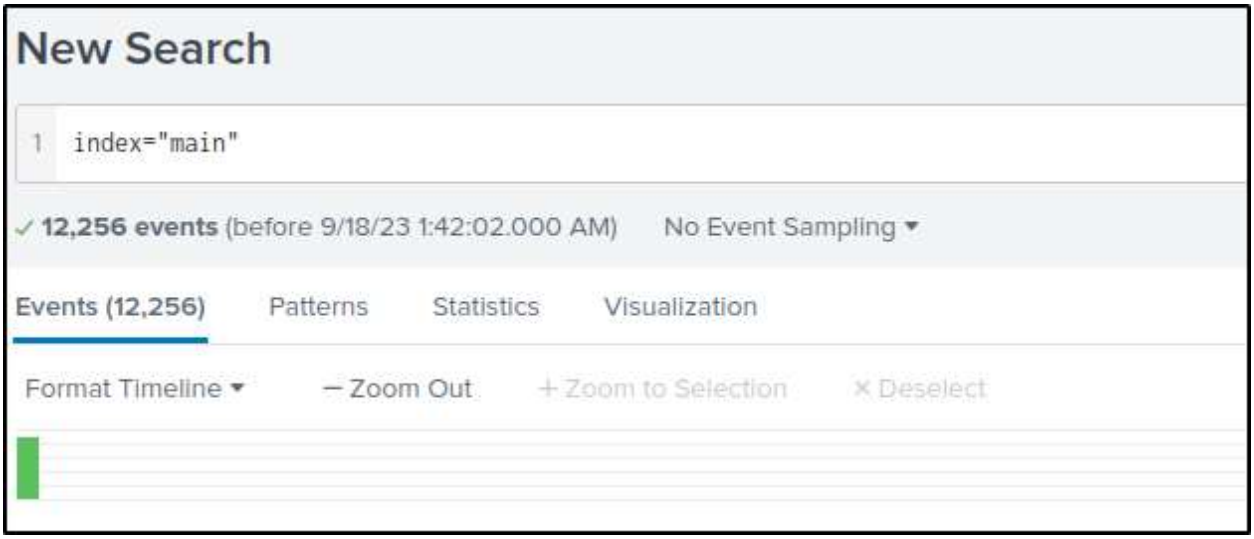
Investigation with Splunk

Scenario: SOC Analyst **Johny** has observed some anomalous behaviors in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some backdoor. His manager has asked him to pull those logs from suspected hosts and ingest them into Splunk for quick investigation. Our task as SOC Analyst is to examine the logs and identify the anomalies.

Query the “main” index and check the events.

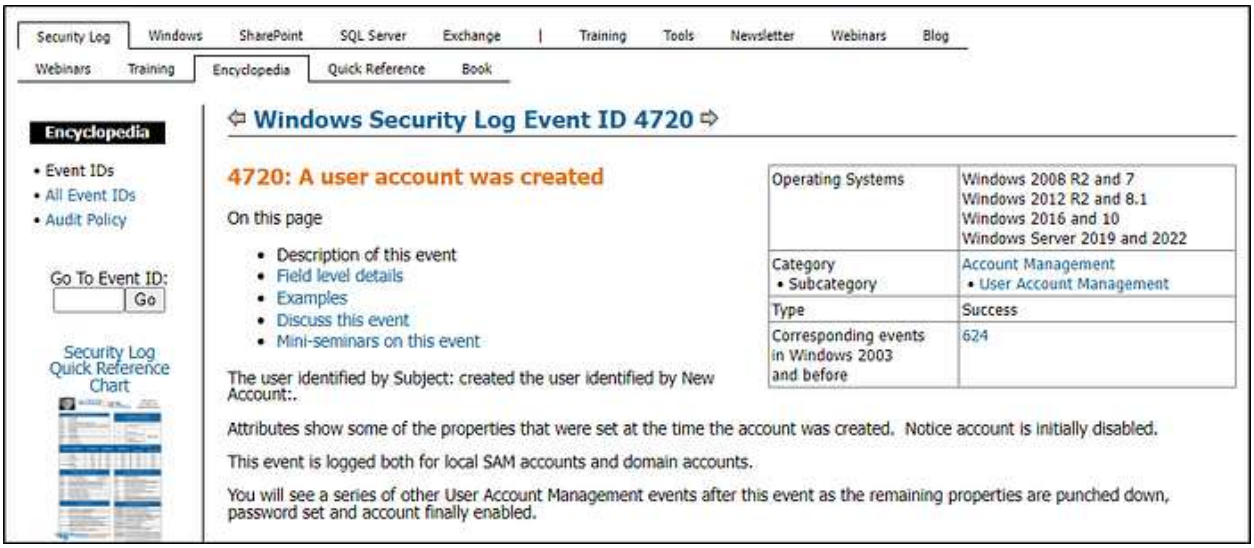
index="main”

