OSINT Crew

Open-Source Threat Intelligence

Autumn Report

By

Jeanette Fremmergård, Travis Clark,

Espen Ringstad and Selin Iren Aydin

In

Studio 2

UC2ST2103

Submission: 21/12/2020

Word Count: 3006

Introduction

The retail industry is vulnerable in many different ways. With the introduction of technology, these vectors of vulnerability have only increased. A top priority in the past was physical security, which has shifted to include cybersecurity. Online sales through the internet have opened the doors for new attacks. Threat Intelligence, both physical and cyber, can be a vital tool for combating theft and fraud. Threat Intelligence comes in many forms and price levels. Do retail businesses need to purchase Threat Intelligence services, or are the available open-source tools good enough to provide value?

This Report will focus on four areas where Threat Intelligence analysis could be of particular importance to the retail industry. These areas are general risks within the retail industry, social media, cyber-, and physical Threat Intelligence.

The general risks for the retail industry

The retail industry is fifth on the list of most frequently compromised industries, according to the 2018 report of the cost of data breach study (Recorded Future Team, 2019). This industry needs to protect its properties and data from criminal groups who aim to steal and manipulate confidential data for commercial gain. It is also essential for the industry to protect their store, systems, networks, people, and consumer and their information from being abused (The Echosec Team, 2019).

Statistics show that crime in the retail industry can cost retailers around 30 billion dollars every year. Criminals work hard to steal credit card data and other valuable assets and sell them on the black market (Insights Defend Forward, 2019). Personal information can also be leaked through the dark web. Criminals will use these credit cards to buy whatever they want before drawing attention from the banks, and the credit cards are deactivated. The lack of security is one of the significant issues for the retail industry, and studies have shown that only 53 percent of US retailers have invested in better security. In comparison, still, 10 percent have not made any changes (BDO, 2019). The retail industry in the US is looking forward to getting a similar GDPR regulation like Europe. They are trying to catch up to criminals and implement necessary security protocols to minimize the risk of crime against their stores and financial damage (Intsights Defend Forward, 2019).

Threat Intelligence can help retail businesses detect vulnerabilities that are deliberately exploited to be resolved immediately (Recorded Future Team, 2019). Intelligence gathering on controlled threats can provide insight into the background in which security professionals will need to protect sensitive assets and systems appropriately. This means understanding the industry's unique threats, who is behind them, and what their motives are (Cyber Proof, n.d.). Before threats occur, information helps companies protect themselves against established and emerging threats. This information can be gathered through the use of public sources or with the assistance of paid Threat Intelligence providers. There would be a significant amount of information to analyze, which can be overwhelming for companies (Cyber Proof, n.d.). With a large volume of data, the most critical threats can be hard to identify, and the most relevant threat information should, for that reason, be analyzed to prevent accidents from occurring. This is where the companies might decide to use a third party to examine the significant amount of

data so that they do not miss anything relevant to the company and their future. Threat intelligence can also be used to help the retail companies address their weaknesses when it comes to their security and how they can fix it to reduce attacks. To be one step ahead can also prevent the companies from having a financial loss and damaging downtime. Threat Intelligence can prevent companies from being exploited for a confidential data breach, which will protect the company, its reputation, and its customers.

Cyber Threat Intelligence

The Retail Industry has no shortage of threats. Cyber threats have only increased in the last decade. Network attacks, credit card compromises, point of sale attacks are only a few of the types of cyber-attacks the retail industry is dealing with. Cyber Threat Intelligence plays a growing role in how the Retail Industry is trying to stay ahead of the attackers.

To address their clients' growing needs, Deloitte LLP put together its first Retail Cyber Risk Leadership Forum in 2015. Allison Kenney Paul VC and US Retail & Distribution Leader of Deloitte LLP opened the forum with this remark "Despite heightened attention and unprecedented levels of security investment, the number of cyber incidents and their associated costs continues to go up. No retail or distribution organization is immune." (Deloitte, 2015). During this same period, Deloitte also conducted research on the current state of retailers' cyber risk and security programs, 40 organizations participated. Combining the data from the survey and the Leadership Forum, Deloitte produced a report in 2015, "Cyber risk in retail. Protecting the retail business to secure tomorrow's growth."

