

Automated Threat Hunting for JavaScript-based Obfuscated Phishing Email Attachments

MSc Industrial Internship MSc Cyber Security

Saraunsh Shewale Student ID: X21215057

School of Computing National College of Ireland

Supervisor: Industry Mentor: Vikas Sahni Colm Gallagher

National College of Ireland Project Submission Sheet School of Computing



Student Name:	Saraunsh Shewale
Student ID:	X21215057
Programme:	MSc Cyber Security
Year:	2023-2024
Module:	MSc Industrial Internship
Supervisor:	Vikas Sahni
Submission Due Date:	05/01/2024
Project Title:	Automated Threat Hunting for JavaScript-based Obfuscated
	Phishing Email Attachments
Word Count:	729
Page Count:	15

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Saraunsh Shewale
Date:	29th January 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	
Attach a Moodle submission receipt of the online project submission, to	
each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both for	
your own reference and in case a project is lost or mislaid. It is not sufficient to keep	
a conv on computer	

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Automated Threat Hunting for JavaScript-based Obfuscated Phishing Email Attachments

Saraunsh Shewale X21215057

1 Introduction

This configuration manual details a step-by-step guide to successfully install and set up all required project dependencies to host an automated phishing analysis workflow. The project is configured on a **cloud-based SaaS service** known as **Tines**¹. It allows the execution of customized automated workflows and generates the output in the form of events. These events appear in JSON notation and can be further parsed according to one's requirements. Parsed output can be delivered through email to a single or list of email recipients.

2 Prerequisites

This project requires the following dependencies to satisfy the pre-requisites criterion for successful installation and execution.

- 1. A free or paid account subscription to Tines (Smart, secure workflows).
- 2. API Key for VirusTotal²
- 3. API Key for URLScan.io³
- 4. API Key for EmailRep.io⁴
- 5. API Key for $OpenAI^5$
- 6. Install Firefox (Version used 121.0)
 - OR

Chrome Web Browser (Version used - 120.0.6099.130)

¹https://www.tines.com

 $^{^{2}} https://www.virustotal.com/gui/join-us$

³https://urlscan.io/user/signup

⁴https://emailrep.io/free

⁵https://platform.openai.com/signup

3 Sign Up for Tines

- 1. Create a free account on Tines (Smart, secure workflows).
- 2. Enter the required information and proceed.
- 3. Once signed up successfully, a unique sign-in link will be shared to the registered email address. Click on the link to verify the account.

🖨 tines		Light Mode 🛞
	Welcome to Tines	
	By continuing you agree to the terms of service and privacy policy.	
	G Sign up with Google	
	Sign up with email	
	Trusted by the world's leading security teams	
OCIRCLE Canva 0	coinbase 😂 databricks 🕀 GitLab M£KESSON	• OpenTable: 🐨 reddit

Figure 1: Tines - Account Sign Up

🖨 tines	
	We just need a few details
	First name
	Last name
	Company
	Next →

Figure 2: Tines - Provide Required Information



Figure 3: Tines - Verify Email Address

Tines sign in link Inbox ×				¢	
Tines Support <support@tines.io> to me ▼</support@tines.io>		22:44 (O minutes ago)	☆	¢	:
	🖨 tines				
	Sign in to Tines 🖊				
	Click the button below to sign in to Tines.				
	Sign in				

Figure 4: Tines - Account Confirmation

4. After signing in, Tines will redirect the user to the story dashboard.

Saraunsh Shewale	Your first team > Stories	Import + New story
Q Search Ctrl K	iou nist team / stores	e import
Reporting	Q Frank	D Tara Z Silva Z
③ Recent	Q SeefCh	Viags - Pilter U
♡ Favorites		
 Your drafts 	Simple story 8 actions • Edited -2h ago	
Your teams		
 Your first team 		
> 🔒 Stories		
> 🔿 Credentials		
> Resources		
+ Create new team		

Figure 5: Tines - Story Dashboard

4 Setting up API Keys

4.1 VirusTotal

- 1. Sign up for a free account on VirusTotal and verify the email address.
- 2. Go to the Profile section and click on the API key. Save the Key in a safe place as it will be imported at a later stage.

