Número 109

Febrero de 2021
Año 15

Not@-Bytes

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

EDITORIAL

El tapabocas inteligente de Razer: sostenible, transparente y con iluminación personalizada

Razer presentó en el CES 2021 su concepto de máscara inteligente, que evita la generación de deshechos, permite ver los gestos de la cara y cuenta con iluminación personalizada.

El concepto de máscara de Razer, Project Hazel, cuenta con el respirador de calidad médica N95 que utiliza ventiladores activos desmontables y recargables, así como cápsulas inteligentes que regulan el flujo de aire para una transpirabilidad óptima.

La compañía explicó que los SmartPods de alta eficacia de filtración bacteriana (BFE) filtran al menos el 95 % de las partículas en el aire y tienen una alta resistencia a fluidos, como recoge en un comunicado.

Razer también pensó en la interacción social, y por ello Project Hazel tiene un diseño claro y transparente, que permite a las demás personas ver los gestos faciales, y facilita que las personas con dificultad auditiva puedan leer los labios.

Tiene también luces interiores que se activan automáticamente en la oscuridad, para que los usuarios puedan seguir expresándose independientemente de las condiciones de iluminación. Y para potenciar la voz, Razer ha incluido su tecnología VoiceAmp, que utiliza un micrófono y un amplificador para mejorar el habla del usuario.

Project Hazel utiliza ventiladores de tipo disco reemplazables y recargables que se pueden desinfectar dentro de su caja de carga rápida inalámbrica de doble propósito de uso, con una luz interior UV desinfectante. Esto evita la generación de desechos. La carga completa permite el uso de la máscara durante todo el día.

Esta máscara es impermeable y resistente a los arañazos. Está hecha de plástico reciclable y forrada de silicio, con refrigeración y regulación activa de aire. Cuenta, además, con dos zonas de iluminación con tecnología Razer Chroma RGB personalizable, que ofrece 16,8 millones de colores y un conjunto de efectos de iluminación dinámica.

Resumen tomado de: www.elespectador.com, Tecnología, 13 de enero/2021
https://www.elespectador.com/noticias/tecnologia/la-mascara-inteligente-de-razer-sostenible-transparente-y-con-iluminacion-personalizada/

Comité Editorial:
Carlos Alberto Vanegas,
Sonia Alexandra Pinzón,

La lucha contra las tecnologías de reconocimiento facial.

La organización de defensa de derechos humanos Amnistía Internacional (AI) lanzó este lunes una campaña global para buscar prohibir estas herramientas.

"Existe el riesgo de que el reconocimiento facial se utilice como un arma por las fuerzas del orden contra comunidades marginadas por todo el mundo", aseguró en un comunicado de prensa el investigador de Inteligencia Artificial y Derechos Humanos de Amnistía Internacional, Matt Mahmoudi.

"Desde Nueva Delhi hasta Nueva York, esta tecnología invasiva pone nuestras identidades en nuestra contra y mina los derechos humanos", agregó.

La campaña de Amnistía Internacional, llamada "Ban the Scan" (Prohibir el escaneo), arranca en Nueva York para enfocarse más tarde en el uso de este tipo de identificación por todo el mundo en 2020.

El grupo asegura que los sistemas de reconocimiento facial son una forma de vigilancia en masa que viola los derechos a la privacidad y amenazan los derechos a la libertad de asamblea pacífica y de expresión.

Además, apuntan, exacerba el racismo sistemático, puesto que podría afectar más a personas de color, que ya sufren discriminaciones y violaciones de sus derechos por parte de las fuerzas del orden, dice Amnistía Internacional.

"Los neoyorquinos podrían salir y hacer su vida sin que sean rastreados por el reconocimiento facial. Otras importantes ciudades en EE.UU. ya han prohibido el reconocimiento facial, y Nueva York debería hacer lo mismo", instó Mahmoudi.

En la Gran Manzana, Amnistía Internacional colabora en este esfuerzo con otras organizaciones como Inteligencia Artificial para el Pueblo, la Unión de Libertades Civiles de Nueva York o la Coalición para la Privacidad de Nueva York.

"El uso policial de la tecnología de reconocimiento facial sitúa a los neoyorquinos en perpetuas ruedas de identificación y viola nuestros derechos a la privacidad. El reconocimiento facial es ubicuo, no está regulado y debería estar prohibido", afirmó en el comunicado Mutale Nkonde, fundadora y consejera delegado de Inteligencia Artificial para el Pueblo.

