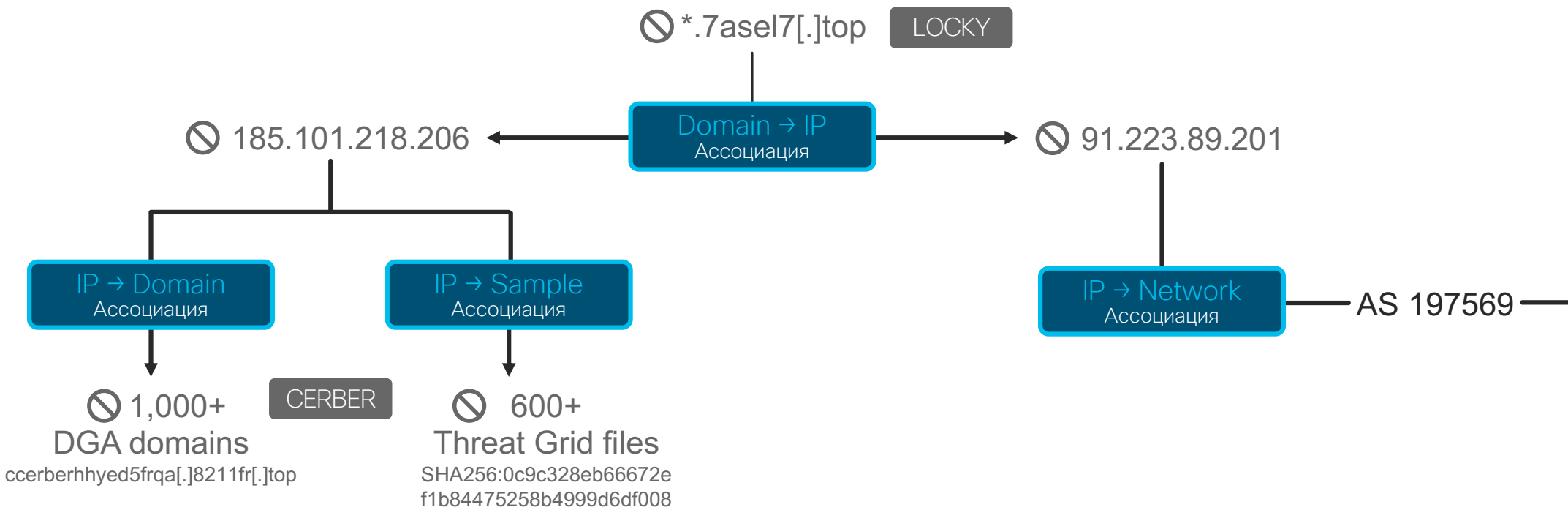
Специфические детали угроз

# Знакомо ли вам имя Locky?

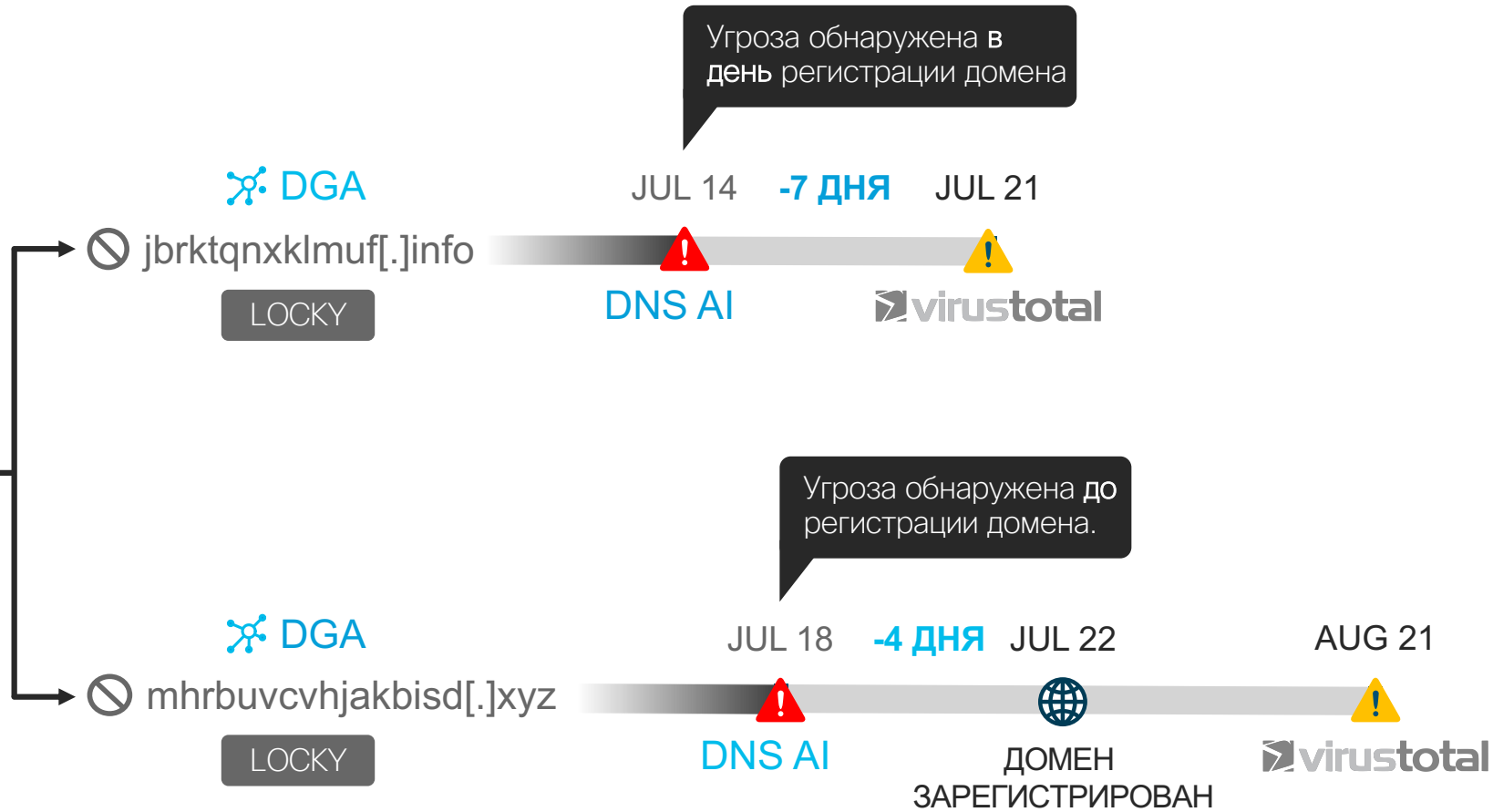
- Через вложение Email в фишинговой рассылке
- Шифрует и переименовывает файлы с .locky расширением
- Примерно 90,000 жертв в день
- Выкуп порядка 0.5 – 1.0 BTC (1 BTC ~ \$601 US)
- Связан с операторами кампании Dridex



