

יום חמישי 15 אוגוסט 2024 16:08

Alonzo Spire is fascinated by AI after noticing the recent uptick in usage of AI tools to help aid in daily tasks. He came across a sponsored post on social media about an AI tool by Google. The post had a massive reach, and the Page which posted had 200k+ followers. Without any second thought, he downloaded the tool provided via the Post. But after installing it he could not find the tool on his system which raised his suspicions. A DFIR analyst was notified of a possible incident on Forela's sysadmin machine. You are tasked to help the analyst in analysis to find the true source of this odd incident.

By checking the Edge browser history file using DB Browser, I found the Facebook URL:

Answer: <https://www.facebook.com/AI.ultra.new/posts/pfbid0BqpxXypMtY5dWGy2GDfpRD4cQRppdNEC9SSa72FmPVKgik9iWNa2mRkpx9xzIAS1>

I extracted the timestamp 13355296200136503 from the last_visit_time field. Upon researching online, I found it to be in WebKit timestamp format. I used the following Python script for conversion:

```
def convert_webkit_timestamp(webkit_timestamp):
    # Convert microseconds to seconds
    seconds_since_1601 = webkit_timestamp / 1e6

    # Define the start date (January 1, 1601)
    epoch_start = datetime(1601, 1, 1)

    # Calculate the actual date and time
    visit_datetime = epoch_start + timedelta(seconds=seconds_since_1601)

    # Format the datetime in the desired format
    return visit_datetime.strftime('%Y-%m-%d %H:%M:%S')
```

```
C:\Users\Bubble\Desktop
λ python hara.py
Formatted Date and Time: 2024-03-19 04:30:00
```

Task 3:
Alonzo downloaded a file on the system thinking it was an AI Assistant tool. What is name of the archive file downloaded?

downloads														
Filter in any column														
id		guid	current_path	target_path	start_time	received_bytes	total_bytes	state	danger_type	interrupt_reason	hash	end_time		
Filter	Filter		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1		29db9070-82f3-4810-adb9-86622f918df2	C:\Users\alonzos.spire\Downloads\PSTools.zip	C:\Users\alonzos.spire\Downloads\PSTools.zip	1333855602705659	5282424	5282424	1	4	0		13338556030541184		
2		9ffc9c1c-a907-4a4f-8c13-77007660f36	C:\Users\alonzos.spire\Downloads\Windows_Dev Package.zip	C:\Users\alonzos.spire\Downloads\Windows_Dev Package.zip	133548812092344463	1114	1114	1	4	0		13354881212365338		
3		13514236-07fe-4f27-8701-a2650c276dd8	C:\Users\alonzos.spire\Downloads\theme.theme	C:\Users\alonzos.spire\Downloads\theme.theme	1335489506686876	2718	2718	1	4	0		13354895057371913		
4		5808e2fd-5318-4155-b529-e649db9c12c2	C:\Users\alonzos.spire\Downloads\theme.theme	C:\Users\alonzos.spire\Downloads\theme.theme	13354895302486473	2718	2718	1	4	0		13354895303133838		
5		216dbdc-cell1-4321-af3e-23aab4083af	C:\Users\alonzos.spire\Downloads\ALGemini Ultra For PC V1.0.1.rar	C:\Users\alonzos.spire\Downloads\ALGemini Ultra For PC V1.0.1.rar	1335529622571356	404274	404274	1	4	0		133552962233478287		

Task 4:
What was the full direct URL from where the file was downloaded?

referrer
Filter
https://learn.microsoft.com/
https://www.dropbox.com/
https://l.facebook.com/l.php?...

You're going to a link outside Facebook

The link you tried to go to is outside Facebook:
https://drive.usercontent.google.com/u/2/uc?id=1z-SGNVJCPE0fHA_Faz6N7mD5qf0E-A76Hl8export=download

Are you sure you want to follow this link?

[Go back](#) [Follow Link](#)

Walkthroughs Page 1

Answer: https://drive.usercontent.google.com/download?id=1z-5GnYICPE0HA_Faz6N7mD5qf0E-A76H&export=download

Task 5:
Alonzo then proceeded to install the newly download app, thinking that its a legit AI tool. What is the true product version which was installed?

