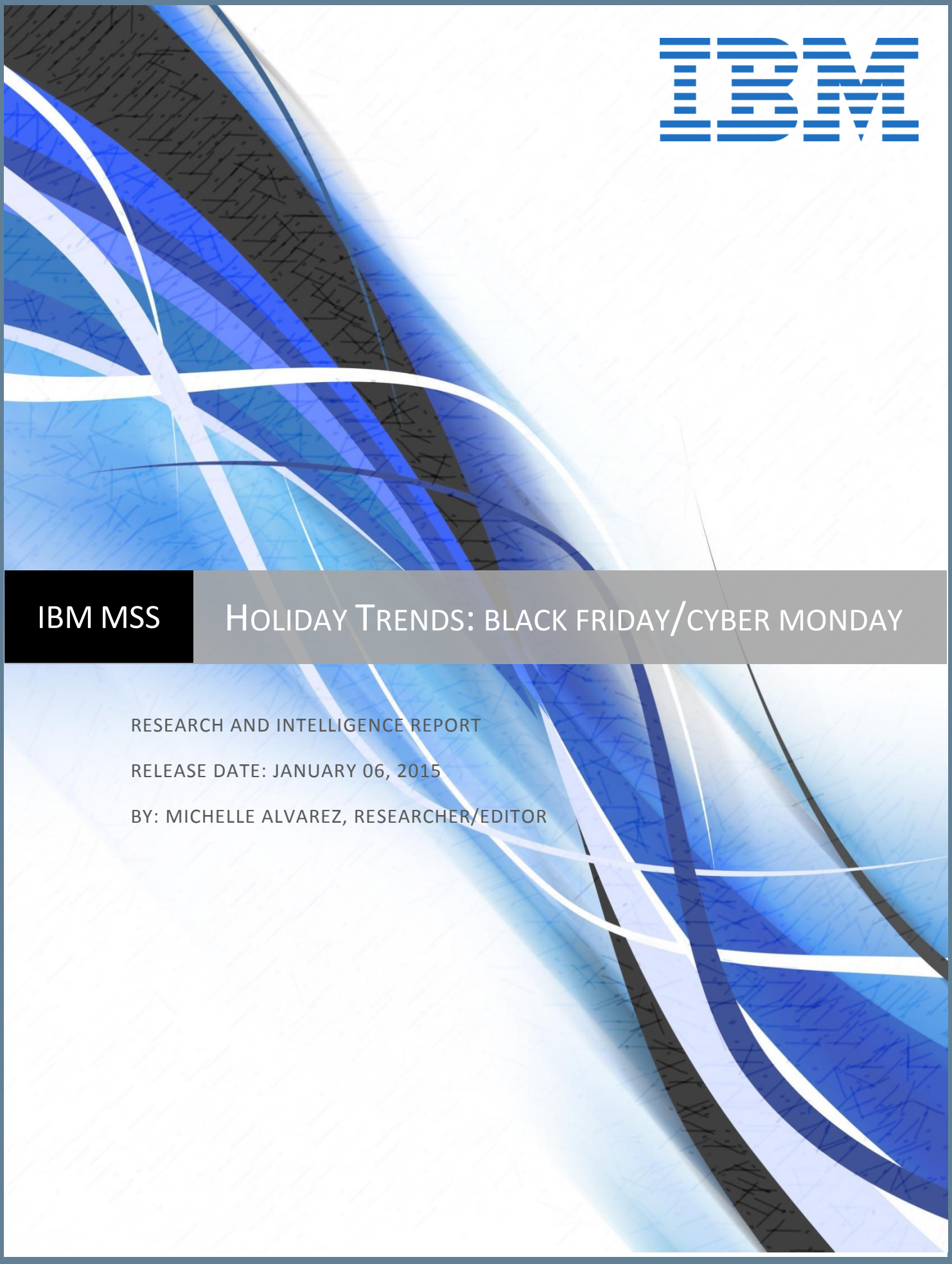

IBM MSS

HOLIDAY TRENDS: BLACK FRIDAY/CYBER MONDAY

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: JANUARY 06, 2015

BY: MICHELLE ALVAREZ, RESEARCHER/EDITOR

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

Tis the season to be jolly? For many, it is. However, if you're part of your organization's skeleton crew working during the holidays, these days may be less merry and bright and more stressful and worrisome. Fewer hands on deck means there are less resources available to put out fires. Business as usual could put a strain on a short-staffed security department, let alone an increase in incidents or attacks. Organizations may even opt to increase their security staff during this time period in anticipation of an increase in threats.

