Autopsy CTF 2

Keegan R. Heaton

University of Advancing Technology

Computer Forensics Essentials - SP24101

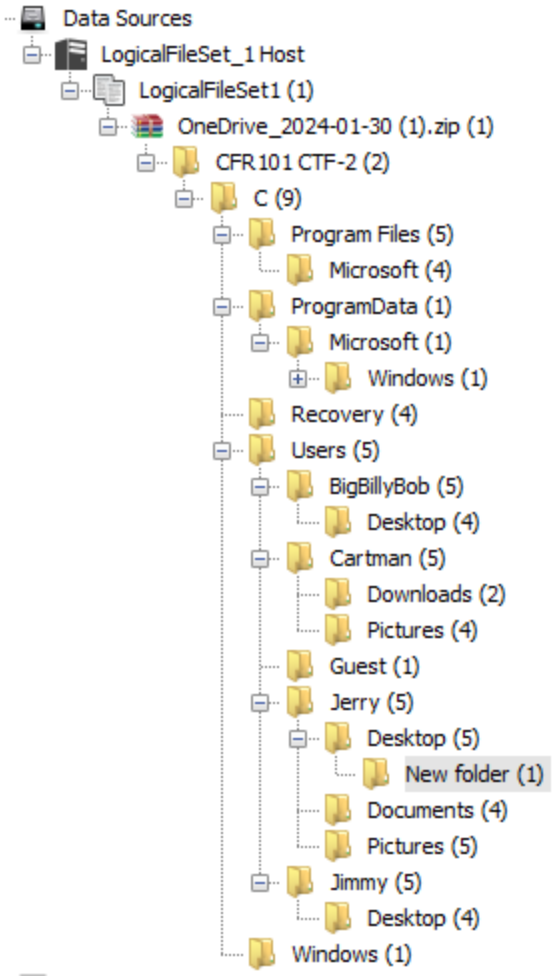
Aaron Rodriguez

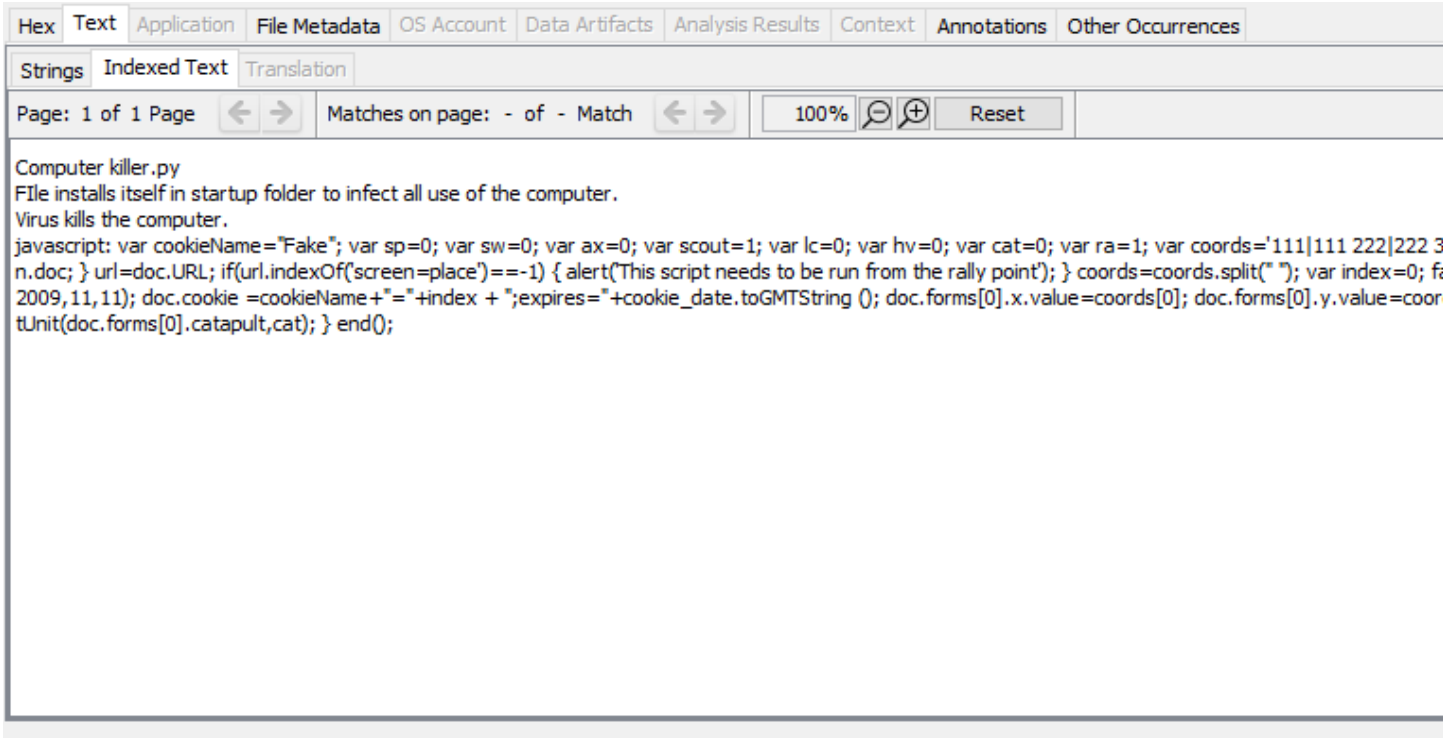
2/22/2024

1. Opened OneDrive_2024_01-30 (1) on 02/20/2024
    a. Used Autopsy Ver. 4.19.3 to scan OneDrive_2024_01_30 (1)
        i. Searching for malware or malfunctions inside OneDrive_2024_01_30 (1)
            1. Suspicious Activity

OneDrive_2024_01_30 (1) is a copied operating system with an unknown problem. I started my scan of the operating system by checking user accounts. The accounts on the system included BigBillyBob, cartman, guest, Jerry, and Jimmy. There was nothing of note in BigBillyBob or cartman as most of their content was filled with memes. The guest account also had nothing suspicious and was nearly empty. Jerry's user account had some suspicious activity inside the desktop > New Folder. In the New Folder I found Computerkiller.py. This file held coding which caused the computer to fail on start-up. I deemed this highly suspicious and most likely the cause of the computer's destruction. I tagged the file and plan to connect with Jerry to find the reason behind Computer Killer. I suggest removing Computerkiller.py after talking with Jerry. The nature of computerkiller.py is to fully infect all files, so salvaging the computer is slow. However, removing it is still up in the air as we don't know their

