Задания.

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

NIC Handle.............: PS-KZ-1444738125

Name...................: Evgeniy

Phone Number...........: +7 727 2585955

Fax Number.............: +7 727 2585955

Email Address..........: [domains@kaspibank.kz](mailto:domains@kaspibank.kz)

Nameserver in listed order

Primary server.........: ns.bc.kz Primary ip address.....: 194.187.247.138

Secondary server.......: ns2.bc.kz Secondary ip address...: 194.187.246.238

Secondary server.......: ns2.kaspi.kz Secondary ip address...: 194.187.244.250

Secondary server.......: ns.kaspi.kz Secondary ip address...: 194.187.245.19

"name": "Kaspi Bank",

"organization": "Kaspi Bank",

"street": "ul. Nauryzbay batyra, 154 \"A\"",

"city": "Almaty",

"state": "Almaty",

"postalCode": "050013",

"country": "KAZAKHSTAN"

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

SOA TTL – это промежуток времени, в рамках которого кэшируется информация,

предназначенная для передачи через DNS-серверы.

MNAME — это отсылка к DNS-серверам, где хранятся другие ресурсные записи.

Hostname или RNAME — электронная почта администратора зоны.

Serial number — серийный номер файла зоны. При любых изменений его значение повышается. Это сигнал вторичным серверам о том, что пора обновлять данные.

Refresh — 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.

Retry — время, отведённое под обновление данных, если в первый раз этого не произошло.

Expire — 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.

Minimum TTL — время хранения в кэше информации о зоне

|  |  |
| --- | --- |
| MX | **pri** = 10 **target** = bmss-02d.kaspi.kz |

Приоритет 10

Имя хоста bmss-02d.kaspi.kz

**тип** DNS-записи, предназначенный для маршрутизации электронной почты

|  |  |
| --- | --- |
| MX | **pri** = 10 **target** = bmss-01d.kaspi.kz |

Приоритет 10

Имя хоста bmss-01d.kaspi.kz

|  |  |
| --- | --- |
| TXT | **txt** = MS=9238427DD52EC9DDBA9DD9CB62F3FA550E585A12 **entries** = |

это TXT-запись DNS, которая сообщает почтовым серверам, принимать или не принимать сообщения с данного IP-адреса

|  |  |
| --- | --- |
| PTR | kaspi.kz |

тип DNS-записи, которая сопоставляет IP-адрес с доменом

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Mail From:** | elndjeni@visa.com | **Mail To:** | Djenish, Elnura elndjeni@visa.com |
| **Mail From Name:** | Djenish, Elnura | **Reply To:** | MN2PR10MB4077A18A3D6553004AADD2E5D84D0@MN2PR10MB4077.namprd10.prod.outlook.com |

### Message Details

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject:** | PFD-19-052-Visa Secur ity Alert - Phishing Campaign Linked to Si lence | **Content-Type:** | multipart/mixed |
| **Date:** | Fri, 29 Nov 2019 08:40:40 +0000 | **UTC Date** | Fri Nov 29 08:40:40 2019 |
| **MessageID:** | MN2PR10MB4221A02215806FE944C42765B3460@MN2PR10MB422 1.namprd10.prod.outlook.com | |

### Message Transfer Agent (MTA) - Transfer Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mail Server From:** |  | | **Mail Server To:** |  | |
| [**Mail Server From IP:**](https://en.wikipedia.org/wiki/IP_address) |  | | [**Mail Server To IP:**](https://en.wikipedia.org/wiki/IP_address) |  | |
| **Mail Country From:** |  | https://www.google.com/maps/search/,/@54.6138286,83.8092801,1066796m/data=!3m2!1e3!4b1 | **Mail Country To:** |  | https://www.google.com/maps/search/,/@54.6138286,83.8092801,1066796m/data=!3m2!1e3!4b1 |
| [**AS Name From:**](http://en.wikipedia.org/wiki/Autonomous_System_%28Internet%29) |  | | [**AS Name To:**](http://en.wikipedia.org/wiki/Autonomous_System_%28Internet%29) |  | |
| [**AS Number From:**](http://en.wikipedia.org/wiki/Autonomous_System_%28Internet%29) |  | | [**AS Number To:**](http://en.wikipedia.org/wiki/Autonomous_System_%28Internet%29) |  | |
| **Distance (All Hops/Summary):** | 0/ KM | | **Hops (All/Public):** | 3 / | |
| [**MTA Encryption**](http://en.wikipedia.org/wiki/STARTTLS) | Good (\*) | | **Delivery Time:** | 0 days, 0 hours, 0 min, 0 sec | |
| **Your IP:** | 46.34.193.85 | | **Your GeoLoc:** | [Lat:52.9382 Lon:70.1895](http://maps.google.com/?q=52.9382,70.1895&t=k) | |

