Wednesday, 13 February 2019

Threat Hunting #23 - Microsoft Windows DNS Server / Analytical

DNS queries and responses are a key data source for network defenders in support of incident response as well as intrusion discovery. If these transactions are collected for processing and analytics in a big data system, they can enable a number of valuable security analytic scenarios.

In this post we suppose that you have already configured DNS Analytical and the logs are being forwarded to your Log Management or SIEM solution (not part of this post). Our main objective in this post is to share with you some basic use cases that you can start with to have some visibility on eventual suspicious DNS communications.

The main MS DNS Analytics events we will be using are limited to:

- 256 - QUEY_RECEIVED -> DNS query
- 257 - RESPONSE_SUCCESS -> DNS response

Example of 256 event:

```
QUERY_RECEIVED: TCP=0; InterfaceIP=1.2.3.4; Source=192.168.0.16; RD=1; QNAME=login.live.com.; QTYPE=1;
XID=33615; Port=65478; Flags=256;
PacketData=0x834F0100000100000000000056C6F67696E046C69766503636F6D0000010001; AdditionalInfo =
VirtualizationInstanceOptionValue: .
```

Example of 257 event:

```
RESPONSE_SUCCESS: TCP=0; InterfaceIP=1.2.3.4; Destination=192.168.0.16; AA=0; AD=0;
QNAME=ctldl.windowsupdate.com.; QTYPE=1; XID=706; DNSSEC=0; RCODE=0; Port=55896; Flags=33152; Scope=Default;
Zone=..Cache; PolicyName=NULL;
PacketData=0x02C2818000010007000000000563746C646C0D77696E646F777375706461746503636F6D0000010001C00C0005
00010000073700240A6175646F776E6C6F61640D77696E646F7773757064617465056E73617463036E657400C03500050001000
0006E000F02777509617A75726565646765C054C0650005000100000044000802777502656 3C068C0800005000100000012C001F
02777503777063096170722D35326464320B6564676563617374646E73C054C09400050001000000B2001203686C620B6170722
D35326464322D30C0A5C0BF00050001000000B2001104637331310377706305763063646EC054C0DD000100010000075300045
DB8DDF0; AdditionalInfo= VirtualizationInstance:.
```

As can be see above, the fields of interest we will need for our use cases are the following:

- Source or Destination IP of the machine that initiated the DNS request or that will receive the DNS Lookup answer.
- QNAME that contains the domain name that was requested.
- QTYPE indicate the requested DNS attribute (A, AAAA, MX, PTR, TXT etc.).
- RCODE indicate the operation result code (i.e. 0 No-error, 3 Non Existent Domain etc.).

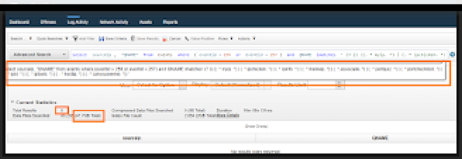
Use Case 1 - DNS requests to public IP online resolution web services:

Many malwares in the wild implement a first check to verify the public IP of the organization they've already infected and if it's within their targeted geographical scope they will operate accordingly, others implement the same check to avoid malware researchers and/or known online malware sandboxes. Below an example of an AQL hunting query you can use directly or turn it into a detection rule:

Blog Archive

► 2022 (2)
► 2021 (3)
► 2020 (4)
▼ 2019 (39)
► November (2)
► July (1)
► April (3)
► March (7)
▼ February (26)
Threat Hunting #24 - RDP over a Reverse SSH Tunnel
Threat Hunting #23 - Microsoft Windows DNS Server ...
IronPort: Password-Protected Archives
Threat Hunting #22 - Detecting user accounts set w...
Threat Hunting #21 - Hiding in plain sights with r...
IronPort: Blacklisted Attachments
Threat Hunting #20 - Detecting Process Doppelgängi...
Threat Hunting #19 - Procdump or Taskmgr - memory ...
Threat Hunting #18 - Run/RunOnce - Shell-Core El...
Threat Hunting #17 - Suspicious System Time Change
Threat Hunting #16 - Lateral Movement via DCOM - S...
Threat Hunting #15 - Detecting Doc with Macro invo...
Threat Hunting #14 - RDP Hijacking via RDPWRAP | f...
Threat Hunting #13 - Detecting CACTUSTORCH using S...
Threat Hunting #12 - Suspicious strings in Regist...
Threat Hunting #11 - Exposed Passwords
Threat Hunting #10 - Renamed/Modified Windows (ab)...
Threat Huting #9 - Impacket\Secretdump remote exec...

select sourceip, "QNAME" from events where (eventid=256 or eventid=257) and QNAME imatches '(?i)((.*myip.*)|(.*ipchicken.*)|(.*ipinfo.*)|(.*ipaddr.*)|(.*meineip.*)|(.*meuip.*)|(.*portquiz.*)|(.*portchecktool.*)|(.*ipid.*)|(.*iptools.*)|(.*hostip.*)|(.*canyouseeme.*))'



Note that you can expand the query to include more known good IP location WebService (to get through WebProxy reputation filters) .

Use Case 2 - DNS request to suspicious TLDs:

In this UC we will be comparing the queried domain names with a list of less business oriented Top Level Domain (i.e. .xyz, .ninja) which are not necessarily tied to malware or cyber attack activity, but as a Threat Hunter you will need to have this visibility and can be correlated with other building block events (i.e. unsigned program running from programdata and issuing DNS queries to a .xyz TLD).

