Communiqués de presse

Etude IBM : Les entreprises, plus susceptibles de payer des rançons que les consommateurs

70% des entreprises impactées ont payé les cybercriminels, la moitié a payé plus de 10 000$ - Les consommateurs sont motivés pour payer quand des informations financières ou des souvenirs de famille sont menacés

Paris - 14 déc. 2016: L'entité sécurité d'IBM annonce aujourd'hui les résultats d'une étude qui révèle que 70% des entreprises infectées par un ransomware (rançongiciel) ont payé une rançon pour récupérer l'accès aux données et aux systèmes de l'entreprise. Comparativement, plus de 50% des consommateurs interrogés ont déclaré qu'ils ne paieraient pas pour récupérer des données ou des équipements personnels, à l'exception des données financières.

L'étude d'IBM X-Force "Ransomware: How Consumers and Businesses Value Their Data" (Ransomware : comment les consommateurs et les entreprises valorisent leurs données") a interrogé 600 chefs d'entreprises et plus de 1000 consommateurs aux Etats-Unis pour déterminer la valeur accordée à différents types de données. Voici quelques-unes des principales constatations concernant les consommateurs :

- Alors que plus de la moitié des consommateurs interrogés ont indiqué dans un premier temps qu'ils ne paieraient pas la rançon, lorsqu'ils ont été interrogés à propos de certains types de données, 54% ont signalé qu'ils paieraient probablement pour récupérer des données financières.

- De plus, plus de la moitié (55%) des parents interrogés seraient disposés à payer pour l'accès aux photos numériques de famille contre 39% des répondants sans enfants.

D'après le centre de recherche IBM-X-Force, les ransomwares représentaient près de 40% de tous les courriers indésirables envoyés en 2016, ce qui démontre une augmentation significative de la propagation de cet outil d'extorsion.

Les enterprises qui payent

Près d'un chef d'entreprise interrogé sur deux a connu des attaques de ransomware sur son lieu de travail, ce qui démontre l’impact de celles-ci auprès des entreprises. L'étude a révélé que 70% de ces dirigeants ont déclaré que leur entreprise avait payé pour résoudre l'attaque, et la moitié de ceux qui ont payé ont versé plus de 10 000 $ et 20% ont payé plus de 40 000 $.

Dans le cadre de l'enquête, près de 60% de tous les dirigeants d'entreprises ont indiqué qu'ils seraient prêts à payer une rançon pour récupérer des données. Les types de données pour lesquels ils étaient prêts à payer incluaient des dossiers financiers, des dossiers clients, la propriété intellectuelle et les plans business.

Les consommateurs peuvent être motivés pour payer

Un consommateur sur deux ayant répondu à l’enquête a indiqué qu'il ne serait pas disposé à payer un pirate pour récupérer l'accès à ses données. Lorsqu'on leur a mentionné certains types de données, leur volonté de payer a commencé à augmenter.

Par exemple, 54% des participants seraient prêts à payer pour des données financières et 43% seraient prêts à payer pour récupérer l'accès à leur appareil mobile. Lorsqu'on leur a demandé de mettre une valeur sur différents types de données, 37% des consommateurs ont déclaré qu'ils allaient payer plus de 100 $ pour récupérer leurs données. À titre de comparaison, IBM X-Force voit typiquement des ransomware exigeant environ 500 $ ou plus, selon la victime et le laps de temps qu'ils attendent avant de payer.

Là où les cybercriminels ont le plus de succès, c’est lorsqu’ils utilisent le ransomware contre des parents. En fait, 39% des parents interrogés ont de l'expérience en matière de rançon tandis que 29% des non-parents ont indiqué avoir une certaine expérience.

“Alors que les consommateurs et les entreprises ont des expériences différentes par rapport au ransomware, les cybercriminels n’ont aucune frontière quand il s’agit de leurs cibles. » a déclaré Limor Kessen, Executive Security Advisor, IBM Security et auteur du rapport. « «La numérisation des souvenirs, les informations financières et les secrets commerciaux exigent une vigilance renouvelée pour les protéger des programmes d'extorsion tels que le ransomware. Les cybercriminels profitent de notre dépendance vis-à-vis des appareils et des données numériques, créant des points de pression qui mettent à l'épreuve notre volonté de perdre des souvenirs précieux ou une sécurité financière ».