### Spam Scoring Details

|  |  |
| --- | --- |
| **Score** | **Spam Description** |

|  |  |
| --- | --- |
| **Total Score (Max:5)** | **Spamassassin prediction** |
| 0 | **No Spam = Good!** |

### Hop Details

|  |  |  |  |
| --- | --- | --- | --- |
| **Hop 1/3** | **Internal Mail Routing** | | |
| **By MTA** | exch3.localhost | **By IP** | UNKNOWN (\*) |
| **From MTA** | exch3.localhost | **From IP** | 10.1.1.1 (\*) |
| **Date MTA** | Fri, 29 Nov 2019 14:41:31 +0600 | [**UTC Date**](http://en.wikipedia.org/wiki/Coordinated_Universal_Time) | Fri Nov 29 08:41:31 2019 |
| [**Epoch**](http://en.wikipedia.org/wiki/Unix_time) | 1575038491 | **UTC Epoch** | 1575016891 |
| [**MTA Encryption**](http://en.wikipedia.org/wiki/STARTTLS) | **TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384** | | |
| [**MTA (Guess)**](http://en.wikipedia.org/wiki/Message_transfer_agent) | Microsoft SMTP Server | | |
| **RAW** | Received: from exch3.localhost (10.1.1.1) by exch3.localhost (10.1.1.1 with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.1.1147.3 via Mailbox Transport; Fri, 29 Nov 2019 14:41:31 +0600 | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hop 2/3** | **Internal Mail Routing** | | | | |
| **By MTA** | exch3.localhost | **By IP** | | UNKNOWN (\*) | |
| **From MTA** | exch3.localhost | **From IP** | | 10.1.1.1 (\*) | |
| **Date MTA** | Fri, 29 Nov 2019 14:41:31 +0600 | [**UTC Date**](http://en.wikipedia.org/wiki/Coordinated_Universal_Time) | | Fri Nov 29 08:41:31 2019 | |
| [**Epoch**](http://en.wikipedia.org/wiki/Unix_time) | 1575038491 | **UTC Epoch** | | 1575016891 | |
| [**MTA Encryption**](http://en.wikipedia.org/wiki/STARTTLS) | **TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384** | | | | |
| [**MTA (Guess)**](http://en.wikipedia.org/wiki/Message_transfer_agent) | Microsoft SMTP Server | | | | |
| **RAW** | Received: from exch3.localhost (10.1.1.1) by exch3.localhost (10.17.160.57) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.1.1147.3; Fri, 29 Nov 2019 14:41:31 +0600 | | | | |
| **Hop 3/3** | Internal Mail Routing | | | | |
| **By MTA** | exch2.localhost | | **By IP** | | UNKNOWN (\*) |
| **From MTA** | nodename.kaspi.kz | | **From IP** | | 10.1.1.2 (\*) |
