Case 1 - Amaya's browser issues

22 February 2023

Noah Beckman
Contact: Noah.beckman@mymail.champlain.edu

Table of Contents

Introduction and Scope

On August 7th 2019, suspicious web traffic was detected originating from Amaya's PC and the forensic team was contacted to investigate the activity. Orko Electric would like the forensic team to find out what is causing Amaya's issues and analyze its potential threat to the corporation. The team received various evidence files from Orko Electric for full forensic examination.

Executive Summary

After conducting a thorough analysis of the provided evidence, the forensic team found malicious activity that led to data exfiltration and data encryption for impact. The findings result in a loss of confidentiality and integrity for the business. Any data or information that was worked on could have potentially been exfiltrated by the threat actor. The threat actors have the ability to see all keystrokes, searches, web history, and receive screen captures.The host system is compromised and should be reverted to backups. In addition, ransomware was found on one of the provided computers resulting in complete data encryption of sensitive files.

Note

All technical terms are defined in the **glossary** at the end of this report for further clarification.

Evidence Analyzed

Full forensic copies of the following computers:

Evidence Name	Evidence Type	SHA1 Hash:	Notes
PC-1-08-14-18-END.vhd	VHD Disk Image	EDCD8A78BBBDE8F803642F4032D6B4CA57CFC2DB	Full forensic image of Computer
PC-2-08-14-18-END.vhd	VHD Disk Image	228DE7B71E93E95A23A4611FC9781F8AB758EA72	Full forensic image of Computer
PC-3-08-23-18-END.vhd	VHD Disk Image	C508CCA5C8C4B49353EC2438E4FC680D02041693	Full forensic image of Computer
Pcaps.7z	Network Logs	B3851175318109E3C7F2F498335E5382D4D16AE0	Network Activity logs for the following time frame Aug 7, 2018 - Aug 23, 2018
SMTP.7z	Email Files	1AE8E0E271D1126B658FFD8E2DBA02A8DC61C4DB	Email Data for following users ● alabank ● asarea ● ebeltze
Memory.7z	Memory Capture	12980C9ED7F43F7B843540387741B351F9836ADA	Memory Dump of computer

Methodology

1. On February the 7th, I began the forensic acquisition process of the provided evidence. Prior to the acquisition of the evidence, the analyst documented all impacted computers and preserved the chain of custody.
2. After completing the forensic acquisition, I extracted and analyzed the evidence with forensic tools
3. The used the following tools for forensic analysis, which are licensed to this examiner:
    a. Magnet Axiom v4.6.0.21968
    b. RegistryExplorer v2.0.0.0
    c. SysTools EML Viewer Pro+
    d. Wireshark v4.0.0

Tool Summary

Magnet Axiom — v4.6.0.21968

- Magnet Axiom is a digital investigation program that allows investigators to acquire and analyze forensic data.

RegistryExplorer — v2.0.0.0

- A tool used by investigators to display and parse registry hives and user profiles.

SysTools EML Viewer Pro+

- A tool that allows users to view EML / SMTP files.

Wireshark — v4.0.0

- An open source packet analyzer that can be used for packet analysis.

WinPrefetchView — v1.37

- A tool used to view prefetch file information in GUI interface.

Process Monitor

- A tool used to see system operations in regards to different processes on the system

Timeline

Malicious Chrome Extension Timeline

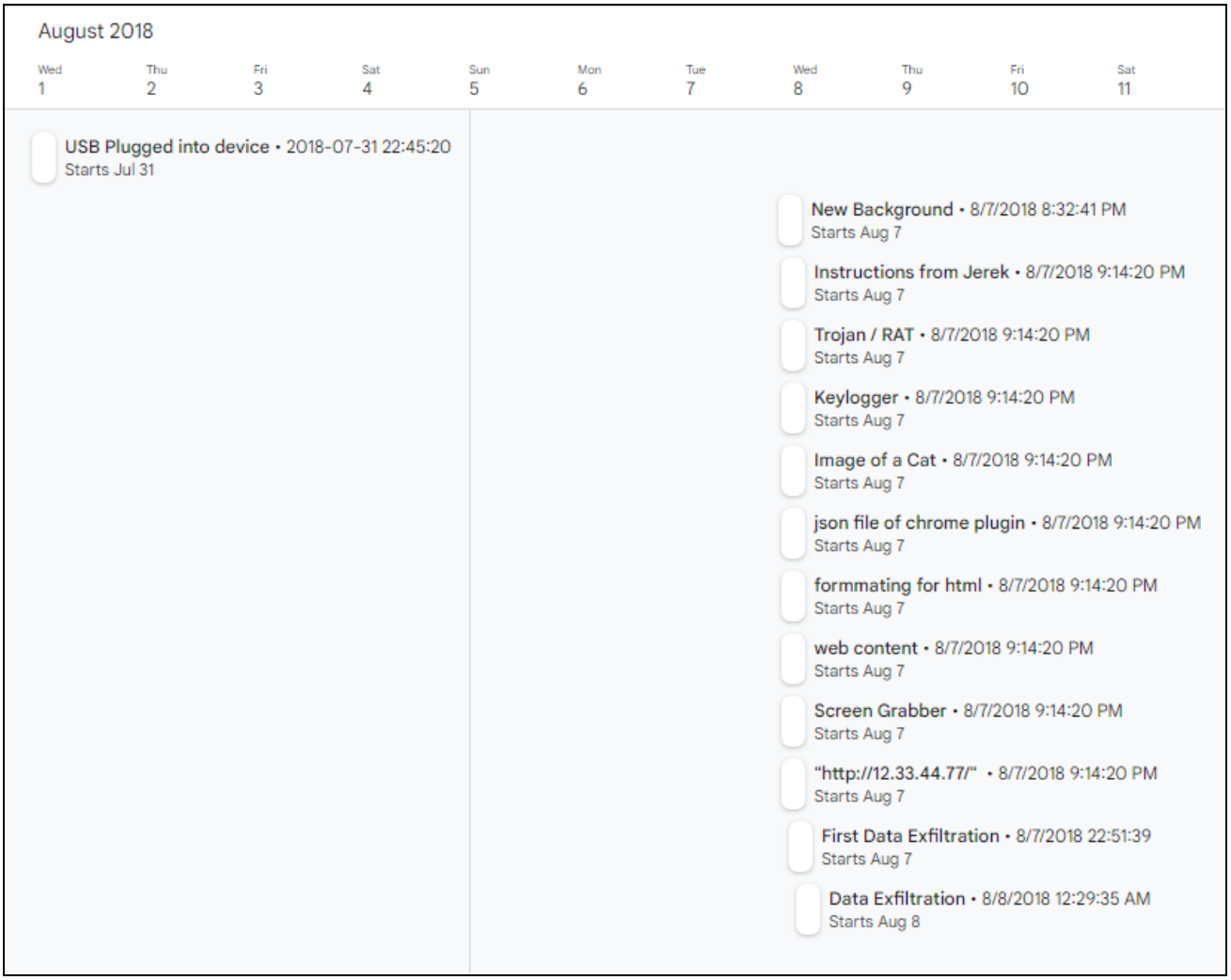


Figure 1 - Timeline of Malicious Chrome Extension Events

The timeline above in Figure 1 shows the events that took place frome when the Chrome Extension was installed to when data was exfiltrated. The event started on **2018-07-31 10:45:20** and data exfiltration occurred on **8/7/2018 10:51:39.** All events in between are documented in the timeline

Suspicious Onion.zip File Timeline

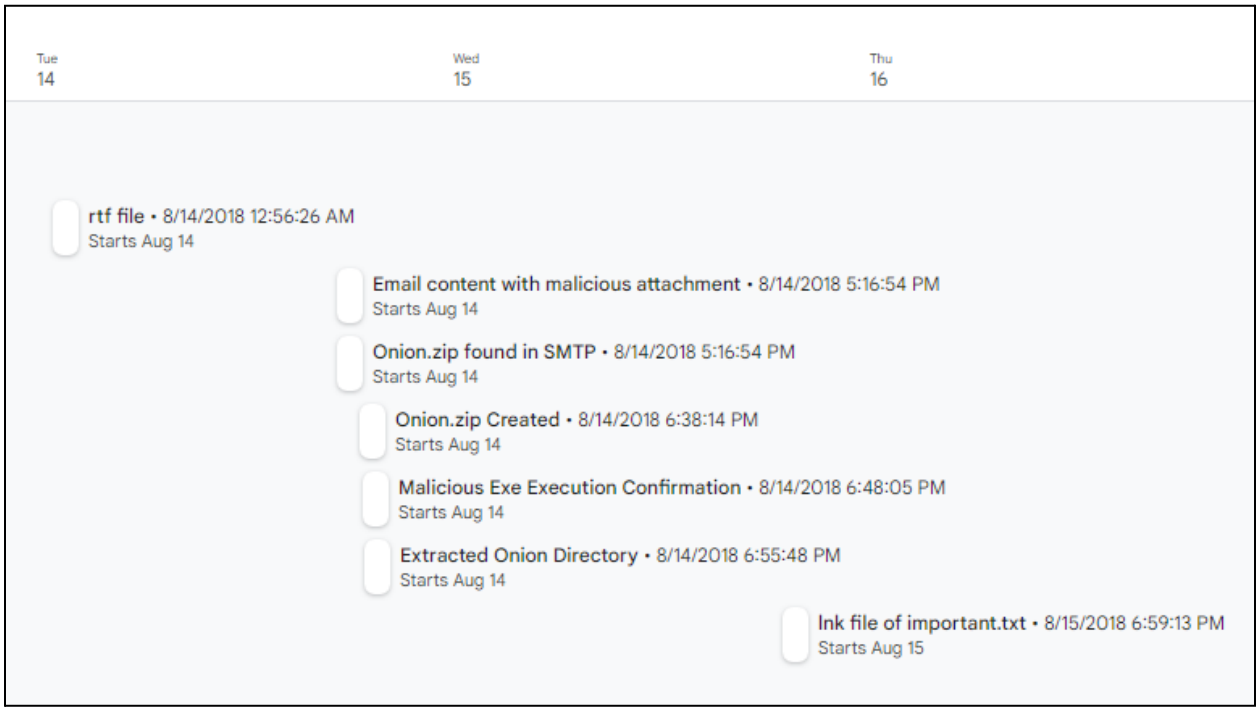
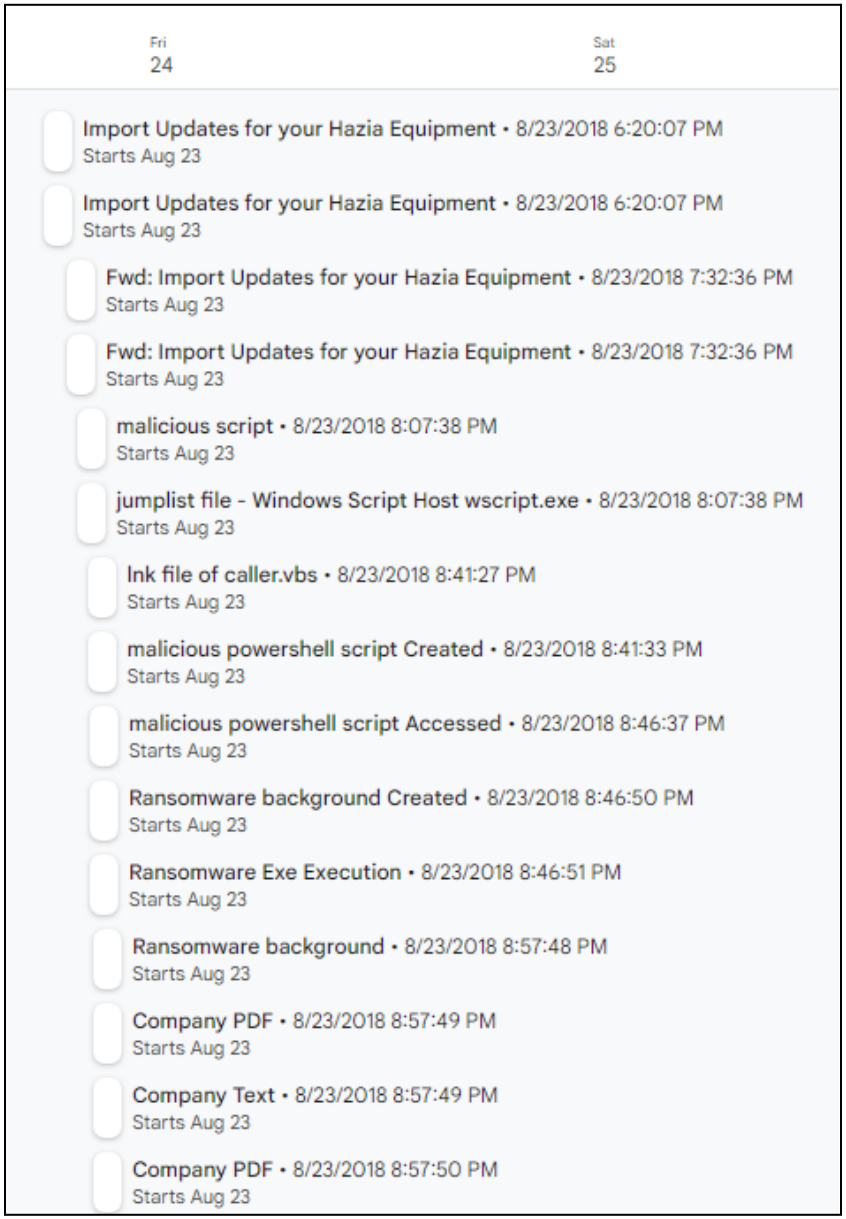
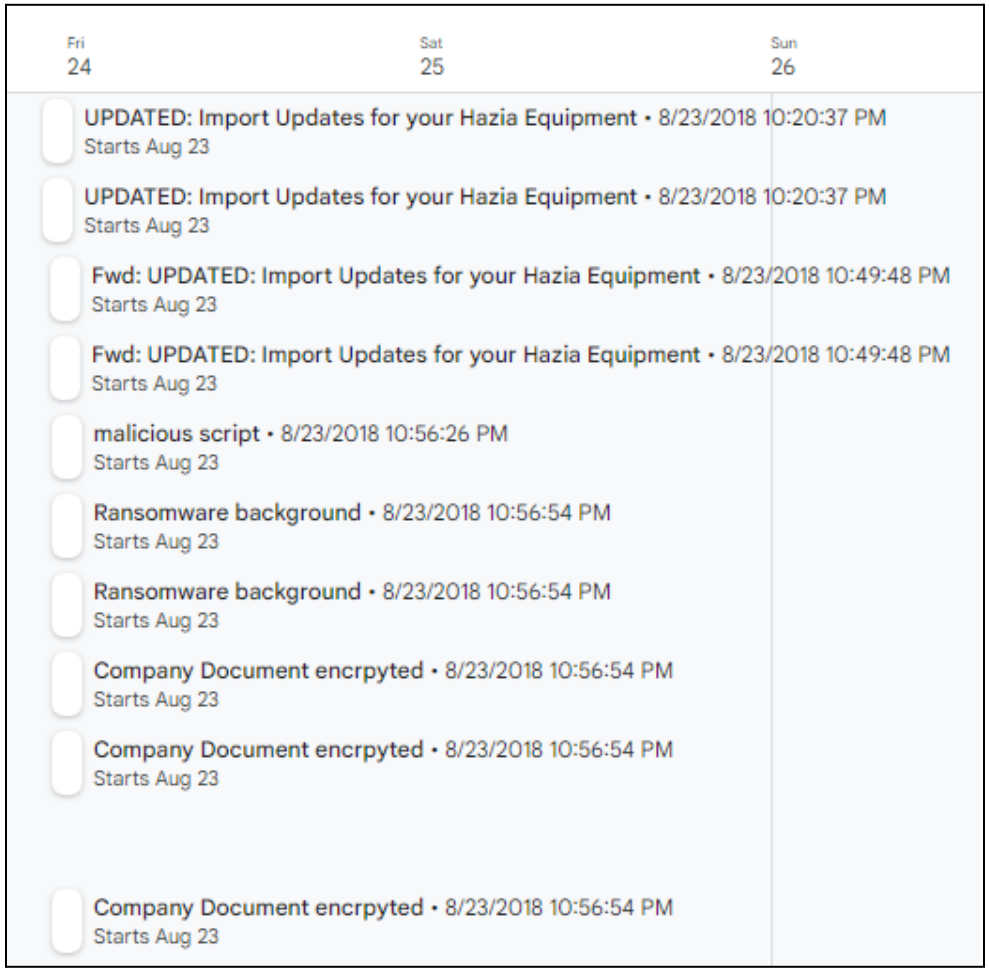


