أهمية أمن المعلومات للشركات والأعمال

المحاور

هو ممارسة الدفاع عن جميع التجهيزات والشبكات والأجهزة المتصلة بالإنترنت من الوصول الغير مصرح به.

مثال عن هذه الأجهزة:

- أجهزة الكمبيوتر (جهاز مكتبي، لابتوب، سيرفر)
- أجهزة محمولة (موبايل، جهاز لوحي، ساعة ذكية)
- أجهزة ترفيه (منصات العاب، تلفاز ذكي، مشغلات موسيقى)
- أجهزة ملاحة GPS
- أجهزة تواصل تناظرية Pager

المصدر: https://www.cisa.gov/uscert/ncas/tips/ST04-001

ما هو الأمن السيبراني؟

هو ممارسة الدفاع عن جميع التجهيزات والشبكات والأجهزة المتصلة بالإنترنت من الوصول الغير مصرح به.

مثال عن هذه الأجهزة:

- أجهزة الكمبيوتر (جهاز مكتبي، لابتوب، سيرفر)
- أجهزة محمولة (موبايل، جهاز لوحي، ساعة ذكية)
- أجهزة ترفيه (منصات العاب، تلفاز ذكي، مشغلات موسيقى)
- أجهزة ملاحة GPS
- أجهزة تواصل تناظرية Pager

المصدر: https://www.cisa.gov/uscert/ncas/tips/ST04-001

الغرض من الأمن السيبراني؟

حماية المعلومات والحفاظ على:

السرية: تعني أن الأشخاص المصرح لهم فقط هم من يمكنهم رؤية المعلومات.

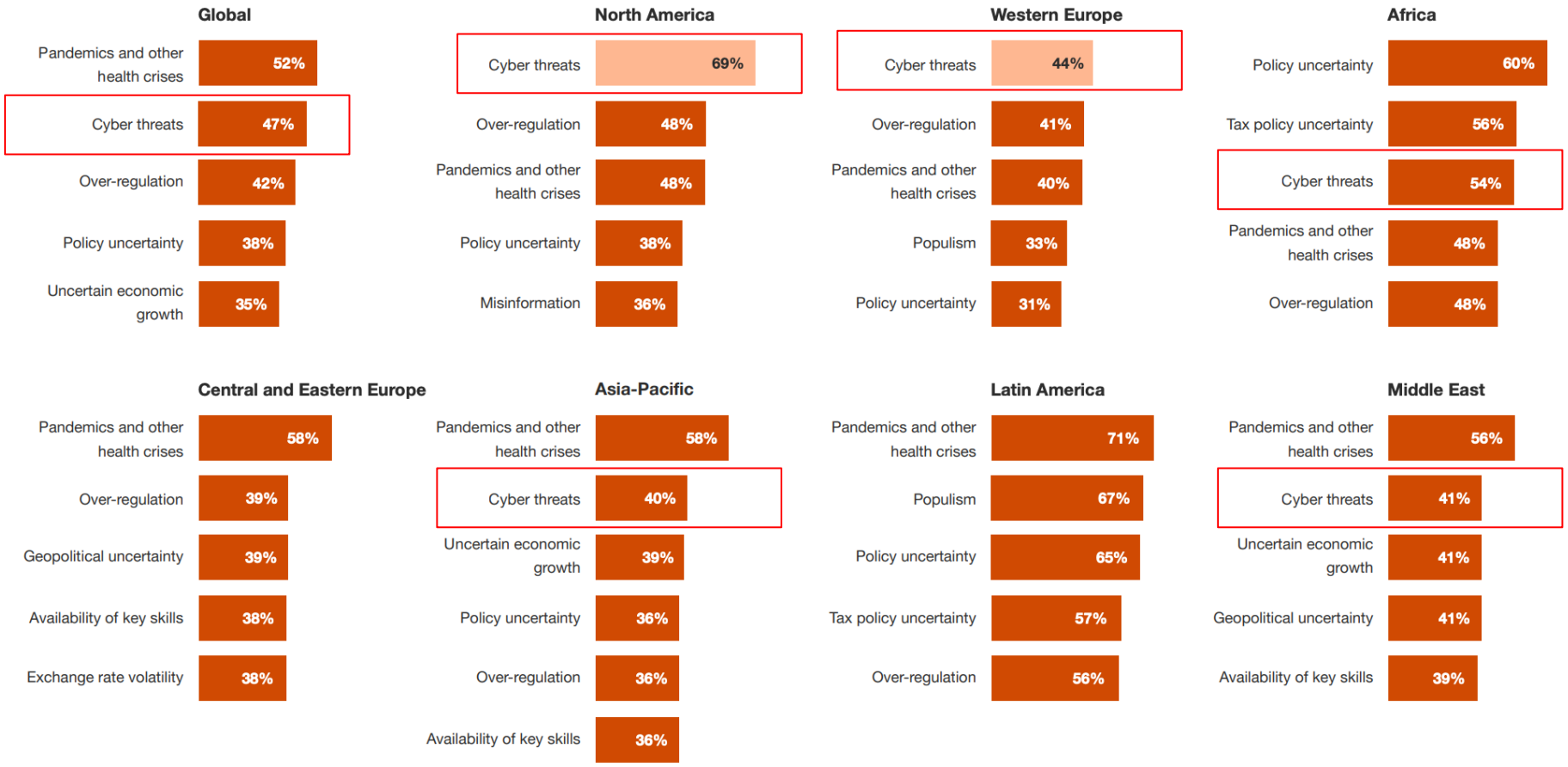
النزاهة: وتعني أن المعلومات لا يمكن أن تتغير إلا بطريقة مضبوطة.

التوافر: تعني أن هذه المعلومات يجب أن تكون متاحة للأشخاص المناسبين عند الحاجة.

مثلث CIA

ما هو تأثير الهجمات الالكترونية على الاعمال حول العالم؟

اجرت شركة PWC للدراسات استبيانا حول مدى قلق المدراء التنفيذيين بشأن العوامل الاقتصادية التي تأثر سلباً على أعمالهم، تم عرض ردود "قلق للغاية" فقط.