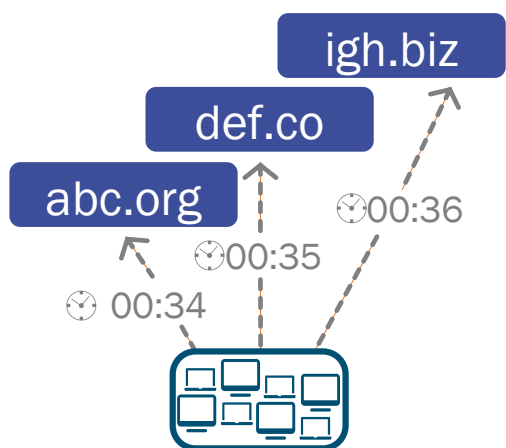




Network → Domain  
Ассоциация

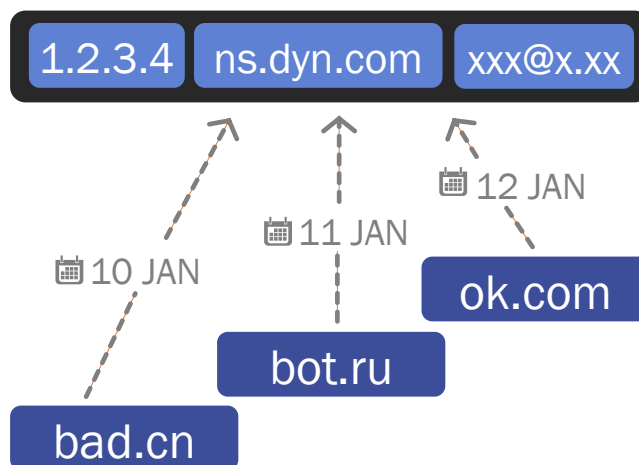


# Корреляция DNS, WHOIS и BGP



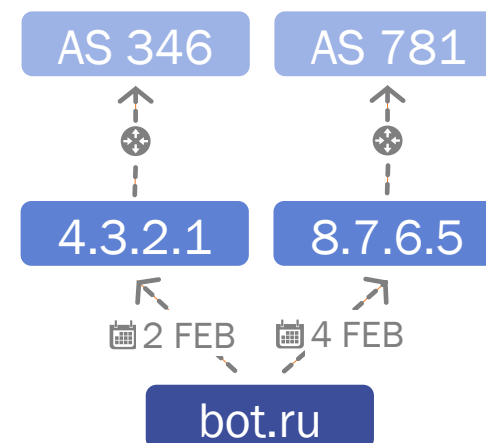
## СОВМЕСТНЫЕ ЗАПРОСЫ

Запросы вида домен-к-домену через рекурсивный DNS



## ПАССИВНЫЙ DNS И WHOIS

Текущие и прошлые связи для домен-к-IP/nameserver/email через authoritative DNS и DNS registrars



## ИНФРАСТРУКТУРЫ

Домен-к-IP-к-AS взаимоотношения через графы BGP данные маршрутов

# Геолокационный анализ IP

Хостится в более чем 28+ странах



## ХОСТ ИНФРАСТРУКТУРА

Расположение сервера  
IP адреса, связанные с  
доменом

Только заказчики из US связываются с .RU TLD



## DNS ЗАПРОШИВАЮЩИЕ ХОСТЫ

Расположение сетевые и вне-сетевые  
IP адреса запрашивающих домен

# Финансовая помощь от государства?..



## СЛУЖБА ФИНАНСОВОЙ ЗАЩИТЫ ПОТРЕБИТЕЛЕЙ по возврату невыплаченных денежных средств СЗП ВНС



Вы находитесь на официальном сайте уполномоченного подразделения по финансовой защите населения.

### Вы уже получили компенсацию?



#### От 12 000 до 300 000 рублей

Срочные компенсации Н.Д.С. начисляются гражданам за последние 36 месяцев.

