Introduction to Hunting Microsoft BITS

Silent but deadly

Mohamad khorram

WHOAMI

THREAT DETECTION ENGINEER AT SECUREMIND
HTTPS://WWW.LINKEDIN.COM/IN/MOHAMMAD-KHORRAM-608430199

CERTIFICATION

EC-COUNCIL CERTIFIED SECURITY ANALYST (CSA)

MICROSOFT BITS

Background Intelligent Transfer Service (BITS) is used by programmers and system administrators to download files from or upload files to HTTP web servers and SMB file shares. BITS will take the cost of the transfer into consideration, as well as the network usage so that the user's foreground work has as little impact as possible. BITS also handles network interruptions, pausing and automatically resuming transfers, even after a reboot. BITS includes PowerShell cmdlets for creating and managing transfers as well as the BitsAdmin command-line utility.

https://docs.microsoft.com/en-us/windows/win32/bits/background-intelligent-transfer-service-portal?redirectedfrom=MSDN

HOW BITS JOBS CAN BE CRATED

BITS can be accessed from BITSADMIN tool and PowerShell or Windows API

bitsadmin.exe /transfer /Download /priority Foreground #{remote_file} #{local_file}

Start-BitsTransfer -Priority foreground -Source #{remote_file} -Destination #{local_file}

WHAT DATASOURCE YOU NEED FOR HUNTING BITS

https://attack.mitre.org/techniques/T1197/

ID: T1197

Tactic: Defense Evasion, Persistence

Platform: Windows

Permissions Required: User, Administrator, SYSTEM

Data Sources: API monitoring, Packet capture, Windows event logs

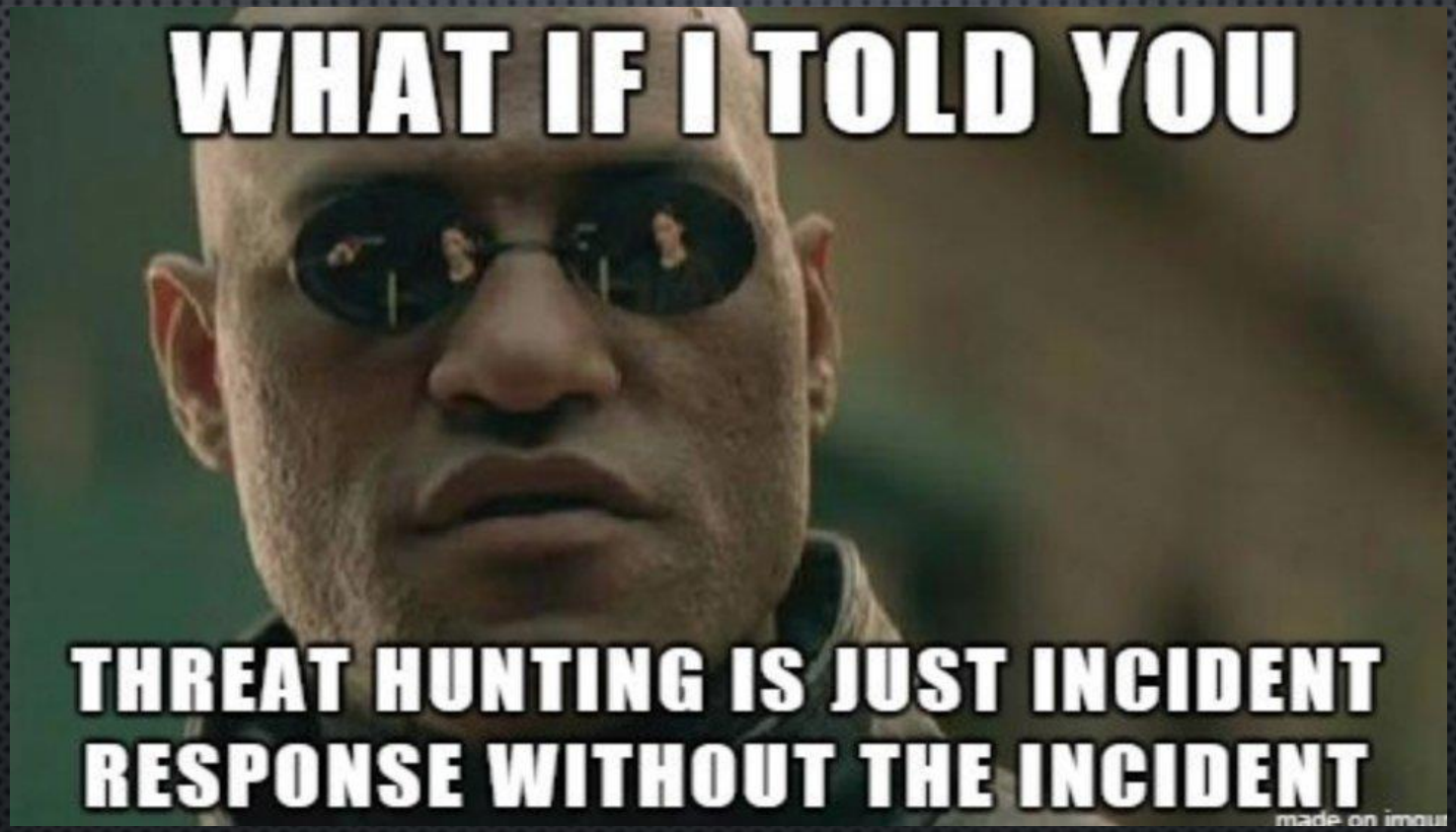
Defense Bypassed: Firewall, Host forensic analysis