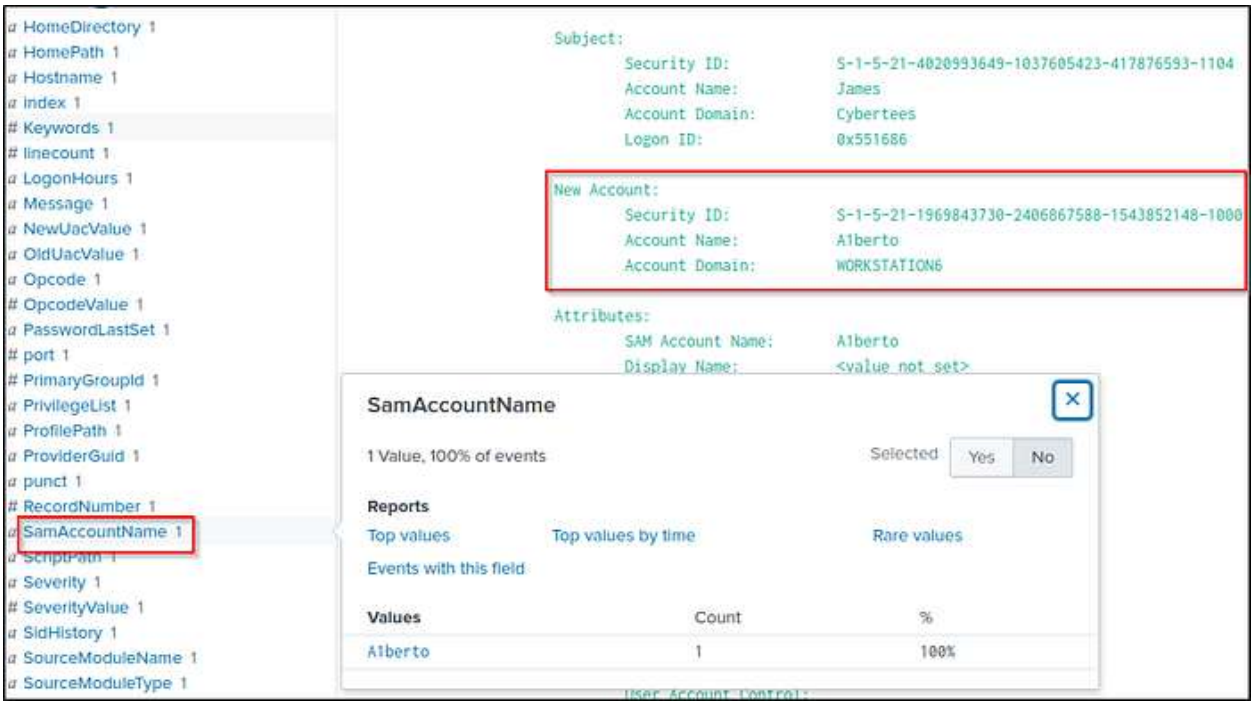


On one of the infected hosts, the adversary was successful in creating a backdoor user. To find let’s use the below command.