Figure 2 - Suspicious Onion.zip / Onion.rtf files

Figure 2 shows the different events on a timeline related to the rtf file being downloaded to execution of the rtf.

Malicious Ransomware Timeline





The Screenshots above detail out the events related to the ransomware found on PC3. This started on **8/23/2018 6:20:07 PM** until the users files were all encrypted on **8/23/2018 10:56:54 PM**

Overview of Findings

Malicious Files

Artifact File	Source	Value	Timestamp	Path	Description	Hash
background.js	PC-2-08-14-18-END.vhd	Data Exfil Tool	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\background.js	Javascript file that contains comments talking about keylogger, history grabber, form grabber, and screen capture. Contains malicious remote ip address	BCEA0C70CC856070AD702CE9E6C7F36D43266EC1
content.js	PC-2-08-14-18-END.vhd	Keylogger	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\content.js	Script contains keylogging and history grabber code	DD315CE88FE6B1D14FB5CD6D34EF280553F1BE1D
icon.png	PC-2-08-14-18-END.vhd	Image of a Cat	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\icon.png	Png image of a cat smiling	825A23909C51A1070F4B8974BAA268624D663F25
manifest.json	PC-2-08-14-18-END.vhd	json file of chrome plugin	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\manifest.json	Runs content.js as main content and background.js in the background	DC06513C8733D584B8B489E6E185DD30F36E656E
popup.html	PC-2-08-14-18-END.vhd		8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\popup.html	html file with a cat gif, runs popup.js	CB372AF72293D583BCAA6B7118794A697913A243
popup.js	PC-2-08-14-18-END.vhd	Screen Grabber	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\popup.js	Screen grabber script	89A7601572A92C50425447851B5A9D64E8DE0342
background.js	PC-2-08-14-18-END.vhd	Ip found "http://12.33.44.77/"	8/7/2018 9:14:20 PM	Users\alabankada\Documents\from Jerrek\CATS\background.js	Malicious ip found within file	BCEA0C70CC856070AD702CE9E6C7F36D43266EC1

Chronological Findings

CATS Directory

The investigation first starts with a Windows registry event from **PC-2-08-14-18-END.vhd**. The system detected a usb event on **2018-07-31 22:45:20**. This can be seen in the SYSTEM registry hive under SYSTEM/MountedDevices path. Figure 3 shows a screenshot of the registry artifact and Figure 4 has the related data.

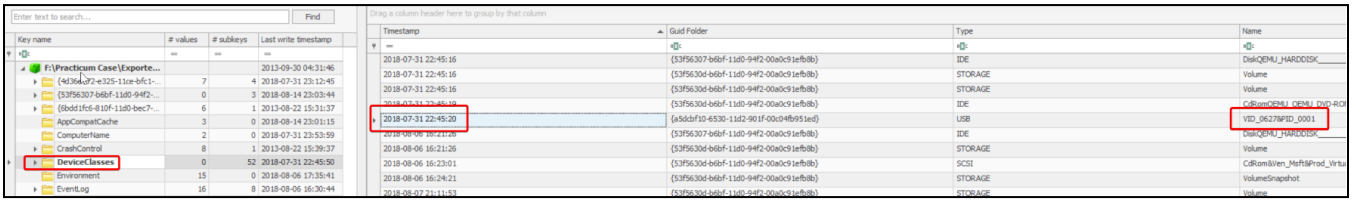


Figure 3 - PC2 System Hive - USB

File Name	Image	Path	Type & Name	Timestamp
SYSTEM	PC-2-08-14-18-END.vhd	SYSTEM/Device Classes	USB & VID_0627&PID_0001	7/31/2018 10:45:20 PM

Figure 4 - Relevant Registry Values

Next, after analyzing the user alabankada's Documents folder, a text document can be found with instructions on how to download a chrome extension. Figure 5 shows the contents of the instructions.txt file. We can confirm the use of the USB that was plugged in with the instructions the users received from a supposed lover. We can see the file created time of instruction.txt in Figure 6 along with other relevant metadata.

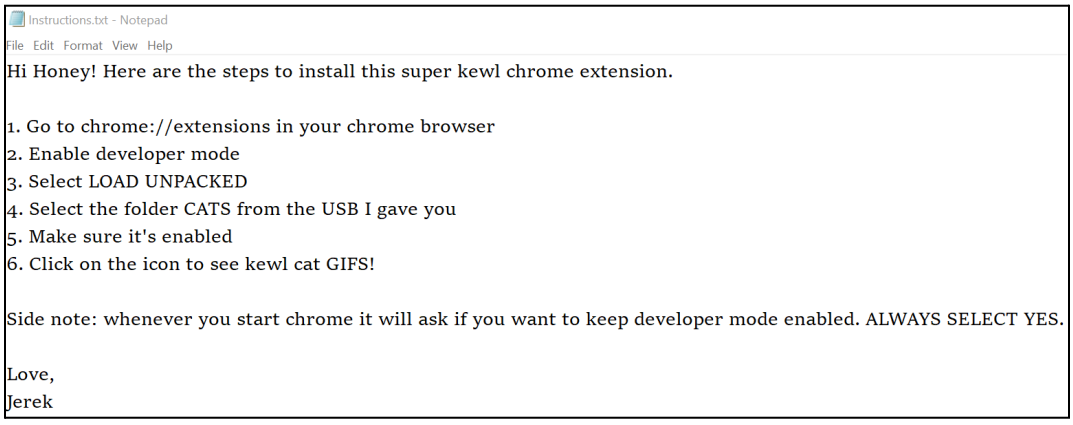


Figure 5 - Instructions.txt contents

File Name	Image	Path	Timestamp
Instructions.txt	PC-2-08-14-18-END.vhd	Users\alabankada\Documents\from Jerrek\Instructions.txt	8/7/2018 9:14:20 PM

Figure 6 - Instructions.txt metadata

After analyzing the contents of the CATS folder the user copied to their system from Jerek's USB, various malicious files can be seen in Figure 7.

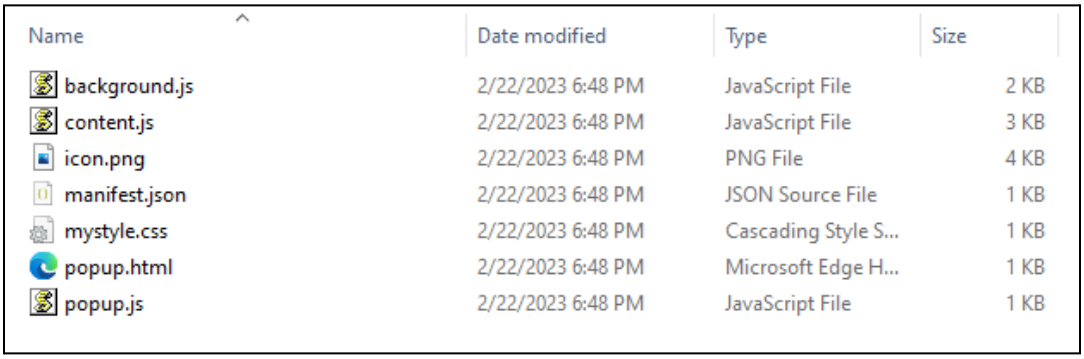


Figure 7 - CATS directory Contents

The first malicious file that is in this directory is background.js. As seen in Figure 8, background.js contains comments describing how the script will communicate with a remote server, contains comments for script functions that will keylog, grab history, grab form submissions, and screen capture the users open window. A remote server ip can also be found within the code. These things can be seen in the red boxes in Figure 8. This specific javascript file Figure 9 shows background.js within the chrome.exe prefetch file confirming its execution on the system.

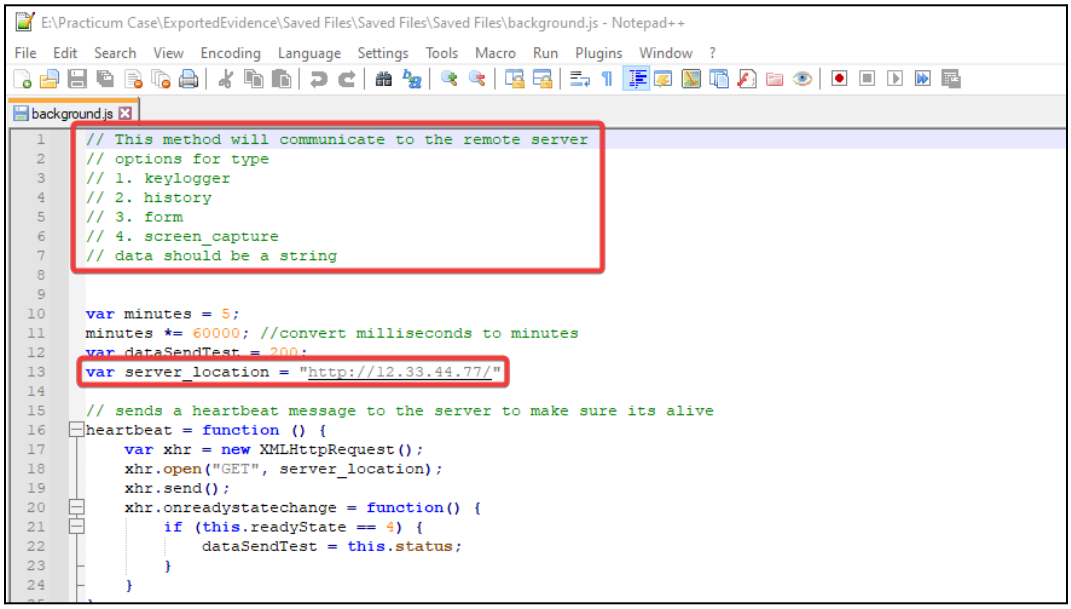


Figure 8 - background.js contents

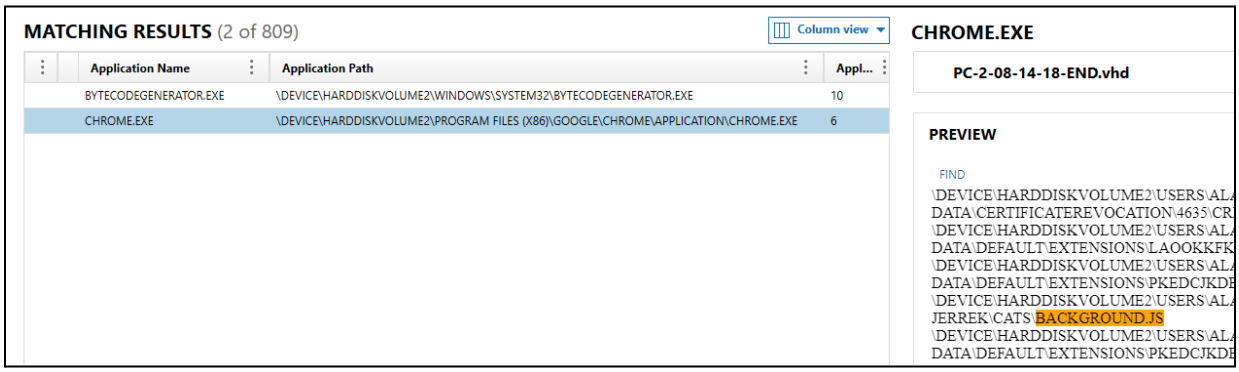


Figure 9 - Background.js prefetch execution confirmation

The next malicious file contained within the CATs folder is the content.js script. This script contains the code for the keylogger, and history grabber. The script can be seen in Figure 10. The red box shows the part of the script that reads any alphanumeric key presses and the blue box shows any special button presses such as backspace, tab, or enter.

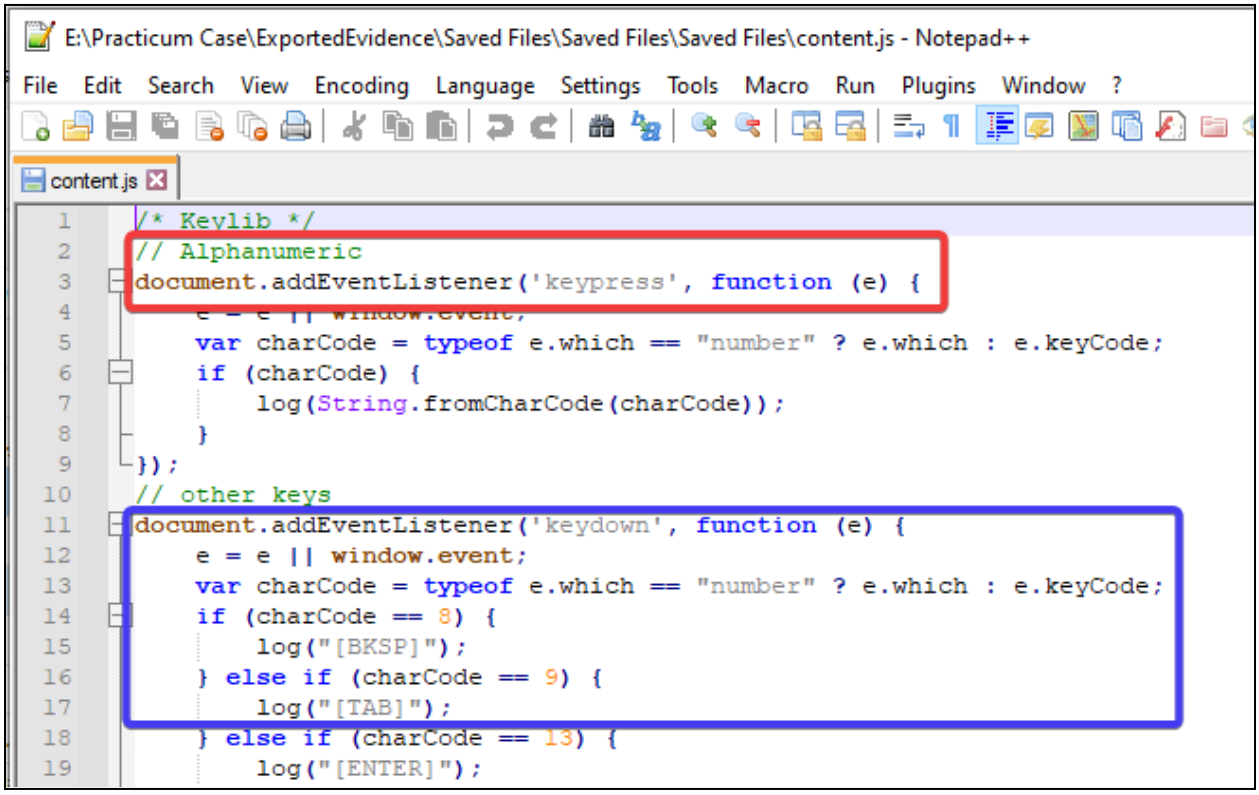


Figure 10 - content.js contents, Keylogger

Content.js also includes code for a history grabber. This can be seen in Figure 11 in the red box.

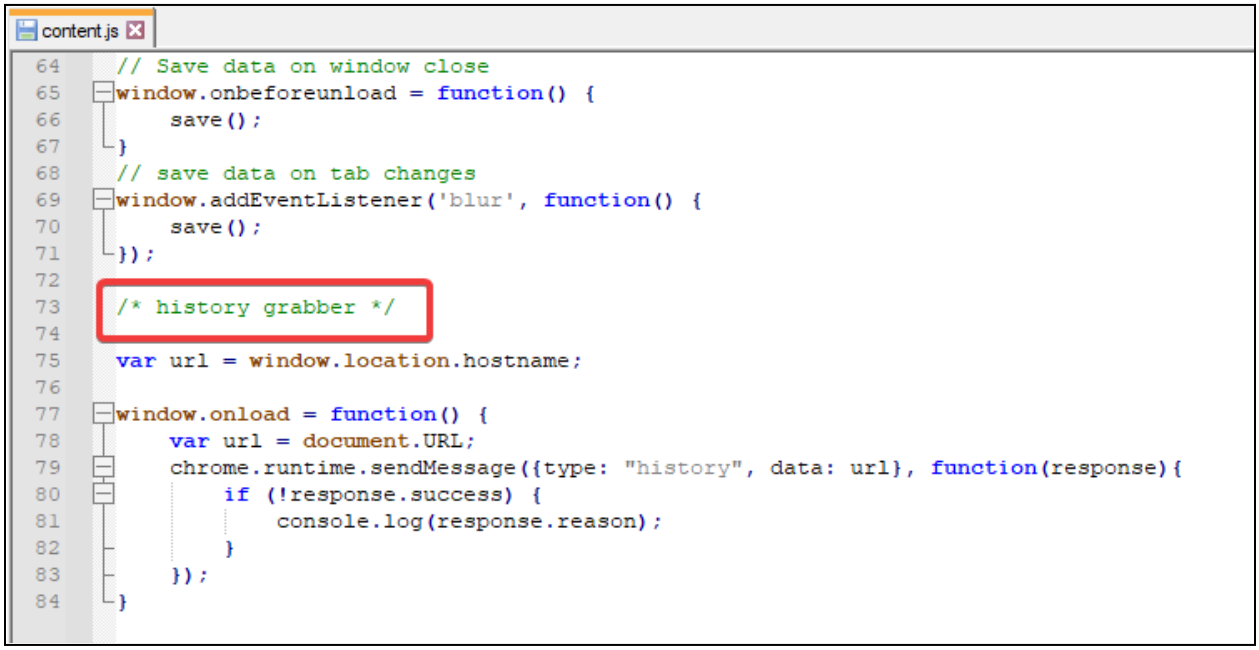


Figure 11 - content.js also contains history grabber

File Name	Image	Path	Timestamp
content.js	PC-2-08-14-18-END.vhd	Users\alabankada\Documents\from Jerrek\CATS\content.js	8/7/2018 9:14:20 PM

Figure 12 - content.js metadata

To verify the execution of this malicious script, we can see the script within the chrome.exe prefetch file. This can be seen in Figure 13.

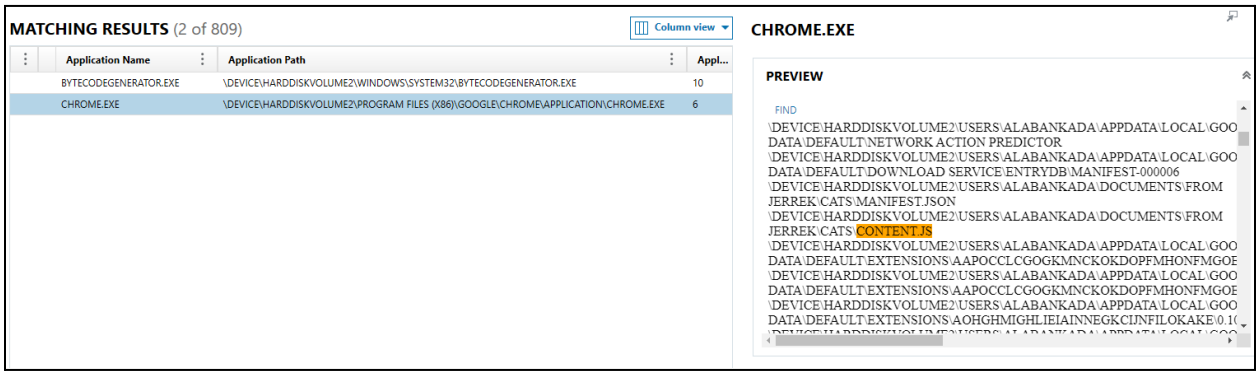


Figure 13 - Content.js prefetch execution confirmation

Another malicious file within the CATs folder is manifest.json. Figure 14 shows the contents of the file and relevant evidence in red boxes. First, the extension name can be seen: We Love Cats! Next, the default popup is set to popup.html. This file will be discussed next. Content and background scripts are set respectively to the last two files analyzed. The description of the manifest also infers “doesn't do anything malicious”. Figure 15 shows the confirmation of execution through a prefetch file and Figure 16 contains the files metadata.

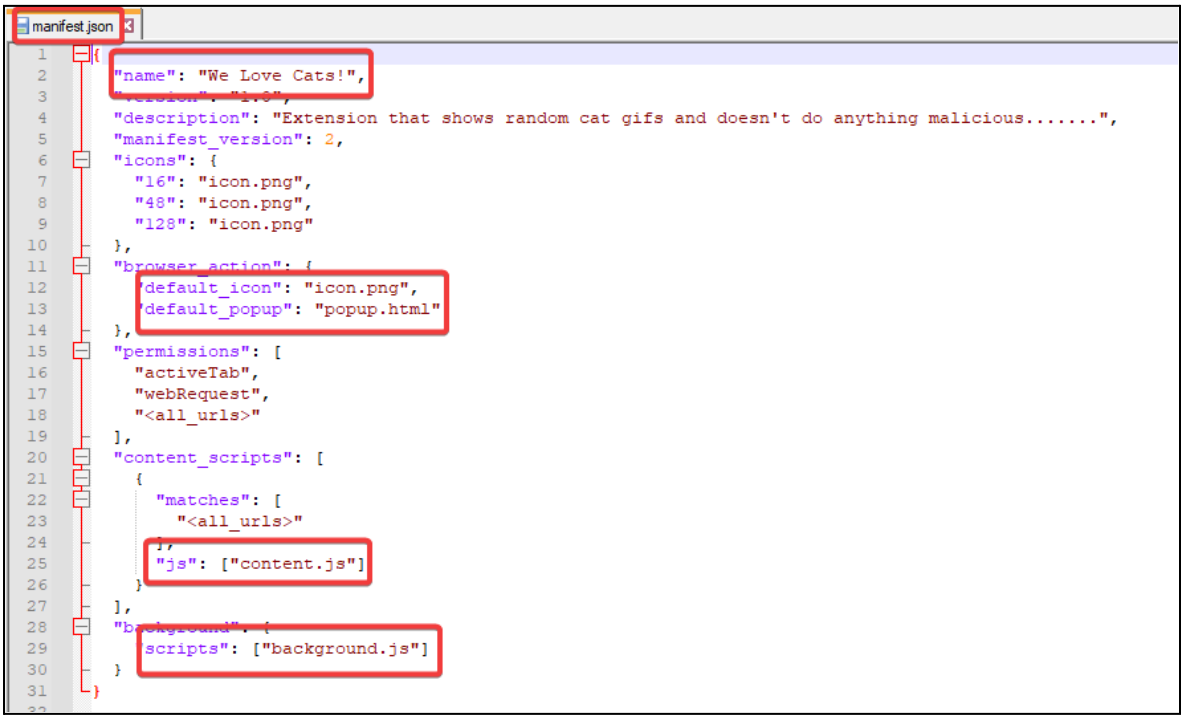


Figure 14 - manifest.json with references to other malicious scripts

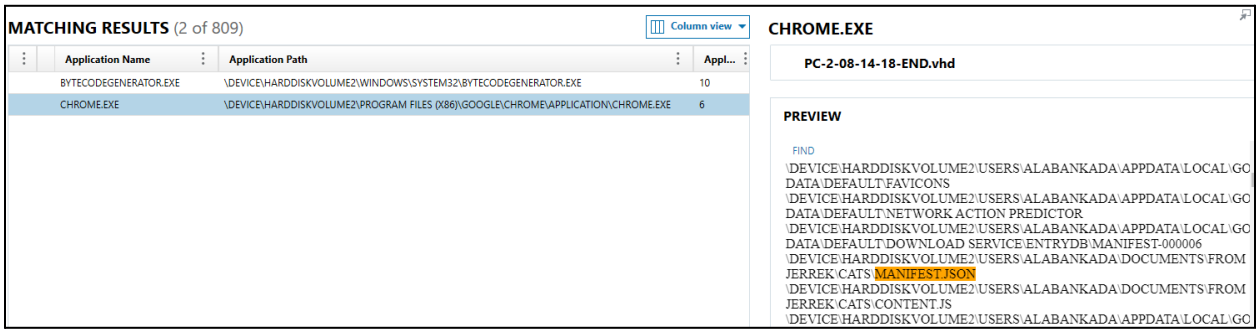


Figure 15 - Manifest.json prefetch execution confirmation

File Name	Image	Path	Timestamp
Manifest.json	PC-2-08-14-18-END.vhd	Users\alabankada\Documents\from Jerrek\CATS\manifest.json	8/7/2018 9:14:20 PM

Figure 16 - Manifest.json metadata

Figure 17 shows the contents of another file, popup.html. This is the html file that starts the malicious plugin and additional scripts and renders the cat gif. The documents metadata can be seen in Figure 18.

```
<!doctype html>
<html>
  <head>
<script src="popup.js"></script>
  </head>
  <body>
    <a href="http://thecatapi.com"><img src="http://thecatapi.com/api/images/get?format=src&type=gif"></a>
  </body>
</html>
```

Figure 17 - popup.html contents

File Name	Image	Path	Timestamp
popup.html	PC-2-08-14-18-END.vhd	Users\alabankada\Documents\from Jerrek\CATS\popup.html	8/7/2018 9:14:20 PM

Figure 18 - popup.html metadata

After seeing all of these malicious files and confirmation that they were run by prefetch, further investigation was conducted. Using the ip address found in the background.js file, a filter for the Pcap files can be created in Wireshark and analysis of files around the timestamp of the files. The activity started at **8/7/2018 10:51:39 UTC.** This can be seen in Figure 19. The timestamp has been converted to UTC.

```
Frame 2195: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  7, 2018 17:51:39.731947000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
```

Figure 19 - First Data Exfiltration Event Timestamp

Figure 20 shows the TCP stream of the first Data Exfiltration Packet. Hidden inside the POST request is a base64 encoded string. This can also be seen at the bottom of Figure 21.

Figure 20 - TCP Stream of Exfiltrated Data Packet

After inputting the encoded string into CyberChef, the output decodes into exfiltrated form data. Figure 21 shows the full contents of an email sent from Jerek, the main suspect, about installing the chrome extension. This data was exfiltrated.

Figure 21 - Decoded Base64 String from TCP Packet

The next relevant form of data exfiltration that was confirmed through packet analysis was keylogging . This occurred the same day a few seconds after the last exfiltration, on **8/7/2018 10:53:21 UTC** This can be seen in Figure 22 and was converted to UTC.

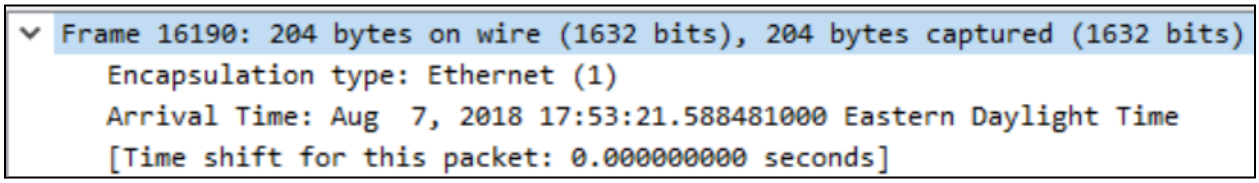


Figure 22 - Form Data Exfiltration Event Timestamp

The packet TCP stream can be seen below in Figure 23. This shows the encoded base64 string appended to the packet as well.

Figure 23 - Appended base64 string

The encoded string can be decoded in CyberChef to reveal the keylogging strings captured. These can be seen in Figure 24.

Figure 24 - Decoded Base64 String from TCP Packet

Another type of data exfiltration that occurred was the screen grabbing. This occurred at **8/7/2018 10:48:32 UTC** and found in **2018-08-07_14-42-02.pcap** as seen in Figure 25.

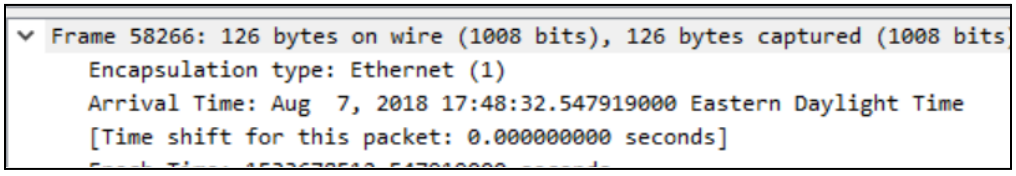


Figure 25 - Keylogger Data Exfiltration Event Timestamp

The TCP stream for this is significantly larger as the size of an encoded image can be large. This can be seen in Figure 26.

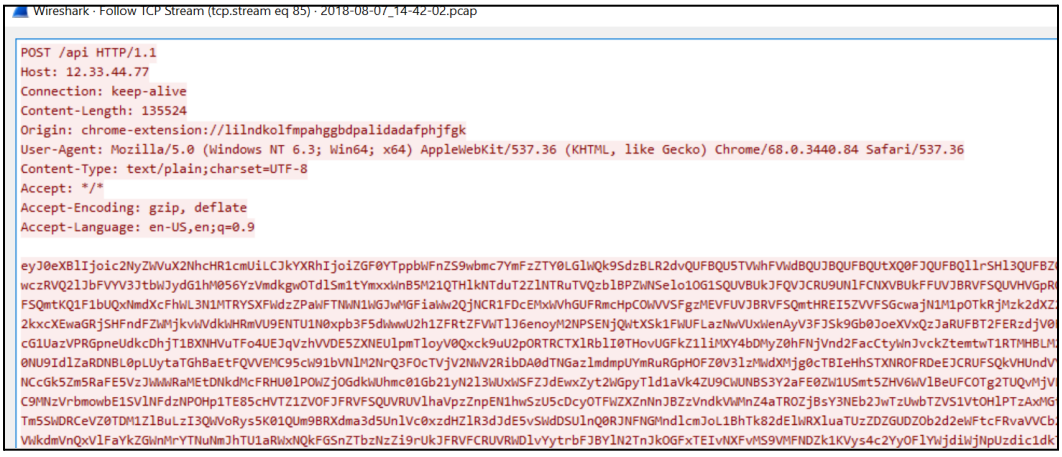


Figure 26 - Screen Grabber TCP Stream with Encoded Image

Using CyberChef, the string can be decoded then rendered. The first image exfiltrated is an image of the user's email inbox. This can be seen below in Figure 27.

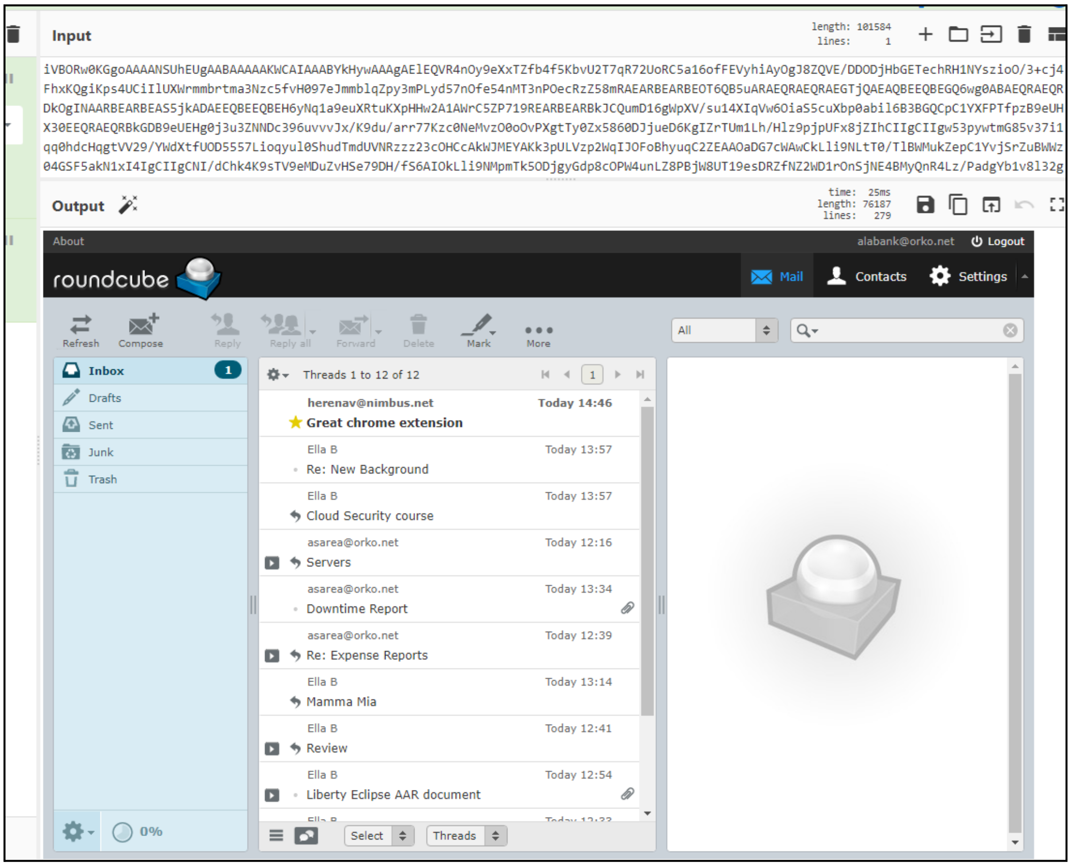


Figure 27 - Screen Grabber Exfiltration Decoded

Lastly, confirmation of the third type of data exfiltration can be seen in Figure 28. This is the exfiltration of the users chrome history. This event occurred at **8/7/2018 10:51:13 UTC** and found in **2018-08-07_14-42-02.pcap**

```
Frame 92196: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  7, 2018 17:51:13.348833000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1533678673.348833000 seconds
    [Time delta from previous captured frame: 0.000626000 seconds]
```

Figure 28 - History Grabber Data Exfiltration Event Timestamp

The TCP stream for the history grabber can be seen in Figure 29 below.

Figure 29 - History Grabber TCP Stream

The encoded string can be decoded in CyberChef as seen in Figure 30.

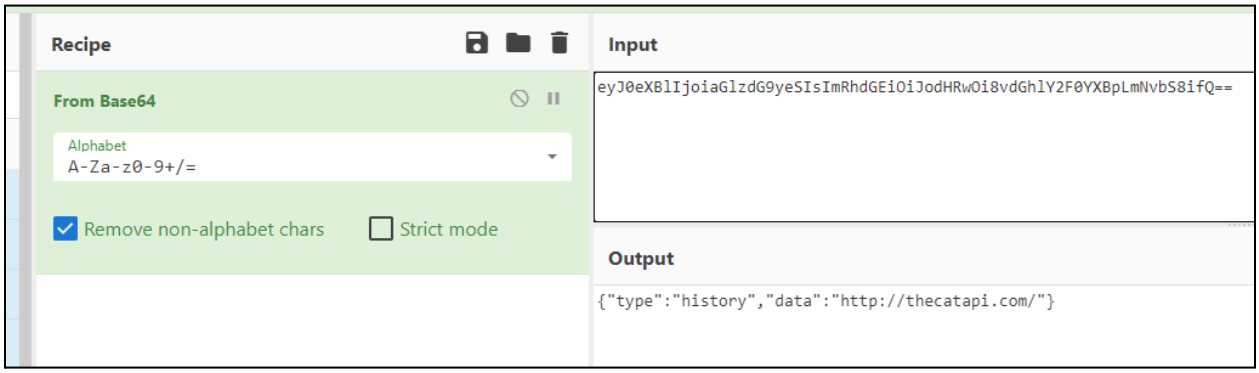


Figure 30 - History Grabber Encoded string decoded

Onion.zip

Another suspicious file that was sent around the organization was the onion.zip and onion.rtf files. This can be seen in Figure 31 and metadata in Figure 32.

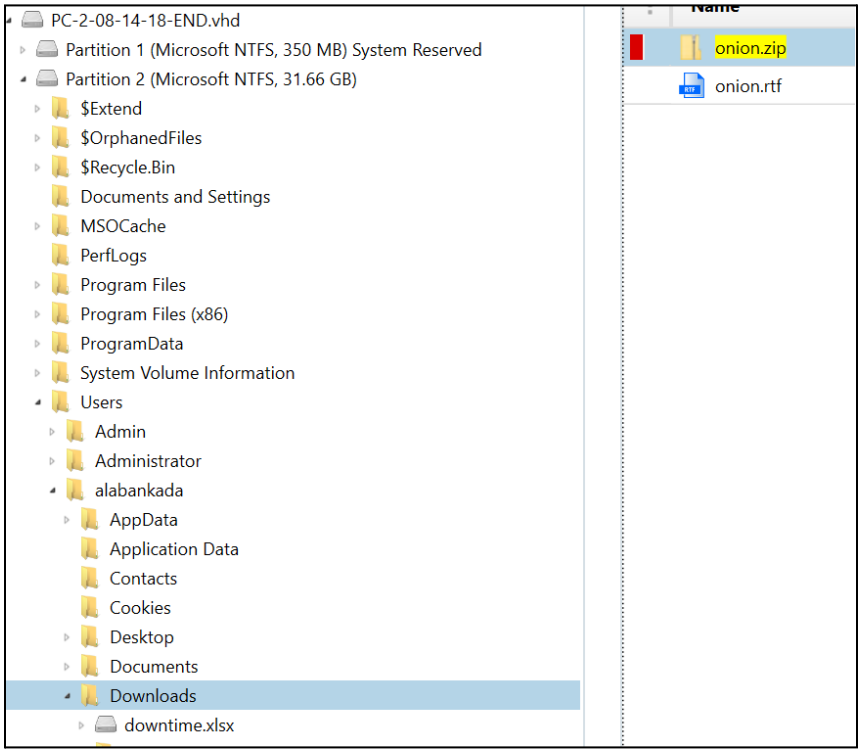


Figure 31 - Onion.zip Location

File Name	Image	Path	Timestamp
onion.zip	PC-2-08-14-18-END.vhd	Users\alabankada\Downloads\onion.zip	8/14/2018 6:38:14 PM

Figure 32 - Onion.zip File Metadata

This file was found after analyzing the SMTP email files. Figure 33 below shows the message with the onion.zip file as an attachment. This email was sent on **8/14/18** at **5:16:54 PM**

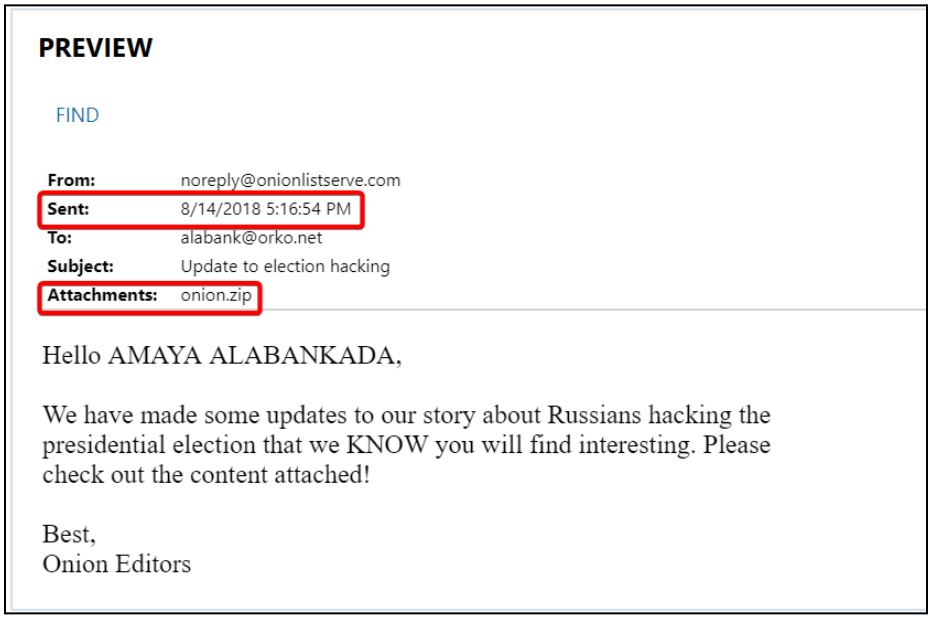


Figure 33 - Email with malicious onion.zip attachment

The attachment can be extracted and onion.rtf can be found inside. This can be placed in a personal malware processing virtual machine to further determine what it does. When opened, it looks like Figure 34 below.

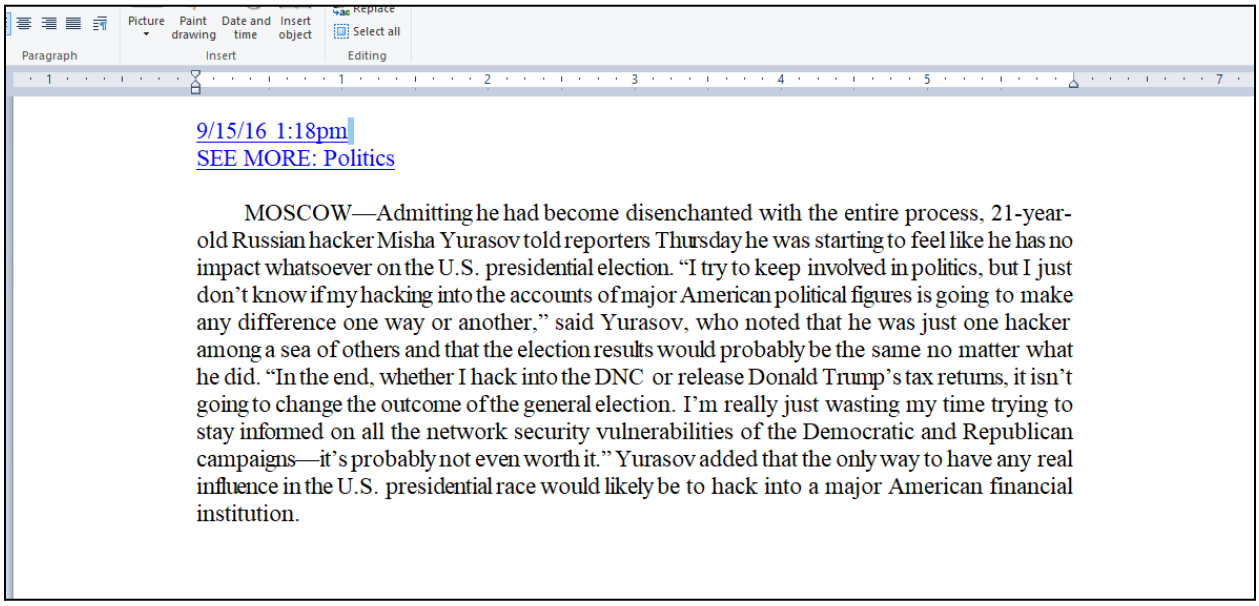


Figure 34 - Onion.rtf content

On the second page of the document, a hidden exe file can be found — e.exe (Figure 35). This executable is malicious and can be seen automatically being executed in Figure 35 and analyzed in process monitor in Figure 36.

The publisher could not be verified. Are you sure you want to run this software?

Name: e.exe

Publisher: **Unknown Publisher**

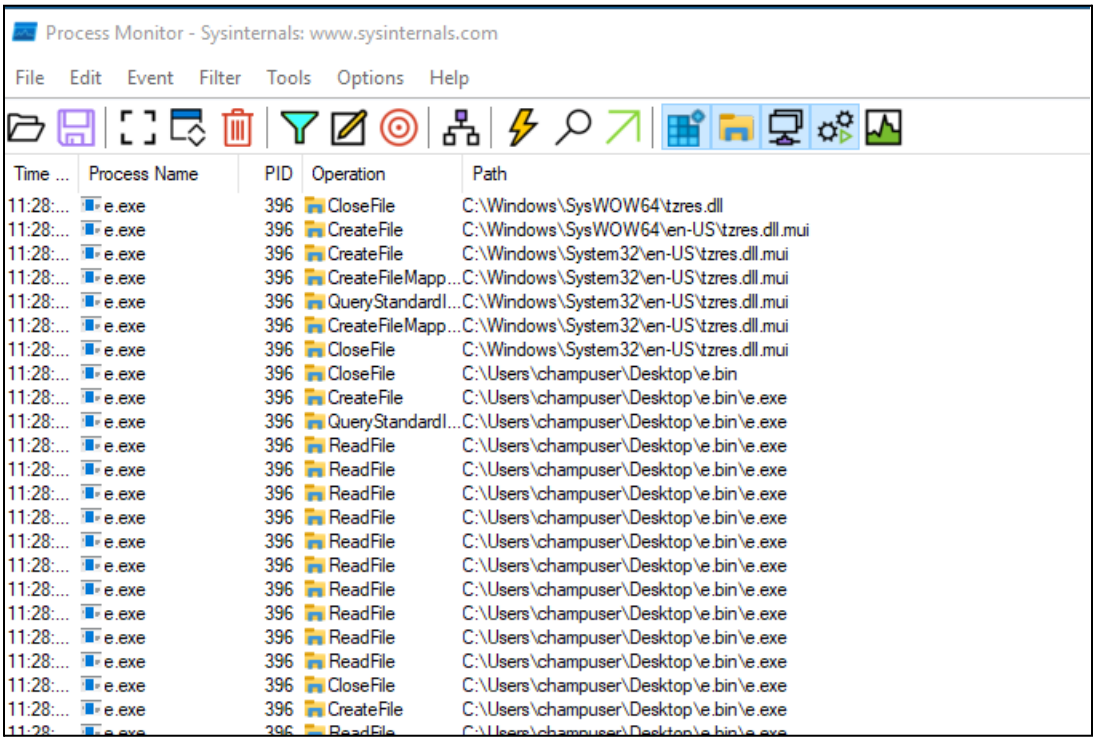
Type: Application

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.

How can I decide what software to run?

Figure 35 - Hidden e.exe executable inside onion.rtf

Some of the process monitor operations can be seen below in Figure 36. While there are lots of events, many of them are registry keys being checked and changed. No new processes are created and no outbound connections are attempted.



```
Time ...  Process Name   PID  Operation          Path
11:28:... e.exe          396  CloseFile          C:\Windows\SysWOW64\tzres.dll
11:28:... e.exe          396  CreateFile         C:\Windows\SysWOW64\en-US\tzres.dll.mui
11:28:... e.exe          396  CreateFile         C:\Windows\System32\en-US\tzres.dll.mui
11:28:... e.exe          396  CreateFileMapp...  C:\Windows\System32\en-US\tzres.dll.mui
11:28:... e.exe          396  QueryStandardI...  C:\Windows\System32\en-US\tzres.dll.mui
11:28:... e.exe          396  CreateFileMapp...  C:\Windows\System32\en-US\tzres.dll.mui
11:28:... e.exe          396  CloseFile          C:\Windows\System32\en-US\tzres.dll.mui
11:28:... e.exe          396  CloseFile          C:\Users\champuser\Desktop\e.bin
11:28:... e.exe          396  CreateFile         C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  QueryStandardI...  C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  ReadFile           C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  CloseFile          C:\Users\champuser\Desktop\e.bin\e.exe
11:28:... e.exe          396  CreateFile         C:\Users\champuser\Desktop\e.bin\e.exe
```

Figure 36 - process monitor with e.exe filter

The information from the process monitor shows that once the rtf is opened, e.exe drops itself in the temp folder, and was dropped from a different process. It also reads the computer name. Figure 37 contains more metadata about the executable.

File Name	Image	Path	Timestamp
e.exe	PC-2-08-14-18-END.vhd	Users\alabankada\AppData\Local\Temp\e.exe	N/A

Figure 37 - e.exe metadata

Suspicious Invoice

Another suspicious file that was sent over email was a variety of invoices. The first invoice pdf was sent at **8/21/2018 9:02:08 PM.** The contents can be seen below in Figure 38. The attachment TCinc_Invoice_20170-4072-00.pdf was sent with it.

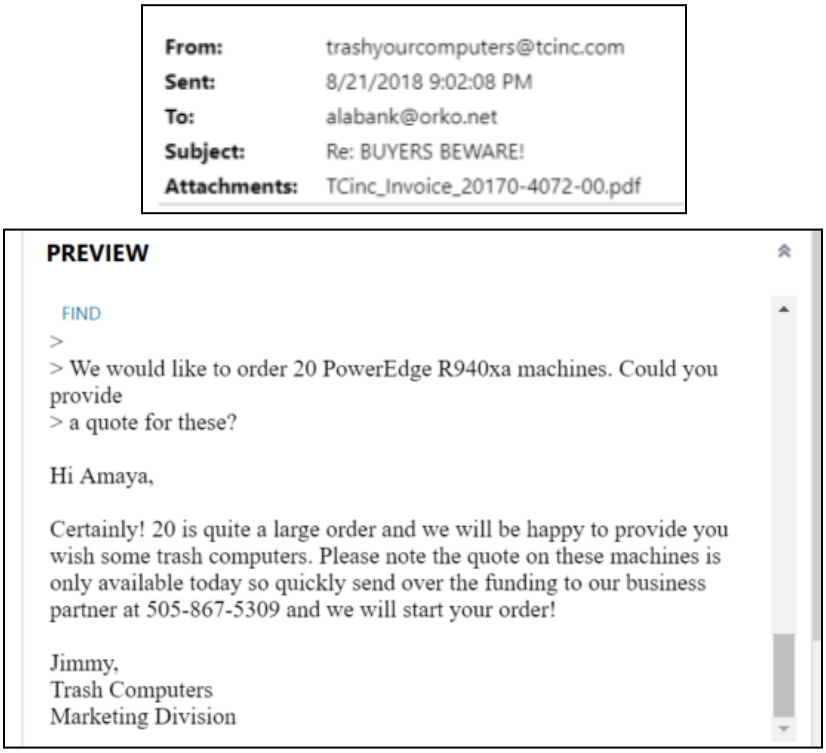


Figure 38 - Mail information and Mail Content

When viewing this pdf, it looks benign and like a normal invoice. A screenshot of the pdf can be seen in Figure 39.

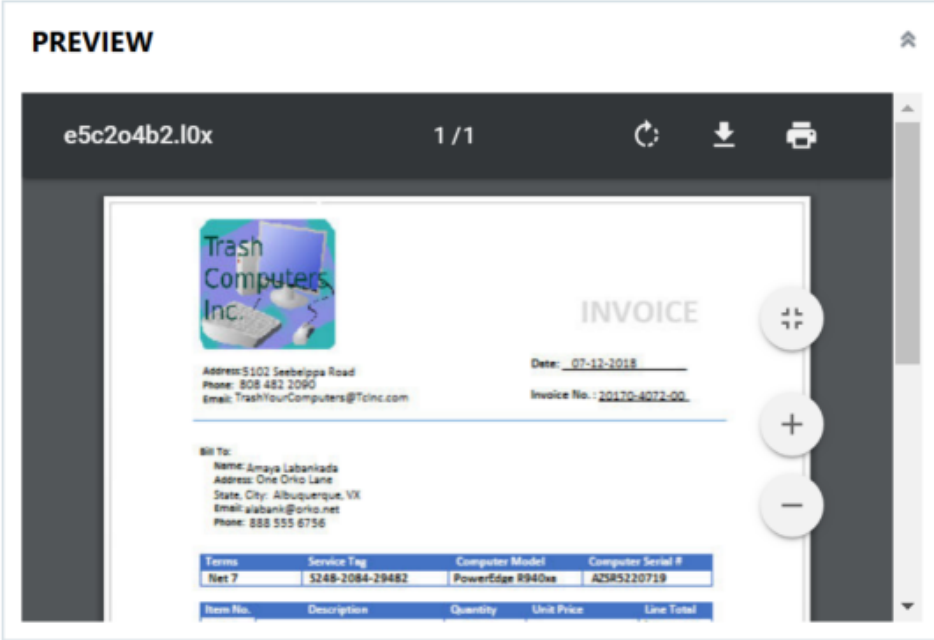


Figure 39 - Invoice screenshot

In a follow up email, the invoice was updated. This can be seen in Figure 40.

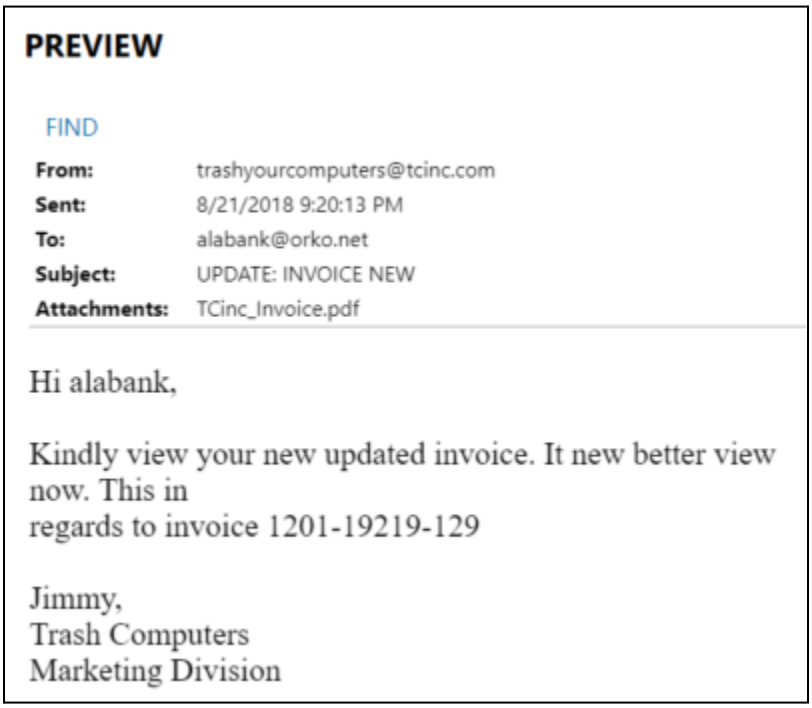


Figure 40 - Follow up email with new invoice

This version of the document comes with a fake secure login as seen in Figure 41. However, when downloading the document to a virtual machine, the fake popup is not interactable. This tracks as the users had difficulties logging in also and followed up with the provider and received another suspicious pdf document a few minutes later at **8/21/2018 9:43:49 PM** seen in Figure 42 .

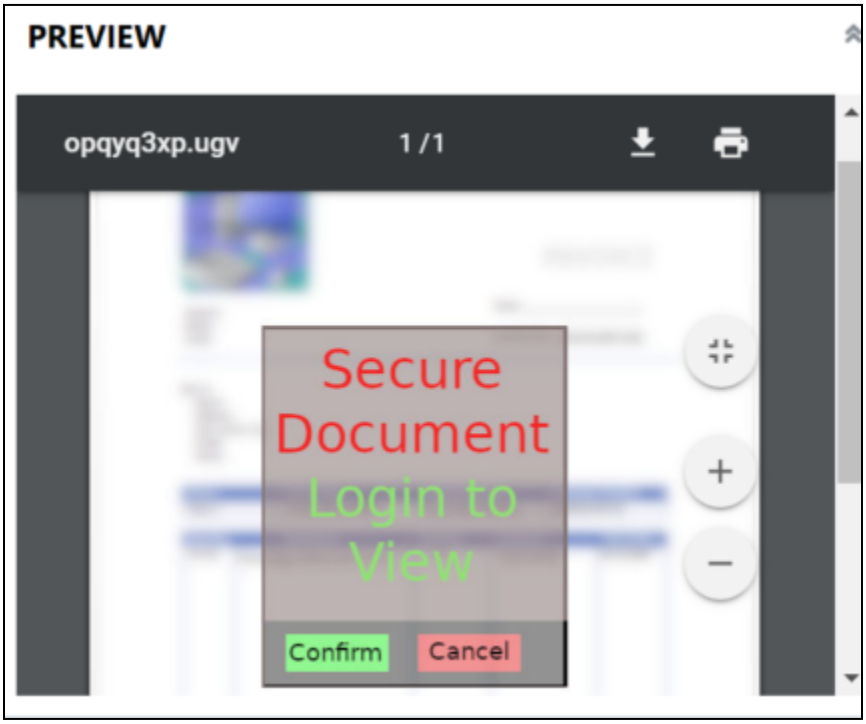


Figure 41 - Document with broken “Secure login”

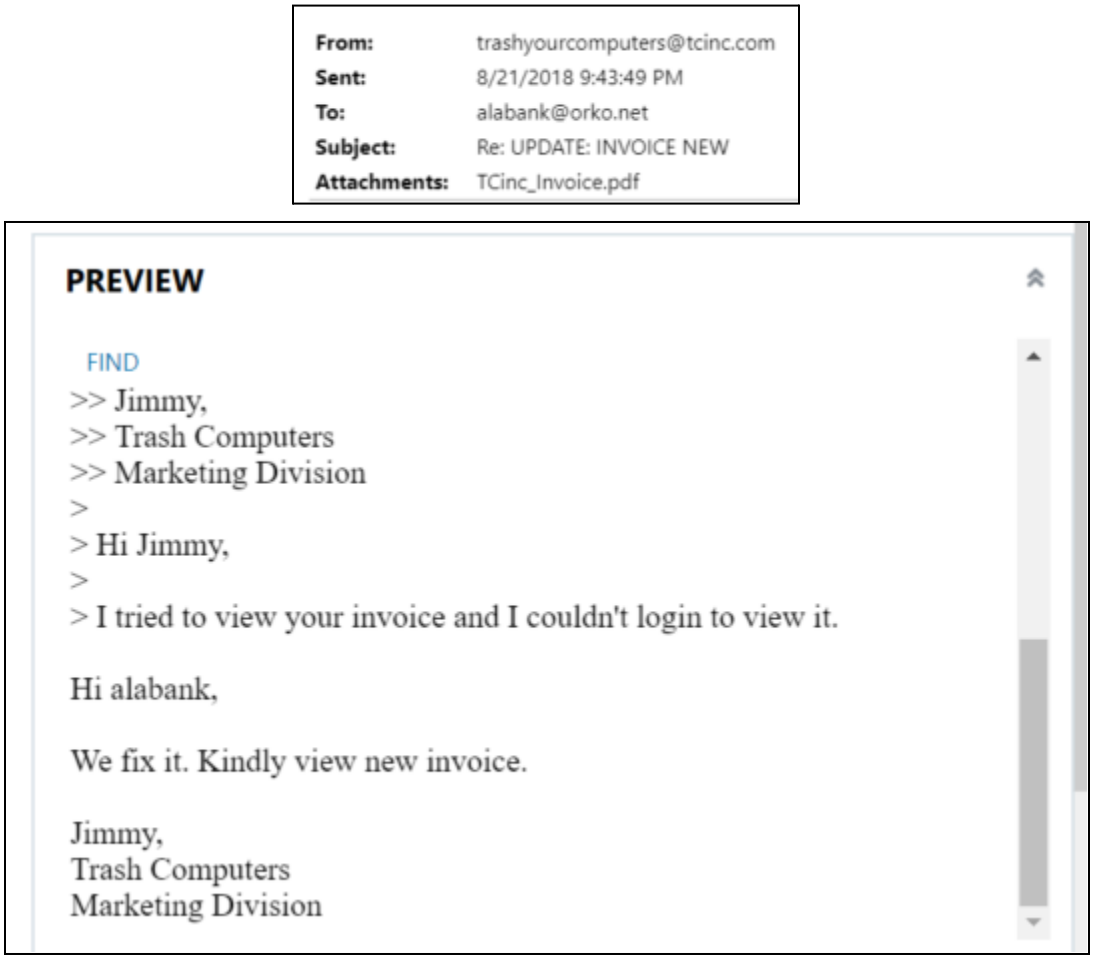


Figure 42 - Follow up email and email information

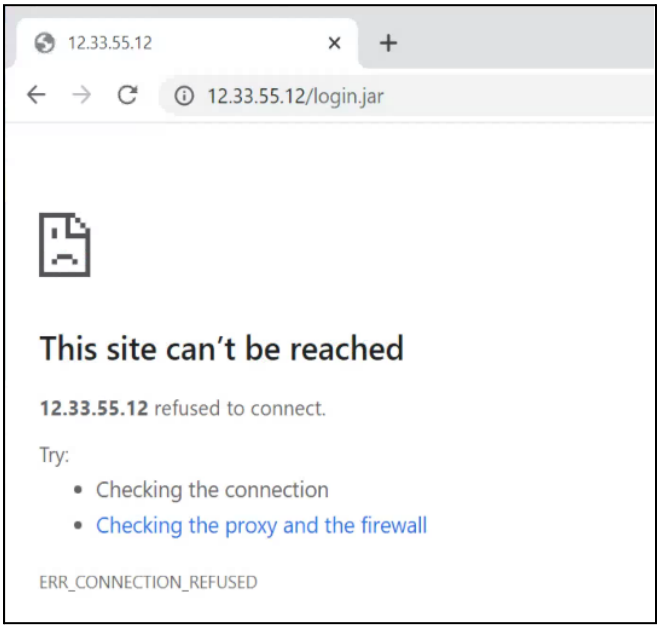


Figure 43 - PDF attempts to navigate to site at 12.33.55.12/jar

The site in Figure 43 above is no longer available as it was used for credential harvesting.

Caller.vbs

The last malicious file located on the system is caller.vbs. This file originated from an email chain from someone at Hazia, or potentially posing as an employee. Figure 44 shows the content of the email and Figure 45 shows the caller.vbs attachment.

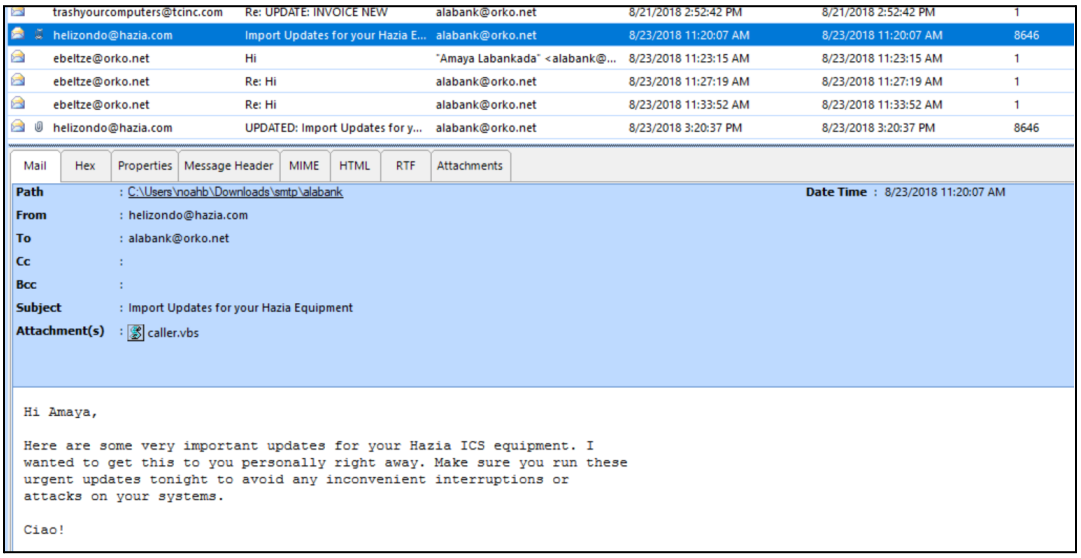


Figure 44 - First caller.vbs Email Content

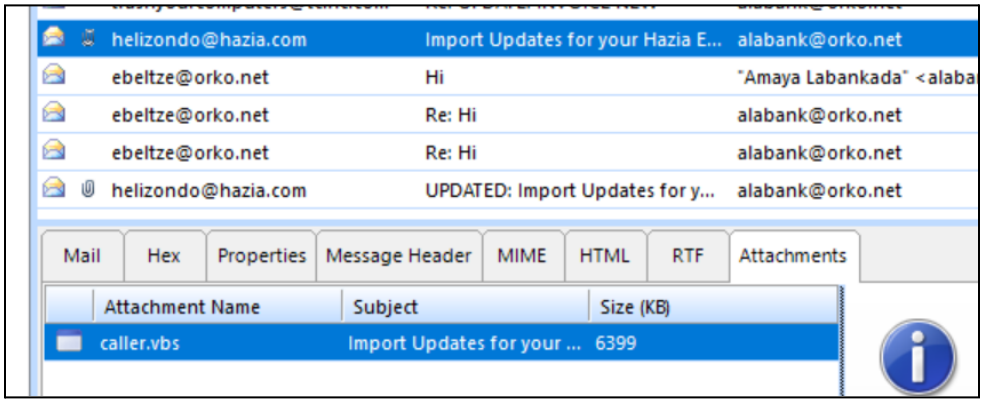


Figure 45 - first Caller.vbs attachment

The first file creation event timestamp of caller.vbs can be seen in Figure 46 below. This is the time when the file was downloaded.

File Name	Image	Path	Timestamp
caller.vbs	PC-3-08-23-18-END.vhd	Users\ebeltzetan\Downloads\caller.vbs	8/23/2018 8:07:38 PM

Figure 46 - Caller.vbs File Download / Creation Time

The content of the caller.vbs script can be viewed in Axiom. The file in Figure 47 seems to be a form of powershell executable.

Figure 47 - caller.vbs content

There is confirmation of execution in a few files such as the jump list. This can be seen in Figure 48. Caller.vbs can be seen in the jump list of Quick Access, Notepad, and wscript.exe.

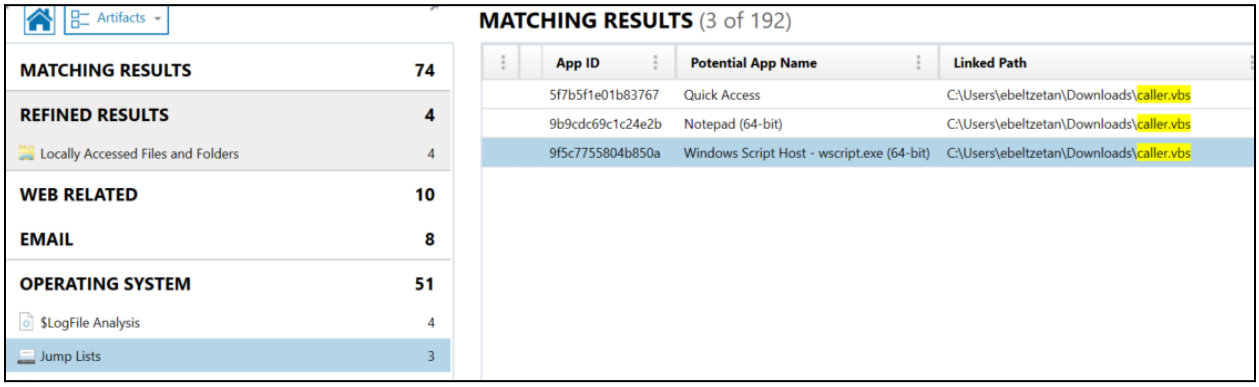


Figure 48 - caller.vbs inside inside jumplist

We can also see confirmation of execution inside the lnk files and the prefetch files. This can be seen in Figures 49 and 50.

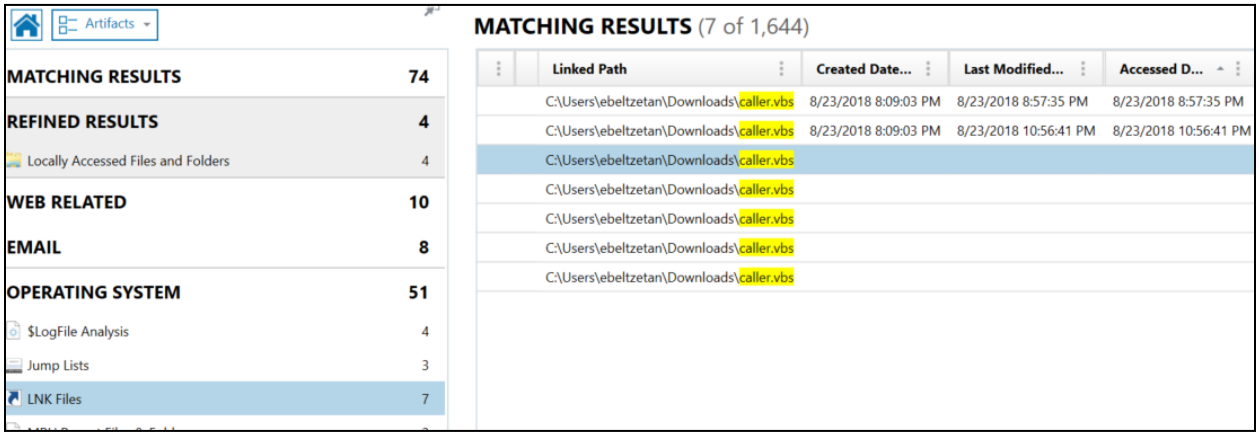


Figure 49 - caller.vbs inside inside LNK files

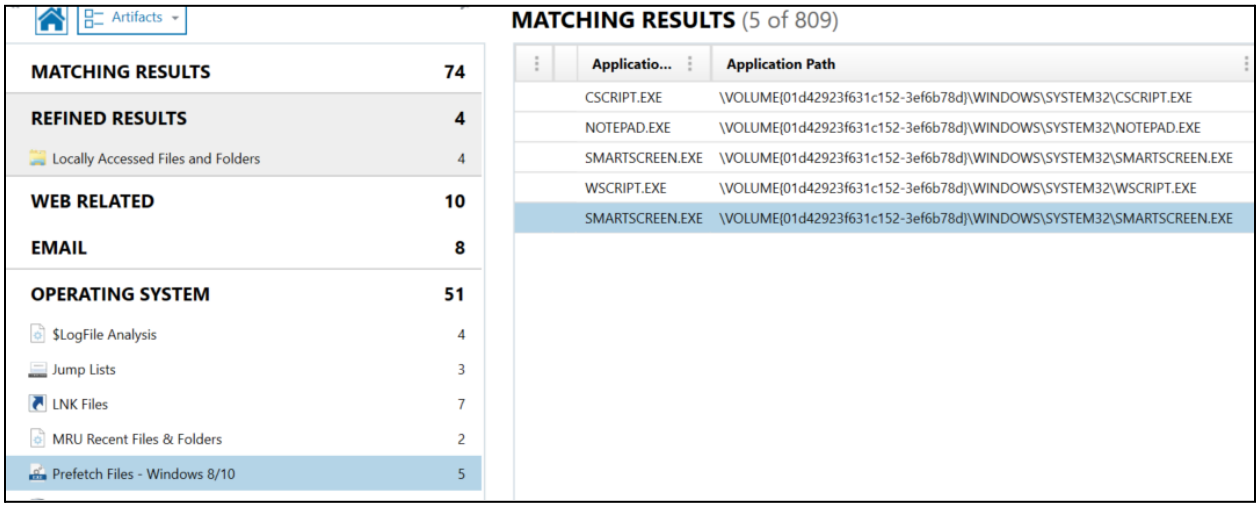


Figure 50 - caller.vbs prefetch file confirmation

When the caller.vbs script is run a few things happen. First the script is run through wscript.exe. This lines up as in Figure 50 above the caller.vbs script has a prefetch entry in wscript.exe and can be seen below in Figure 51 after running it in a personal virtual machine.

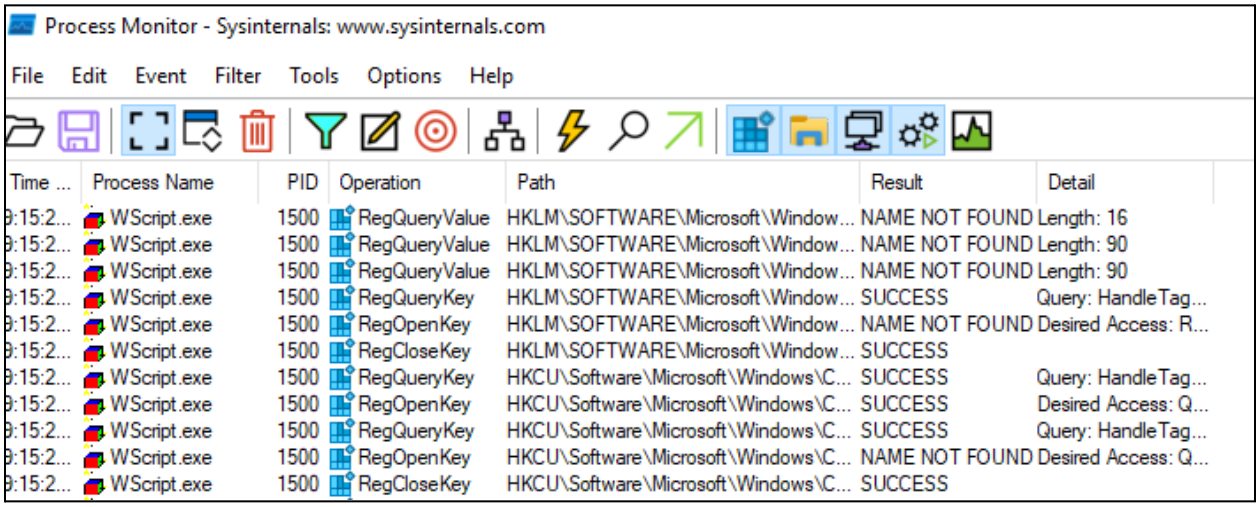


Figure 51 - ProcessMonitor of Caller.vbs execution

Next, the script runs a powershell command that drops and starts a new file called: aisoundfwemidf.ps1. This is a new powershell script. This script then creates and runs an executable file called aisoundfwemidf.exe. This can be seen in Figure 52

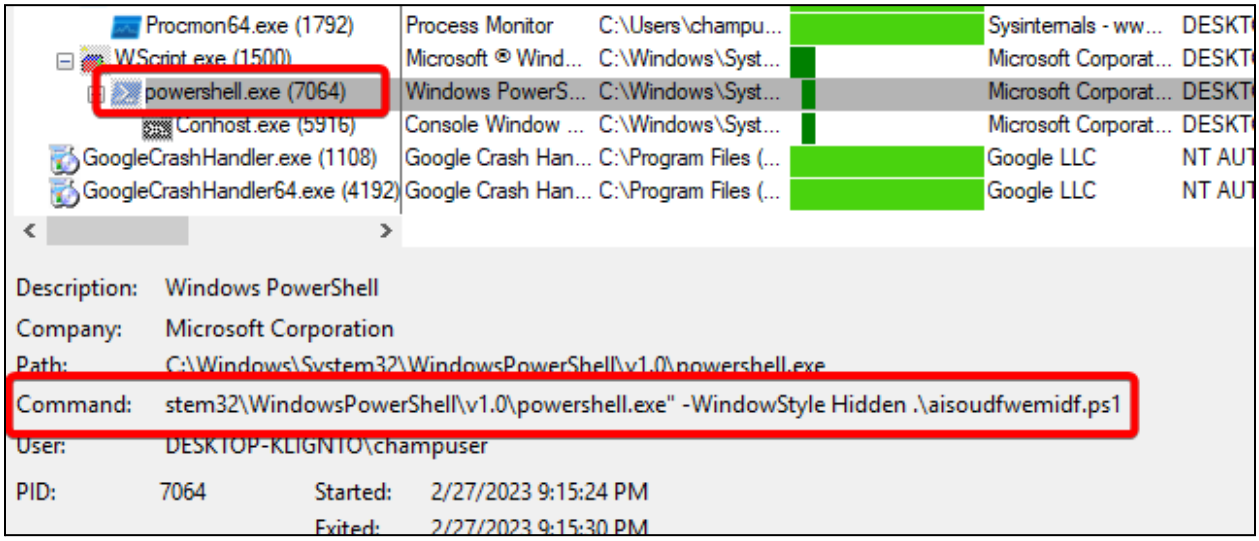


Figure 52 - powershell execution of script

This new executable file is ransomware. Once this executes, it encrypts all files on the system. If you are on 32-bit windows, it also sets the background to a ransomware image Figure 54. We can confirm this information by running it through a forensic virtual machine.

Since we know it drops a file called aisoundfwemidf.ps1, we can search for the file specifically. The file was created on **8/23/2018 8:41:33 PM** and accessed on **8/23/2018 8:46:37 PM.** We can confirm the execution of the aisoundfwemidf.ps1 script in prefetch. This can be seen in Figure 53.

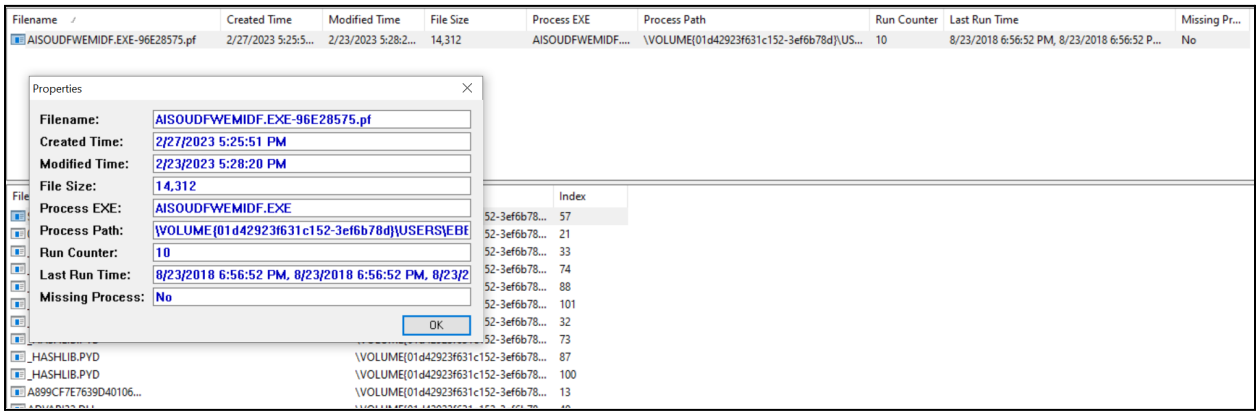


Figure 53 - Prefetch Data for aisoundfwemidf.ps1

After execution, host files become encrypted with the .cryptified extension and the photo in Figure 54 gets set to the user's background. The image says how all your files are encrypted and to send 3 monaro to a crypto wallet in order to decrypt the files.

Figure 54 - Ransomware Background

An example of encrypted files can be seen below in Figure 55 showing before and Figure 56 showing after.

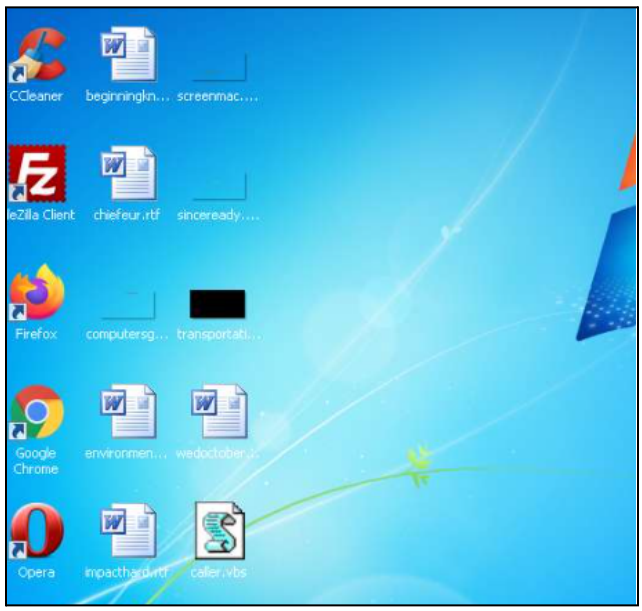


Figure 55

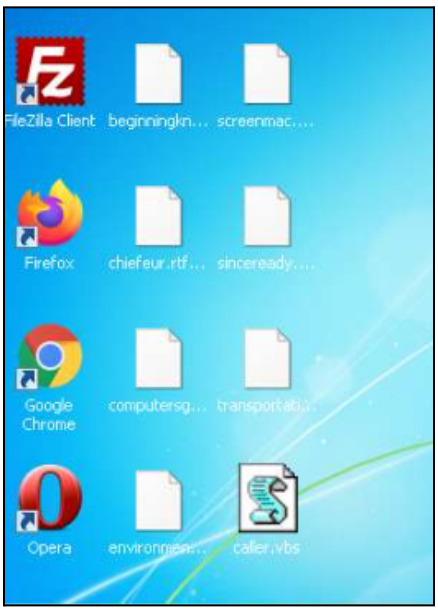


Figure 56

One of the user's documents that was encrypted was a file called: LE FINAL Exercise Summary 1May2017_Public Doc.pdf.Cryptified. All files the user had were encrypted, an example of one of these can be seen below. The file looked like Figure 57 before it was encrypted and was unreadable after.

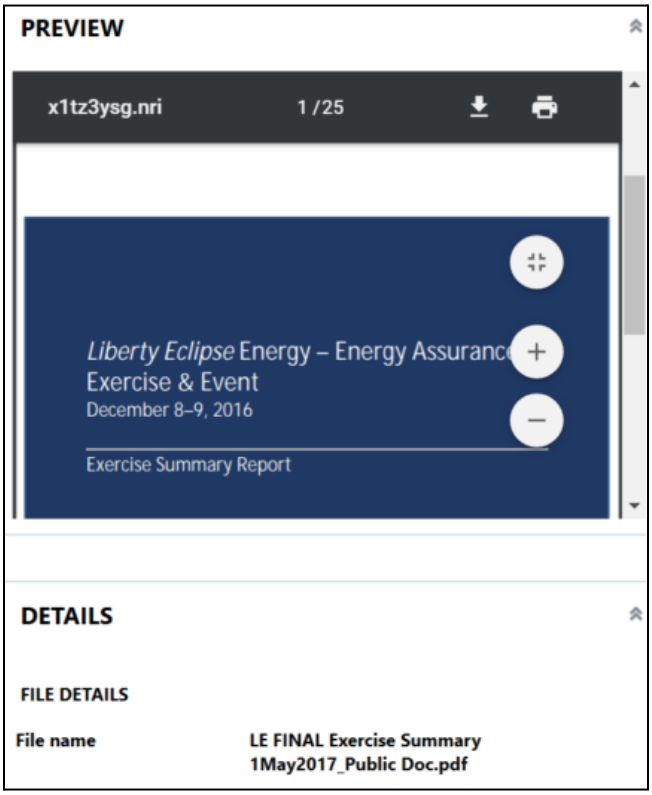


Figure 57 - Example encrypted user file

Conclusion / Summary

In conclusion, there are a variety of severe breaches that occurred with Orko Electric. First the malicious chrome extension exfiltrating sensitive company data. This occurred through unauthorized use of a USB device to install a chrome extension that should not have been installed. In order to remediate, I would recommend a full removal of the extension and restart of the pc at minimum. In order to ensure full remediation, I would recommend a full installation of windows or reversion to a backup.

The malicious rtf document on the system was downloaded from a phishing email. Users should be more careful about what documents they are downloading from external sources. Phishing is becoming a big problem in the workplace now and training should be done to protect end users.

The ransomware is one of the most impactful security events on the system. The user has lost complete access to sensitive company files, lost the ability to work, and the company may have to pay the ransom if no backups are present and the data needs to be recovered. Luckily, it seems that some of the encrypted files can be recovered through file carving.

Overall, users need computers to be remediated and training company wide should be conducted on phishing and how it can potentially destroy a business.

Glossary

Threat Actor - An individual or group that attempts to harm a company or its assets through cyber attacks.
Data Exfiltration - The unauthorized transfer of data from a company's network to an external location.
Data Encryption - The process of converting data into a secret code to prevent unauthorized access.
Computer Image - A copy of a computer's hard drive or specific files that can be used for backup or analysis purposes.
Pcap File - A file that captures and stores network traffic, which can be used to analyze network activity or troubleshoot issues.
Windows Registry - A database that stores configuration settings and options for Microsoft Windows operating system.
Registry Hive - A portion of the Windows Registry that contains a specific set of configuration information.
Prefetch File - A file created by the Windows operating system that helps speed up the launching of frequently used applications.
LNK file - A file type used by Windows operating system to create shortcuts to applications, files or folders.
JumpList - A list of recently opened files or applications, displayed by Windows operating system, which allows users to quickly access them.
TCP Stream - A sequence of data exchanged between two devices over a TCP/IP network connection.
Base64 - A binary-to-text encoding scheme used to represent data in ASCII format, commonly used in email attachments and HTML web pages.
Phishing - A type of cyber attack where an attacker sends a fake message or email, impersonating a trustworthy source, in order to trick the recipient into sharing sensitive information or taking an action that will compromise their system.
Trojan - A type of malware that appears legitimate but actually contains harmful code that can damage, disrupt or steal data from a computer system.
Virtual Machine - A software environment that emulates a complete hardware system, allowing multiple operating systems to run on a single physical machine.
IP Address - A unique numerical identifier assigned to each device on a computer network, used for communication and network routing.
Credential Harvesting - The process of obtaining user login credentials through various means, such as phishing, keylogging or brute-force attacks.
SMTP - A protocol used to send and receive email messages over the Internet.
Powershell - A command-line shell and scripting language developed by Microsoft, used for system administration tasks and automation.
Ransomware - A type of malware that encrypts a victim's files or blocks access to their system until a ransom is paid to the attacker.
Crypto currency - A digital or virtual currency that uses cryptography to secure and verify transactions, and to control the creation of new units.