TRIPLE R

Examination Report

CASE #: 002-2022

Examiner: Zachary Rousseau

# Table of Contents

Contents

[Table of Contents 1](#_Toc120642082)

[Summation 2](#_Toc120642083)

[Background 2](#_Toc120642084)

[Summary of Findings 2](#_Toc120642085)

[Acquisition and Data Analysis Tools 3](#_Toc120642086)

[Acquisition 3](#_Toc120642087)

[Data Analysis Tools Used 3](#_Toc120642088)

[Analysis 3](#_Toc120642089)

[User Account 3](#_Toc120642090)

[Emails 4](#_Toc120642091)

[Internet Artifacts 7](#_Toc120642092)

[Recycle Bin 9](#_Toc120642093)

[Target List 1.xlsx 9](#_Toc120642094)

[Executable Files 10](#_Toc120642095)

[USB Device Attached 10](#_Toc120642096)

[Recommendations 10](#_Toc120642097)

# Summation

## Background

Triple R received a request to conduct a digital forensic examination. Mrs. Genevieve Belvins reported that her bank account had been hacked. One logon IP[[1]](#footnote-1) addresses geo-located to Vermilion City where the Internet Service Provider (ISP) confirmed that the IP was public WiFi for the Verminlion City Gym. Detective Ash identified Jessie and James of Team Rocket due to their frequent attendance and the gym and their long criminal history. Detective Ash encountered a laptop stashed away in a back room as potentially suspicious. Detective Pikachu collected and imaged the device at 08:05 PST on 11 April 2021.

Triple R has been asked to examine the E01 image for the following:

* Any evidence identifying the person(s) who own the device
* Any evidence related to the theft of bank account information
* Items indicating what the suspect(s) indented to do with the data
* Any other item of interest within the scope of the warrant

## Summary of Findings

The examination determined that the flash drive contained suspicious data. The following data was identified:

* Web browser bookmarks, cache, cookies, and downloads containing showing frequent visits to online bank accounts.
* Usage of services and visits to websites containing VPNs [[2]](#footnote-2)and Tor[[3]](#footnote-3) providing anonymity while accessing the internet.
* Suspicious internet search terms.
* User account TeamRocket and associated email.

A suspicious Microsoft Office .xlsx document

* 1 deleted file located in the recycle bin
* 1 USB device was attached to the system
* (8) Emails exchanges in which the transfer of lists as well as accounts for money is discussed.

# Acquisition and Data Analysis Tools

## Acquisition

Examiner Rousseau received an E01 image from Det. Pikachu created using FTK Imager 4.5.0.4. The log indicates that the image was created by Det. Pikachu on 11 April 20221. Utilizing QuickHash v3.3.1, the image file was verified to match the hash values contained in the log.

Acquisition and verification hashes[[4]](#footnote-4):

MD5[[5]](#footnote-5): a1e2eb4ddfec6a3de3b81bb6a565b38b

SHA1[[6]](#footnote-6): 3a55fbb3a053752069eba328680c91ed69ee8b9b

## Data Analysis Tools Used

For this examination the following tools were used, previously validated by Triple R:

* QuickHash v3.3.1
* Autopsy v4.19.3

# Analysis

### User Account

TeamRocket

The user account TeamRocket was located and related to SID[[7]](#footnote-7) 1004. The account had the associated email address [James39933@outlook.com](mailto:James39933@outlook.com) and was created on 2021-04-11 8:22:40 PST. The account was last accessed on 08:22:59 PST of the same day.

The email address references the suspect James, and the account references the affiliated group Team Rocket.

### Emails

2000006b\_5da3e6d3d79fad.eml

MD5: FFE9DE9631817ACF6D41A858D07E9D5D

SHA-1: 1D4F390965F49D0C1E3330BE8EF83C3720830FE6

This emailed containing the subject line “Re: ?” Contains an exchange between [James39933@outlook.com](mailto:James39933@outlook.com) and [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) sent on Sunday 11 April 2021 at 8:55 AM PST. In the email exchange emails are signed “J” from [James39933@outlook.com](mailto:James39933@outlook.com) and “Musashi” from [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com). Email contents discuss [James39933@outlook.com](mailto:James39933@outlook.com) receiving and using a list from Jessie11445@protonmail.com.

Graphical user interface, text, application, email

Description automatically generated

##### 20000002\_322748d0f2841c.eml

MD5: B775DE1D78276D6773802D5AF00CAAF5

SHA-1: 3D60E278F267D562151AE4D33C3E9452043F39FB

This email contains an alert from [account-security-noreply@accountprotection.microsoft.com](mailto:account-security-noreply@accountprotection.microsoft.com) to [James39933@outlook.com](mailto:James39933@outlook.com) on Sunday 11 April 2021 at 08:22 AM PST. In this exchange [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) was added as a secondary user to [James39933@outlook.com](mailto:James39933@outlook.com) account providing [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) access.

Graphical user interface, text, application, email

Description automatically generated

20000066\_49a41fdee2c47c.eml

MD5: 46A6CBB0DD778F02DCAF44AEA46C5585

SHA-1: 9670CBA15346F71025608A3997D8E9FA76189D95

This email contains an exchange from “Meowth Rocket” [meowth55788@gmail.com](mailto:meowth55788@gmail.com) to [james39933@outlook.com](mailto:james39933@outlook.com) on Sunday 11 April 2021 at 08:44 AM PST. In this exchange “Meowth Rocket” states that they obtained a new list and for [james39933@outlook.com](mailto:james39933@outlook.com) to obtain said list from “Jessie.”

Graphical user interface, text, application, email

Description automatically generated

20000066\_96d5afcafecfa1.eml

MD5: C25AF546BA0ADB4709A4BAC2D771A2AA

SHA-1: 82F4A11D554430B3BE8E5AB96D59639797B404A6

The email containing the subject line “Fw: New List” Contains an exchange to [James39933@outlook.com](mailto:James39933@outlook.com) from [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) on Sunday 11 April 2021 at 08:36 AM PST. In the exchange [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) forwards an email from [meowth55788@gmail.com](mailto:meowth55788@gmail.com) discussing selling accounts for $10 each. [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com) states to [James39933@outlook.com](mailto:James39933@outlook.com) “You know what to do. Don’t mess it up this time!” signing as Musashi.

Graphical user interface, text, application, email

Description automatically generated

20000066\_89191f22174adf.eml

MD5: 2DE9BDD5F838D65E1C7793D28AE8241B

SHA-1: F9A3A76DEF5E3E1F6139E37073B1D5954261E2A0

The emailed subjected “Get started on OneDrive for Windows” from [email@onedrive.com](mailto:email@onedrive.com) to [Jamese39933@outlook.com](mailto:Jamese39933@outlook.com) was delivered on Sunday 11 April 2021 at 08:29 AM PST. This email from [email@onedrive.com](mailto:email@onedrive.com) is typically delivered when the OneDrive service has been set up for the receivers email.

Graphical user interface, text, application

Description automatically generated

### Internet Artifacts

Google Chrome bookmarks

The following Google Chrome bookmarks were found

* <https://connect.secure.wellsfargo.com/auth/login/present>
* <https://secure.bankofamerica.com/login/sign-in/signONV2Screen.go>
* <https://privatebank.jpmorgan.com/gl/en/login>
* <https://www.unionbank.com/personal/digital-banking>

The associated bookmarks link to the online bank accounts suggesting frequent visits to these sites.

Firefox bookmarks

The following Firefox bookmark found

* <https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html>

The associated bookmarks link to a page discussing ways to access the deep and dark web[[8]](#footnote-8) and its contents.

Internet downloads

The following files were downloaded from the internet

* TunnelBear-Installer.exe
  + MD5: 8395BEF7D0E81FEEB343BF7C5A514776
  + SHA-1 8D92177FB17C3992DB04ADFCF3DD7CBC1AC163D3
* ProtonVPN\_win\_v1.18.5.exe
  + MD5: 4328C8ADD156AE46095B9DCA33124965
  + SHA-1 5619D8300AE539380E6E8F9BD162C4B1E2A758A3
* torbrowser-install-win64-10.0.15\_en-US.exe
  + MD5: DBAFD3E0277AC2FB835588CD5EC0F470
  + SBA-1: EDBC15F52F27CC009DD64185D9E096B9BD121239

All of these downloads appear to be application installers. The first two downloads appear to be for VPN services while the third appears to be a method for accessing the dark web. These are all methods for providing anonymity over the internet. These files were installed on the system indicating that the services were installed on the system.

Browser Cache

The browser cache suggests multiple visits to the following websites:

* protonvpn.com
* tunnelbear.com
* torproject.com
* wellsfargo.com
* jpmorgan.com
* bankofamerica.com
* unionbank.com
* chasecdn.com

These websites encompass online banking, VPNs and the dark web.

Browser Cookies

The browser cookies suggests multiple visits to the following websites:

* protonvpn.com
* tunnelbear.com
* torproject.com
* wellsfargo.com
* jpmorgan.com
* bankofamerica.com
* unionbank.com
* chasecdn.com
* Norton.com

These websites encompass online banking, VPNs, and the dark web.

Search Terms

The following search terms were found:

* “tunnelbear free”
* “protonvpn”
* “Where can I sell Bank accounts”
* “well fargo login”
* “bank of america login”
* “jp morgan login”
* “union bank login”
* “How to get on the dark web”

Activities suggest the user was looking for VPN providers and accessing bank logins. Further it appears the user was trying to discover well to sell bank accounts and moreover how to gain access to the dark web, a place where one could sell illegally obtained bank accounts.

### Recycle Bin

The recycle bin contained the file Motto.txt which was deleted on 2021-04-11 08:29:36 PST. Contents of the file are unknown.

### Target List 1.xlsx

MD5: 95F04B7311A29324CB2D72ED82ACB095

SHA-1: 88EF1E7EDB35E85DFC4D096D0E97BC0E164CBA29

Target List 1.xlsx contains a list of individuals along with their bank account credentials and account number. The file was created by “Meowth” (possibly referring to the affiliate of Team Rocket) on 11 April 2021 at 8:49:05 PST. The list includes the information about Genevieve Blevins and her Bank of America account.

Graphical user interface, application

Description automatically generated

### Executable Files

protonvpn.exe

MD5: 75A56C7B47FD08918C0E13B51927EF48

SHA-1: 129F1A65F531BD8513B9225031ECEF33A398F061

protonvpn.exe was found installed on the system. It was executed three times at 08:30:50, 08:47:09 and 8:59:00 PST on 11 April 2021. It appears the file allows the user to access the ProtonVPN service.

tor.exe

MD5: 4719BF403BCAFA7F8D0EF1B4093174D1

SHA-1: 5B4610CAC710514E3D8A10EA12472D50A813B94C

tor.exe was found installed on the system. It was executed once at 8:59:00 PST on 11 April 2021. It appears the file allows the user to access the dark web.

### USB Device Attached

One USB device was found attached to the system on 11 April 2021 at 8:25:29 PST. The device was an Alcor Micro Corp. flash drive with the device ID 06524F76. Contents and location of the USB device are unknown.

# Recommendations

Triple R recommends the following actions that could help further the investigation:

* Interview members of Team Rocket including Jessie, James and Meowth Rocket to discuss the content found on the laptop and their knowledge regarding the data found on the drive.
* Investigate the owner of [James39933@outlook.com](mailto:James39933@outlook.com), [Meowth55788@gmail.com](mailto:Meowth55788@gmail.com), and [Jessie11445@protonmail.com](mailto:Jessie11445@protonmail.com).
* Subpoena TunnelBear and ProtonVPN service providers for activities, logs, and usage on the laptop
* Subpoena the ISP provider of the gym and determine if the Bank of America login IP matches with the device at the time of logon.
* Subpoena the OneDrive of [James39933@outlook.com](mailto:James39933@outlook.com) to investigate any files located in the OneDrive.
* Develop a timeline of activity on the device along with the timeline of when the crime occurred. Time irregularities between activities occurring on the device and time of seizure need to be addressed.
* Locate and investigate the attached USB device and its contents.
* There is evidence to suggest Jessie, James, and Meowth Rocket as being creators of the illicit data on the laptop.

1. An Internet Protocol (IP) address is an alpha-numeric identifier associated with a device when connected to a network such as the internet. [↑](#footnote-ref-1)
2. A virtual private network (VPN) grants online privacy and anonymity by creating a private network through a public internet connection. The VPN masks your activities creating anonymity that is virtually untraceable. [↑](#footnote-ref-2)
3. The Onion Router (Tor) enables anonymous communication through the dark web. [↑](#footnote-ref-3)
4. A digital fingerprint generated using a one-way cryptographic algorithm. [↑](#footnote-ref-4)
5. MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value [↑](#footnote-ref-5)
6. SHA-1 is an acronym that stands for Secure Hash Algorithm 1. It produces a 160-bit hash value. [↑](#footnote-ref-6)
7. A security identifier (SID) is used to unique identify accounts on the Windows 10 Operating System. [↑](#footnote-ref-7)
8. The dark web provides anonymity to users and is commonly used to host illicit content. [↑](#footnote-ref-8)