Every year, we warn our customers of the potential for attackers to utilize the holiday season to their advantage via spam, malicious greeting cards, phishing, and compromised web sites. Holiday malware has been surfacing since the late 80's. Spam, phishing and Search Engine Optimization (SEO) campaigns targeting consumers and utilizing this particular theme do ramp up during the holiday period. However, does this necessarily equate to increased attack activity against some or all industry sectors?

IBM security research analysts reviewed cyber attack data from the last few years and found that there is not an uptick in activity targeting industries during the period of time known as Black Friday through Cyber Monday. These results are surprising since this time-frame is ripe for attack. However, during the two-week holiday period analyzed for 2013, for instance, there was only an average of 4200 security attacks per day across IBM's MSS clients. This is nearly 39,000 fewer attacks than the daily average for last year. Even more surprising, the retail and wholesale industry ranked last in the top five industries attacked during this time period in both 2012 and 2013.

Despite our findings, this report in no way makes claim that serious compromises and attacks do not occur during the holidays. They certainly do, as realized with high-profile compromises such as the recently disclosed Sony Pictures Entertainment (SPE) breach and last year's Target breach. Organizations are encouraged to not let their guard down during November and December. However, while there have been several high-profile incidents announced around Black Friday, the timing of the announcement and the date of the actual compromise do not always coincide. In other words, vigilance against cyber attacks is a year-round activity and one that organizations cannot afford to skip.

ATTACK METRICS

In order to observe a true trend in activity, we assessed the time period several days before Black Friday and several days after Cyber Monday since 2012 through 2014. There are a few interesting observations that can be gleaned from Figure 1 below.