Some of the key takeaways from the Report include:

- "Compliance does not always equal risk management
- Breach response readiness is top-of-mind as companies scramble to shore up detection
- External Intelligence will play a crucial role in the war against cyber threats
- Cyber risk is a business issue. " (Deloitte, 2015).

The survey concluded with some numbers to show if the organizations were taking the risks seriously or not. A surprising 20% admitted to having no incident response plan. Only 23% of the organizations that had a plan ever performed a cyberwar game simulation to rehearse their strategy. Only 57% had some cyber insurance (Deloitte, 2015). These numbers are surprisingly low when considering the high-profile nature of the retail industry breaches.

In 2017 Visa produced a report on the top 5 Retail Point of Sale Cyberthreats. According to the Report, by 2017, retailers begun investing heavily in cybersecurity to protect payment card data and personally identifiable information. This is a swift change from 2015. Visa customers were experiencing 41% of threats coming from e-commerce, with a sharp increase of card not present attacks. The number one source of the attacks is vulnerable E-commerce payment applications. Their conclusion: There is no end in sight to the cyberattacks on the retail industry. However, the nightmares of a breach can be avoided by having the programs in place that include technology, people, and processes (Jones, 2015).

In 2020 the risks have only increased as a global pandemic has forced many consumers to stay home and purchase a greater percentage online. Dan Pitman wrote an article for Forbes summing up the challenges of using the cloud and easing customer purchase barriers. His recommendations included open web application security project (OWASP), full testing, sanities' user input, monitor 3rd party vendor sites, and authenticate everything and everyone (Pitman, 2019)

The research of these three ranged from surveys to extensive data crunching. The final research report will not be possible to crunch petabytes of customer data as Visa did. The Report will need to use a hybrid approach using open-source tools to compile data from other sources.

Social media analysis

Since the dawn of social media, the Threat Intelligence community has been asking: “Is there value in analyzing social media for Threat Intelligence and threat actors?”. For some of those years, the answer has been no, but as social media platforms have developed, and new various of platforms have come forth.

These social media platforms give new opportunities for Threat Intelligence gathering. At first, a lot of the information posted was either inaccessible, maybe because you needed to be someone's friend in order to see their posts and pictures, or because the platform was not well indexed. In more modern times, and especially in 2020, this could not be further from the truth. Social media has an important place in modern Threat Intelligence, especially for the retail industry (Ciarnellio, 2019). The information gathered from social media has exploded as people have become more comfortable sharing all aspects of their life, as seen in Figure 1 (Echosec Systems, 2020). The majority of the largest Threat Intelligence platforms offer social media analysis and indexing as one of their selling points. This includes features like alerts when someone uses a specific hashtag, recognizes objects in images, and keywords used near or related to a brand or a retail location.

Figure 1: A user bragging about how they found a vulnerability in a retail store on a social media platform called Raddle. They used this vulnerability to steal a TV (Echosec Systems, 2020).

Social media has also proven as a good way of evaluating how the public may react to different events, even in real-time. During the 2020 election, the retail industry reacted quickly to growing tensions in social media as increasing numbers of groups were planning violent demonstrations the night before the election.

The Threat Intelligence community had learned a lot from the 2016 election, where there also were riots in the street after Donald Trump won the election. This time around, the industry had learned and prepared early for physical destruction based on Intelligence gathered from social media (Nettitude.com, 2020).

Figure 2: Louis Vuitton retail shop in NYC barred up during election day 2020 (Therealdeal.com, 2020)

Now that the Threat Intelligence industry agrees that social media has an important place as a source for valuable information, solutions are coming forward to serve that need (blog.nettitude.com, 2020). The industry has become great at scraping and gathering raw data from different sources, even in real-time. The difference, especially in the products and platforms provided, are in the features that analyze the gathered data. They can now give the data context and extract the key information that should be included in a report or to be sent as a tip to a local retail store.

According to Echosec Systems, the industry has now recognized the importance of going outside of the mainstream social media platforms and branching out to lesser-known platforms, like 4chan, Reddit, Raddle, and Discord.

Even though the major platforms can be great for Intelligence, the less monitored and regulated platforms are often the ones providing the most unique and valuable Intelligence.

