

Northeastern University

College of Computer and Information Science

Case Project

CY5210 Information System Forensics

Instructor: Elton Booker

Samriddhi

EXECUTIVE SUMMARY

The Shield SOC received a network alert that over the weekend (01-20-2019), two tools: BitTorrent and a Privacy Cleaner utility that were against the company's acceptable use policy and may be potentially unwanted programs (PUPs) were downloaded on one of their company assets. The incident response team identified the system of interest and requested that the forensic team further investigate the situation at hand. From the forensics team, Elton Booker was asked to image the system to perform an analysis in order to find out if there was any potential company policy violation.

To understand the extent and severity of the incident, the analysis performed by the forensics team determined that a USB device by the name "Kingston DataTraveler" was connected to the company's asset which had some documents related to the company. Additionally, certain software installations suggested that the company's data might have been copied and transferred to external sources.

Evidence indicates that the USB device was connected to the system while a user named S. Rogers was logged on. To prevent proprietary data from being removed from the company, it is essential to retrieve this USB device and conduct a thorough interrogation. Failure to do so may necessitate initiating legal action against the employee.

INTRODUCTION

The Shield SOC received a network alert that over the weekend (01-20-2019), two tools: BitTorrent and a Privacy Cleaner utility that were against the company's acceptable use policy and may be potentially unwanted programs (PUPs) were downloaded on one of their company assets. The next day, 01-21-2019, the incident response team was able to identify the system and requested the forensic team to further investigate the system and perform an analysis. From the forensics team, Elton Booker was asked to image the system in order to find out if there was any potential company policy violation. By using the Access Data FTK Imager tool, it was concluded that the image was acquired on 01-21-2019 at 7:56:28 PM on a Win 201x OS with a sector count of 125,829,120. The image's source data size was 61440 MB with 512 bytes per sector. The below figure shows that hashes were verified, and they matched the original image and the verification done by E. Booker.

```
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Verification Hashes]
MD5 verification hash: ed8faefff8b27232b542a17a08208742
SHA1 verification hash: 6226f14c9a2ad69f213548ecc08ccefdde903891
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 125,829,120
[Image]
Image Type: E01
Case number: 2019_Lab1
Evidence number: 001
Examiner: E. Booker
Notes: Potential Violations of Acceptable Use Policy
Acquired on OS: Win 201x
Acquired using: ADI3.1.1.8
Acquire date: 1/21/19 7:56:28 PM
System date: 1/21/19 7:56:28 PM
Unique description: Win10 Shield Image
Source data size: 61440 MB
Sector count: 125829120
[Computed Hashes]
MD5 checksum: ed8faefff8b27232b542a17a08208742
SHA1 checksum: 6226f14c9a2ad69f213548ecc08ccefdde903891

Image Information:
Acquisition started: Thu Sep 16 14:03:06 2021
Acquisition finished: Thu Sep 16 14:16:26 2021
Segment list:
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E01
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E02
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E03
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E04
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E05
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E06
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E07
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E08
D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy.E09

Image Verification Results:
Verification started: Thu Sep 16 14:16:27 2021
Verification finished: Thu Sep 16 14:24:42 2021
MD5 checksum: ed8faefff8b27232b542a17a08208742 : verified
SHA1 checksum: 6226f14c9a2ad69f213548ecc08ccefdde903891 : verified
```

Figure 1: Hash verification

ANALYSIS

REGISTRY ANALYSIS

The Windows registry is a database that records system and user configurations. With the help of registry analysis, an investigator can identify user accounts, installed and configured software, connected USB devices, malware, etc.

The Windows registry for AVENGERS01 was analyzed for specific system configurations and settings, user specific settings, using Access Data FTK Imager v4.7.1 and user activity using Windows Registry Ripper v3.0. The SAM, SYSTEM, SOFTWARE and user hives (NTUSER.DAT and USRCLASS.DAT) were also reviewed for relevant information for this investigation.

