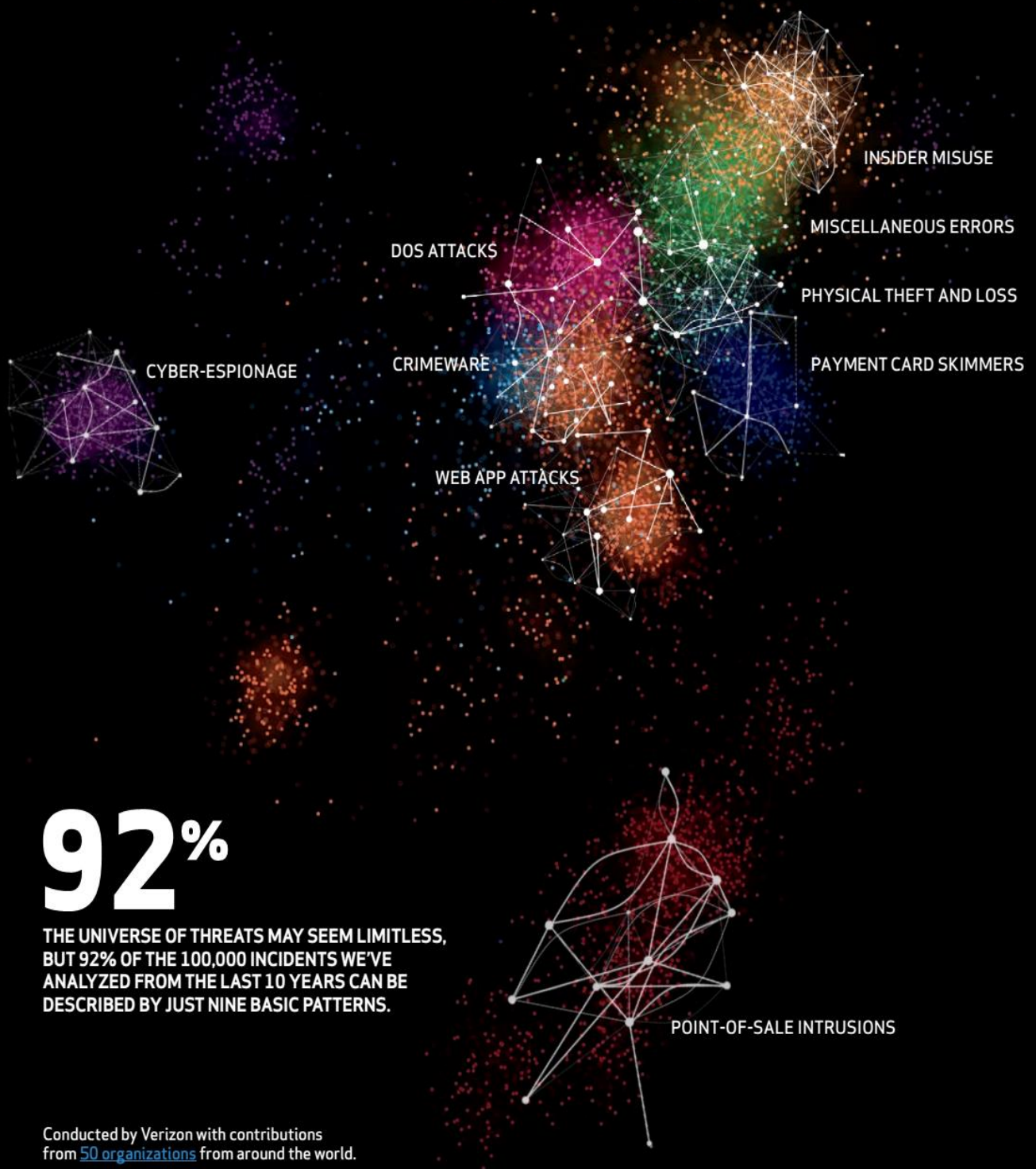
2014 DATA BREACH INVESTIGATIONS REPORT



92%

THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.

Conducted by Verizon with contributions from 50 organizations from around the world.

2014 DATA BREACH

INVESTIGATIONS REPORT

تقرير التحقيقات في خرق البيانات لعام 2014

محتويات البحث:

تمهيد

يقوم مركز أمن المعلومات في الهيئة الوطنية لخدمات الشـبكة بإعداد دراسـات دورية في مجال أمن المعلومات وتوثيق الاختراقات الحاصلة في هذا المجال بطريقة علمية احترافية.

ونظراً لأهمية موضوع أمن المعلومات وضرورة العمل الدائم على نشر الوعي في هذا المجال للأفراد والمؤسسات على حدٍ سـواء، فقد قام المركز بترجمة واختصـار الدراسـة المقدمة من مؤسـسـة Verizon المتخصـصـة في مجال أمن المعلومات عن اختراقات البيانات الحاصلة خلال عام 2013.

وجميع المعلومات الواردة في التقرير هي نقلاً عن التقرير الأساسي من مؤسسة Verizon والموجود على الرابط التالي:

http://www.verizonenterprise.com/DBIR/2014

مقدمة

نقدم لكم التقرير السنوي الخاص عن التحقيقات في مجال خرق أو انتهاك البيانات لعام 2014. حيث كانت أول نشرة أمنية قد تم اصدارها في هذا المجال عام 2008، ونأمل في هذا العام ان تكون هذه النشرة من شأنها تحسين الوعي والممارسة في مجال أمن المعلومات ودعم القرارات.

حيث تتألف مجموعة البيانات التي تدعم هذا التقرير بأكثر من 63.000 من الحوادث الأمنية المؤكدة. وهذا الرقم ليس من قبيل التخويف ولا يعتمد فقط على تأكيد لخروقات في البيانات ولكن هذا التطور في التقرير يعكس تجربة العديد من ممارسي الأمن والمديرين التنفيذيين الذين يعرفون أن هذا الحادث ليس من الضروري أن يؤدي إلى فلترة لهذه البيانات من أجل أن يكون لها تأثير كبير على الأعمال المستهدفة.

حتى تستطيع فهم ما نأمل فقد حضرنا مجموعة بيانات لهذا العام 2013 ثم نقدم عدد قليل من العينات السكانية وذلك لنحصل على المنحى مع مجموعة البيانات. المقطع التالي يجسد 10 أعوام من حوادث البيانات التي قد تكون مفضلة لدينا. سنقوم بعد ذلك بتقديم تحليل لأنماط تصنيف الحادث السالف الذكر وننتهي مع بعض الاستنتاجات ونمط السيطرة الأمنية على أساس ممارسة رسم الخرائط.

نظرة إلى عام 2013:

في تقييم شامل لعام 2013 كان عام من الانتقال من الهجمات الجيوسياية إلى هجمات واسعة النطاق على أنظمة بطاقات الدفع.

- شهر كانون الثاني:

وشهد سلسلة من تقارير عن هجمات مستهدفة من قبل جهات فاعلة ربما كانت ترعاها الدولة.

حملة تجسس أكتوبر الأحمر السيبرانية (Red October cyber) كانت مسؤولة عن استهداف وكالات الحكومة والمؤسسات البحثية على الصعيد العالمي ولكن في البلدان الناطقة باللغة الروسية على وجه الخصوص، حيث كانت هناك سلسلة مختلفة من الهجمات بدءا من هجوم (watering hole) على الموقع الالكتروني (cfr.org) لمجلس العلاقات الخارجية. وفي الوقت نفسه كانت كتائب عز الدين القسام السيبرانية (QCF) في المرحلة الثانية من عملية أبابيل لحجب الخدمة Ababil Distributed Denial of Service (DDoS) حيث مارست هجمات على شركات الخدمات المالية في الولايات المتحدة.

➢ شباط:

زودت segue في شباط الماضي صحيفة نيويورك تايمز ووول ستريت جورنال، مع تقارير جديدة من هجمات التجسس السيبرانية. وذكرت Sophos في تقرير لها أن حصان طروادة (Trojan) جديد قد وضع لمهاجمة أنظمة نقاط البيع (Point-Of-Sales) باستخدام معالج بطاقة الدفع الكندية.

أيضا تعرض موقع www.iphonedevsdk.com لهجمات من نوع (watering hole)، وذلك باستخدام هجوم مفاجئ على جافا في وقت متأخر من الشهر.

وكما صدرت في بداية شباط تقارير لخروقات في البيانات من الشركات الكبيرة فيس بوك، توتير، مايكروسوفت، أبل، ...

➢ آذار:

- خمسين مليون مستخدم ل Evernote أجبروا على تغيير كلمات السر لحساباتهم.
- يوم 20 آذار، عانت جمهورية كوريا من هجوم إلكتروني على نطاق واسع الذي أدى إلى تلف الأقراص.
- في نهاية آذار أدى هجوم سيبراني Cyberbunker-CloudFlare-Spamhaus DoS attack إلى قطع الانترنت.
- ذكرت مجموعة IB- عن تروجان يدعى "تفريغ الذاكرة المنتزع" (الملقب BlackPOS)، واستهداف نقاط بيع جديدة، وتصدر هذا الخبر في العناوين الرئيسية للصحف اليومية.

➢ نيسان:

- في نيسان سجل خرق جديد في نقاط البيع POS للدفع الالكتروني في الولايات المتحدة الأمريكية.
- الجيش السوري الالكتروني (SEA) يلحق بعض الضرر عندما خطف حساب التويتر لوكالة اسوشيتد برس، وإرسال تغريده عن انفجار في البيت الأبيض مما سبب تشنج في وول ستريت.
- أيضا استمرت عملية أبابيل من قبل كتائب عز الدين القسام (QOC) بواسطة هجوم حجب الخدمة DOSعلى العديد من البنوك الأوربية.

➢ أيار:

- واصلت التجسس السيبرانية هجماتها في شهر أيار، وذلك حسب التقارير الواردة من شركة QinetiQ وفريق مهندسي الجيش الأمريكي.

- خطف الجيش السوري الالكتروني SEA حسابات تويتر من كلا الجارديان والفاينانشيال تايمز.
- أيضـا قام فريق سـايبر للتجسـس عن طريق هجوم (watering hole) باسـتهداف الباحثون في الأسـلحة النووية في الولايات المتحدة الأمريكية، وربما الصين أيضاً.
- وشـملت أكثر التقارير عن عمليات التجسـس السـيبرانية في أيار عمليات هجومية على الباكسـتان ومنغوليا والعمليات التي تقوم بها الجهات الفاعلة Sunshop ضد نشطاء التبت.

➢ حزيران:

– في مطلع حزيران ذكرت تقارير عن حصول خروقات جديدة في أنظمة الدفع الالكتروني في عدد من مخازن البقالة في كل من كاليفورنيا ونيفادا في الولايات المتحدة الأمريكية.

- حملة التجسـس السـيبرانية العالمية وعن طريق هجمات NetTraveler التي تسـتهدف الديبلوماسـيين في الدول التي لها مصالح لا تتماشى مع الصين.

➢ تموز:

– قد تم تسجيل أكبر عملية خرق للبيانات في الولايات المتحدة بواسطة شركة Harbor Freight وهي شركة أمريكية لبيع الأدوات وتم أيضـا اختراق 445 متجر أي ما يقارب 200 مليون عميل ولم يعرف كيفية الوصـول لسجلات هؤلاء.

- بدأت الحملة الرابعة لعملية أبابيل عن طريق QCF كتائب القسـام. والجيش السـوري الالكتروني يخترق سجلات viberو tango .
- اتهمت وزارة العدل الأمريكية أربعة روس وواحد أوكراني بتهمة خرق سـجلات البيانات لأنظمة الدفع في Heartland and Global Payments.

➢ آب:

– الجيش السـوري الالكتروني SEAيسـرق الحسـاب الرسـمي على التويتر لكل من سـي ان ان CNN وواشنطن بوست ومجلة التايم و صحيفة نيويورك تايمز ونيويورك بوست.

- استهداف قمة الثمانية الكبار التي عقدت في سان بطرس برغ في روسيا من قبل التجسس السيبرانية.

➢ أيلول:

- شركة فودافون للاتصالات تبلغ مليونين من عملائها بانتهاك الحسابات الشخصية والمالية لهم.
- ارتباط جديد للاستخبارات في هجوم على شركة BIT9للحماية، وهجومات أخرى على المؤسسات المالية اليابانية.
- عملية اختراق تطال كبرى الشركات الأمريكية مثل: Lexis-Nexis،Kroll ، & Dun and Bradstreet.
- شركة Cryptolocker كان أول ظهور لها في شهر أيلول، حيث قامت بابتزاز الضحايا التي كانت على استعداد لدفع المال لفك تشفير الملفات الأساسية الخاصة بهم.

➢ تشرين الأول:

- أعلنت شركة أدوبي أنها قد انتهكت أنظمتها؛ وفي نهاية المطاف تم تحديد 38 مليون عدد من الحسابات المتضررة.
- انتصاران كبيران الأول هو اعتقال ديمتري "كرش" فيدوتوف في روسيا والمسؤول عن استغلال blackhole وهي برمجيات خبيثة انتشرت في الحواسيب وظهرت آثار حزمة برمجيات الجريمة في انفجار جرائم الإنترنت على مدى السنوات القليلة الماضية، الثاني هو اغلاق موقع طريق الحرير وهو سوق الإنترنت السوداء حيث تم استضافة ما يقرب من 13.000 من قوائم المبيعات للمواد الخاضعة للرقابة، بما في ذلك الماريجوانا، والهيروين والكوكايين والمخدرات بأنواعها.

➢ تشرين الثاني:

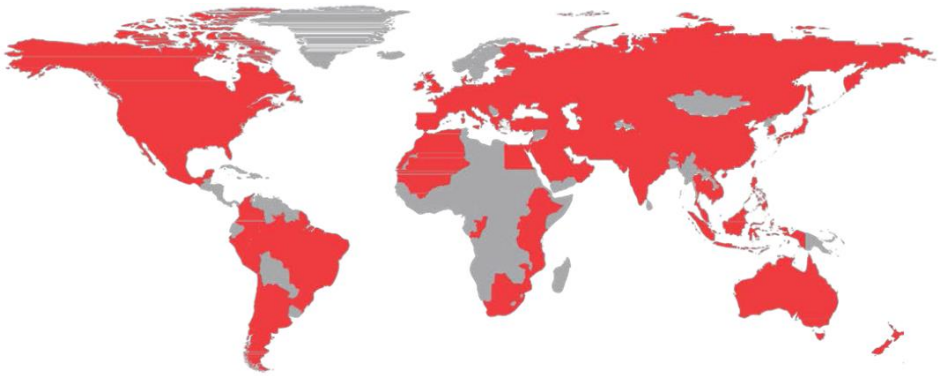
تطوير برامج مصرفية خبيثة حيث تعرض BIPS معالج الدفع الأوربي الرئيسي لواحدة من أكبر عمليات السطو.

➢ كانون الأول: كان دخولا قويا للتجسس السيبراني لعام 2013 حيث تم استهداف وزارت الخارجية في البلدان الأوروبية من خلال عملية Ke3chang.

التوزع الجغرافي للمنظومات المستهدفة

لقد أظهر تقرير BRID 2013 خروقات في المنظمات التابعة ل 27 دولة في العالم، وفي هذا العام نجد في هذا التقرير صعود بنسبة 350% عن العام الماضي، وذلك في 95 دولة مختلفة في العالم، كما يوضح الشكل رقم 1. حيث يوجد أكثر عدد من فرق الاستجابة للطوارئ لأمن الحواسيب الوطنية CSIRTs من أي وقت مضى.

ولكن ليس بهذه البساطة وذلك لأن الدقة والتركيز والأساليب وأشياء أخرى تختلف بين مجموعات ال CSIRTs المختلفة.



الشكل رقم 1: البلدان الممثلة في عدد القضايا الأمنية مجتمعة

المناطق باللون الأحمر هيَ مناطق يوجد فيها حوادث أمنية.
المناطق باللون الرمادي هيَ مناطق غير مصابة.

Industry	Total	Small	Large	Unknown
Accommodation [72]	212	115	34	63
Administrative [56]	16	8	7	1
Agriculture [11]	4	0	3	1
Construction [23]	4	2	0	2
Education [61]	33	2	10	21
Entertainment [71]	20	8	1	11
Finance [52]	856	43	189	624
Healthcare [62]	26	6	1	19
Information [51]	1,132	16	27	1,089
Management [55]	10	1	3	6
Manufacturing [31,32,33]	251	7	33	211
Mining [21]	11	0	8	3
Professional [54]	360	26	10	324
Public [92]	47,479	26	47,074	379
Real Estate [53]	8	4	0	4
Retail [44,45]	467	36	11	420
Trade [42]	4	3	0	1
Transportation [48,49]	27	3	7	17
Utilities [22]	166	2	3	161
Other [81]	27	13	0	14
Unknown	12,324	5,498	4	6,822
Total	**63,437**	**5,819**	**47,425**	**10,193**

الشكل 2: جدول يوضح عدد الحوادث الأمنية بالمقارنة بين طبيعة عمل المنظومة الضحية وحجم المنظمة لعام 2013.

Industry	Total	Small	Large	Unknown
Accommodation [72]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	**1,367**	**243**	**144**	**980**

الشـــكل رقم 3: جدول يؤكد عدد الحوادث الأمنية مع خروقات بيانات مؤكدة وذلك بالمقارنة بين طبيعة عمل المنظومة الضحية وحجم المنظمة لعام 2013.

Large: المنظمات التي تحوي على أكثر من 1000 موظف.

SMALL: المنظمات التي تحوي على أقل من 1000 موظف.

UNKNOW: غير معروف.

Some of victim industries : Agriculture / زراعة – Construction / إنشاءات – Education / تعليم – Real Estate / عقارات– Trade / تجارة– Transportation / نقل – Utilities / خدمات..

