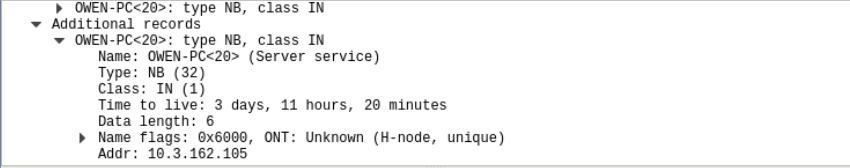
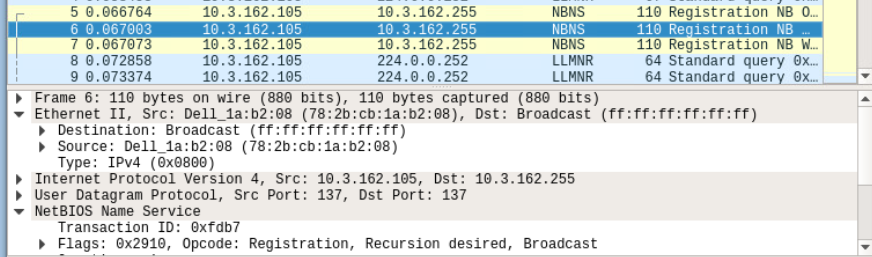
**Assessment 3- Security Incident Report**

# Introduction

From the network packet capture analysis, the details of the victim machine have been identified in the image below



The details of the victim machine analyzed from the packet capture reveal the mac address (78:2b: cb: 1a:b2:08), which further depicts that it is Dell\_PC. The NetBIOS Name Service (NBNS), shows the host name and the associated IP address that it holds (10.3.162.105). below depicted are the complete details

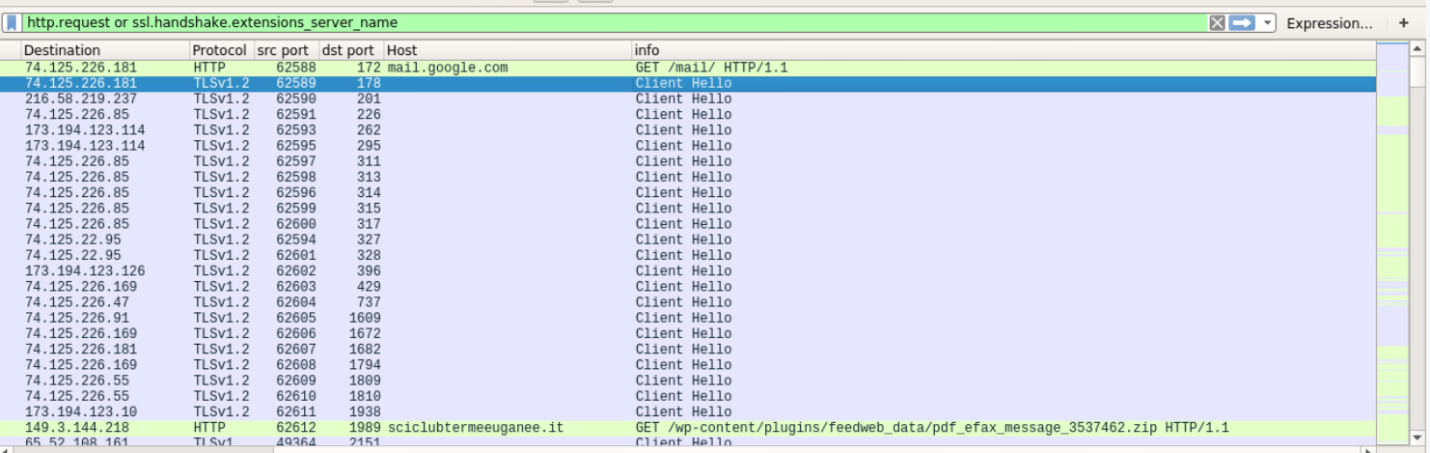
Device: Dell-1a:b2:08

Mac Address: 78:2b: cb: 1a:b2:08

IP Address: 10.3.162.105 (IPv4)