Se préparer et répondre au ransomware

Avec un retour financier pour les cybercriminels croissant à un milliard de dollars sur les ransomwares dans l’hémisphère Nord, IBM s'attend à ce qu'ils continuent à croître au même titre que d’autres programmes d'extorsion. A la fois les entreprises et les consommateurs peuvent prendre quelques mesures pour se défendre contre les ransomwares. Les experts d’IBM X-Force recommandent les conseils suivants pour vous protéger et protéger les entreprises :

- **Etre vigilent :** Si un email semble trop beau pour être vrai, c’est probablement le cas. Soyez prudent lors de l'ouverture des pièces jointes et lorsque vous cliquez sur les liens.

- **Sauvegardez vos données :** Planifiez et maintenez des routines de sauvegarde régulières. Assurez-vous que les sauvegardes sont sécurisées et ne sont pas constamment connectées au réseau. Testez vos sauvegardes régulièrement afin de vérifier leur intégrité et leurs accessibilités en cas d'urgence.

- **Désactiver les macros** : Les macros de document ont été un vecteur commun d'infection pour les ransomwares en 2016. Les macros d'emails et de documents doivent donc être désactivées par défaut pour éviter l'infection.

- **Patcher et purger :** Maintenez les mises à jour logicielles régulières pour tous les périphériques, y compris les systèmes d'exploitation et les applications. Mettez à jour tout logiciel que vous utilisez souvent et supprimez les applications auxquelles vous accédez rarement.

Pour obtenir des conseils et des détails supplémentaires sur les résultats de l'enquête, vous pouvez télécharger le rapport complet ici : https://ibm.biz/RansomwareReport.

Si vous êtes victime d’un ransomware :

- En Europe, vous pouvez le signaler via le site Internet de déclaration de cybercriminalité d'Europol : https://www.europol.europa.eu/report-a-crime/report-cybercrime-online
- En France, vous pouvez le signaler via le site : https://www.ssi.gouv.fr/en-cas-dincident/

A propos de la division sécurité d’IBM

La division sécurité d’IBM propose un portefeuille de solutions de sécurité pour les entreprises parmi les plus avancés et les plus intégrés. Ce portefeuille est supporté par IBM X-Force, organisation de recherche connue mondialement et permet aux organisations de gérer efficacement les risques et de se défendre contre les menaces émergentes. IBM dispose d’une organisation de recherche et développement et de mise en œuvre parmi les plus importantes au monde, gère 35 milliards d’événements de sécurité par jour dans plus de 130 pays et possède plus de 3 000 brevets de sécurité.

Pour plus d'informations : http://www.ibm.com/security/fr-fr/

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

A propos de l'étude :

L'enquête a été conçue avec Ketchum Global Research and Analytics. La collecte de données a été menée par Braun Research Inc. (audience des entreprises - 600 réponses) et ORC International (audience des consommateurs - 1 021 réponses).

La marge d'erreur de l'étude pour l'ensemble des entreprises interrogées est de +/- 3,88% avec un niveau de confiance de 95% (et +/- 5,5% avec un niveau de confiance de 95% pour chaque taille d'entreprises). La marge d'erreur pour l'étude des consommateurs est de +/- 3,07% avec un niveau de confiance de 95%.

###

IBM Study: Businesses More likely to Pay Ransomware than Consumers

70% of Businesses Impacted Paid Cybercriminals; half paid over $10,000

Consumers Motivated to Pay When Financial Info, Digital Family Memories Threatened

CAMBRIDGE, MA – December 14, 2016 – IBM Security today announced results from a study finding 70 percent of businesses infected with ransomware have paid ransom to regain access to business data and systems. In comparison, over 50 percent of consumers surveyed said they would not pay to regain access back to personal data or devices aside from financial data.

Ransomware is an extortion technique used by cybercriminals where data on computers and other devices is encrypted and held for ransom until a specified amount of money is paid. The IBM X-Force study, "Ransomware: How Consumers and Businesses Value Their Data" surveyed 600 business leaders and more than 1,000 consumers in the U.S. to determine the value placed on different types of data. Some key findings from consumers include:

- While over half of consumers surveyed initially indicated they would not pay the ransom, when asked about specific data types, 54 percent indicated they would likely pay to get financial data back.
- Also, more than half (55%) of parents surveyed would be willing to pay for access to digital family photos vs. 39 percent of respondents without children.

Ransomware was one of the leading cybersecurity threats in 2016 with the FBI estimating cybercriminals, in the first three months of this year, making a reported $209 million. This would put criminals on pace to make nearly $1 billion in 2016 from their use of the malware. In fact, according to IBM X-Force research, ransomware made up nearly 40 percent of all spam e-mails sent in 2016, demonstrating a significant increase in the spread of the extortion tool.

