Número 86

Notibytes

1

Julio de 2018
Año 12

Universidad Distrital Francisco José de Caldas - Facultad Tecnológica
Proyecto Curricular Tecnología en Sistematización de Datos e Ingeniería en Telemática.

EDITORIAL

Los criminales son los visitantes más fieles de los comercios electrónicos

De acuerdo con un informe de la empresa de seguridad digital Shape Security, 90 % de los intentos de acceso al comercio electrónico en el mundo proviene de criminales que han robado las credenciales de millones de personas.
El método es el siguiente. Una empresa, ojalá una bien grande, como Yahoo o Equifax, pierde la información personal de sus usuarios en una filtración o un ataque digital: esto implica la publicación de información personal de miles o millones de personas. Desde preguntas y respuestas de seguridad, pasando por fechas de cumpleaños, nombres verdaderos, direcciones de correo y, claro, contraseñas.
Dado que una enorme cantidad de personas no actualiza sus contraseñas y, en general, utiliza una sola para decenas de servicios, es posible para un atacante probar con los datos robados de estas filtraciones en cientos o miles de comercios electrónicos en el mundo.
¿Qué buscan los atacantes? Desde transferencias de dinero, pasando por reservas de tiquetes aéreos, hasta queso y botellas de vino costosas.
Según el informe de Shape Secutiry, empresa con sede en Silicon Valley, el sector que más presenta accesos con registros robados (una técnica conocida popularmente como credential stuffing) son los comercios electrónico (91 %), seguido de las aerolíneas (60 %), banca de consumo (58 %) y cadenas hoteleras (44 %).
Curiosamente, los sitios de entretenimiento para adultos no presentan este tipo de accesos. Y esto resulta interesante porque no sólo comprenden a millones de usuarios, sino que muchas de estas páginas requieren la vinculación de una tarjeta de crédito o un método de pago electrónico, de la misma forma que un comercio electrónico de ropa, por ejemplo.
Los investigadores de Shape tienen varias hipótesis para explicar este hallazgo: los sitios de porno invierten más en tecnología y seguridad que otros (posible, aunque la diferencia no debería ser tan significativa) o simplemente no reportan cuando pierden la información personal de sus usuarios, o puede que tampoco se hayan dado cuenta.
Sólo en el año pasado, Shape calcula que 2.300 millones de credenciales de acceso fueron robadas de las bases de datos de más de 50 organizaciones a nivel global.

Resumen tomado de: elespectador.com, Tecnología, 22 de Julio/ 2018
https://www.elespectador.com/tecnologia/los-criminales-son-los-visitantes-mas-fieles-de-los-comercios-electronicos-articulo-801686

La tecnología que permite ver a través de las paredes.

¿Alguna vez soñaste con tener una visión de rayos X como Supermán? Un grupo de científicos del MIT ha hecho realidad ese sueño gracias a un software de inteligencia artificial. ¿Cómo lo lograron?
Ver a través de las paredes como Supermán siempre fue cosa de la ciencia ficción. Pero ya es una realidad. Al menos, dentro del laboratorio del prestigioso MIT (Instituto Tecnológico de Massachusetts), en Estados Unidos.
Un grupo de científicos ha desarrollado un software capaz de identificar con gran exactitud si alguien se encuentra al otro lado de un muro opaco y cómo se mueve.
El equipo, dirigido por la investigadora Dina Katabi, del Laboratorio de Ciencias de la Computación e Inteligencia Artificial (CSAIL) del MIT, creó un sistema basado en inteligencia artificial capaz de identificar y recrear movimientos humanos.
Pero, ¿cómo funciona y cómo garantizar que no se use para espiar a los demás?

El poder de la radiofrecuencia.

Los especialistas le dieron el nombre al software el nombre de RF-Pose y a la tecnología que lo rige EL DE RF-Capture, porque utiliza ondas de radiofrecuencia (RF).
"Usamos una cámara y tomamos imágenes de gente en un lugar, y emitimos allí señales radiofónicas", le dijo Katabi a la BBC.
Poco a poco, los informáticos fueron enseñando a la máquina cómo "ver" usando varios ejemplos para identificar a las personas. Así, la red neuronal puede analizar las señales y generar una figura esquelética en 3D que camine, se siente, corra, baile o gesticule como un humano, imitando los movimientos que está haciendo la persona en ese momento.
El MIT espera que dentro de unos años este software les sirva a los médicos para identificar señales tempranas de enfermedades como el Parkinson, la esclerosis múltiple o la distrofia muscular, sobre todo en personas de edad avanzada.
La idea es entender mejor la progresión de esos males que afectan al movimiento corporal, pero también ayudar a las personas mayores a tener más independencia.
De hecho, el MIT asegura que su equipo está colaborando actualmente con doctores para comenzar a aplicar el sistema en el campo de la medicina.

