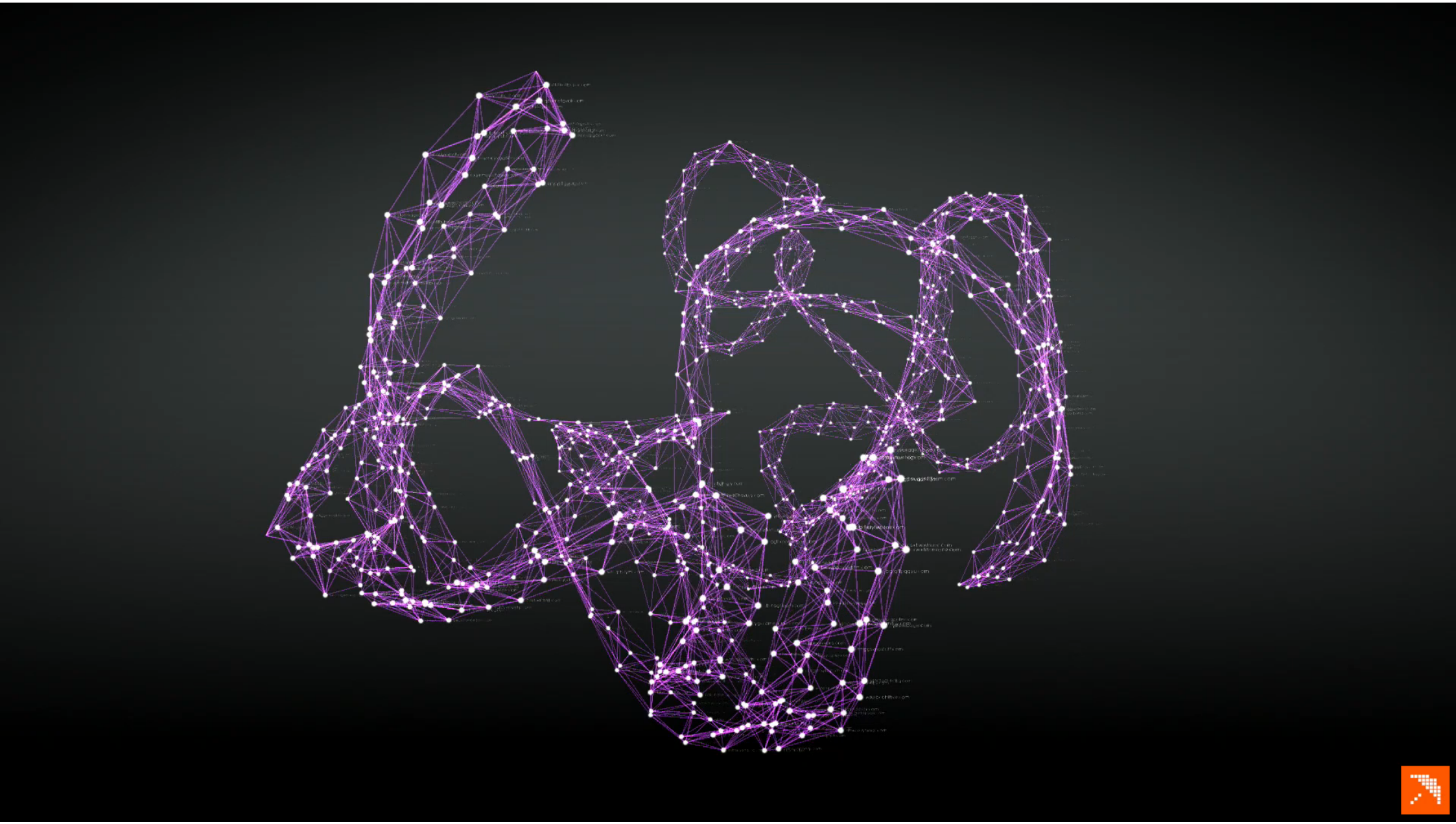
Как ловить кибермафию с помощью DNS

И попутно повышать доверие к Президенту России

08 сентября 2020



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?

Анализ энтропии

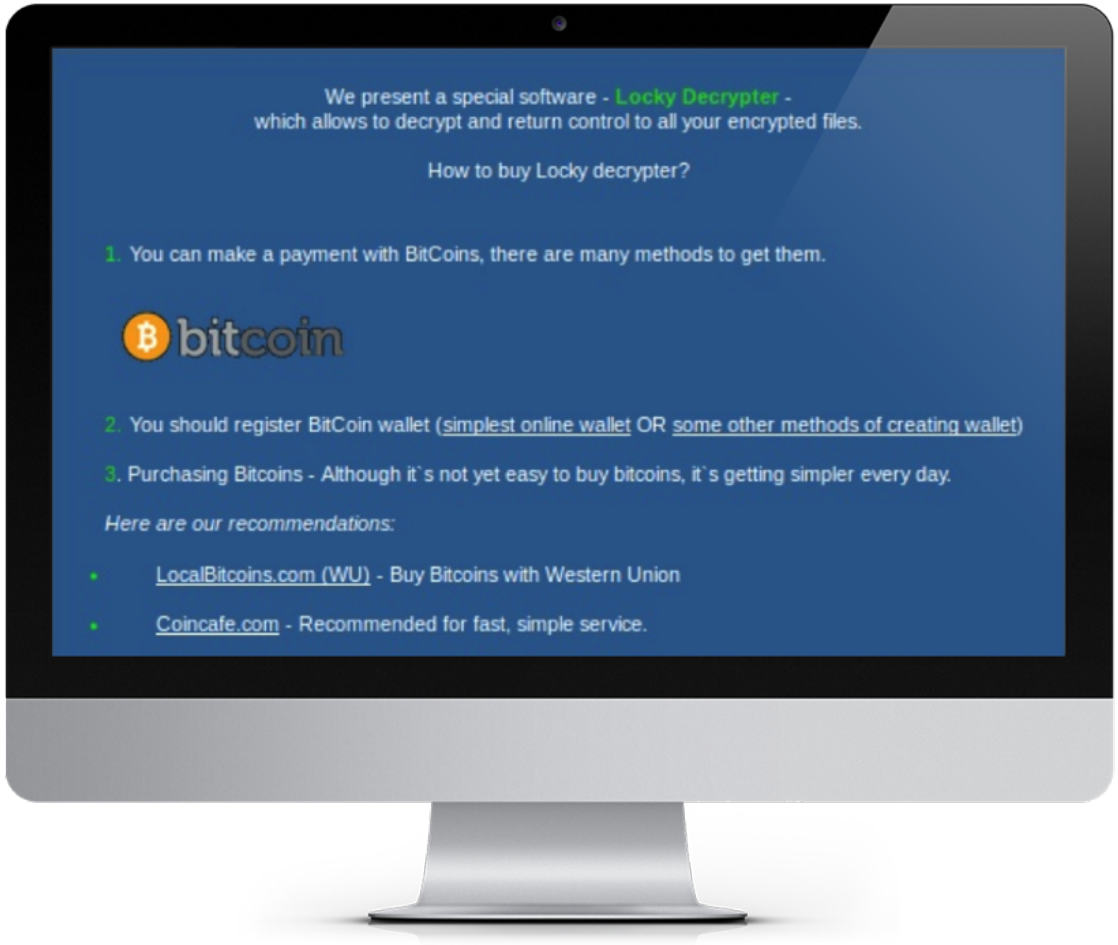
Не выглядит ли распределение символов случайным?