| **Date MTA** | Fri, 29 Nov 2019 14:41:31 +0600 | | [**UTC Date**](http://en.wikipedia.org/wiki/Coordinated_Universal_Time) | | Fri Nov 29 08:41:31 2019 |
| [**Epoch**](http://en.wikipedia.org/wiki/Unix_time) | 1575038491 | | **UTC Epoch** | | 1575016891 |
| [**MTA Encryption**](http://en.wikipedia.org/wiki/STARTTLS) | **TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256** | | | | |
| [**MTA (Guess)**](http://en.wikipedia.org/wiki/Message_transfer_agent) | Microsoft SMTP Server | | | | |
| **RAW** | Received: from nodename.kaspi.kz (10.1.1.2) by exch2.localhost(10.1.1.2) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256) id 15.1.1147.3 via Frontend Transport; Fri, 29 Nov 2019 14:41:31 +0600 Received-SPF: Pass (bmss-01d.kaspi.kz: domain of elndjeni@visa.com designates 198.241.159.88 as permitted sender) identity=mailfrom; client-ip=198.241.159.88; receiver=bmss-01d.kaspi.kz; envelope-from="elndjeni@visa.com"; x-sender="elndjeni@visa.com"; x-conformance=spf\_only; x-record-type="v=spf1"; x-record-text="v=spf1 ip4:198.241.162.0/24 ip4:198.241.168.0/24 ip4:198.241.159.0/24 ip4:72.46.234.0/24 ip4:66.185.181.0/24 ip4:198.241.174.0/24 ip4:74.116.91.0/24 ip4:198.80.42.3 ip4:69.20.125.232 ip4:198.241.175.106 ip4:216.251.253.98 ip4:67.208.216.61 ip4:198.247.174.175 ip4:67.220.120.24 ip4:66.185.186.2 ip4:198.241.171.12 ip4:204.75.142.27 ip4:66.165.175.189 ip4:67.192.139.34 ip4:67.192.157.83 ip4:174.143.100.191 ip4:198.241.158.43 ip4:128.242.118.200 ip4:198.241.207.0/24 ip4:198.241.206.0/24 ~all" Authentication-Results: bmss-01d.kaspi.kz; spf=Pass smtp.mailfrom=elndjeni@visa.com; dkim=pass (signature verified) header.i=@visa.com; dmarc=pass (p=quarantine dis=none) d=visa.com ISDR: t8KdcHKNGsnIFoRduNxVi801dhnj8onUloLtoaBD9LswZ5EPM3iJIWfAju2LX0/iG9sAHESFxI 7OqTWEHs8BgIVokqBytAtqOOvW/5tULW3uLUttGO6sig6tP3B5br1u6vVUljQAorj9MAve6EGW 3yD60wjhcCue15fg5wizVI3dq533iGDLu4NZIr6EozKlCne/Q/mSXyjxuv3UQCU1etJHS7EbOa tIZPWkuTrvXheCESuw8+KbBmAoax9VYVDO5omM7nENRd/TBHbadhUqhw6DgvcwRirbwJwUgX+K cMMk69xd8wWuFtbXO5InaRxT IPHdr: =?us-ascii?q?9a23=3APH/cOxzkVdgEOoXXCy+O+j09IxM/srCxBDY+r6?= =?us-ascii?q?Qd0uoeLPad9pjvdHbS+e9qxAeQG9mCsLQd1bqd6vq6EUU7or+5+EgYd5JNUx?