After thorough investigation, I found the answer in the SOFTWARE registry under CurrentVersion > TaskCache > Uninstall.

2024-03-19 04:31:20	(ABCCE01-78A5-4554-A32A-4402 A4E838B3)	Install	3.32.3	Google	20240319	C:\Users\alonzospire\Downloads\AI_Gemini Ultra For PC V1.0.1\	MalExec.exe /([ABCCE01-78A5-4554-A32A-4402 A4E838B3)
---------------------	--	---------	--------	--------	----------	---	--

Answer: 3.32.3

Task 6:
When was the malicious product/package successfully installed on the system?

Using MFTCmd to parse the MFT file into a CSV file and analyzing it with Timeline Explorer, I found the MSI file with the timestamp.

Parent Path	File Name	Extension
=	=	=
.\Users\alonzospire\Downloads	AI_Gemini Ultra For PC V1.0.1	
.\Users\alonzospire\Downloads\AI_Gemini Ultra For PC V1.0.1	Google AI_Gemini Ultra For PC V1.0.1.msi	.msi

I checked the "Last Access0x10" tab

Last Access0x10
=
2024-03-19 04:33:05
2024-03-19 04:31:33

Answer: 2024-03-19 04:31:33

Task 7:
The malware used a legitimate location to stage its file on the endpoint. Can you find out the Directory path of this location?

This task was one of the latest, took me sometime to understand the answer is not the full path.
The first time I found this path is at task 8.

Answer: C:\Program Files (x86)\Google

Task 8:
The malware executed a command from a file. What is name of this file?

While exploring the logs for another task, I noticed a powershell script inside the powershell logs

Provider "Variable" is Started.

Details:
ProviderName=Variable
NewProviderState=Started
SequenceNumber=11
HostName=ConsoleHost
HostVersion=5.1.19041.2031
HostId=13df8b27-4a3b-49f2-9f21-e7f728e6bc0
HostApplication=powershell -ExecutionPolicy Bypass -File C:\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic/ru.ps1
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

So I search on the MFT for the path "Program Files (x86)\Google\Install" and then I found several files.

Parent Path	File Name	Extension
=	=	=
.\Program Files (x86)\Google\Install	nmmhkkgccagldglimedpic	
.\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic	background.js	.js
.\Program Files (x86)\Google\Install	New Folder #5d2	
.\Program Files (x86)\Google\Install\New Folder #5d2	account_manager (22).xls	.xls
.\Program Files (x86)\Google\Install	System.Deployment.dll	.dll
.\Program Files (x86)\Google\Install	Microsoft.VisualStudio.Dll	.Dll
.\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic	favicon.png	.png
.\Program Files (x86)\Google\Install	System.Web.DynamicData.Design.dll	.dll
.\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic	manifest.json	.json
.\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic	ru.ps1	.ps1
.\Program Files (x86)\Google\Install\New Folder #5d2	account_manager (21).xls	.xls
.\Program Files (x86)\Google\Install	install.cmd	.cmd
.\Program Files (x86)\Google\Install\New Folder #5d2	list_page (3).xlsx	.xlsx
.\Program Files (x86)\Google\Install\New Folder #5d2	account_manager (20).xls	.xls
.\Program Files (x86)\Google\Install	logo.ico	.ico
.\Program Files (x86)\Google\Install\nmmhkkgccagldglimedpic	content.js	.js

So I assumed that if the malware executed command from a file it will be from the cmd file.

Answer: install.cmd

Task 9:
What are the contents of the file from question 8? Remove whitespace to avoid format issues.

