Sextorsión: un nuevo malware graba la pantalla cuando el usuario mira pornografía

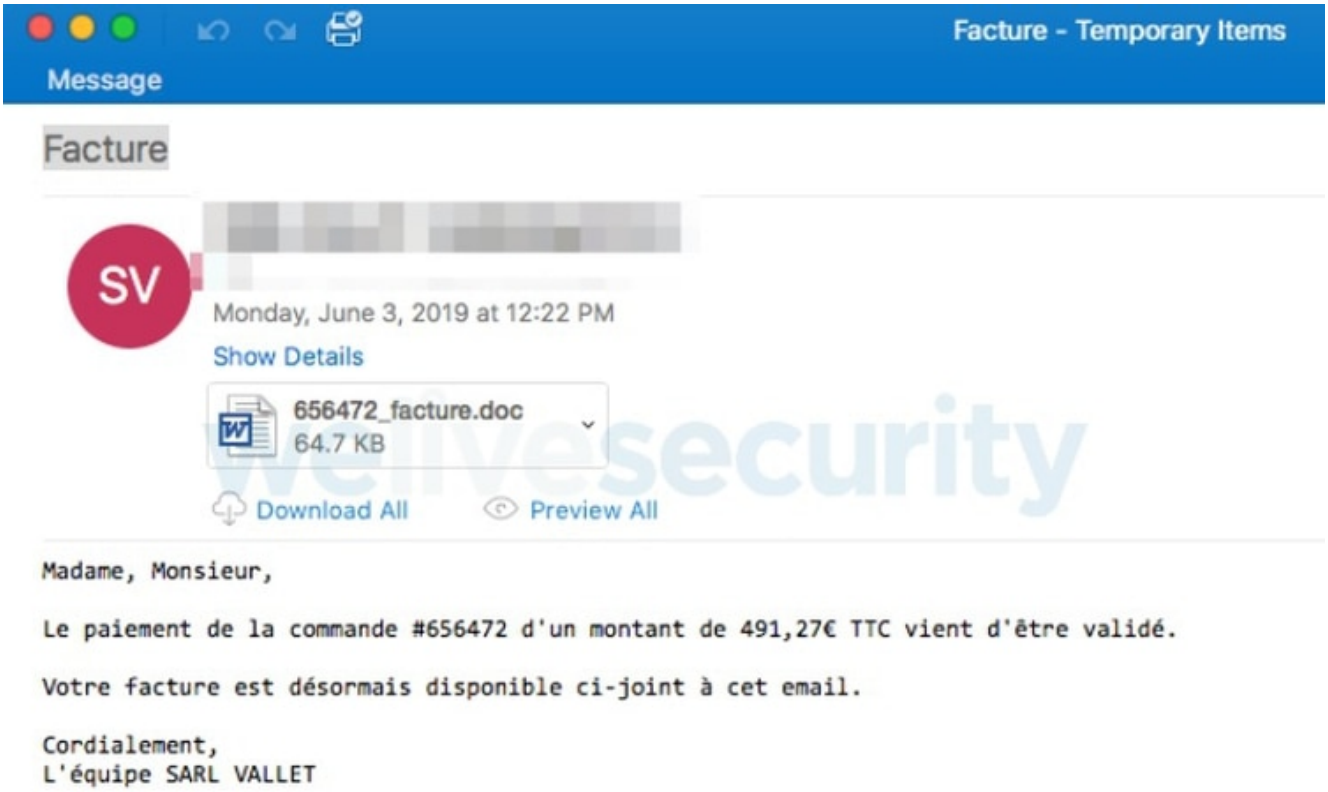
Varenyky es el nombre de un nuevo malware que graba la pantalla de los usuarios mientras miran pornografía. Este virus informático se identificó en mayo y recién hace unos días se supo de su existencia luego de que la firma de ciberseguridad Eset difundiera un artículo explicando cómo actúa.

Este virus informático se infiltra en los equipos mediante un bot que envía spam con un archivo adjunto malicioso. Ese adjunto dice ser la factura de un servicio. Al abrir el archivo el usuario ve un mensaje que dice que el documento está protegido y que se requiere verificar al usuario, al

hacer clic en aceptar, el spyware se comienza a ejecutar.

El malware se comunica anónimamente con el servidor en manos de los cibercriminales y toma control del equipo infectado. Así puede robar contraseñas y acceder a cuentas de la víctima. A su vez, está configurado para comenzar a grabar cada vez que el usuario ingresa en una página web con contenido para adultos.

“Una vez infectado el equipo entre los módulos que descarga se pueden ver uno para robar contraseñas, otro para grabar videos con la webcam, y otro para hacer capturas de pantalla. **En estos últimos módulos también se vio, en el análisis del código, que buscan específicamente activarse cuando el usuario infectado navega páginas de carácter pornográfico** (esto se realiza por palabras claves que busca el malware)”, explicó a **Infobae** Luis Lubeck, especialista en seguridad informática de ESET Latinoamérica.



El malware se distribuye a través de un adjunto que llega por correo.

La grabación de ese contenido se podría usar para llevar adelante una sextorsión: es decir para pedirle dinero a la víctima a cambio no publicar el material; o bien para simplemente obtener material sensible. Cabe recordar que el sistema puede grabar la pantalla o sea que también podría hacerlo para obtener datos de credenciales, información bancaria, etc.

Según un artículo publicado por *ABC*, ya se registró un caso de sextorsión que involucra a una víctima francesa (cabe remarcar que este tipo de ataques con Varensky se registraron en Francia, por el momento) a la que se le pidió un pago de 750 euros en bitcoins para no compartir material donde se lo ve consumiendo contenido para adultos.

Desde Eset explican que, en los casos analizados, sólo se vio

que Varensky grabó la pantalla del dispositivo y no desde la cámara, de todos modos, la tecnología permitiría hacerlo.

Por otra parte, desde la firma remarcan que se trata de un malware con persistencia y conectado a un servidor de comando y control, con lo que no se descarta que en caso de no eliminarse del equipo la amenaza pueda ir mutando y agregando funcionalidades.

“En el servidor de comando y control, el cibercriminal maneja todos los nodos infectados y puede realizar actualizaciones a su malware, al igual que recibir toda la información que las terminales le envían como capturas de pantallas, credenciales, etc.”, concluyó Lubeck.

Fuente: **Infobae**