ولفهم معمق أكثر عن الجدول نأخذ مثالاً عملياً حيث في الشكل رقم 2 الجدول الأول السطر السابع، سنجد أنه يتحدث عن عدد الضـحايا الموجودين ضـمن القطاعات أو المنظمات المالية وعدد الحوادث الأمنية التي حصـلت ضـمن هذه القطاعات الكبيرة منها والصـغيرة (LARGE & SMALL) والمجموع العام للحوادث التي تعرض لها الضـحايا داخل المنظمات المالية (TOTAL).

بالتالي كان المجموع العام لهذه الأحداث في جميع المنظمات وعلى اختلاف طبيعتها وفي معظم أنحاء العالم والتي تعرضت لهجمات تجسسية 36.436. والمؤكدة منها كانت 1.367 حادثة كما في الشكل رقم 3.

حيث نلاحظ أن بعض المنظمات أو الجهات المالية تكون أكثر جاذبية من قبل الجهات الفاعلة للتجسـس عليها أو انتهاكها.

الجميع عرضـة لنوع من هذه الأحداث. حتى لو كنت تعتقد مؤسـستك في خطر منخفض للهجمات الخارجية، لا تزال هناك إمكانية سوء استخدام من الداخل والأخطاء التي تضر أنظمة وفضح البيانات.

A DECADE of DBIR DATA

عقد كامل على تقارير DBIR

يحاول هذا القسم من التقرير إنشاء مجموعة نتائج مشابهة قدر الإمكان لنتائج التقارير السابقة وذلك من حيث الصياغة والأسلوب، تشمل هذه النتائج في التقرير الحالي كلاً من الاختراقات التي حدثت بين عامي 2004-2012 بالإضافة إلى حوادث كشف البيانات المؤكدة في العام 2013 والتي بلغ عددها 1367 حادثة.

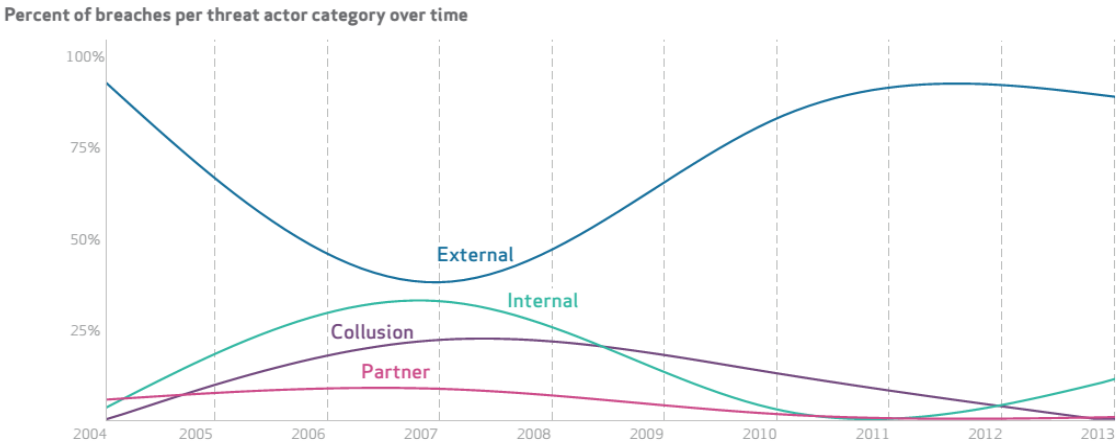
مقدمة مختصرة لكل من VERIS،VCDB :

VERIS: Vocabulary for Event Recording and Incident Sharing

مجموعة من المقاييس تم تصميمها بحيث تشكل توصيفاً للحوادث الأمنية بطريقة منظمة وقابلة للتكرار. إذاً جمع بيانات تفصيلية عن الحوادث الأمنية اعتماداً على مصادر متعددة و"ترجمة" هذه البيانات بأسلوب معين يتميز بالوضوح والمنهجية والدقة في العرض، يستخدم التقرير أسلوبVERISلعرض بعض الاحصاءات والبيانات.

VCDB: VERIS Community Database

مبادرة عامة لتنظيم بيانات الحوادث الأمنية على المستوى العمومي وعرضها باستخدام إطار العمل VERIS. إذاً فهي عبارة عن قاعدة بيانات أولية لآلاف الحوادث الأمنية يتم تشاركها بواسطة ترخيص عام للجميع بحيث يتاح تحميل هذه البيانات واقتراح حلول من أجل التطوير والتحسين.



يظهر الشكل السابق بيانات إحصائية عن السنوات العشرة السابقة توضح الاختراقات بدلالة نوع التهديد حيث نرى أربعة أنواع من التهديدات:

External: تهديد خارجي، Internal: تهديد داخلي، Collusion: تهديد متآمر، Partner: تهديد الشريك.

من الواضح بأن التهديدات ذات الطبيعة الخارجية حصلت على النسبة الأكبر للسنوات العشرة.

:BREACHES (VS) INCIDENTS

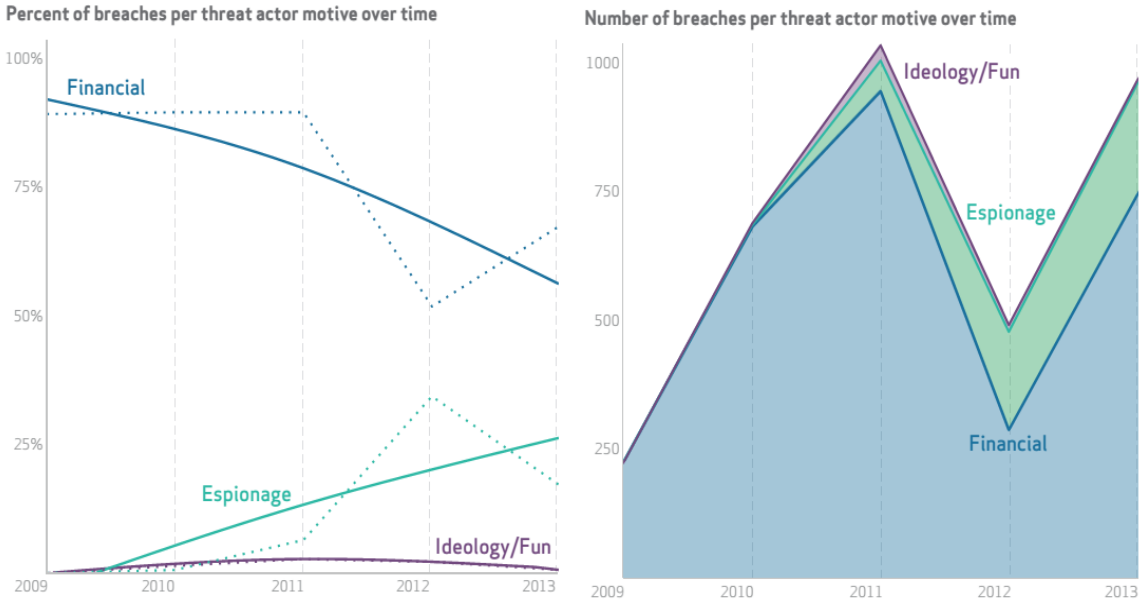
يستخدم التقرير العديد من المصطلحات سيصار إلى شرحها تباعا:

Incident: حدث أمني يقوم بالتأثير على التكاملية، الوثوقية والتوافرية للنظم المعلوماتية.

Breach: وهو عبارة عن Incident يؤدي بالنتيجة إلى الكشف أو التعرض المحتمل للبيانات.

Data Disclosure: وهو عبارة عن Breachقد قام بالفعل بكشف البيانات بشكل مؤكد وليس فقط التعرض لها.

إحصائية دوافع التهديدات الأمنية للسنوات الخمس الماضية:



الدوافع الثلاثة الأكثر شيوعا وتأثيراً:

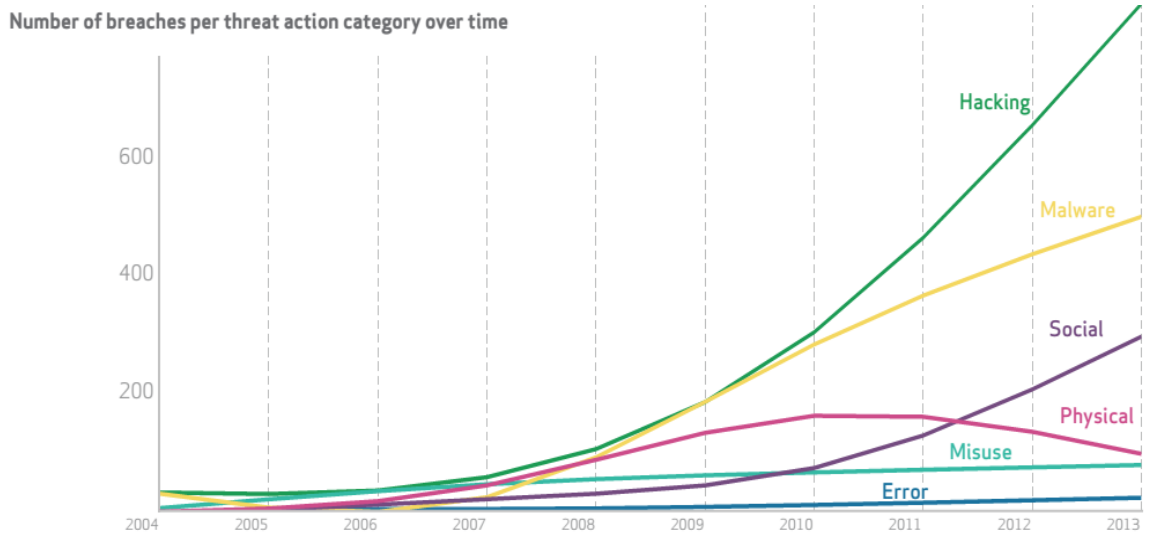
Financial: دوافع مالية ومصرفية، Espionage: دوافع تجسسية، Ideology/Fun: دوافع أخرى كالدوافع العقائدية والفكرية أو دوافع تتعلق بالتسلية والهواية.

من الواضـــح أن الدوافع التي تتعلق بالمال كبطاقات الدفع الالكتروني والعمليات المصـــرفية والتجارة عبر الشـــبكة قد سيطرت على الحصة الأكبر للسنوات الخمس بحسب الإحصائية السابقة.

الشكل الأول إلى اليمين: يظهر عدد الدوافع بالنسبة للسنوات الخمس الماضية.

الشكل الثاني إلى اليسار: يظهر النسبة المئوية بين الدوافع سابقة الذكر.

عدد الاختراقات بدلالة السلوك العملي للتهديد:



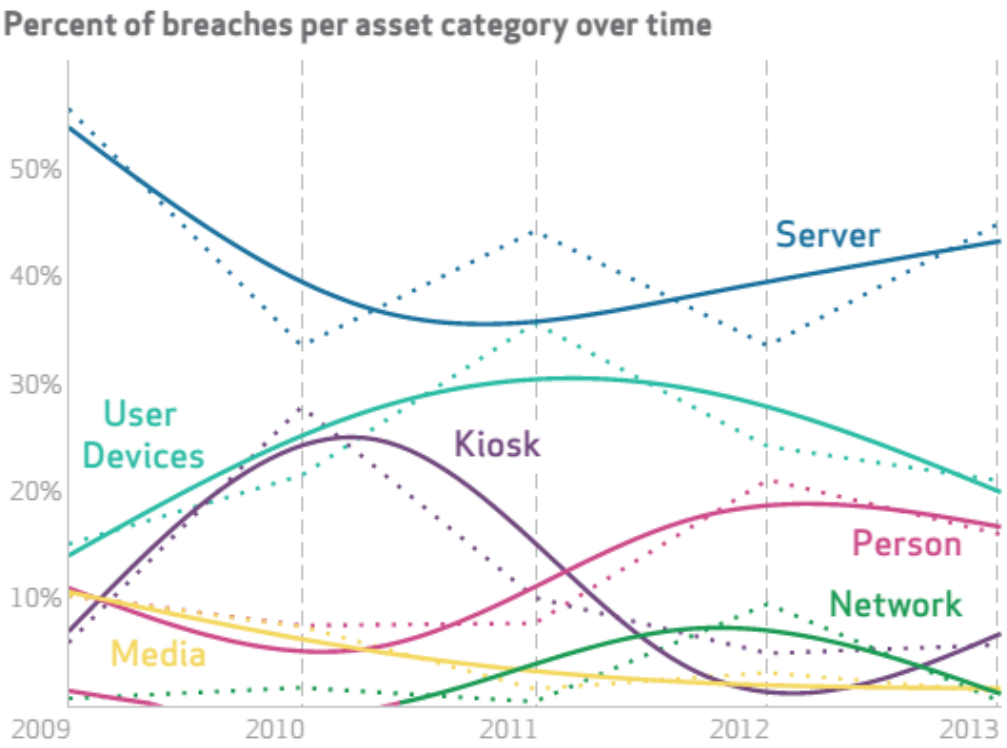
يوضح الشكل السابق عدد كل من الاختراقات بدلالة سلوكها العملي في السنوات العشر السابقة وهي:

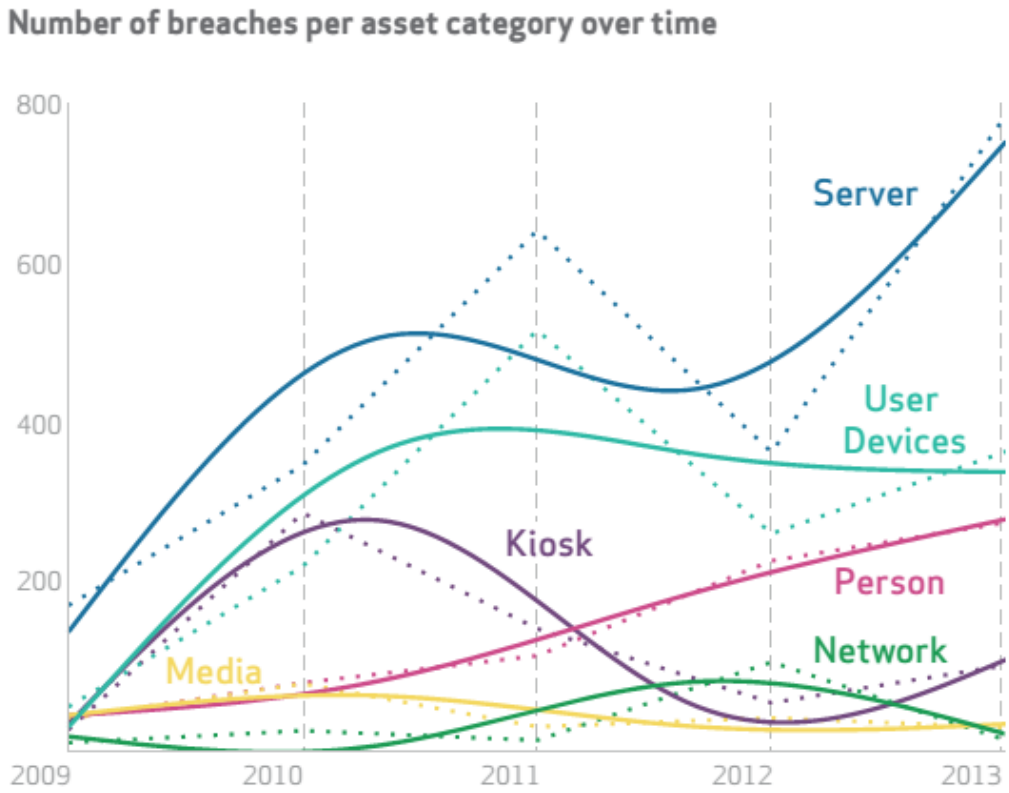
Hacking: الاختراق، Malware: البرمجيات الخبيثة، Social: الاختراقات ذات السلوك الاجتماعي كالهندسة الاجتماعية، Physical: السلوك الفيزيائي، Misuse: سلوك إساءة الاستخدام، Error: الأخطاء.

اعتماداً على الشكل السابق يبدو بأن عمليات الاختراق Hacking بأنواعها العديدة هي الأسلوب والطريقة المفضلة لدى المهاجمين لتنفيذ اختراقاتهم على مدى العقد السابق.

إحصائيات الاختراقات بحسب أنوع التجهيزات بدلالة الزمن وهو النصف عقد الأخير:

Server: مخدم، Kiosk: واجهة العمليات المالية الالكترونية، User Devices: التجهيزات المختلفة والمملوكة من قبل المستخدمين، Person: تجهيزات شخصية، Network: الشبكة والتجهيزات المكونة والرديفة، Media: تجهيزات الوسائط المتعددة:





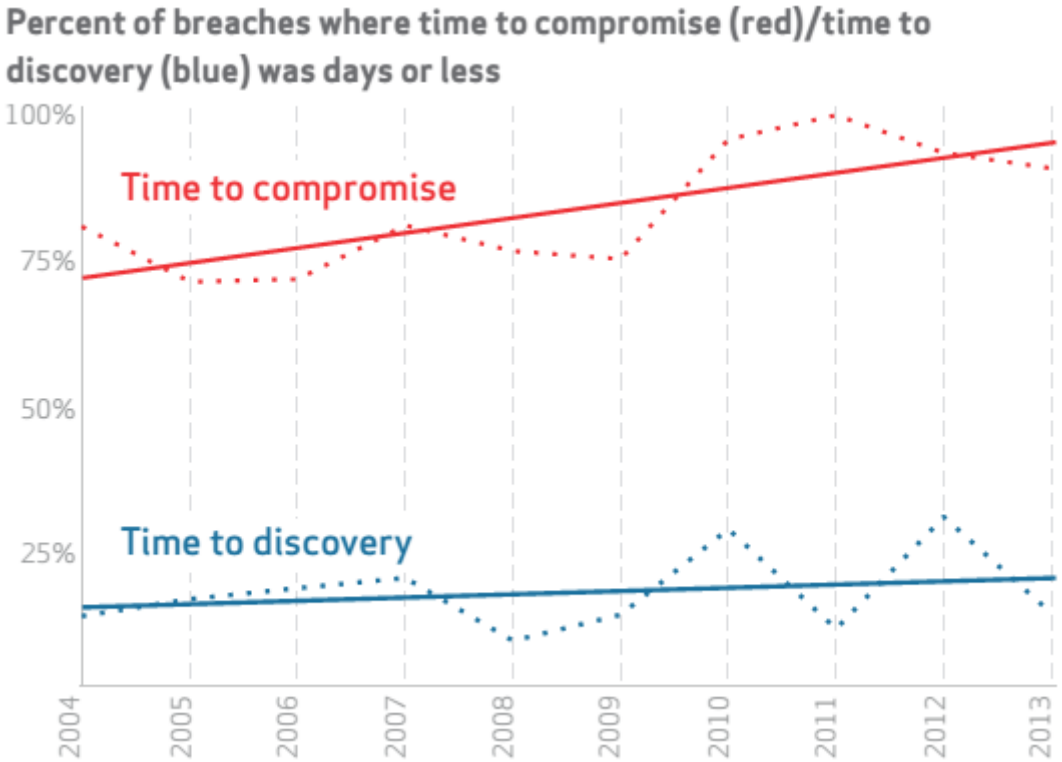
المخدمات كانت التجهيزات الأكثر عرضــة للاختراق في العقد الســابق بنســبة 53% تليها تجهيزات المســتخدمين ثم واجهات التعاملات الالكترونية فالتجهيزات الشخصية ثم الشبكات والتجهيزات الرديفة لها أما تجهيزات الوسائط المتعددة

فقط كانت الأقل اختراقاً وعليه يجب التأكيد على ضـرورة تطوير خطط ووسـائل حماية إضـافية للمخدمات لما تتمتع به هذه الأجهزة من أهمية بالغة على مستوى المنظومات والشبكات.