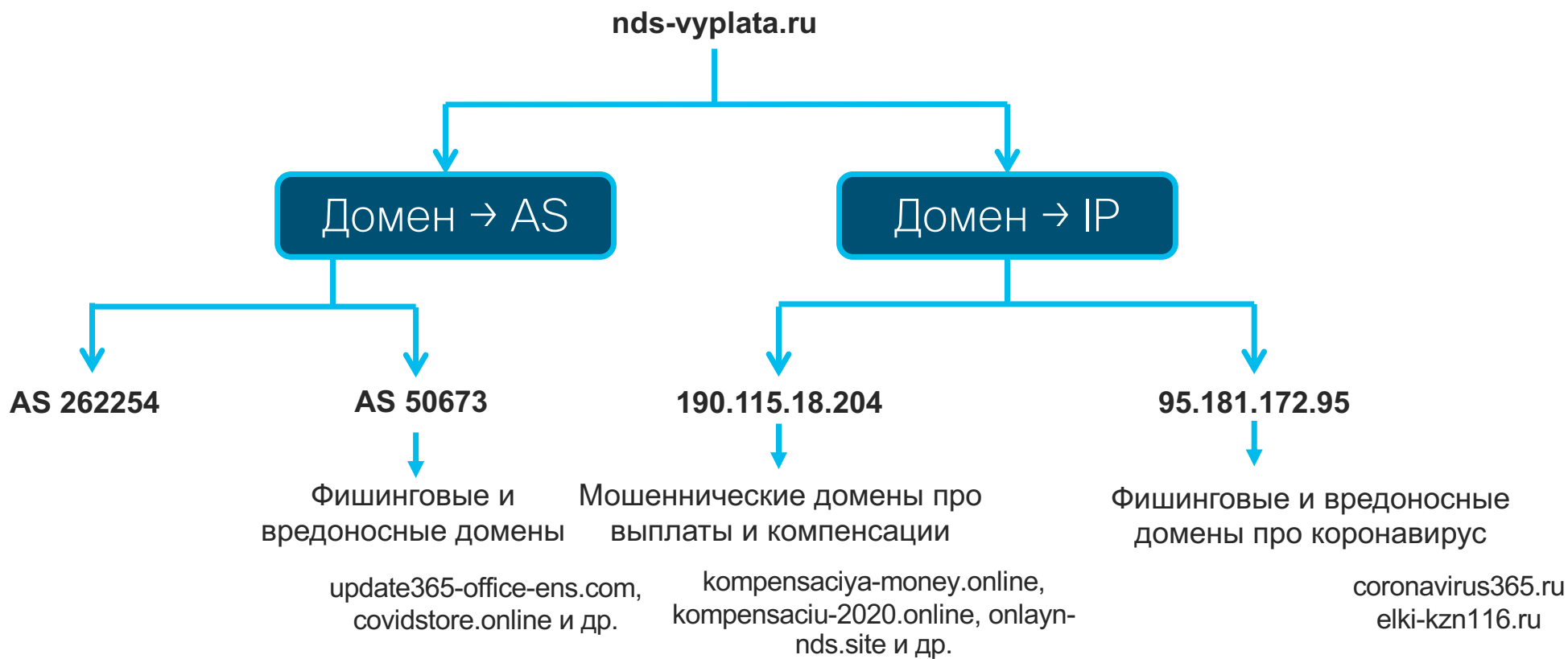
Вся сумма выплачивается на банковскую карту сразу в день подачи заявки.