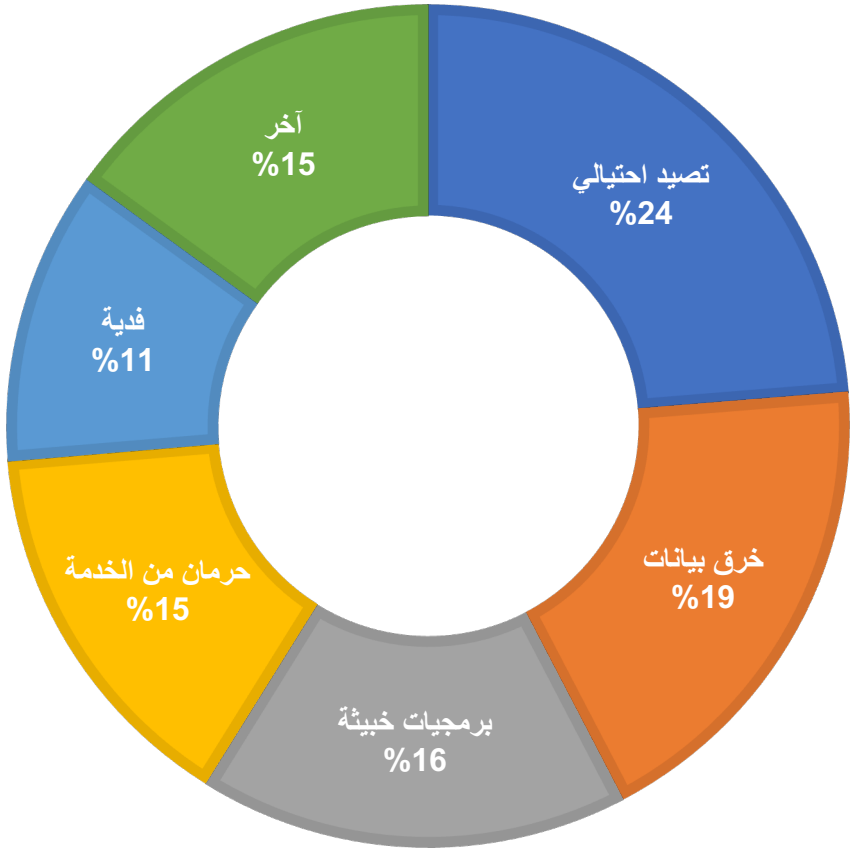


المصدر: https://www.pwc.com.tr/tr/publications/arastirmalar/assets/24-ceo-arastirmasi/24-kuresel-ceo-arastirmasi.pdf#page=7

42٪ من المؤسسات حول العالم

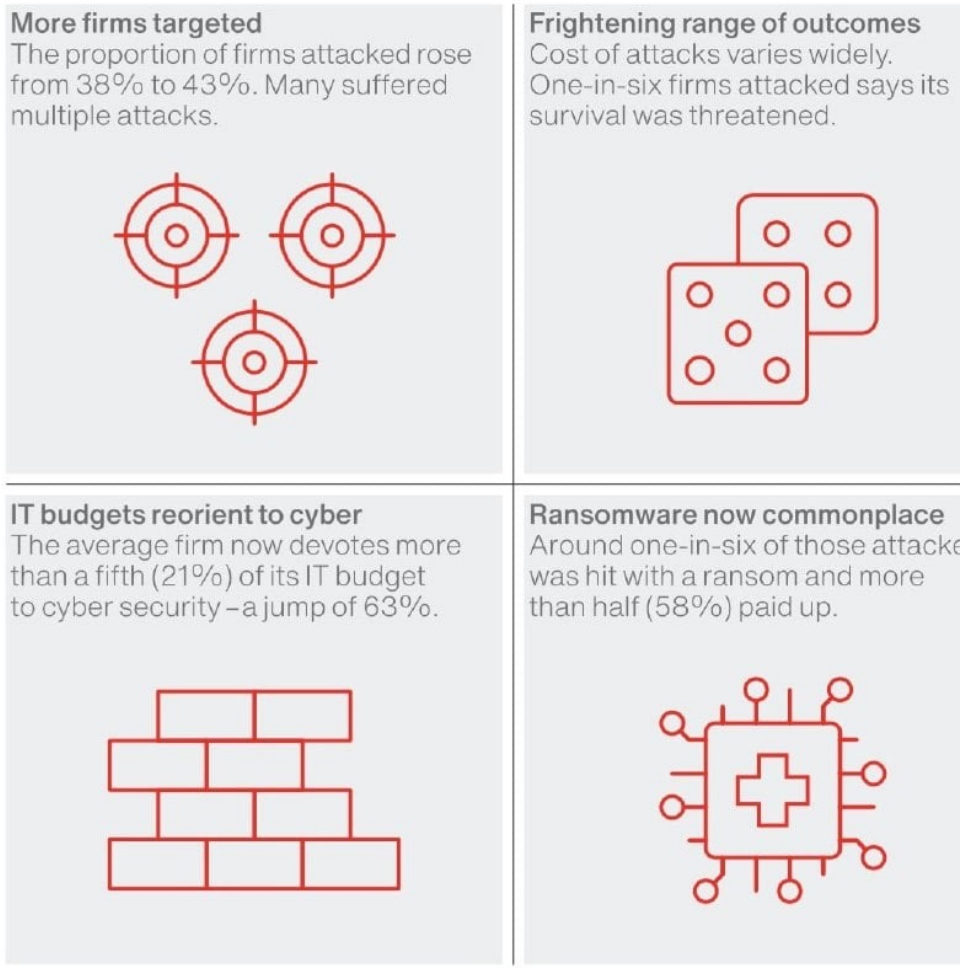
الصغيرة والمتوسطة تعرضت لهجمات، أي ما يعدل نصف الشركات الصغيرة تقريباً تعرضت لهجمات الكترونية خلال عام 2021

.



المصدر:
https://advisorsmith.com/data/small-business-cybersecurity-statistics/#:~:text=42%25%20of%20small%20businesses%20experienced,23.7%25%3A%20Phishing%20attack.

