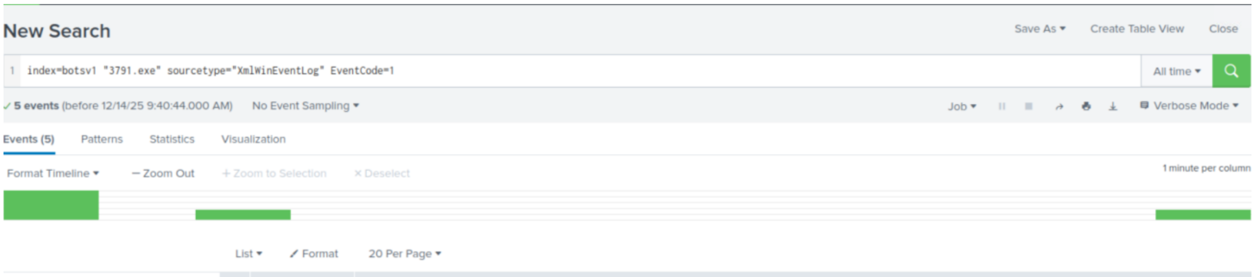
SPLUNK INSTALLATION 2025/12/14

Once the attacker has successfully exploited the security of a system, he will try to install a backdoor or an application for persistence or to gain more control of the system. This activity comes under the installation phase.

In the previous Exploitation phase, we found evidence of the webserver iamreallynotbatman.com getting compromised via brute-force attack by the attacker using the python script to automate getting the correct password. The attacker used the IP" for the attack and the IP to log in to the server. This phase will investigate any payload / malicious program uploaded to the server from any attacker's IPs and installed into the compromised server.

To begin an investigation, we first would narrow down any http traffic coming into our server **192.168.250.70** containing the term ".exe." This query may not lead to the findings, but it's good to start from 1 extension and move ahead.

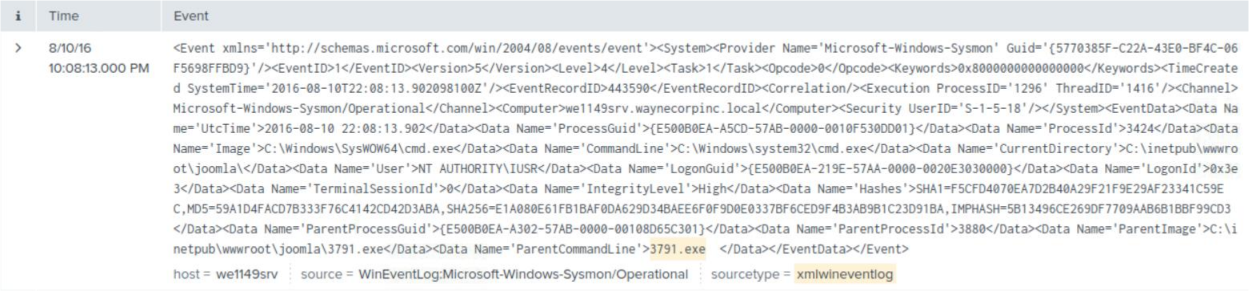
STEP 1: Sysmon also collects the Hash value of the processes being created. What is the MD5 HASH of the program 3791.exe?



```
index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1
```

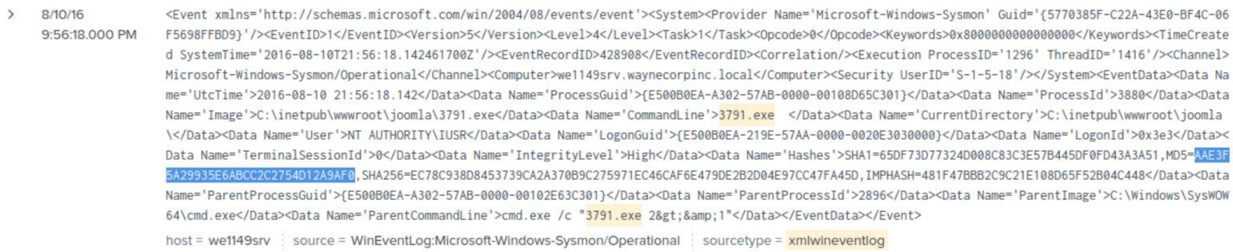
✓ 5 events (before 12/14/25 9:40:44.000 AM)

I queried the index using the process name, sourcetype, and process creation event code to initiate the investigation: index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1.