Este tipo de tecnología puede ser desarrollada copiando imágenes de perfiles de las redes sociales o de carnés de conducir sin el permiso de los individuos, tras lo un programa informático analiza imágenes captadas por cámaras de seguridad para tratar de identificar a personas.

Amnistía Internacional señaló asimismo que, aunque ciudades como Boston, Portland o San Francisco han prohibido su uso, la Policía de Nueva York sigue utilizándolo para "intimidar" a ciudadanos, "como se ha podido ver en las protestas de Black Lives Matter del año pasado".

Por ejemplo, apuntan, el activista Dwreck Ingram fue grabado en vídeo en una de estas manifestaciones en Nueva York en junio de 2020, y el 7 de agosto decenas de policías trataron de entrar en su apartamento bajo acusaciones de haber atacado a un agente.

La organización, que afirma que uno de los agentes implicados en este intento de arresto fue fotografiado con un documento que daba a entender que se había utilizado un sistema de reconocimiento facial, asegura que la Policía informó incorrectamente de sus derechos a Ingram, trató de interrogarle sin la presencia de un abogado y rodeó su residencia.

"La Policía se fue solo después de que Dwreck transmitiera en vivo en las redes sociales el suceso", dice Amnistía Internacional, que agrega que la Policía usó su foto de perfil de Instagram para identificarle, que luego fue utilizada en un cartel de "se busca" que las fuerzas de seguridad colgaron en su vecindario.

"Los activistas son específicamente objeto de estas tecnologías dado lo que estamos protestando y porque estamos tratando de desmontar un sistema del que la Policía forma parte", declaró Ingram.

La campaña "Ban the Scan" comenzará con el lanzamiento de una página web donde los residentes de Nueva York pueden generar comentarios sobre el uso de la tecnología de reconocimiento facial, y más tarde presentar peticiones para saber exactamente dónde se está utilizando.

Resumen tomado de: www.elespectador.com, Tecnología, 25 de enero/ 2021
https://www.elespectador.com/noticias/tecnologia/la-lucha-contra-las-tecnologias-de-reconocimiento-facial/

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

¡Ojo! Así se pueden infectar sus equipos con software maliciosos.

La firma de ciberseguridad ESET compartió los métodos más comunes de los ciberdelincuentes para atacar computadoras, celulares y tabletas.
Un *malware* o *software* malicioso es un programa informático diseñado para infectar dispositivos y dañarlos con diversos fines. Pueden manifestarse en forma de virus, troyanos, spyware y demás, lo que los convierte en una de las amenazas cibernéticas más comunes.
La compañía de seguridad informática ESET reveló algunas de las formas que utilizan los delincuentes para infectar equipos con malware y cómo identificarlas.

Phishing y 'spam': El 'phishing' es una estrategia con la que se busca hacerse pasar por una institución confiables, como un banco, para robar información sensible de los usuarios, como credenciales de acceso de algún servicio o el código de seguridad de la tarjeta de crédito. Estas campañas suelen llegar en forma de correo electrónico.
ESET advierte que, además del engaño, estas piezas también pueden incluir archivos o enlaces que pueden comprometer el dispositivo con malware. "Si se observa con atención, probablemente se puedan identificar las estafas. Las señales que indican esto suelen ser errores de ortografía, la evocación de una sensación de urgencia, la solicitud de información personal o correos enviados desde un dominio sospechoso", dijo la compañía.

Sitios web fraudulentos: El 'phishing' también se apoya en replicar sitios web de marcas u organizaciones reconocidas para que las víctimas entreguen su información, hagan clic o descarguen aplicaciones maliciosas. Según ESET, estos sitios suelen tener un dominio similar al original, pero con alguna letra o símbolo diferente. En caso de tener dudas sobre la autenticidad de una página, los expertos recomiendan buscarla directamente desde el navegador y no por medio de enlaces de origen dudoso. Soluciones de seguridad, como antivirus, también advierten sobre estas amenazas e impiden que los usuarios ingresen a sitios maliciosos.

Memorias USB: Aunque muchos utilizan a diario dispositivos de almacenamiento externo para guardar y transferir archivos, estos también conllevan algunos riesgos. La compañía de ciberseguridad cuenta que todavía es común la estrategia de dejar memorias USB "perdidas" para que otros las encuentren y usen.
"Una vez que una unidad afectada está conectada al equipo y es abierta, su dispositivo puede infectarse con un algún tipo de código malicioso, como un *keylogger* (que monitorean la actividad de las teclas) o un *ransomware* (que restringe el acceso a archivos y exige algo a cambio)". Por el uso que se les da normalmente a estas memorias, aumentan las posibilidades de contaminar más de un equipo. Las soluciones de seguridad suelen tener opciones para escanear unidades externas y advertir si contienen algo sospechoso.