التأثير على الشركات



بحسب تقرير الجاهزية للهجمات السيبرانية لعام 2021 الذي اصدرته شركة هيسكوكس Hiscox بعد اجراء استقصاء شمل اكثر من 6000 شركة، أفضت هذه الدراسة إلى أن:

- عانت الشركات من هجمات الكترونية متعددة، بواقع هجوم طلب فدية Ransomware Attack لكل شركة من أصل 6 شركات
- 58% من الشركات المستهدفة بدفع هذه الفدية مع تصاعد المخاوف من مخرجات هذه الهجمات
- شعرت شركة واحدة من أصل 6 شركات قامت بدفع الفدية بالتهديد والتشكيك في استمرارها ضمن سوق العمل.

المصدر: https://www.hiscoxgroup.com/cyber-readiness

التأثير على الاقتصاد العالمي

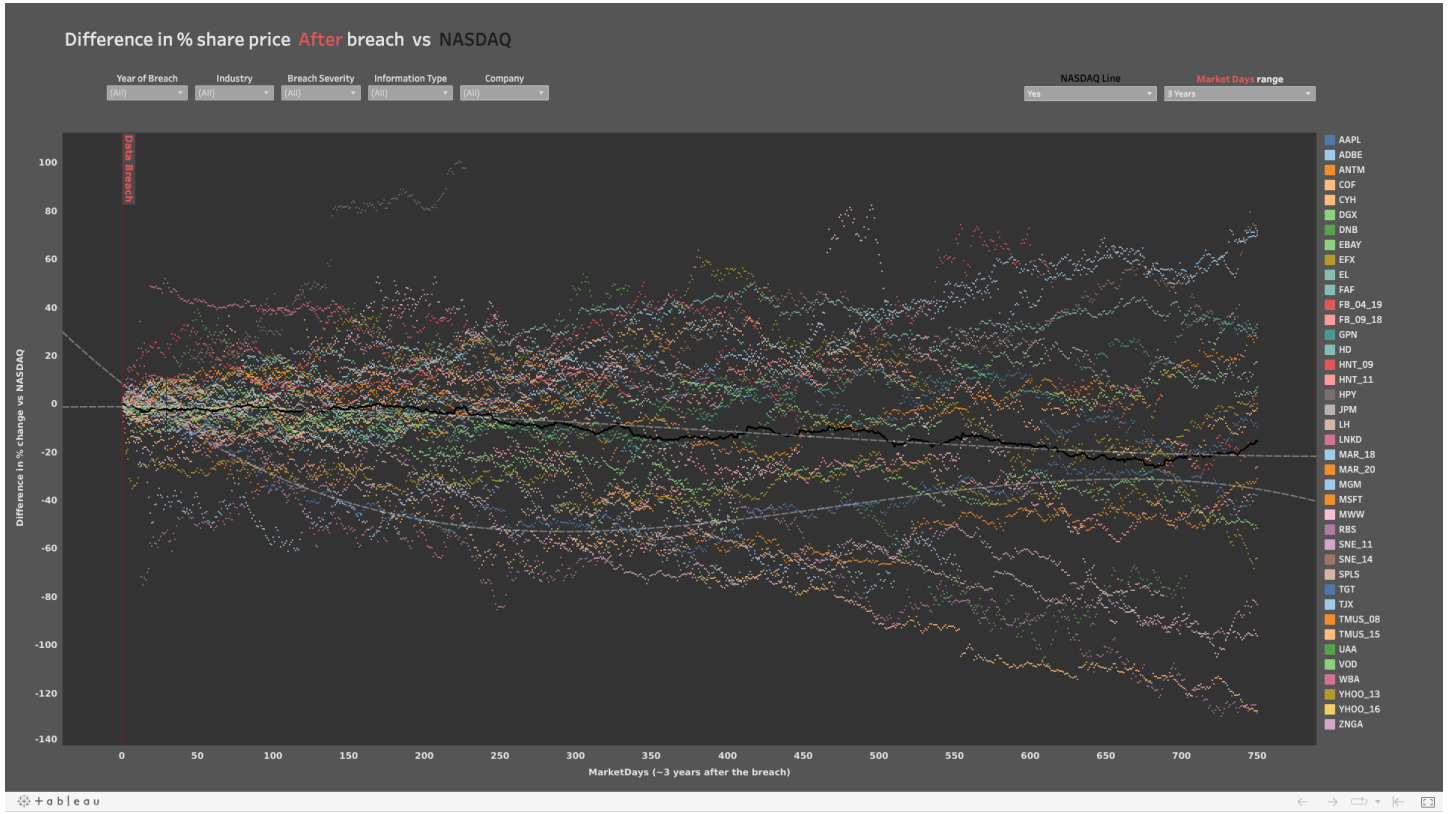
- تتوقع شركات الأمن السيبراني أن تنمو تكاليف الجرائم الإلكترونية العالمية بنسبة 15٪ سنويًا على مدى السنوات الخمس المقبلة ، لتصل إلى 10.5 تريليون دولار أمريكي سنويًا بحلول عام 2025 ، ارتفاعًا من 3 تريليونات دولار أمريكي في عام 2015.

- تزداد عمليات الاحتيال في الإعلانات الرقمية بشكل حاد. تخسر صناعة الإعلانات ما يقرب من 51 مليون دولار يوميًا بسبب الاحتيال في الإعلانات وبحلول عام 2023 سيرتفع هذا الرقم إلى 100 مليار دولار سنويًا ، وفقًا لتقرير بلومبرج.