The retail industry has identified four key aspects of their core business where they see that open-source threat intelligence gathered from social media can assist in gaining insight and preventing unwanted events (The Echosec Team, 2019):

- Protecting assets, employees, customers and executives
- Crisis situations, like active shooter situations or bomb threats
- Detecting brand sentiment and reactions to new products, services, or press releases from the company
- Customer complaints

There is a clear belief among threat researchers specializing in social media that we are still learning how to utilize social media platforms for threat intelligence. The ever-evolving tech-landscape will bring on new data points, new types of platforms, and how data is gathered and analyzed.

Physical security Intelligence

Physical Security Intelligence was used to keep track of shoplifters and workers who tried to rob retailers. New times brought modern issues. In several different respects, the physical store is at risk, and in order to gain insight into how assets can be secured in a more technical environment, risk intelligence is required (Burton, 2020). Sometimes when public protests turn to violence and incidents between police and protesters increase, workers are at risk. They will also be at risk if protesters disrupt retail stores by blocking exits or trying to bypass security guards to enter stores where employees and customers are (Moeller, 2015). Physical protection requires guards, cameras, and their general purpose is to protect themselves from threats. This can be done by significant comprehension and using knowledge to solve crucial problems (Moeller, 2015).

There is no such thing as 100 percent security but knowing the vulnerabilities and being prepared for them will decrease the risk of potential harm. Depending on the store's size and location, the retail stores need to analyze physical vulnerabilities and determine how to protect

them from being exploited (Landoll, 2006). This section will look at physical security risks and methods to decrease them as retail security should be proactive in using threat intelligence and add the online threat intelligence aspect to their risk assessments. An attack and target could be anything from theft, burglary, kidnapping, bombing, holding customers or employee's hostage, and planned by organized crime actors and opportunistic customers. Many of these threatening signals could be found digitally, as some criminals need to brag about their plans or actions (Burton, 2020).