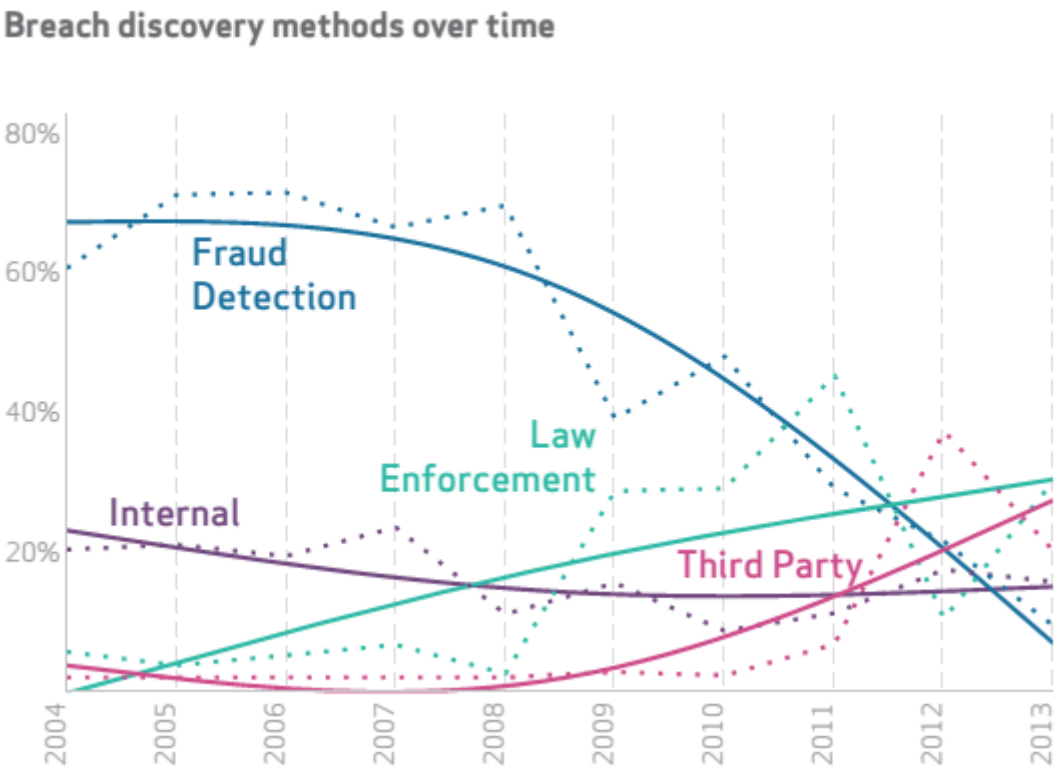
الاختراقات في العقد الماضي ممثلة بنسبة زمن الاختراق إلى زمن الكشف:

Time to compromise: الوقت اللازم لإنجاز عملية الاختراق.

Time to discovery : الوقت اللازم لكشف عملية الاختراق.



يبدو أن الفجوة الزمنية بين الوقت اللازم لإنجاز عملية الاختراق والوقت اللازم لكشف هذه العملية تعتبر كبيرة نسبياً كما يوضـح الشـكل وهذا يعني وجود مشـكلة حقيقية وهي عبارة عن تأخير زمني كبير بين المدافعين والمهاجمين أو بمعنى آخر يقوم المهاجم بإتمام عمله وبعد وقت طويل نسبياً يكتشف المدافع حدوث هذا الاختراق.



تمثيل الطرق الرئيسية لكشف الاختراقات خلال العقد الماضي:

يمثل الشكل السابق المنحنيات البيانية لطرق كشف الاختراقات بدلالة سنوات العقد الماضي حيث:

Fraud Detection: أساليب كشف الاحتيال.

Law Enforcement: الأساليب القانونية كالسياسات الأمنية العامة.

Internal: الأساليب والطرق الذاتية المتعلقة بالضوابط والسياسات الأمنية المطورة بشكل ذاتي فردي أو مؤسساتي.

Third Party: أساليب الكشف المنفذة من قبل جهة ثالثة كشركات الأمن والحماية.

الملاحظة الأساسية على البيانات السابقة هي الانخفاض شبه الحاد بنسبة طرق كشف الاحتيال بل وانخفاض هذه النسبة إلى ما دون الطرق الأخرى في كشف الاختراقات خلال العام 2013، وذلك لأن طرق الاحتيال تعتبر الأساليب المفضلة لدى المهاجمين عن بعد وخاصة في مجال الاختراقات المتعلقة بالأمور المالية والمصرفية وعليه يجب العمل على وضع مقترحات وخطط للعمل على تطوير هذه الطرق والأساليب بالشكل الأمثل.

RESULTS AND ANALYSIS

نتائج وتحليلات

تبدأ النتائج بعرض خلاصـــة بيانات العام 2013 أي الاختراقات التي حدثت في العام الماضـــي، مجموعة النتائج هذه كبيرة نســبياً وعليه تم الأخذ بعين الاعتبار تقليص وتحجيم النتائج ما أمكن من خلال العرض مقدار محدد من البيانات أي خلاصة نماذج الهجمات الأكثر أهمية وذلك اعتماداً على تركيبات معينة من المهاجم أو المسبب والأسلوب وطريقة الهجوم والهدف وتكرار الحدوث؛ بالنتيجة حصلنا على ثلاثة أنواع من الهجمات وتوصلنا إلى أن هذه الأنواع تحقق ما نسبته 68% من إجمال حجم البيانات، لنطلع على الشكل التالي:

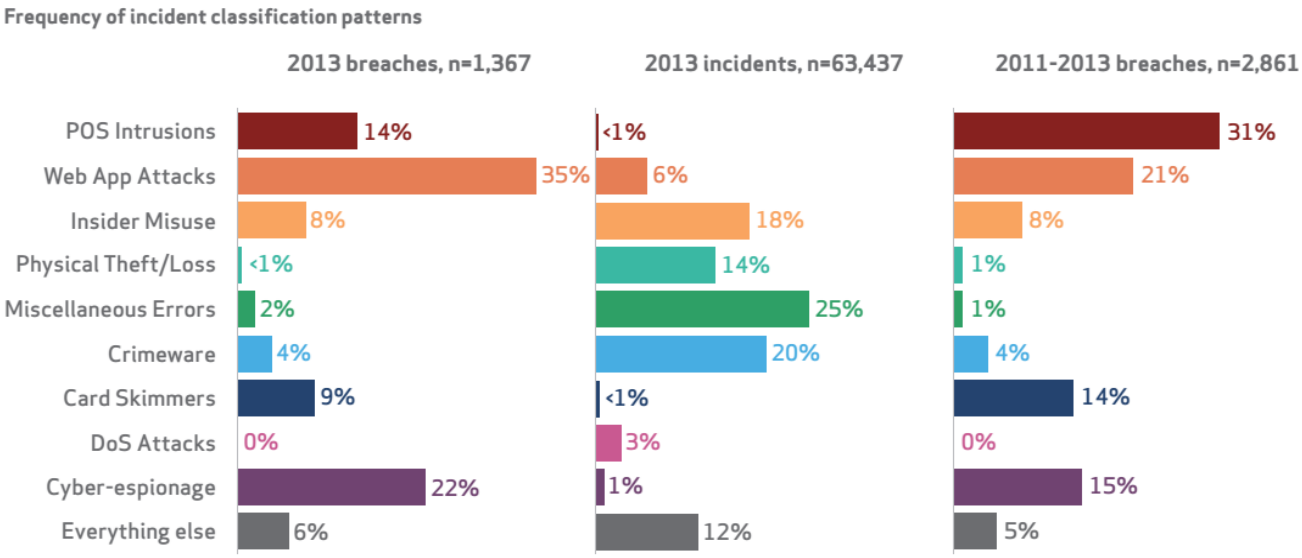
Scratch paper calculations from the 2013 DBIR for commonly-observed incident patterns

111	POS smash-and-grab
190	Physical ATM
+ 120	Assured Penetration Technique
421	
÷ 621	Total Breaches
68%	

لقد اعتمدنا على تعدادات بيانات نظام VERIS للحصـــول على تجمعات للبيانات Clusters حيث لاحظنا وجود تجميعات واضحة كعمليات الاصطياد الالكتروني والاجتماعي والعمليات المتعلقة بالبريد الالكتروني، والاهم كان البحث عن تجمعات للبيانات تقوم بوصف تصنيفات شاملة للحوادث الأمنية وليس مجرد حوادث أمنية متكررة...

وقد تم التوصل للنتيجة الهامة التالية:

نستطيع وصف (تسعة من عشرة) من مجمل الاختراقات بواسطة (تسعة) نماذج رئيسية.



يوضح الشكل السابق البيانات الخاصة بتردد ورود نماذج تصنيفات الحوادث الأمنية خلال العام 2013

POS Intrusions: اختراقات نقاط البيع

Web App Attacks: هجمات تطبيقات الويب

Insider Misuse: إساءة الاستخدام–هجمات المستخدمين الداخليين المرخصين

Physical Theft/Loss: الاختراقات الفيزيائية

Miscellaneous Errors: أخطاء متنوعة

Crimeware: البرمجيات الخاصة بالجرائم الالكترونية

Card Skimmers: ناسخي بيانات البطاقات الالكترونية

DoS Attacks: هجمات منع تقديم الخدمة

Cyber–espionage: التجسس السيبراني

Everything else: أي اختراقات أو حوادث أمنية لا تنتمي إلى التصنيفات السابقة.

الملاحظات: تجدر الإشارة إلى النماذج الأربعة الأولى وهي على الترتيب:

Web App Attacks_1: هجمات تطبيقات الويب،

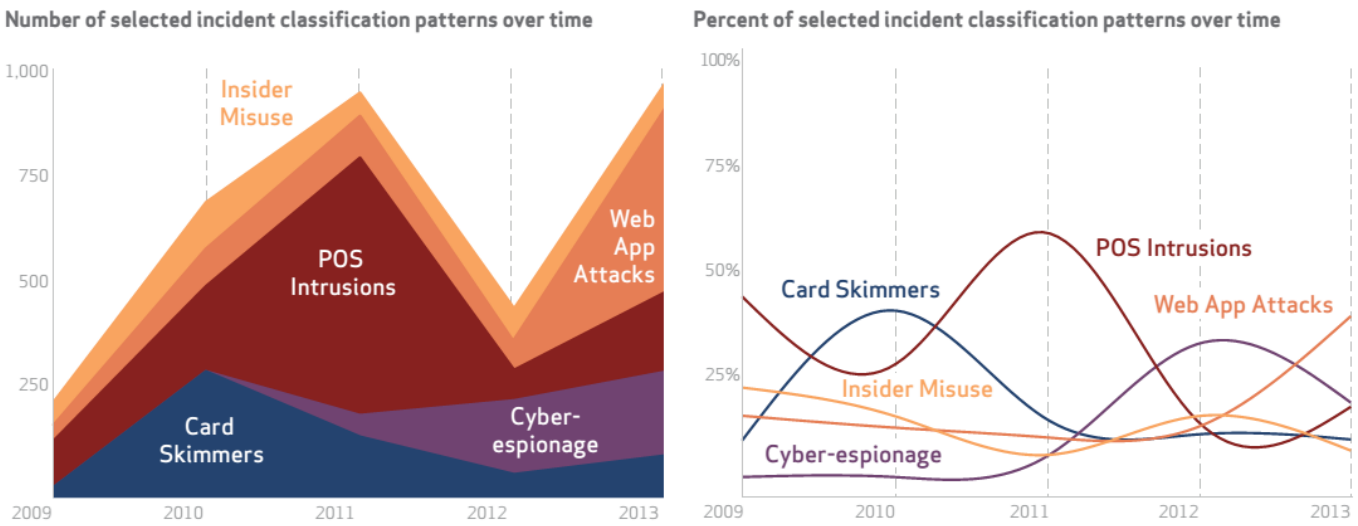
2_Cyber-espionage: التجسس السيبراني

3_POS Intrusions: اختراقات نقاط البيع،

4_Card Skimmers: عمليات قرصنة البطاقات.

وذلك على أساس معيار نوعية (البيانات المكشوفةData Disclosure) حصراً.

يبين الشكل البياني التالي مجموعة مختارة من نماذج التصنيفات السابقة منسوبة لنموها إلى الوقت:



الوقت: السنوات الخمس الماضية (نصف العقد الماضي).

تمت الإشارة فيما سبق إلى التصنيفات الأساسية للاختراقات والحوادث الأمنية على أساس معايير البيانات المكتشفة بشكل أساسي، يبين الشكل التالي هذه التصنيفات على أساس نوع وماهية الشركات المستهدفة، للاستزادة فيما يخص تصنيفات الشركات وأنواعها مراجعة نظام:

North American Industry Classification System :NAICS

Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING 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%	20%	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%	40%	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

العمود إلى اليسار يصنف الشركات المستهدفة بحسب نوعها أما الأعمدة التالية فهي عبارة عن نماذج تصنيفات الاختراقات والحوادث الأمنية التي تم الحديث عنها سابقاً.

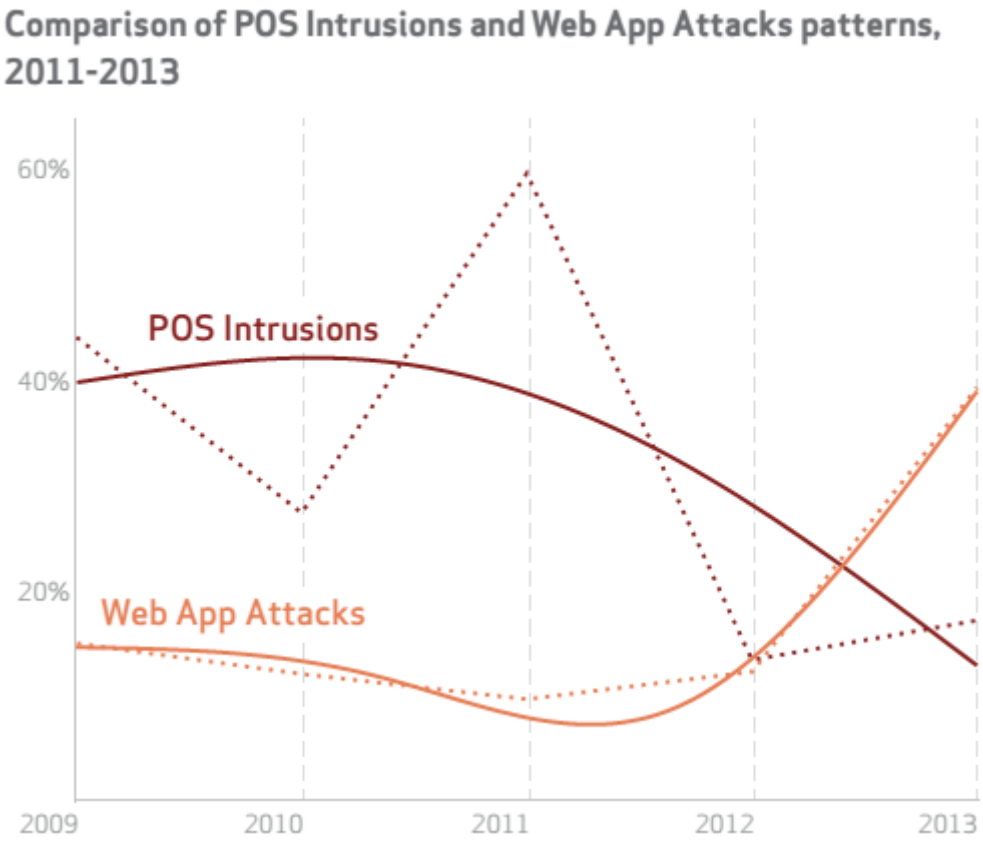
بالنسبة للألوان فقد اعتمد المصمم على تدرج لوني للنسب حيث النسب العالية تتميز بلون فاقع تليها النسب الأقل مباشرة بلون أقل سطوعاً وهكذا...