المصدر: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/

تأثير الهجمات على قيمة أسهم الشركات

على المدى الطويل خلال، انخفض قيمة أسهم الشركات التي تعرضت للاختراق بنسبة 8.6٪ للسنة الأولى، 11.9٪ للسنة الثانية، وصولاً إلى 15.6٪ للسنة الثالثة

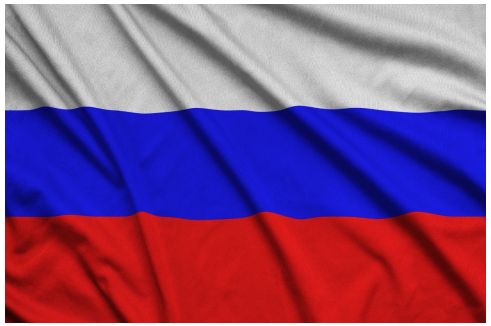


المصدر/https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

بالنسبة لتركيا

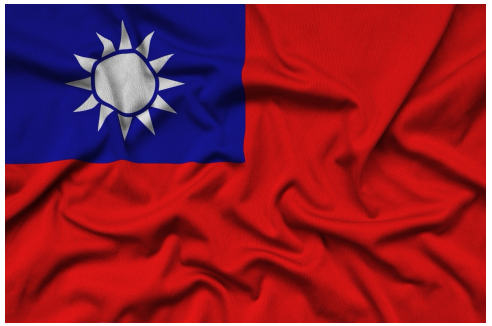
تقع تركيا في المركز الثالث عالميا ضمن قائمة الدول الأكثر تعرضاً للهجمات بواسطة البرمجيات الخبيثة بعد الصين وتايوان

.

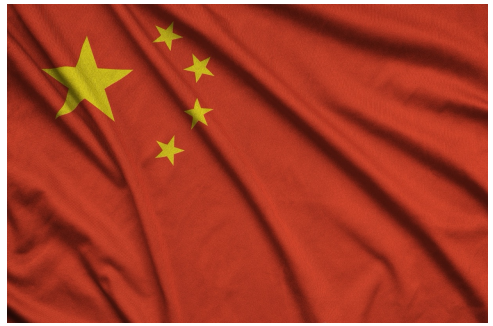


39%

40%



47%



49%

المصدر: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/

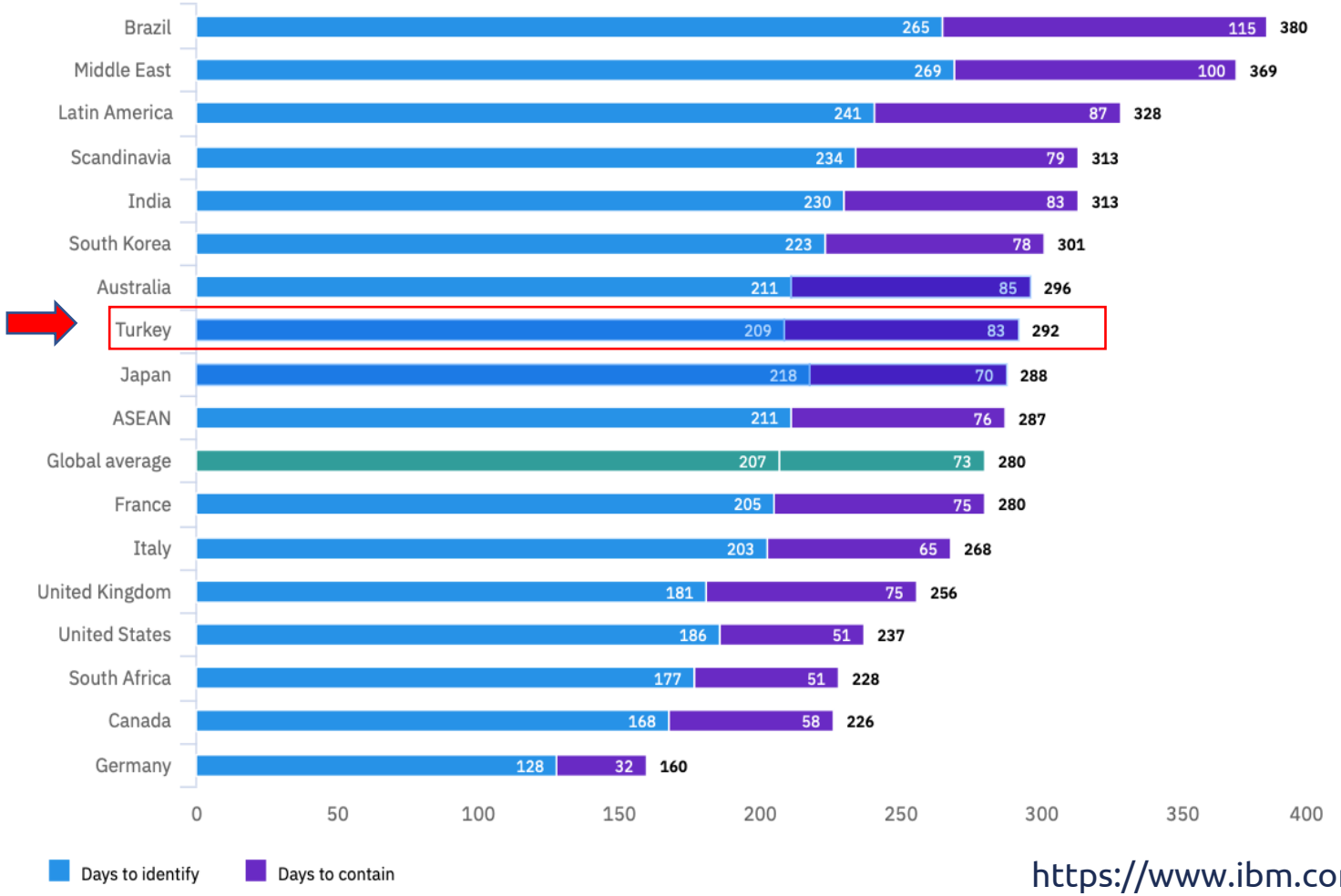
صرحت وكالة الأناضول للأنباء عن عدد الهجمات الالكترونية في تركيا، وبحسب دراسات مركز Watch Gard الأمريكي ازدادت الهجمات الإلكترونية عن طريق البرمجيات الخبيثة في تركيا خلال عام 2020 بنسبة 81٪ عن عام 2019 بمتوسط 3 هجمات في الدقيقة الواحدة أي ما يعادل 4675 هجوم الكتروني يومياً.