intentions. Below are screenshots of the directory and computerkiller.py contents.


Data Sources
LogicalFileSet_1 Host
LogicalFileSet1 (1)
OneDrive_2024-01-30 (1).zip (1)
CFR101 CTF-2 (2)
C (9)
Program Files (5)
Microsoft (4)
ProgramData (1)
Microsoft (1)
Windows (1)
Recovery (4)
Users (5)
BigBillyBob (5)
Desktop (4)
Cartman (5)
Downloads (2)
Pictures (4)
Guest (1)
Jerry (5)
Desktop (5)
New folder (1)
Documents (4)
Pictures (5)
Jimmy (5)
Desktop (4)
Windows (1)


Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset
Computer killer.py
FIle installs itself in startup folder to infect all use of the computer.
Virus kills the computer.
javascript: var cookieName="Fake"; var sp=0; var sw=0; var ax=0; var scout=1; var lc=0; var hv=0; var cat=0; var ra=1; var coords='111|111 222|222 3
n.doc; } url=doc.URL; if(url.indexOf('screen=place')==-1) { alert('This script needs to be run from the rally point'); } coords=coords.split(" "); var index=0; fa
2009,11,11); doc.cookie =cookieName+"="+index + ";expires="+cookie_date.toGMTString (); doc.forms[0].x.value=coords[0]; doc.forms[0].y.value=coor
tUnit(doc.forms[0].catapult,cat); } end();