Σ	URL, IP address, domain, or file hash	Q 🛧 🏭 🏸 🕲 Saraunsh Shewale
	API Key	Request premium API key
	АРІ Кеу: ******* () []	This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submissions with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submissions. Learn more
	API quota allowances for your user	Upgrade API
	You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to VirusTotal premium services. You are subjected to the following limitations:	
	Access level A Limited, standard free public API Upgrade to premium Usage Must not be used in business workflows, commercial products or services.	() () () () () () () () () () () () () (
	Request rate 4 lookups / min Daily quota 500 lookups / day	API reference Python client Golang library Command-line interface
	Monthly quota 15.5 K lookups / month Want to learn more about how VirusTotal can supercharge your security operations? check our 36	
	overview brief.	Go premium Use in browser Discover feeds Other services

Figure 6: VirusTotal - API Key

4.2 URLScan.io

- 1. Sign up for a free account on URLScan.io
- 2. Navigate to Settings & API, and create a new API key with a relevant description.

Q Recent Scans	Security Change Pas Two-Factor Authentication (2FA)	sword © 2FA is not enabled □ Enable 2FA						
Active User Saraunsh Shewale ^{⊚2FA Disabled}	API Keys API documentation						+c	reate new API key
Last login 3 minutes ago	You currently have an A	ctive Team. Any new scan you j	perform via the L Public	JI or API will Unlisted	be visible to Private	o membe Total	ers of that team. Last Submit	
	Key: e88b3626- Comment: Tines-URLScan	io	0	0	0	0	Never	O Disable

Figure 7: URLScan.io - API Key

4.3 EmailRep.io

- 1. Request a free or commercial API key from the EmailRep.io support team. (Free plan provides 10 requests/day and the commercial plan has no daily limits.)
- 2. An API key will be sent to the requested email address in 48 hours.

Ĉ		DOCS	API KEY CONTACT LOGIN 💆 🎧
	Requ	uest a free API	Key
		Yes, we said free	
	Community Full API response	Commercial Full API response	Enterprise For high-volume or throughput
	Free	\$20/month	Custom depending on your needs
	250 queries per month up to 10 queries/day	1000 queries per month no daily limit email support	high-volume API available no daily limit support with SLA
	Request	Select	Contact Us

Figure 8: EmailRep.io - API Rate Limits

ê		DOCS	API KEY	CONTACT	LOGIN	У	0
	Community /	AP					
	Request your free API key be	elow					
	Your full name						
	Your email address						
	I'm not a robot	CAPTCHA acy - Terms					
	REQUEST						

Figure 9: EmailRep.io - Request API Key

4.4 OpenAI API

1. Sign up for an account on $OpenAI^6$ and verify the email address.

Create your account			
Continue			
Already have an account? Log in			
G Continue with Google			
Continue with Microsoft Account			
Continue with Apple			

Figure 10: OpenAI - Sign Up

- 2. Once logged in to the account, navigate to API Keys and add the phone number to be able to create an API key.
- 3. Once verified, create a new secret key and provide a relevant name.

\$	API keys				
Playground Assistants	Your secret API keys after you generate th	are listed below. Please n nem.	ote that we do not display y	your secret API key	/s again
Fine-tuning	Do not share your Af protect the security	PI key with others, or expo of your account, OpenAI n	se it in the browser or othe nay also automatically disa	r client-side code. ble any API key tha	In order to at we've
Files	found has leaked pu	blicly.	CREATED	LAST USED ①	
OsageSettings	JS-DeObfuscator	sk18Iz	Dec 7, 2023	Dec 7, 2023	C
	+ Create new secre	t key			



⁶https://platform.openai.com/signup

5 Import Phishing Analysis Workflow

- 1. Log in to the Tines account with valid user credentials.
- 2. Navigate to Stories under Your First Team.

Saraunsh Shewale	Verin first team of Charles	
Q Search Ctrl K	Your first team > Stories	Import + New story
曲 Reporting	0 Sayah	Tags - Filter - 0
() Recent		
♡ Favorites		
 Your drafts Your teams 	Simple story 8 actions • Edited -2h ago	
 Your first team 		
> 🛛 Stories	0	
> 🔿 Credentials		
>		
+ Create new team +		

Figure 12: Tines - Story Dashboard

3. Click on the Import button and select the project JSON file (i.e., phishing-analysisautomated-work-flow.json)

Your draft	s > Stories	Import + New story
Q Sean	Import a story Story files contain all actions and their sources/receivers. These files do not contain any of the event data.	ি Tags 〒 Filter য় o
n i	 phishing-analysis-automated-work-flow.json 回 Rename to: 	5
N	Phishing Analysis Automated Work Flow Import as a new story	
	Import	

Figure 13: Tines - Import Story

4. After successful import, the user will be redirected to the story workflow where phishing email analysis takes place.



Figure 14: Tines - Story Workflow

6 Importing API Keys

The provisioned API keys must be imported into the Tines platform to allow HTTP request components to access them. To do that, follow the below steps for each of the API keys.

