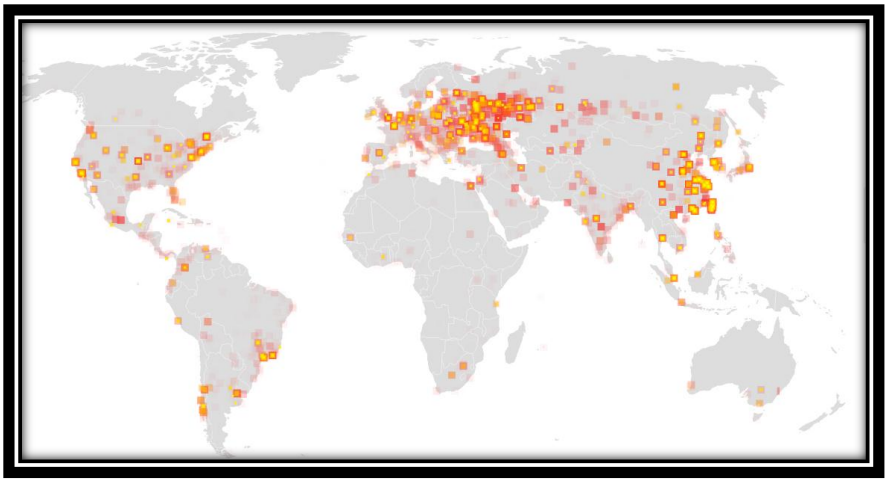
فيروس الفدية Wanna Cry_

بدأت – الجمعة ١٢ مايو ٢٠١٧ – هجمات إلكترونية «غير مسبوقة» لبرمجيات «الفدية الخبيثة» من نوع«ransomware » ، استهدفت عشرات الدول والمؤسسات حول العالم من بينها شركات اتصالات ومستشفيات، وتضرر منها عشرات الآلاف من الحواسب الآلية.

إلى أي مدى انتشرت الـ«وانا كراي»؟ وكيف ردّت مايكروسوفت؟

لاقت تلك البرمجيات الخبيثة انتشارًا واسعًا حول العالم، وقدّرت شركة أفاست للبرمجيات ومضادات الفيروسات، وصول الـ«وانا كراي» إلى 99 دولة حول العالم، وإصابتها لـ٥٧ ألف جهاز عالميًا، ووصلت برمجيات الفدية الخبيثة إلى دول كالولايات المتحدة وبريطانيا والصين وإسبانيا والبرتغال وإيطاليا وفيتنام، فيما كانت دول: روسيا وأوكرانيا وتايوان الأكثر استهدافًا بالبرمجيات الخبيثة.



خريطة تظهر انتشار الـوانا كراي حول العالم (المصدر :نيو يورك تايمز)

كيف يمكن لفيروس الفدية أن يخترق أجهزتك؟

تصل رسالة أو رابط من شخص مجهول، ويكون محتوى الرابط عبارة عن ملفّ يحتوي على برمجيات خبيثة، ثم يغري المرسل الضحية بتنزيل الملف عبر خداعه بأنه ملفّ مهم أو شخصي، فيقوم المستخدم بتحميل الملفّ في حاسبه الآلي أو هاتفه الذكي.

على إثر ذلك يعمل الفيروس على تشفير البيانات المهمة في الجهاز أو تشفير الجهاز بأكمله، بحيث لا يستطيع المستخدم الوصول إلى بياناته، ثم يطلب المجرم من الضحية مبلغاً مالياً "فدية" مقابل فكّ التشفير عن البيانات وإعادتها لطبيعتها.

صورة توضح ما يظهر على جهاز الضحية التي شُفرت ملفاته

ليس هذا فحسب، وإنما يضع القراصنة أيضًا حدًا زمنيًا مدته ثلاثة أيام للدفع، وإن لم تدفع الضحية الفدية المطلوبة قبل انتهاء الحد الزمني، تتضاعف لتصل إلى ٦٠٠ دولار، أما إذا تأخر الضحية عن الدفع قبل مرور نحو سبعة أيام من تشفير الملفات؛ فإنه سيفقدها تمامًا بحسب القراصنة.

