Large U.S. Retailer's in-house CTI Program

Boosted with Best-in-class Managed Intelligence Suite

Cyberint

Cyberint helped a large U.S. retailer enhance its Cyber Threat Intelligence (CTI) capabilities, utilizing its unique combination of expert cyber analysts, and Argos™, our proprietary threat intelligence platform.

Closely working with the in-house CTI team, Cyberint enabled the Retailer to identify emerging threats, investigate, contextualize, and prioritize alerts, and ultimately act upon the intelligence to effectively mitigate cyber threats.

CUSTOMER PROFILE

A Fortune 100 U.S. retailer, specializing in home improvement goods, was running a Cyber Threat Intelligence (CTI) program based on a commercial CTI platform, operated by an in-house dedicated Threat Intelligence (TI) team.

> **The biggest inhibitor is the lack of trained staff and skills associated with fully utilizing CTI.**
>
> 2020 SANS Cyber Threat Intelligence Survey

OVERVIEW

Organizations face many challenges while establishing an effective Cyber Threat Intelligence (CTI) Program. According to the 2020 SANS CTI Survey, the biggest inhibitor is the lack of trained staff and skills associated with fully utilizing CTI. Other inhibitors include lack of time to implement TI processes, lack of technical capabilities to integrate CTI tools, and lack of confidence in using the information to make decisions.

Recognizing these challenges, the Retailer sought to collaborate with a partner who would complement its CTI capabilities with a team of trained TI analyst experts, leveraging a powerful CTI platform.

> **Cyberint's high-touch partnership provided the Retailer with enriched, contextualized threat intelligence, while also eliminating noise and false positives. These strengths allowed the Retailer to gain increased operational efficiency while minimizing digital risks.**

Cyberint is ideally positioned to offer intelligence that focuses on the retail sector's threat landscape.

Based on its extensive experience, Cyberint was chosen to provide the Retailer managed TI services. The partnership focused on securing the digital journey across various channels, touchpoints, and third-party systems, against prominent risks such as fraud and privacy breach. Argos™, modular platform and flexible managed service model allowed the Retailer to customize the service offering to answer its own business and operational needs.

Cyberint's high-touch partnership provided the Retailer with enriched, contextualized threat intelligence, while also eliminating noise and false positives. These allowed the Retailer to focus its efforts and gain increased operational efficiency while minimizing digital risks.

CHALLENGES | BREAKING THE BARRIERS TO AN EFFECTIVE CTI PROGRAM

“CTI PROGRAMS REQUIRE THE RIGHT PEOPLE AND THE RIGHT TOOLS”

2020 SANS Cyber Threat Intelligence Survey

Effective CTI is based on a combination of the right technology to bring the raw intelligence and the right people to make it actionable. Trained TI analysts, who are familiar with the business specific needs, on one hand, and the threat actors’ scene, on the other, are key competency in the organization’s ability to conduct effective investigations and provide the 5WHs[1] that connect the dots and provide the “big picture”, and facilitate decision making.

To be effective, a CTI program requires both tools and skills—the infrastructure to automatically monitor and analyze intelligence sources; and the skills to investigate and contextualize.

The combination of a well-trained and experienced cyber analyst team armed with the right TI platform augments a CTI program’s effectiveness in several aspects:

Proactively detect threats with automatic and virtual human intelligence[2]

Provide the ability to communicate directly with threat actors, attribute their activity to specific campaigns and gain more context and intelligence

Create the context and required data for identifying the severity of threats and understanding the “big picture”

Allow effective responses by better prioritizing and focusing on the most important threats

Recommend and remediate threats, as necessary

[1] The “Five W’s” (Who, What, When, Why and How) are the basic elements of intelligence investigation and are key for providing contextualization.
[2] Virtual Human Intelligence (HUMINT) refers to 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.

USE CASE | EFFECTIVELY MITIGATING MULTIPLE PHISHING SITE THREATS

Phishing campaigns are prominent across the retail sector. Many retailers are targeted daily by phishing campaigns, orchestrated by cybercriminals. Cyberint detected dozens of potential phishing sites targeting the Retailer, thanks to its technology, which enables faster detection of duplicated sites.

Acting upon phishing alerts involves multiple activities, from verifying false-positives, to DNS/site-takedowns, and in some cases, involving the authorities. These efforts are costly and labor-intensive. Therefore, they need to be prioritized based on the threat level they present to the business. The threat level is derived from the threat actor's motivation, capabilities, opportunity, and impact.