الهجمات على تركيا

المصدر: https://www.aa.com.tr/en/science-technology/turkey-malware-attacks-up-81-in-2020/2105600

التعرض للاختراق

متوسط الوقت لتحديد واحتواء خرق بالأيام، في تركيا متوسط زمن اكتشاف الاختراق هو 209 أيام و 82 يوم لاحتوائه، المجموع 292 يوم



المصدر: https://www.ibm.com/security/data-breach

تكلفة الهجمات الالكترونية في حال التعرض لها

بحسب تقرير تكلفة الاختراقات من IBM لعام 2021 بلغ متوسط تكلفة سرقة السجل الواحد Stolen Record

$ 171

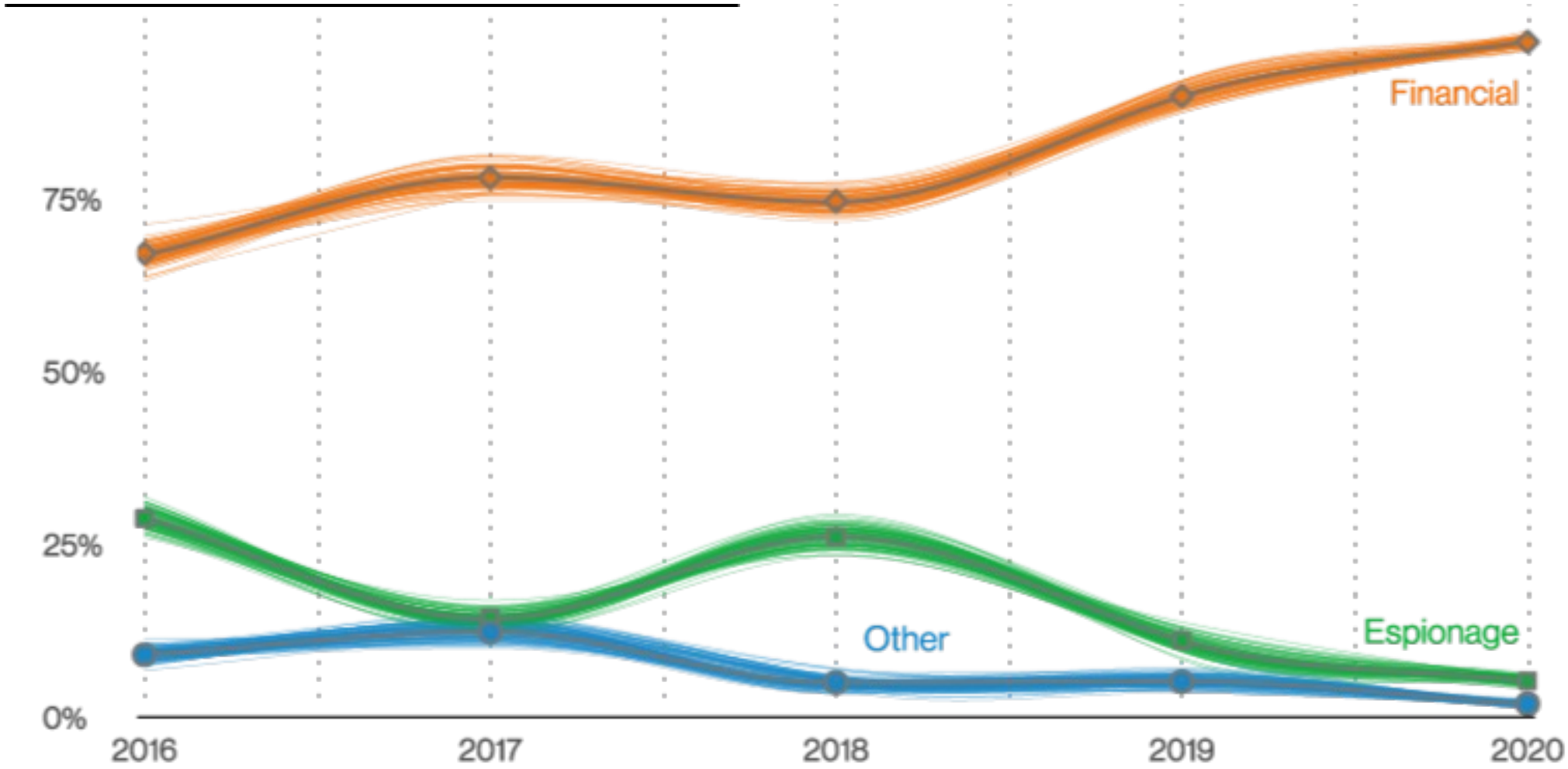
سجل يحدد الهوية الشخصية للعميل

$ 146

سجل عام

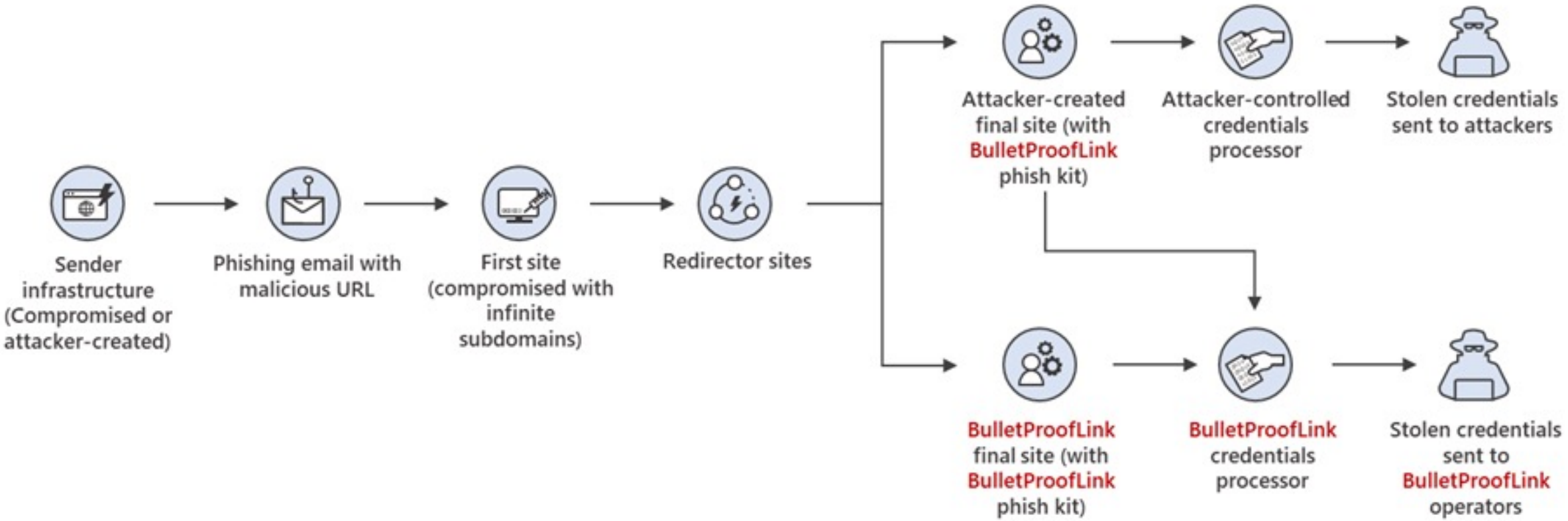
المصدر: https://www.ibm.com/security/data-breach