HIVES:

- USRCLASS.DAT: this file contains information about users and their personal setting and other customized options. For this investigation, it was found under the location NONAME [NTFS]/[root]//Users/srogers/AppData/Local/Microsoft/Windows/UsrClass.dat for the user S. Rogers.
- NTUSER.DAT: a personalized file that keeps track of how you like to use your system, and has information like email associated with a user's profile. Location NONAME [NTFS]/[root]//Users/srogers/NTUSER.dat
- SAM(Security Account Manager) Hive: an important hive that is used for user authentication and access control on a Windows system. Found under the location NONAME [NTFS]/[root]/Windows/System32/config/SAM, this hive stores information related to user account names, hashes of passwords, SIDs, etc.
- SYSTEM Hive: Found under the location NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM, this hive has data like configurations related to system, device drives, information about installed hardware components.
- SOFTWARE Hive: this hive can be found at NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE, has all the essential data of installed programs with their associated files.
- SECURITY Hive: the SECURITY hive has information about security policies, user rights and is present at location NONAME [NTFS]/[root]/Windows/System32/config/SECURITY.

USER/GROUP INFORMATION

- **Users:**
 - Username: Administrator
SID: S-1-5-21-263698462-3103634936-1936700066-500
Last Login Date: Never

Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 500
--> Password does not expire
--> Account Disabled
--> Normal user account

- Username: Guest
SID: S-1-5-21-263698462-3103634936-1936700066-501
Last Login Date: Never
Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 501
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account

- Username: DefaultAccount
SID: S-1-5-21-263698462-3103634936-1936700066-503
Last Login Date: Never

- Username: srogers
SID: S-1-5-21-263698462-3103634936-1936700066-1001
Last Login Date: 2019-01-21 18:56:51Z
Pwd Reset Date : 2019-01-19 03:11:57Z
Pwd Fail Date : 2019-01-20 19:46:19Z
Login Count : 10
Embedded RID : 1001
--> Password does not expire
--> Password not required
--> Normal user account

- **Groups:**

- Group Name : Guests
LastWrite : 2019-01-19 06:04:22Z
Users : S-1-5-21-263698462-3103634936-1936700066-501
- Group Name : IIS_IUSRS
LastWrite : 2019-01-19 06:04:22Z
Users : S-1-5-17
- Group Name : Users

LastWrite : 2019-01-20 02:44:10Z

Users : S-1-5-4

S-1-5-11

- Group Name : System Managed Accounts Group

LastWrite : 2019-01-19 06:04:22Z

Users : S-1-5-21-263698462-3103634936-1936700066-503

- Group Name : Administrators

LastWrite : 2019-01-19 03:12:54Z

Users : S-1-5-21-263698462-3103634936-1936700066-500

S-1-5-21-263698462-3103634936-1936700066-1001

SYSTEM INFORMATION

- **Microsoft OS Version:** Windows 10 Pro
- **Build Version:** 16299.rs3_release_svc.180808-1748
- **Current Control Set:** ControlSet001
- **OS Install Date:** 2019-01-19 03:06:56Z
- **Computer Name:** AVENGERS01
- **Time Zone:** Eastern Standard Time
- **Network Interfaces with Last Connection Time:**
 - DhcpIPAddress: 10.0.0.81
 - DhcpServer:10.0.0.1
 - Last Connection Time: 2019-01-21 18:41:10Z
 - Adapter: {8b5e6c44-b0c7-45d8-88d9-64a45650730f}
- **Autostart Programs:**
 - SecurityHealth - %ProgramFiles%\Windows Defender\MSASCuiL.exe
 - VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
 - Dropbox - "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup
- **Last Shutdown Time:** January 20, 2019, at 21:11:38Z

USER ACTIVITY

- **Windows Search History:** S. Rogers has not appeared to have searched for a term using the Windows search bar according to the lack of evidence identified under the registry key WordWheelQuery at location NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
- **Typed Paths:** S. Rogers has not appeared to have searched for specific paths on the system according to the lack of evidence identified under the registry key TypedPaths at location NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths.

- **RecentDocs:** By analyzing the NTUSER.DAT registry, the following documents were accessed by S. Rogers under the RecentDocs registry key at location Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs:
9 = Personal 17 = Random Accounting Spreadsheet.xlsx 10 = USB Backup 16 = Selection_of_materials.ppt 5 = Chapter 4.pdf 15 = Cap-2.jpg 14 = Cap-1.jpg 7 = Shield Documents 13 = Presentation with Sensitive IP.pptx 12 = This PC 11 = Documents 8 = S. Rogers Resume.docx 6 = Confidential Alloy Expense Accounts.xlsx 3 = Shield_USB (E:) 4 = Alloys.pptx 2 = Alloys.ppt 0 = The Internet 1 = network.
- **Last Executed Commands:** S. Rogers did not run any commands from the START -> RUN box because under the location Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU LastWrite Time 2019-01-21 05:04:19Z, it says “has no values”.
- **UserAssist:** the any programs executed by the user, S. Rogers were found at location Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist in the UserAssist key of NTUSER.dat file. The following programs can be of interest with respect to this investigation:

Table 1 – UserAssist analysis for the user S. Rogers

Local Path	Application File Name	LastWrite Time
C:\Users\srogers\Documents\USB Backup\privacy-eraser-setup.exe (1)	privacy-eraser-setup.exe	2019-01-21 05:33:07Z
C:\Users\srogers\Downloads\torbrowser-install-win64-8.0.4_en-US.exe (1)	torbrowser-install-win64-8.0.4_en-US.exe	2019-01-21 05:06:24Z
C:\Users\srogers\Downloads\DropboxInstaller.exe (1)	DropboxInstaller.exe	2019-01-20 21:13:26Z
C:\Users\srogers\Downloads\BitTorrent.exe (1)	BitTorrent.exe	2019-01-20 21:10:08Z

USB DEVICE ANALYSIS

By using the USB Detective tool v1.3.6, one USB device with the name “Kingston DataTraveler 2.0 USB Device” seems to be connected to the system while incident took place as the first time and last time connected for the device was on 1/21/2019 12:00:14 AM and 1/21/2019 12:17:03 PM respectively.

The log file under the location NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log with the other hives were combined for this USB analysis.

Table 2 – USB Devices Connected to AVENGERS01

Device Name	Serial Number	User Account	First Time	Last Time
Kingston DataTraveler 2.0 USB Device	200706200000000059187F6F	srogers	1/21/2019 12:00:14 AM	1/21/2019 12:17:03 PM

APPLICATION ANALYSIS

In the NTUSER.DAT, under the “uninstall” registry key, there were two applications: BitTorrent v.7.10.4.44847 (2019-01-20 21:27:13Z) and Microsoft OneDrive v.18.240.1202.0004 (2019-01-20 02:46:39Z), which can suggest that S. Rogers was trying to upload company-related documents onto the OneDrive.

The execution of programs like Dropbox and OneDrive seems suspicious, as it might indicate that S. Rogers may have uploaded the data to cloud storage and then tried to clear the evidence by running the Privacy Eraser tool.

Also, applications like BitTorrent and Tor Browser directly violate the company policy.

PREFETCH ANALYSIS

Prefetch analysis helps in examining the files within the prefetch folder to gain insights into the programs that have been executed on the system. For this investigation, with the help of Access Data FTK Imager and Eric Zimmerman’s PECmd (Prefetch parser) v 1.5.0.0 tools, the following information about the applications were concluded:

Table 3 – Prefetch Analysis for AVENGERS01

Application Name	Times Ran	First Run	Last Run
TORBROWSER-INSTALL-WIN64-8.0.	1	1/21/2019 5:10:04 AM	1/21/2019 5:10:14 AM
PRIVACY-ERASER-SETUP.EXE	2	1/21/2019 4:57:41 PM	1/21/2019 4:57:45 PM
DROPBOX.EXE	5	1/20/2019 9:17:55 PM	1/20/2019 9:17:55 PM
BITTORRENT.EXE	2	1/20/2019 9:26:03 PM	1/20/2019 9:27:18 PM
ONEDRIVE.EXE	7	1/19/2019 3:14:59 AM	1/20/2019 9:12:38 PM

SHELL ITEM ANALYSIS

Shellbag analysis is done to obtain information from the metadata that is stored in the Windows shellbags. It helps in reconstruction of user’s folder and file access history even after it was deleted or overwritten. Eric Zimmerman’s SBECmd (Shellbag Parser) v2.0.0.0 tool was used to do the shellbag analysis, for the incident.

It was observed that NTUSER.dat.csv did not have any shellbag information, which can indicate that no shellbags were created from the user’s desktop. But, in the USRClass.DAT.csv file there were 34 shellbags found.

Also, the Shield Documents folder was originally present at “Desktop\E:\\Shield Documents” and from there it had been moved to the location “Desktop\\Shared Documents Folder (Users Files)\\Dropbox\\Shield Documents”, which might indicate that the employee could have stored the files on Dropbox.