Contributors: Ricardo Dias; Red Canary

Version: 1.0

Created: 18 April 2018

Last Modified: 16 July 2019


WHAT IF I TOLD YOU
THREAT HUNTING IS JUST INCIDENT RESPONSE WITHOUT THE INCIDENT

HUNTING WITH PROCESS MONITORING

With sysmon EventCode 1 we can monitor BITSADMIN.exe execution.

(EventCode=1 Image="*\\bitsadmin.exe" CommandLine IN ("*/create*" , "*/transfer*" , "*/Download*" , "*/priority*" "*/addfile" , "*/setnotifycmdline" , "*/complete" , "*/resume"))

(EventCode=1 Image=="*\\bitsadmin.exe") | stats count by CommandLine

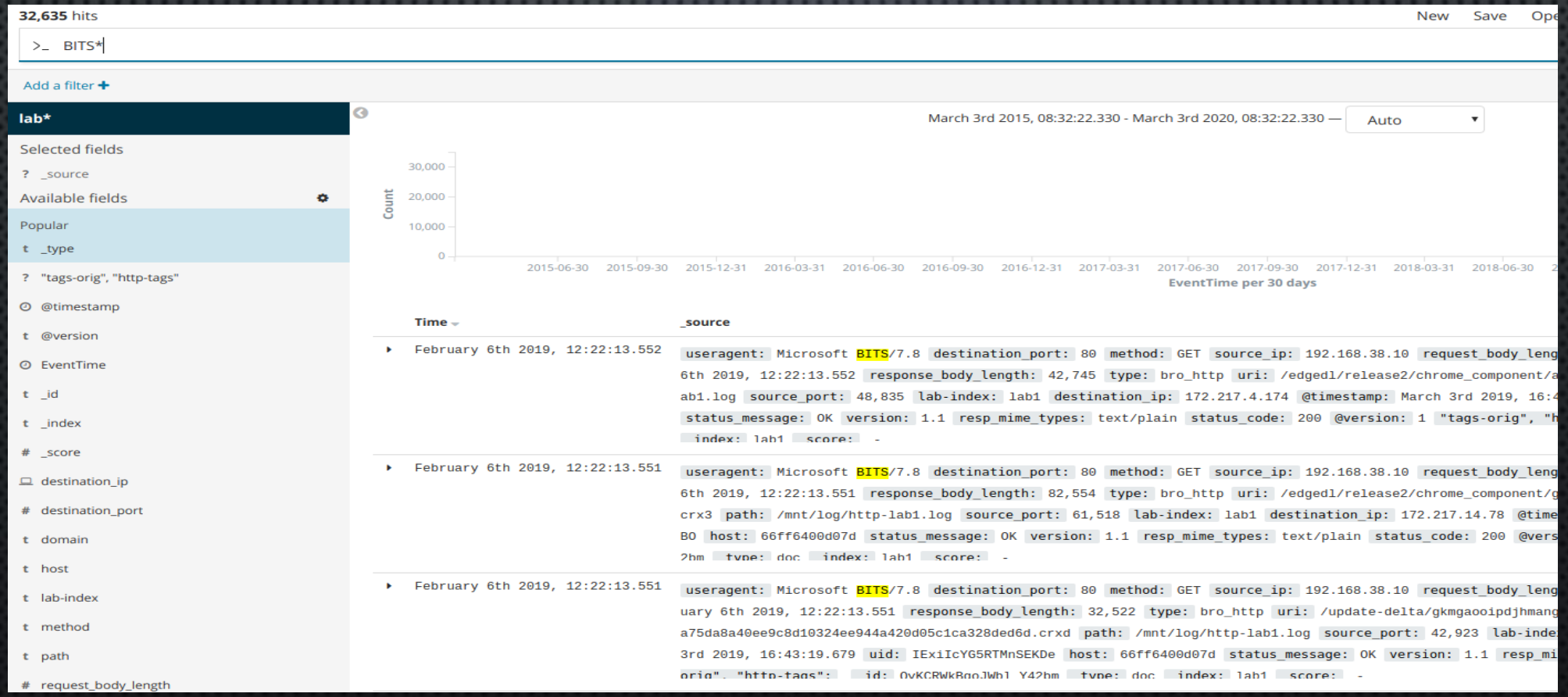
False positive: BITS jobs can be used by regular browsers or legal softwares. You should find what software's use BITS as a user agent and create baseline based on that and hunt what seems suspicious . It's recommended to use Second rule at first step to find out what BITS jobs is legal in your environment then finding the anomalies and the suspicious traffics.