POINT-OF-SALE (POS) INTRUSIONS

اختراقات نقاط البيع

من المعروف أن نقاط البيع هي عبارة عن البنية التحتية المؤلفة من تجهيزات وبرمجيات موزعة ضمن مناطق جغرافية ومربوطة بأنظمة مركزية لإنجاز التعاملات والمناقلات ذات الحجم الصغير بواسطة بطاقات الكترونية خاصة، والتي تشكل بمعظمها تعاملات بالمستوى الفردي.

تتميز الهجمات على أنظمة نقاط البيع بأنها لا تملك التنوع الكبير الموجود لدى الهجمات على الأنظمة الأخرى كتطبيقات الويب والشبكات مثلاً، يعد هجوم "محاولة الاتصال البعيد عبر القوة الشاملة" الهجوم الرئيسي على أنظمة نقاط البيع بشكل عام Brute forcing remote access connections to POS؛ أما بالنسبة لعام 2013 فقد كانت هجمات الذاكرة بواسطة البرمجيات الخبيثة هي الهجوم الرئيسي A resurgence of RAM scraping malware.

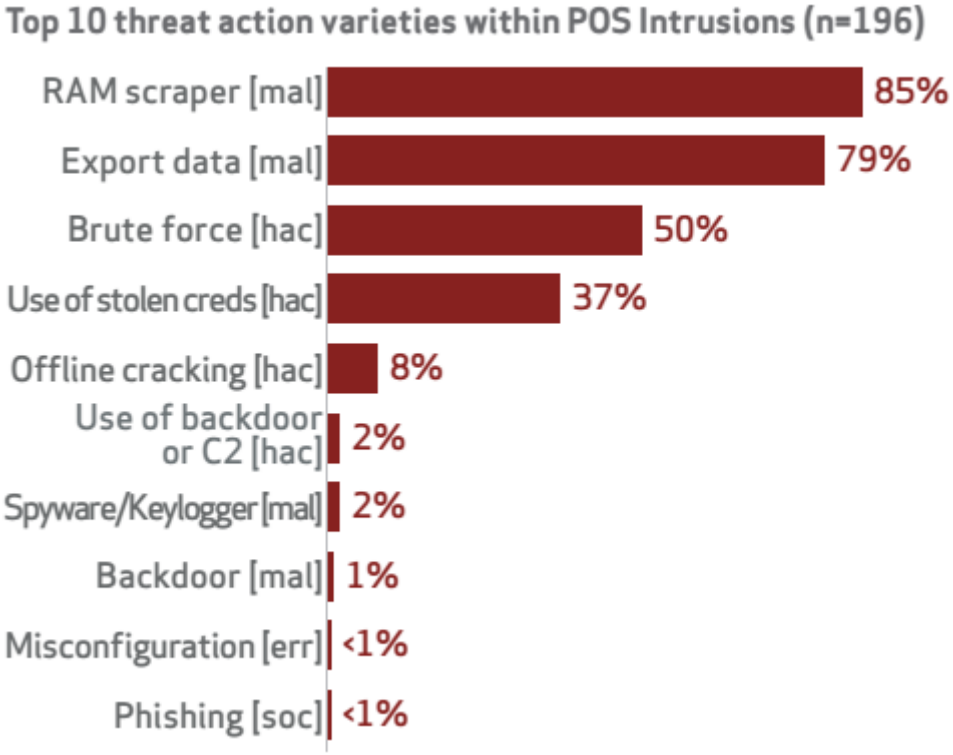


لمقاربة موضوع تراجع الهجمات على نقاط البيع مقارنة بالهجمات على الأنظمة الأخرى وضعنا البيانات النسبية ضمن شكل بياني (الشكل السابق) والذي يظهر نتائج مقارنة هجمات نقاط البيع بهجمات تطبيقات الويب خلال الأعوام الخمسة الماضية.

قام معدو هذا التقرير بدراسة 200 حالة من حالات الهجوم على أنظمة نقاط البيع التي حدثت في العام 2013 والتي كان معظم أهدافها عبارة عن الفنادق والمطاعم ومحلات بيع التجزئة بالإضافة إلى الشركات المتخصصة بإنشاء المباني.

المراحل الرئيسية لمعظم الهجمات على أنظمة نقاط البيع:

1. Compromise the POS device: السيطرة (السطو) على نقطة البيع الهدف.
2. Install malware: تنصيب برمجيات خبيثة.
3. Collect magnetic stripe data in process: جمع معلومات الشريط الممغنط قيد الاستخدام (حالياً).
4. Retrieve data: استعادة (جمع) بعض البيانات الضرورية لعملية الهجوم.
5. Cash in: تنفيذ العملية المالية.



التهديدات العشر الأولى (الشكل السابق) المستخدمة ضمن الهجمات على أنظمة نقاط البيع.

1) RAM scraper (mal): هجمات الذاكرة.
2) Export data (mal): جمع البيانات.
3) Brute force (hac): القوة الشاملة.
4) Use of stolen creds (hac): استخدام البطاقات المسروقة.
5) Offline cracking (hac): الاختراق بدون اتصال.
6) Use of backdoor or C2 (hac): استخدام الأبواب الخلفية.

7) Spyware/Keylogger (mal): أنظمة التجسس

8) Backdoor (mal): الأبواب الخلفية

9) Misconfiguration (err): الإعدادات الخاطئة

10) Phishing (soc): التصيد الالكتروني

Mal: برمجيات خبيثة، hac: اختراق، err: خطأ، soc: اجتماعي.

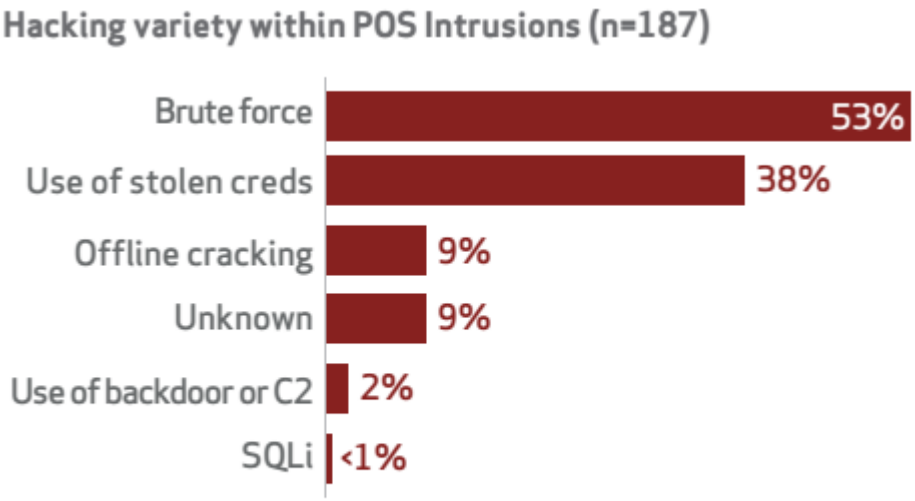
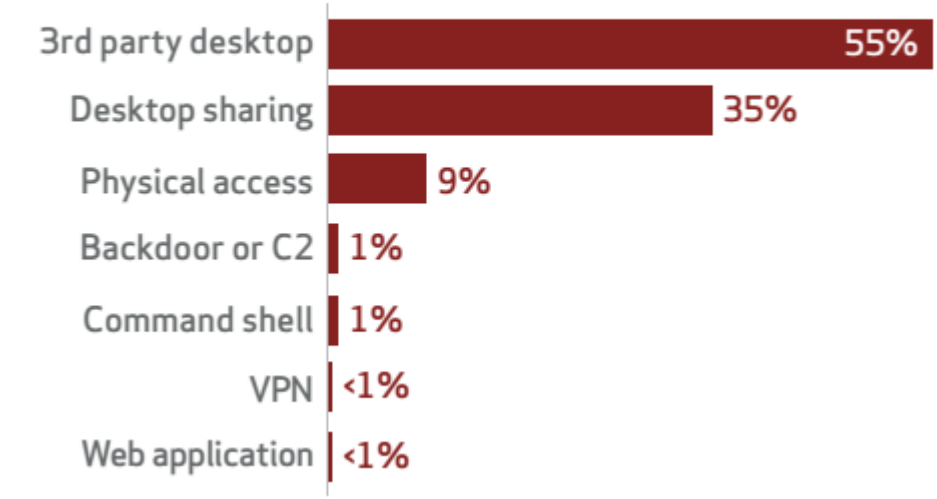


Figure 23.
Hacking vector within POS Intrusions (n=187)



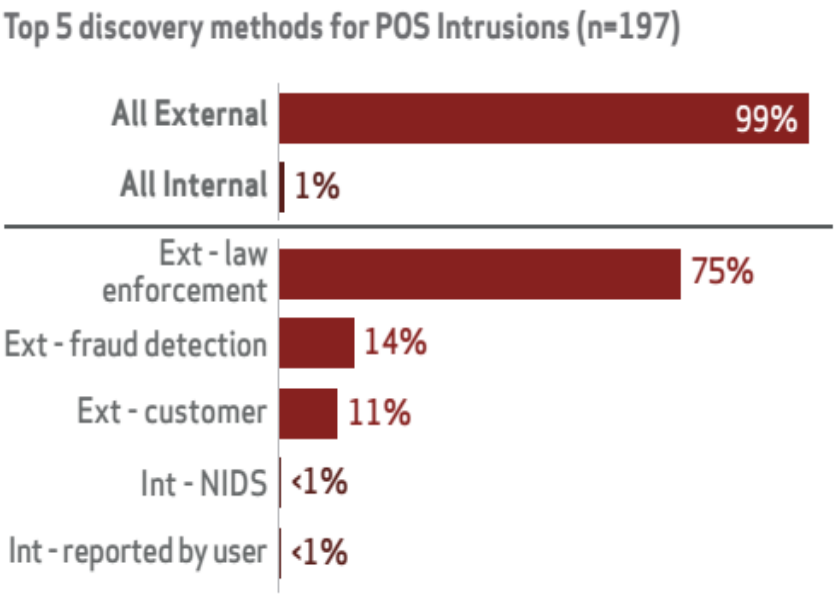
يبين الشكل السابق النسب المئوية لأنواع الاختراقات المتبعة في هجمات نقاط البيع بالإضافة إلى نسب الوسائل والأغراض المستخدمة في هذه الهجمات.

منهجيات كشف الهجمات على نقاط البيع:

منهجيات كشف الهجمات على نقاط البيع الخمس الأولى من حيث النسبة وهي:

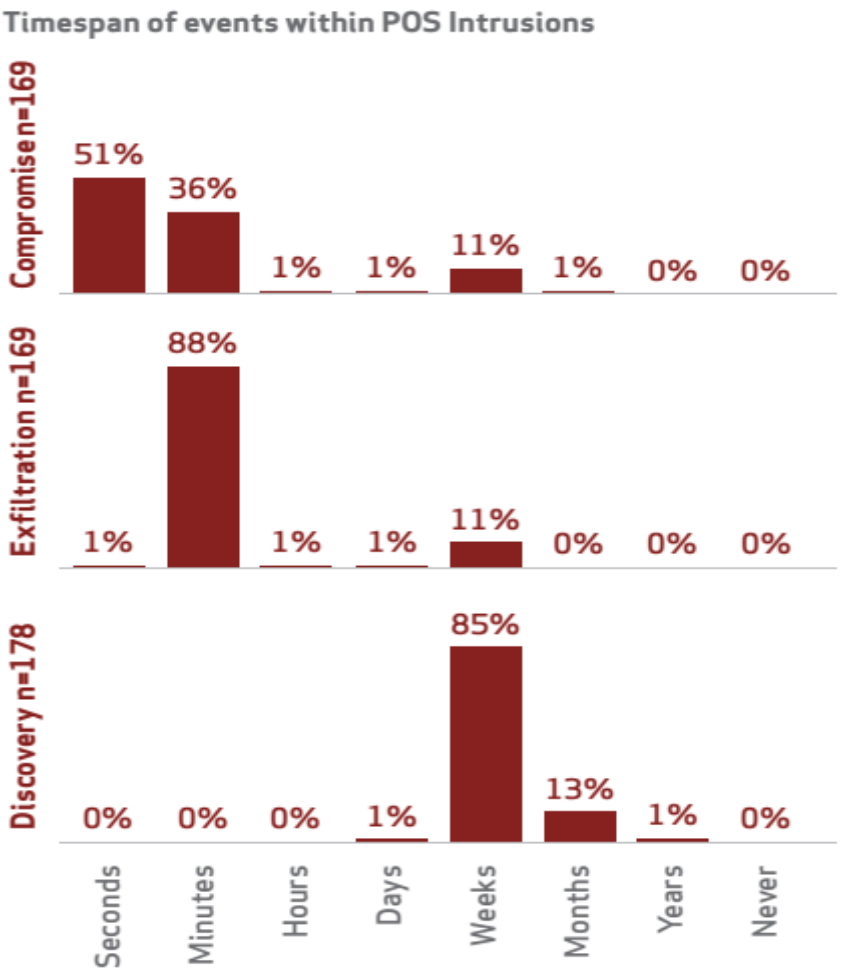
1. Ext – lawenforcement: فرض تطبيق القانون
2. Ext – fraud detection: إجرائيات لكشف عمليات الاحتيال
3. Ext – customer: المتعاملون.
4. Int– NIDS: أنظمة كشف عمليات التطفل.
5. Int – reported by user: التقارير الصادرة عن المستخدمين.

Ext: منهجيات خارجية، Int: منهجيات داخلية.



يبين الشكل نسب المنهجيات سابقة الذكر.

الشكل البياني الأخير في موضوع الهجمات على نقاط البيع يتعلق بعامل الزمن حيث تم تصميم هذا الشكل ليربط بين الوسائل المستخدمة في الهجمات Compromise Vectors ومنهجيات كشف هذه الهجمات Discovery Methods والزمن اللازم لكشف الهجمات.



➢ **توصيات وضوابط:**

مجموعة التوصـيات والضـوابط التي يوصـى بها بشـدة من أجل العمل على الحد من الهجمات وعمليات قرصـنة نقاط البيع:

التوصيات الخاصة بجميع الشركات:

- فرض قيود كافية على الوصول إلى نقاط البيع.
- تحقيق سياسة قوية وتطويرها باستمرار لكلمات المرور.
- عدم استخدام أنظمة نقاط البيع لغير مهمتها الأساسية.
- تنصيب وتحديث وإدارة أنظمة مكافحة البرمجيات الخبيثة بشكل دوري.

التوصيات الخاصة بالشركات الكبيرة متعددة الفروع:

- المراقبة الدائمة للوصلات بين الفروع والإدارة المركزية.
- البحث الدائم عن أي نشاط مشبوه على كامل الشبكة.
- تجهيز الشبكة بطريقتين من طرق التحقق من الهوية على الأقل

WEB APPLICATIONS ATTACKS

الهجمات التي تستهدف تطبيقات الويب

لدى دراســة الهجمات التي تســتهدف تطبيقات الويب في عام 2013 تبين أنه يمكن تقســيم هذه الهجمات إلى ثلاث مجموعات بحسب الدوافع والأسباب الكامنة وراء الهجمة:

1) **الهجمات ذات الدوافع المالية FINANCIALLY MOTIVATED ATTACKS:**

تشكل هذه الهجمات نسبة 33% من الهجمات التي تستهدف تطبيقات الويب وتهدف إلى حصول المخترق على المال والمكاسب المادية وتستهدف جميع وسائل الدفع الالكتروني أو الخدمات المصرفية، ويمكن للمخترق تنفيذ هذه الهجمات من خلال الوصول إلى واجهة التطبيق المصرفية الخاصة بالمستخدم أو من خلال استغلال الثغرات الأمنية في التطبيق المستخدم نفسه وغالباً ما تكون هذه الواجهات محمية عن طريق اسم مستخدم وكلمة مرور ويقوم المخترق هنا باستخدام وسائل معينة من أجل الحصول على بيانات المستخدم مثل تقنيات التصيد من خلال خداع المستخدم وذلك بتصميم واجهة تشبه واجهة المستخدم الخاصة بالمصرف الذي يتعامل معه وإرسال رابط إلى بريده الالكتروني يحثه على إدخال بياناته الشخصية ليتم إرسالها إلى حاسب المخترق بدل إرسالها إلى مخدم المصرف، كما يمكن للمخترق تنصيب برمجيات مؤذية تقوم بالتجسس وسرقة بياناته الشخصية وإرسالها للمخترق، كما يمكن أن يقوم المخترق بتنفيذ هجمة المسح الشامل Brute Force Attack للحصول على كلمة المرور الخاصة بالمستخدم كما يمكن أن يستخدم هجمة الحقن بلغة الاستفسار البنيوية SQL Injection أو غيرها من الوسائل.

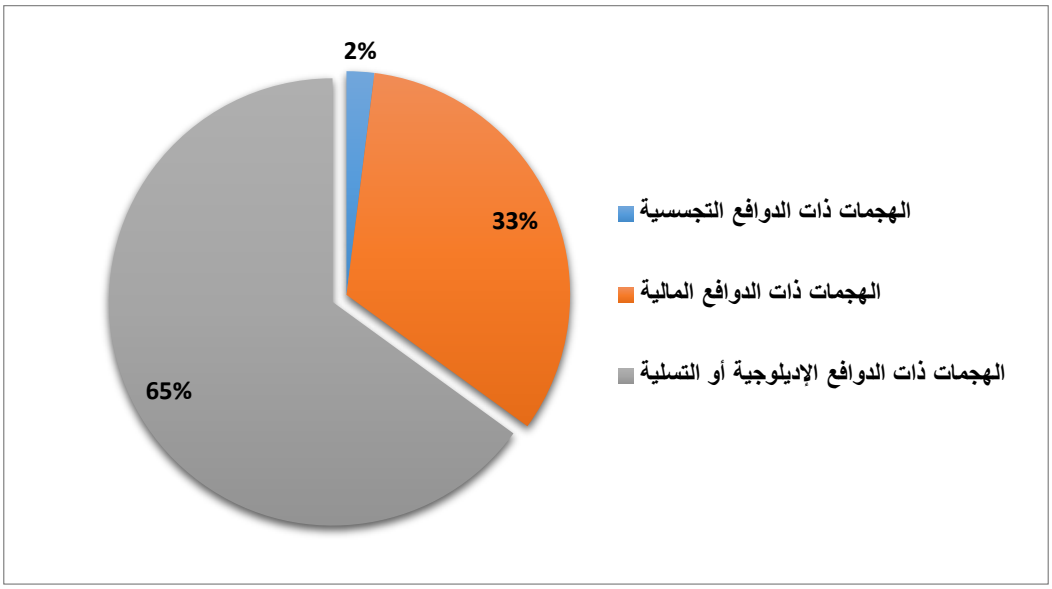
2) **الهجمات ذات الدوافع الإيديولوجية IDEOLOGICALLY MOTIVATED ATTACKS:**

ويمكن لأن تكون الأسباب ورائها سياسية أو اجتماعية أو مجرد التسلية وتحتل هذه الهجمات الجزء الأكبر من الهجمات التي تستهدف تطبيقات الويب حيث تشكل نسبة 65% منها، ويمكن أن تستغل هذه الهجمات العديد من الثغرات ضمن تطبيقات الويب على سبيل المثال عدم فلترة أو تدقيق المدخلات والمتغيرات التي تمرر للتطبيق سواء كان هذا التطبيق نظام إدارة محتوى Content Management Systems (CMS) مثل Joomla! ، Drupalأو WordPress أو غيرها من التطبيقات.