Torrents e intercambio de archivos P2P: Estas herramientas se utilizan bastante para la descarga de *software*, películas, juegos y archivos, como también para compartir plataformas de código abierto, sin embargo, los expertos advierten que también contribuyen a difundir malware.
De hecho, ESET afirma que sus investigadores descubrieron recientemente a cibercriminales utilizando el protocolo de BitTorrent y la red Tor para distribuir KryptoCibule, un ladrón de criptomonedas. "Para minimizar el riesgo de ser comprometido, se debería utilizar una solución VPN confiable para cifrar el tráfico y conservarlo a salvo de intrusos", sugiere la firma.

Software comprometido: Los ataques de cadena de distribución son aquellos en los que los atacantes comprometen un software legítimo. ESET cita en su blog el software CCleaner, una aplicación muy conocida que se utiliza para limpiar archivos no deseados. "En estos ataques, los cibercriminales inyectan el malware directamente en la aplicación, que luego utilizan para propagar el malware cuando los usuarios desprevenidos la descargan. Al ser CCleaner una aplicación conocida y confiable, el usuario puede que no haga un escrutinio profundo. Sin embargo, este caso recuerda la importancia de ser cuidadoso al descargar cualquier tipo de software, incluso uno en el que se confía", añadió la compañía. Además de las soluciones mencionadas, ESET destaca que es clave actualizar las aplicaciones regularmente e instalar los parches de seguridad que vienen con estas actualizaciones. "Los parches de seguridad usualmente lidian con vulnerabilidades y fallos de seguridad que se encuentran en las aplicaciones afectadas", explica.

Adware: El *adware* muestra publicidad no deseada, redirige las solicitudes de búsqueda del usuario a sitios web de publicidad y puede recopilar sus datos comerciales. Algunos sitios web tienen estos anuncios, y aunque suelen buscar visitas, pueden tener software malicioso. Es recomendable procurar no hacer clic en dichos anuncios o usar bloqueadores de anuncios confiables para el navegador.

Aplicaciones falsas: Son aplicaciones que se hacen pasar por otras para ser descargadas fácilmente en dispositivos. "Pueden disfrazarse de cualquier cosa, haciéndose pasar por herramientas para el seguimiento del estado físico, aplicaciones de criptomonedas o incluso por apps de rastreo de contactos de COVID-19. Sin embargo, en lugar de recibir los servicios prometidos, los dispositivos se infectarán con varios tipos de malware, como *ransomware, spyware* o *keyloggers*", advierte ESET. Para evitar caer en apps falsas, es clave buscar las verdaderas, aquellas que cuenten con la firma de desarrolladores confiables, que cuenten con registro verificable y varias reseñas usuarios. Mantener los dispositivos parcheados y actualizados también protege de estas amenazas. "Mientras que la lista de estrategias utilizadas por cibercriminales para apuntar a usuarios desprevenidos es larga y puede ser aún más extensa -ya que los cibercriminales siguen desarrollando nuevas tácticas maliciosas, hay muchas formas de mantener los datos seguros y dispositivos protegidos. Estas amenazas pueden ser controladas mediante buenas prácticas de ciberseguridad, que incluye la utilización de soluciones de seguridad con buena reputación y mantener tus sistemas parcheados y actualizados", concluye el equipo de ESET Latinoamérica.

Resumen tomado de: www.elespectador.com, Tecnología, 19 de enero/ 2021
https://www.elespectador.com/noticias/tecnologia/ojo-asi-se-pueden-infectar-sus-equipos-con-software-malicioso/

Pare Oreja

Dicen que….

- Fecha límite para reportar Segundo corte de calificaciones (35%). Febrero 20 de 2021.
- Los exámenes inician el 22 de Febrero de 2021.
- Fecha límite para reportar Último corte de calificaciones (30%) Marzo 06 de 2021.

Link de Interés:

- **¿Por qué deberías eliminar tus correos antes que archivarlos?** https://computerhoy.com/noticias/tecnologia/deberias-eliminar-correos-antes-archivarlos-799127
- **Así avanzan los planes piloto 5G en Colombia** https://www.eltiempo.com/tecnosfera/novedades-tecnologia/5g-como-avanzan-los-planes-piloto-en-colombia-de-redes-5g-554580
- **Cómo limpiar la caché de Windows 10 para mejorar su rendimiento al instante** https://computerhoy.com/noticias/tecnologia/como-limpiar-cache-windows-10-mejorar-rendimiento-instante-799293

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