Ex 12

From: LAM, Johnny
To: MCELROY, Amber
Subject: RE: 2022-66177
Date: Monday, October 24, 2022 13:46:10
Attachments: 2022-66177 proxy logs.pdf

Hi Amber,

I've reviewed the logs during that time frame and there is limited info in regards to the site "desicapuano.com" however I can confirm for your level of internet access, it does not include "desicapuano.com" and will be blocked by our proxy rules. Proxy is a different security appliance than a firewall but functions similarly.

Attached is the logs for "desicapuano.com" during that timeframe. Below are some key info to help decipher the logs.

1. Top left date and time is when I searched for this record
2. The "New Search" section lists the URL in question and the timeframe
3. "chancellor2.vpd.bc.ca" is the hostname of our proxy. The host IP is 10.250.33.37
4. The 14 log entries all refer to different files from that site "desicapuano.com" unable to be scanned by our sandbox which does show there was network activity to this URL

Thanks,

Johnny Lam | CISSP, CCNP
Manager, Infrastructure and Client Support
Information and Communications Technology Section
VANCOUVER POLICE DEPARTMENT | *Beyond the Call*
V1

From: MCELROY, Amber V1
Sent: Wednesday, October 12, 2022 3:32 PM
To: LAM, Johnny V1
Subject: 2022-66177

Hello,

I have a request from Crown Counsel in regards to our VPD Firewall. On May 16th I conducted an interview in Room 333 of our Annex location. At approximately 1415-1430 hours the suspect asked me to pull up a website on the neighbouring computer in the attached monitor room and I was unable to access it. It was like it was blocked due to our firewall. Would there be a record of this attempt? I believe that it was blocked by our firewall.

This is Crown Counsel's request:

A request by Mr. Fox for:

-"computer firewall rules which were in effect within the VPD's internal computer network at 236 E Cordova St, Vancouver, which could have affected the ability of computers on that network to access a website potentially located at "desicapuano.com" on 2022-05-16."; and

-"computer firewall access logs for the VPD's internal computer network at 236 E Cordova St, Vancouver, Relating to any attempts to access any website at "desicapuano.com" on 2022-05-16."

Could you confirm whether or not what Mr. Fox describes exists?

And if it does exist, can you ensure that the relevant rules and/or logs are not deleted while his disclosure request is still outstanding?

Thank you in advance,

Amber

Det/Cst 2343 Amber McElroy
Special Investigations Section
Domestic Violence & Criminal Harrassment Unit

VANCOUVER POLICE DEPARTMENT
3585 Graveley Street ¦Vancouver BC ¦V5K 5J5
V1
V1 | www.vpd.ca

New Search

desicapuano.com

from May 16 through May 17, 2022

✓ **14 events** (5/16/22 12:00:00.000 AM to 5/18/22 12:00:00.000 AM) No Event Sampling

Events (14)

Format Timeline 1 hour per column

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
date_hour 3
date_mday 1
date_minute 4
a date_month 1
date_second 8
a date_wday 1
date_year 1
a date_zone 1
a eventtype 1
a ids_type 1
a index 1
linecount 1
a product 1
a punct 3
a signature 1
a splunk_server 1
a splunk_server_group 4
timeendpos 1
timestartpos 1
a vendor 1
a vendor_product 1

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1665615258.534)

Time	Event
5/16/22 2:25:55.000 PM	May 16 14:25:55 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[271868954]: filename[desicapuano.com.siteindices.com&dtd=297] filemime[application/octet-stream] file_extension[com&dtd=297] length[28516b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[9b3f00dcfcd6f35a86e181817a190c74a53dfb866f09ba96b16734669907ac99] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[7] Active faster connections[7] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 2:25:55.000 PM	May 16 14:25:55 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[271868910]: filename[desicapuano.com.siteindices.com&dtd=307] filemime[application/octet-stream] file_extension[com&dtd=307] length[31145b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[d13be2d858fb3cdf75de7c8d55de2db4708e28fa989e564ddead924568bb5ee4] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[9] Active faster connections[9] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new