Table 4 – Shellbag Analysis for AVENGERS01

AbsolutePath	ShellType	Value	LastWriteTime	FirstInteracted	LastInteracted
Desktop\\This PC\\Documents\\USB Backup\\Personal	Directory	Personal	1/21/2019 7:16:09 PM	1/21/2019 7:16:09 PM	1/21/2019 7:16:09 PM
Desktop\\E:\\Forensic Tools	Directory	Forensic Tools	1/21/2019 7:57:23 PM		
Desktop\\E:\\SANS To Sort	Directory	SANS To Sort	1/21/2019 7:57:23 PM	1/21/2019 7:57:05 PM	
Desktop\\E:\\Shield Documents	Directory	Shield Documents	1/21/2019 7:57:23 PM	1/21/2019 5:00:39 AM	
Desktop\\E:\\Imaging and Triage Lab	Directory	Imaging and Triage Lab	1/21/2019 7:57:23 PM	1/21/2019 7:57:23 PM	1/21/2019 7:57:23 PM
Desktop\\E:\\Forensic Tools\\Imager_Lite_3.1.1	Directory	Imager_Lite_3.1.1	1/21/2019 7:50:33 PM	1/21/2019 7:50:33 PM	1/21/2019 7:50:33 PM
Desktop\\This PC\\Documents\\USB Backup	Directory	USB Backup	1/21/2019 5:06:52 AM		1/21/2019 5:06:52 AM
Desktop\\Shared Documents Folder (Users Files)\\Dropbox\\Shield Documents	Directory	Shield Documents	1/21/2019 5:21:16 AM	1/21/2019 5:21:16 AM	1/21/2019 5:21:16 AM

Jump List Analysis

There were 4 unique files also identified on USB were which differed with the LNK analysis below.

- S. Rogers Resume.docx
- Alloys.ppt
- Confidential Alloy Expense Accounts.xlsx
- Chapter 4.pdf

Additionally, there were two machine IDs, “desktop-16pttv2” and “avengers01” that might indicate that the employee could have renamed the original machine ID to “avengers01”. While, the “avengers01” machine ID have many files of interest:

Table 5 – Jump List Analysis for AVENGERS01

Path	Appld	MachineID	Source Created (First)	Source Modified (Last)
C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx	5f7b5f1e01b83767	avengers01	1/19/2019 3:13:10 AM	1/21/2019 7:16:10 PM
E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx	83dd64e7fa560bd5	avengers01	1/21/2019 5:05:04 AM	1/21/2019 7:16:10 PM
E:\Personal	f01b4d95cf55d32a		1/19/2019 3:12:58 AM	1/21/2019 7:16:14 PM
E:\Alloys.ppt	ecd1a5e2c3af9c46		1/21/2019 5:00:45 AM	1/21/2019 7:15:47 PM
C:\Users\srogers\Documents\USB Backup\Selection_of_materials.ppt	ecd1a5e2c3af9c46	avengers01	1/21/2019 5:00:45 AM	1/21/2019 7:15:47 PM
C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf	5f7b5f1e01b83767	avengers01	1/19/2019 3:13:10 AM	1/21/2019 7:16:10 PM

LNK File Analysis

For the LNK file analysis, files were collected from machineID : avengers01. Upon further investigation it was found Removable storage media connected to the system with the name "Shield_USB". There were several files of interest:

Table 6 – LNK File Analysis for AVENGERS01

Filename	Location	User Account	Source Created (First)	Source Modified (Last)
Alloys.pptx	C:\Users\srogers\Desktop\Alloys.pptx	srogers	1/21/2019 5:04:43 AM	1/21/2019 5:04:43 AM
Chapter 4.pdf	C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf	srogers	1/21/2019 5:04:46 AM	1/21/2019 7:14:41 PM
Random Accounting Spreadsheet.xlsx	C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx	srogers	1/21/2019 7:16:10 PM	1/21/2019 7:16:10 PM
Selection_of_materials.ppt	C:\Users\srogers\Documents\USB Backup\Selection_of_materials.ppt	srogers	1/21/2019 7:15:47 PM	1/21/2019 7:15:47 PM
Presentation with Sensitive IP.pptx	C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx	srogers	1/21/2019 5:07:00 AM	1/21/2019 5:07:00 AM

ACTIVITY TIMELINE

- 21 January 2019, 18:56:51Z: User "srogers" logs into the system.
- 21 January 2019, 21:13:26Z: DropboxInstaller.exe executed according to UserAssist analysis.