8/10/16 10:08:13.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06
F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreate
d SystemTime='2016-08-10T22:08:13.902098100Z'/><EventRecordID>443590</EventRecordID><Correlation/><Execution ProcessID='1296' ThreadID='1416'/><Channel>
Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149srv.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Na
me='UtcTime'>2016-08-10 22:08:13.902</Data><Data Name='ProcessGuid'>{E500B0EA-A5CD-57AB-0000-0010F530DD01}</Data><Data Name='ProcessId'>3424</Data><Data
Name='Image'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe</Data><Data Name='CurrentDirectory'>C:\inetpub\wwwro
ot\joomla\</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>{E500B0EA-219E-57AA-0000-0020E3030000}</Data><Data Name='LogonId'>0x3e
3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=F5CFD4070EA7D2B40A29F21F9E29AF23341C59E
C,MD5=59A1D4FACD7B333F76C4142CD42D3ABA,SHA256=E1A080E61FB1BAF0DA629D34BAEE6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA,IMPHASH=5B13496CE269DF7709AAB6B1BBF99CD3
</Data><Data Name='ParentProcessGuid'>{E500B0EA-A302-57AB-0000-00108D65C301}</Data><Data Name='ParentProcessId'>3880</Data><Data Name='ParentImage'>C:\i
netpub\wwwroot\joomla\3791.exe</Data><Data Name='ParentCommandLine'>3791.exe  </Data></EventData></Event>
host = we1149srv   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog
```



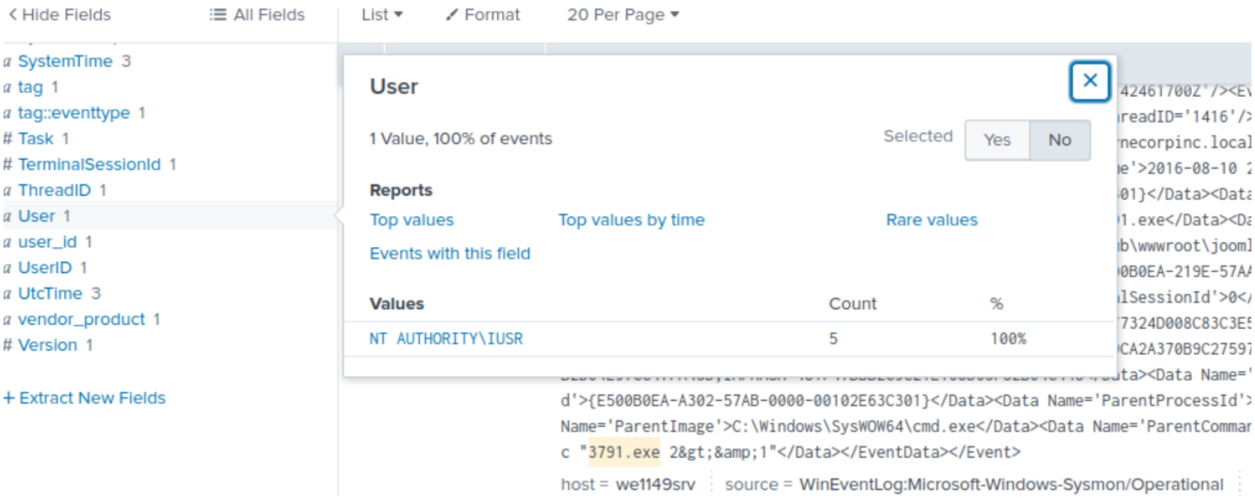
8/10/16
9:56:18.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06
F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreate
d SystemTime='2016-08-10T21:56:18.142461700Z'/><EventRecordID>428908</EventRecordID><Correlation/><Execution ProcessID='1296' ThreadID='1416'/><Channel>
Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149srv.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Na
me='UtcTime'>2016-08-10 21:56:18.142</Data><Data Name='ProcessGuid'>{E500B0EA-A302-57AB-0000-00108D65C301}</Data><Data Name='ProcessId'>3880</Data><Data
Name='Image'>C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Name='CommandLine'>3791.exe  </Data><Data Name='CurrentDirectory'>C:\inetpub\wwwroot\joomla
\</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>{E500B0EA-219E-57AA-0000-0020E3030000}</Data><Data Name='LogonId'>0x3e3</Data><
Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F
5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448</Data><Data
Name='ParentProcessGuid'>{E500B0EA-A302-57AB-0000-00102E63C301}</Data><Data Name='ParentProcessId'>2896</Data><Data Name='ParentImage'>C:\Windows\SysWOW
64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /c "3791.exe 2&gt;&amp;1"</Data></EventData></Event>
```