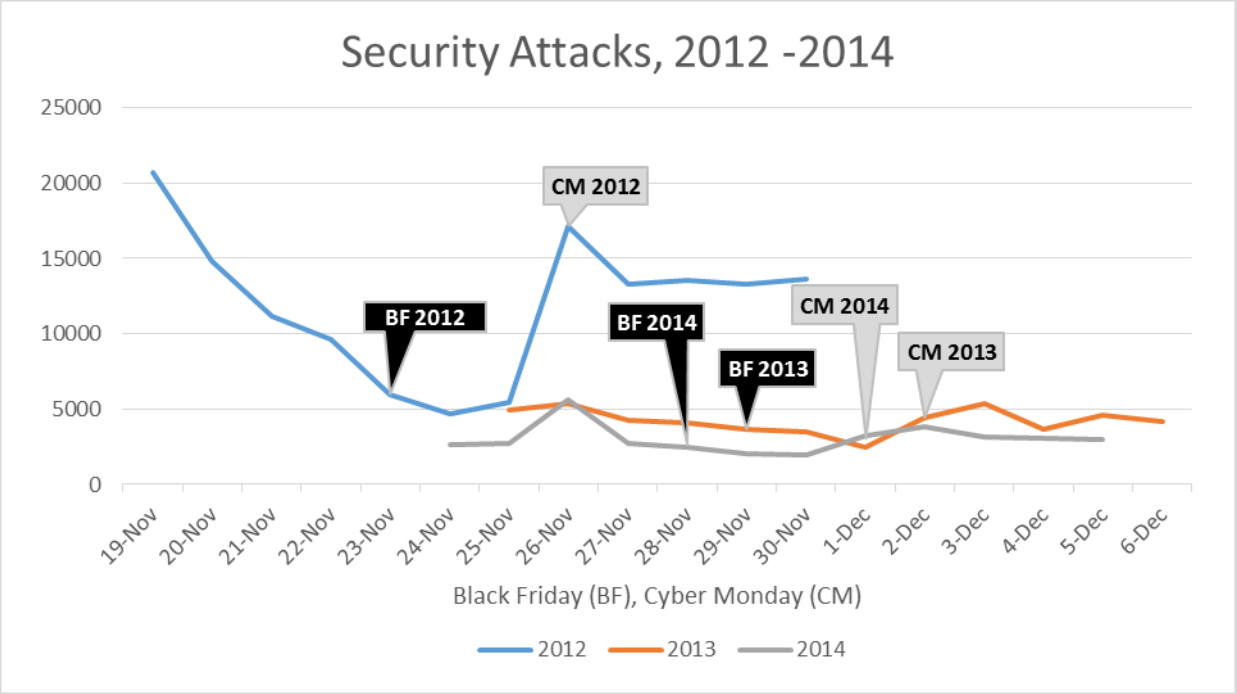

Figure 1. Security Attacks, 2012 – 2014 (Black Friday through Cyber Monday)

In the past three years, there has not been a notable uptick either on Black Friday or Cyber Monday with the exception of Cyber Monday in 2012. This uptick is still lower than the number of attacks seen at the beginning of the Thanksgiving week for that year. In fact, security attacks year over year since 2012 during this time period have been declining.

The lower-than-average number of daily security attacks during this time can possibly be the result of attackers performing their dirty work earlier in the year to then reap the benefits during the holiday shopping frenzy. Often, attackers infiltrate targeted systems and then spend months stealthily collecting data before any announcement is made or the organization becomes aware of the compromise.

Has user education made an impact on the security trend during the holidays? This is certainly a plausible argument. There are so many warnings during this time of year that users may actually be more wary. Hence, fewer are perhaps clicking on the dancing Santa in the holiday e-card that installs malware or the flashing “Discount” image that leads them to a malicious site. The extra attention and vigilance during this time may also be the reason why there are fewer attack attempts. Why attack when everyone is watching?

From an industry perspective, there are also a few surprises as shown in Figure 3 below. Manufacturing, not retail and wholesale, ranked first amongst the top five attacked industries during this time period for both 2012 and 2013. In fact, the retail and wholesale industry ranked last amongst the top five industries

attacked for those years. This ranking changed in 2014 with the retail and wholesale industry leaping to first place as most targeted industry and manufacturing dropping to third place.