- 21 January 2019, 21:27:13Z: BitTorrent v.7.10.4.44847 installed according to uninstall registry key analysis.
- 21 January, 2019, 12:00:14 AM Kingston DataTraveler USB device connected to the system, as per USB Detective log analysis.
- 21 January 2019, 05:07:00 AM Presentation with Sensitive IP.pptx was modified.
- 21 January 2019, 05:21:16 AM Shield Documents moved/copied to a new folder, indicating that it might be backed up on cloud.

USER ACTIVITY

The following files that were found in various folders like Recycle Bin, Documents, Downloads and Desktop of the user shows intent :

- At location C:\Users\srogers\Downloads\ChromeSetup.exe was downloaded on 2019-01-19 03:11:11Z, which can be suspicious as in some organization we need prior approval for installing other browsers.
- Dropbox Installer.exe downloaded on 01/20/2019 at 03:02:31 AM
- BitTorrent.exe downloaded on 01/20/2019 at 07:24:37 PM
- Installer.exe downloaded on 01/21/2019 at 05:30:19 AM

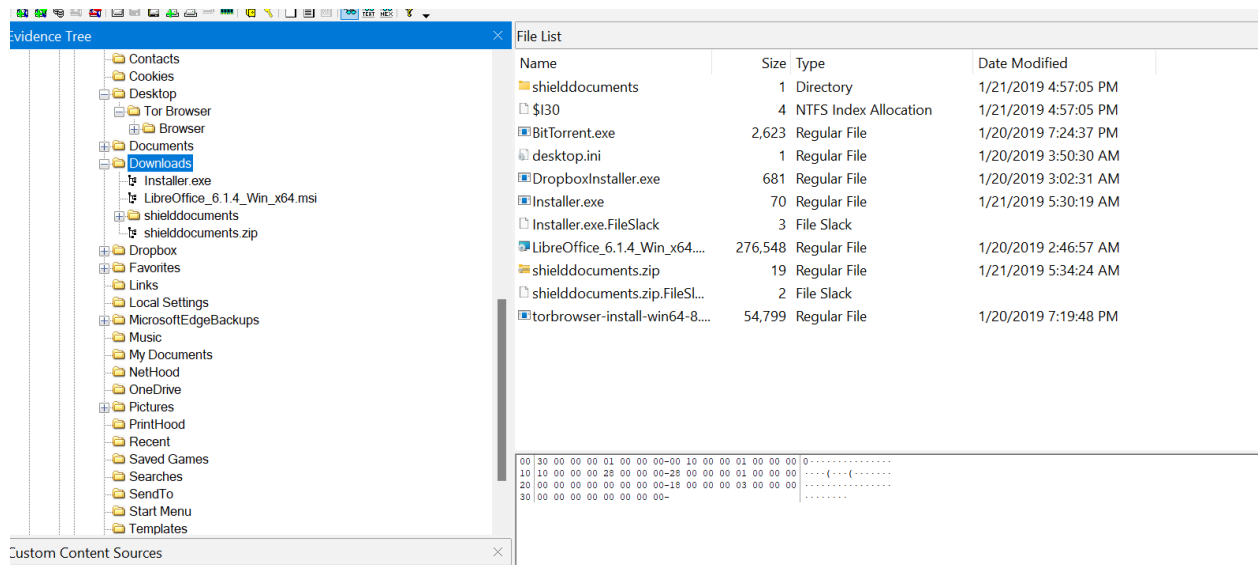


Figure 2: Downloads Folder

- USB Backup folder under Documents, there are SHIELD documents like Confidential Alloy Expense Accounts.xlsx