إن معظم حالات هذه الهجمات تستهدف مخدمات الويب وذلك لاختراق مواقع الكترونية محددة وإرسال رسالة معينة أو استغلال المخدم نفسه لإطلاق هجمات على أهداف أخرى مثل تنفيذ هجمات الحرمان من الخدمة الموزعة DDOS Attacks، ولكن هذا لا يعني التركيز فقط على حماية مخدمات الويب وإهمال تجهيزات الشبكة الأخرى كما لا يعني أن الشبكة لا تكون عرضة للاختراق في حال عدم وجود مخدمات ويب ضمنها.

3) الهجمات ذات الدوافع التجسسية:

تهدف هذه المجموعة من الهجمات إلى التجسس سواء على بيانات مستخدم محدد أو بيانات جهة ما وتحتل النسبة الأقل بين الهجمات التي تستهدف تطبيقات الويب لعام 2013 حيث تشغل نسبة 2% من هذه الهجمات كما يبين الشكل التالي النسبة المئوية للهجمات التي تستهدف تطبيقات الويب بحسب الدوافع الكامنة وراء هذه الهجمات:



الشكل يبين النسبة المئوية للهجمات التي تستهدف تطبيقات الويب بحسب الدوافع الكامنة وراء الهجمة

- **توصيات وضوابط:**

مجموعة من التوصيات الخاصة بتلافي الهجمات التي تستهدف تطبيقات الويب:

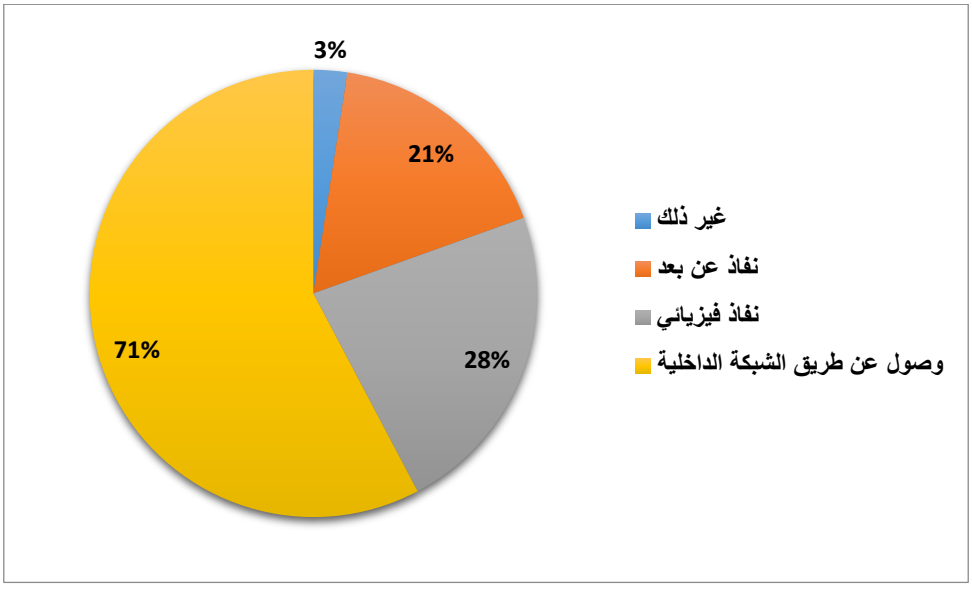
- استخدام أكثر من مستوى مصادقة وبتقنيات مختلفة وعدم الاكتفاء بالاعتماد على كلمات المرور للتحقق من هوية المستخدم وخصوصاً في الجهات التي تقدم خدمات مالية أو يتم تناقل بيانات مهمة عبر الشبكة ضمنها.
- يجب على مطوري الويب ومسؤولي المواقع الالكترونية إجراء مسح دوري لاكتشاف الثغرات الأمنية والعمل على تلافيها قبل اكتشافها واستغلالها من قبل المخترقين، كما يتوجب تفحص الكود المصدري لتطبيقات الويب والعمل على فلترة المدخلات ضمن الصفحات التي تسمح للمستخدم بإدخال بيانات ضمنها.
- يجب فرض سياسات معينة لمنع هجمات المسح الشامل على سبيل المثال السماح بعدد محدود من محاولات الإدخال.
- يجب على المستخدم العادي أو مدير الشبكة مراقبة الاتصالات الواردة أو الصادرة عن الحواسب والتجهيزات الشبكية مع ضرورة وجود تجهيزات حماية مثل الجدران النارية وأنظمة كشف/منع التطفل.

INSIDER THREATS

التهديدات الداخلية

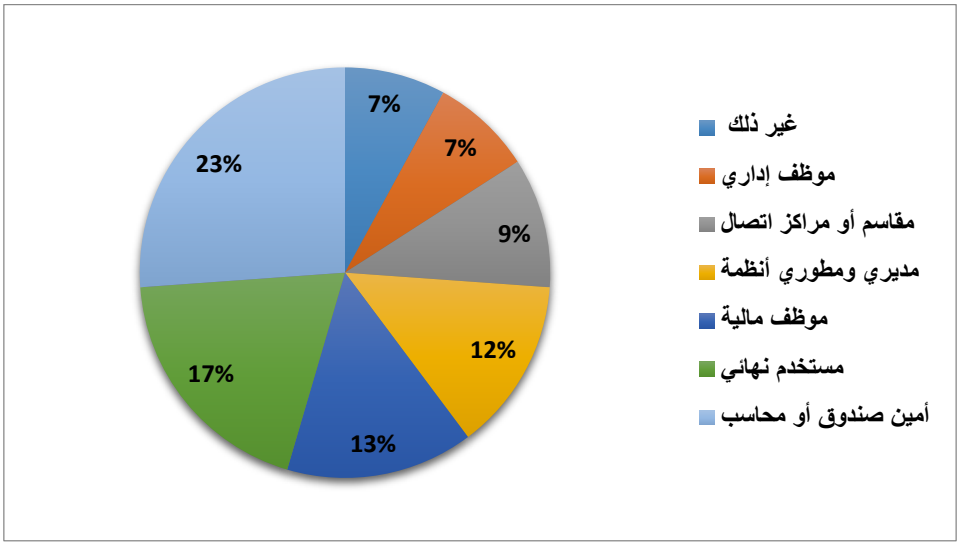
يتمثل هذا التهديد بشخص موظف لدى جهة ما أو أي شخص لديه معلومات أو صلاحيات معينة ضمن الجهة سواء كانت هذه الصلاحيات خاصة بالنفاذ إلى الشبكة الداخلية أو أي منظومة أو بيانات ضمن الجهة، حيث يقوم هذا الشخص أو الموظف باستغلال هذه الصلاحيات عن قصد أو عن طريق الاستخدام الخاطئ لها فيؤثر سلباً على سرية أو سلامة محتوى أو متاحية البيانات ضمن هذه الجهة.

لدى دراسة مجموعات إحصائية من عينات لحوادث ناتجة عن تهديدات داخلية تبين أن النسبة الأكبر من هذه الحوادث تتم عن طريق الوصول عبر الشبكات الداخلية للجهات المستهدفة والشكل التالي يبين ذلك:



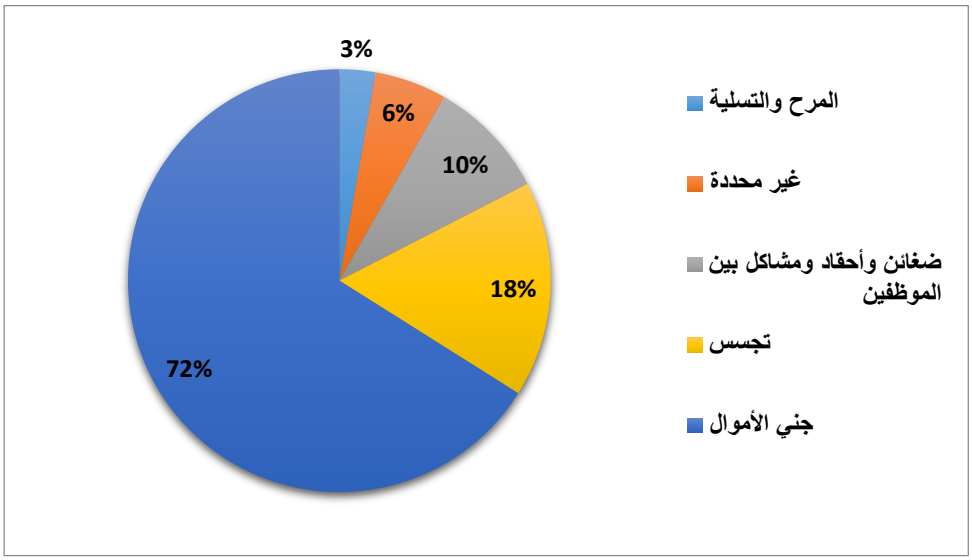
الشكل يبين نسبة الحوادث الناجمة عن تهديدات داخلية

كما تمت دراسة النسبة بين الأشخاص الذين يقفون وراء هذه الحوادث ضمن هذه الجهات وكانت النتائج كما في الشكل التالي:



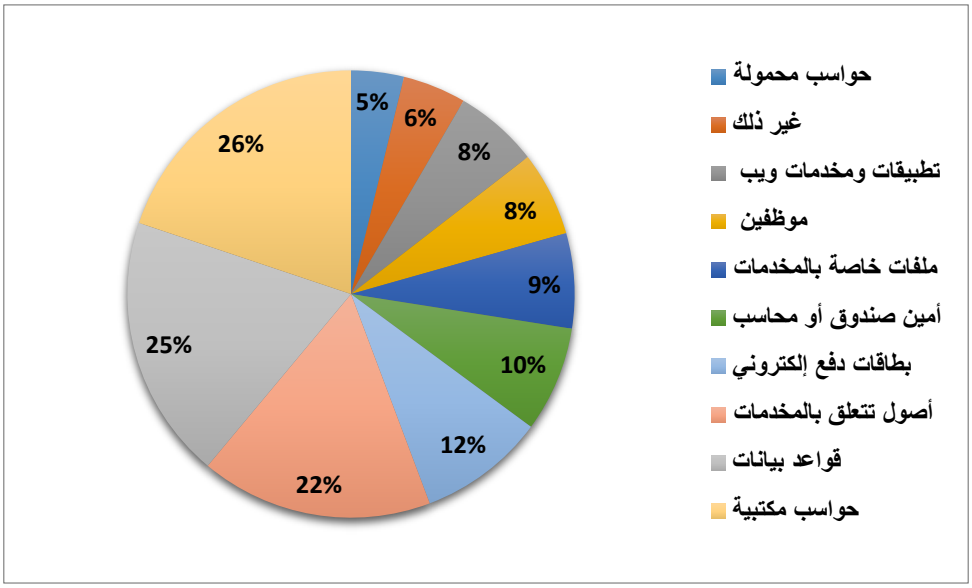
الشكل يبين النسبة بين الأشخاص الذين يقفون وراء الحوادث الناجمة عن تهديدات داخلية

وقد تمت دراسة عينات الحوادث الناجمة عن التهديدات والأخطار الداخلية بالنسبة للمحفزات والأسباب الكامنة وراء تنفيذ هذه الحوادث وقد تبين أن النسبة الأكبر بينها ذات محفزات مالية أي تهدف للكسب المالي والبعض الأخر أهدافه تجسسية بينما يهدف البعض منها إلى التسلية والمرح أو بسبب ضغائن ومشاكل بين الموظفين والشكل التالي يبين ذلك:



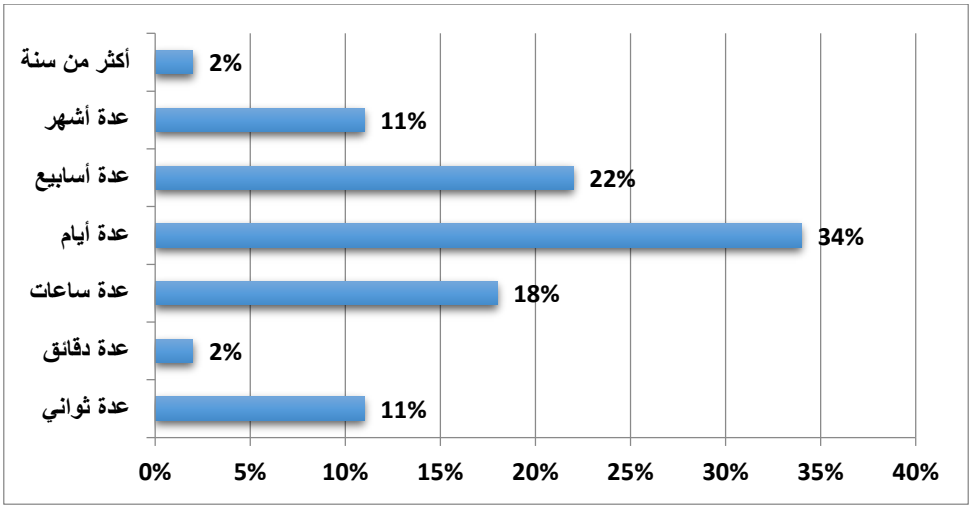
الشكل يبين المحفزات والأسباب الكامنة وراء هذا النوع من الهجمات

ولدى دراسة هذه العينات من الحوادث تم تحديد الأصول المعلوماتية الأكثر عرضة لهذا النوع من الحوادث وقد تبين أن الحواسب الشخصية تحتل النسبة الأكبر بين الأصول التي تعرضت لهذه الحوادث ضمن العينات المدروسة ومن ثم قواعد البيانات وبطاقات الدفع الالكتروني والملفات والبيانات الخاصة بالمخدمات وكذلك أمناء الصناديق أو المحاسبين كما في الشكل:



الشكل يبين الأصول الأكثر عرضة للتهديدات الداخلية ضمن عينات الحوادث التي تمت دراستها

وقد تمت دراسة العينات الإحصائية للحوادث التي تم دراستها من حيث الزمن الذي تم خلاله اكتشاف وقوع الحادث وقد تبين أن النسبة الأكبر منها احتاجت إلى عدد من الأيام حتى تم اكتشافها بينما تم اكتشاف بعضها خلال عدة أسابيع أو عدة أشهر والبعض الأخر خلال أكثر من سنة والشكل يبين ذلك:



الشكل يبين النسبة بين الزمن اللازم لاكتشاف الحادث

- **توصيات وضوابط:**

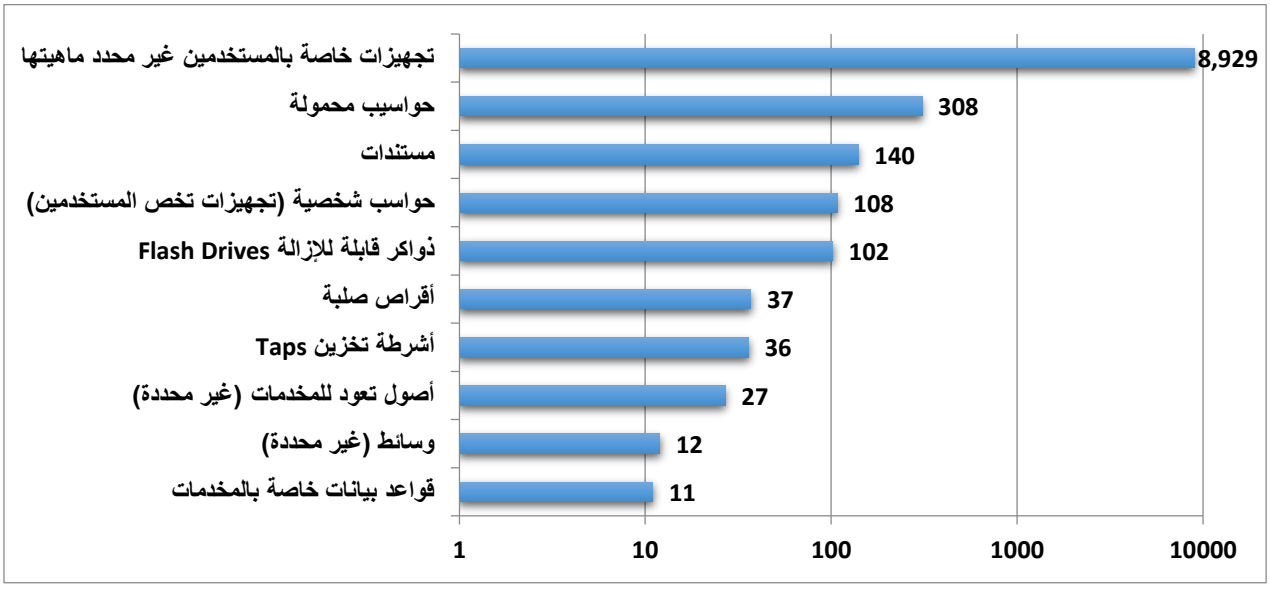
مجموعة من التوصيات الخاصة بتلافي الحوادث الناجمة عن تهديدات داخلية:

- يتوجب على الجهات أن تمتلك معلومات عن بياناتها وأصولها والأشخاص أو الجهات المخولة بالوصول إليها.
- يجب على أي جهة أن يكون لديها سياسات محددة لحسابات المستخدمين مع تحديد صلاحيات كل مستخدم بالنفاذ إلى أصول الجهة ومراجعة هذه الحسابات بشكل دائم والعمل على حذف حساب الموظف مباشرة في حال تركه العمل في الجهة أو تغيير صلاحياته في حال انتقاله إلى موقع جديد لا يحتاج فيه إلى نفس الصلاحيات الممنوحة له سابقاً.
- يجب على الجهات وضع ضوابط وسياسات لحماية أصولها بما فيها البيانات ومنع انتقالها خارج الجهة إلا لضرورات العمل.
- وجود سياسة واضحة ونظام عقوبات في حال تجاوز أي شخص واستغلاله للصلاحيات الممنوحة له بأعمال تضر بعمل الجهة وتوعية الموظفين والعاملين لديها إلى أهمية هذه السياسات.