الدافع وراء الجريمة الالكترونية



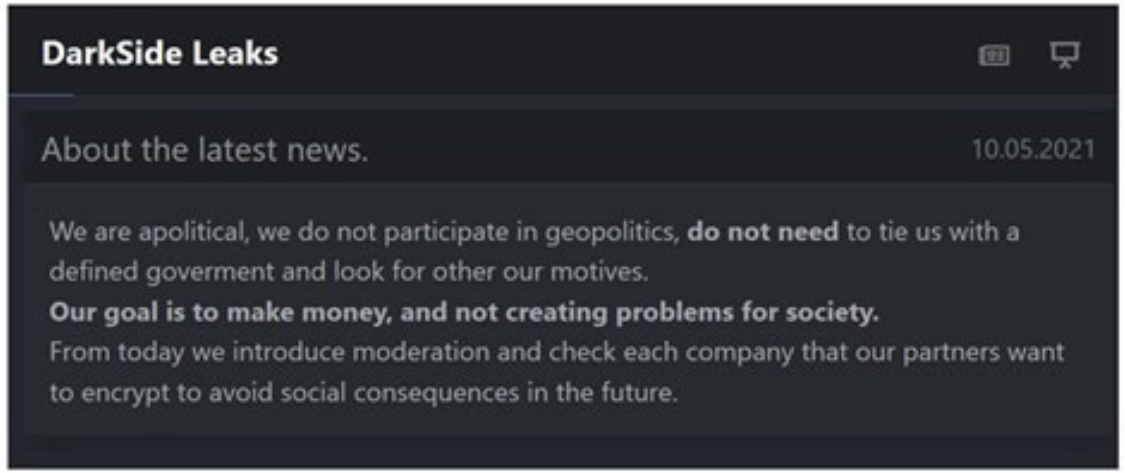
المصدر: https://www.verizon.com/business/resources/reports/dbir/

RaaS



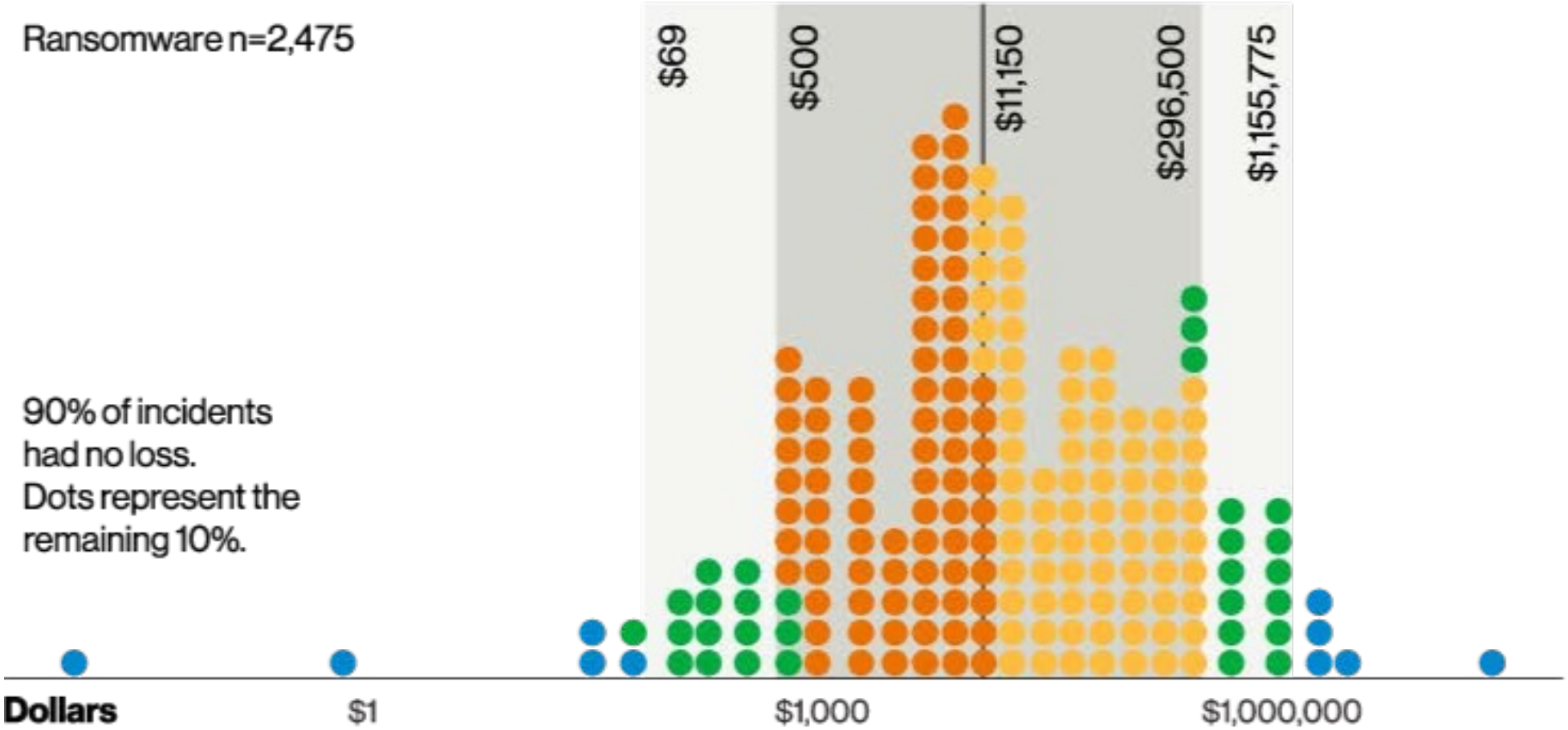
المصدر :
https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

