Données : Le vol d'identifiants est à la base de deux attaques sur trois

Deux violations de données sur trois sont réalisées par des hackers ayant utilisé des identifiants volés ou détournés, d'après l'édition 2014 du DBIR (Data Breach Investigations Report) de Verizon. *« Tenter d'obtenir des identifiants valides est à la base de la plupart des types d'attaques étudiés »*, explique **Jay Jacobs**, analyste chez Verizon et co-auteur du rapport.

1 367 violations de données

Sur **63 437 incidents de sécurité informatique** étudiés l'an dernier dans plus de 95 pays, **1 367 violations de données** ont été confirmées (contre 621 lors de la précédente édition bien moins étendue).

En 2013, la majorité des incidents a concerné des **identifiants volés** (422 attaques l'année dernière, contre 203 en 2012). Suivent : le vol de données par **malwares** (327 attaques, contre 183 en 2012), le **phishing** (245 contre 181), le « **RAM scraping** » ou collecte de données stockées en RAM (223 attaques, contre 27) et les logiciels pour ouvrir des **backdoors** – le seul mode d'attaque du top 5 ayant baissé (165 en 2013, contre 209 en 2012).

9 types d'attaques

Avec le recul, **92% des 100 000 incidents examinés ces dix dernières années** par l'opérateur télécom américain et 50 organisations dans le monde – de l'US-CERT au Centre européen de lutte contre la cybercriminalité (EC3) – **correspondent à 9 types d'attaques** seulement, à savoir : l'**intrusion des points de vente** (à travers les terminaux de paiement comme dans l'affaire Target), les attaques par **web apps**, les attaques d'**initiés**, la perte ou le **vol de données**, les attaques liées à des **erreurs diverses**, l'utilisation de **logiciels malveillants**. Mais aussi le détournement de **cartes de paiement**, les attaques par **déni de service (DoS)** et, enfin, le **cyberespionnage**.

Alors que la distribution est l'activité la plus ciblée par les attaques de points de vente, les médias et le secteur financier sont davantage sujets aux attaques web et en déni de services. L'industrie de la santé doit faire face au vol de données par malwares. Tandis que la production et l'industrie lourde sont plus touchées par le cyberespionnage et les attaques par saturation.

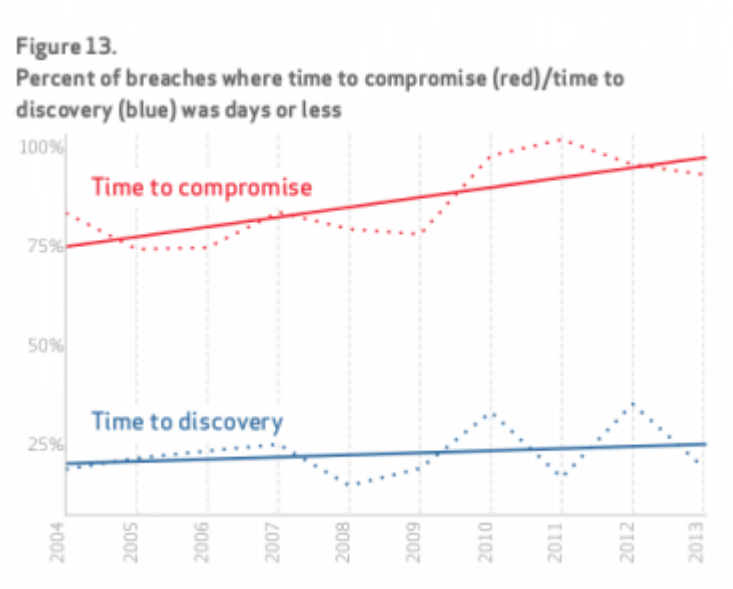
Figure 19.
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	26%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	42%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

For more information on the NAICS codes (shown above) visit: https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

Les hackers prennent l'ascendant

Les cybercriminels sont **plus efficaces et mieux armés**, alors que les entreprises peinent à assurer la sécurité de leurs réseaux et systèmes d'information, en témoigne l'attaque contre Target en décembre 2013. *« Les pirates sont plus affûtés et plus rapides, leurs victimes potentielles n'innovent pas aussi vite »*, commente Jay Jacobs. *« Les attaques sont plus complexes, plus sophistiquées et étendues. Les cybercriminels prennent l'ascendant »*, ajoute-t-il.



Dans les trois quarts des cas, **les cybercriminels mettent quelques jours pour atteindre leur cible**, voire moins, d'après le rapport 2014 de Verizon. Les organisations qui en sont victimes le découvrent en quelques jours ou moins, mais dans un quart des cas seulement.

Lire aussi

Faille Heartbleed : la check-list pour s'en sortir