For this example we will be using a list for the 2018 Top Shady TLDs by Symantec (note that the malicious TLDs are way more than those 20):

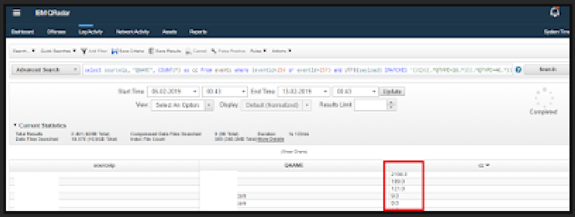
select sourceip, "QNAME" from events where QNAME IMATCHES '(.*country)|(.*stream)(.*download)|(.*xin)|(.*gdn)|(.*racing)|(.*jetzt)|(.*win)|(.*bid)|(.*vip)|(.*ren)|(.*kim)|(.*loan)(.*mom)|(.*party)|(.*review)|(.*trade)|(.*date)|(.*wang)|(.*accountants)'

Use Case 3 - DNS TXT or RRSIG Exfiltration:

A peak of DNS queries of type "TXT" or "RRSIG" (QTYPE=16 or QTYPE=46) may indicate some data exfiltration or DNS tunneling activity, for more information about DNS Query Types check here.

AQL query:

select sourceip, "QNAME", COUNT(*) as cc from events where (eventid=256 or eventid=257) and UTF8(payload) IMATCHES '(?i)((.*QTYPE=16.*)|(.*QTYPE=46.*))' GROUP BY sourceip, QNAME last 7 DAYS



Look for high count in short period (i.e. in 1 day more than 100 of TXT DNS requests from same source IP and the domain is not a known email provider).

Use Case 4 - DGA - Too many NX response from same source IP:

A peak in NXDomain responses (RCODE=3) may indicate a Domain generation algorithm activity (before landing on the newly DGA domain, the malware will perform several attempts, which majority of them are non existent domain names):

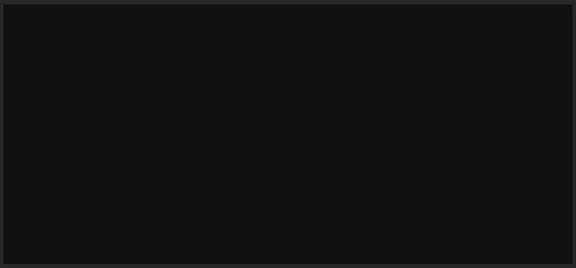
select sourceip, "QNAME", COUNT(*) as cc from events where eventid=257 and UTF8(payload) IMATCHES '(?i)(.*QTYPE=1.*RCODE=3.*)' GROUP BY sourceip, QNAME last 7 DAYS

Threat Hunting #6 - Hiding in plain sights with re...
Threat Hunting #5 - Detecting enumeration of users...
Threat Hunting #4 - Detecting Excel/Word documents...
Threat Hunting #3 - Detecting PsExec execution usi...
Threat Hunting #2 - Detecting PsLoggedOn exec usin...
Threat Hunting #1 - RDP Hijacking traces - Part 1

Use Case 5 - DNS requests to Very Long Domain Names :

Long domain names could be indicative of DGA or malware kill-switch or simply a legit long domain name (we've excluded QTYPE=249 "Transaction Key" for false positives removal).

select qname from events where "EventID"=256 and strlen("QNAME")>30 and not (UTF8(payload) IMATCHES '.*QTYPE=249.*') last 7 DAYS



Use Case 6 - DNS requests to known Dynamic DNS providers:

For this UC, you will need to build a reference list of known dynamic domain providers and map every QNAME of QTYPE=1 (A record) to this list. Example of such as list can be found here.

Usually ddns are associated either to malware activity or to IoT, like home camera, routers etc.

References:

https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6
https://gist.githubusercontent.com/neu5ron/8dd695d4cb26b6dcd997/raw/5c31ae47887abbff76461e11a3733f26bddd5d44/d

Posted by MENASEC at 02:00

Labels: dns, exfiltration, Microsoft DNS Analytical, threathunting, TLD

8 comments:

DedicatedHosting4u 30 April 2019 at 11:22

Thanks for sharing that such good information.

Reply

MENASEC 3 May 2019 at 22:55

Thanks for your feedback!

Reply

Richard H. Black 18 July 2019 at 12:32

Thanks for taking the time to discuss this, I feel strongly about it and love learning more on this topic. If possible, as you gain expertise, would you mind updating your blog with extra information? It is extremely helpful for me. CCTV Systems in Parramatta

Reply

james john 17 October 2019 at 14:26

The article was up to the point and described the information very effectively. Thanks to blog author for wonderful and informative post.
Security Solution consultant

Reply

Hello, this weekend is good for me, since this time i am reading this enormous informative article here at my home. Serious Security Melbourne

Reply

Jamison Tuesday 27 July 2020 at 16:48

Very detailed information, thank you!

Reply

Neu5ron (Nate Guagenti) 3 December 2020 at 12:34

Hey thanks for the refernce and great blog.
I believe the link was broken to the gist - should be https://gist.github.com/neu5ron/8dd695d4cb26b6dcd997

Reply

Qasim Khan 21 January 2022 at 09:38

I think this bolg is sesame and its provided fitness and good health information These weight loss supplements are generally made to be taken for just a brief hire american essay writers online timeframe and regularly contain a lot of caffeine and different stimulants.

Reply

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.