La tecnología es capaz de identificar con eficacia a alguien en una fila de 100 personas en el 83% de los casos. "No ves detalles de la cara o los dedos de la persona, pero puedes hacerte una idea de la altura y anchura de la persona", le contó a la BBC Fadel Adib, otro de los científicos involucrados en el proyecto.
"En el futuro podremos ver a través de las paredes incluso en alta definición", agregó. "Y probablemente también a través de los cuerpos de la gente usando señales inalámbricas".
Desarrollarlo no fue fácil: hizo falta más de una década y reunir miles de imágenes de personas en movimiento. El sistema crea lo que se conoce como "imágenes de calor" y las convierte en figuras que se mueven en el espacio, identificando las distintas partes del cuerpo y mostrando los movimientos de forma natural.
Más allá de la medicina, el sistema podría usarse en el sector de los videojuegos, el entretenimiento o la seguridad. Pero también podría tener aplicaciones maliciosas o que presenten dilemas éticos.

Solo con consentimiento
Uno de los puntos principales para que funcionara era lograr proteger la privacidad de los usuarios.
"Si alguien quiere usar esta tecnológica para monitorear a alguien sin su consentimiento, tenemos un test que hace que el dispositivo compruebe si la persona dio su consentimiento", explicó Katabi.
"Después separamos cualquier información identificable y la encriptamos".
"Tienen que existir políticas que regulen cómo se usa la tecnología".
¿Serán estos los primeros pasos de una tecnología que será omnipresente dentro de unos años?

Resumen tomado de: semana.com, Tecnología, 12 de Julio de 2018.
https://www.semana.com/tecnologia/articulo/la-tecnologia-que-permite-ver-a-traves-de-las-paredes/575036

CONOZCAMOS NUESTROS PRINCIPIOS...

Tecnología en Sistematización de Datos

Visión:
El proyecto curricular de Tecnología en Sistematización de Datos deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportados en el uso de las herramientas tecnológicas suficientes para mantenernos ubicados en la frontera del conocimiento de los sistemas modernos de procesamiento y transmisión de información

Misión:
Formación de Tecnólogos íntegros, críticos e idóneos, altamente calificados en el área de los sistemas informáticos, capaces de identificarlos y mejorarlos empleando la ciencia y la tecnología para optimizar su funcionamiento.

Ingeniería en Telemática

Visión:
El proyecto curricular de Ingeniería en Telemática deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportado en la capacidad de convertir sistemas convencionales de comunicaciones en otros que puedan calificarse de avanzados, tanto por sus características teleinformáticas actuales como por sus proyecciones de mejoramiento y crecimiento.

Misión:
La misión del Proyecto curricular de Ingeniería en Telemática constituye la formación de profesionales con un alto nivel académico e investigativo, humanamente formados, científicamente fundamentados y tecnológicamente calificados en el área de telemática, capaces de servir a la sociedad y dar soluciones convenientes a sus requerimientos y necesidades mediante la creación, desarrollo y adaptación de tecnologías, promoviendo el cambio y la innovación

Boletín Informativo

Boletín Noti-bytes

Los 10 peores ataque hacker de la historia

No existe ningún sistema informático invulnerable, y los hackers aprovechan esto en su beneficio: encuentran vulnerabilidades y las explotan para perpetrar ataques maliciosos. Dependiendo de su naturaleza, características y objetivos, algunos malware son más mortíferos que otros.
A continuación te dejamos la lista de los peores ataques hacker de la historia, ordenados cronológicamente.

- *Gusano Morris:* El gusano Morris es uno de los peores virus informáticos de la historia. Fue creado por el estudiante universitario Robert Morris, a quien debe su nombre, y se propagó por Internet (entonces ARPANET) el 2 de noviembre de 1988. El objetivo de este ataque consistía en obtener las contraseñas de otros ordenadores aprovechando algunos defectos en la versión de Unix **de** la Universidad de Berkeley. El gusano Morris es el primer malware autorreplicable, diseñado para reproducirse a sí mismo de manera indefinida en lugar de eliminar datos. Afectó a unos 6.000 de los 60.000 servidores conectados a la red, incluyendo el centro de investigación de la NASA, dejando casi inútiles algunos de ellos.
- *ILOVEYOU*: Otro de los peores ataques hacker de la historia es el del virus ILOVEYOU. El virus responsable del ataque es un gusano que se autoreplica y sobrescribe con su código los ficheros con extensiones .VBS y .VBE, y elimina los ficheros con extensión .JS, .JSE, .CSS, ,WSH, .SCT y .HTA, creando otros con el mismo nombre y extensión .VBS son su código. Además, también elimina los archivos .JPG, .JPEG, .MP3 y MP2. El gusano ILOVEYOU se propagó como la pólvora en el mes de mayo del año 2000. Utilizó el correo electrónico como vector para extenderse a todo el mundo, reenviándose a la libreta de direcciones de cada víctima una vez que era abierto y ejecutado.