OS: Windows

WorkStation: Owen-PC

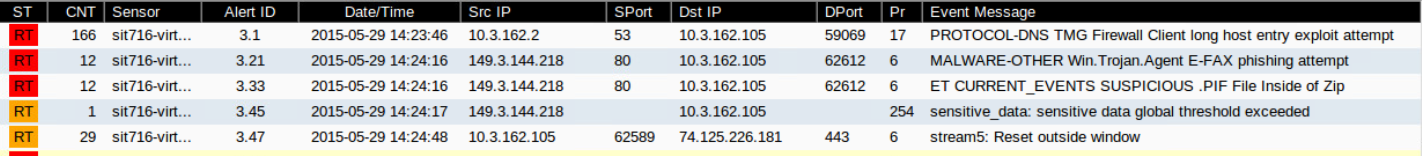


From the packet capture analysis, it seems the victim had visited Gmail and downloaded the downloaded a zip file which was disguised as an eFax message (pdf\_efax\_message), that contained the actual exploit in our analysis. The victim had received the malicious PDF to their Gmail account that led the attacker to conduct the attack.

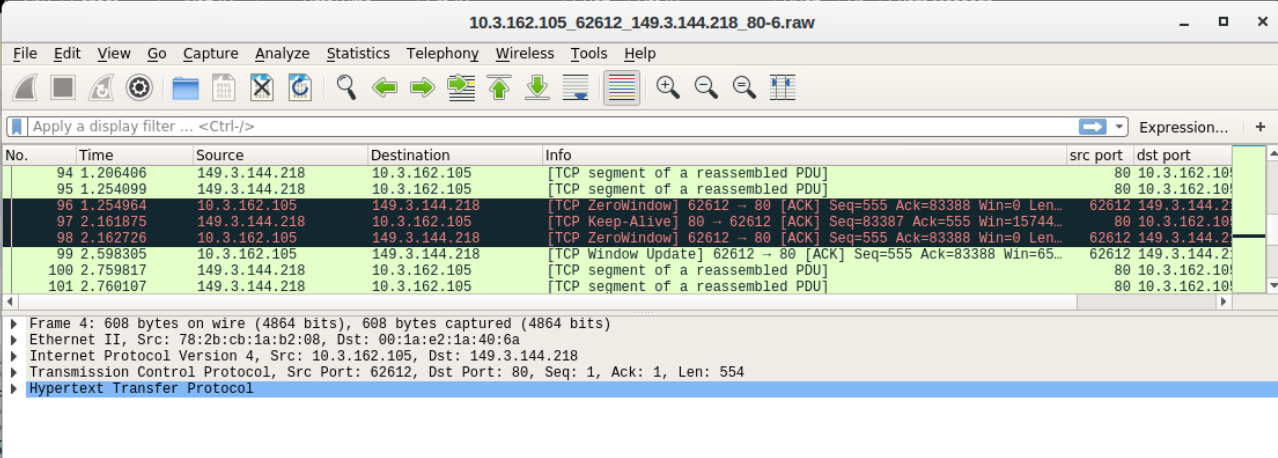
# Elements of the attack

## Event ID 3.21: MALWARE-OTHER Win.Trojan.Agent E-FAX phishing attempt

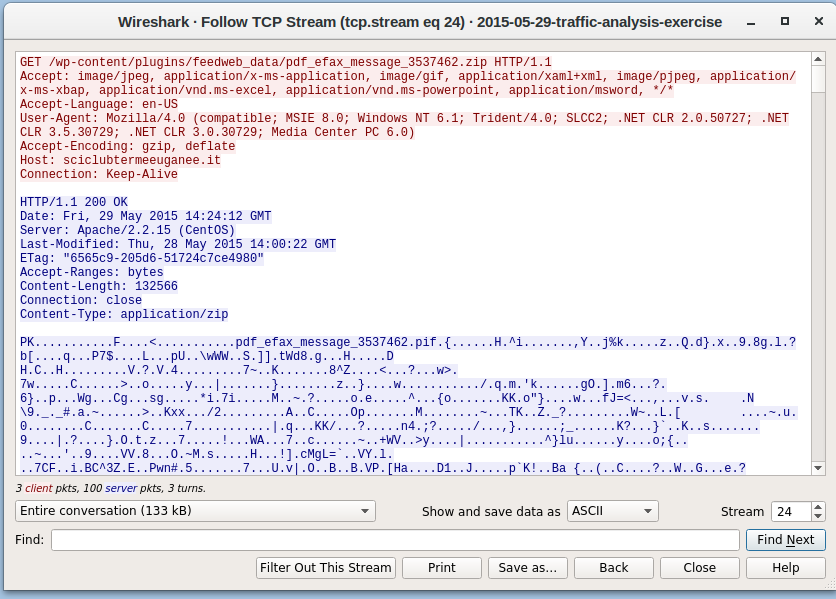
Event ID: 3.33: ET CURRENT\_EVENTS SUSPICIOUS.PIF File inside of ZIP