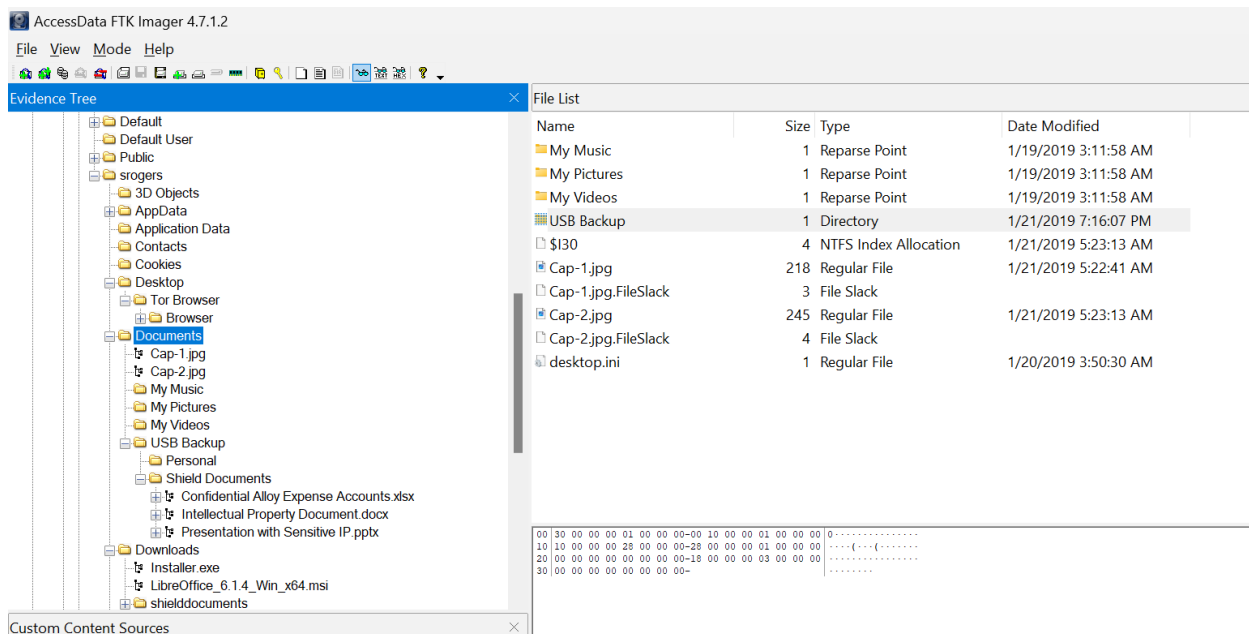


Figure 3: Documents Folder

- Under the Desktop folder, Tor Browser was present along with other files that violated the company policy.