Time	Event
5/16/22 2:25:55.000 PM	May 16 14:25:55 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[271868894]: filename[desicapuano.com.siteindices.com&dtd=285] filemime[application/octet-stream] file_extension[com&dtd=285] length[30153b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[789dfd7237c4ed2634d39b13694c81bd086203d8d86ce9e590661ad8adf9b970] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[10] Active faster connections[10] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 2:22:51.000 PM	May 16 14:22:51 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[271840933]: filename[desicapuano.com.ico] filemime[application/octet-stream] file_extension[ico] length[780b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[4535e4573cf901ea455b825327d1d48c9eeb160bcabe6a75d58581fdef11501a] From[Cache] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 2:22:49.000 PM	May 16 14:22:49 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[271840752]: filename[www.desicapuano.com.ico] filemime[application/octet-stream] file_extension[ico] length[780b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[4535e4573cf901ea455b825327d1d48c9eeb160bcabe6a75d58581fdef11501a] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new

Time	Event
5/16/22 7:19:21.000 AM	May 16 07:19:21 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267449993]: filename[www.desicapuano.com.ico] filemime[application/octet-stream] file_extension[ico] length[780b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[4535e4573cf901ea455b825327d1d48c9eeb160bcabe6a75d58581fdef11501a] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:34.000 AM	May 16 06:14:34 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267063004]: filename[desicapuano.com.siteindices.com&dtd=127] filemime[application/octet-stream] file_extension[com&dtd=127] length[34846b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[db66cbe87382fa23ed415b5330e778dfe1a4e8175a78dfdfe91987ac234d299a] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:33.000 AM	May 16 06:14:33 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267062917]: filename[desicapuano.com.siteindices.com&dtd=112] filemime[application/octet-stream] file_extension[com&dtd=112] length[25447b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[2780ce78d0b3a88b5a58c9d7a3c5efb7c6db5c0176740e9c4eb619b0e8af1e6a] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new

Time	Event
5/16/22 6:14:33.000 AM	May 16 06:14:33 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267062791]: filename[desicapuano.com.siteindices.com&dtd=147] filemime[application/octet-stream] file_extension[com&dtd=147] length[38704b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[f48bedac035a509daaaacafd761973d6c59e7438fd964443666b4099d3575f43] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:33.000 AM	May 16 06:14:33 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267062790]: filename[desicapuano.com.siteindices.com&dtd=153] filemime[application/octet-stream] file_extension[com&dtd=153] length[35954b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[7192df80b38a414f92066d93fc542e4a92bf5b90abb393eed1fbcb6c80992627] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[4] Active faster connections[4] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:26.000 AM	May 16 06:14:26 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267061978]: filename[desicapuano.com.siteindices.com&dtd=1834] filemime[application/octet-stream] file_extension[com&dtd=1834] length[35241b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[3022ace1c75ccf26dd792fe5a840a7f56eb82394537570be3fc17e781fd2790f] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new

Time	Event
5/16/22 6:14:25.000 AM	May 16 06:14:25 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267061868]: filename[desicapuano.com.siteindices.com&dtd=161] filemime[application/octet-stream] file_extension[com&dtd=161] length[23143b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[d6f84a034b0a8f97fb67cfb572e65311cf1f7dc203f4e02ba63a1f44cea1b843] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[5] Active faster connections[5] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:25.000 AM	May 16 06:14:25 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267061814]: filename[desicapuano.com.siteindices.com&dtd=167] filemime[application/octet-stream] file_extension[com&dtd=167] length[33106b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[285824741d96d55343c25a97ea8d5e61041444a8141a33ac41082f719beefb4f] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[3] Active faster connections[3] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new
5/16/22 6:14:25.000 AM	May 16 06:14:25 chancellor2.vpd.bc.ca amp_logs_splunk: Info: Binary scan on instance[0] id[267061813]: filename[desicapuano.com.siteindices.com&dtd=153] filemime[application/octet-stream] file_extension[com&dtd=153] length[32972b] ampverdict[(1, 1, 'amp', '', 0, 0, False)] scanverdict[0] malwareverdict[0] spyname[] SHA256[6ca006355b4926f41ca3e99338e2a8d1e8727bb9c861c0049d5ce77eb922cba9] From[Cloud] uploadreason[File type is not configured for sandboxing] verdict_str[UNSCANNABLE] is_slow[0] scans_in_flight[4] Active faster connections[4] Active slower connections[0] host = 10.250.33.37 source = cisco.wsa_11.7 sourcetype = cisco:wsa:squid:new