# Selon une étude IBM, le nombre de cyberattaques touchant les détaillants diminue de moitié ; Les données de plus de 61 millions de consommateurs ont été volées en 2014

**Les cybercriminels diminuent le nombre d'attaques y compris durant les deux jours de shopping les plus importants de l'année**

**Paris - 06 janv. 2015:** Selon des résultats dévoilés aujourd'hui par IBM, alors que le nombre de cyberattaques aux Etats-Unis touchant les commerçants de détail a diminué de moitié, le nombre de données qui leur sont volées atteint presque un niveau record. Du fait de la sophistication et de l'expertise croissante des cybercriminels, les chercheurs d'IBM Security rapportent qu'en 2014, plus de 61 millions d'informations clients ont été volées aux détaillants, et ce malgré la diminution du nombre d'attaques.

Contrairement aux idées reçues, la majorité des cyberattaquants aux Etats-Unis ont diminué leurs efforts de piratage durant le Black Friday et le Cyber Monday en 2014, dates auxquelles les dépenses atteignent des pics. Les rapports "[2014 Retail Research and Intelligence Report](#)" et "[Holiday Trends: Black Friday/Cyber Monday Research and Intelligence Report](#)" ont été développés par une équipe d'analystes de l'IBM Managed Security Services qui contrôlent plus de 20 milliards d'incidents de sécurité chaque jour.

Selon ces études, les cyberattaquants utilisent de nouvelles techniques de plus en plus sophistiquées pour obtenir des quantités très importantes de données confidentielles, et ce avec un succès croissant. Depuis 2012 le nombre de violations signalées par les détaillants a diminué de moitié mais malgré ce déclin, les hackers ont réussi à toucher un plus grand nombre de victimes à chaque incident.

***

**IBM Study: Number of Cyber Attacks on Retailers Drops by Half; Criminals Still Stole Over 61 Million Customer Records in 2014**

*Cyber Thieves Scale Back, Take Off Two Biggest Shopping Days of the Year*

**ARMONK, N.Y. - 05 Jan 2015:** According to findings released today by IBM (NYSE: IBM), despite an 50 percent decline in the number of cyber attacks against U.S. retailers, the number of records stolen from them remains at near record highs. IBM Security researchers report that in 2014, cyber attackers still managed to steal more than 61 million records from retailers despite the decline in attacks, demonstrating cyber criminal's increasing sophistication and efficiency.

Contrary to what most would expect, the majority of cyber attackers scaled back their hacking efforts around Black Friday and Cyber Monday in 2014 rather than capitalize from the massive spike in retail spending. The 2014 Retail Research and Intelligence Report and the Holiday Trends: Black Friday/Cyber Monday Research and Intelligence Report were created by IBM's Managed Security Services team of analysts, who monitor more than 20 billion security incidents every day.

According to the research, cyber attackers are becoming increasingly more sophisticated, using new techniques to obtain massive amounts of confidential records with increased efficiency. Since 2012, the number of breaches reported by retailers dropped by 50 percent. Despite this decline, the perpetrators were able to impact a far greater number of victims with each incident.

*"The threat from organized cyber crime rings remains the largest security challenge for retailers,"* said **Kris Lovejoy, General Manager, IBM Security Services**. *"It is imperative that security leaders and CISOs in particular, use their growing influence to ensure they have the right people, processes and technology in place to take on these growing threats."*

**Black Friday and Cyber Monday**

Identified as the two biggest shopping days of the year by IBM's Digital Analytics Benchmark, cyber attackers reduced their activity across all industries on Black Friday and Cyber Monday, rather than taking action. When looking at the two week period (Nov 24 - Dec 5) around these days, the data shows the following activity across all industries:

- The number of daily cyber attacks was 3,043, nearly one third less than the 4,200 average over this period in 2013.
- From 2013 and 2014, the number of breaches dropped by more than 50 percent for Black Friday and Cyber Monday.
- In 2013, there were more than 20 breaches disclosed including several large breaches that caused the number of records compromised to rise drastically, reaching close to 4 million.
- Over the same period in 2014, 10 breaches were disclosed which resulted in just over 72,000 records getting compromised

Despite this "cyber threat slow down," the retail and wholesale industries emerged as the top industry target for attackers in 2014, a potential result of the wave of high profile incidents impacting name brand retailers. In the two years prior, manufacturing ranked first amongst the top five attacked industries while the retail and wholesale industry ranked last. This past year, the primary mode of attack was unauthorized access via Secure Shell Brute Force attacks, which surpassed malicious code, the top choice in 2012 and 2013**.**

**Top Breaches Overshadow Growing Trend**

Attackers secured more than 61 million records in 2014, down from almost 73 million in 2013. However, when the data was narrowed down to only  incidents involving less than 10 million records (which excludes the top two attacks over this timeframe, Target Corporation and The Home Depot), the data shows a different story--the number of retail records compromised in 2014 increased by more than 43 percent over 2013.

**Sophisticated Methods of Attack**

While there has been a rise in the number of Point of Sale (POS) malware attacks, the vast majority of incidents targeting the retail sector involved Command Injection or SQL injection. The complexity of SQL deployments and the lack of data validation performed by security administrators made retail databases a primary target. Over 2014, this Command Injection method was used in nearly 6,000 attacks against retailers. Additional methods include Shellshock as well as POS malware such as BlackPOS, Dexter, vSkimmer, Alina and Citadel.

The data for the number of records compromised and breaches disclosed was analyzed by IBM security experts and was made publically available by Privacy Rights Clearinghouse. The remaining data came from IBM's Managed Security services team.

**About IBM Security**

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations.

For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.