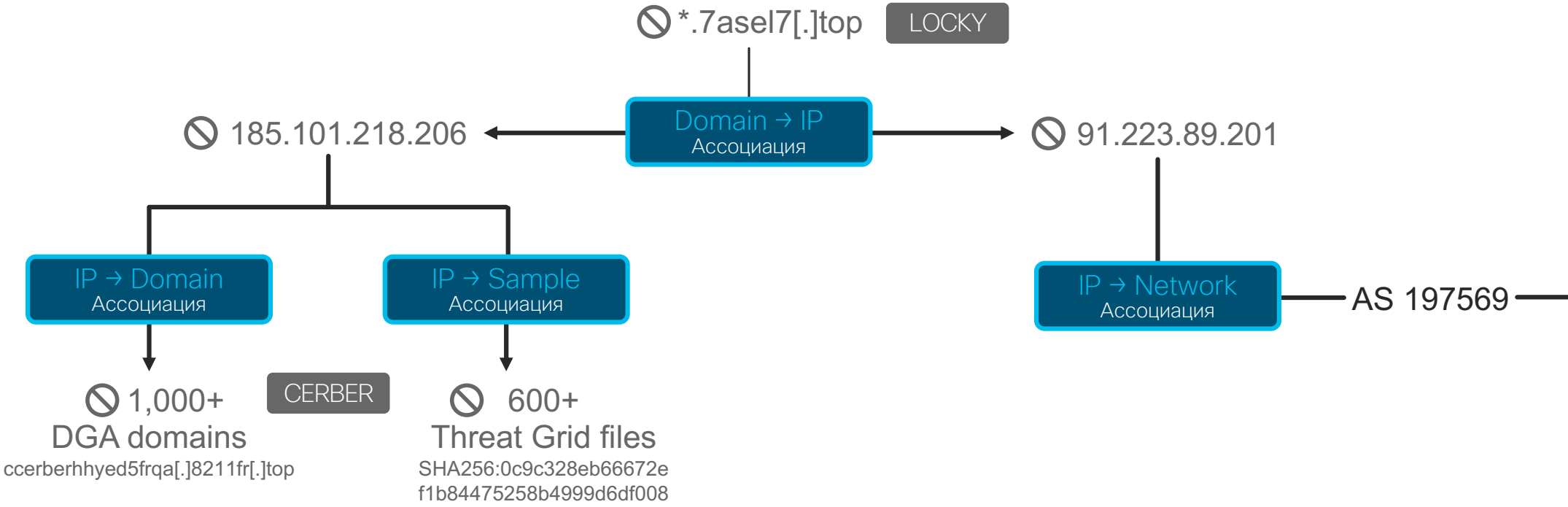
Что можно вытащить из DNS-трафика: уровень III

