Virtual Humint

Countering Fraud with Test Purchase Operation

WHAT IS 'VIRTUAL HUMINT'?

Collecting intelligence in the virtual cyber world by humans: Cyberint's intelligence analysts proactively engage with threat actors on their own channels in order to gather additional information as part of deep dive Investigations, and provide the context required to mitigate a threat in the most effective way.

WHAT'S THE VALUE?

- Identifying a threat is imminent and real
- Obtaining the threat vector, the tools, tactics and procedures (TTPs), threat actor's motivation and the web of accomplices – whether insiders, other threat actors, or 3rd party vendors who have been unknowingly compromised to be the channel into an organization's network
- Gathering additional indicators of compromise (IOCs) to further investigate and correlate additional accounts or compromised data with the specific threat in focus

Cyberint

USE CASE: VIRTUAL HUMINT IN ECOMMERCE

FRAUDULENT ACTIVITY ABUSING ECOMMERCE REFUND POLICY

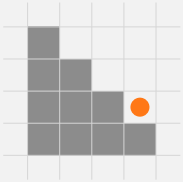
Customer Profile

Large global retail marketplace selling products from over 500 brands.

Fraudulent Refund Service and Its Potential Impact

Fraudulent refund service is an activity where threat actors are defrauding a retail store via their return processes. Taking advantage of company refund policies in order to obtain goods or monetary payback from online retailersdoesn't necessarily require any special technical capability or hacking skills. As a result, such cybercrime activity is has been detected all over the globe by multiple threat actors. The impact of such fraudulent activity is direct revenue loss to the retailer, manipulate the inventory management process, and if publicized can indirectly damage the retailer's brand reputation.

BUSINESS IMPACT



Revenue Loss

Inventory Management Manipulation

CYBERINT APPROACH TO ONLINE FRAUD

Leveraging its threat intelligence suite, expertise and, investigation with Virtual Humint services, Cyberint provides full visibility into the threat actors' malicious activities targeting specific brands and industries to execute fraudulent activity by manipulating the refund policy.

RTO MITIGATION ACTIONS (“REFUND TEST OPERATION”)

VALIDATING THE ‘REFUND AS A SERVICE’ FRAUDULENT THREAT:

In Summer 2019 Cyberint encountered multiple posts on dark web fraud forums by a threat actor, claiming to have successfully performed a fraudulent refund from one of the largest European retailers.