= =?us-ascii?q?JXwe43pCcHRPC/NEvgMfTxZDY7FskRHHVs/nW8LFQHUJ2mPw6arXK99yMdFQ?= =?us-ascii?q?viPgRpOOv1BpTSj8Oq3Oyu5pHfeQpFiCezbL9oMRm7rAbcusYLjYd8NKo61w?= =?us-ascii?q?fErGZPd+lK321jOEidnwz75se+/Z5j9zpftvc8/MNeUqv0Yro1Q6VAADspL2?= =?us-ascii?q?466svrtQLeTQSU/XsTTn8WkhtTDAfb6hzxQ4r8vTH7tup53ymaINH2QLUpUj?= =?us-ascii?q?ms86tnVBnlgzoBOjUk8m/Yl9Zwgbpbrhy/uhJ/34DaboKbNPV8YqzScsgXRW?= =?us-ascii?q?9dUsleTSFNHp+wY5UJAuEcPehYtY79p14WoBewCwesBv3gyjlJhn/t3a02y/?= =?us-ascii?q?kqHw7C3AwmAtIOqm7boNvoP6oVT++1yK/IwijBb/xI3zf96ZPFcg4gofGXR7?= =?us-ascii?q?18a9beyU4qFw7ciFibtILrPzSQ1usXsmib6fJtVfyui248sQ5xpT6vxsMtio?= =?us-ascii?q?nPmI0Z0EzL9SJ8wIszONa2S1Z7bMa5HJZUtCyWLZV6T8w/T21ypSo3yrkLtY?= =?us-ascii?q?S4cSUJzpks2gTRZOadc4eS5xLuTOaRLil8hHJiYL+/nxGy8VK8yuLmUsm4zl?= =?us-ascii?q?FKojBbktnNrXACzQbf5dSASvt45kuh2DCP2B7P6uxcPEw5kanWJ4Q/zrM/i5?= =?us-ascii?q?Yfq1nPEy/ylUnsj6KbdV0o+u2y5OTmZrXmqIWcN4hxigzmLKsunsq/Dvk6Mg?= =?us-ascii?q?cQWWib+P+x1KPi/U3iWrpGlOE5kq7csJzCP8QUura5AxNJ0oYk8xuxCjCm0N?= =?us-ascii?q?IDnXkbNl1Ffg6Hj4nvO13UOv73E+u/g0mvkDdrwPDGIKbsApbXIXjYiLfhfK?= =?us-ascii?q?xx601dyQAr19BQ+4pUCq0dIPL0QkLxtcDYDgQnPAOo2urnE9J92Z8FVGKMGK?= =?us-ascii?q?CZK7vSsV6S6uIsIuiGfJUVtyrlK/g5+/7uimc0lEEdfamo25sXZ3G4Hu98L0?= =?us-ascii?q?iEe3Xsgc0BHn0KvwUgUuznk16CXiRIZ3aqXqIw/DI7CYO+B4fZWo+tmKCB3D?= =?us-ascii?q?u8HpBOem5JEEuMEXfpd4qZQfsCdj+SItVukjMeVbmuVZEh2AqttADg0LpnNu?= =?us-ascii?q?vU9jcbtZPizNJ1/fHclQku9TxoCMSQy2KCQHtunmwWQj85xrpzr0tgyleYyq?= =?us-ascii?q?h4gvpYGsZI6vNKSAg6Lobcz+1gB9DxWwPLZs2JR0q+QtW6HTExSco8zcMPY0?= =?us-ascii?q?Z7AdqikgrP0Ci0DL8Ol7yLAYY786LC0HjvPMt9yGzJ1LI5j1knWMdPNmyn1e?= =?us-ascii?q?ZD8F2ZK4zElUSCl+LiWKAawTTEvi/XwG6IsENVVg9YT6TeVDYUYU6A/vrj4U?= =?us-ascii?q?aXBZOsBLImKQsFgeOGLLZQY5eh2VhCQvvhNdLfS3ywgG72DhGNkODfJLH2cn?= =?us-ascii?q?kQiX2OQHMPlBoeqC7faFoSJQaE5k/ABThzHE7uZEWyrLQstibiHQc9mhuRZg?= =?us-ascii?q?h617Pvp0BGzffJUPIWxrYJ/zwgri1wEQXYvZqeB4+ephFoOq5bZIB14QJvy2?= =?us-ascii?q?PCvkp2OZnzZ7k3ilgFNBhnoxCmzEB8DZ9Yic8wsHoun28QYeqEhQocKG7AhM?= =?us-ascii?q?6gZOOEYnmnpU73NfOLgAGAjoXzmO9H6KE2sVLm7h2uRFE/+Xdq2MUH33KA68?= =?us-ascii?q?fPAREJWJ38F0c7pQJ3qbzAby826piG1HspK6Ssti6Hx9V7YYltgl6lftJSdb?= =?us-ascii?q?2JDhTzFMtJYqrmYOYqzmeWVxlbILB3qpQ/Bdq8Z/er5IirH7hqgA+2kG4Xo6?= =?us-ascii?q?RC9hOOrjBEd8Lv55lQkJT6lkONAhDmy2WZlObJwKJWZTQgJTGE4g/7WN5If7?