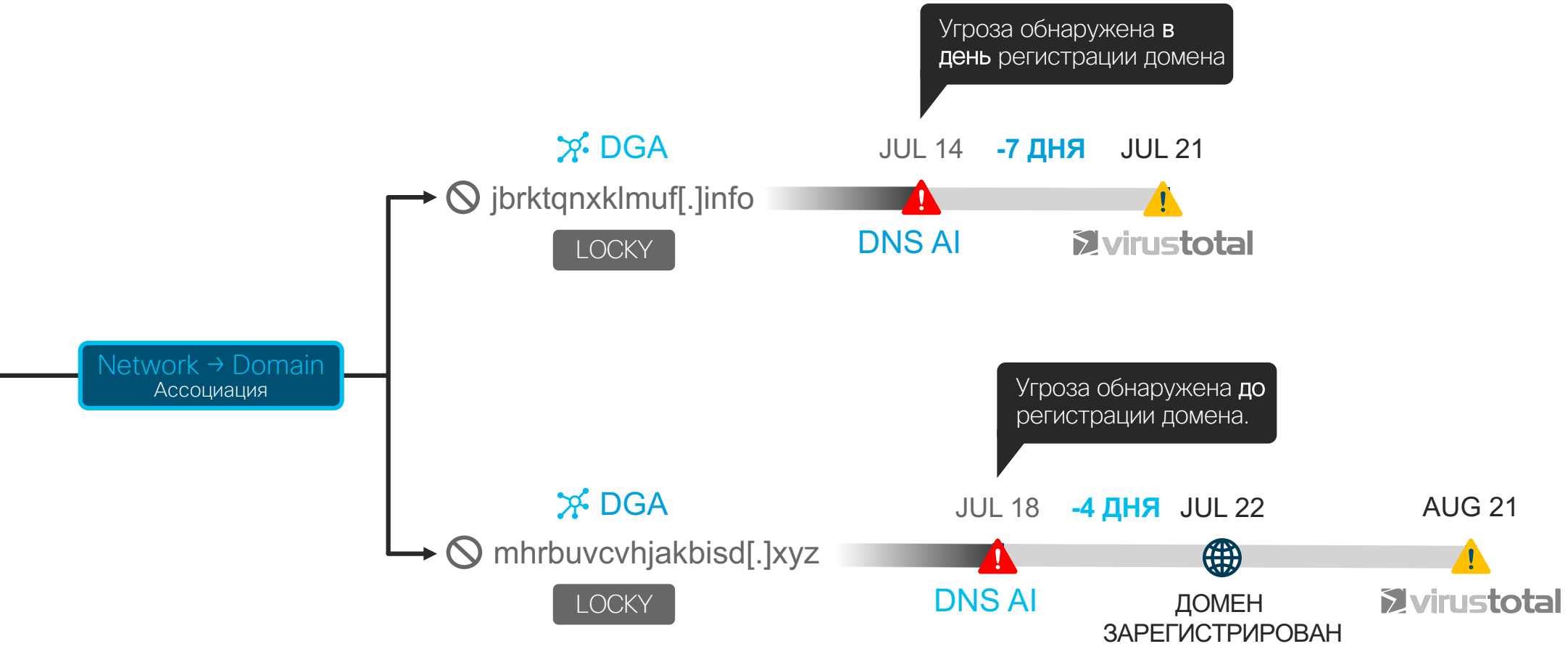
- Энтропия / распределение символов в FQDN
- Взаимосвязи между доменами / IP-адресами / e-mail владельцев / автономными системами (ASN)
- Вредоносная активность, связанная с доменом / IP / e-mail владельцев / автономными системами (ASN)

Знакомо ли вам имя Locky?

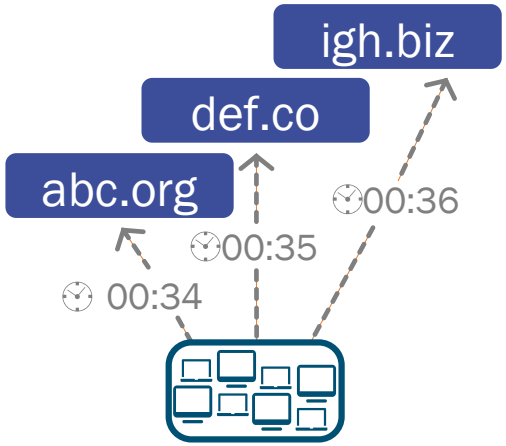
- Через вложение Email в фишинговой рассылке
- Шифрует и переименовывает файлы с .locky расширением
- Примерно 90,000 жертв в день
- Выкуп порядка 0.5 – 1.0 BTC (1 BTC ~ $601 US)
- Связан с операторами кампании Dridex