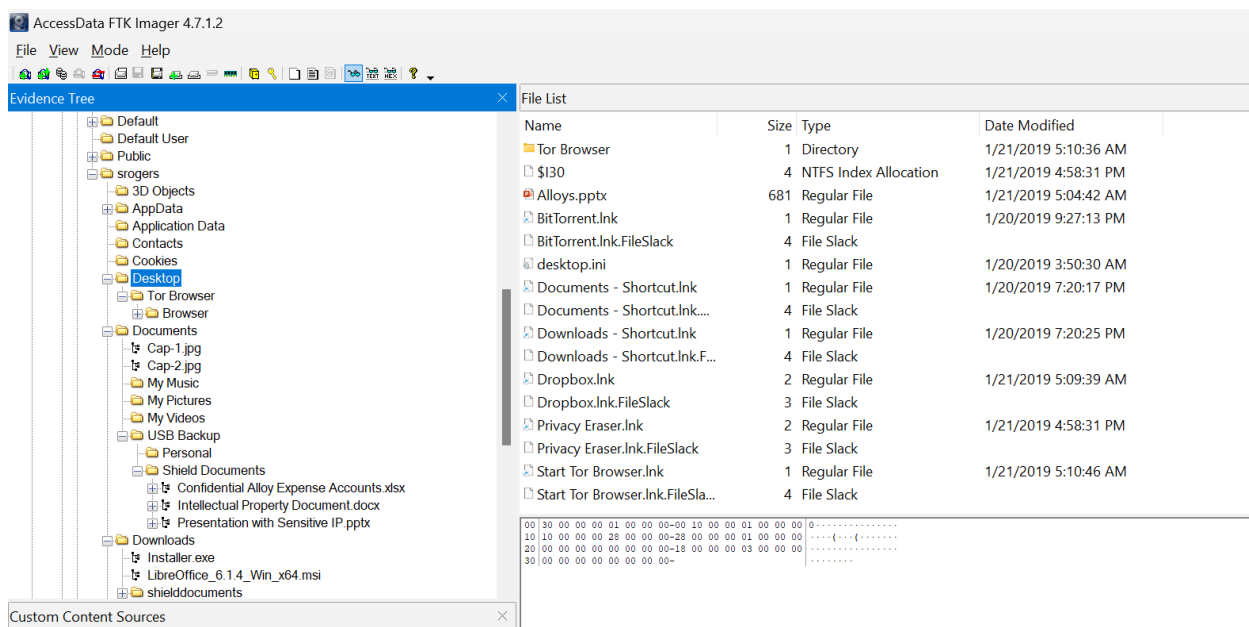
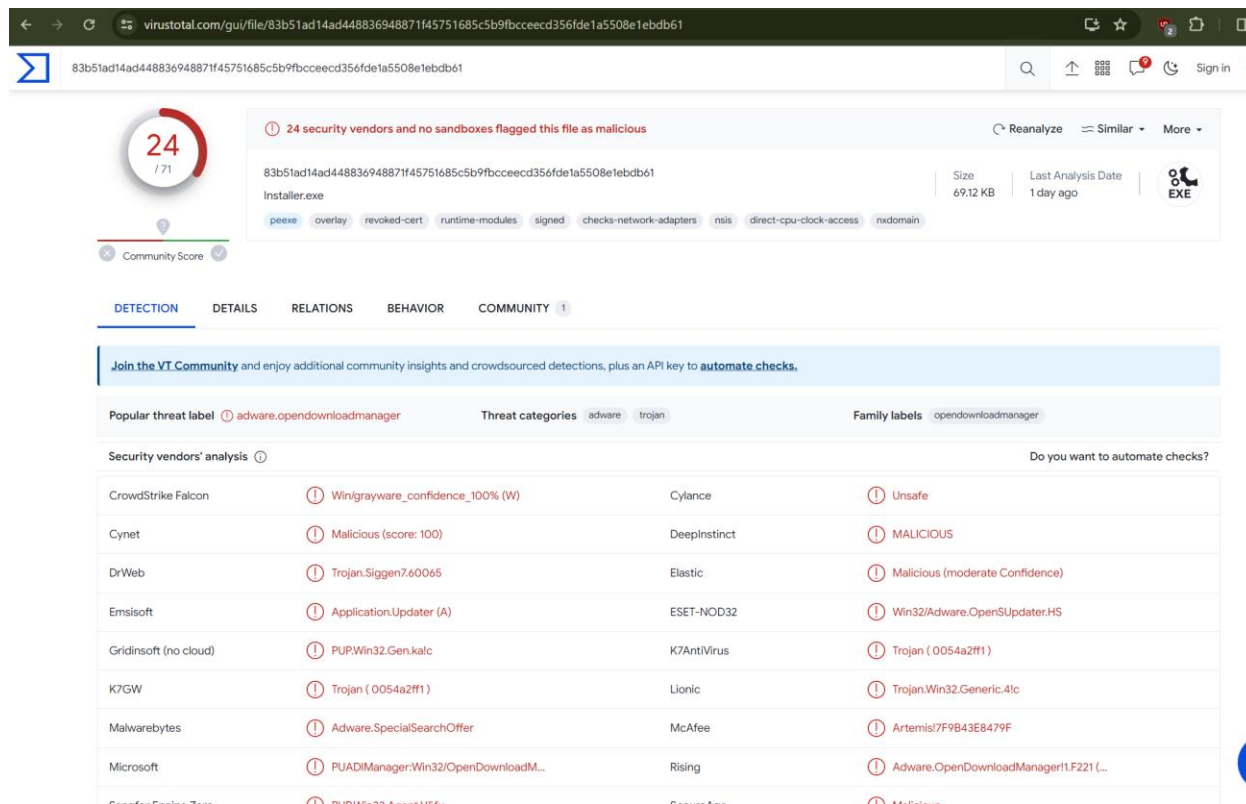


Figure 4: Desktop Folder

MALWARE ANALYSIS

By analyzing the image with the help of FTK imager and navigating the location NONAME [NTFS]/[root]/Users/srogers/Downloads, the file installer.exe seems to be a malware. Samriddhi further analyzed the suspicious file with the help on VirusTotal tool which flagged the file as malicious.