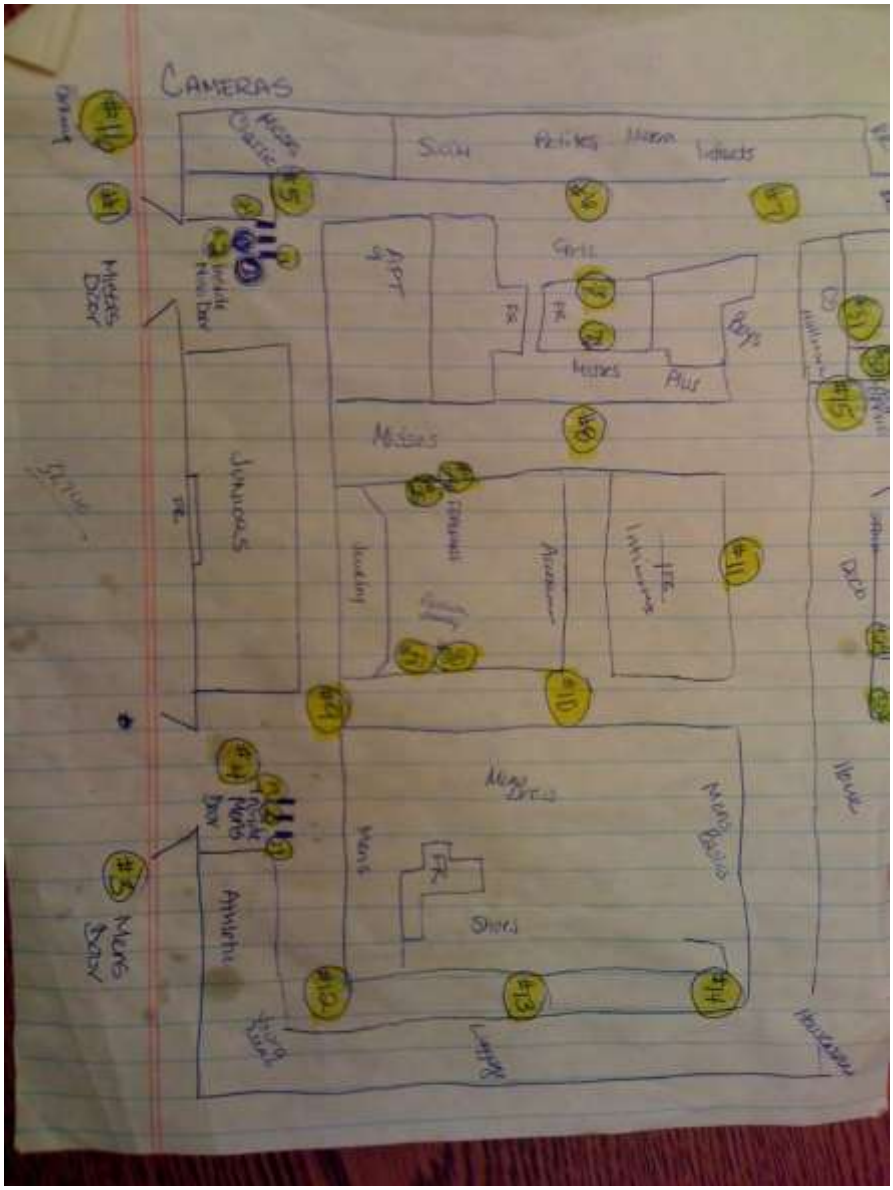

Figure 3: Hand drawn map of a US department store (Imgur, n.d.)

It has also become more common for organized crime and small-theft customers to share resources and knowledge online, specifically sharing how to exploit a vulnerability or share something new they have learned. Figure 3 was shared on Reddit in 2020, where a US department store chain employee decided to map out a typical store-layout to showcase surveillance camera blind-spots.

Not only did the image share critical information about this particular chain's camera layout, but a discussion also ensued in the comments where people shared all kinds of information and exploits related to this particular chain. They even discussed the employee routine for theft, stating that "if no guard is present in the building, you can walk out with products as this chains employee policy forbids them from physically stopping any ongoing theft." This information is now indexed. A simple Google search can lead an actor to this information, preparing them on how they may want to execute a robbery, theft of specific items, or what to expect if they were caught in the act. Luckily, in this case, the chains threat intelligence platform picked up on this forum post, alerting them that their policies and routines were being discussed online. It is not clear what changes this chain made after realizing their routines are now in the public domain, but they said to have made changes to routines that were pointed out as flawed by the criminals discussing this.

Common physical retail store vulnerabilities are theft and burglary. Hiring a security guard and placing the guard at the building entrance would help a customer with good intentions feel safer as soon as the customer enters the building (Landoll, 2011). A security guard at the entrance or patrolling the store will also limit thieves or persons with harmful intentions from attacking the store, its employees, and customers.

Technology presents a new challenge for the physical security of retail businesses. All the networking, monitoring devices, and electronic payment systems that increase profitability also increase a store’s attack surface. Today's threat is dynamic, and original physical security is under constant change. In modern times we are now concerned with cameras, cashiers, networks, and other technological supplements vulnerable to unauthorized persons (Zola, 2020).

Threat intelligence can provide the necessary insight to defend against new threats. A five-step intelligence cycle is a framework to use when physical security needs to be configured. Knowing the store's vulnerabilities and figuring out how to decrease the likelihood of these vulnerabilities to be attacked would help the store reduce the risk of unwanted events, which could lead to monetary loss. Physical security is used to ensure a store's personnel and customers' safety and their information, assets, and network.

1. Planning:
   - The groundwork for physical security is figured at this step. This step will look at the store's vulnerabilities and critical questions that need to be answered to address the security needs.

2. Collection:
   - Gather information to identify relevant threats. Collection sources could be social media, news media, and other online platforms. It is also possible to gather information by using Geographic Information Systems (GIS) and Global Positioning Systems (GPS), by, for instance, looking for specific keywords or mentions of a particular retail store. This makes it possible to do crime mapping and geographical profiling (Purpura, 2010).

3. Analysis:
   - At this step, the information gathered needs to be analyzed to answer the questions from the planning. With this information, it will be possible to determine present threats and their likelihood to happen.

4. Production:
   - The outcome of the analysis would be used to produce a formal security implementation plan. Detailed information about cameras, access controls, blind spots issues, escape routes, to mention some.

5. Dissemination and feedback:
   - The feedback can be from employees, customers, or extracted from surveillance cameras. What worked? What did not work, and how should the store solve it?