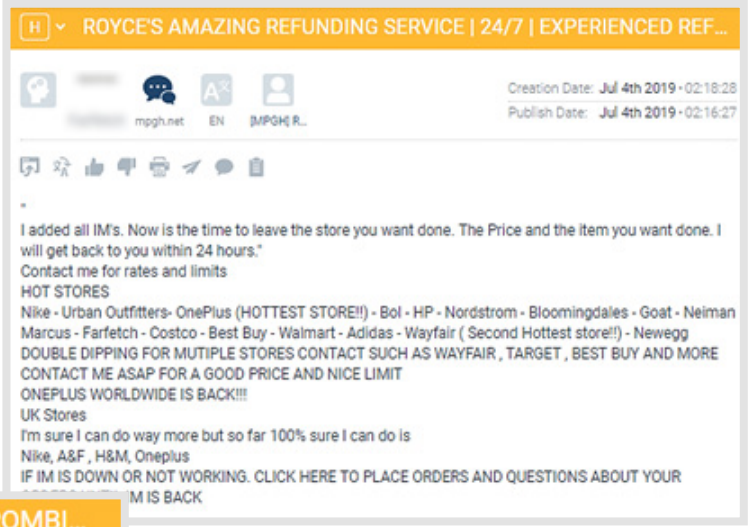


Figure 1 Threat actor post

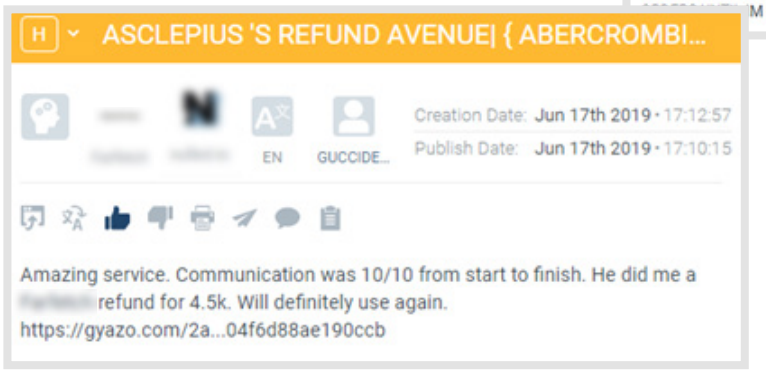


Figure 2: Threat actor's customer post

After alerting the affected retailer, Cyberint suggested to start a Virtual Humint operation, including performing a test purchase to uncover the threat actor's methodology and verify the IOCs involved in those activities.

Phase 1 | **Pre-Engagement**

- Initial analysis of the information on the threat actor (username, other means of communications and profile pages, origin, contact information, earlier posts and messages)
- Creating a legit profile on an isolated machine for further interaction - trustworthy (with profile history, images, movie and browser history, etc.

Phase 2 | **Interacting with a Threat Actor**

- Cyberint team communicating with a Threat Actor eventually requesting to obtain his services.
- Discovering details of the refund fraud methods applied

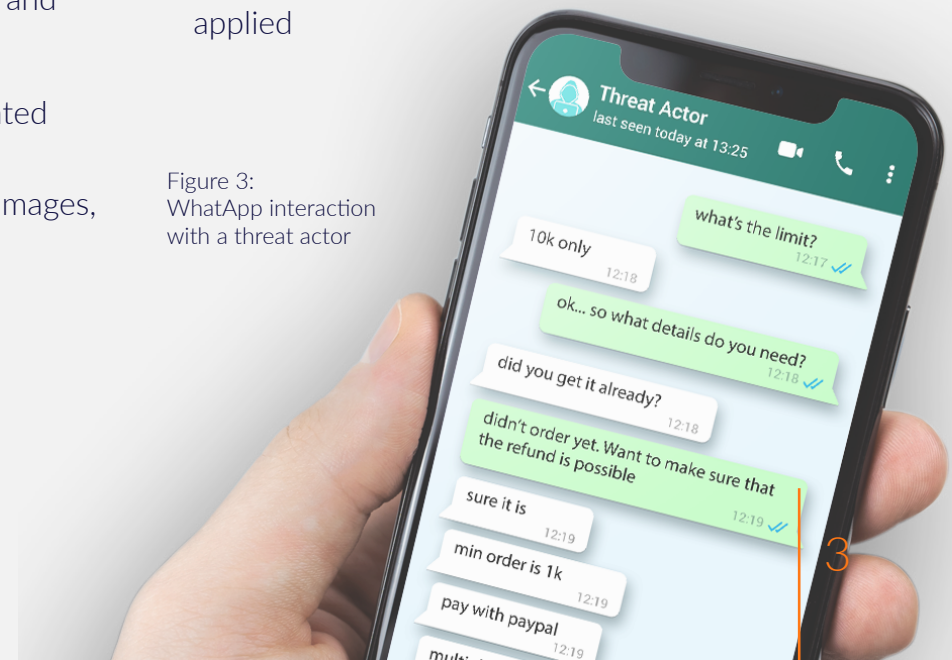


Figure 3:
WhatApp interaction with a threat actor

Cyberint

Phase 3 | **Performing The Test Purchase**

- Cyberint team making a test purchase, according to the Threat Actor instructions
- Alignment with a threat actor on the guidance to submit a legit-looking refund claim.

1. Cyberint Analyst uses a credible avatar as their online profile
2. The analyst opens an account on the retailer's website and orders a product
3. The analyst communicates with the threat actor
4. Cyberint shares the intelligence to decide on next steps of mitigation

Fraudulent threat mitigation

- Threat actor's methodology was uncovered and neutralized with suspicious IPs being blocked and alerted
- Following Cyberint's report, retailer reviewed rules transaction authorization for against similar fraud activities
- Obtained IOCs were highlighted on internal systems to identify other accounts involved in fraudulent activities
- Retailer reduced refund scam by 90% within 1-year engagement

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
Tel:+1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL
Tel:+972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM
Tel:+44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE
Tel:+65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM
Tel:+507-395-1553
Panama City