Noted,勒索調查

Sherlock Scenario

Simon, a developer working at Forela, notified the CERT team about a note that appeared on his desktop. The note claimed that his system had been compromised and that sensitive data from Simon's workstation had been collected. The perpetrators performed data extortion on his workstation and are now threatening to release the data on the dark web unless their demands are met. Simon's workstation contained multiple sensitive files, including planned software projects, internal development plans, and application codebases. The threat intelligence team believes that the threat actor made some mistakes, but they have not found any way to contact the threat actors. The company's stakeholders are insisting that this incident be resolved and all sensitive data be recovered. They demand that under no circumstances should the data be leaked. As our junior security analyst, you have been assigned a specific type of DFIR (Digital Forensics and Incident Response) investigation in this case. The CERT lead, after triaging the workstation, has provided you with only the Notepad++ artifacts, suspecting that the attacker created the extortion note and conducted other activities with hands-on keyboard access. Your duty is to determine how the attack occurred and find a way to contact the threat actors, as they accidentally locked out their own contact information.

* * *

About Noted

Simon, a developer working at Forela, notified the CERT team about a note that appeared on his desktop. The note claimed that his system had been compromised and that sensitive data from Simon's workstation had been collected. The perpetrators performed data extortion on his workstation and are now threatening to release the data on the dark web unless their demands are met. Simon's workstation contained multiple sensitive files, including planned software projects, internal development plans, and application codebases. The threat intelligence team believes that the threat actor made some mistakes, but they have not found any way to contact the threat actors. The company's stakeholders are insisting that this incident be resolved and all sensitive data be recovered. They demand that under no circumstances should the data be leaked. As our junior security analyst, you have been assigned a specific type of DFIR (Digital Forensics and Incident Response) investigation in this case. The CERT lead, after triaging the workstation, has provided you with only the Notepad++ artifacts, suspecting that the attacker created the extortion note and conducted other activities with hands-on keyboard access. Your duty is to determine how the attack occurred

and find a way to contact the threat actors, as they accidentally locked out their own contact information.

文件:

LootAndPurge.java@2023-07-24 145332

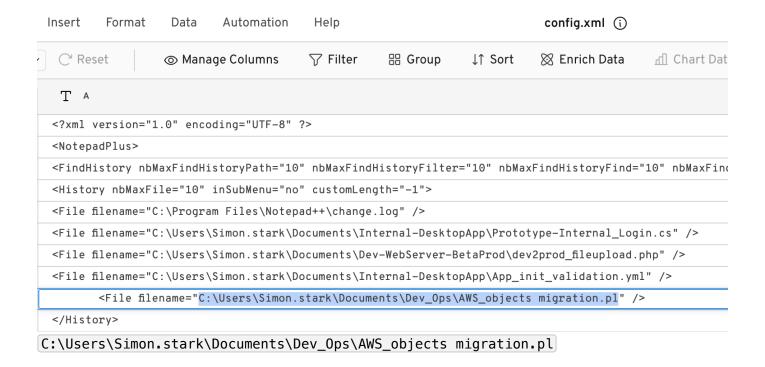
YOU HAVE BEEN HACKED.txt@2023-07-24 150548

config.xml

session.xml

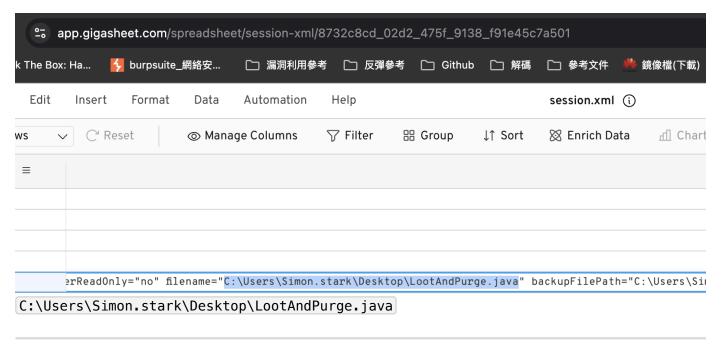
Task 1

What is the full path of the script used by Simon for AWS operations?



