Log file Analysis

Details

#1 NGINX

NGINX writes information about client requests in the access log right after the request is processed.

Here I found-

10.1.2.3 private IP requested to the server IP 109.166.59.44 at 17/Nov/2019:03:17:59 +0600.

Method: GET

URL: https://kaspi.kz/shop/p/gerbor-vusher-reg1w2d2s-13-9-l-p-nimfea-al-ba-belyi-gljanets-14701657/?c=551010000/shop-ext/suggestions/?i=productDetails&m=true&t=IP&pi=14701657&u=3729495

Server status: 200 (success)

Client Browser: Mozilla/5.0

Device: Redmi Note 7 (Android 9)

Server name: AppleWebKit/537.36

#2 Custom web log

Custom logs are logs that contain diagnostic information from custom applications, other cloud providers, or an on-premise environment.

Here i found two web session:

Session 1:

Src IP: 89.36.164.62

Dst IP: 172.1.2.3

Port: 8080

Method: GET

Url_path: /rest/profile/photo/download/client

Session 2:

Src IP: 2.75.209.33

Dst IP: 172.1.2.3

Port: 8080

Method: GET

Url_path: /rest/profile/photo/download

dd__persistedKeys=**["user.anonymousId"]**

#3 Proxy Server

A proxy server is a system or router that provides a gateway between users and the internet.

Here I found two proxy server for 2 session.

(1) <30>Dec 4 12:21:59 mwg-prx1 mwg: LEEF:1.0

```
src=10.8.9.8

usrName=ivanov123

httpStatus=101

dst=52.202.62.251

urlCategories=Web Meetings

url=https://zpnspbx.zoom.us/ws


(2) <30>Dec  4 12:21:59 mwg-prx1 mwg: LEEF:1.0

src=10.7.8.9

usrName=petrov_123

Device OS: Windows NT 10.0; Win64; x64

Server name: AppleWebKit/537.36

httpStatus=200

dst=149.154.167.99

urlCategories=Instant Messaging

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

#4 ASA

The ASA has an internal buffer that we can use for syslog messages.

<166>Dec 04 2019 12:21:59 ASA1234 :

Deny TCP (no connection) from

Src IP: 90.143.47.21/42968 to dst IP:194.187.247.147/443 flags ACK on interface outside

Here, 443 port is refers to https port from server side, is also known as destination port.

And 42968 is epharmal port and also source port. Src ip try to make TCP connection with dst ip. But the connection is not establish. Because there have no SYN flag.

#5 Mail Log

Mail logs show the list of all emails.

Here have three session. **In first session occurs reverse DNS**.

IP: 62.141.46.147 **Hostname:** vps2305103.dedi.server-hosting.expert

```
<22>Dec 04 12:22:00 Text_Mail_Logs: Info: New SMTP ICID 11444342 interface MAIL
(172.1.2.3) address 62.141.46.147 reverse dns host s2.kipersam.art verified yes
```

In second session we see client pc check the SBRS(SenderBase Reputation Score). **Here SBRS score is -3 and -1.** So it was accepted by receiver. Which is come from germany.

```
<22>Dec 04 12:22:00 Text_Mail_Logs: Info: ICID 11444342 ACCEPT SG
SUSPECTLIST match sbrs[-3.0:-1.0] SBRS -1.6 country Germany
```

In the third session the SBRS score is -10 and -3. We this is spam score. So here the receiver reject the mail as **spam**. Which is come from Mongolia.

```
<22>Dec 04 12:22:00 Text_Mail_Logs: Info: ICID 11444341 REJECT SG BLACKLIST
match sbrs[-10.0:-3.0] SBRS -5.5 country Mongolia
```

#6 FW

fw log or follow log Shows the saved entries that match the specified conditions.

Here you can see all information are already listed.

```
DeviceType=Estreamer      DeviceAddress=10.10.10.1(private IP)

CurrentTime=1575440517963         recordType=FILE_MALWARE_EVENT
recordLength=258     timestamp=04 Dec 2019 12:21:55     netmapDomainRef=0
fileEventData.connectionInstance=10          fileEventData.connectionCounter=3278
fileEventData.connectionTimestamp=1575440514
fileEventData.fileEventTimestamp=1575440514
fileEventData.sourceAddress=172.2.3.4       fileEventData.destinationAddress=172.2.3.5
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   fileEventData.fileSize=46197
fileEventData.direction=2       fileEventData.uri=       fileEventData.signature=
fileEventData.sourcePort=46037       fileEventData.destinationPort=30
fileEventData.protocol=6        fileEventData.clientAppId=2634
fileEventData.archiveSHAHash=       fileEventData.archiveName=
fileEventData.archiveDepth=0          fileEventData.httpResponse=0
fileEventData.managedDevice.managedDeviceId=14
fileEventData.managedDevice.name=gw1-module1
fileEventData.SHAHash.SHAHashData.SHAHash=CD22437892392E03BF5375B597AA
77DE6F0E5D9F26B1832339B79DA19F050BF7
fileEventData.SHAHash.SHAHashData.fileNameOrDisposition=Unknown
fileEventData.SHAHash.SHAHashData.disposition=0
fileEventData.SHAHash.SHAHashData.userDefined=false
fileEventData.fileType.fileTypeId=9    fileEventData.fileType.fileTypeName=PDF
fileEventData.webAppRef=0
fileEventData.sslCertificateFingerprintRef=000000000000000000000000000000000000
0000    fileEventData.sourceCountryRef=0    fileEventData.destinationCountryRef=0
fileEventData.securityContextRef=00000000000000000000000000000000
fileEventData.sslActualAction.sslActualAction=0
fileEventData.sslActualAction.description=Unknown
fileEventData.sslFlowStatus.sslFlowStatus=0
fileEventData.sslFlowStatus.description=Unknown
fileEventData.accessControlPolicyRef=FB8E85A86E2111E8BF10C9DF28307955
fileEventData.application.serviceId=836
fileEventData.application.serviceName=SMTP(short message transfer protocol)
fileEventData.user.userId=9999997   fileEventData.user.protocolRef=0
fileEventData.user.userName=No Authentication Required
```

Here a malicious PDF file is injected through SMTP or mail server.

New session:

```
DeviceType=Estreamer        DeviceAddress=10.10.10.2(private ip)
CurrentTime=1575440517955          recordType=NEW_TCP_SERVICE
recordLength=94       timestamp=04 Dec 2019 12:21:55     netmapDomainRef=0
detectionEngineRef=5           ipAddress=0.0.0.0      MACAddress=10:05:CA:AF:5C:C0
hasIPv6=true  eventSecond=1575440514    eventMicroSecond=975996
eventType=NEW_TCP_SERVICE     fileNumber=1F4CE75D
```

```
filePosition=15320100        ipV6Address=10.23.170.180  hostService.port=4899
        hostService.hits=1   hostService.lastUsed=1575440528
hostService.confidence=0
```