host = we1149srv | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

I investigated the first 2 events looking to find the difference and which I would select moving forward. Sysmon Event ID 1 recorded the execution of the 32-bit Command Prompt (cmd.exe) from the SysWOW64 directory, providing visibility into the process path, parent process, and command-line activity sourced from the second event. This validated my search for the MD5 hash.

STEP 2: Looking at the logs, which user executed the program 3791.exe on the server?



a SystemTime 3
a tag 1
a tag::eventtype 1
Task 1
TerminalSessionId 1
a ThreadID 1
a User 1
a user_id 1
a UserID 1
a UtcTime 3
a vendor_product 1
Version 1

+ Extract New Fields

User

1 Value, 100% of events

Selected Yes [✓ No]

Reports

Top values | Top values by time | Rare values

Events with this field

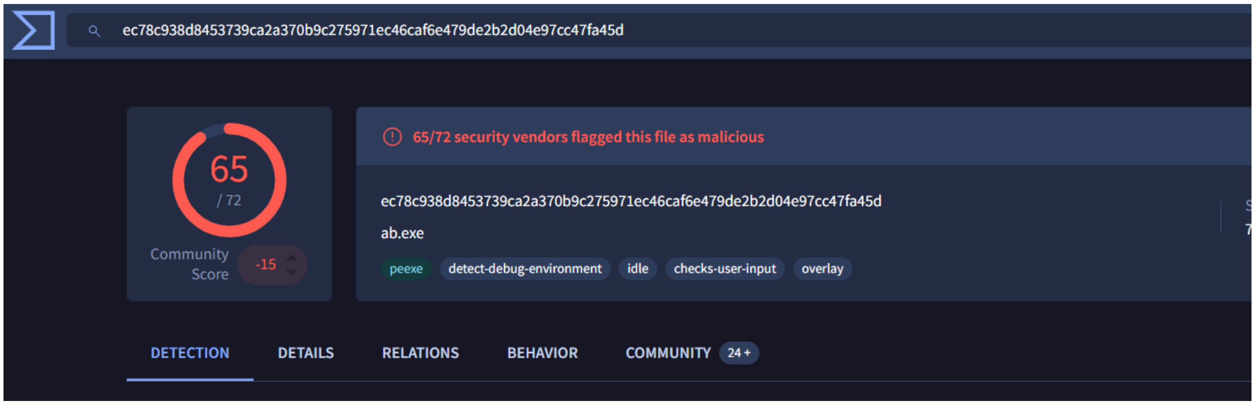
Values	Count	%
NT AUTHORITY\IUSR	5	100%

```
d'>{E500B0EA-A302-57AB-0000-00102E63C301}</Data><Data Name='ParentProcessId'>
Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentComman
c "3791.exe 2&gt;&amp;1"</Data></EventData></Event>
```

host = we1149srv | source = WinEventLog:Microsoft-Windows-Sysmon/Operational

I navigated to the left side of the page and scrolled down the fields looking to identify the 'User' – NT AUTHORITY\IUSR

STEP 3: Search hash on the virustotal. What other name is associated with this file 3791.exe?



ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

65/72 security vendors flagged this file as malicious

ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

ab.exe

I opened up a new window and searched up virustotal to find the name associated with the file – **ab.exe.**

Conclusion Summary

In the installation phase, Splunk and Sysmon logs were analysed to identify post-exploitation activity on the compromised web server. The investigation confirmed the execution of a suspicious executable, 3791.exe, following the brute-force compromise. Process creation events revealed the MD5 hash, the executing user account, and execution context. VirusTotal enrichment linked the file to a known malicious variant, confirming malicious installation and attacker persistence.