HUNTING BITS WITH ZEEK/BRO LOGS

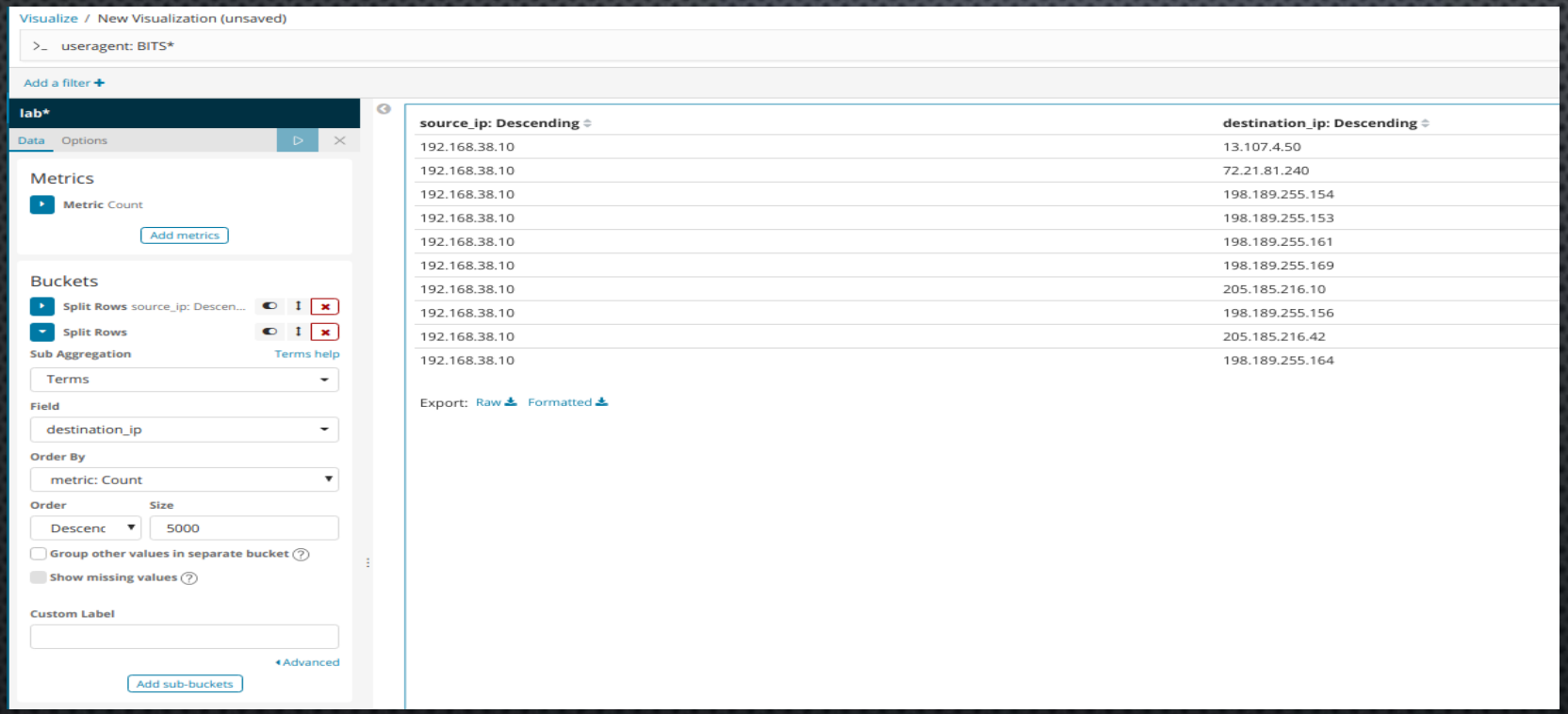
Another way to hunting BITS is using zeek/bro logs

You can also hunt for BITS jobs with NSM solutions like security onion or selks. In this example I used security onion and kibana visualization to manipulate data to something understandable to hunt.
In this scenario You will see BITS communication between one source IP and multiple destination addresses.

1-LETS SEE HOW MANY BITS LOGS WE HAVE IN OUR ENVIRONMENT



2-VISUALIZE DATA (SEE ADDRESSES ASSOCIATED WITH THIS TRAFFICS)



One easy things to do in this step is to check the destination addresses.
If the destination addresses are not associated with famous companies like Microsoft , google , adobe It can be suspicious

3-VISUALIZE DATA (SEE DOMAINS ASSOCIATED WITH THIS TRAFFICS)

domain.keyword: Ascending	Count
9.au.b1.download.windowsupdate.com	1
appexfinanceappupdate.blob.core.windows.net	1
bg.ds.a.dl.ws.microsoft.com	1
bg2.v4.a.dl.ws.microsoft.com	1
definitions.symantec.com	1
financeeus01.blob.appex.bing.com	1
ftp20.us.nero.com	1
im-ak.solidworks.com	1
im.solidworks.com	1
install10.nero.com	1

Export: Raw Formatted

1 2 3 4 5 ... 15

In this scenario i sorted domains In ascending order. as you navigate thorough pages you will see legal software's that use BITS as a update mechanism and it is ok but maybe if you look closely you will see odd stuff too. In my case I saw domains like pastebin.com and micusoft.bikeshops.tk
In the next step you can do forensic on the infected machines and find the cause of the infection

- For more information about latest threats and free detection rues please visit our website and LinkedIn page:
- https://www.threathunting.se/
- https://linkedin.com/company/threat-hunting

Thank you