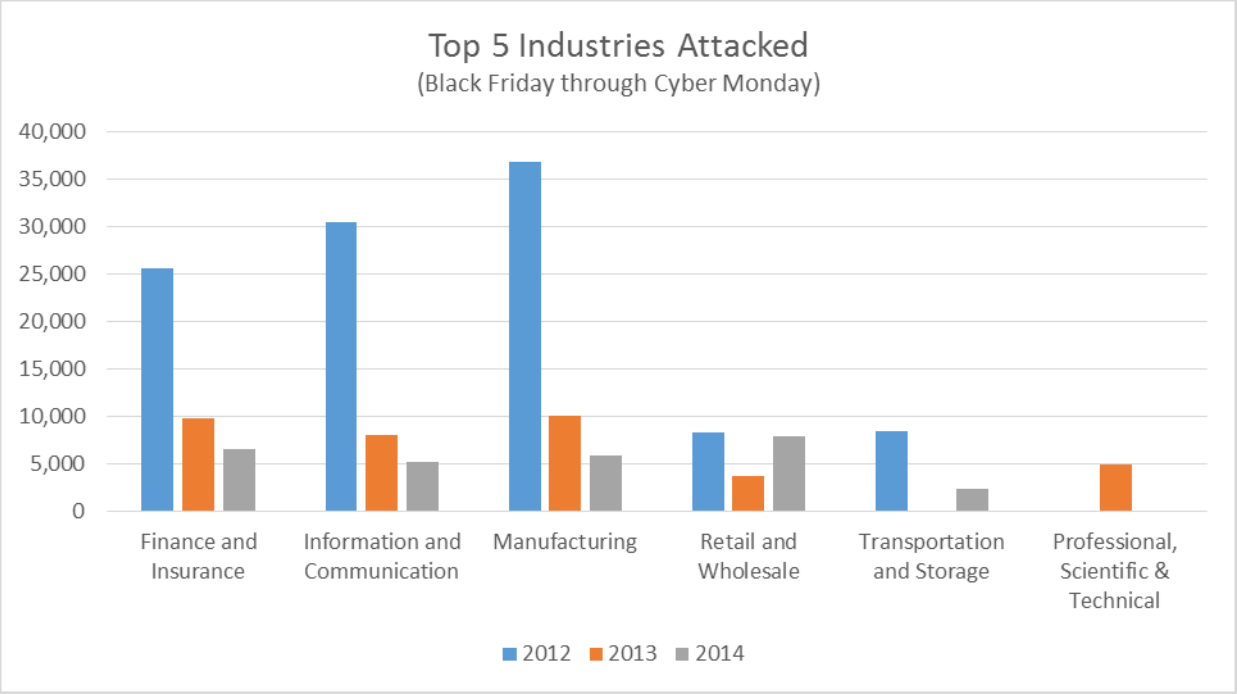

Figure 3. Top 5 Industries Attacked (Black Friday through Cyber Monday)

As expected, the finance and insurance industry ranked high all three years. Additionally, the same industries made the top five all three years in a row with one exception. Instead of transportation and storage, the professional, scientific and technical industry made up the top five in 2013.

We also assessed the type of incidents occurring during this time. Do attackers favor one type of attack over another when it comes to the holiday season? Some of the results were surprising.

Malicious code was the primary mode of attack in 2012 and 2013, as depicted in Figure 4 below. This is consistent with what we observed over the full year in terms of ranking amongst the types of incidents and the percentage of volume held by each type. In 2014, however, unauthorized access attempts rose to first place – accounting for 50 percent of the security incidents observed during Black Friday/Cyber Monday. Malicious code incidents dropped by more than half the volume observed in the previous two years, landing it in third place.

