<IW\_chat,2.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW\_chat,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-"> - [ Request Details: ID = 285721822, User Agent = "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.9 Safari/537.36", AD Group Memberships = ( NONE ) - ] [ Tx Wait Times (in ms): 1st byte to server = 0, Request Header = 0, Request to Server = 0, 1st byte to client = 0, Response Header = 0, Client Body = 0 ] [ Rx Wait Times (in ms): 1st request byte = 0, Request Header = 5, Client Body = 0, 1st response byte = 0, Response header = 0, Server response = 0, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0, WBRS response = 0, WBRS total = 1, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = %>, Sophos total = %<, Webroot response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; Latency = 6; "07/Nov/2017:00:00:05 -0400" ]

1719360000.000 6 10.0.10.198 TCP\_MISS\_SSL/200 GET http://gfx.ms "Ernesto@contoso.com" DIRECT/www.gfx.ms text/html BLOCK\_WEBCAT\_12-DefaultGroup-DefaultGroup-Oubound\_Malware\_Scannng-NONE-NONE-NONE 1 1 <IW\_chat,2.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW\_chat,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-"> - [ Request Details: ID = 285721822, User Agent = "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.9 Safari/537.36", AD Group Memberships = ( NONE ) - ] [ Tx Wait Times (in ms): 1st byte to server = 0, Request Header = 0, Request to Server = 0, 1st byte to client = 0, Response Header = 0, Client Body = 0 ] [ Rx Wait Times (in ms): 1st request byte = 0, Request Header = 5, Client Body = 0, 1st response byte = 0, Response header = 0, Server response = 0, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0, WBRS response = 0, WBRS total = 1, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = %>, Sophos total = %<, Webroot response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; Latency = 6; "07/Nov/2017:00:00:05 -0400" ]

1719360000.000 6 10.0.10.198 TCP\_MISS\_SSL/200 GET http://gfx.ms "Ernesto@contoso.com" DIRECT/www.gfx.ms text/html BLOCK\_WEBCAT\_12-DefaultGroup-DefaultGroup-Oubound\_Malware\_Scannng-NONE-NONE-NONE 1 1 <IW\_chat,2.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW\_chat,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-"> - [ Request Details: ID = 285721822, User Agent = "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.9 Safari/537.36", AD Group Memberships = ( NONE ) - ] [ Tx Wait Times (in ms): 1st byte to server = 0, Request Header = 0, Request to Server = 0, 1st byte to client = 0, Response Header = 0, Client Body = 0 ] [ Rx Wait Times (in ms): 1st request byte = 0, Request Header = 5, Client Body = 0, 1st response byte = 0, Response header = 0, Server response = 0, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0, WBRS response = 0, WBRS total = 1, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = %>, Sophos total = %<, Webroot response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; Latency = 6; "07/Nov/2017:00:00:05 -0400" ]

1719360000.000 6 10.0.1.49 TCP\_MISS\_SSL/200 GET http://gfx.ms "Darryl@contoso.com" DIRECT/www.gfx.ms text/html BLOCK\_WEBCAT\_12-DefaultGroup-DefaultGroup-Oubound\_Malware\_Scannng-NONE-NONE-NONE 9857 15153