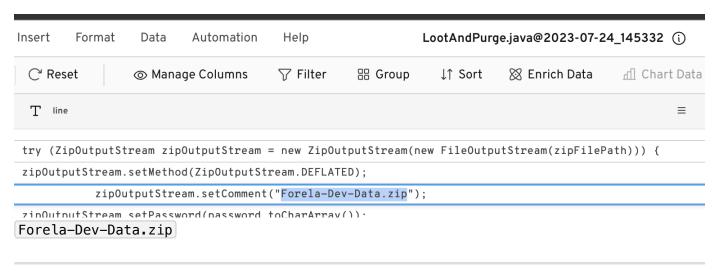
Task 2

The attacker duplicated some program code and compiled it on the system, knowing that the victim was a software engineer and had all the necessary utilities. They did this to blend into the environment and didn't bring any of their tools. This code gathered sensitive data and prepared it for exfiltration. What is the full path of the program's source file?



Task 3

What's the name of the final archive file containing all the data to be exfiltrated?



Task 4

What's the timestamp in UTC when attacker last modified the program source file?

originalFileLastModifTimestamp="-1354503710"
originalFileLastModifTimestampHigh="31047188"

原本想放入 Epoch 但好像怪怪的,卡很久,算不出來,我在htb論壇有找到別人的腳本參考:https://forum.hackthebox.com/t/noted-sherlock/307329/4

here is the code for the answere import datetime

These are the two parts of the timestamp

timestamp_low = -1354503710 timestamp_high = 31047188

O Combine the two parts to get the full timestamp

full_timestamp = (timestamp_high << 32) | (timestamp_low & 0xFFFFFFFF)

The timestamp is in 100-nanosecond intervals since January 1, 1601

Convert it to seconds and then to a datetime object

timestamp_seconds = full_timestamp / 10**7
timestamp = datetime.datetime(1601, 1, 1) + datetime.timedelta(seconds=timestamp_seconds)
print(timestamp)

腳本: https://github.com/a6232283/HTB/blob/main/Sherlocks/High-precision-timestamps.py

```
(root@ kali)-[/home/kali/Desktop]
# python3 High-precision-timestamps.py
2023-07-24 09:53:23.322723
Respendence of the control of
```

2023-07-24 09:53:23

Task 5

The attacker wrote a data extortion note after exfiltrating data. What is the crypto wallet address to which attackers demanded payment?

備份到這邊

-ormat	Data	Automation	Help			session.xml (i)
	⊚ Mana	ige Columns	∀ Filter	⊞ Group	↓↑ Sort	⊠ Enrich Data	<u>ரி</u> Chart Da
up\Loot/	AndPurge	.java@2023-07-	-24_145332"	originalFilel	_astModifTi	mestamp="-13545	03710" origina
						07-24_150548" <u>o</u>	
有3個鏈	接 						
Insert	Format	Data Auto	mation Help	Y	OU HAVE BEE	N HACKED.txt@2023	-07-24_15 (i
∨ C F	Reset	⊚ Manage Col	umns 🎖 Fi	lter 🔠 Group	↓↑ Sort	⊠ Enrich Data	_ Chart Data
Т	line						
						You have been hack	
	in. He mad		3011011110 40	rea and aproduce		20. 1110 2020 20 02	
	PAY US						
WE DO	NOT RELE	ASE YOUR COMPANY	' SECRETS TO P	UBLIC AND RETUR	N YOUR DATA S	AFELY TO YOU	
Fail	iure to ob	lige will result	in immediate	data leak to t	he public.		
For	detailed i	nformation and p	process , Visi	t any of the be	low links		

但都需要密碼:

i) https://pastebin.ai/bigbsy36toii) https://pastebin.com/xmTkajd5iii) https://pastecode.io/s/Orqtutec

```
√ Filter

                                                 器 Group
                                                             ↓↑ Sort

    ∴ Chart Data

 T line
Import java.utii.List,
import java.util.zip.ZipEntry;
import java.util.zip.ZipOutputStream;
public class Sensitive_data_extort {
public static void main(String[] args) {
String username = System.getProperty("user.name");
String desktopDirectory = "C:\\Users\\" + username + "\\Desktop\\";
List<String> extensions = Arrays.asList("zip", "docx", "ppt", "xls", "md", "txt", "pdf");
List<File> collectedFiles = new ArrayList<>();
collectFiles(new File(desktopDirectory), extensions, collectedFiles);
String zipFilePath = desktopDirectory + "Forela-Dev-Data.zip";
      String password = "sdklY57BLghvyh5FJ#fion_7";
```

輸入密碼後3個網頁顯示一樣內容



0xca8fa8f0b631ecdb18cda619c4fc9d197c8affca

Task 6

What's the email address of the person to contact for support?

同上

CyberJunkie@mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion