# Important - How to Use this Report Template

For your engagement, this page would be **removed.**

Because this is a template report, this page stands to explain how to utilize the entire document. Before you go further, please read through this page so that you know how to use this document.

Below, you will find modules meant for various types of OSINT investigations as well as templates meant to keep certain OSINT documentation organized, like sock puppets.

This report template was designed in a modular way to allow the investigator to remove what is not necessary for their investigation.

For example, if you were doing research into a company for an external pentest, you may end up using:

* Website OSINT
* Email OSINT
* Password OSINT
* Etcetera

If you need further direction, please refer to the “Writing an OSINT Report” section of the TCM Security OSINT course.

A logo of a unicorn

Description automatically generated

A logo with a cross between the letters

Description automatically generated

Open-Source Intelligence (OSINT) Investigation

Table of Contents

[Important - How to Use this Report Template 1](#_Toc159368924)

[Confidentiality Statement 4](#_Toc159368925)

[Disclaimer 4](#_Toc159368926)

[Contact Information 4](#_Toc159368927)

[Assessment Overview 5](#_Toc159368928)

[Summary – Monarch Migration 6](#_Toc159368929)

[Technical Evidence – Reverse Image Search 7](#_Toc159368930)

[Technical Evidence – Google Search Operators 8](#_Toc159368931)

[Summary – Emotet Timeline 9](#_Toc159368932)

[Technical Evidence – Google Search Operators 10](#_Toc159368933)

[Technical Evidence – Research & Analysis 11](#_Toc159368934)

[Summary – Email Recon 13](#_Toc159368935)

[Technical Evidence – Google Search Operators 14](#_Toc159368936)

[Summary – Challenge 4 15](#_Toc159368937)

[Technical Evidence – XXX 16](#_Toc159368938)

# Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

This Open-Source Intelligence (OSINT) report has been compiled by TCM Security based on information available in the public domain as of [INSERT DATE HERE]. While efforts have been made to ensure the accuracy of the information, it is subject to change. An OSINT investigation is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

TCM Security assumes no responsibility for any decisions made or actions taken based on this report. The use of this information is at the reader's own risk, and TCMS disclaims any liability for inaccuracies or omissions. This report is confidential and not intended for public distribution.

# Contact Information

|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| DEMO CORP | | |
| Jane Smith | Chief Information Security Officer | jsmith@democorp.com |
| TCM Security | | |
| Heath Adams | Lead Penetration Tester | heath@tcm-sec.com |

# Assessment Overview

From [START DATE] to [END DATE], the OSINT Investigator conducted an Open-Source Intelligence (OSINT) assessment. The findings presented in this overview are derived from open-source data and do not involve any unauthorized access to private or confidential information. An OSINT risk assessment emulates the role of a threat actor employing methods like those utilized by malicious entities to gather information. Through data collection and analysis, an investigator will search open sources to identify potential risks, culminating in an assessment and profiling of discovered information.

This OSINT investigation aims to provide a realistic representation of the information landscape from a threat actor's perspective, enabling a proactive approach to strengthening organizational resilience.

Phases of the OSINT investigation include the following:

* Planning and Direction
* Collection
* Processing
* Analysis and Production
* Dissemination and Integration

A diagram of a process

Description automatically generated

# Summary – Monarch Migration

Objective

Geolocating this place may not be hard but the threatened arthropods that can be found in this place sure makes a hard migration every few generations.   
  
You should be able to find a few decorative posters that have been made to commemorate this mighty migration. In one poster, a specific interstate highway is mentioned. What is this interstate highway and how many states does it go through?   
  
Incredibly, scientists have able to identify a single member of this species with the longest travel. How many miles was the longest known individual migration identified by this species?

Key Findings

TCMS determined that the image provided was from the Great Smoky Mountains.

In reading the Great Smoky Mountains National Park Service website TCMS identified that the Monarch butterfly is the only endangered arthropod that can be found in the park that makes a long migration.

Through further research, it was identified that the Monarch butterfly is featured on a poster of the US Highway 35. This highway system goes through six (6) US states. Finally, the longest known individual migration was determined to be 2880 miles.

Photograph of Subject

A forest of trees in the mountains

Description automatically generated

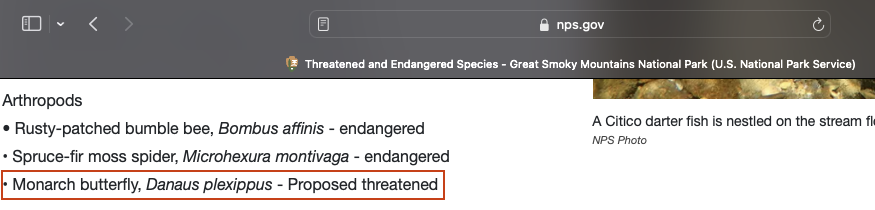
## Technical Evidence – Reverse Image Search

|  |  |
| --- | --- |
| OSINT: | Used Google Lens to reverse image search and Google search operators to identify the location and threatened arthropod. |
| Link(s): | * [https://www.nps.gov/grsm/learn/nature/te-species.htm](file:///Users/angb/Downloads/•%09https:/www.nps.gov/grsm/learn/nature/te-species.htm) * [https://www.fs.usda.gov/wildflowers/pollinators/Monarch\_Butterfly/migration/index.shtml](file:///Users/angb/Downloads/•%09https:/www.fs.usda.gov/wildflowers/pollinators/Monarch_Butterfly/migration/index.shtml) |
| Notes: | It was important to carefully focus on the mountain range to get a match to Great Smoky Mountains. The National Park website confirmed that the Monarch was on the threatened list. |

*A screenshot of a photo shop

Description automatically generated*

*Figure 1: Geolocation confirmed by Google Lens*

**

*Figure 2: Monarch identified as threatened arthropod*

## Technical Evidence – Google Search Operators

|  |  |
| --- | --- |
| OSINT: | Performed a google search for “monarch migration”, “monarch migration "highway poster"”, and finally “monarch migration longest trip recorded”. |
| Link(s): | * [https://www.fs.usda.gov/wildflowers/pollinators/Monarch\_Butterfly/migration/index.shtml](file:///Users/angb/Downloads/•%09https:/www.fs.usda.gov/wildflowers/pollinators/Monarch_Butterfly/migration/index.shtml) * [https://entnemdept.ufl.edu/walker/ufbir/chapters/chapter\_35.shtml#:~:text=Monarch%20Watch%20lists%20the%20longest,%2C%201989%20in%20Austin%2C%20Texas](file:///Users/angb/Downloads/•%09https:/entnemdept.ufl.edu/walker/ufbir/chapters/chapter_35.shtml#:~:text=Monarch%20Watch%20lists%20the%20longest,%2C%201989%20in%20Austin%2C%20Texas) |
| Notes: | At the bottom, the website section “The Monarch Highway Poster” provides details that the interstate highway is called I-35” and that it goes through six (6) US states. |

A close up of a sign

Description automatically generated

*Figure 1: Proof of Monarch migration*

*A screenshot of a computer screen

Description automatically generated*

*Figure 2: “The Monarch Highway Poster” detailing interstate highway information*

**

*Figure 3: Research paper documenting the longest recorded flight*

# Summary – Emotet Timeline

Objective

You are an intelligence analyst working for a cybersecurity firm. Your task is to investigate a series of cyber-attacks where Emotet was utilized, targeting financial institutions. The attacks have resulted in significant financial losses and reputation damage for the institution.

Your objective is to create a detailed timeline of these cyber-attacks based on open-source information.

After the timeline has been made, identify open-source intelligence sources such as cybersecurity blogs, research papers, threat intelligence reports, forums, and social media platforms for information related to Emotet campaigns to create a list of tactics, techniques, and procedures (TTPs) employed by the threat actors behind the campaigns in 2024.

Key Findings

**Initial Emergence (2014-2016):** Emotet first emerged as a banking trojan around 2014, primarily targeting financial institutions and users' banking credentials. It spread via malicious email attachments and infected systems to steal sensitive information.

**Evolution into a Malware Delivery Platform (2017-2018):** By 2017 and 2018, Emotet evolved into a sophisticated malware delivery platform capable of distributing other malware payloads, including ransomware and information stealers. It expanded its target base beyond financial institutions to include organizations across various sectors.

**Periodic Takedowns and Resurgences (2019-2020):** Throughout 2019 and 2020, law enforcement agencies, cybersecurity firms, and international partnerships conducted several takedowns of Emotet infrastructure, disrupting its operations temporarily. However, Emotet consistently resurfaced with new tactics and infrastructure.

**Global Impact and Notoriety (2019-2021):** Emotet gained notoriety as one of the most prolific and widespread malware threats globally during this period. Its modular architecture and polymorphic capabilities made it challenging to detect and mitigate, leading to significant financial losses and data breaches for affected organizations.

**Disruption Efforts and Arrests (2021-2023):** Law enforcement agencies intensified efforts to disrupt Emotet operations, resulting in multiple arrests of key individuals associated with the malware distribution network. These actions temporarily disrupted Emotet's infrastructure and reduced its prevalence in the threat landscape.