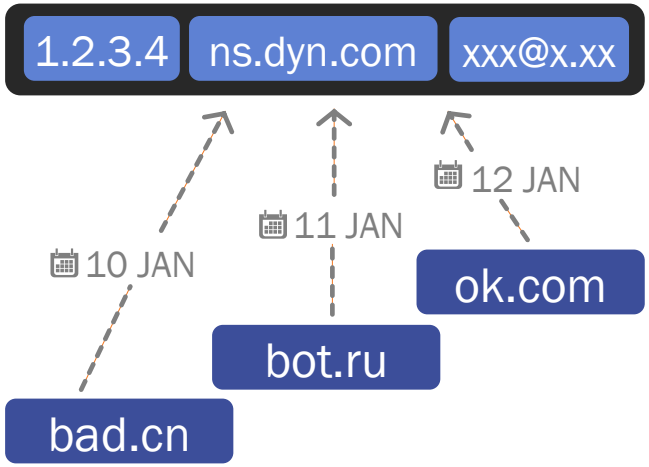


Корреляция DNS, WHOIS и BGP



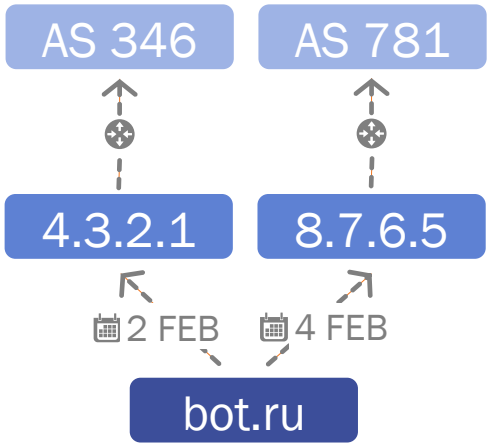
СОВМЕСТНЫЕ ЗАПРОСЫ

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

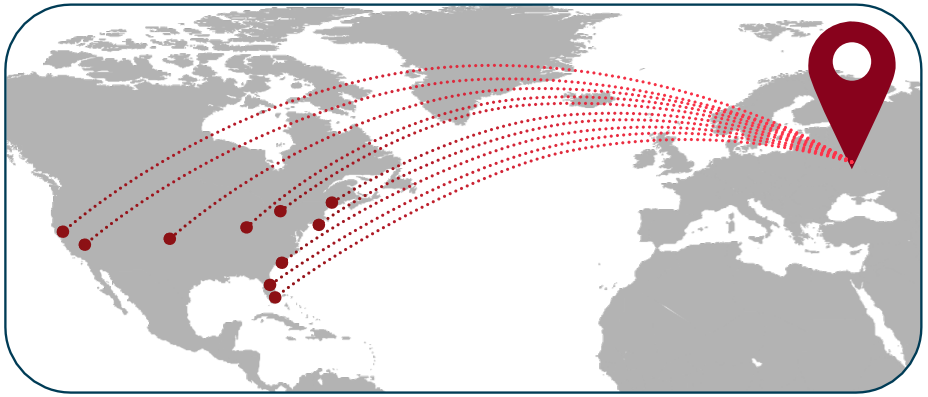
Геолокационный анализ IP

Хостится в более чем 28+ странах

ХОСТ ИНФРАСТРУКТУРА

Расположение сервера
IP адреса, связанные с доменом

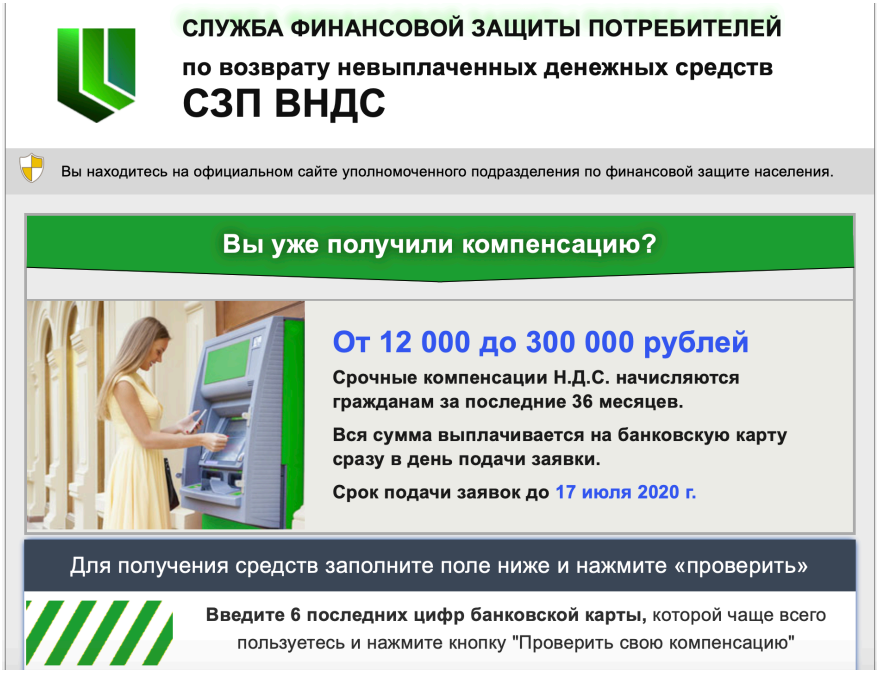
Только заказчики из US связываются с .RU TLD