- *Code Red*: es otro de los peores ataques hacker de la historia. Este gusano, que fue descubierto en julio de 2001, explotaba una vulnerabilidad muy común conocida como buffer overflow, utilizando una larga cadena de caracteres hasta desbordar el buffer y colapsar el servidor. El gusano Code Red consiguió una gran notoriedad en el momento debido a que colapsó todos los servidores web de la Casa Blanca a través de un ataque DDoS. El virus infectó a más de 225.000 sistemas en todo el mundo y supuso unas pérdidas de más de 1.200 millones de dólares.
- *Gusano Storm*: es un gusano que empezó a propagarse por correo electrónico a principios de 2007. El malware recibe su nombre del asunto que utilizaba el email, que suplantaba una noticia de una catastrófica tormenta en Europa que había producido 230 muertos. El gusano Storm es un troyano con distintas versiones para ordenadores Windows que tenía el objetivo de sumar los equipos infectados a la botnet Storm. Se estima que en septiembre de 2007 contaba con entre 1 y 10 millones de ordenadores zombi y ha sido utilizada para perpetrar diversas actividades criminales.
- *Stuxnet*: En junio de 2010, la compañía de seguridad bielorrusa VirusBlokAda descubrió el virus Stuxnet, un gusano capaz de espiar y reprogramar sistemas industriales, entre ellos infraestructuras críticas como centrales nucleares. De acuerdo con medios como *BBC* o *Daily Telegraph*, el objetivo de este gusano eran las infraestructuras de alto valor de Irán, ya que el 60% de los ordenadores infectados estaban en este país. Los equipos infectados en Irán ascendieron a casi 63.000, poco más de 13.000 en Indonesia, unos 6.500 en India, casi 3.000 en Estados Unidos y cerca de 2.500 en Australia.
- *Zeus*: En septiembre de 2011 comenzó a desarrollarse otro de los ataques hacker más peligrosos de la historia. En esta ocasión el protagonista fue Zeus, un malware que se propagaba mediante campañas de phishing. Después de infectar el dispositivo, era capaz de interceptar las transacciones bancarias de la víctima y copiar sus credenciales de inicio de sesión.*Carbanak*: es una campaña de tipo APT (Advanced persistent threat o amenaza persistente avanzada, en español) dirigida contra instituciones financieras que empezó a atacar en el año 2014. El ataque comenzaba cuando los criminales conseguían infiltrarse en la intranet del banco, algo que conseguían mediante correos electrónicos fraudulentos. Después, el malware se hacía con el control del equipo y el grupo de hackers lo utilizaba como punto de acceso a la entidad. A continuación, analizaban las herramientas financieras empleadas por el banco, para luego retirar el dinero mediante transferencia de dinero SWIFT o creando cuentas bancarias falsas. Mediante este malware, los cibercriminales consiguieron robar cerca de 1.000 millones de dólares a más de 100 instituciones financieras en unos 40 países distintos.
- *WannaCry*: sin lugar a dudas, el del ransomware WannaCry ha sido uno de los peores ataques hacker de la historia y el más importante de la época actual, cuyas pérdidas, alcance y repercusiones han supuesto un antes y un después en el mundo de la ciberseguridad. WannaCry se propagó el 12 de mayo de 2017 y no solo consiguió paralizar miles de empresas de todo el mundo, sino que también puso de manifiesto lo frágil que puede ser el sistema ante determinados ataques. El malware era capaz de secuestrar un ordenador encriptando todos sus archivos y bloqueando el acceso del administrador y los demás usuarios. Para devolver el control del equipo, como otros ransomware pedía el pago de un rescate. El ransomware WannaCry afectó a más de 360.000 equipos de 180 países.

Resumen tomado de: computerhoy.com, Tecnología, 21 de Julio de 2018,
https://computerhoy.com/listas/tecnologia/10-peores-ataques-hacker-historia-277193

Pare Oreja

Dicen que….

- **Inicio de clases segundo semestre /2018**
  - **Agosto 1.**
- **Terminación de clases:**
  - **Noviembre 17 de 2018.**
- **Adición de asignaturas:**
  - **Hasta el 10 de Agosto/2018.**
- **Cancelación de asignaturas:**
  - **Hasta el 24 de Agosto /2018.**
- **Fechas límite para la captura de notas son:**
  - Primer corte: Septiembre 29 de 2018.
  - Segundo corte: Noviembre 17 de 2018.
  - Examen final: Diciembre 8 de 2018**.**

Link de Interés:

- **¿Cambiarán las nuevas tecnologías y el análisis de datos el futuro de la educación?**
  https://www.semana.com/educacion/articulo/cambiara-la-inteligencia-artificial-y-el-analisis-de-datos-el-futuro-de-la-educacion/574986

- **Por qué los cables baratos pueden matar tu celular al cargarlo**
  https://www.semana.com/tecnologia/articulo/por-que-los-cables-baratos-pueden-matar-tu-celular-al-cargarlo/573293

SI QUIERES FORMAR PARTE DE LA ELABORACIÓN DE ESTE BOLETÍN PREGUNTA EN LA COORDINACIÓN DE LA CARRERA
tecsistematizaciondatos@udistrital.edu.co