طرق وأساليب التحقيق الجنائي التقني

قبل كل شيء سنبدأ معكم بسرد أسباب خضوع الأجهزة للتحقيق الجنائي أو الأمني الالكتروني ومن ثم ننتقل إلى أساليبها، وفقاً للقانون الدولي للجرائم الالكترونية الموضح هنا

إن الجرائم الالكترونية تقسم إلى ثلاث أقسام :

العنف عبر الحاسوب

نذكر أمثلة عنها

- المنشورات أو التعليقات الارهابية و المثيرة للاحتقان الجماهيري.
- ومقاطع الفيديو التي تحتوي على عنف جسدي.

- الجنس للأطفال ما دون 18 سنة.

جرائم الحاسوب

وهي الجرائم التي يتم القيام بها من خلال جهاز الحاسوب بشكل مباشر مثل :

- بعض المواقع فيما يسمى بالويب العميق تستخدم التكنلوجيا لتوظيف القتلة المأجورين.
- لتنسيق الأعمال الارهابية.
- استخدام معلومات في الأذى الجسدي أو النفسي للأشخاص.
- التهديد.

الجرائم ذات الصلة بالحاسوب

وهي الجرائم التي تتطلب خبرة تقنية لكي يتم تحقيقها وتشمل جميع أنواع الهاكينغ مثل

- سرقة معلومات شخصية.
- سرقة نقود.
- اختراق اجهزة.
- التلصص على خصوصيات الآخرين.

ارفقنا روابط ضمن المصادر للمزيد من التوسع حول الجرائم الالكترونية رغم ذكرنا لأهمها.

متى يجب أن نلجأ إلى الجهات المختصة للتحقيق في أجهزة شركاتنا أو المشتبه بهم ؟

أكثر نسبة جرائم الكترونية منتشرة في الوطن العربي هي سرقة الصور إما بالإقناع أو بالخبرة التقنية ومن ثم التهديد بنشر الصور في ظل مجتمع غير متسامح أبداً مع هذا النوع من القضايا، ولذلك نتمنى رفع مستوى الوعي لدى الأهل أو لدى الفتيات في حال تم تهديدكم أو ابتزازكم بمعلومات خاصة عليكم فورا التوجه إلى السلطات المختصة في بلدكم وسيتم كشف الموضوع بسهولة كما سنوضح في بقية المقال.
أيضا بالنسبة للشباب المبتدئين في استخدام الحاسوب والذين يزورون منتديات مشبوهة لتعليم الهاكر، كما يسمونها، عليكم الحذر دائماً من الوقوع في الجرائم الالكترونية، لكي لا تتم محاسبتكم على أمور لم يكن علم بعواقبها.
في حال تعرضت أنت أو شركتك الى السرقة الالكترونية، بادر فوراً بتقديم الشكوى للجهات المسؤولة.

ما هي الوسائل والأساليب المستخدمة في التحقيق الجنائي وهل هي فعلا نافعة ؟

إن أول قاعدة يجب أن تعلمها عن التحقيق الجنائي الالكتروني هي (**حافظ على الدليل**).
في حال وجدت الحاسوب المشتبه به مطفئاً لا تشغله، وفي حال وجدته يعمل لا تطفئه، اترك كل شيء كما هو واستخدم احد تقنيات التصوير الرقمي من نوع bit by bit والتي تنشئ صورة عن محتويات القرص الصلب بشكل مطابق تماماً للنسخة الأصلية ويتوفر نوعين من هذه التقنية إما برامج نذكر منها **FTK imager**، أو أجهزة خاصة تقوم اوتوماتيكياً بتصوير الهارد كاملاً على هارد أخر كما في الصورة :

جهاز تصوير الهارد بتقنية bit to bit

ثاني شيء يقوم به المحققون هو استخدام أحد البرامج المجانية أو المدفوعة الثمن للبحث في صورة القرص المراد فحصه مع العلم أن الفحص **يشمل الملفات المحذوفة أيضاً**، وأشهر هذه البرامج هو برنامج مفتوح المصدر اسمه **autopsy** يقوم بفحص كامل صورة القرص باحثاً عن كلمات مفتاحية مدرجة من قبل المسؤول، كما يقوم البرنامج تلقائياً بتوليد تقارير مشيراً لمصدر المحتوى المخالف والإشارة إلى موقعه بدقة.

والآن مع السؤال الأهم هل هذه الطرق مجدية حقاً ؟

فمن هذا الغبي الذي لن يغير اسم الملفات المخالفة للقوانين، أو لن يشفرها، أو مثلا على الأقل يغير لاحقة ملفاتها لكي تظهر وكأنها ملفات من نوع آخر.
حسناً أبشركم بأن الأمن الالكتروني ليس بالغباء الذي كنا نعتقده فعمليات البحث التي تتم في برامج التحقيق الجنائي لا تقوم على الكلمة كما تقرأها أنت بل تقوم بتفكيك المحتوى إلى لغة الآلة وبهذا ستجد الملف المطلوب حتى لو أخفيته بأي شكل من الأشكال، وأحد الأمثلة

عن البرامج التي تقوم بقراءة الملفات وصور الهاردات بلغة الألة هو البرنامج المشهور **hex editor**، والذي لا يهمه ماذا غيرت بالملف، فهو لن يقرأه أصلاً بامتداده بل سيحوله الى لغة **hexadecimal** الخاصة بالآلة وسيبحث على هذا الأساس عن المحتوى المطلوب.

لذلك نقول للمجرمين الالكترونيين، حظاً أوفر في المرة القادمة.

للمزيد من المعلومات حول تصنيفات الجرائم الالكترونية :
http://www.hg.org/computer-crime.html

- التاريخ: 2016-12-19
- التصنيف: تكنولوجيا

#أمن معلومات #security

المصادر

- sleuthkit
- csrc
- lynda

المساهمون

- إعداد
  - عصام عباس
- تحرير
  - أنس عبود
- تصميم
  - نور سلمان
- نشر
  - عصام عباس