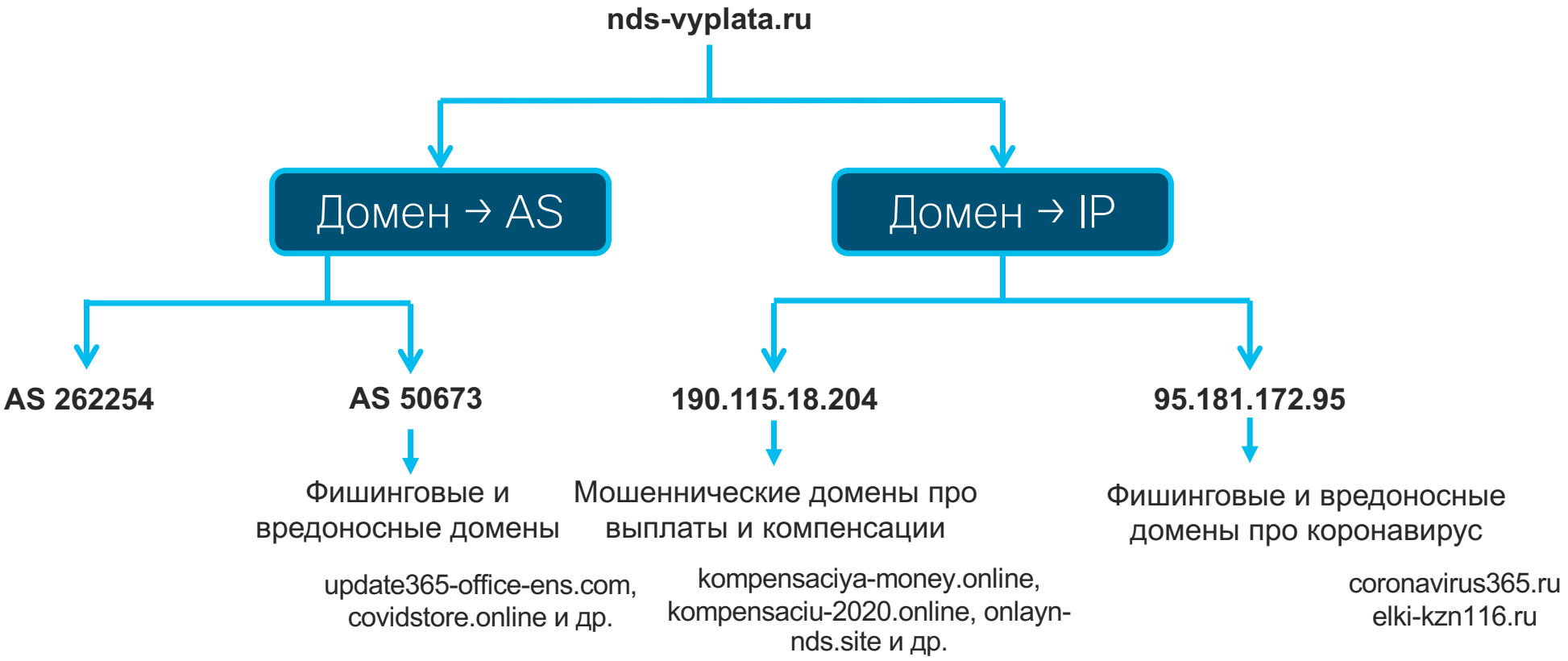


DNS ЗАПРОШИВАЮЩИЕ ХОСТЫ

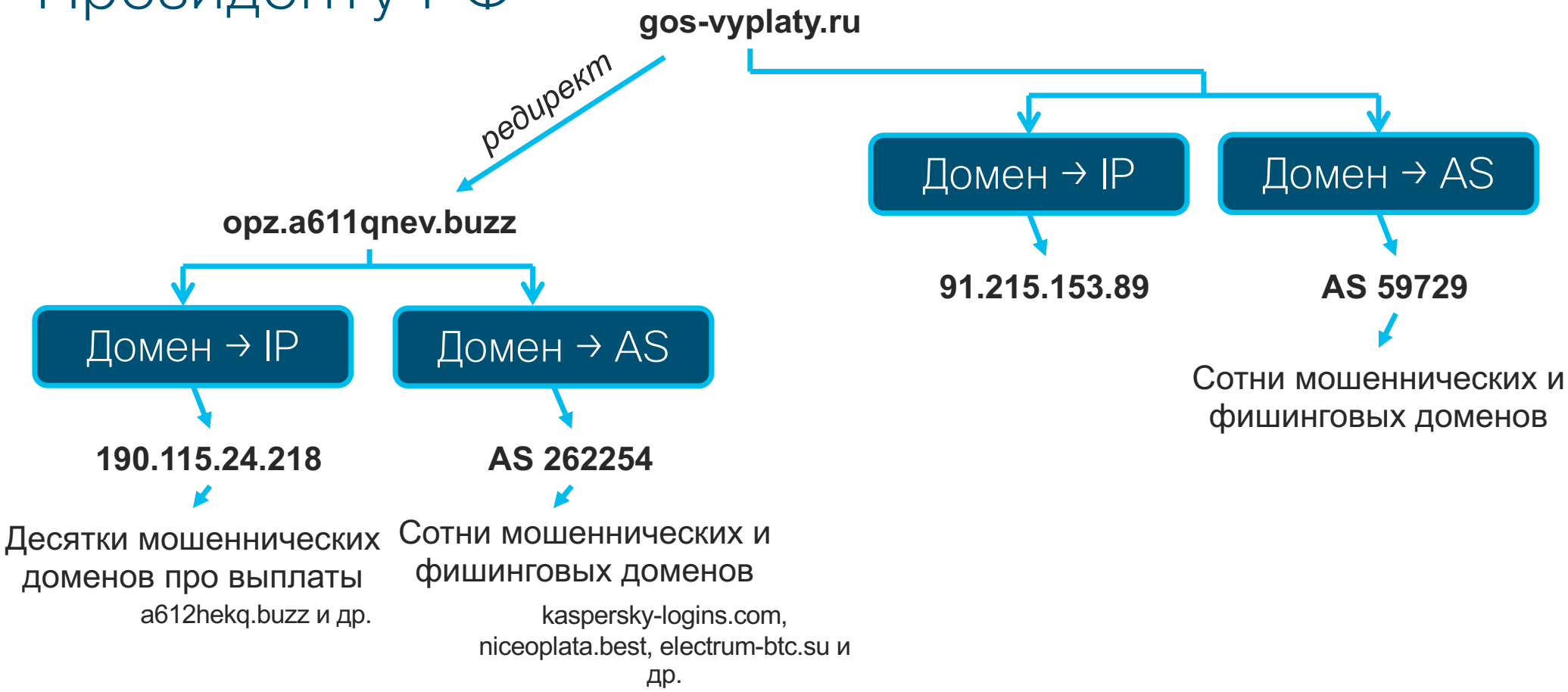
Расположение сетевые и вне-сетевые
IP адреса запрашивающих домен

Финансовая помощь от государства?..