PHYSICAL THEFT/LOSS

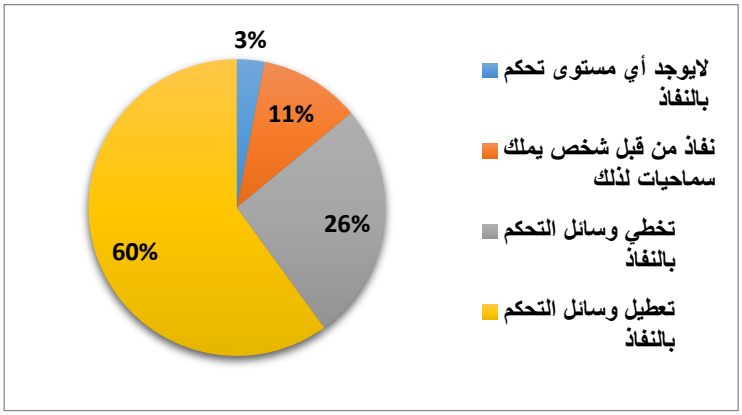
الاختراقات الفيزيائية

وتعني سـرقة أو فقدان التجهيزات أو البيانات من مكانها الفيزيائي حيث تعتبر عملية النفاذ الفيزيائي وسـرقة التجهيزات أو البيانات أو قواعد البيانات من الهجمات الخطيرة التي تحتل مرتبة كبيرة ضـمن الهجمات التي حدثت عام 2013 حيث تمت دراسة 9678 حالة وتصنيفها بحسب نوع التجهيزة أو البيانات التي تمت سرقتها أو فقدانها مع الأخذ بعين الاعتبار أن فقدان الأصول لا يعني بالضرورة أنها تعرضت للسرقة وقد تبين أن الجزء الأكبر من الأصـول التي فُقدت أو سُـرقت هي أصـول تعود للمسـتخدمين ولم تحدد الجهات التي تم جمع العينات منها ماهية هذه الأصـول في معظم الحالات، ولكن على الأغلب هي تجهيزات حواسب شخصية أو أقراص مضـغوطة أو أقراص ليزرية أو أي نوع من وسـائط التخزين أو الحواسـب المحمولة كما كان هنالك جزء من الأصـول عبارة عن وسـائط كملفات أو بيانات أو غيرها والشكل التالي يبين ذلك:



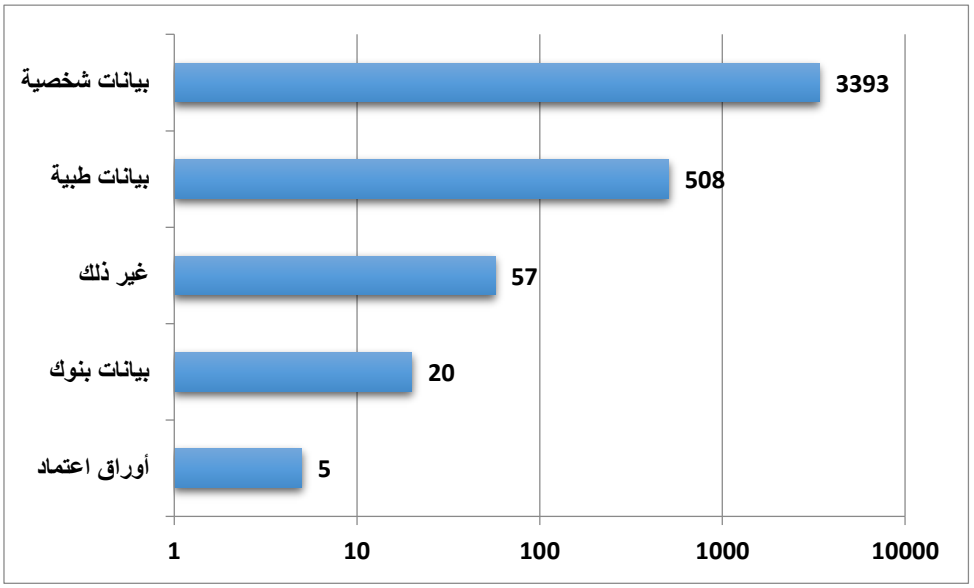
الشكل يوضح مخطط يوضح نسبة أنواع التجهيزات أو البيانات التي فقدت أو سرقت من بين 9678 عينة مدروسة

ومن الجدير بالذكر أن معظم حالات سـرقة الأصـول من غير الممكن تحديد الطريقة التي تم عن طريقها النفاذ إلى المكان الفيزيائي الذي تتواجد فيه الأصـول المسـروقة أو المفقودة ولكن إن 80% من الحالات التي تمت دراسـتها تم النفاذ عن طريق تعطيل أو تخطي الوسائل المستخدمة للتحكم بالنفاذ إلى هذه الأصول والشكل التالي يبين ذلك:



الشكل يوضح النسبة المئوية للطرق التي تم النفاذ فيزيائياً من قبل المخترق إلى مكان وجود الأصول من ضمن العينات المدروسة

والمخطط التالي يبين أكثر أنواع البيانات المعرضة لخطر السرقة من خلال دراسة تتضمن 3824 حالة تمت فيها سرقة بيانات حيث تبين أن أكثر حالات سرقة البيانات ضمن العينات التي تم جمعها عبارة عن سرقة البيانات الشخصية والشكل التالي يبين ذلك:



الشكل يوضح تصنيف البيانات الأكثر عرضة لخطر السرقة ضمن العينات المدروسة

- **توصيات وضوابط:**

مجموعة من التوصـــيات الخاصـــة بتقليل احتمال خطر تعرض الأصـــول للســـرقة أو الفقدان عن طريق النفاذ الفيزيائي:

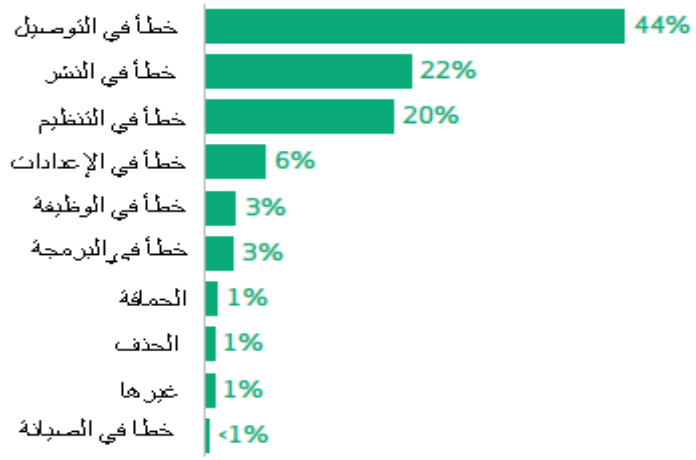
- يجب تشـفير التجهيزات أو وسـائط التخزين التي تحتوي على البيانات الحسـاسـة والعمل على التأكد من فعالية التشـفير المسـتخدم بشـكل دوري وذلك لمنع تسـرب البيانات في حال سـرقة التجهيزات التي تحتوي عليها.
- تعويد الموظفين أو المستخدمين على اصطحاب التجهيزات القابلة للحمل والمعرضة للسرقة معهم بشكل دائم وعدم تركها في الأماكن العامة أو في السيارة أو أي مكان يعرضها للخطر.
- عمل نســـخ احتياطي لجميع البيانات الموجودة على التجهيزات في أمكان منفصـــلة عنها وذلك من أجل استعادتها في حال حصول أي حادثة سرقة أو فقد للتجهيزات.
- يجب التأكد دائماً من قفل المكاتب أو غرف البيانات وأماكن تخزينها بشـكل جيد وعدم السـماح بالدخول إليها إلا من قبل الأشخاص المخولين بدلك.

MISCELLANEOUS ERRORS

أخطاء متنوعة

وهي الحوادث التي تؤدي إلى اختراقات أمنية وتكون أسبابها غير مقصودة.

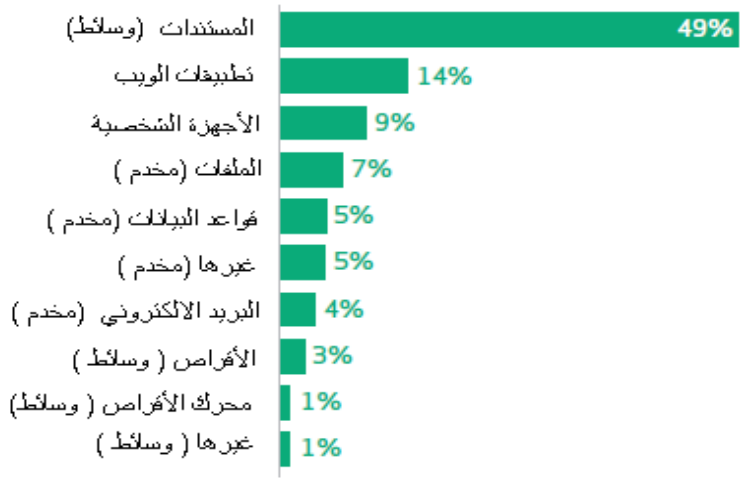
وكما يقال البشـــر يخطؤون ويكون خطؤهم في معظم الأحيان متعلقاً بالعمليات المتكررة والمملة التي تُعنى بمعالجة المعلومات الحساسة. ونكاد نقول إنه لا يخلو حادث أمني من خطأ بشري يشترك في الأسباب، فعلى سبيل المثال: الفشل في تطبيق التحديث الأمني في Wordpress يجعل التطبيق عرضة للاختراق ولكنه لا يؤدي لذلك بشكل مباشر حيث يحتاج الاختراق إلى أفعال أخرى. وتتنوع أشكال الأخطاء التي تكون سبباً لاختراقات أمنية فمنها ما يكون خطأ بالتوصيل أو خطأ في النشر وغيرها كما في الشكل التالي:



النسبة المئوية للأخطاء الأكثر شيوعا بين الاخطاء المتنوعة (العدد الكلي =558).

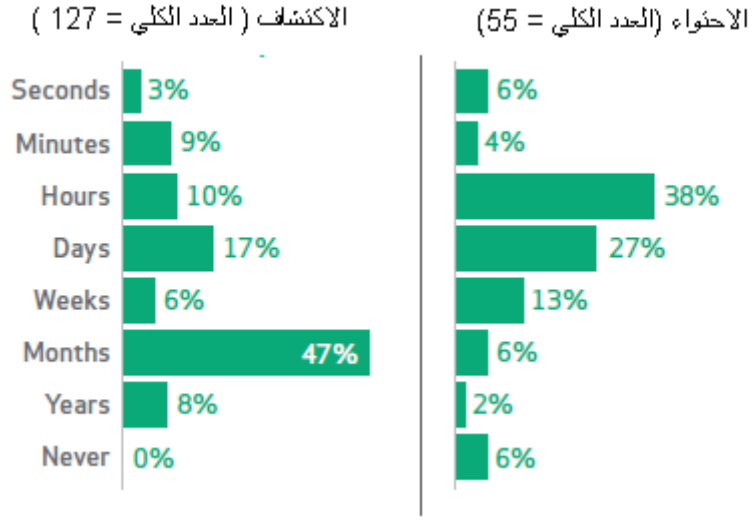
ويوضح الشكل السابق أن خطأ التوصيل هو الأكثر شيوعاً بين الاخطاء ويؤدي إلى كشف معلومات حساسة ويشمل إرسال مستندات ورقية أو رسائل بريد الكتروني إلى الأشخاص الخطأ.

وتؤثر الأخطاء المتنوعة على مساحة واسعة من الموجودات تختلف من مخدمات إلى حواسب شخصية ومن مستندات ورقية إلى بريد الكتروني وغيرها.



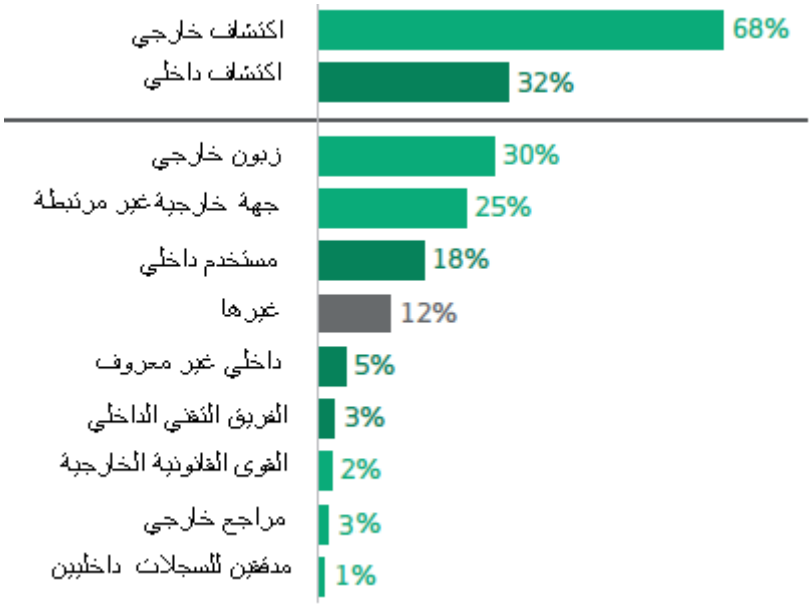
النسبة المئوية لأكثر عشر موجودات تتأثر بالأخطاء المتنوعة (العدد الكلي =546)

تقع مسـؤولية الأخطاء المتنوعة على عاتق الجميع الموظفين، المسـتخدمين النهائيين، مسـؤولي النظام والمطورين. وتتراوح أزمنة اكتشاف هذه الأخطاء من ثواني إلى سنوات وتشير الاحصائيات أن ما يقارب نصف المنظمات تستغرق ما يقارب الأشهر لاكتشاف هذه الأخطاء. وكذلك الأمر بالنسبة إلى أزمنة احتواء هذا الخطأ بمعالجته أو بطرق أخرى.



النسبة المئوية لزمن اكتشاف واحتواء الأخطاء المتنوعة

كما تشـير الاحصـائيات إلى أن ما يقارب ثلث المنظمات تكتشـف أخطائها بنفسـها فيما يتم إعلام الباقي بالخطأ من مصدر خارجي وغالبا ما يكون هذا المصدر الخارجي هو الزبائن.



أكثر عشرة عناصر يتم من خلالها اكتشاف الاخطاء (العدد الكلي =148)

- **توصيات وضوابط:**

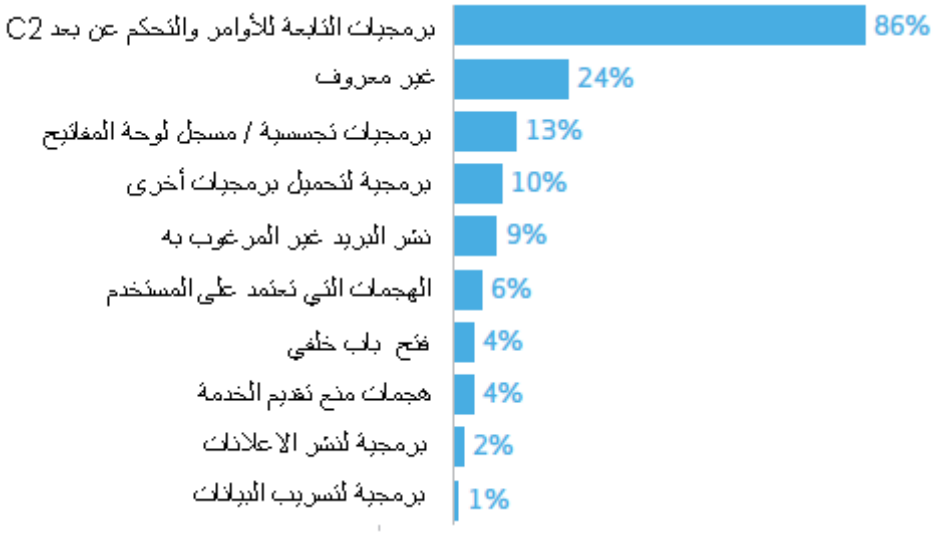
مجموعة من النصائح للوقاية من الأخطاء المتنوعة:

- استخدام تقنيات لحماية ضياع البيانات الحساسة فبرنامج حماية المعلومات الحساسة يمكنه التعرف على هذه المعلومات (أرقام بطاقات ائتمانية، كلمات مرور) وغيرها ومراقبة إرسال هذه المعلومات.
- مراقبة المعلومات المنشورة على الوسائط العامة من خلال زيادة عمليات مراجعة المعلومات التي يتم نشرها مما يقلل من أخطاء النشر.
- أي عملية لتبادل أو كشف أو بيع للمعلومات يجب أن تتم تحت إدارة الفريق التقني.