= =?us-ascii?q?14Z60lFWqueveN2+ps2ZrSQVdT2gSzBm026uD2dwSNCj61lUVqi043vXyrhS?= =?us-ascii?q?m/7iFdgnYg96mB4zH828DQKRYAKGlza1dBiXuyI4O1lMk9QESWSgF3sR2gvF?= =?us-ascii?q?/DwOs+xuw3Z1vtbRZVcHHSCkxsa/Ot7rfBe+JUyp0Hqy5RadazS3vLde/yhB?= =?us-ascii?q?4D6AK7FTVy32k+ahGhvLzewSZbqAf/ZD479F/0KctJgg+O44CMHMIB8mBcQz?= =?us-ascii?q?BJ0mfnKkaTFcWM7+2xy5vpk8a9cXr/SrBJfwbg792vs3XguzxwZH/317id2e?= =?us-ascii?q?DoPzUIzBfW2sZ2TQnjpQr3P4zU8LugLME3U1EwIUGg0JcmIqh1zo8tgK8C3S?= =?us-ascii?q?A0vcq2wV8bjmGWU50TkbDZc38cdGET5cLz/VX5+BAzCE23nLP5UmuF+OdfVd?= =?us-ascii?q?XqM1NK4iEH9vJqJI6w3pFWsA1q4QvptgaAeZ0f1n9Vxq57uzYKxuATvww1yT?= =?us-ascii?q?+BR6ofBlRcIXn0ng+TvInj/ol0RUPqXKa50Fd3gdGmCu3d+lNCDS+qMp53Bz?= =?us-ascii?q?R5q95/OQiRji674dT+dd3Zfd8f8QeZlx7QguQGTfB5mq8UhDFuOGT2+3ojzu?= =?us-ascii?q?8wlxt12p+m+oOALjYl5/eiDxpVPSHyfZpW5DD2hKdYlYOR2YWuFY9mATIFQN?= =?us-ascii?q?7jSvf7dVBataHJLQGLQhE1tnrJIqfVHwKU9BVDomnUGp+mclC7dlIey8lvQg?= =?us-ascii?q?XYGF1HjVIxfRAX26A0DBurw8qzQAJc3XU89lX4ox1Dx6dTOh/zX332iCyoZz?= =?us-ascii?q?w3G/39ZBBWuwhe+kznHu/HtexSBBwBxLi7pQizGHTHTltuK0gQdEnZCWLeDK?= =?us-ascii?q?G25v2f1efNVY/cZ/GbWpOU9uxGR/yYxYDszNt4zy+0H8OhGkdkAL58+VpYDG?= =?us-ascii?q?1bJ/jEnh5QZXERyRrXXdXDvijh/TBF9f2xwaTtWiff4MzIBJl8G8pN9x7pmI?= =?us-ascii?q?aIOPfMj3Z+Ix8b5ssV6iOXk709xm5OkCg1JyiBKJNfugfRSb3CnZ1HMkQGMw?= =?us-ascii?q?IwZMhj8IED/SkVPcuDkNrVy6xg0NURGwxCaVyi2fyqesYzckC3c13qPEGlLP?= =?us-ascii?q?e4ZhLmlpK/cea9U7pWlOJOq1iqtC2GF1O2ODmeiyPgU0PnIaRNliadJBtEpM?= =?us-ascii?q?SwaAxqEz3FS9TrOUDpHPpetxZvmO1m3jfmMGcGOgJxeERXou/Y9XZBn/xlEm?= =?us-ascii?q?pd73xoaaGckDrMtrGAbt4Nqa5tBSJ506pT7Hc7zu5PqGlNX+R7zTGW5sRzqg?= =?us-ascii?q?SV0qaDzzN9Wy1HpTljjZ+XvQN4NLnE7J9YUGrEuhQA8SrUQ01S+4s4VYO3+p?= =?us-ascii?q?UUzN/Jmfipeh5f79LZ+9cdDMHIKcWBdUAsKgftBCWNUVRXRzuwLiSH3kAbk/?= =?us-ascii?q?iJ7nzTrYpp4oP0ls82Q6RAHEcwCutcD01kGNIYJ5IiUzcinbyWis8g+3ulpV?= =?us-ascii?q?/aQ8AJ9pzEV/fHGfz0M37ZlrhLYRIU3Kn1ZZoeLIz12kFuKxF6kY3GFlCWXI?= =?us-ascii?q?VlvCx6Z0k/p0AeuHR7R3c4jlrscRjloGdGDOO9hBcwlgp4bKwh9Sy55VAxKx?= =?us-ascii?q?uCqH4ukVI4397ihGnLIgT8J6qxQ4xaThHMmRhqY8HDSh1uJU24mFd/cW+dS/?= =?us-ascii?q?RShqB4dCZoml2UtZxKEP9aBapKBX1YjfyTYfkq3FJdgjum3kYB7uzAQZdvjw?= =?us-ascii?q?old5ewomkIglMzKoRpfOqJefsPnggYj7nGpiKy0+Et3AISQiRFuHiffiIFog?