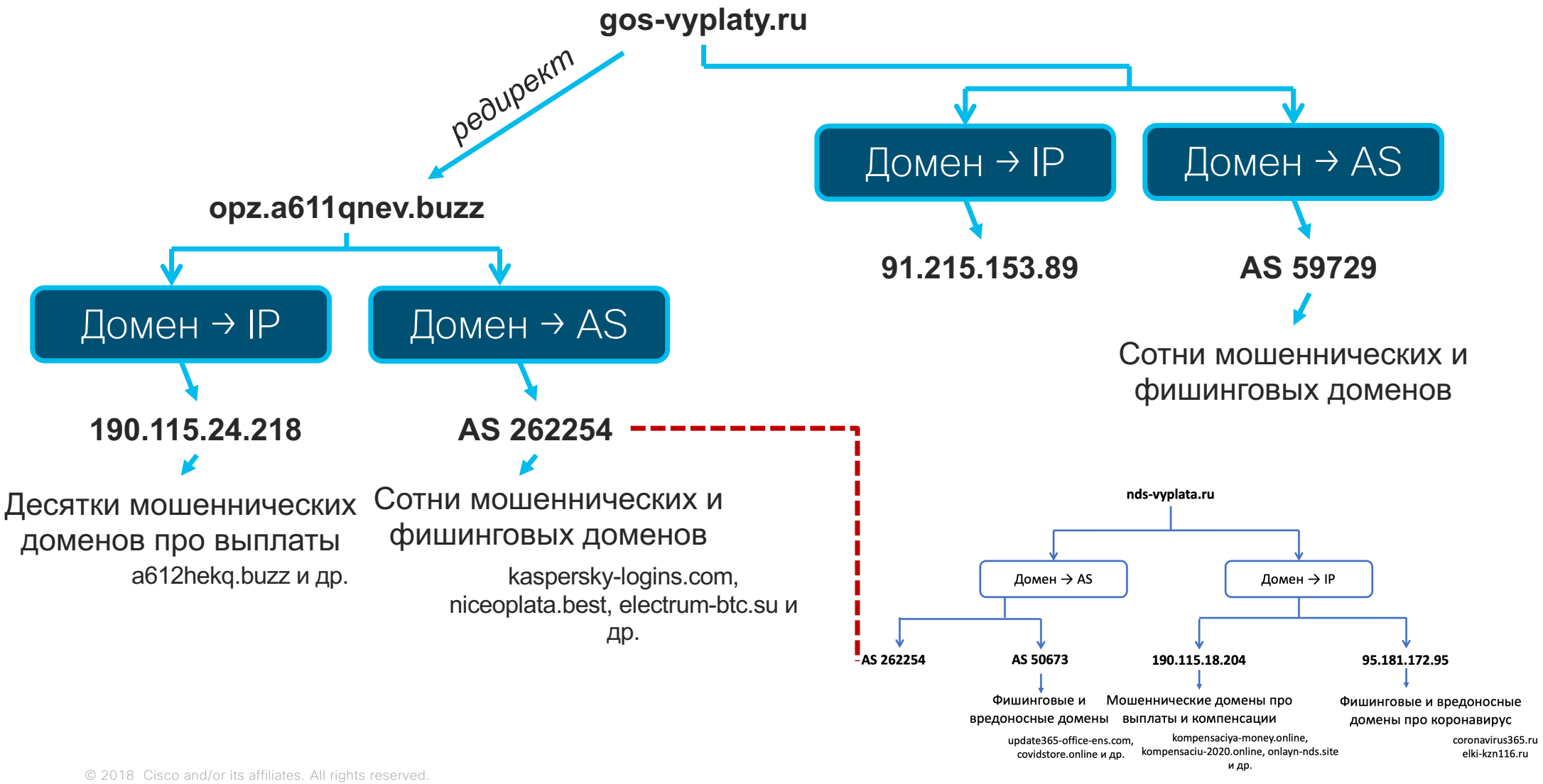


Как мошенники подрывали доверие к Президенту РФ



Заодно атаковались и все популярные антивирусы

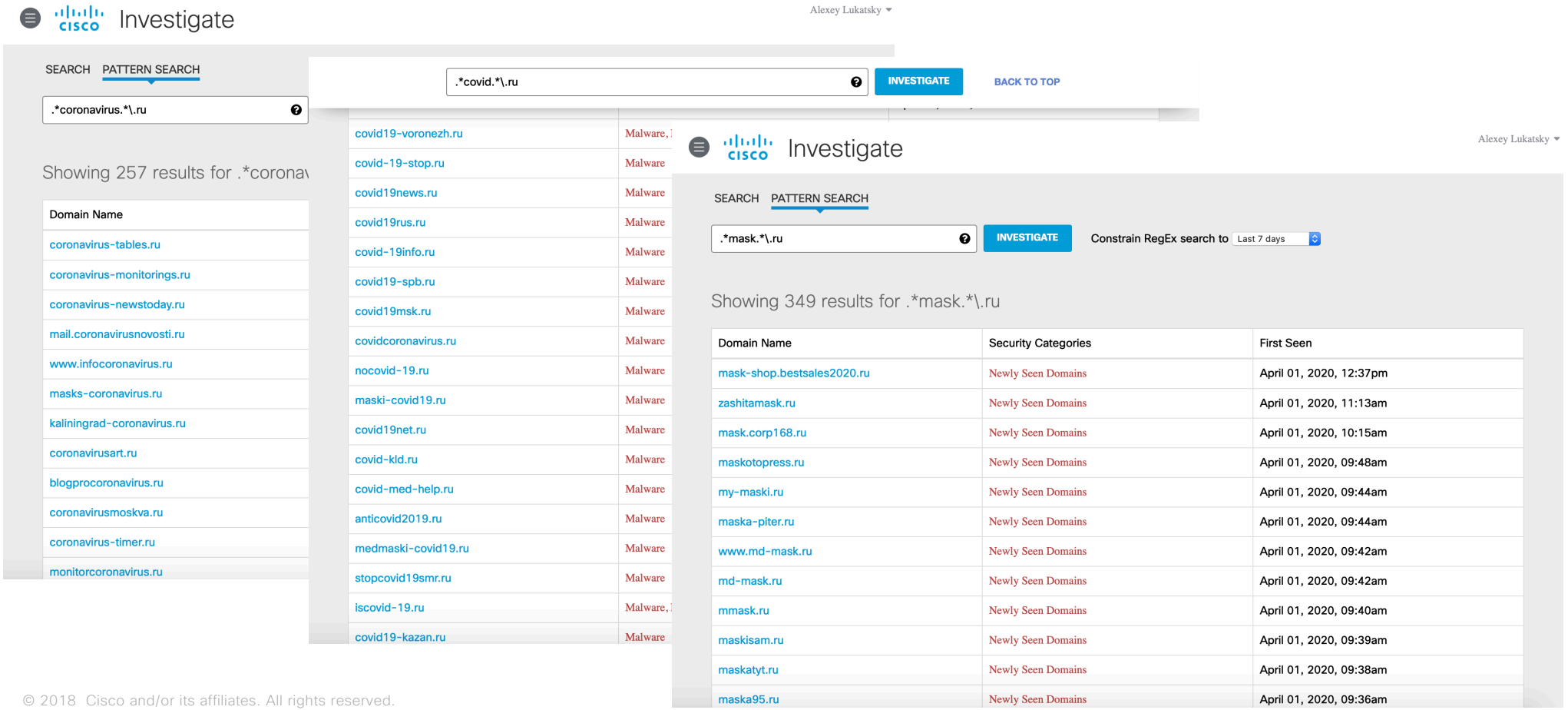
goattlogin.com bitdefender-centrals.com
bitdefender-centralx.com bitdefender-loginn.com
iwebrootcomsafe.com kaspersky-loginn.com
kaspersky-logins.com kasperskylogins.com
malwarebyteslogins.com malwarebytesloginz.com
mcafeecom-activatez.com mcafeelogins.com
mcafeeloginz.com myavastz.com
mynortoncomnu16.com 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 trendmicrodownloadd.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



