عملية #OPPETROL

الملخص التنفيذي

ما هي العملية "#OpPetrol"؟ ومن المسؤولون عنها؟ ولماذا يقومون بها؟ وماذا يمكن أن نتوقع نتيجة لهذه العملية؟

عملية #OpPetrol

المسؤولون عن العملية: جماعة «أنونيموس»، وهي مجموعة سياسية من نشطاء القرصنة الإلكترونية. وستقوم جماعتي أنونجوست (AnonGhost) والمخترقين الموريتانيين (Mauritanian Hackers)، على وجه التحديد، باستضافة هذه العملية.

الهدف: شن هجمات إلكترونية على شركات النفط والغاز والطاقة، ولا سيما على صناعة النفط في الشرق الأوسط.

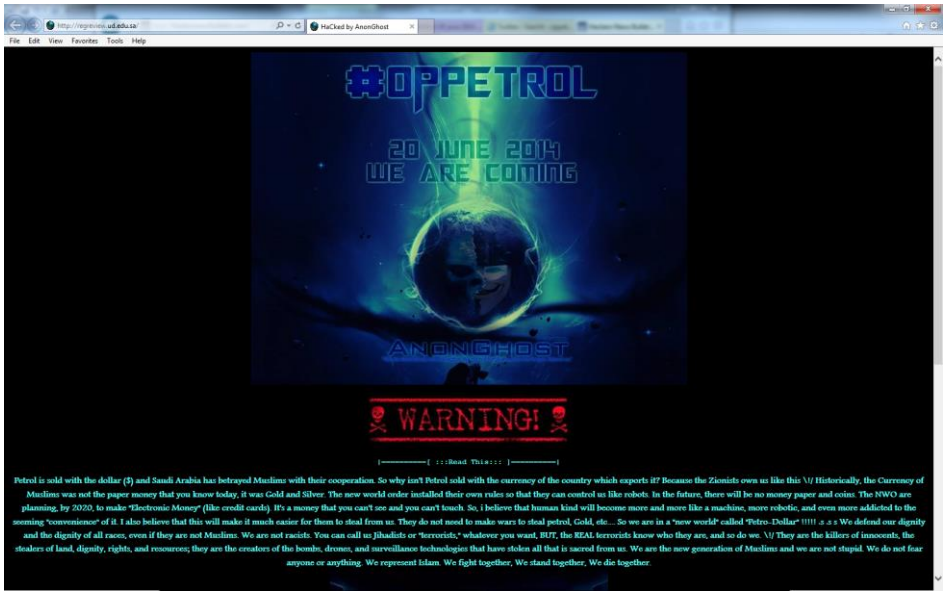
متى: قبل وأثناء وبعد يوم 20 يونيو 2014. وقد يقوم المخترقون بشن هجمات عبر مناطق زمنية مختلفة مستغلين فروق التوقيت.

لماذا: تأتي هذه العملية اعتراضًا من جماعة «أنونيموس» على استخدام عملة الدولار الأمريكي في عمليات بيع وشراء النفط.

مقدمة

قامت مجموعة من نشطاء القرصنة الإلكترونية خلال اليومين الماضيين بتدشين حملة موجهة ضد شركات النفط في عدد من الدول. ووضعت هذه المجموعة، التابعة لجماعة «أنونيموس»، خطة عمل لبدأ عملية #OPPETROL بتاريخ 20 يونيو 2014، مكررة بذلك نفس الهجمات التي وقعت تقريبًا في الفترة ذاتها من عام 2013. وقد تؤثر هذه العملية على قطاعات أخرى، مثل القطاع الحكومي.

وهناك أسباب وجيهة تدعونا للاعتقاد بأن العملية قد بدأت بالفعل، حيث تعرضت مجموعة من المواقع الإلكترونية إلى الاختراق في دول أخرى، كما هو موضح في المثال التالي (صورة من الموقع الإلكتروني للجامعة السعودية بعد اختراقه):



ماذا حدث أثناء عملية #OpPetrol التي تم تنفيذها العام الماضي؟

<u>لم يتم رصد أي هجمات مؤثرة خلال العام السابق</u>، لكن ذلك لا يعني عدم اتخاذ الاحتياطات اللازمة هذا العام.