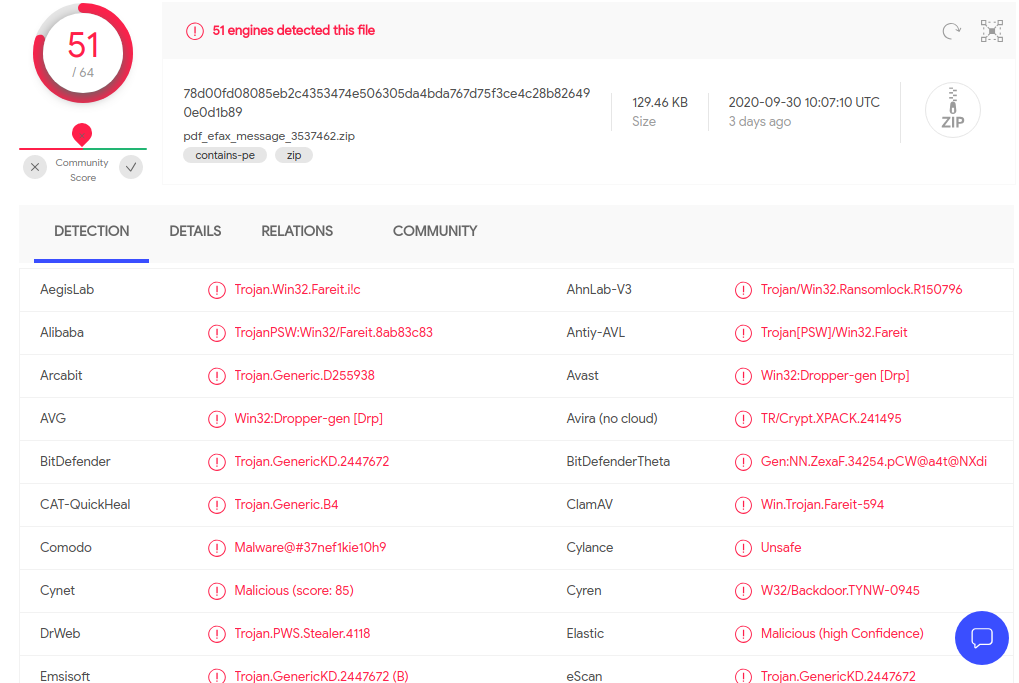
The above events depict the TCP exchange that took place between the victim (10.3.162.105) and the host IP 149.3.144.218. The malware presented in the eFax message was trying to transmit the file to the victim by keeping the TCP connection alive (TCP-Alive), even though the victim machine had requested a TCP-Zero Window, meaning the buffer is full and cannot take receive more data.



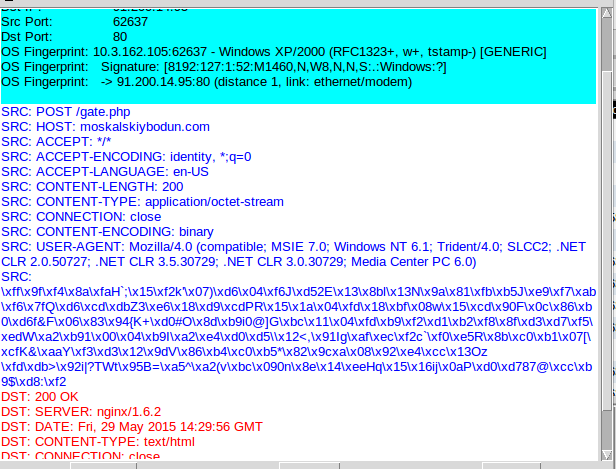
This raised the event message of the E-FAX phishing attempt, where it’s possible the attacker would be trying to disguise a file and send the actual exploit victim. Event ID 3.33 the malware was contained in the zip file in the form of a malicious redirect script tag (\*/\*) as per the Event ID 3.71 and the user to accept files of image/gif from which the fiesta EK payload was delivered. The following TCP stream reveals the results. The redirect script tag was used to direct the user to the compromised website when an ad was clicked.



