**CEF Raw Log Entry**

04-08-2016 08:11:01 User.Alert 127.0.0.1 1 2016-04-08T08:11:01.10-07:00 PC-WIN123 Malwarebytes- Endpoint-Security 824 - - ï»¿CEF:0|Malwarebytes|MBMC|1.7.0.3208 MBAM:1.80.2.1012 DB:913030101 MBAE:1.08.2.1189|DETECTION|Exploit ROP attack blocked|5|deviceExternalId=d6961b91-6098-48c4-a64e- ff75c9e5550e dvchost=PC-WIN123 deviceDnsDomain=WORKGROUP deviceMacAddress=00-0C-29-7C-15-AB dvc=192.168.10.50 rt=Apr 08 2016 08:10:57 -07:00 cn1=1 cn1Label=ObjectTypeScanned cs6= cs6Label=ObjectScanned cat=DETECTION cn2=1 cn2Label=Action act=BLOCK outcome=success suser=jdoe cs5=data cs5Label=Data msg=Attacked application: C:\\Users\\jdoe\\Desktop\\iexplore.exe; Parent process name: explorer.exe; Layer: Protection Against OS Security Bypass; API ID: 453; Address: 0x76F5FE07; Module: ; AddressType: ; StackTop: 0x002F0000; StackBottom: 0x002ED000; StackPointer: ; Extra: fname=Internet Explorer filePath=C:\\Users\\jdoe\\Desktop\\iexplore.exe sourceServiceName=MBAE cs1= cs1Label=Payload cs2= cs2Label=PayloadChecksum cs3= cs3Label=PayloadUrl cs4= cs4Label=PayloadProc

**CEF Log Entry**

|  |  |  |
| --- | --- | --- |
| **HEADER** |  |  |
| Syslog Prefix | 04-08-2016 08:11:01 User.Alert 127.0.0.1 1 2016-04-08T08:11:01.10-07:00 PC-WIN123 Malwarebytes-Endpoint-Security 824 - - ï»¿CEF:0| | Basic Syslog Prefix. Typically does not need to be parsed (parsed by Default by most of SIEMs) |
| Device Vendor | Malwarebytes| | Malwarebytes is the only value currently |
| Device Product | MBMC| | MBMC is the only value currently |
| Device Version | 1.7.0.3208 MBAM:1.80.2.1012 DB:913030101 MBAE:1.08.2.1189| | Version of MBMC; versions of software and rules database |
| Device Event Class ID | DETECTION| |  |
| Name | Exploit ROP attack blocked | Name of threat (might me the name of explit technique or the name of malware such as “Ransom.Petya” or “backdoor.Bot.Gen” etc) |
| Severity | 5 |  |
| **EXTENSION** |  |  |
| deviceExternalId | d6961b91-6098-48c4-a64e-ff75c9e5550e | Internal ID of the client in Management Console |
| dvchost | PC-WIN123 | Hostname of attacked host |
| deviceDnsDomain | WORKGROUP | Domain of attacked host |
| deviceMacAddress | 00-0C-29-7C-15-AB | MAC address of attacked host |
| dvc | 192.168.10.50 | IP address of attacked host |
| rt | Apr 08 2016 08:10:57 -07:00 | Time on client |
| cn1 | 1 |  |
| cn1Label | ObjectTypeScanned |  |
| cs6 |  |  |
| cs6Label | ObjectScanned |  |
| cat | DETECTION | Category of event. In current release of MBMC there is only |
| cn2 | 1 |  |
| cn2Label | Action |  |
| act | BLOCK | Taken action |
| outcome | success | Result of action taken |
| suser | jdoe | Source host user |
| cs5 | data |  |
| cs5Label | Data |  |
| msg | Attacked application: C:\\Users\\jdoe\\Desktop\\iexplore.exe;  Parent process name: explorer.exe;  Layer: Protection Against OS Security Bypass; API ID: 453;  Address: 0x76F5FE07;  Module: ;  AddressType: ;  StackTop: 0x002F0000; StackBottom: 0x002ED000; StackPointer: ;  Extra: | Detailed message which might be optionally parsed to extract additional fields |
| Fname | Internet Explorer | Source process name |
| filePath | C:\\Users\\jdoe\\Desktop\\iexplore.exe | Full path to the process |
| sourceServiceName | MBAE | Detection product. Might be 2 values: MBAM or MBAE |
| cs1 |  |  |
| cs1Label | Payload | Payload. Applies to file-based attacks only (MBAM) |
| cs2 |  |  |
| cs2Label | PayloadChecksum | Payload CRC. Applies to file-based attacks only (MBAM) |
| cs3 |  |  |
| cs3Label | PayloadUrl | Payload URL. Applies to file-based attacks only (MBAM) |
| cs4 |  |  |
| cs4Label | PayloadProc | Payload process. Applies to file-based attacks only (MBAM) |

Catch All - With Threat - Backwards

^.\*?CEF:0\|Malwarebytes\|MBMC\|[^|]\*\|(?<vendorinfo>.\*?)\|Type:\s\w+,\sPort:\s\d+,\sProcess:\s[a-zA-Z0-9.]\*\|\d+\|.\*?act=(?<threatname>[a-zA-Z0-9\s]\*).\*?$

^.\*?CEF:0\|Malwarebytes\|MBMC\|[0-9.]\*\sMBAM:(?<version>[0-9.]\*)\sDB:\d+\|(?<vendorinfo>.\*?)\|Type:\s\w+,\sPort:\s\d+,\sProcess:\s[a-zA-Z0-9.]\*\|\d+\|.\*?act=(?<threatname>[a-zA-Z0-9\s]\*).\*?$

Catch All - With Threat

^.\*?CEF:0\|Malwarebytes\|MBMC\|[^|]\*\|(?<vendorinfo>.\*?)\|(?<threatname>.\*?)\|.\*?$

^.\*?CEF:0\|Malwarebytes\|MBMC\|[0-9.]\*\sMBAM:(?<version>[0-9.]\*)\sDB:\d+\|(?<vendorinfo>.\*?)\|(?<threatname>.\*?)\|.\*?$

Catch All

^.\*?CEF:0.\*?$

Threat Names:

Adware.PennyBee

Backdoor.Agent

Backdoor.Agent.NOIP

Backdoor.Agent.PGen

Backdoor.Andromeda

Backdoor.BetaBot

Backdoor.Bladabindi

Backdoor.Bot

Backdoor.Bot.Gen

Backdoor.LuminosityLink

Backdoor.Neutrino

Backdoor.Orcus

Backdoor.XTRat

Backdoor.Zapchast

CheatTool.CETTrainer

CrackTool.Agent

CrackTool.Agent.Keygen

CrackTool.Agent.Steam

CrackTool.KMSPico

FraudTool.YAC

HackTool.Agent

HackTool.Agent.Steam

HackTool.AutoKMS

HackTool.CheatEngine

HackTool.FilePatch

HackTool.Sniffer.WpePro

HackTool.WpaKill

Hijack.AutoConfigURL

Hijack.ControlPanelStyle

Hijack.HostFile

Hijack.Shell

PUP.Optional.Amonetize

PUP.Optional.APNToolbar

PUP.Optional.Ask

PUP.Optional.AuslogicsBoostSpeed

PUP.Optional.AuslogicsDiskDefrag

PUP.Optional.BrowseFox

PUP.Optional.BundleInstaller

PUP.Optional.Conduit

PUP.Optional.Coupoon

PUP.Optional.CrossBrowse

PUP.Optional.Crossrider

PUP.Optional.DNSUnlocker

PUP.Optional.DriverUpdate

PUP.Optional.FindingDiscount

PUP.Optional.GlobalUpdate

PUP.Optional.IFEO

PUP.Optional.InstallCore

PUP.Optional.Komodia

PUP.Optional.Linkury

PUP.Optional.Mindspark

PUP.Optional.ModGoog

PUP.Optional.MorePowerfulCleaner

PUP.Optional.Multiplug

PUP.Optional.MyPCBackup

PUP.Optional.OnlineIO

PUP.Optional.OpenCandy

PUP.Optional.PrxySvrRST

PUP.Optional.Qone8

PUP.Optional.Reimage

PUP.Optional.RelevantKnowledge

PUP.Optional.Sanbreel

PUP.Optional.SearchProtect

PUP.Optional.Softonic

PUP.Optional.SolutionReal

PUP.Optional.Somoto

PUP.Optional.StrongSignal

PUP.Optional.Tuto4PC

PUP.Optional.VOPackage

PUP.Optional.Vosteran

PUP.Optional.Wajam

PUP.Optional.WindowsProtectManager

PUP.Optional.Winsock

PUP.Optional.Yontoo

Ransom.Cerber

Ransom.Spora

RiskWare.Agent

RiskWare.BitCoinMiner

RiskWare.DontStealOurSoftware

Riskware.Downloader

RiskWare.ExtensionMismatch

Riskware.GameHack

RiskWare.IFEOHijack

RiskWare.Injector

RiskWare.IStealer

RiskWare.Tool.CK

RiskWare.Tool.HCK

Rogue.Agent.D.Generic

Rogue.ForcedExtension

Rogue.Multiple

Rogue.TechSupportScam

Rootkit.Fileless.MTGen

Rootkit.Komodia.PUA

Spyware.Agent

Spyware.InfoStealer

Spyware.PasswordStealer

Spyware.Zbot

Trojan.Agent

Trojan.Agent.CLK

Trojan.Agent.ED

Trojan.Agent.MSDGen

Trojan.Agent.Trace

Trojan.Agent.WR

Trojan.Banker

Trojan.Bedep

Trojan.BitCoinMiner

Trojan.BlockAV

Trojan.Boaxxe

Trojan.Clicker

Trojan.Crypt

Trojan.Crypt.NTH

Trojan.DNSChanger

Trojan.DNSChanger.ACMB2

Trojan.Downloader

Trojan.Dropper

Trojan.Egguard.PrxySvrRST

Trojan.Elex

Trojan.FakeMS

Trojan.Fileless.MTGen

Trojan.Glupteba

Trojan.Injector

Trojan.KillAV

Trojan.Kryptic

Trojan.Malpack

Trojan.Miuref

Trojan.ProxyAgent

Trojan.Qhost

Trojan.Reconyc

Trojan.Sefnit

Trojan.ServStart

Trojan.SProtector

Trojan.StartPage

Trojan.StolenData

Trojan.Swrort

Trojan.Upatre

Trojan.Vilsel

Trojan.Wdfload

Trojan.WisdomEyes

Trojan.WMIHijacker.ClnShrt

Virus.Neshta

Virus.Ramnit

Worm.Agent

Worm.Autorun

Worm.AutoRun.FLDGen

Worm.Brontok

Worm.Parite

Worm.Passwordstealer