Event ID 4720 is logged when a user account is created.

index="main" EventID="4720”





On the same host, a registry key was also updated regarding the new backdoor user.

This would query to Sysmon events that logged modifications of a registry value.

index="main" EventID=13 A1berto

Event ID 13: RegistryEvent (Value Set)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type `DWORD` and `QWORD`.

Click on the "TargetObject" field to display the value of the object that was modified.

Examine the logs and identify the user that the adversary was trying to impersonate.

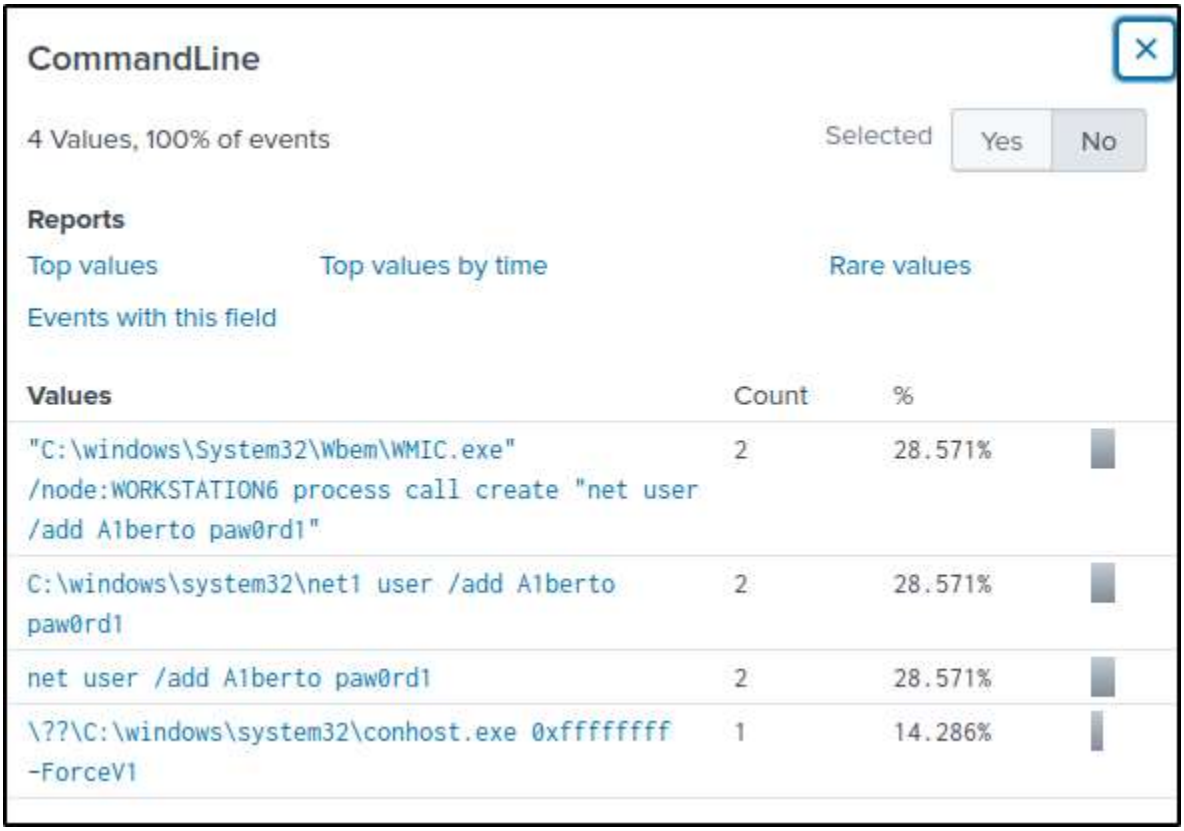
index="main"

The names of users are found in the "User" field. The newly created user "A1berto" is not the same as "Alberto"; therefore, "Alberto" is being impersonated.

