Доржу Ондар
brozerk@mail.ru
+7(771)135-66-17

Задание 1

kaspi.kz	IN	A	**ip** = 194.187.245.10	32 сек.

Связали домен kaspi.kz с IP-адресом 194.187.245.10

kaspi.kz	IN	NS	**target** = ns.kaspi.kz	300 сек.
kaspi.kz	IN	NS	**target** = ns2.bc.kz	300 сек.
kaspi.kz	IN	NS	**target** = ns.bc.kz	300 сек.
kaspi.kz	IN	NS	**target** = ns2.kaspi.kz	300 сек.

Указываются имена DNS-серверов ns.kaspi.kz, ns2.bc.kz, ns.bc.kz и ns2.kaspi.kz, которые хранят зону домена kaspi.kz и предоставляют информацию о ресурсных записях других DNS-серверов

kaspi.kz	IN	SOA	**mname** = ns.bc.kz **rname** = telecomdev.kaspi.kz **serial** = 2018122633 **refresh** = 600 **retry** = 150 **expire** = 28800 **minimum-ttl** = 300	300 сек.

SOA-запись, где хранится следующая информация:

1) mname = ns.bc.kz - отсылка к DNS-серверу, где хранятся другие ресурсные записи
2) rname = telecomdev.kaspi.kz - контактный адрес лица, который отвечает за администрирование файла зоны
3) serial = 2018122633 - серийный номер файла зоны
4) refresh = 600 - время, отведённое под запрос данных от вторичного DNS-сервера к первичному. Если получен ответ, что Serial number изменён, сведения на вторичном сервере в обязательном порядке обновляются
5) retry = 150 - время, отведённое под обновление данных, если в первый раз этого не произошло
6) expire = 28800 - промежуток времени, когда сведения о зоне могут применяться на вторичном сервере. Когда время заканчивается, но данные при этом не успевают обновиться, запросы о данной зоне перестают обрабатываться
7) minimum-ttl = 300 - время хранения в кэше информации о зоне

kaspi.kz	IN	MX	**pri** = 10 **target** = bmss-02d.kaspi.kz	300 сек.
kaspi.kz	IN	MX	**pri** = 10 **target** = bmss-01d.kaspi.kz	300 сек.

Для домена kaspi.kz указаны 2 почтовых сервера с одинаковым приоритетом, то есть основного и второстепенного нет, сервер выбирается случайным образом

kaspi.kz	IN	TXT	**txt** = v=spf1 mx a:bmss-05d.kaspi.kz a:bmss-06d.kaspi.kz a:bmss-07d.kaspi.kz a:bmss-08d.kaspi.kz -all **entries** =	1742 сек.

Это SPF-запись, содержащая информацию о списке серверов, которые имеют право отправлять письма от имени заданного домена.

1) v=spf1 — версия используемой записи SPF
2) mx - разрешает приём почты, если отправляющий сервер указан в одной из записей MX для домена
3) a:bmss-05d.kaspi.kz a:bmss-06d.kaspi.kz a:bmss-07d.kaspi.kz a:bmss-08d.kaspi.kz - задает разрешенные почтовые серверы на основе доменного имени
4) -all - если запись SPF содержит элемент -all, серверы получателей могут отклонять письма от отправителей, которые не включены в запись SPF

kaspi.kz	IN	TXT	**txt** = google-site-verification=x-9S3SCWGLPV4449a3riJHAdsBWLD44A8YGrmESd0gA **entries** =	1742 сек.
kaspi.kz	IN	TXT	**txt** = cisco-ci-domain-verification=6d7c1ed23f91f130f16c4c55c2dbcf542b5af5d1dcab6ef6b63a0503ab963359 **entries** =	1742 сек.
kaspi.kz	IN	TXT	**txt** = MS=9238427DD52EC9DDBA9DD9CB62F3FA550E585A12 **entries** =	1742 сек.
kaspi.kz	IN	TXT	**txt** = amazonses:U0XCDK9kpTUP+WOfqxBZEII+O42o2T4ocDhpmeax4BA= **entries** =	1742 сек.