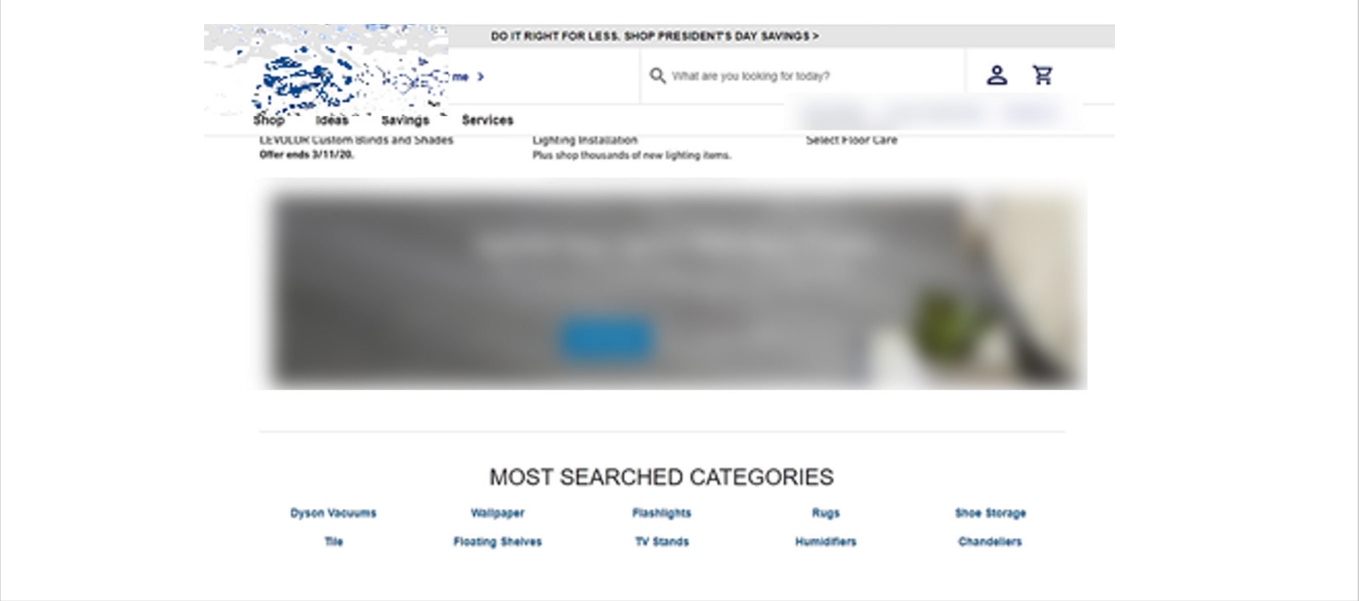
> Acting upon phishing alerts involves multiple activities, from verifying false positives, to site-takedowns, sometimes involving authorities. These efforts are costly and labor-intensive

That is where Cyberint's expertise comes into play; Based on code similarities and inserted scripts, Cyberint discovered that the phishing sites were created by an automated tool used by the same threat actor from Asia.

Following further investigations, Cyberint found that only a few of the phishing sites were actually weaponized to gather and dispatch credentials: the other sites were used for SEO purposes and appeared to remain dormant, rather than being part of an active phishing campaign.

IMPACT

Cyberint's investigation and analysis allowed the Retailer to prioritize and initiate adequate mitigation procedures. Where required, Cyberint provides end-to-end take-down services for phishing sites and domains.



Argos™ Detection of potential phishing websites

USE CASE | HANDLING CUSTOMERS' CREDENTIAL LEAKS

Leaked credential dumps make the news every month. Each credential leak seems to be larger than the last one. Timely identification of leaked credentials and swiftly acting to mitigate the impact, are one of the main tasks of security and intelligence teams.