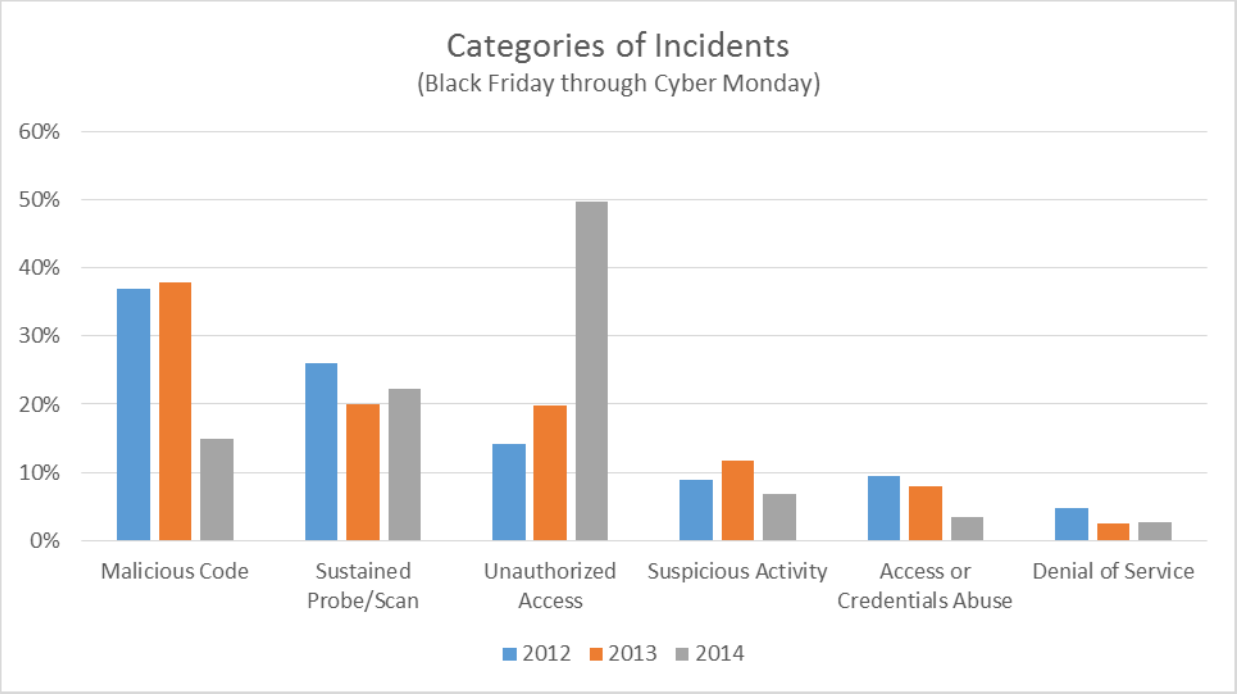

Figure 4. Categories of incidents, 2012-2014 (Black Friday through Cyber Monday)

It will be interesting to see if this change is also reflected when assessing the data for all of 2014. The IBM Security Services 2015 Cyber Security Intelligence Index, scheduled to be released in Q2 2015, will provide an update on this trend.

BLACK FRIDAY / CYBER MONDAY COMPROMISES

Using the same methodology as with the attack metrics, we reviewed data on compromises occurring during the time period several days before Black Friday and several days after Cyber Monday. The Privacy Rights Clearinghouse provides a database of publicly disclosed compromises in the United States.

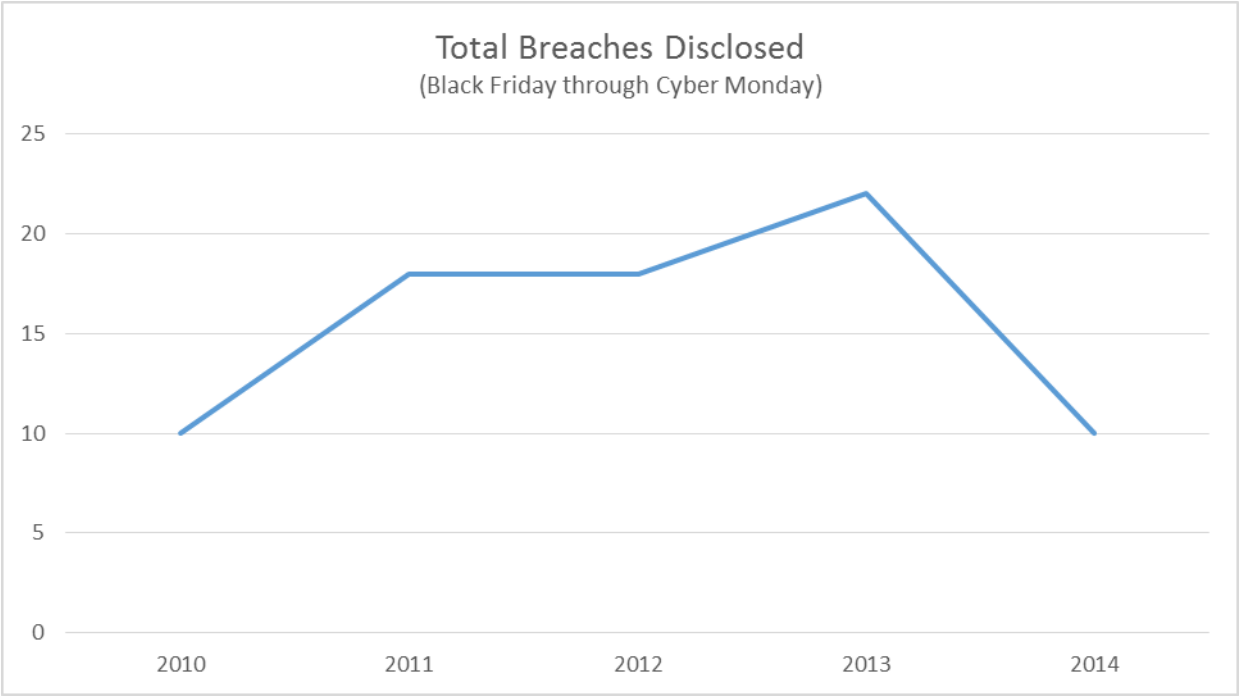

Figure 5. The number of breaches disclosed Black Friday through Cyber Monday. Source: Privacy Rights Clearinghouse.