Срок подачи заявок до **17 июля 2020 г.**

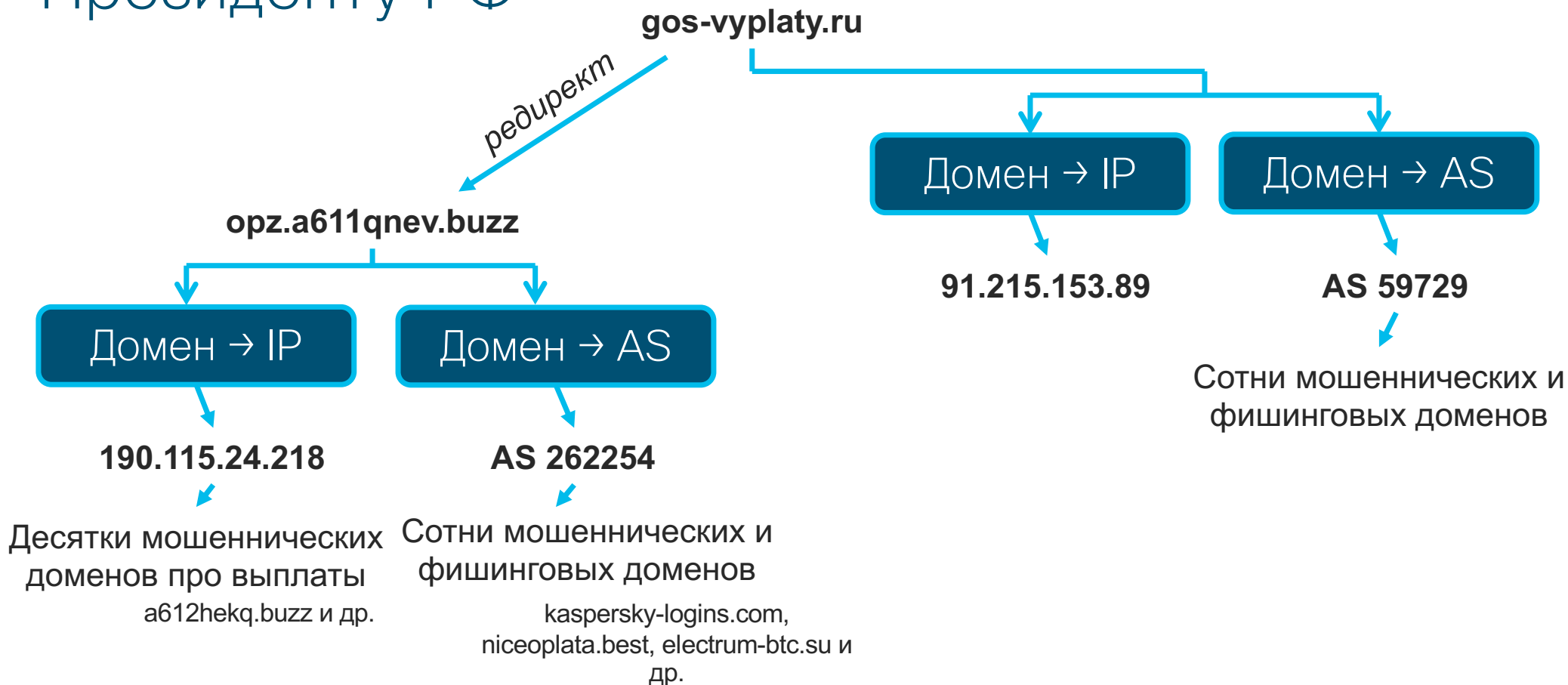
Для получения средств заполните поле ниже и нажмите «проверить»