Filter events with ID of 4688 of Sysmon event ID of 1.

index="main" EventID=1 OR EventID=4688 A1berto

Select the "CommandLine" field. Of the values, the first set of commands is a command a remote user would use because the "wmic" is a command-line tool which can be leveraged for remote execution of commands.



⇦ Windows Security Log Event ID 4688 ⇨

4688: A new process has been created

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Process Tracking • Process Creation
Type	Success
Corresponding events in Windows 2003 and before	592

Event 4688 documents each program that is executed, who the program ran as and the process that started this process.

When you start a program you are creating a "process" that stays open until the program exits. This process is identified by the Process ID:. You can correlate this event to other events by Process ID to determine what the program did while it ran and when it exited (event 4689).

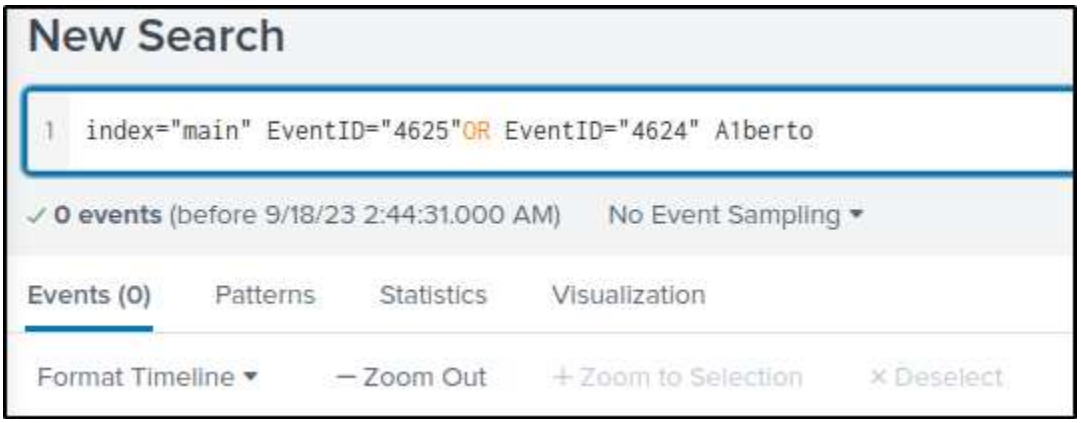
Win2012R2 adds Process Command Line.

Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The `ProcessGUID` field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the `HashType` field.

The query will filter events where successful and failed account logon attempts were made by the backdoor user.

index="main" EventID="4625" OR EventID="4624" A1berto



⇦ Windows Security Log Event ID 4624 ⇨

4624: An account was successfully logged on

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Logon/Logoff • Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

⇦ Windows Security Log Event ID 4625 ⇨

4625: An account failed to log on

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Logon/Logoff • Logon
Type	Failure
Corresponding events in Windows 2003 and before	529 , 530 , 531 , 532 , 533 , 534 , 535 , 536 , 537 , 539

This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.

The following query would filter Powershell events.

index="main" EventID="4104" OR EventID="4103"

Only one host was identified where the PowerShell commands were executed.