تصريح فدية منظمة Revil الإجرامية



المصدر : https://blog.reddefenders.com/burglary-and-wars-without-blood/

هجمات طلب الفدية



المصدر: https://www.verizon.com/business/resources/reports/dbir/

هجمات بداعي التجسس

تعرضت شركة ThyssenKrupp "تيسين كروب" الألمانية للاختراق من قبل الصين وسرقة اسرار صناعية وحقوق ملكية فكرية، لم تستطع الشركة تحديد قيمة الخسارة المادية لكن تم وصفها بمئات المليارات من الدولارات.

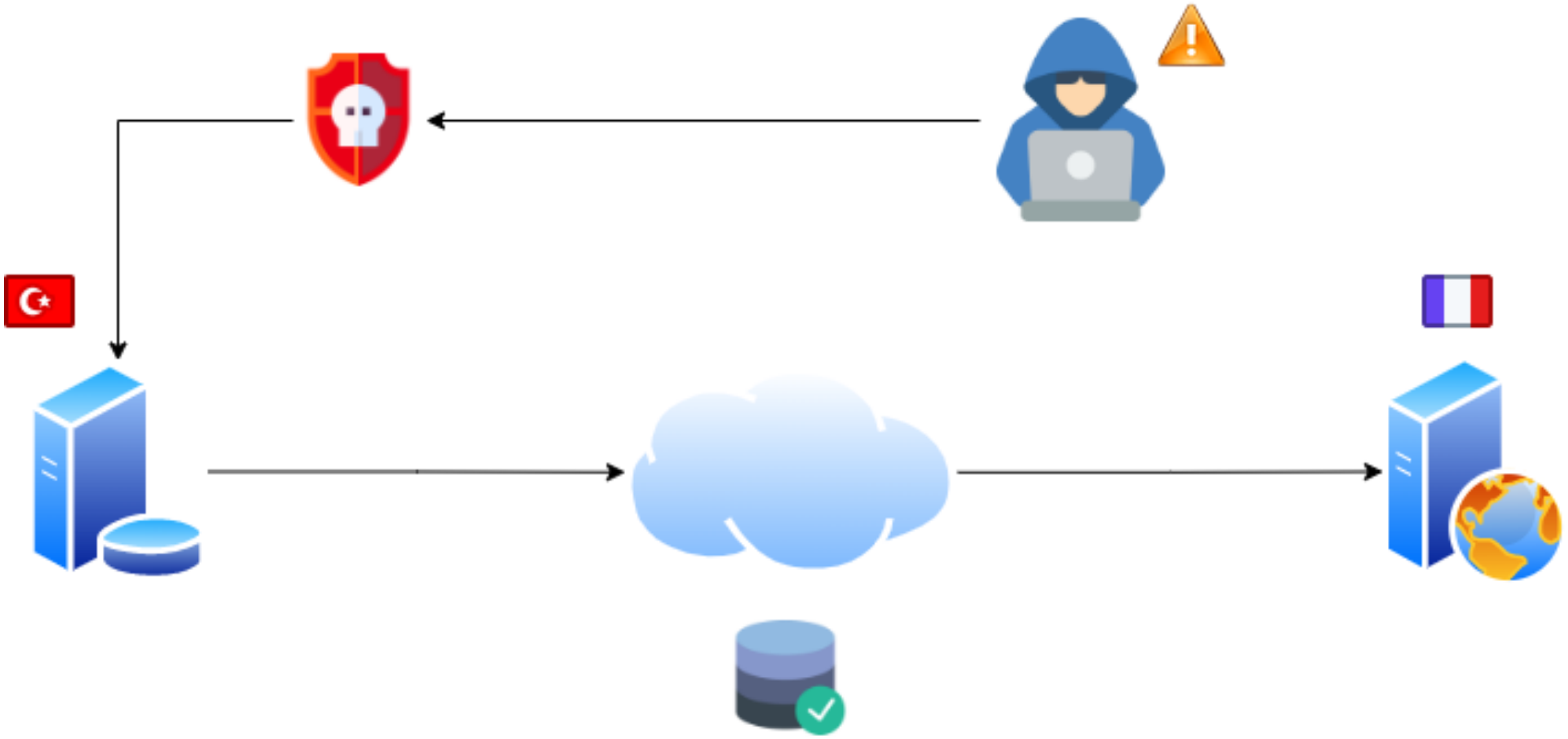
المصدر: https://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13X0VW

بعض أهم هجمات العام الماضي

محلياً

عالميا

الهجوم



سجلات العملاء والمعلومات الشخصية

سجلات البريد الإلكتروني

السجلات المالية (السجلات المحاسبية، أرقام الحسابات البنكية، أرقام بطاقات إئتمانية)