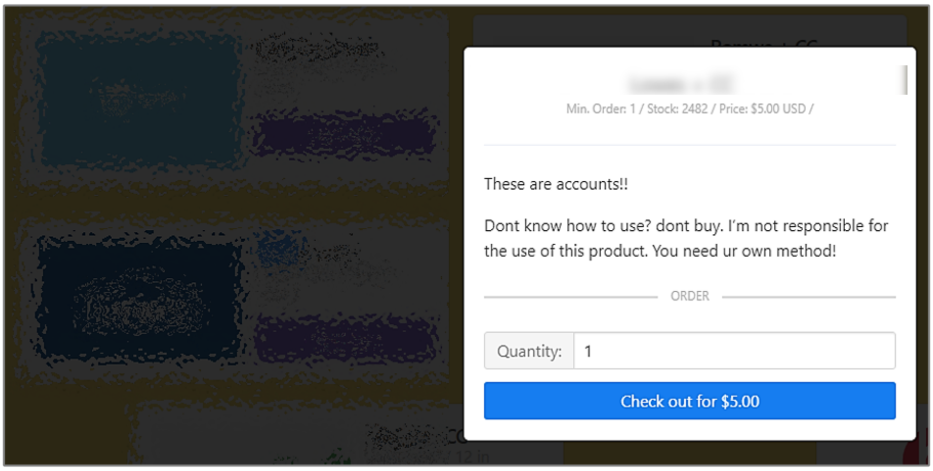
To provide timely identification of credential leaks, Cyberint employs different measures such as monitoring dark web forums and C2 malware repositories. Leveraging its in-house technology, Cyberint detected that thousands of the Retailer's customer credentials appeared on a darknet file sharing repository. The same information was shared on several dark web forums and was acknowledged by several members of these forums. Cyberint obtained the list of credentials and provided it to the Retailer, who confirmed that the credentials were valid, and then acted promptly to reset their credentials and verify that they were not misused.

Understanding the root cause enabled the Retailer to focus on effective measures to minimize the impact of the leak and mitigate the threat of credential stuffing

To identify the source of the leak, i.e. how the information was obtained by the threat actor, Cyberint compared user samples of the list against past data breaches. The investigation showed that the customers were victims of past breaches. Based on Cyberint's knowledge of the retail sector threat-actors' Tactics, Techniques and Procedures (TTPs), the analysts team assumed that the credentials were obtained through a credential stuffing attack (using an automatic tool checking of "combo-lists" of breached credentials) rather than a direct file or database leak. Further investigation, leveraging Cyberint virtual HUMINT capabilities, established a confirmation from the threat actor that the credentials were indeed "harvested" through a credential stuffing attack.

IMPACT

Cyberint discovered who pasted the credentials on the dark web, who stood behind the leak and how the credentials were obtained. Thanks to vast domain expertise, Cyberint helped improve the Retailer's defense mechanisms and reduced exposure to future credential stuffing attacks, and consequently, to legal and regulatory risks.



[redacted]

Min. Order: 1 / Stock: 2482 / Price: $5.00 USD /

These are accounts!!

Dont know how to use? dont buy. I'm not responsible for the use of this product. You need ur own method!

Quantity: 1

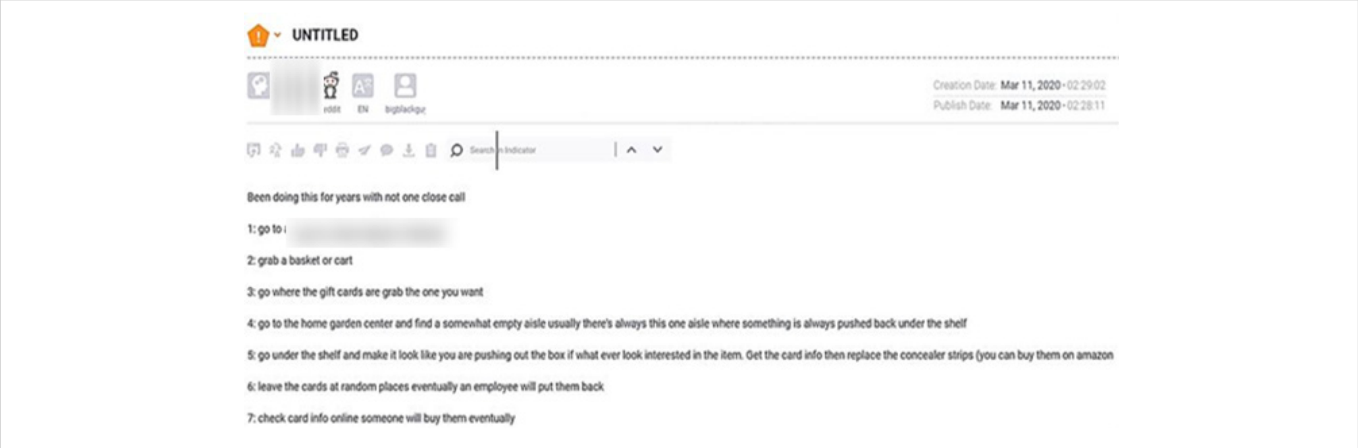
Argos™ Detection - Accounts offered for sale on threat actor's marketplace

USE CASE | THWARTING GIFT CARD CLONING SCHEME

Cyberint's deep intelligence capabilities focus on threats to digital business. Leveraging its familiarity with retail-specific threats, Cyberint uncovered a gift-card cloning scheme. Cyberint analysts exposed the details of the method by which the threat actor obtained and abused the Retailer's gift-card. The scheme was reported to the Retailer and measures were taken to frustrate that method of fraud.