The screenshot shows the VirusTotal web interface for a file named 'installer.exe' with SHA256 hash 83b51ad14ad448836948871f45751685c5b9fbccecd356fde1a5508e1ebdb61. The file is 69.12 KB and was analyzed 1 day ago. It is flagged as malicious by 24 security vendors. The file is categorized as 'adware.opendownloadmanager' and 'trojan'. The 'Security vendors' analysis' section shows the following results:

Security vendor	Detection	Security vendor	Detection
CrowdStrike Falcon	Win/grayware_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Siggen7.60065	Elastic	Malicious (moderate Confidence)
Emsisoft	Application.Updater (A)	ESET-NOD32	Win32/Adware.OpenSUpdater.HS
Gridinsoft (no cloud)	PUP.Win32.Gen.kalc	K7AntiVirus	Trojan (0054a2ff1)
K7GW	Trojan (0054a2ff1)	Lionic	Trojan.Win32.Generic.41c
Malwarebytes	Adware.SpecialSearchOffer	McAfee	Artemis!7F9B43E8479F
Microsoft	PUAD!Manager:Win32/OpenDownloadM...	Rising	Adware.OpenDownloadManager1.F221 (...)
Sentinel Endpoint T...	BI ID 0054a2ff1	Symantec	Malicious

Figure 5: Malware found with the help of VirusTotal tool

RECYCLE BIN

Using the SID of S. Roger, there were multiple .exe files in the recycle bin of the system. The bin contains \$I492Q4Q.exe, \$IGKYW9H.exe and other .exe files and desktop.ini file that might be interest for this case.

Evidence Tree

[root]

\$BadClus

\$Extend

\$Recycle Bin

S-1-5-18

S-1-5-21-263698462-3103634936-1936700066-1000

S-1-5-21-263698462-3103634936-1936700066-1001

\$Secure

\$UpCase

Documents and Settings

PerfLogs

Program Files

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

All Users

Default

Default User

Public

srogers

3D Objects

AppData

Application Data

Contacts

Cookies

Desktop

Custom Content Sources

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Ind...	1/21/2019 5:14...
\$I492Q4Q.exe	1	Regular F...	1/20/2019 3:05...
\$IFV3F7W.exe	1	Regular F...	1/21/2019 5:14...
\$IGKYW9H.exe	1	Regular F...	1/21/2019 5:14...
\$R492Q4Q.exe	681	Regular F...	1/20/2019 3:05...
\$RFV3F7W.exe	681	Regular F...	1/21/2019 5:13...
\$RGKYW9H.exe	1,110	Regular F...	1/20/2019 2:43...
\$RGKYW9H.exe.FileSlack	3	File Slack	
desktop.ini	1	Regular F...	1/19/2019 3:13...

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00

10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00

20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00

30 00 00 00 00 00 00 00 00-00

Figure 6: Setup files in the recycle bin of S. Rogers

CONCLUSION

The forensic investigation's conclusions make it clear that there was a significant policy violation that may have compromised confidential firm information. On one of the company's assets, illegal software, including BitTorrent and a Privacy Cleaner tool, along with other applications like DropboxInstaller.exe, Tor Browser was downloaded and installed without authorization.

Additionally, evidence points to the possibility that "Kingston DataTraveler" a USB device, was used to copy and distribute confidential company data to outside sources. This USB device may have been involved in the data breach because it was attached to the system while S. Rogers was logged in.

Prompt action is required to maintain the integrity of the company's proprietary information and reduce the danger of additional data loss. Retrieving the USB device is essential for more research and questioning of the implicated employee, S. Rogers. If they don't, there could be legal consequences for the organization as well as the individual.

In conclusion, this forensic report emphasized how serious the incident was and how crucial it is to have strong cybersecurity safeguards and teach staff members to avoid similar incidents in the future. To prevent illegal access and data exfiltration, the investigation's conclusions should act as a spur to strengthen the company's acceptable use policy and implement stronger security measures.

TOOLS

Access Data Registry Viewer v 2.0.0

Access Data FTK Imager v 4.7.1

Registry Ripper v 3.0

Eric Zimmerman's tools:

- LECmd (LNK files parser) v 1.5.0.0

- JLECmd (Jump List parser) v 1.5.0.0

- SBECmd (Shellbag parser) v 2.0.0.0

- PECmd (Prefetch parser) v 1.5.0.0

USBDetective v.1.3.6

VirusTotal