- 1. Navigate to the Credentials tab from the left sidebar.
- 2. Click on New Credential and select Text.
- 3. Provide a relevant name for the API key and description if needed as shown in figure 15
- 4. Copy the generated API key from section 4 and paste it into the Value field.

S	Saraunsh Shewale	Q					
	, I		١	Details Test details Actions	đ		+ New credential
ι α	Search	Ctrl K				*	
1	Reporting			Name			
0	Recent			EmailRep.io			÷ Filter ÷↓ 0
\heartsuit	Favorites		-	Description			
~	Your drafts			EmailRep.io API key			
	G Stories						
	O Credentials						
	Resources			Value			
	Archived stories		(

Figure 15: Tines - Import API Key

- 5. Click on save and the API key will be imported successfully.
- 6. Follow the same steps for each of the API services.



Figure 16: Tines - All API Keys Imported

7 Email Analysis

To initiate the analysis process for suspicious emails, follow the below steps -

1. Navigate to the imported analysis workflow by clicking on the story name under Stories.



Figure 17: Tines - Imported Story

2. Click on Receive Email Action from the storyboard and copy the email address from the right sidebar as highlighted in figure 18.

- 3. Now forward any suspicious email to the Tines email address for analysis.
- 4. A detailed analysis report will be sent to the email forwarder in 100 seconds.

Your drafts / 👔	Phishing Analysis Automated Work Flow 🛛 🗸	S Q Q Publish :
		Build Status Logs
· · · · · · · · · · · · · · · · · · ·		Until you publish this story, emails can only be received while you're working on it.
		Name
		Receive Email
		Description ~
· · · · · · · · · · · · · · · · · · ·		Mode
Webhook Analyze Em	ail Receive Email	email v
	▷ Run 🛱 Test ① Events 🗁 🔽 🗊 🗄	Email address
Event Transfor	Event Transform	
Parse EML	Parse EML	<> Editor

Figure 18: Tines - Receive Email Action

Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Saraunsh Shewale	Student number:	x21215057
Company:	CommSec	Month Commencing:	October 2023

This month was spent mostly researching existing literature on threat intelligence, specifically regarding phishing email analysis. Multiple research papers were analysed along with an exploration of various existing open-source projects.

The research methodology was determined for the project development along with the selection of an incremental model of SDLC.

Monitored and escalated alarms as a part of regular security operations (SOC) within the company's defined responsibilities to secure the client's infrastructure.

Employer comments

Student Signature:	Date: 02/01/2024	
Industry Supervisor Signature:	David McNamara Date: 02/01/2024	

MSc Internship Handbook, School of Computing, National College of Ireland.

Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Saraunsh Shewale	Student number:	x21215057
Company:	CommSec	Month Commencing:	November 2023

A cloud-based SaaS service - Tines was selected to build automated workflows for phishing email analysis. Also, various online threat intel services were determined and API keys for the same have been provisioned.

Automated workflow for email analysis is designed to cater the email analysis requirements. Integrated IP/URL analysis, and email address analysis checks in the workflow along with static analysis checks using regex.

Performed web application and network pentest for the company's clients as a part of role responsibilities.

Employer comments

	1	
Student Signature:	June	Date: 02/01/2024
Industry Supervisor Signatu	Ire: David Mc	Namara _{Date:} <u>02/01/2024</u>

MSc Internship Handbook, School of Computing, National College of Ireland.

Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Saraunsh Shewale	Student number:	x21215057
Company:	CommSec	Month Commencing:	December 2023

The automated analysis workflow was evaluated by testing some sample phishing emails. The outcomes resulted in successful extraction of all associated IOCs from suspicious email.

Along with that regular role responsibilites including SOC operations and web application pentests were performed.

Following security certifications were obtained during internship tenure:

- 1. Junior Penetration Tester (eJPTv2)
- 2. CompTIA Security+
- 3. Tines Certified

Employer comments

Saranush proved himself to be a keen learner with his time with us and was very diligent,	
with a pleasant demeanour.	

	m		
Student Signature:	50	Date:	02/01/2024
Industry Supervisor	Signature:	David McNamara Date:	02/01/2024

MSc Internship Handbook, School of Computing, National College of Ireland.