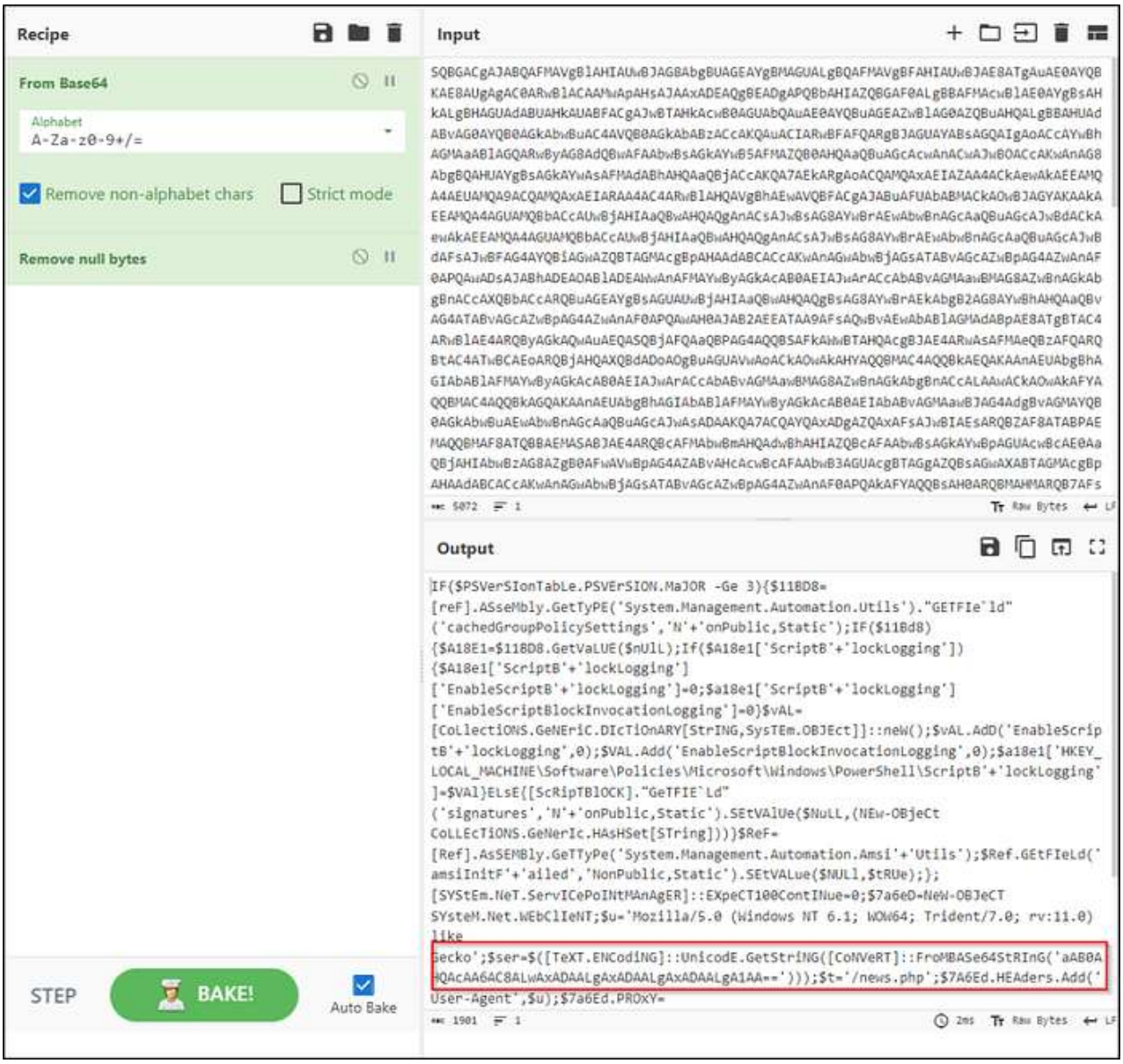
Using the same query from the previous question, there were 79 PowerShell activities that were monitored.

The modified query will extract the value of "Host Application" from the field "ContextInfo", present it on a table without duplicate commands.

```
index="main" EventID="4104" OR EventID="4103"
|rex field=ContextInfo "Host Application = (?<Command>[^\r\n]+)"
| table Command
| dedup Command
```

There is only one command value and it is base64 encoded.

Copied the encoded value and decoded it in cyberchef.



The decoded strings included a script to modify the PowerShell script block logging setting. Additionally, there seems to be a base64-encoded value that may refer to a domain name or an IP address, given that "/news.php" could be a URL or subdirectory.

Copied the value of the base64 string, decoded them, then defanged the output. So the base64 encoded string refers to an IP address.