The number of breaches disclosed rose steadily from 2010 through 2013, as shown in Figure 5 above. In fact, the number of disclosures for this time frame in 2013 was more than double the number for 2010. This year, the total number of disclosures took a sharp dive and equaled that of the number reported in 2010.

The number of disclosures is an interesting viewpoint, but the number of records compromised often tells a more compelling story. For instance, one data breach could yield millions of compromised records; or there could be several breaches consisting of only a few thousands of compromised records each. In this scenario, the single breach would have a larger impact.

Figure 6 below illustrates the trend since 2010 for number of records compromised over Black Friday and Cyber Monday. Clearly, last year was a huge year for number of disclosures and records compromised during this time period. Even with the largest compromise removed (2.5 million records affecting students, staff and graduates of Maricopa County Community (MCC) College), the peak for 2013 remains. There were several other large breaches contributing to this spike, including those affecting the University of Washington Medicine and JPMorgan Chase.

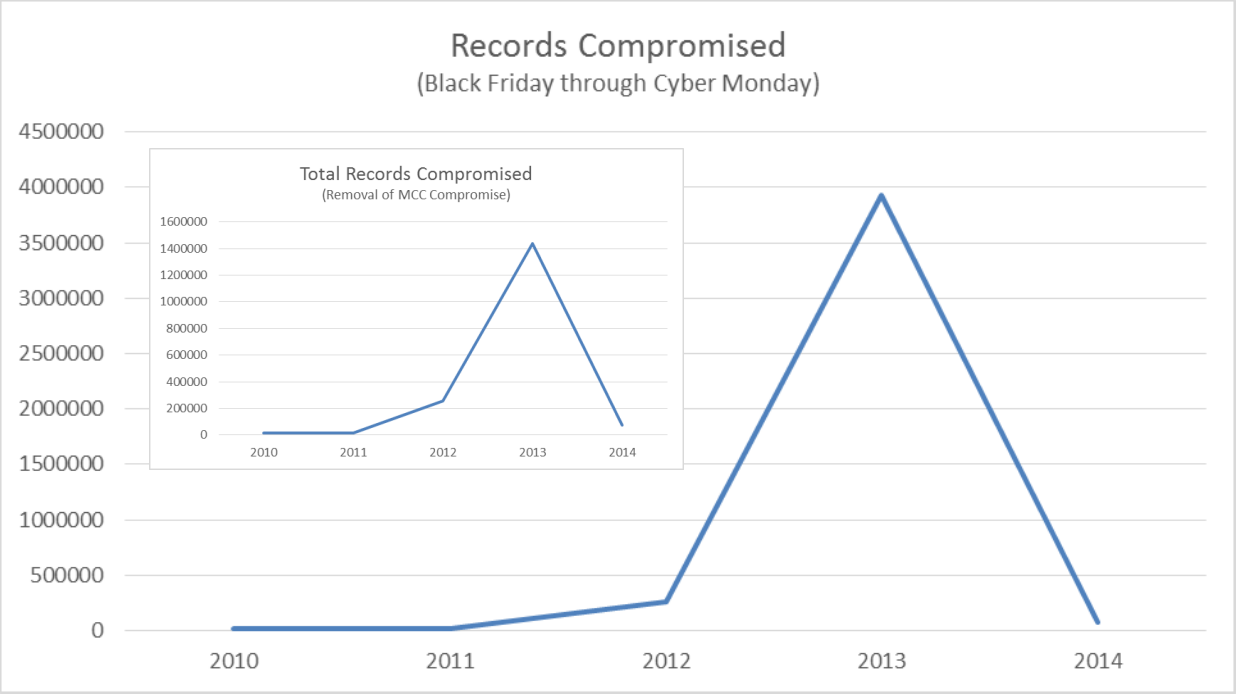

Figure 6. The number of records compromised Black Friday through Cyber Monday. Smaller chart represents the number of records compromised after removing the MCC breach of 2013. Source: Privacy Rights Clearinghouse.

The number of records compromised over this period in 2014 was over 72,000, which is still less than a third of the total records compromised in 2012 during the same time.