Вспомним про коронавирус

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

Сотни «горячих» доменов



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	AS 7979	SERVERS, US 86400
88.212.232.0/21	AS 7979	SERVERS, US 86400

Malicious domains hosted by 88.212.232.188

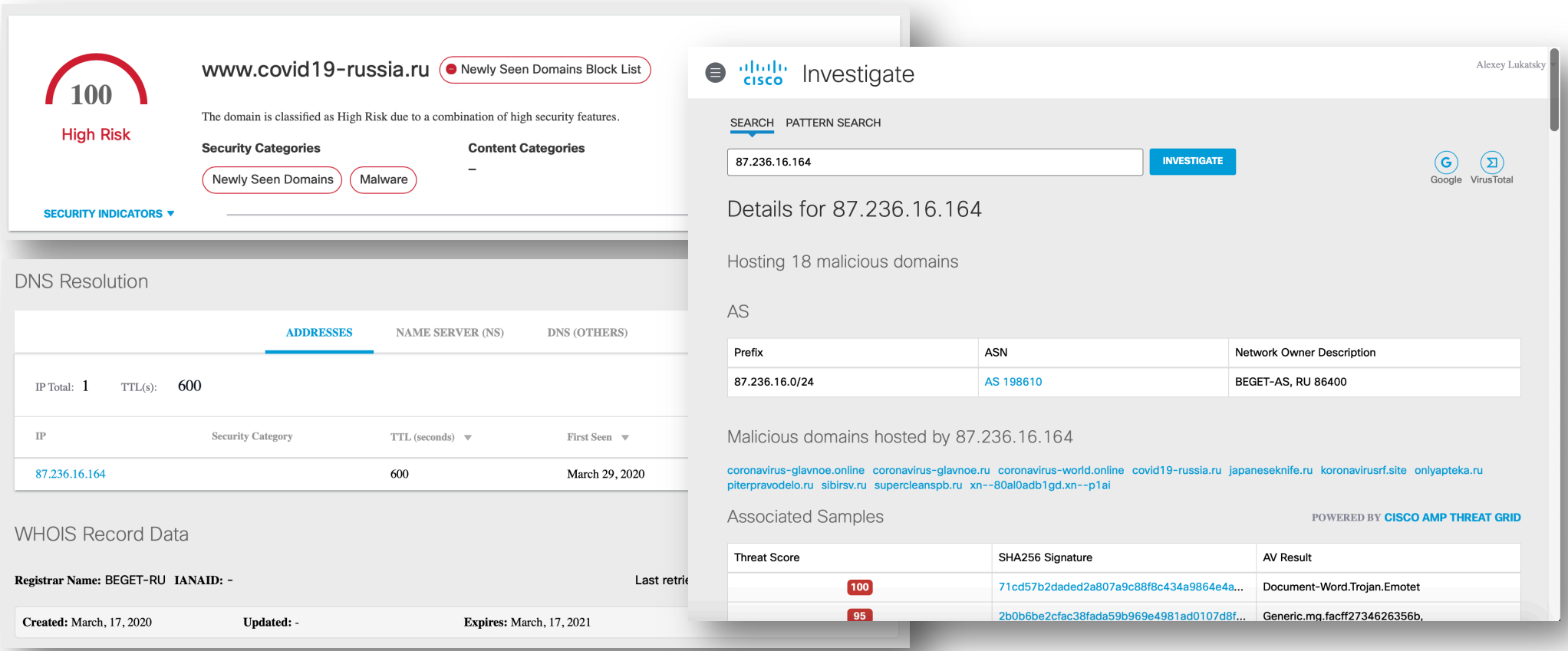
bryansk-coronavirus.ru chelyabinsk-coronavirus.ru coronavirus-belgorod.ru coronavirus-ekaterinburg.ru coronavirus-ekb.ru coronavirus-habarovsk.ru coronavirus-kazan.ru coronavirus-krasnodar.ru coronavirus-krym.ru coronavirus-lipetsk.ru coronavirus-moskva.ru coronavirus-novosibirsk.ru coronavirus-omsk.ru 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 coronawirus.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