= =?us-ascii?q?1AN7UrITap4v057AWDnzVZf21fH/Euo/9s6gY8I7HZnnKmieIabBnsZqrPf/?= =?us-ascii?q?D82SCIj8ODT1Iu21ldnUxe5v0uiMtlcEOPT0Fpz6nCcnZBfcfENwxRaNJfsX?= =?us-ascii?q?bJeiPb++jJx553MoO8Pv7pVubIv6ERyBHBfk5hD8EX48INE4P5mkzcK8vlIb?= =?us-ascii?q?gE4Qss/w2tL1KARqcBaFeAlzEJpNu6xZl80NxGPj8qBmN5IHbShP6ftkowjf?= =?us-ascii?q?GERttzfmYCU95OKCctQMPj0X0RrzFaATKwyO5c1AWS82q2uHHLFDelCrgrLP?= =?us-ascii?q?aMOUE1WYHwo2lmtfHo0xiPtc+Cb2DiaYY764+Js79D4c/ZW7UMCuMh1iWU04?= =?us-ascii?q?hAGy7zAj6JS4LsYcGtOs90KoaoQneiDg7g0XRpEYGrZ4rrdu/S3UnpXdoG7t?= =?us-ascii?q?fdhWB+c5btT3dGXE0swoNLrKNkOV9aMsp9O0Kx8V1ha+rnZ13EmtS2HzTydX?= =?us-ascii?q?0PFqcZnLz8P/sNk2ItdrPokSpwCMFiibXttxVoJtlCjwmCl6jyIdMGF3GpRz?= =?us-ascii?q?oHIF+HpDJlxTEwZqBonr55mUyV9wBEbXiKbLA7MjUa+YthXBXIfC4wWzpdJR?= =?us-ascii?q?fUjJKfsFDzmepKr20HxogSj7QNsWCi7MaOMHT2BPPt8MqJ9XN/MJAnu/Ejb9?= =?us-ascii?q?OleJHe8sqExnqFEPyy+kWESHLoSaQcw4gNZnsIHr8S0WA9ZZ5f6NoHsxZoEJ?= =?us-ascii?q?5hfvoWUuEtvuz4M2I4S3FPi3ZFDcXag1lgyq+9w+eIyEnWKcp/dkVb7dMb0o?= =?us-ascii?q?pVUjYqMH1B4vbyDcOPzD7CETRDIR9Pv1oToltRzMkpI7+jsNGtLtcEyiYK8a?= =?us-ascii?q?srDm2SSsIurgOjDDjH2BD5UKnzyr35m1gOlbS1j4ldBEU3CFABlb8Mxg1ydO?= =?us-ascii?q?sxcvBA+NSS6lrqPQv7pD6/kbr2YgMNkIuOLwK+VM2f6SL9SnFOoCxEA9UTkT?= =?us-ascii?q?eFTcpUy00jNO49rVFIatn3KHa73CQtwsFSJ5f9UMmqw1g/qnNfH3W0EsFITe?= =?us-ascii?q?phtQCOVQ=3D=3D?= X-IPAS-Result: =?us-ascii?q?A0E6AABz2OBdh1if8cZiAxwBAQEBAQcBAREBBAQBAYFsB?= =?us-ascii?q?QEBCwGBG39xK00EIQEBEpJhjEiMQIMJFIEQAxg8CQEBAQEBAQEBAQMBKwQEA?= =?us-ascii?q?QEChD4Cgi4BNgcOAgECAQEBAwIFAQEBAwEBAQIBAQEDAgEBAQECEAEBAQgNC?= =?us-ascii?q?QgpHwNggiyBQQ0FCQQwDII7Ims4ATIBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA?= =?us-ascii?q?QEBAQEBAQEBAQEBAQEFAm0fHgEBHgIBAwUBCxQIARIBAQMwBQ8CASUBAQEfB?= =?us-ascii?q?wIVAQIMIAwFAQEEEgEGAgYMgwgBgXhOAwkWHqF1AYwhgg2DQoJ+AQEFgTUBg?= =?us-ascii?q?2IYghAHAwYJAYEsAYFSiQKBW4FCPoFYgh6DRAwBAgEBBRSBDwUBEgEhFQoMC?= =?us-ascii?q?RGCe4IsiDCFBYIRhiCBCQmINwSFHgKCZYUOgXwDB4Iug1GCNQGBF45WgkGHb?= =?us-ascii?q?YsBE4RhhD+IVUaJLJFXggUJgRFxcBVIDkkBAjcKgURNAQIBAQENAQIBAQ8BA?= =?us-ascii?q?QEBiFEag1mKU3QBAQEBCI8fgjIBAQ?= X-I-AV: E=McAfee;i="6000,8403,9455"; a="35746514" X-I-AV: E=Sophos;i="5.69,256,1571680800"; d="scan'";a="35746514" | | | | |