Подтверждение владения доменом

10.245.187.194.in-addr.arpa	IN	PTR	kaspi.kz	

Обратная DNS-запись, которая связывает IP-адрес сервера с его доменом

Задание 2

Received содержит информацию о маршруте сообщения, пройденных серверах, дату и время отправки.

Received-SPF говорит, что проверка SPF была пройдена.

В Authentication-Results написано, что проверки SPF, DKIM и DMARC пройдены.

Message-ID - MN2PR10MB4221A02215806FE944C42765B3460@MN2PR10MB4221.namprd10.prod.outlook.com

Created at - 29.11.2019, 14:40:40 GMT+6

From: "Djenish, Elnura" <**elndjeni@visa.com**>

To: "Djenish, Elnura" <**elndjeni@visa.com**>

Subject: PFD-19-052-Visa Security Alert - Phishing Campaign Linked to Silence Group

Задание 3

С IP-адресов 10.1.22.33:63303 и 10.1.22.33:63322 идет подключение к IP-адресам 34.202.85.54:80 и 54.164.20.117:80, которые являются CNC-серверами - серверами, с помощью которых злоумышленник способен, например, контролировать ботнет и отдавать команды его участникам, управлять шпионским ПО и т.п. Уведомление говорит, что трафик содержит вредоносный код Win.Trojan.Banker - система обнаружила подключение к злонамеренному программному обеспечению по типу банковского трояна.

Банковские трояны могут перехватывать данные, вводимые пользователем — логины, пароли, номера карт и др. Также они способны открывать злоумышленникам доступ к системе, поэтому после обнаружения такого подключения нужно изолировать зараженные узлы, провести проверку систем и обезопасить сети и компьютеры.

Задание 4

#1 NGINX

IP-адрес источника — 10.1.2.3

IP-адрес назначения — 109.166.59.44

Дата и время - 17/Nov/2019:03:17:59 +0600

Запрос - GET /shop-ext/suggestions/?i=productDetails&m=true&t=IP&pi=14701657&u=3729495 HTTP/1.1

Статус запроса — 200

Реферер - https://kaspi.kz/shop/p/gerbor-vusher-reg1w2d2s-13-9-l-p-nimfea-al-ba-belyi-gljanets-14701657/?c=551010000

Информация о браузере, операционной системе и устройстве пользователя - 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

Время ответа сервера — 0.009

Время передачи данных — 0.008

IP-адрес и порт сервера - 10.2.3.4:9001

#2 Mail Log

Дата и время - <22>Dec 04 12:22:00

Событие - New SMTP ICID 11444342

IP-адрес источника — 172.1.2.3

IP-адрес назначения — 162.141.46.147

Проверка обратного DNS - s2.kipersam.art

Подтверждение — yes

#3 Proxy Server

Имя пользователя - petrov_123

Дата и время - Dec 4 12:21:59

Событие - LEEF:1.0|PRXName|Web Gateway|7.8.2.11.0|0

IP-адрес источника — 10.7.8.9

IP-адрес назначения — 149.154.167.99

Информация о браузере, операционной системе и устройстве пользователя - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36

HTTP-статус: 200

URL - https://venus.web.telegram.org/apiw1

#3 ASA

Дата и время - Dec 04 2019 12:21:59

IP-адрес источника — 90.143.47.21/42968

IP-адрес назначения — 194.187.247.147/443

#4 Mail Log

Дата и время - Dec 04 12:22:00

ICID — 11444342

ACCEPT

SG SUSPECTLIST

country Germany и Mongolia - страна отправителя

#5 FW

IP-адрес устройства — 10.10.10.1

Длина записи в байтах — 258

IP-адрес отправителя — 172.2.3.4

P-адрес получателя — 172.2.3.5

Имя файла — online_126657052_3.pdf

SHA-хеш файла - CD22437892392E03BF5375B597AA77DE6F0E5D9F26B1832339B79DA19F050BF7