CRIMEWARE

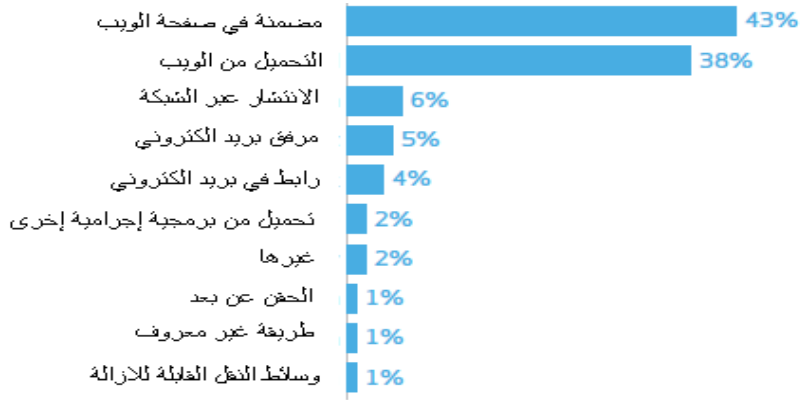
البرمجيات الخاصة بالجرائم الالكترونية

وهي البرمجيات التي يتم استخدامها بهدف الاختراق والسيطرة على الأنظمة لأهداف غير مشروعة كسرقة البيانات الحساسة والتجسس، استخدام هذه الأجهزة للمشاركة في هجمات تعطيل الخدمة، نشر بريد الكتروني غير مرغوب به وغيرها. وتعد أكثر وسائل انتشار هذه البرمجيات الإجرامية التحميل عن طريق الويب والانتقال عبر الوسائط المتعددة. بعض هذه البرمجيات الإجرامية يقوم بالسيطرة على كامل حاسوب الضحية ويتلقى أوامره من مخدمات التحكم والأوامر ويدعى ب C2، وبعضها يقوم بتسجيل الكتابة على لوحة المفاتيح وإرسالها إلى عنوان محدد مسبقا وهدفه تجسسي لسرقة بيانات معينة، وبعضها يقوم بنشر إعلانات على متصفح الضحية وغيرها يقوم بنشر رسائل بريد الكتروني غير مرغوب بها من حساب الضحية وغيرها. ويوضح الشكل التالي أكثر هذه البرمجيات انتشارا:



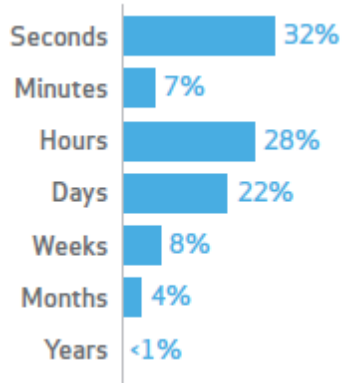
البرمجيات الإجرامية الأكثر انتشاراً (العدد الكلي = 2274)

وعند دراسة الطرق التي تعتمد عليها البرمجيات الإجرامية في انتشارها تبين أن أكثر هذه الطرق هي التضمين في صفحة الويب والتحميل من الانترنت وغيرها من الطرق بنسب ضئيلة:



الطرق العشرة الأبرز في انتشار البرمجيات الإجرامية (العدد الكلي =337)

لابد لنا عند استعراض هذه البرمجيات الإجرامية ذكر أهمية البرامج المضادة للفيروسات وأنظمة كشف التطفل IDS في الحماية منها حيث أن عملية الكشف السريعة المبينة في الشكل التالي تؤكد على أهمية هذه البرامج وضرورة استخدامها:



زمن اكتشاف البرمجيات الإجرامية (العدد الكلي = 1017)

- **توصيات وضوابط**

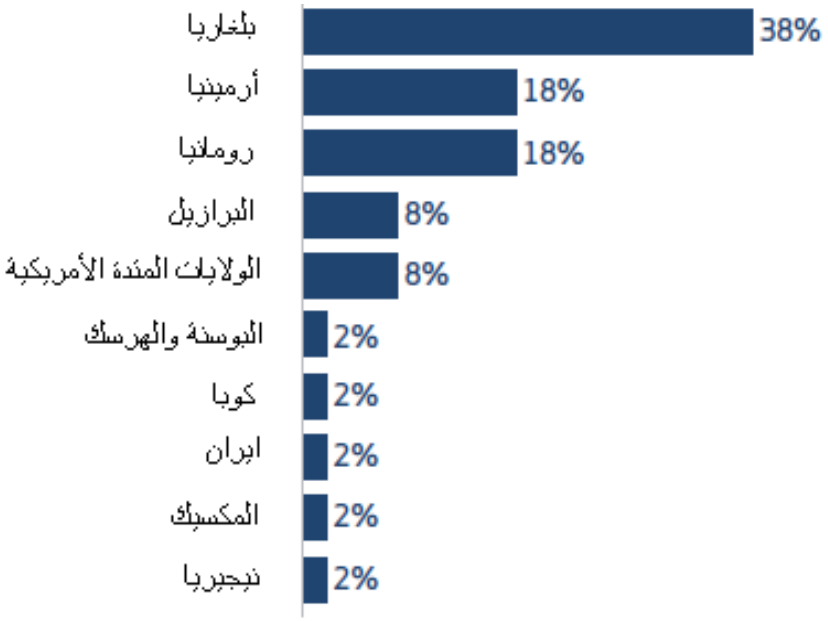
مجموعة من النصائح للوقاية من البرمجيات الإجرامية:

- تحديث المتصفحات بشكل دوري ودائم مما يساعد على الحماية من الاختراقات الأمنية.
- تعطيل ال JAVA في المتصفح.
- استخدام وسائل مصادقة ثنائية تهدف إلى التأكد من شخصية المستخدم، لمنع استفادة البرمجيات الإجرامية من البيانات المسروقة.
- البحث عن أساليب عمل الملفات الخبيثة لتطوير عملية الكشف والاستجابة السريعة بدلا من عملية المعالجة.
- زيادة فعالية التغذية الخلفية من خلال إرسال بيانات الملفات الخبيثة والعناوين المنطقية وعناوين النطاق التي يتصل بها للحد منها وإيقافها عند أجهزة أخرى.

CARD SCKIMMERS

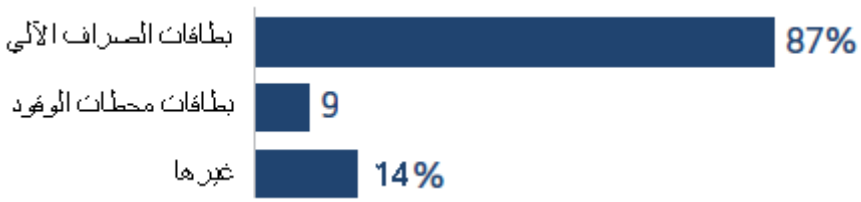
ناسخي بيانات البطاقات الالكترونية

تعتمد هذه الطريقة على زرع جهاز يقوم بقراءة البطاقة الالكترونية في أماكن الصـــرافات الآلية أو نقاط البيع أو أماكن تعبئة الوقود مما يمكن الســـارقين من محاكاة بطاقة الدفع الالكتروني ووضـــع كميرا مراقبة أو وضـــع لوحة مفاتيح تقوم بسرقة كلمات المرور أيضـا. وتعتبر هذه الطريقة ذات انتشـار واسـع في سـرقة معلومات بطاقات الدفع وترتبط معظمها بأشـخاص من أوروبا الشـرقية وتكون ضـحيتها منظمات في الولايات المتحدة الأمريكية كما توضـح الأرقام:



أصل المنفذين لعملية قارئي بطاقات الدفع الالكتروني (العدد الكلي =40)

تشكل الصـرافات الآلية العامل الأكثر تعرضـاً لهذه السـرقات لكونها في أماكن عامة وبدون وسـيلة حماية، وتأتي بعدها نقاط الدفع في تعبئة الوقود والتي يمكن وضعها بإلهاء العامل المسؤول.



الموجودات الأكثر تعرضاً لعميلة السرقة عبر محاكاة بطاقات الدفع (العدد الكلي =537)

ومازالت هذه الطريقة في السـرقة والاحتيال في تطور ففي السـابق كان السـارق مضـطرا لعودة إلى مكان الجريمة للحصول على المعلومات بينما حاليا يتم إرسال المعلومات عبر البلوتوث أو عبر شبكات الخليوي وغيرها.
وغالبا ما يتم اكتشـاف هذه السـرقات من خلال شـركات الدفع الالكتروني أو المسـتخدمين الذين تتم سـرقتهم أو من خلال القوى القانونية التي تلقي القبض على سيارة تحتوي على أدوات السرقة.

- **توصيات وضابط:**

مجموعة من النصائح للوقاية من نسخ بطاقات الدفع:

1. ما يتعلق بشركات الدفع:

- مراقبة الصـــرافات وأماكن الدفع الالكتروني بشـــكل دائم وتدريب الموظفين على ملاحة التغيرات المريبة.
- وضـع دلالات لوجود خرق في نقاط الدفع كوضـع لصـاقة ورقية تشـير إلى عملية العبث أو وضـع كميرات مراقبة للحوادث الغريبة.
- العمل على اختيار نقاط دفع الكتروني محمية من العبث بتصميمها.

2. ما يتعلق بالمستخدمين:

- تغطية الرقم السري عند إدخاله.
- ثق بحدسك وعند شعورك بحركة غريبة حولك أو بتغيير في شكل الصراف لا تضع بطاقتك.
- عند ملاحظة تغيير في الصراف الآلي قم بإخبار القوى القانونية أو الشركة المالكة.

CYBER-ESPIONAGE

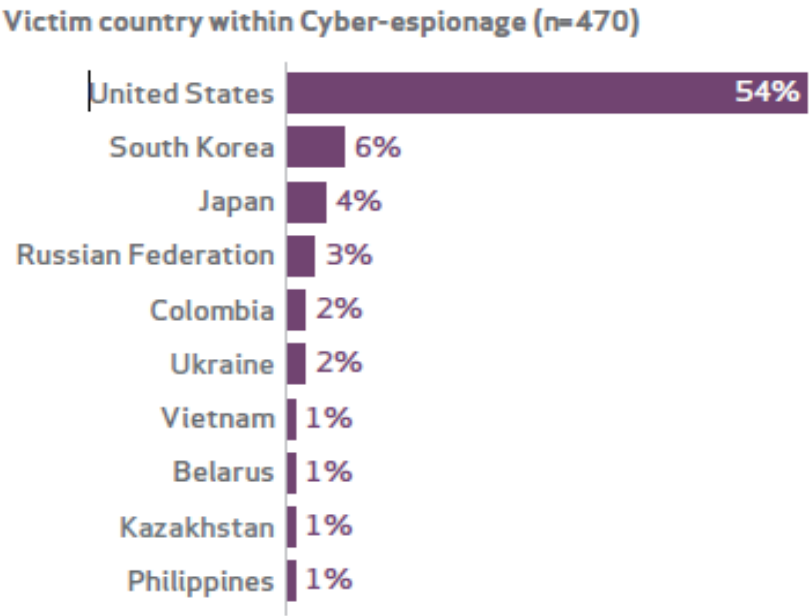
التجسس السيبراني

هو فعل أو ممارسة للحصول على معلومات سرية من شركات وأفراد دون الحصول على إذن صاحب المعلومة من خلال استخدام تقنيات للنفاذ غير المشروع للأنظمة والبرمجيات الخبيثة بما في ذلك أحصنة طروادة (Trojan) وبرامج التجسس.

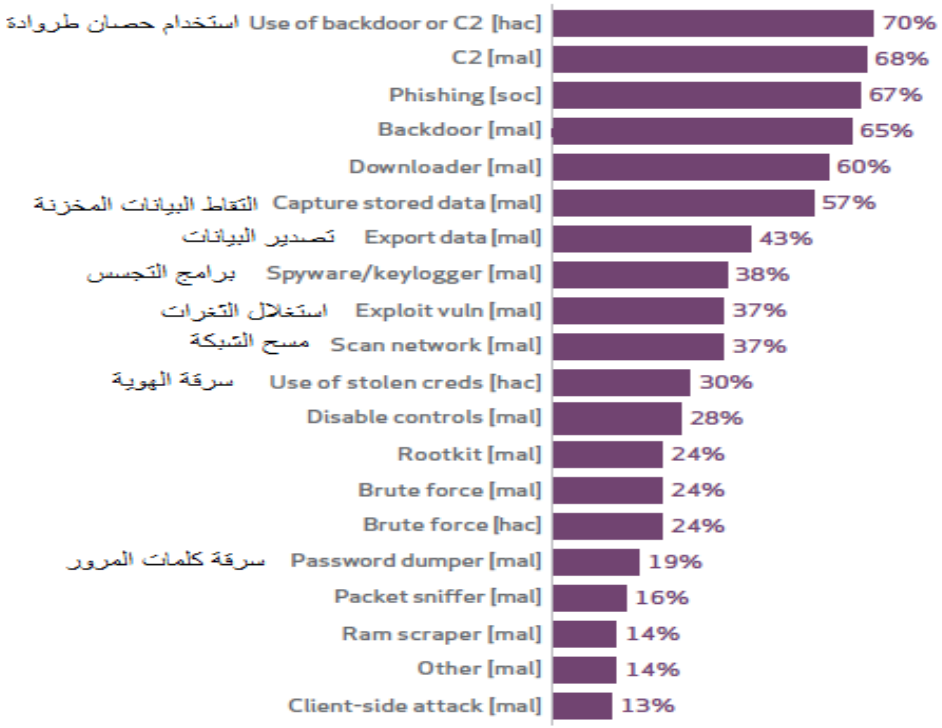
تقوم معظم الشركات حفاظاً على السرية بإخفاء حصول سرقة للمعلومات بالإضافة ليس هناك خوارزمية لتنبيه الضحايا عن الاستخدام غير المشروع لهذه البيانات مما يترك العديد من الحالات غير معرضة للاكتشاف، لذلك إن معظم ما نعرفه عن هذه الاختراقات يكون من قبل المستجيبين للطوارئ الأمنية أو محللي البرمجيات الخبيثة.

إن عدد حوادث التجسس التي تم التبليغ عنها وصلت في عام 2013 إلى حوالي 511.

إذاً لم يتم تغطية جميع حالات التجسس حيث لم يتم الإبلاغ عن أي حالة تجسس في ايطاليا على الرغم من أن هذا غير منطقي، وفيما يلي مخطط بأكثر البلدان التي قد تعرضت للتجسس:

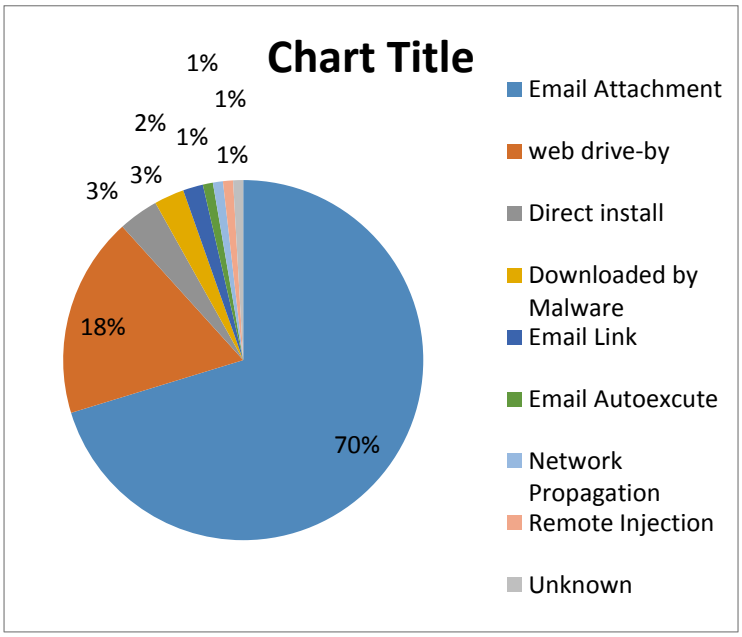


كما أن هناك العديد من المخاطر الأمنية ترافق التجسس السيبراني باستخدام طرق متعددة وفيما يلي مخطط يوضح أكثر الأدوات المستخدمة في التجسس السيبيري:



للنفاذ إلى حاسـوب الضـحية والتجسـس عليه يتم إتباع عدة طرق منها مرفقات البريد الالكتروني، البرمجيات الخبيثة، والتنصت على الشبكة وغيرها.