خطط العمل

أفكار تجارية جديدة

خطط التسويق

الملكية الفكرية

تصميم المنتج

طلبات براءات الاختراع

سجلات الموظفين التي يمكن أن تتضمن معلومات شخصية حساسة

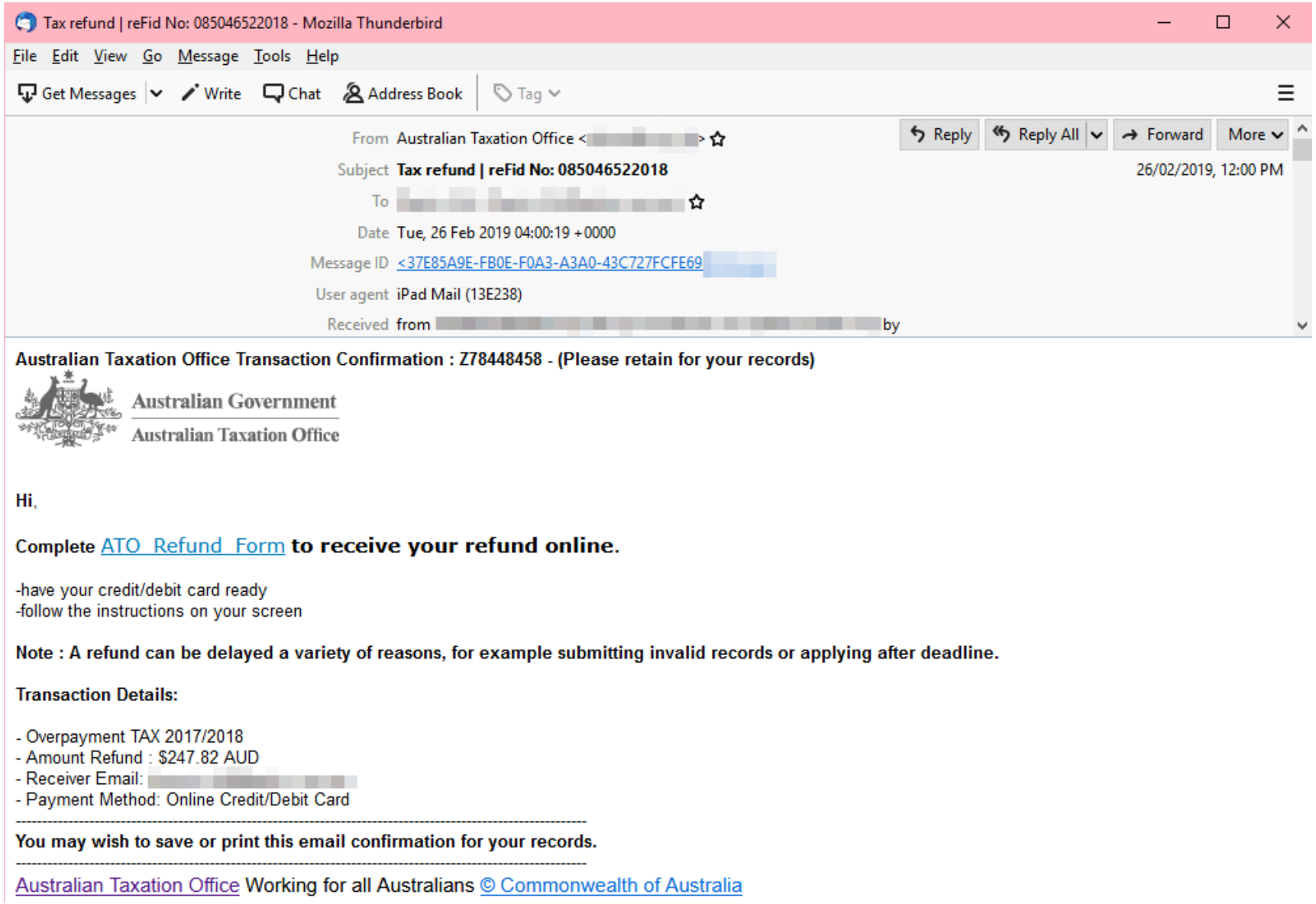
البيانات المهددة

- سجلات العملاء والمعلومات الشخصية
- سجلات البريد الإلكتروني
- السجلات المالية (السجلات المحاسبية، أرقام الحسابات البنكية، أرقام بطاقات إئتمانية)
- خطط العمل
- أفكار تجارية جديدة
- خطط التسويق
- الملكية الفكرية
- تصميم المنتج
- طلبات براءات الاختراع
- سجلات الموظفين التي يمكن أن تتضمن معلومات شخصية حساسة

أكثر الهجمات شيوعاً

- التصييد الاحتيالي
  - التصييد عبر البريد الالكتروني Phishing
  - انتحال الشخصية CEO Fraud
  - رسائل احتيالية في موسم التحصيل الضريبي Tax Scams
  - رسائل احتيالية عن طريق الفواتير Invoice Scams
  - التصييد عبر الرسائل Smishing
  - التصييد عبر الهاتف Vishing
- البرمجيات الخبيثة
- فيروسات الفدية
- الاختراق الفيزيائي عبر تجهيزات مثل فلاشات، دارات الكترونية

رسائل احتيالية في موسم التحصيل الضريبي Tax Scams



Tax refund | reFid No: 085046522018 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

Reply | Reply All | Forward | More

From Australian Taxation Office <[redacted]>

Subject **Tax refund | reFid No: 085046522018** 26/02/2019, 12:00 PM

To [redacted]

Date Tue, 26 Feb 2019 04:00:19 +0000

Message ID <37E85A9E-FB0E-F0A3-A3A0-43C727FCFE69[redacted]

User agent iPad Mail (13E238)

Received from [redacted] by

Australian Taxation Office Transaction Confirmation : Z78448458 - (Please retain for your records)

Australian Government
Australian Taxation Office

Hi,

Complete ATO Refund Form **to receive your refund online.**

-have your credit/debit card ready
-follow the instructions on your screen

Note : A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Transaction Details:

- Overpayment TAX 2017/2018
- Amount Refund : $247.82 AUD
- Receiver Email: [redacted]
- Payment Method: Online Credit/Debit Card

You may wish to save or print this email confirmation for your records.

Australian Taxation Office Working for all Australians © Commonwealth of Australia

التصييد عبر الهاتف

Vishing

فيروسات الفدية

Ransomware Attack

كيف أحمي مؤسستي من الاختراق؟

- توعية أفراد فريق العمل والموظفين بمخاطر الأمن السيبراني عن طريق تدريبات خاصة
- تنصيب مضادات فيروسات
- تحديث أنظمة التشغيل والتطبيقات بشكل دوري
- اجراء نسخ احتياطي دوري للبيانات عن طريق تجهيزات خاصة
- استخدام كلمات سر قوية "برامج إدارة كلمات مرور"
- تفعيل المصادقة الثنائية 2FA
- تدريب فريق تكنولوجيا المعلومات في شركتك
- الاستثمار في تجهيزات أمنية مثل الجدران النارية وأنظمة الحماية من الاختراق

قائمة المراجع

https://hamedalfaisal.notion.site/e890283ba83843a19dbb4ed3fb0fcaac

شكراً لكم