**Transition to Private Sector Control (2023):** In 2023, Emotet comes back online with a focus on the private sector.

## Technical Evidence – Google Search Operators

|  |  |
| --- | --- |
| OSINT: | Utilized “Search engine operators” to identify Emotet research done from each year. |
| Link(s): | 2014   * <https://thehackernews.com/2014/06/new-banking-malware-with-network.html>   2015   * <input link(s) here>   2017   * <input link(s) here>   2019   * <input link(s) here>   2021   * <https://www.justice.gov/file/1402226/download>   2023   * <input link(s) here> |
| Notes: | <Input notes from findings here> |

*Figure 1: Timeline of events based on the above research*

*<insert image here>*

*Figure 2: 2014 article detailing new malware*

## Technical Evidence – Research & Analysis

|  |  |
| --- | --- |
| OSINT: | Identified recent public Emotet samples, compiled a list of TTPs. |
| Link(s): | * <https://any.run/report/6393fe8dd4721190f240e22feeb769675b6194a70cabd5a415c2364686a9089c/4cc23eeb-9243-4314-b6ac-c782437d5d19> * <https://any.run/report/d50d98dcc8b7043cb5c38c3de36a2ad62b293704e3cf23b0cd7450174df53fee/ae225123-614a-4b35-9590-1016a38d5645> |
| Notes: | Recent samples of Emotet have been known to be capable of the following malicious activities:  **Delivery**  Emotet delivers malicious documents via phishing emails or other vectors.  **Execution**  It executes payloads using legitimate processes like WINWORD.EXE to blend in with normal activity.  **Persistence**  Emotet establishes persistence by modifying system settings, such as autorun values in the registry.  **Evasion**  It employs techniques like concealing program windows or using WMI to hide its presence from users and security solutions. |

A screenshot of a computer

Description automatically generated

*Figure 1: Malicious activity Identified from link 1 (emotet.exe)*

*A screenshot of a computer

Description automatically generated*

*Figure 2: Malicious activity Identified from link 2 (sample.bin)*

*A close-up of a message

Description automatically generated*

*Figure 3: Suspicious activity Identified from link 1 (emotet.exe*

*A screenshot of a computer program

Description automatically generated*

*Figure 3: Suspicious activity Identified from link 1 (emotet.exe)*

# Summary – Email Recon

Objective

Identify three (3) email accounts owned by Apple that have to do with security. Provide context about who owns them or what they are for.

In order to successfully complete this challenge, the email accounts need to be discovered on official Apple documentation.

Key Findings

All email accounts identified below were found on an Apple Support article titled “Recognize and avoid phishing messages, phony support calls, and other scams”.

Email Accounts

[reportphishing@apple.com](mailto:reportphishing@apple.com)

A place to report suspicious emails or SMS texts to Apple.

[reportfacetimefraud@apple.com](mailto:reportfacetimefraud@apple.com)

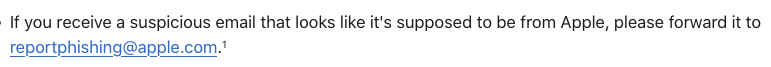
A place to report a suspicious FaceTime call or link to a FaceTime call in Messages or Mail.

[abuse@icloud.com](mailto:abuse@icloud.com)

A place to report iCloud email spam.

## Technical Evidence – Google Search Operators

|  |  |
| --- | --- |
| OSINT: | Searching “"@apple.com" email” identifies three cyber security focused email accounts in one official Apple support article. |
| Link(s): | * <https://support.apple.com/en-us/102568> |
| Notes: | N/A |



*Figure 1: Information identified about reportphishing@apple.com*

*A screenshot of a computer

Description automatically generated*

*Figure 2: Information identified about reportfacetimefraud@apple.com*

**

*Figure 3: Information identified about abuse@icloud.com*

# Summary – Challenge 4

Objective

<Input the objective here>

Key Findings

<Input key findings here>

Photograph of Subject

<input any photographs here or erase if unneeded>

Personal Information

<Name:

Date of Birth:

Phone number:

Address:

Erase if unneeded>

Usernames and Email

<input usernames here or erase if unneeded>

Location Information

<input location information here or erase if unneeded>

## Technical Evidence – XXX

|  |  |
| --- | --- |
| OSINT: | <Detail the OSINT performed to answer the challenge here> |
| Link(s): | * <input link(s) here> |
| Notes: | <Input notes from findings here> |

*Figure 1: XXX*

*Figure 2: XXX*

*Figure 3: XXX*