Введите 6 последних цифр банковской карты, которой чаще всего пользуетесь и нажмите кнопку "Проверить свою компенсацию"



# Как мошенники подрывали доверие к Президенту РФ



# Заодно атаковались и все популярные антивирусы

goattlogin.com bitdefender-centrals.com  
bitdefender-centralx.com bitdefender-loginn.com  
iwebrootcomsafe.com kaspersky-loginn.com  
kaspersky-logins.com kasperskylogins.com  
malwarebyteslogins.com malwarebytesloginz.com  
mcafeecom-actvatez.com mcafeelogins.com  
mcafeeloginz.com myavastz.com  
mynortoncomnu16.com mynortonnu16.com  
norton-comnu16.com norton-logins.com  
nortoncom-setupz.com nortoncomnu16.com  
nortoncomsetupo.com nortonlogins.com  
nortonloginz.com trendmicro-loginn.com  
trendmicro-logins.com trendmicrodownload.com  
trendmicrologins.com trendmicrologinx.com  
webroot-loginn.com webrootcomsafex.com  
webrootloginn.com webrootlogins.com  
webrootloginz.com finway.top sbcglobal-login.us  
mailaolcomz.com pay-epay.net att-loginz.com  
sbcgloballoginn.com sbcgloballoginz.com



gos-vyplaty.ru

редирект

opz.a611qnev.buzz

Домен → IP

Домен → AS

91.215.153.89

AS 59729

Сотни мошеннических и фишинговых доменов

Домен → IP

Домен → AS

190.115.24.218

AS 262254

Десятки мошеннических доменов про выплаты a612hekq.buzz и др.

Сотни мошеннических и фишинговых доменов kaspersky-logins.com, niceoplata.best, electrum-btc.su и др.

nds-vyplata.ru

Домен → AS

Домен → IP

AS 262254

AS 50673

190.115.18.204

95.181.172.95

Фишинговые и вредоносные домены

Мошеннические домены про выплаты и компенсации

Фишинговые и вредоносные домены про коронавирус

update365-office-ens.com, covidstore.online и др.

kompensaciya-money.online, kompensaciyu-2020.online, onlayn-nds.site и др.

coronavirus365.ru elki-kzn116.ru

# Вспомним про коронавирус

- Сотни доменов с «coronavirus» в названии
- Сотни доменов с «covid» в названии
- Десятки доменов с «mask» в названии