Same picture from task 8, I took the Entry number 51471 and used --de 514741 on MFTCmd.exe

54502	<input type="checkbox"/>	51471	4	51349	4	<input checked="" type="checkbox"/>	.\Program Files (x86)\Google\Install	install.cmd
-------	--------------------------	-------	---	-------	---	-------------------------------------	--------------------------------------	-------------

```
ASCII: @echo off
powershell -ExecutionPolicy Bypass -File "%~dp0nmmhkkgccagldglimedpic/ru.ps1"
```

Then I went to CyberChef and used the Remove whitespace recipe

```
Input

@echo off
powershell -ExecutionPolicy Bypass -File "%~dp0nmhkkegccagldgiimedpic/ru.ps1"

Output

@echooffpowershell-ExecutionPolicyBypass-File"%~dp0nmhkkegccagldgiimedpic/ru.ps1"

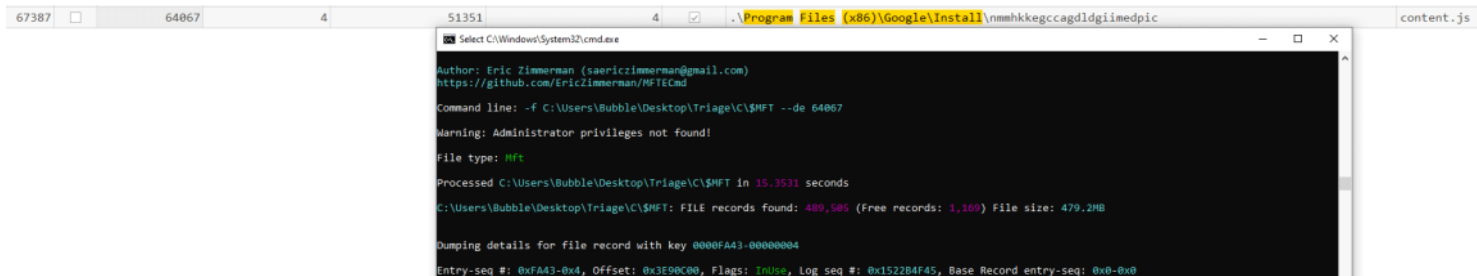
Answer: @echooffpowershell-ExecutionPolicyBypass-File"%~dp0nmhkkegccagldgiimedpic/ru.ps1"
```

Task 10:
What was the command executed from this file according to the logs?
Same as task 8, I found the command from the powershell logs.

```
Provider "Variable" is Started.
Details:
  ProviderName=Variable
  NewProviderState=Started
  SequenceNumber=11
  HostName=ConsoleHost
  HostVersion=5.1.19041.3031
  HostId=13d08a7-4a2b-49f2-9f21-ec7f028e6bc9
  HostApplication=powershell -ExecutionPolicy Bypass -File C:\Program Files (x86)\Google\Install\nmhkkgccagldgiimedpic/ru.ps1
  EngineVersion=
  RunspaceId=
  PipelineId=
  CommandName=
  CommandType=
  ScriptName=
  CommandPath=
  CommandLine=

Answer: powershell -ExecutionPolicy Bypass -File C:\Program Files (x86)\Google\Install\nmhkkgccagldgiimedpic/ru.ps1
```

Task 11:
Under malware staging Directory, a js file resides which is very small in size. What is the hex offset for this file on the filesystem?
I took the entry number and used the MFTECmd on it



Answer: 3E90C00

Task 12:
Recover the contents of this js file so we can forward this to our RE/MA team for further analysis and understanding of this infection chain. To sanitize the payload, remove whitespaces.
Same output in MFTECmd from task 11

```
ASCII:  var isContentScriptExecuted = localStorage.getItem('contentScriptExecuted');
if (!isContentScriptExecuted) {
  chrome.runtime.sendMessage({ action: 'executeFunction' }, function (response) {
    localStorage.setItem('contentScriptExecuted', true);
  });
}
```

I did the same thing in CyberChef like in Task 9

Input

```
var isContentScriptExecuted = localStorage.getItem('contentScriptExecuted');
if (!isContentScriptExecuted) {
  chrome.runtime.sendMessage({ action: 'executeFunction' }, function (response) {
    localStorage.setItem('contentScriptExecuted', true);
  });
}
```

Output

```
var isContentScriptExecuted=localStorage.getItem('contentScriptExecuted');if(!isContentScriptExecuted)
{chrome.runtime.sendMessage({action:'executeFunction'},function(response){localStorage.setItem('contentScriptExecuted',true)}};}
```

Answer: var isContentScriptExecuted=localStorage.getItem('contentScriptExecuted');if(!isContentScriptExecuted){chrome.runtime.sendMessage({action:'executeFunction'},function(response){localStorage.setItem('contentScriptExecuted',true)}};}

Task 13:
Upon seeing no AI Assistant app being run, alonzo tried searching it from file explorer. What keywords did he use to search?