HOLIDAY BREACH ANNOUNCEMENTS – START OF A NEW TREND?

If attacks against industries are not trending upward and the number of disclosures have not been historically higher over the holidays, then why the recent heightened focus on potential attacks around Black Friday/Cyber Monday? Two words: “Target” and “Sony”. Major breaches targeting these two companies were announced during the holiday season.

Last year in mid-December, Target Corporation disclosed that attackers accessed customer debit and credit card information used at their stores between November 27, 2013 and December 15, 2013. This breach is one of the largest reported retail compromises – between 70 and 110 million records affected. The compromise was traced back to a phishing attack targeting employees at Target’s HVAC contractor, Fazio Mechanical, which contained a type of Point-of-Sale (POS) malware. Results of the breach: several

class-action lawsuits, loss of consumer trust and a reported loss of $148 million[i] – and this figure is expected to rise due to the possibility of future breach-related expenses.

On November 24, 2014 (four days prior to Black Friday), a post appeared on a popular Internet forum claiming that an image was appearing worldwide on Sony Pictures Entertainment (SPE) computers. The links contained within the image a large repository of filenames that a group called Guardians of Peace (GOP) claimed they had, and would release if demands were not met. Large amounts of data including highly sensitive information has been made publicly available. It's suspected that possibly petabytes of data have been compromised. This incident and specific details regarding the breach including source and method of attack are currently under investigation.

In the case of Target, the breach was discovered by the company and then announced to the public. With SPE, a third-party announced the breach which then prompted the investigation. Regardless of the source of the announcement, the effects are the same – the thoughts "our organization could be next year's holiday disaster" penetrate a corporation's psyche. This is where statistical and historical data take a backseat and organizations focus on not becoming the following year's holiday breach announcement.

RECOMMENDATIONS/MITIGATION TECHNIQUES

We have not observed a significant increase in attack activity targeting industries over Black Friday/Cyber Monday the last few years – this is good news. However, attacks do occur during this time period – the SPE and Target compromises are serious reminders of the existence of this threat. Organizations should not become lax in their protection strategies. Sometimes it only takes one sophisticated targeted attack to cause substantial financial loss and damage to an organization's brand – and this can happen at any time of the year. There are a few things organizations can do to prepare for cyber attacks before and during the holiday season:

- User Education – This is one that we continuously harp on; however, it actually goes a long way to protecting a company's network. Users have become wary of holiday-themed techniques and this appears to have had some success in thwarting attack attempts. Consider implementing a phishing awareness campaign a few weeks prior to the holiday season to test users' ability to identify phishing attacks.
- Prepare Holiday Staff – The remaining employees left to man the stations and hold the fort down do not have time to figure out what the appropriate escalation path is during a crisis. Make sure incident response plans are up-to-date.
- Retail & POS Malware – The retail and wholesale industry should be particularly concerned about securing their endpoint sales mechanisms against possible POS malware. The IBM Threat Research Group published a paper with specific recommendations for this particular threat, see references.

REFERENCES

A short history of Christmas malware
http://nakedsecurity.sophos.com/2010/12/15/christmas-malware-short-history/

Privacy Rights Clearinghouse
https://www.privacyrights.org/data-breach

Target Provides Preliminary Update on Second-Quarter Expenses Related to the Data Breach and Debt Retirement
http://pressroom.target.com/news/target-provides-preliminary-update-on-second-quarter-expenses-related-to-the-data-breach-and-debt-retirement

I used to work for Sony Pictures. My friend still works there and sent me this. It's on every computer all over Sony Pictures nationwide.
https://www.reddit.com/r/hacking/comments/2n9zhv/i_used_to_work_for_sony_pictures_my_friend_still/

Industry Overview - Retail
https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/industry_overview_retail_11-21-2014.html

CONTRIBUTORS

John Kuhn – Senior Threat Researcher, Threat Research Group

Nick Bradley - Practice Lead, Threat Research Group

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. This information is provided “AS IS,” and without warranty of any kind.

[i] Chronology of Data Breaches | Privacy Rights Clearinghouse https://www.privacyrights.org/data-breach-asc?title=target