# Сотни «горячих» доменов

SEARCH PATTERN SEARCH

Showing 257 results for .\*coronavirus.\*\,ru

Domain Name	Security Categories
<a href="#">covid19-voronezh.ru</a>	Malware, ...
<a href="#">covid-19-stop.ru</a>	Malware
<a href="#">covid19news.ru</a>	Malware
<a href="#">covid19rus.ru</a>	Malware
<a href="#">covid-19info.ru</a>	Malware
<a href="#">covid19-spb.ru</a>	Malware
<a href="#">covid19msk.ru</a>	Malware
<a href="#">covidcoronavirus.ru</a>	Malware
<a href="#">nocovid-19.ru</a>	Malware
<a href="#">maski-covid19.ru</a>	Malware
<a href="#">covid19net.ru</a>	Malware
<a href="#">covid-kld.ru</a>	Malware
<a href="#">covid-med-help.ru</a>	Malware
<a href="#">anticovid2019.ru</a>	Malware
<a href="#">medmaski-covid19.ru</a>	Malware
<a href="#">stopcovid19smr.ru</a>	Malware
<a href="#">iscovid-19.ru</a>	Malware
<a href="#">covid19-kazan.ru</a>	Malware

SEARCH PATTERN SEARCH

Showing 349 results for .\*mask.\*\,ru

Domain Name	Security Categories	First Seen
<a href="#">mask-shop.bestsales2020.ru</a>	Newly Seen Domains	April 01, 2020, 12:37pm
<a href="#">zashitamask.ru</a>	Newly Seen Domains	April 01, 2020, 11:13am
<a href="#">mask.corp168.ru</a>	Newly Seen Domains	April 01, 2020, 10:15am
<a href="#">maskotopress.ru</a>	Newly Seen Domains	April 01, 2020, 09:48am
<a href="#">my-maski.ru</a>	Newly Seen Domains	April 01, 2020, 09:44am
<a href="#">maska-piter.ru</a>	Newly Seen Domains	April 01, 2020, 09:44am
<a href="#">www.md-mask.ru</a>	Newly Seen Domains	April 01, 2020, 09:42am
<a href="#">md-mask.ru</a>	Newly Seen Domains	April 01, 2020, 09:42am
<a href="#">mmask.ru</a>	Newly Seen Domains	April 01, 2020, 09:40am
<a href="#">maskisam.ru</a>	Newly Seen Domains	April 01, 2020, 09:39am
<a href="#">maskatyt.ru</a>	Newly Seen Domains	April 01, 2020, 09:38am
<a href="#">maska95.ru</a>	Newly Seen Domains	April 01, 2020, 09:36am

# Разные домены под разные города

88.212.232.188

INVESTIGATE

BACK TO TOP

Hosting 68 malicious domains

AS

Prefix	ASN	Network Owner Description
88.212.232.0/21	<a href="#">AS 7979</a>	SERVERS, US 86400
88.212.232.0/21	<a href="#">AS 7979</a>	SERVERS, US 86400

Malicious domains hosted by 88.212.232.188


[bryansk-coronavirus.ru](#) [chelyabinsk-coronavirus.ru](#) [coronavirus-belgorod.ru](#) [coronavirus-ekaterinburg.ru](#) [coronavirus-ekb.ru](#) [coronavirus-habarovsk.ru](#) [coronavirus-kazan.ru](#) [coronavirus-krasnodar.ru](#) [coronavirus-krym.ru](#) [coronavirus-lipetsk.ru](#) [coronavirus-moskva.ru](#) [coronavirus-novosibirsk.ru](#) [coronavirus-omsk.ru](#) [coronavirus-samara.ru](#) [coronavirus-smolensk.ru](#) [coronavirus-sochi.ru](#) [coronavirus-tolyatti.ru](#) [coronavirus-tomsk.ru](#) [coronavirus-tver.ru](#) [coronavirus-vladivostok.ru](#) [coronavirus-volgograd.ru](#) [coronavirusekaterinburg.ru](#) [coronaviruskazan.ru](#) [coronavirusmoskva.ru](#) [coronavirusspb.ru](#) [coronavirusufa.ru](#) [coronavirusvoronezh.ru](#) [coronavirus.ru](#) [covid19-ekaterinburg.ru](#) [covid19-irkutsk.ru](#) [covid19-kazan.ru](#) [covid19-krasnoyarsk.ru](#) [covid19-moskva.ru](#) [covid19-nn.ru](#) [covid19-saratov.ru](#) [covid19-spb.ru](#) [covid19-tambov.ru](#) [covid19-voronezh.ru](#) [ekaterinburg-coronavirus.ru](#) [handmy.ru](#) [kaliningrad-coronavirus.ru](#) [karta-koronavirus.ru](#) [kazan-coronavirus.ru](#) [koronavirus-msk.ru](#) [koronavirus-spb.ru](#) [moscow-coronavirus.ru](#) [perm-coronavirus.ru](#) [ryazan-coronavirus.ru](#) [samara-coronavirus.ru](#) [spb-coronavirus.ru](#) [tyumen-coronavirus.ru](#) [voronezh-coronavirus.ru](#)