Businesses Paying Up

Demonstrating ransomware's success with businesses, nearly one in two business executives surveyed have experienced ransomware attacks in the workplace. The study found 70 percent of these executives said their company has paid to resolve the attack, with half of those paying over $10,000 and 20 percent paying over $40,000.

As part of the survey, nearly 60 percent of all business executives indicated they would be willing to pay ransom to recover data. The data types they were willing to pay for included financial records, customer records, intellectual property and business plans. Overall, 25 percent of business executives said, depending upon the data type, they would be willing to pay between $20,000 and $50,000 to get access back to data.

Small businesses remain a ripe target for ransomware. Only 29 percent of small businesses surveyed have experience with ransomware attacks compared to 57 percent of medium size businesses. While cybercriminals may not view these businesses as offering a big payday, a lack of training on workplace IT security best practices can make them vulnerable. The study found that only 30 percent of small businesses surveyed offer security training to their employees, compared to 58 percent of larger companies.

Consumers Can be Motivated to Pay

One out of two consumers participating in the survey indicated they would be unwilling to pay a hacker to regain access to their data. When presented with specific data types their willingness to pay began to increase.

For example, 54 percent of participants would be willing to pay for financial data and 43 percent were willing to pay for access back to their mobile device. When asked to put a value on different types of data, 37 percent of consumers said they would pay over $100 to get data back. For comparison, IBM X-Force typically sees ransomware demanding approximately $500 or higher, depending upon the victim and the time lapse they wait before paying.

Cybercriminals are having their best success leveraging ransomware against parents. In fact, 39 percent of parents surveyed have experience dealing with ransomware while overall 29 percent of non-parents indicated some experience.

IBM's analysis determined that parents are more motivated to pay due to sentimental value and children's happiness. For example, 71 percent of parents surveyed were most concerned about their family digital photos and videos being threatened with only 54 percent of non-parents showing the same concern. Overall, 55 percent of parents would pay for access back to the photos while only 39 percent of non-parents would pay.

Access to gaming devices, likely used by children, were also highly ranked by parents as most concerning to them. In fact, it was second to photos and video with 40 percent of parents reported being worried about losing access to these devices versus 27 percent of non-parents.

"While consumers and businesses have different experiences with ransomware, cybercriminals have no boundaries when it comes to their targets," said Limor Kessem, Executive Security Advisor, IBM Security and the report's author. "The digitization of memories, financial information and trade secrets require a renewed vigilance to protect it from extortion schemes like ransomware. Cybercriminals are taking advantage of our reliance on devices and digital data creating pressure points that test our willingness to lose precious memories or financial security."

Preparing for and Responding to Ransomware

With the financial returns on ransomware growing north of a $1 billion for cybercriminals, IBM anticipates it and other extortion schemes will continue to grow. Both businesses and consumers can take some steps to help defend themselves from ransomware. IBM X-Force experts recommends the following tips to protect yourself and your business:

- **Be Vigilant:** If an email looks too good to be true, it probably is. Be cautious when opening attachments and clicking links.

- **Backup Your Data**: Plan and maintain regular backup routines. Ensure that backups are secure, and not constantly connected or mapped to the live network. Test your backups regularly to verify their integrity and usability in case of emergency.

- **Disable Macros:** Document macros have been a common infection vector for ransomware in 2016. Macros from email and documents should be disabled by default to avoid infection.

- **Patch and Purge**: Maintain regular software updates for all devices, including operating systems and apps. Update any software you use often and delete applications you rarely access.

For additional tips and details on the survey findings, you can download the full report at: https://ibm.biz/RansomwareReport.

In addition, Resilient, an IBM Company, today announced an industry-first Dynamic Playbook to help organizations respond to ransomware and other complex attacks. Resilient Dynamic Playbooks orchestrate response in real-time, adapting the actions organizations need to take in response to cyberattacks as they unfold.

If you are a victim of ransomware, the FBI and other law enforcement agencies advise victims to avoid paying a ransom to cybercriminals. They do recommend you report a cybercrime, including becoming the victim of ransomware to the appropriate authorities:

- In the U.S. report via the FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/default.aspx
- In Europe report via Europol's Cybercrime Reporting website: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About the Study

The survey was designed with Ketchum Global Research and Analytics. Data collection was conducted by Braun Research Inc. (business audiences – 600 completes) and ORC International (consumer audience – 1,021 completes).

The margin of error for the study for the total business audience is +/- 3.88% at the 95% confidence level (and +/- 5.5% at the 95% confidence level for individual company sizes). The margin of error for the consumer study is +/- 3.07% at the 95% confidence level.