Threats will always be dynamic, and this framework should not only be looked at one time but should be used before an event, such as black Friday sales, or combined with information extracted from online sources. Addressing challenges in context and subject-matter should not be overlooked (Gray, 2019). Geopolitical events, such as a terrorist attack, violent demonstration, natural disaster, and global pandemic, could be used to analyze a store's threats. Using geopolitical Intelligence will help the store find real-time events that could be an effective way to protect the store and its assets. Monitoring geopolitical events would also make it easier to understand when to set up a new intelligence cycle to analyze an upcoming or ongoing event (Recorded Future, 2020).

Conclusion

Threat Intelligence has found its place in modern risk assessments and threat assessments, especially digital threat intelligence. While the field is still rising strong and new ways of collecting information on threats are yet being developed, it is clear that choices increase our society's evolution. The bulk of the study carried out is by large companies with large customers. However, the strategies and techniques used can be scaled down to smaller and medium-sized organizations that do not have their more prominent colleagues' limitless budgets but are also targeted by similar attacks. In the last five years, the threshold for information collection and intelligence production has been significantly reduced. Small companies can profit from these publicly available data sources. The question to be addressed in the study is whether, relative to the cost/gain of paid services, the quality of information offers advantages. A framework will be included for the methods of investigation used. This framework will consist of methods and tools that can be used to get an insight into real-time threats.

Resources

BDO. (2019). *BDO retail rationalized survey*. Retrieved from: https://www.bdo.com (Gathered 14.12.20)

Burton, F. (2010). *A Call for Change in Physical Security.* Retrieved from: https://www.darkreading.com (Gathered 15.12.20)

Ciarniello, A. (2020). *Social Media Threat Intelligence: Are Facebook And Instagram Relevant?* Retrieved from: https://www.echosec.net (Gathered 14.12.20)

Cyber Proof. (n.d.). *Managed Threat Intelligence.* Retrieved from: https://www.cyberproof.com (Gathered 14.12.20)

Deloitte. (2015). *Cyber Risk in Retail: Protecting the retail business to secure tomorrow's growth.* Retrieved from: https://www2.deloitte.com (Gathered 14.12.20)

Gray, I. W. (2019). *The Physical Security Intelligence Cycle*. Retrieved from: https://www.flashpoint-intel.com (Gathered 15.12.20)

Hamer, A. J. (2018). *5 Reasons why threat intelligence matters to your company.* Retrieved from: https://www.anomali.com (Gathered 14.12.20)

Hayes, R (2014). *Retail Security and Loss Prevention.* Retrieved from: https://link.springer.com (Gathered 14.12.20)

Imgur.com. (2016). *Map.* Retrieved from: https://imgur.com (Gathered 16.12.20)

Intsights Defend Forward. (2019). *Cyber (attack) Monday: Hackers target the retail industry as E-Commerce Thrives.* Retrieved from: https://wow.intsights.com (Gathered 14.12.20)

Jones, G. (2017). *The Top 5 Retail Point of Sale Cyber Threats.* Retrieved from: http://lp.threatq.com (Gathered 14.12.20)

Landoll, D. J (2006). *The Security Risk Assessment Handbook.* Retrieved from: https://books.google.no/books (Gathered 14.12.20)

Moeller, M. H. The duty of care: using threat intelligence to prepare for physical threats. Retrieved from: Using Threat Intelligence to Prepare for Physical Threats (lookingglasscyber.com) (Gathered 16.12.20)

Pitman, D. (2019). *Cyber Security Risk in Retail and How to Handle it*. Retrieved from: https://www.forbes.com (Gathered 14.12.20)

Purpura, P.P. (2010). *Security: An Introduction.* Retrieved from: https://books.google.no (Gathered 14.12.20)

Recorded Future Team. (2019). *Protecting the retail industry with real-time threat intelligence.* Retrieved from: https://www.recordedfuture.com (Gathered 14.12.20)

Recorded Future. (2020). Retrieved from: https://www.recordedfuture.com (Gathered 15.12.20)

The Echosec Team. (2019). *Open-Source Intelligence for Retail Security.* Retrieved from: https://www.echosec.net (Gathered 14.12.20)

The Real Deal New York. (2020). *Retailers Prepare for Election Day Unrest In NYC*. Retrieved from: https://therealdeal.com (Gathered 14.12.20)

Zola. A. (2020). *IoT Security Threats in Retail: How do we eliminate them?* Retrieved from: https://www.business2community.com (Gathered 15.12.20)