وقد وصفت وكالة تطبيق القانون الأوروبية التي تعرف باسم« اليوروبول «تلك الهجمات الإلكترونية الضخمة بأنها «غير مسبوقة»، وأفادت الوكالة السبت بأن الهجمات تتطلب تحقيقًا دوليًا معقدًا للتعرف على القراصنة الذين يقفون وراءها.

علامات ظهور الفيروس على جهازك (عامة لاغلب انواع الفيروسات):

وفق مشاهده للمدون أحمد الجرنوسي رابط الفيديو/ https://www.youtube.com/watch?v=8GjpCK4wVes&t=188s

١) ظهور رسائل غريبه على الجهاز تظهر وتختفي
٢) بطء في عمل الجهاز رغم مواصفاته العاليه
٣) تغير الامتداد الخاص بالرامج التنفيذيه التي تنتهي بـ .exe
٤) اختفاء وظهور بعض البرامج من تلقاء نفسها

كيف تحمي جهازك من الإصابة بتلك الهجمات؟

-تجميع من قناة المدون أحمد الجرنوسى –

https://www.youtube.com/watch?v=8GjpCK4wVes&t=188s

١) عدم فتح الروابط والملفات التي قد تصل إليهم من مصادر مجهولة، في محاولة خداع ومن ثم اختراق الاجهزه.
٢) عمل نسخه احتياطيه من الملفات على الجهاز على - external hard"هارد خارجي"
٣) الاحتفاظ بنقطة استعادة النظام في الويندوز restore pointحتى تتمكن من العودة للوضع الاصلي لنظام التشغيل على الجهاز

٤) عدم فتح موقع على الانترنت لا يحتوي على secure وعلامة القفل ، خاصة اذا كانت مواقع ستوقوم فيها بعملية شراء

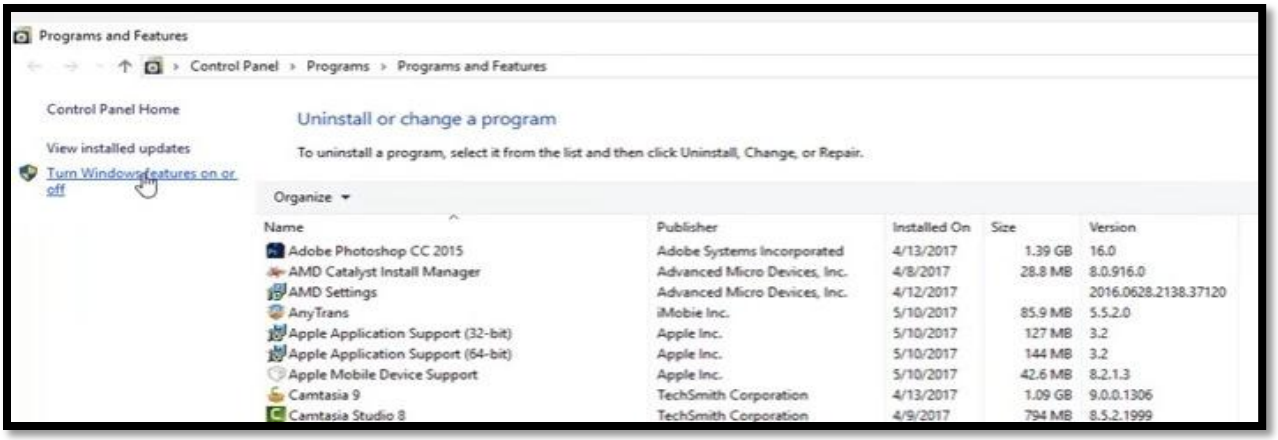
ولسد الثغره الموجوده في نظام تشغيل الـ WinXP عليك باتباع الاتي:

١) متابعة التحديثات الخاصه بنظام التشغيل من على موقع مايكروسوفت – بالطبع لديك النسخة الاصلية حتى تتمكن من اتمام عملية التحديث.

