

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?

```
config.xml ⓘ
Reset | Manage Columns | Filter | Group | Sort | Enrich Data | Chart Data

T A
<?xml version="1.0" encoding="UTF-8" ?>
<NotepadPlus>
<FindHistory nbMaxFindHistoryPath="10" nbMaxFindHistoryFilter="10" nbMaxFindHistoryFind="10" nbMaxFindHistoryReplace="10" />
<History nbMaxFile="10" inSubMenu="no" customLength="-1">
<File filename="C:\Program Files\Notepad++\change.log" />
<File filename="C:\Users\Simon.stark\Documents\Internal-DesktopApp\Prototype-Internal_Login.cs" />
<File filename="C:\Users\Simon.stark\Documents\Dev-WebServer-BetaProd\dev2prod_fileupload.php" />
<File filename="C:\Users\Simon.stark\Documents\Internal-DesktopApp\App_init_validation.yml" />
<File filename="C:\Users\Simon.stark\Documents\Dev_Ops\AWS_objects migration.pl" />
</History>
```

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?

app.gigasheet.com/spreadsheet/session-xml/8732c8cd_02d2_475f_9138_f91e45c7a501

k The Box: Ha... burpsuite_網絡安... 漏洞利用參考 反彈參考 Github 解碼 參考文件 鏡像檔(下載)

Edit Insert Format Data Automation Help session.xml ⓘ

ws Reset Manage Columns Filter Group Sort Enrich Data Chart

```
erReadOnly="no" filename="C:\Users\Simon.stark\Desktop\LootAndPurge.java" backupFilePath="C:\Users\Si
```

C:\Users\Simon.stark\Desktop\LootAndPurge.java

Task 3

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

Insert Format Data Automation Help LootAndPurge.java@2023-07-24_145332 ⓘ

Reset Manage Columns Filter Group Sort Enrich Data Chart Data

T line

```
try (ZipOutputStream zipOutputStream = new ZipOutputStream(new FileOutputStream(zipFilePath))) {  
    zipOutputStream.setMethod(ZipOutputStream.DEFLATED);  
    zipOutputStream.setComment("Forela-Dev-Data.zip");  
    zipOutputStream.setPassword(password.toCharArray());  
}
```

Forela-Dev-Data.zip

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 answer
import datetime

These are the two parts of the timestamp

```
timestamp_low = -1354503710  
timestamp_high = 31047188
```

🔗 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)
```

脚本 : <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
```

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

有3個鏈接

[illegible]

但都需要密碼：

```
Reset Manage Columns Filter Group Sort Enrich Data Chart Data

line
import java.util.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