هل ستتأثر مؤسستي بهذه العملية؟

هناك قائمة بالأهداف المحتملة متاحة على الإنترنت. ومع ذلك، وبالأخذ في الاعتبار سجل جماعة «أنونيموس»، يتضح أن هذه الجماعة معروف عنها تسريب معلومات مضللة بغرض صرف الانتباه عن أهدافها الحقيقية. وبداية من تاريخ 17 يونيو 2014، تُعد هذه العملية ذات تهديد منخفض. هذا يعني أن على جميع الجهات المعنية متابعة أعمالها كالمعتاد، مع الاستعداد للتصعيد ومراقبة ورصد أي نشاط مريب.

كيف يمكن التأكد من كون فريقي مستعدًا؟

في يوم 15 يونيو، قام مركز قطر للاستجابة لطوارئ الحاسبات "Q-CERT" بإصدار نشرة معلوماتية للقطاعات المعنية. وسيقوم المركز بالمتابعة مع إدارة نظم المعلومات بمؤسستك، وتقديم المزيد من التوجيهات للاستعداد لأي هجمات محتملة. وسيضمن التزامك بقائمة المهام المطلوبة، استعداد مؤسستك لمواجهة هذا المستوى من التهديدات. فضلًا عن ذلك، أرسلنا مجموعة من المواد للاطلاع عليها حتى يكون بقية الموظفين مستعدين أيضًا.

نوصي بأن تقوم بالاطلاع على تلك المواد، حيث يُعد المسؤولون التنفيذيون رفيعو المستوى من الأهداف القيّمة لتلك الهجمات. كما أن لدينا خدمة الدعم عبر الخط الساخن على مدار الساعة وطوال أيام الأسبوع، حتى تتمكن الإدارة لديك من الاتصال بنا عند الحاجة.

كيف يمكن أن أساعد؟

يرجو مركز قطر للاستجابة لطوارئ الحاسبات منك المتابعة مع إدارة نظم المعلومات بمؤسستك، وضمان التعامل مع هذا التهديد بجدية واتخاذ كافة التدابير الاحترازية. فعلى الرغم من فشل عملية #OpPetrol التي جرت العام الماضي في إحداث أي أضرار جسيمة، إلا أن الكثير من الأشياء يمكن أن تتغير خلال عام. ونظرًا لكون دولة قطر محل اهتمام وسائل الإعلام، ولاسيما في الآونة الأخيرة، من المتوقع أن يتم استهدافنا على نحو أكبر من العام الماضي.

ويتطلب الحفاظ على الأمن السيبراني مشاركة كافة الأطراف المعنية. فدعمك ليس مهمًا فحسب، بل و**ضروريًا** للتأكيد على ريادة دولة قطر في العالم السيبراني.

ما هي الإجراءات التي اتخذها مركز قطر للاستجابة لطوارئ الحاسبات؟

كعادته دائمًا، يعمل مركز قطر للاستجابة لطوارئ الحاسبات على مدار الساعة وطوال أيام الأسبوع لضمان سلامة شبكاتنا الوطنية. كما قمنا بتزويد إدارة نظم المعلومات بمؤسستك بتوجيهات حول كيفية الاستعداد لهذا التهديد وكيفية التعامل مع المشاكل التي قد تنشأ في حالة حدوث أي هجمات. فضلًا عن ذلك، تأكدنا من إتاحة خدمة الدعم عبر الخط الساخن (3408 4493 974+) على مدار الساعة وطوال أيام الأسبوع، وذلك لتوفير الدعم اللازم في حالات الطوارئ. وبالنسبة للحالات غير الطارئة، قمنا بتوفير قائمة بعناوين البريد الإلكتروني وأرقام الهاتف الخاصة بمكاتبنا.