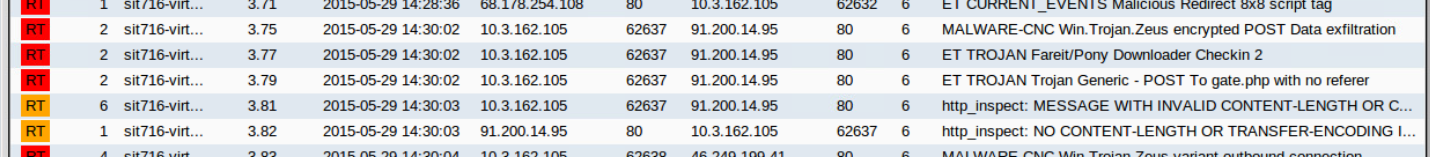
However, sguil raised the “Suspicious.PIF file inside of zip” event message is due to the malicious hash value raised in the security onion show rule, indicating signs of a phishing attempt. Also, scanning the zip file on virus total reveals a total of 51/64 engines malicious engines in the zip file containing Trojans and malwares.



From the file scanned on virus total, reveals the zip file contains a lot of malware and Trojans, which further can depict the behavior for the malware. For instance, the zip file highlights the malware as a password stealer or installing a backdoor in the windows system which the victim apparently has, or an attempt to ransom lock the system through the Trojan. From the files above the Trojan Downloader.Ponik is the likely malware indicates the behavior of having the sensitive data threshold exceeded, which the attacker might be using to steal sensitive information, where it is used to install malware infections on the compromised PC and such can be seen in the transcript, the response to the event being successful.

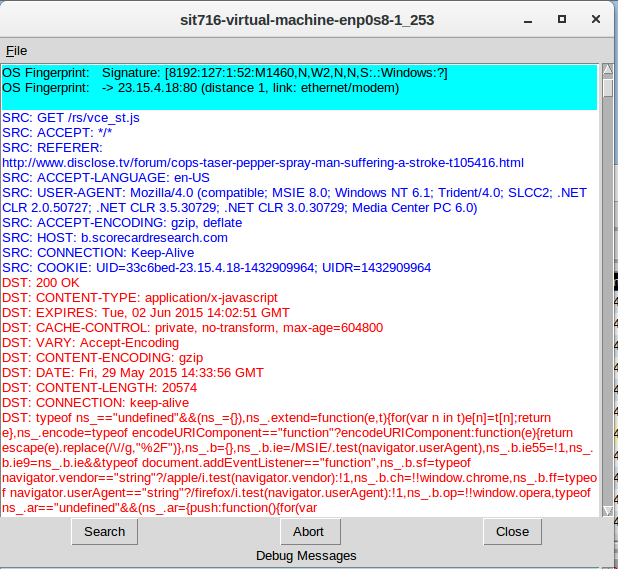


## Event ID: 3.75: MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration

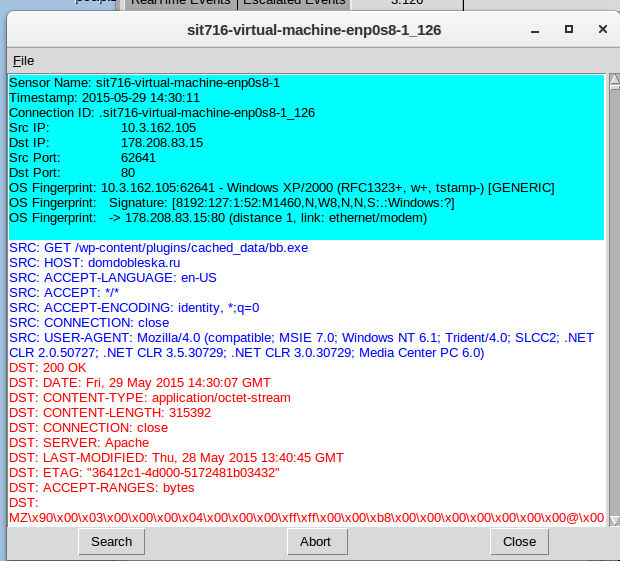


Once the victim clicks the zip file containing the Trojan.Zeus and redirects it to an external link, the malware is able to POST the Gate which contains the actual exploit. Moreover, the malware was most likely trying to call files or other stages from the control server, which gives the sign of infiltration from the attacker, for redirecting traffic back to bot owners. Also the malware might be trying to encrypt victim’s files and post it to the host, so when the files are encrypted the only way to decrypt it is by paying ransom.

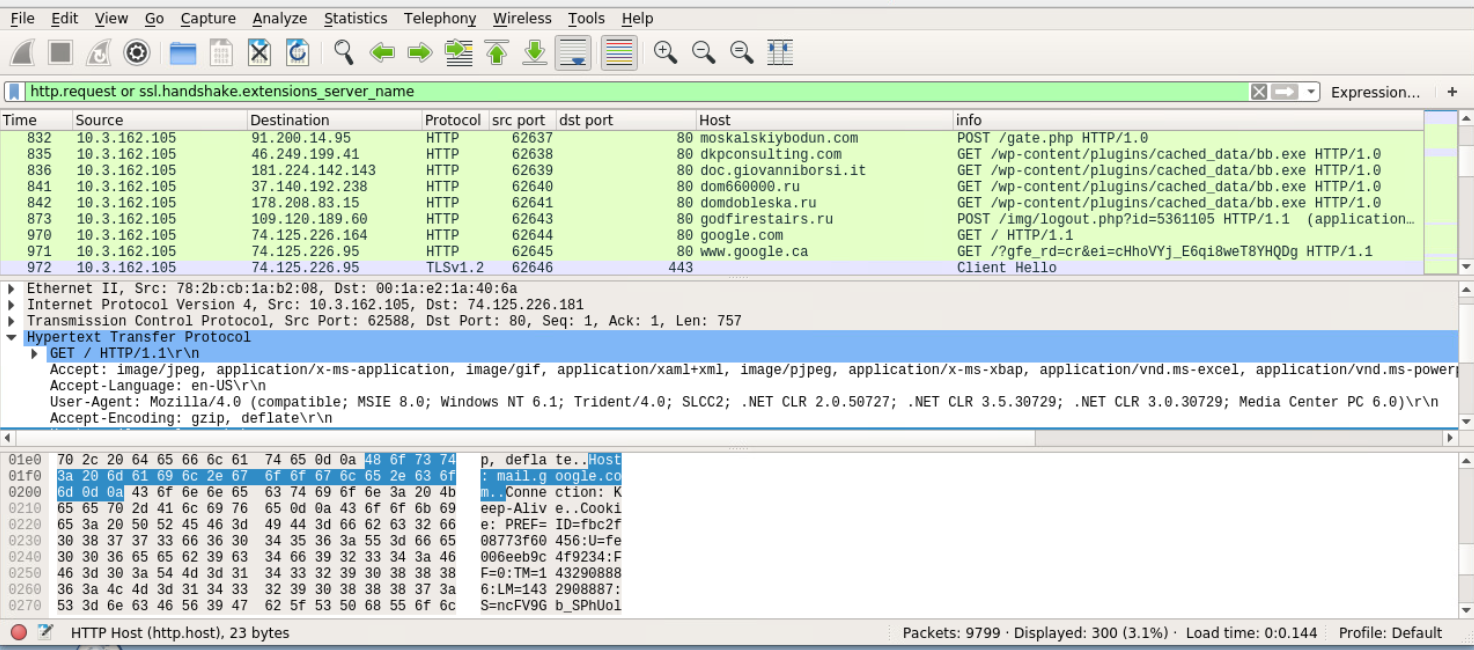
The payload was then downloaded and decrypted as we see the event 3.77(ET Trojan Fariet/ Pony Downloader Checkin 2). The Gate is then able to receive the post infection malicious files as can be seen in the packet capture analysis. The Event message generated itself indicates that the victim was subjected to data exfiltration where the Trojan fariet pony payload could have been used to export the data to the host. In Event ID (3.79) the malware Trojan Generic was trying to redirect the network traffic from the malicious script to the malicious host (b.scorecardresearch.com). The web browser being directed to this domain also indicated that an adware had been delivered from the referrer (compromised website) in the form of a gif file and such can be seen from the transcript below.



Which leads us to event IDs 3.81 and 3.82 where transfer encoding and content where the HTTP response and the transfer encoding seems to be missing. This might be an attempt from the attacker trying to hide his network traffic, thus, snort creates these events. The zip file itself contained an executable file known as PE executable for MS Windows that was executed after the gate was posted that led in the malware to spread across the system through various hosts of the malicious domain dombdobleska.ru. The results of the successful activity can be seen from the following transcript.



The moskalskiybodun.com Gate had provided a way to for the malicious domain to spread the infection the post infection of the malware can be examined below. Once the exploit is executed we can see from the SGUIL events for Fiesta EK (Exploit Kit) Js.Redirect that led in the successful completion of the attack. Moreover, the likely malware to cause this type of activity is caused by the Trojan.GenericKD:2447805 that was included in the zip file, tricking the user into clicking the attachment which actually is a executable program. Once the executable runs, the malicious code is injected in the browser, in our case the victim using Internet Explorer. The malware then has a domain generation algorithm that it uses to determine location of the command and control center (CnC), which it will later try to use it. Below given is a given screenshot of domain generation.



# Recommended actions and training

The Trojan.Generic KD2447805 is a type of malware used by attackers in phishing campaigns to deliver malicious links in the form of zip files for the user to download. This results in a ransomware attack, where users are tricked into thinking the file as legitimate but is actually an attempt to inject malicious code to the victim machine in the form of an executable file. However, to prevent Trojan.Generic from infecting the system

## Elimination

* Use anti-malware software for windows such as MalwareBytes or HitmanPro to eliminate many types of malwares which are undetectable by other programs
* Do a full computer scan on the machine and put the malwares in quarantine from the software stated above
* Restart the machine to remove all unintended registries and programs to clear the infection

## Prevention

* Keep software up-to date, most importantly the operating system and the internet browser. From the case highlighted above, the victim was using windows XP, an outdated OS which is vulnerable to attacks.
* Keep the internet connection as secure as possible which includes setting up firewalls. The firewalls include both software and hardware, in controlling anomalous network traffic, which can stop Trojans from downloading in system
* Use trusted websites only and avoid clicking advertisements and banners that might contain suspicious links

The second malware i.e. the b.scorecardresearch.com redirect, can cause adware programs to appear on web browsers, as is mentioned in the pcap analysis. The following can be used to eliminate from the windows system

## Elimination

* Go to program and features in the control panel section
* Choose uninstall programs
* Scroll the list to find the malicious program
* Malware tools such as Hitman Pro can be used to eliminate the virus that scans the system for malware at places where it resides
* If PC is being redirected to the malicious domain, resetting the browser settings to default can help.

# Conclusion

Concluding, the analysis of our pcap files the Trojan. Generic malware is a ransomware that can cause serious potential damage to the victim. The nature of the ransomware is a zip attachment which contains the ransomware file. By downloading the file injects malicious code into the victims browser and renames the file. The file then removes the registries from the %LOCAL\_APP\_DATA%/temp directory and encrypts the user’s files. The Trojan then drops a ransomware file containing the ransom demand. Such an event could be devastating to the victim, rendering his system unusable till the ransom is paid. Also, the malware aims to take over the Command and Control (CnC) server, by generating domains to find server location. Furthermore, the malware can be injected to record keystrokes, give remote access to PC, inject ads, and browser popups which can damage the system at a great scale. The overall scenario resembled a ransomware attack, where the attacker might be aiming to encrypt user’s files as seen from the event Post Data exfiltration.

# References

* MalwareTips Blogs. (2020). *How to remove Trojan.GenericKD malware (Virus Removal Guide)*. [online] Available at: https://malwaretips.com/blogs/trojan-generickd-removal/ [Accessed 4 Oct. 2020].
* ‌Kaspersky.com.au. (2020). [online] Available at: <https://www.kaspersky.com.au/resource-center/preemptive-safety/avoiding-a-trojan-virus>.
* www.f-secure.com. (n.d.). *Trojan.GenericKD.3016333 Description | F-Secure Labs*. [online] Available at: https://www.f-secure.com/v-descs/trojan\_w32\_generickd\_3016333.shtml [Accessed 4 Oct. 2020].
* MalwareTips Blogs. (2018). *How To Remove B.scorecardresearch.com Redirect (Virus Removal Guide)*. [online] Available at: https://malwaretips.com/blogs/remove-b-scorecardresearch-com/ [Accessed 4 Oct. 2020].