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
95	687e7c01c643d4bb5147e6db9c8d526f91ba5...	Win.Trojan.Virut, Win.Worm.Allapple

# Разные домены – одна инфраструктура



**High Risk**

www.covid19-russia.ru Newly Seen Domains Block List

The domain is classified as High Risk due to a combination of high security features.

**Security Categories**  
Newly Seen Domains Malware

**Content Categories**  
-

SECURITY INDICATORS ▾


### DNS Resolution

ADDRESSES	NAME SERVER (NS)	DNS (OTHERS)	
IP Total: 1    TTL(s): 600			
IP	Security Category	TTL (seconds) ▾	First Seen ▾
87.236.16.164		600	March 29, 2020

### WHOIS Record Data

Registrar Name: BEGET-RU    IANAID: -    Last retrieved: -

Created: March, 17, 2020    Updated: -    Expires: March, 17, 2021



Alexey Lukatsky

SEARCH    PATTERN SEARCH

87.236.16.164    INVESTIGATE

Google    VirusTotal

### Details for 87.236.16.164

Hosting 18 malicious domains

AS

Prefix	ASN	Network Owner Description
87.236.16.0/24	AS 198610	BEGET-AS, RU 86400

Malicious domains hosted by 87.236.16.164

[coronavirus-glavnoe.online](#) [coronavirus-glavnoe.ru](#) [coronavirus-world.online](#) [covid19-russia.ru](#) [japaneseknife.ru](#) [koronavirusrf.site](#) [onlyapteka.ru](#) [piterpravodelo.ru](#) [sibirsv.ru](#) [supercleanspb.ru](#) [xn--80al0adb1gd.xn--p1ai](#)

Associated Samples    POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	71cd57b2daded2a807a9c88f8c434a9864e4a...	Document-Word.Trojan.Emotet
95	2b0b6be2cfac38fada59b969e4981ad0107d8f...	Generic.mq.facff2734626356b,