To better understand the exposure, Cyberint employed virtual HUMINT to engage the threat actor and created a full profile of the threat actor. The investigation revealed a U.S. based threat actor who was actively engaged in the illegal gift-card market for some time. Cyberint's team identified that the threat actor operates an invitaion-only online underground store, where among others, more stolen Retailer's gift cards were traded.

Cyberint's team tracked down and conversed with the threat actor who admitted to selling the stolen customer gift card details



UNTITLED
[redacted]
reddit
EN
bigblackguy
Creation Date Mar 11, 2020 - 02:29:02
Publish Date Mar 11, 2020 - 02:28:11
Search in Indicator

Been doing this for years with not one close call

1: go to [redacted]

2: grab a basket or cart

3: go where the gift cards are grab the one you want

4: go to the home garden center and find a somewhat empty aisle usually there's always this one aisle where something is always pushed back under the shelf

5: go under the shelf and make it look like you are pushing out the box if what ever look interested in the item. Get the card info then replace the concealer strips (you can buy them on amazon

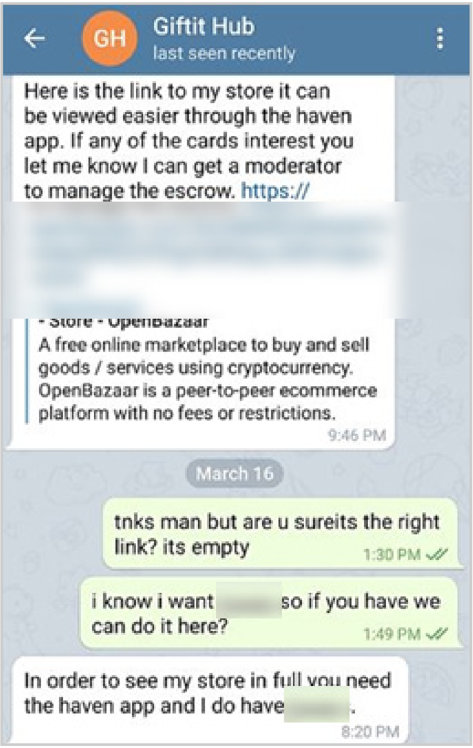
6: leave the cards at random places eventually an employee will put them back

7: check card info online someone will buy them eventually

Argos^{TM} Detection - Gift card methodology revealed on a public forum

IMPACT

By providing full details of the scheme, Cyberint helped the Retailer identify the weakness that was exploited by the threat actor. Consequently, it prevented further fraudulent activities using its gift cards, and minimized revenue loss. This was possible by utilizing its database of entities, threat actors and attribution to maximize context. After identifying the threat actor's online marketplace, Cyberint was able to continuously monitor the threat actor's activities to ensure that no new scheme was underway.



Here is the link to my store it can be viewed easier through the haven app. If any of the cards interest you let me know I can get a moderator to manage the escrow. https://

[redacted]

- Store - OpenBazaar
A free online marketplace to buy and sell goods / services using cryptocurrency. OpenBazaar is a peer-to-peer ecommerce platform with no fees or restrictions.
9:46 PM

March 16

tnks man but are u sureits the right link? its empty
1:30 PM

i know i want [redacted] so if you have we can do it here?
1:49 PM

In order to see my store in full you need the haven app and I do have [redacted].
8:20 PM

Invitation to join online marketplace – threat actor publishing their method on social media

Cyberint

ABOUT CYBERINT

Cyberint is a global TI provider focusing on helping its clients to proactively protect their business against cyber threats. As a partner to businesses worldwide, Cyberint' provides organizations with a unique combination of a market-proven technology and expert cyber analysts. This combination enables effective CTI program while reducing organizations' TCO. We serve more than 100 brands worldwide across industries as diverse as financial services, retail, gaming, entertainment, and media.

If you are a retailer looking for a Threat Intelligence platform to strengthen your CTI solution with a managed service, **contact us**

CONTACT INFORMATION

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

USA

214 W 29th St.
New York, 10001
Tel: +1-646-568-7813

Israel

17 Ha-Mefalsim St.
4951447 Petah Tikva
Tel: +972-37-286-777

United Kingdom

14 Grays Inn Rd, Holborn
WC1X 8HN, London
Tel: +44-203-514-1515

Singapore

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

Latin America

Panama City
Tel: +507-6255-8074