Took me some time but after investigating all the artifacts from Registry I found the answer at the "WordWheelQuery"

WordWheelQuery

Key name	# values	# subkeys	Last write timestamp
C:\Users\Bubble\Desktop\Triage\C\Users\alonzo.spire\NTUSER.DAT			1601-01-01 00:00:00
CurrentVersion	0	39	2024-03-19 04:34:36
Explorer	12	43	2024-03-19 04:40:11
WordWheelQuery	2	0	2024-03-19 04:32:11
WordWheelQuery	2	0	2024-03-19 04:32:11

Search Term	Mru Position	Key Name	Last Write Timestamp
Google AI Gemini tool		WordWheelQuery	2024-03-19 04:32:11

Answer: Google Ai Gemini tool

Task 14:
When did alonzo searched it?

Same place from task 13

Last Write Timestamp

2024-03-19 04:32:11

Answer: 2024-03-19 04:32:11

Task 15:
After alonzo could not find any AI tool on the system, he became suspicious, contacted the security team and deleted the downloaded file. When was the file deleted by alonzo?

Inside the \$Recycle.Bin folder there is an archive file "SR2MU608.rar" which includes the MSI file

SR2MU608.rar

SR2MU608.rar (evaluation copy)

File Commands Tools Favorites Options H

Add Extract To Text View Delete

SR2MU608.rar\AI Gemini Ultra For PC V

Name

Google AI Gemini Ultra For PC V1.0.1.msi

I checked the USN Journal and filtered for the name "SR2MU608.rar" and found the timestamp

Update Timestamp

2024-03-19 04:34:16

2024-03-19 04:34:16

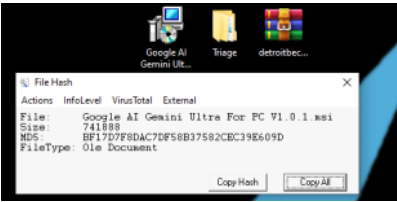
2024-03-19 04:34:16

Answer: 2024-03-19 04:34:16

Task 16:
Looking back at the starting point of this infection, please find the md5 hash of the malicious installer.

Inside the \$Recycle.Bin there is a file "SR2MU608.rar" contains the "Google AI Gemini Ultra For PC V1.0.1.msi" but the archive is protected with a password. After searching online, I found the file on Malware Bazaar with the password "022024" and obtained the hash.

SHA256 hash:	3f79fff587d4eae9ac530408280987e1317bacc7ada5acb163cfd618b9d932
SHA3-384 hash:	4c027fc43b50aafca54f51c9bcc14d043381d4c4ca3a602bf272a58b52ac31c7c9fd4930f1b214fb6a86ffff4d5e81
SHA1 hash:	9123d4abce7af105faa7c32c3a2ea5ad4d219d2c
MD5 hash:	a0af1cc1265b96de8699a4daeab236a7
humanhash:	bulldog-snake-fifteen-floor
File name:	AI.Gemini Ultra For PC V1.0.1.rar
Download:	download sample
File size:	404'274 bytes
First seen:	2024-03-16 11:01:47 UTC
Last seen:	Never
File type:	rar
MIME type:	application/x-rar
Note:	This file is a password protected archive. The password is: 022024
ssdeep	12288:1fdgARzjdLN4IKWGBc2FW2JH8lhnc8hl:1rtRln4HW12FW2l8+7l
TLSH	T1508423938C6C5A1F0ADCAC40E869F17DCEB774562F66C6174DC81688005BAC98802B37
TrID	61.5% (.RAR) RAR compressed archive (v5.0) (8000/1) 38.4% (.RAR) RAR compressed archive (gen) (5000/1)
Reporter	e24111111154168
Tags:	Facebook/Sinater FakeGeminiAI pw-022024 rar



Answer: BF17D7F8DAC7DF58B37582CEC39E609D