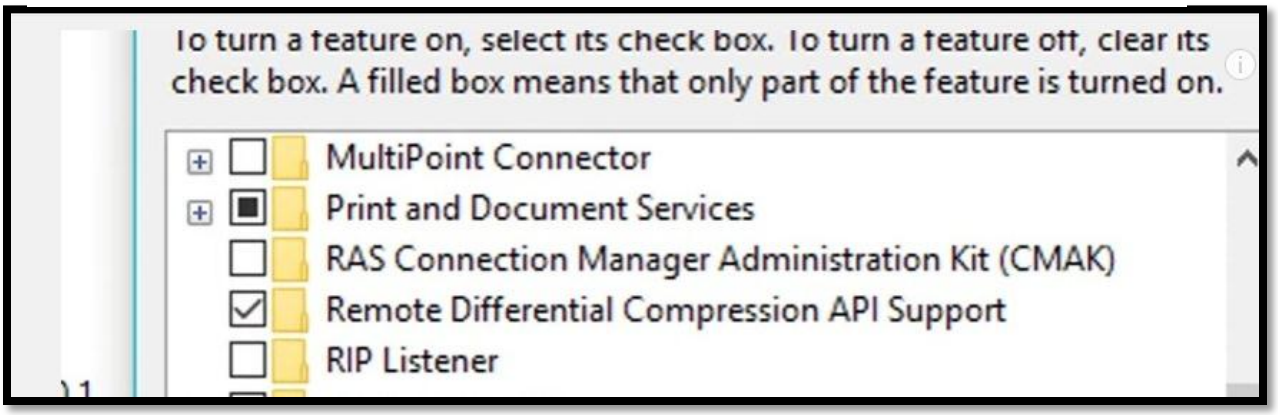
٢) اتبع الخطوات التاليه من على جهازك بنظام WinXP:

١.اختار control panel ثم programs and feature

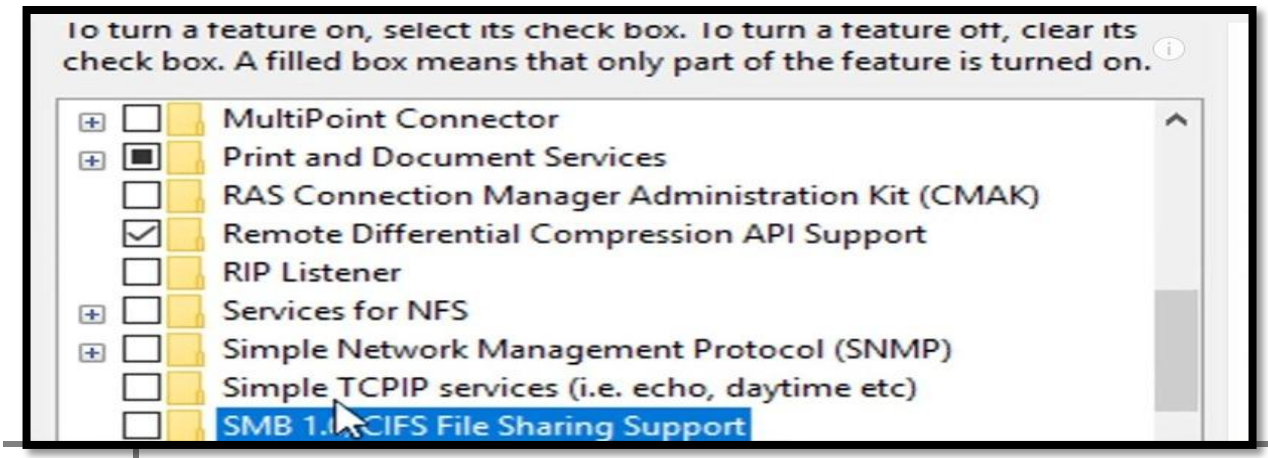
٢. اختار turn windowsdeature on or off



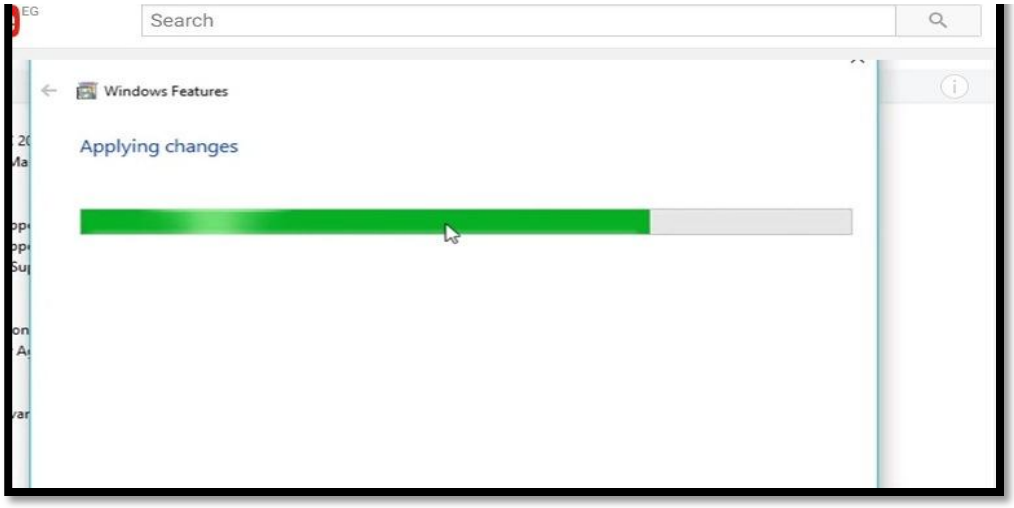
٣. نبحث عن Remote Diferential Compression API Support



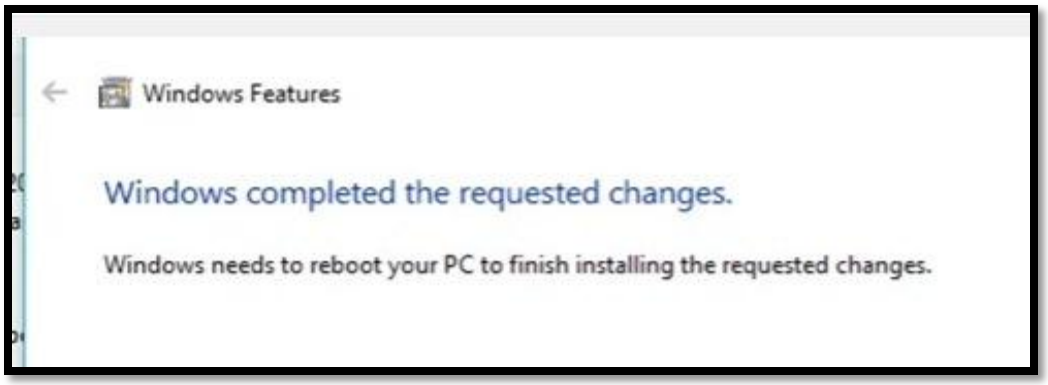
٤. نقوم بالغاء العلامة من امامها



٥. تظهر الرساله التاليه التي توضح تطبيق التغير:



٦. تظهر رسالة تفيد باتمام قبول التغييرات



لمزيد من المعلومات يرجى زيارة المواقع الاكترونيه التاليه:

http://www.bbc.com/arabic/science-and-tech-39911700

http://alkhaleejonline.net/articles/1494756760993844700/%D8%A5%D9%86%D9%81%D9%88%D8%AC%D8%B1%D8%A7%D9%81%D9%8A%D9%83-%D9%83%D9%8A%D9%81-%D8%AA%D8%AD%D9%85%D9%8A-%D9%86%D9%81%D8%B3%D9%83-%D9%85%D9%86-%D8%A7%D9%84%D9%81%D8%AF%D9%8A%D8%A9-/%D8%A7%D9%84%D8%AE%D8%A8%D9%8A%D8%AB%D8%A9

https://www.youtube.com/watch?v=8GjpCK4wVes&t=188