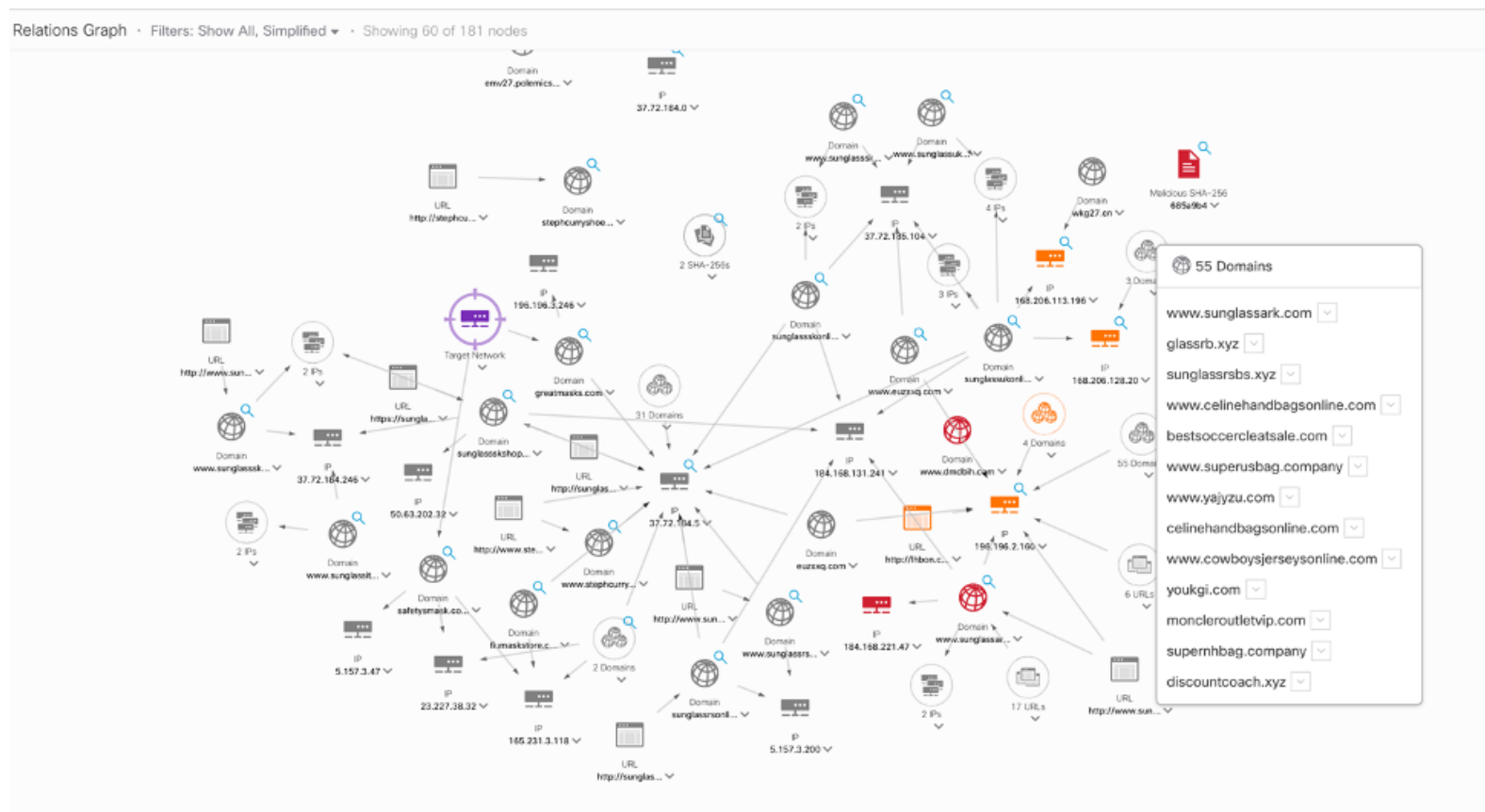
# Интересная AS 197695

- telegramm1.ru
- awitoo.ru и avitio.ru
- Проект «Голос»
- Facebook
- Amazon
- iCloud + сервисы Apple
- Очкарик

The screenshot displays the Cisco Threat Response Investigate interface. The main search bar contains 'telegramm1.ru'. Below it, a 'Relations Graph' shows a central node for 'Malicious Domain telegramm1.ru' connected to various entities: IP 185.250.207.30, IP 89.236.221.8, IP 185.209.22.222, and two URLs: 'http://telega...' and 'https://telegr...'. To the right, the 'Sightings Timeline' for 'My Environment' shows 0 sightings. Below that, the 'Observables' section for 'telegramm1.ru' shows 2 sightings (first on Sep 15, 2018, last on Jan 24, 2020) and a table of judgements.

Module	Disposition	Expiration
VirusTotal	Malicious	in 2 months
Umbrella	Malicious	in a month

# Не только маски и тесты от коронавируса



# В качестве заключения

- 1 Анализ DNS позволяет выявлять не только единичные вредоносные ресурсы
- 2 Необходимо накопление данных о доменах
- 3 Помимо анализа данных о доменах, необходимо анализировать связи
- 4 Обычно даже только по AS можно судить о вредоносности домена
- 5 Анализ DNS позволяет предсказывать многие атаки
- 6 AS и IP часто используются под разные, но вредоносные цели
- 7 Неочевидная и небыстрая процедура делегирования вредоносных доменов
- 8 Существующие базы данных о DNS/IP/AS – частные и, преимущественно, зарубежные



# Вопросы?





[alukatsk@cisco.com](mailto:alukatsk@cisco.com)