### X-Header

|  |  |
| --- | --- |
| **X-IPAS-Result:** | =?us-ascii?q?A0E6AABz2OBdh1if8cZiAxwBAQEBAQcBAREBBAQBAYFsB?= |
| **x-microsoft-antispam- prvs:** | tlook.com> |
| **x-ms-oob-tlc-oobclass ifiers:** | OLM:10000; |
| **x-forefront-prvs:** | 0236114672 |
| **x-forefront-antispam- report:** | SFV:NSPM;SFS:(10009020)(4636009)(366004)(376002)(39860400002)(396003)( 136003)(346002)(189003)(199004)(66446008)(3846002)(6506007)(8936002)(62 00100001)(8676002)(14444005)(256004)(5024004)(81156014)(76176011)(81166 006)(7696005)(25786009)(76116006)(7736002)(5660300002)(66946007)(478600 001)(33656002)(74316002)(99286004)(790700001)(966005)(10290500003)(6475 6008)(413944005)(14454004)(76576003)(86362001)(52536014)(606006)(665760 08)(66476007)(66556008)(6116002)(11346002)(7276002)(4744005)(7416002)(7 1190400001)(7406005)(54896002)(7110500001)(6436002)(236005)(6862004)(73 3005)(65686005)(10310500001)(26005)(10440500001)(446003)(15650500001)(2 420400007)(71200400001)(316002)(7366002)(6306002)(186003)(2906002)(7336 002)(102836004)(66066001)(55016002)(9686003);DIR:OUT;SFP:1101;SCL:1;SRV R:MN2PR10MB4352;H:MN2PR10MB4221.namprd10.prod.outlook.com;FPR:;SPF:None ;LANG:en;PTR:InfoNoRecords;MX:1;A:1; |
| **x-ms-exchange-sendera dcheck:** | 1 |
| **x-microsoft-antispam:** | BCL:0; |
| **x-microsoft-antispam- message-info:** | C7+yx8J6jBd7HTFOs+pvujc15HAgZs9A0gUROeq1K8+e+Hwtv0x3u3TBIH8WXKKKBdTkyb Xzl2RHSzJ1NycC1mT8C5VWT+miVkDzLW9BeaBANXPdOFas60anwUODNG+gHOKJZFKHCf43S OWczOzZx/59G444uyHiani6n9VddDQWxUkD3ghHQDA5R82XKSwXphirbjVg2oMaWFSdxTV5 UtCZlzRTVKEkmdklPdslxZ1qdSgGaFADPHjb++mkBBwc/LuW0knJ+ctL32tMi6cQkltTpqX 9T22NvkO+P5Jyk12ip56qJWGuctrlf9T5EHkZm6ZVIZQD9thaVXRK+Z+n3w878XbE2Fgvrk NIvylwr5m6lzFpiIwKRHVsqSQU5KoL4DEwC2kCmoWooJ3iIJUNibwEMSbCdCZdFDs9SUI0n enNEzyTCsgXVjbfVuVsVhBLbvOCVH8VnCx2nd/ro4umlUMi66GNPX4sbcPo9NvTsUg= |
| **X-MS-Exchange-CrossTe nant-Network-Message- Id:** | 66f4a5ca-59fb-4ee5-9a64-08d774a7d0cd |
| **X-MS-Exchange-CrossTe nant-originalarrivalt ime:** | 29 Nov 2019 08:40:40.3369 |
| **X-MS-Exchange-CrossTe nant-fromentityheader :** | Hosted |
| **X-I-AV:** | E=McAfee;i="6000,8403,9455"; a="35746514" |
| **X-MS-Exchange-CrossTe nant-id:** | 38305e12-e15d-4ee8-88b9-c4db1c477d76 |
| **X-MS-Exchange-CrossTe nant-mailboxtype:** | HOSTED |
| **X-MS-Exchange-CrossTe nant-userprincipalnam e:** | HSIlGZHXr0W8z5qFm05wvFicPhrWtWJs3JHrABmqxsi2GZUbk0+K29Ca6hFGw2YoAn9bOP COxb7WH5fqUaMi4A== |
| **X-MS-Exchange-Transpo rt-CrossTenantHeaders Stamped:** | MN2PR10MB4352 |
| **X-MS-Exchange-Organiz ation-Network-Message -Id:** | c71d9339-de26-46af-c4ce-08d774a7eed9 |
| **X-MS-Exchange-Organiz ation-AVStamp-Enterpr ise:** | 1.0 |
| **X-MS-Exchange-Organiz ation-AuthSource:** | exch1.localhost |
| **X-MS-Exchange-Organiz ation-AuthAs:** | Anonymous |
| **X-MS-Exchange-Transpo rt-EndToEndLatency:** | 00:00:00.3430562 |
| **X-MS-Exchange-Process ed-By-BccFoldering:** | 15.01.1147.001 |
| **X-I-AV:** | E=Sophos;i="5.69,256,1571680800"; |
| **X-Address-Whitelist-F romDLP:** | X-Address-Whitelist-FromDLP |
| **X-MS-Has-Attach:** | yes |
| **x-ms-publictraffictyp e:** | Email |
| **x-ms-office365-filter ing-correlation-id:** | 66f4a5ca-59fb-4ee5-9a64-08d774a7d0cd |
| **x-ms-traffictypediagn ostic:** | MN2PR10MB4352: |
| **x-ms-exchange-transpo rt-forked:** | True |