فيما يلي مخطط يوضح أكثر طرق انتقال البرمجيات الخبيثة في عملية التجسس السيبراني:



- **توصيات وضوابط**

مجموعة من التوصيات للحماية من التجسس السيبراني:

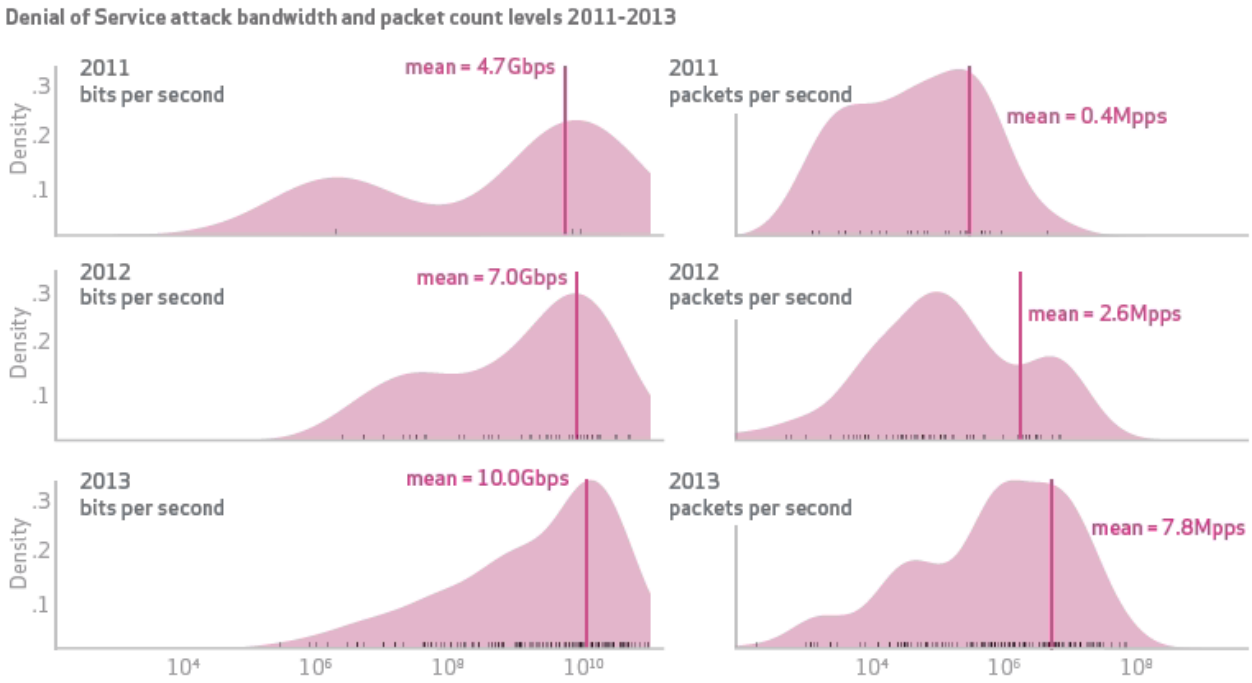
1. تحديث التطبيقات الموجودة على الحاسب ونظام التشغيل بشكل دوري.
2. استخدام وتحديث برامج مكافحة الفيروسات.
3. تدريب المستخدمين وتعريفهم بالحاسب وكيفية حفظ البيانات من الضياع والسرقة والإبلاغ عن الحوادث الأمنية عند الضرورة.
4. تقسيم الشبكة بطريقة جيدة من حيث إعطاء الصلاحيات للمستخدمين.
5. مراقبة الشبكة ورصد حركة المرور للاتصالات المشبوهة والنظام الحاسوبي ونشاط التطبيقات والاحتفاظ بالسجلات ومراقبة نشاط المستخدم.

DENIAL OF SERVICE (DOS) ATTACKS

هجمات منع تقديم الخدمة

هي هجمات تتم عن طريق إغراق المواقع الالكترونية بســـيل من البيانات غير اللازمة مما يؤدي إلى بطء عمل المخدمات أو إيقافها كلياً والازدحام ضمن هذه المواقع.

خلال عام 2013 تعرضـــت العديد من الشـــركات العالمية لهجمات DDos حيث يتم إغراق كامل عرض النطاق الترددي (Bandwidth)



كانت أول مجموعة مسـؤولة عن الهجمات الجديدة من ال DOS Attackهي كتائب عز الدين القسـام التي بدأت نشـاطها في أيلول 2014 حيث قامت بإغراق مؤسـسـات الولايات المتحدة الأميركية و خاصـة المالية منها بطلبات من هجمات منع تقديم الخدمة و ذلك ليس فقط بإرسـال طلبات SYN, UDP فقط بل و بإرسـال HTTPs Get لتحميل ملفات PDF من أنحاء العالم.

إن العديد من الهجمات الحديثة تتم عن طريق تنفيذ هجوم حجب الخدمة المنعكسـة (Reflected Dos Attack) حيث يقوم المهاجم بإرسال مجموعة من استعلامات DNS وذلك بتزوير عنوان المصدر في الطلبات ليجعلها تبدو وكأنها مولدة من الهدف نفسه.

عند فتح ردود DNS يرسل مجموعة من الاستجابة على الطلبات للعنوان الهدف مما يؤدي لإغراق المخدم وازدحام الشبكة.

لا يتطلب هذا النوع من الهجوم العديد من موارد الحاسب بالرغم من الأثر الكبير له.

- **توصيات وضوابط**

بعض التوصيات للحماية من هجمات حجب الخدمة:

- عزل المخدم والتطبيقات ومجموعة العناوين الرقمية للشـبكات الغير مسـتخدمة حالياً في دارات خاصـة مثلاً VLan وعند حصـول هجوم على الشـبكة يتم تحويل المهاجم إلى الشـبكة المعزولة بحيث لا يؤثر على عمل المخدم الأساسي.
- استخدام (IPS(Intrusion Protection System و (IDS (Intrusion Detection System.
- تركيب وتشغيل أجهزة Anti-DDos لمكافحة هجمات منع تقديم الخدمة.
- يجب الاسـتفسـار من مزود خدمة الانترنت عن سـعة خطوط الاتصـال وإن كانت تتحمل جميع الطلبات من المستخدمين

خلاصة وتوصيات

إن الغرض الحقيقي من هذا البحث هو مساعدة الشركات والأفراد في الحد من الخطر الناجم عن هذه المساوئ، حيث أن دراسة نماذج متفاوتة للحادث الأمني ينتج استراتيجيات أمنية أفضل للحد من الخطر.

فقد تبين أن سوء الاستخدام والسرقة وفقدان المعلومات والخطأ تشكل أغلبية أشكال الهجوم الذي يواجهه القطاع (عام)، ومنع فقدان البيانات يساعد في تحديد كل منهم.

القواعد ال 19 الأخرى مهمة (بالتأكيد لا نقول إن على أحد ما تجاهلها)، ولكن وجهة النظر هذه هي حجة قوية للتأكيد على أن الصناعة تولي العنصر CSC 17 الاهتمام وتمنحه الموارد التي يستحقها؛ على وجه التحديد إن الضوابط الفرعية التي تغطي التشفير التام للقرص الصلب (17.3) وكشف سوء نشر المعلومات (17.6).

إن عرض ذلك كدليل يمكن أن يساعد في الإجابة عن السؤال التالي: أين أصبحت صناعة بلدي الآن بناء على ذلك (والذي يعكس الضوابط والتهديدات التي يمكن أن تواجهها)؟ على ماذا نركز لاحقاً؟

أحد هذه العناصر هو ذاتي لدرجة أننا والمجلس حددنا أي من الضوابط سيكون أفضل لعنونة كل نمط من أنماط التهديد، ولكن بنينا تلك القرارات على سلسلة من الأحداث التي لوحظت في مجموعة البيانات، والترجيح الذي قمنا به يستند بقوة على تواتر البيانات التي حصلنا عليها بالنسبة لأنماط الهجوم والمنتجات.

ولذلك فإن الفوارق البسيطة في هذه الأرقام ليست بذات معنى، ونعتقد بوجود حجة قوية لأخذ نظرة فاحصة على الضوابط التي تبرز في الواجهة.

ونأمل كما دائما بأن يكون التقرير لهذه السنة قيما ونتطلع للأمام إلى سماع ملاحظاتكم.

Critical security controls mapped to incident patterns. Based on recommendations given in this report.

Critical Security Controls (SANS Institute)		POS Intrusions	Web App Attacks	Insider Misuse	Physical Theft/Loss	Misc. Errors	Crimeware	Card Skimmers	Cyber-espionage	DoS Attacks
Software Inventory	2.4						●		●	
Standard Configs	3.1						●			
	3.2		●				●		●	
	3.8						●			
Malware Defenses	5.1	●					●		●	
	5.2	●					●		●	
	5.6						●		●	
Secure Development	6.4		●							
	6.7		●							
	6.11		●							
Backups	8.1				●					
Skilled Staff	9.3				●					
	9.4								●	
Restricted Access	11.2	●								
	11.5	●								
	11.6	●								
Limited Admin	12.1	●		●						
	12.2			●						
	12.3	●								
	12.4	●								
	12.5	●								
Boundary defense	13.1						●		●	
	13.7	●	●				●		●	
	13.10	●								
	13.14	●								
Audit Logging	14.5	●		●						
Identity Management	16.1			●						
	16.12			●						
	16.13			●						
Data Loss Prevention	17.1				●					
	17.6			●		●				
	17.9			●		●				
Incident Response	18.1									●
	18.2									●
	18.3									●
Network Segmentation	19.4								●	●

To find out more about the SANS Institute's Critical Security Controls, visit: http://www.sans.org/critical-security-controls/

المنهجية المتبعة في كتابة التقرير

اعتمدت المنهجية على 50 منظمة ساهمت في تقديم البيانات بطرق متعددة وتمَ اتباع عدة أساليب مختلفة في تجميع البيانات في إطار مقاربات متعددة، وجميع الأحداث الأمنية في هذا التقرير تمَ مراجعتها وتحويلها في إطار عمل موحد يدعى VIRES ولكن أساليب تجميع البيانات وتقنيات التحويل تختلف لكل من هذه المنظمات وفي العموم تم استخدام ثلاث طرق أساسية وهي:

1) التسجيل المباشر بواسطة Verizon الذي أطلق تطبيق VIRES لتسجيل الحوادث الأمنية.
2) التسجيل المباشر من قبل المساهمين باستخدام VIRES.
3) إعادة الترميز باستخدام VIRES من المخططات المقدمة من قبل المساهمين، حيث تلقى جميع المساهمين تعليمات حذف أي معلومات قد تشير إلى المنظمات أو الأفراد المعنيين.

1. منهجية Verizon في جمع البيانات:

تستند جميع النتائج على أدلة مباشرة تم جمعها خلال عمليات التحقيق الشرعي الرقمي وعمليات الاستخبارات ذات الصلة في الفترة الممتدة بين عامي 2004–2013م.

القضايا المسجلة في عام 2013 تشكل محور عمليات التحليل في هذا التقرير مع الأخذ بعين الاعتبار كامل المجال الزمني.

حالما يكتمل التحقيق يقوم المحللون باستخدام الأدلة والتقارير والمقابلات لإنشاء سجل VIRES للأدلة، ثم يراجع التقرير ويصدق من قبل أعضاء آخرين في الفريق لضمان موثوقية واتساق البيانات.

2. منهجية للمساهمين باستخدام VIRES:

قام المساهمون من خلال هذا الأسلوب بتزويدنا ببيانات الحوادث الامنية بالصيغة الخاصة ب VIRES وعلى سبيل المثال، استخدم عملاء الخدمة السرية في الولايات المتحدة (USSS) تطبيقا يستند على VIRES لتسجيل تفاصيل القضية ذات الصلة، ومهما كانت طريقة تسجيل البيانات فإن المنظمات المساهمة اعتمدت على تسجيل ملاحظات عن التحقيق والتقارير المزودة وخبرتهم الخاصة الناتجة من التعامل مع هكذا حوادث.

3. منهجية للمساهمين لا تستخدم VIRES:

قامت بعض المنظمات المساهمة بجمع وتخزين بياناتها بطريقتها الخاصة، وخير مثال على ذلك هو فريق الاستجابة للطوارئ المعلوماتية CERT insider Threat Dtabase31 في معهد هندسة البرمجيات بجامعة كارنيجي ميلون، حيث تمَ إعادة صياغة البيانات الأصلية وتسجيلها بشكل سجلات VIRES.

الحوادث الأمنية وانكشاف البيانات

ركز هذا التقرير على الحوادث الأمنية المسببة لانكشاف البيانات المحقق بشكل أوسع من التقرير السابق للعام 2013، حيث تمَ توسيع التقرير ليشمل هجمات منع تقديم الخدمة واستغلال الأنظمة دون فقدان البيانات ومجموعة من الحوادث الأمنية التي لا يمكن فيها تحديد فقد البيانات.

خروقات البيانات وسرقة الهوية هي قضايا معقدة

تمَ التركيز على الأضرار التجارية الناجمة عن اختراق البيانات في هذا التقرير.

فمثلاً عند سرقة هوية الزبون ومن ثم تلقيه رسالة إخطار بحدوث خرق لبياناته: هل يعني ذلك بأنه أصبح ضحية لهجوم سرقة الهوية؟ كلا ليس بالضرورة (حتى الآن).

إن العلاقة بين هجومي اختراق البيانات وسرقة الهوية هي أصعب مما يعتقد وهنالك دراسات كثيرة بهذا الخصوص.

أنواع المعلومات

لقد أصبحت خروقات البيانات أكثر شيوعا وفهما من قبل المستخدمين، ويرجع ذلك لاهتمامهم بالحوادث الأمنية التي حدثت معهم من قبل والدعاية المرافقة لأهم الحوادث، وكنتيجة لذلك يواجه الزبائن حقيقة أن معلوماتهم الشخصية تترك غير آمنة عند أولئك المكلفين بحمايتها...كلمات المرور–أسماء المستخدمين–رسائل البريد الالكتروني–بطاقات الائتمان–معلومات الحسابات المالية وأرقام الضمان الاجتماعي التي جرى استغلالها على نحو مذهل مما هدد هوية الزبائن الكرام على الصعيد الوطني.

هذا التصور ينطبق على الجميع في سيناريو اختراق البيانات وهم الزبون والمنشأة التجارية ولص البيانات طبعاً.

يستخدم الزبائن هذه الأجزاء من المعلومات في الدخول والخروج لحساباتهم وغالباً دون التفكير بقيمتها أو التدابير اللازمة لحمايتها. وفي عالم الأعمال والشركات، إن انكشاف هذه البيانات لا تستدعي الإخطار بحدوث خرق أمني.

حيث يمكن للص الهوية ان يحصل على هذه البيانات بطرق متعددة كإتباع أساليب الهندسة الاجتماعية.

القلق الرئيسي هو حول من المسؤول عن أي خسارة مالية او مصاريف اضافية في حال حصول سرقة للبيانات، حيث يخشـــى العديد من الزبائن أن انكشـــاف هذه المعلومات قد يقود الى ســـرقة هوية الزبون غير مدركين أن ذلك يتطلب الحصول على معلومات أخرى مثل رقم الضمان الاجتماعي وإن استغلال المعلومات المالية محدود بأشكال معينة من الاحتيال المالي هذا إن وجد حساب مالي.

وقد تكون قيمة المعلومة المالية كبيرة، ولكن عادة تفقد قيمتها في حال تصرف الزبون بسرعة وأغلق الحساب. وذلك يتم بالتعاون مع الشركات من خلال إخطار الزبون وتحذيره لاتخاذ تدابير استباقية.

تعتبر أرقام الضمان الاجتماعي المقياس الذهبي لحساسية المعلومات المعرفة للهوية الشخصية وهي الجزء الأمثل من المعلومة والذي يفتح العديد من الأبواب المغلقة في وجه اللص وبوجود هذه البيانات يتمكن اللصـــوص من الولوج إلى حســـابات جديدة ومنافع كثيرة يجنونها من اســـتغلال هذه البيانات كالحصـــول على اعتمادات الإعانات الحكومية والضـــرائب والعمالة والمرافق والرهون العقارية والموارد الطبية. وحده ســـارق البيانات يمكنه تقدير قيمة مثل هذه المعلومات.

تدرك الشـركات الأمريكية أهمية حماية هذه المعلومات الحسـاسـة لأنهم يعلمون ان انكشـاف هذه البيانات سـيطلق إجراءات التنبيه والتحذير في 46 ولاية امريكية.

ومن هنا تأتي حاجة الشـركات لتطبيق أفضـل الاجراءات والسـبل الكفيلة بحماية هذه البيانات وإلا فإنها سـتواجه لاحقاً أعباء مالية للتخفيف من أضرار الاختراق الامني.

الأثر على الضحية (التكلفة غير المالية على الصعيد الشخصي)

بما أن الزبائن الذين تصلهم تحذيرات من الشركات لن يصبحوا جميعهم ضحايا جريمة سرقة الهوية وسيكونون بحاجة للتواصـل مع وكالات وجهات أخرى معنية بحل المشـكلة كالمؤسـسـات المالية والدائنين ووكالات البطاقات الائتمانية، الرعاية الصـحية، ووكالات قانونية أخرى لتدوين الحادثة وتغيير كلمات المرور وأرقام التعريف الشـخصـية، وإغلاق أو

تغيير حســابات البريد الإلكتروني هي فقط بعض الخطوات الممكنة التي قد تحتاج إلى اتخاذها للحد من خطر ســرقة الهوية في المستقبل.

فهم أنواع معلومات التعريف الشخصية والحاجة إلى اتخاذ إجراءات المتابعة

اعتماداً على نوع البيانات الشخصية المعرضة للخطر (الحساسة أو أقل حساسية) في أي حادث معين لخرق البيانات، فإن العديد من المخاطر المرتبطة بها تكون مرهونة على كيفية الســـرعة التي يســـتجيب فيها الزبون للتحذير بحدوث الخرق. هذا هو الســبب في أن توقيت إخطار المســتهلكين يكتســب اهمية كبيرة. وإعلام العميل ســواء كان / الزبون / موظف / طالب لأنه هو الذي يمكنه أن يتخذ تدابير استباقية للحد من مخاطر أي ضرر محتمل.التوصيات:

- لا تحمل بطاقة الضمان الاجتماعي الخاص بك معك.
- ضع كلمات مرور قوية –وعدم استخدام ارقام مثل "12345678" ككلمة مرور لأنه يمكن بسهولة كسرها.
- لا تكن اجتماعيا أكثر من اللازم على وســائل الاعلام واحذر مخاطر الهندســة الاجتماعية التي تقدم معلومات كثيرة تستغل في هجمات التصيّد.
- عدم مشاركة أي مستندات تحوي معلومات حساسة.
- مراقبة البيانات المالية لاكتشاف أي عملية احتيال قد تحدث.
- حماية المعلومات المدونة على المعاملات الصـــحية، وتقليل عدد المرات التي تزود بها مكتب الطبيب بهذه المعلومات قدر الامكان والتأكد من اجراءات الحماية المتبعة من قبل مكتب الطبيب لحماية وتأمين ســـلامة هذه المعلومات.

المراجـــــــــــع:

/http://www.verizonenterprise.com/DBIR/2014