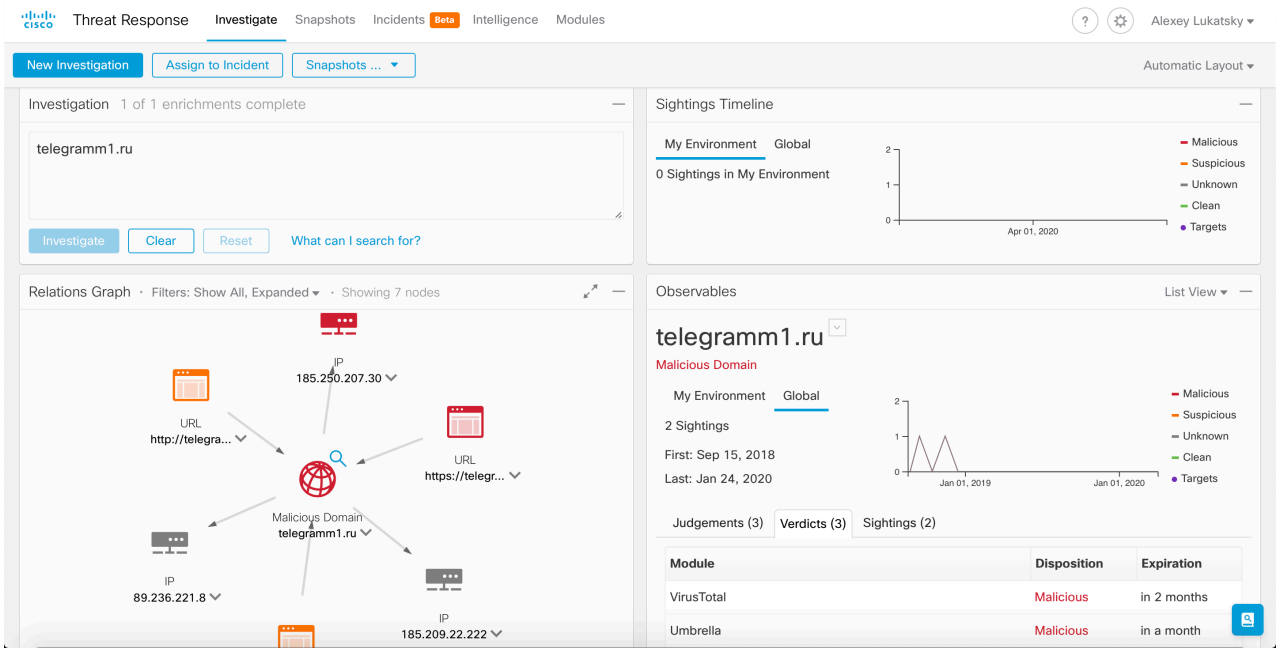
Threat Score	SHA256 Signature	AV Result
95	687e7c01c643d4bb5147e6db9c8d526f91ba5...	Win.Trojan.Virut, Win.Worm.Allaple

Разные домены – одна инфраструктура

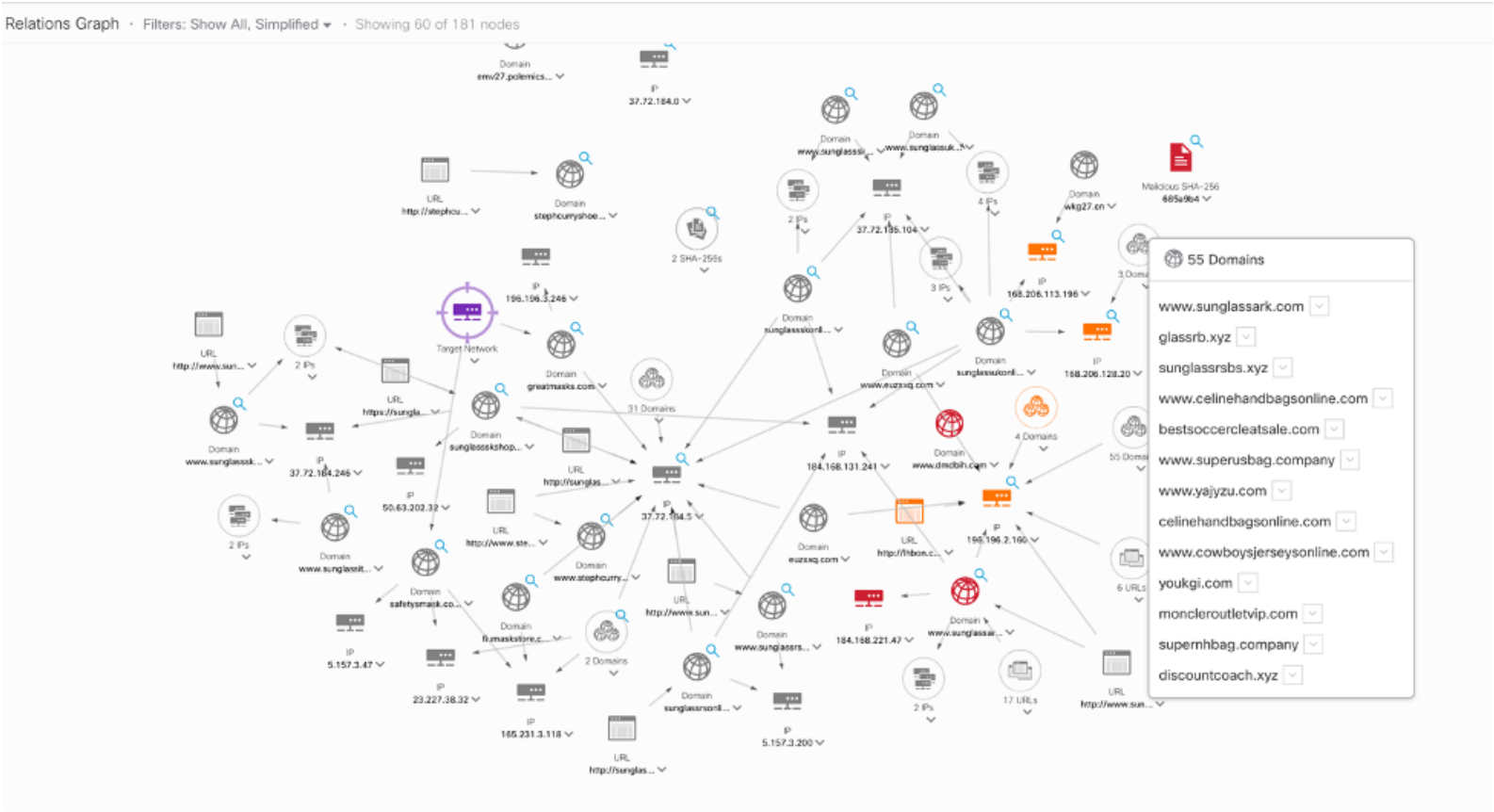


Интересная AS 197695

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



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 разделегирования вредоносных доменов
8. Существующие базы данных о DNS/IP/AS – частные и, преимущественно, зарубежные

Вопросы?

alukatsk@cisco.com