**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)

2019-11-29 11:45:53 gw-dmz tcp 10.1.22.33:63303 -> 34.202.85.54:80 MALWARE-CNC Win.Trojan.Banker variant outbound connection (1:23262:7) (+3)

2019-11-29 11:46:13 gw-dmz tcp 10.1.22.33:63322 -> 54.164.20.117:80 MALWARE-CNC Win.Trojan.Banker variant outbound connection (1:23262:7) (+3)

IPS отрабатывает

**Без этого сообщение [Classification: A Network Trojan was**

**Detected] мы понимаем что исходящий троян не обнаружен**

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.);

10.1.2.3 109.166.59.44 [17/Nov/2019:03:17:59 +0600] "GET /shop-ext/suggestions/?i=productDetails&m=true&t=IP&pi=14701657&u=3729495 HTTP/1.1" 200 "https://kaspi.kz/shop/p/gerbor-vusher-reg1w2d2s-13-9-l-p-nimfea-al-ba-belyi-gljanets-14701657/?c=551010000" "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" 0.009 0.008 10.2.3.4:9001

import re  
  
  
def parse\_log\_line(log\_line):  
 # Define a regular expression to match the log line format  
 log\_regex = r'^(\S+) (\S+) \[(.\*?)\] "(.\*?)" (\d+) "(.\*?)" "(.\*?)" (\d+\.\d+) (\d+\.\d+) (\S+)$'  
  
 # Parse the log line using the regular expression  
 match = re.match(log\_regex, log\_line)  
  
 if match:  
 # Extract the fields from the log line  
 ip\_address, client\_ip, timestamp, request, status\_code, referer, user\_agent, request\_time, upstream\_response\_time, server = match.groups()  
  
 # Return a dictionary with the extracted fields  
 return {  
 'ip\_address': ip\_address,  
 'client\_ip': client\_ip,  
 'timestamp': timestamp,  
 'request': request,  
 'status\_code': status\_code,  
 'referer': referer,  
 'user\_agent': user\_agent,  
 'request\_time': request\_time,  
 'upstream\_response\_time': upstream\_response\_time,  
 'server': server  
 }  
 else:  
 return None  
  
  
# Example usage: parse a log line and print the extracted fields  
log\_line = '10.1.2.3 109.166.59.44 [17/Nov/2019:03:17:59 +0600] "GET /shop-ext/suggestions/?i=productDetails&m=true&t=IP&pi=14701657&u=3729495 HTTP/1.1" 200 "https://kaspi.kz/shop/p/gerbor-vusher-reg1w2d2s-13-9-l-p-nimfea-al-ba-belyi-gljanets-14701657/?c=551010000" "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" 0.009 0.008 10.2.3.4:9001'  
  
parsed\_line = parse\_log\_line(log\_line)  
  
if parsed\_line:  
 print(parsed\_line['ip\_address'])  
 print(parsed\_line['client\_ip'])  
 print(parsed\_line['timestamp'])  
 print(parsed\_line['request'])  
 print(parsed\_line['status\_code'])  
 print(parsed\_line['referer'])  
 print(parsed\_line['user\_agent'])  
 print(parsed\_line['request\_time'])  
 print(parsed\_line['upstream\_response\_time'])  
 print(parsed\_line['server'])

17/Nov/2019:03:17:59 +0600

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

200

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

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

0.009

0.008

10.2.3.4:9001

5.

**На мой взгляд, никаких атак нет, происходят рутинные действия**