50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*