DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/mincom_v2/sites/default/files/styles/noticias/public/69736359_1125621477648728_1683770219622825984_o.png

Informatización en Cuba

Source:
Tomado de Cubadebate, por Omar Pérez Salomón

En la actualidad el desarrollo de malware o software malicioso es una industria muy productiva en la que los ciber delincuentes aprovechan las vulnerabilidades y debilidades en la configuración de los sistemas, así como la ingeniería social para lograr sus objetivos.

La industria de productos de seguridad ha tenido que adaptarse a estos cambios para buscar más efectividad y proactividad. Se caracteriza por grandes inversiones en investigación en aprendizaje automático e inteligencia artificial, capital humano, infraestructura de sensores y sistemas de inteligencia de amenazas.

Una noticia publicada en el sitio de Segurmática el pasado 1ero de noviembre da cuenta de ataques por phishing, móviles dirigidos contra las Naciones Unidas, Cruz Roja, UNICEF, Programa Mundial de Alimentos y diversas organizaciones de ayuda humanitaria.

También sobre las afectaciones ocasionadas por el virus Dtrack que puede hackear cualquier cosa, desde cajeros automáticos hasta plantas nucleares.

Lo cierto es que para que los atacantes tomen el control sobre las redes internas de la organización objetivo, es necesario que existan debilidades de seguridad, como pobre manejo de contraseñas, falta de monitoreo del tráfico, uso de soluciones antivirus inadecuadas, entre otras fallas.

En este contexto la empresa cubana Segurmática, constituida en febrero de 1995 y única de su tipo en Cuba, desarrolla productos y soluciones de seguridad informática avanzados, así como, brinda servicios y consultoría especializada a entidades nacionales y extranjeras, del tal manera de contribuir a fortalecer la ciberseguridad del país.

En este trabajo se dialogará con Miguel Gutiérrez Rodríguez, director general de Informática del Ministerio de Comunicaciones de Cuba, sobre los servicios que ofrece Segurmática y las perspectivas en el desarrollo de sus productos.

—¿Cuáles son los principales servicios que ofrece Segurmática?

— En febrero del próximo año esta empresa cumplirá 25 años y hay que decir que su cartera de servicios ha crecido de manera sostenida. Recuerdo que la primera versión de Segurmática Antivirus (SAV32) salió en el 2006 y la que tenemos hoy ha evolucionado mucho en calidad y alcance, sin dejar de reconocer sus limitaciones y los aspectos que hay que seguir desarrollando y mejorando.

"Con 60 trabajadores como promedio, de ellos un 75% dedicado a las actividades técnicas, comerciales y al desarrollo, alcanzan una productividad de más de 76000 pesos por trabajador.

"Aunque se le conoce en lo fundamental por sus programas antivirus, los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos, alertas de antivirus informáticos, escaneo de puertos, consultoría remota a sitios web, red interna y de cara a Internet, actualización de parches, gestión de incidentes, recuperación de información borrada, elaboración y revisión de planes de seguridad informática, configuración segura de servicios de red, soporte técnico, adiestramientos, custodia de material informático y dictamen de sistemas contables y financieros.

"También utiliza como distribuidores de sus productos a Joven Club, Desoft, Eicma, Sitrans, Info y Aicros. Es socio comercial de Kaspersky Lab".

— ¿Qué dictaminan en el caso de los sistemas contables y financieros?

— Hay todo un proceso para ir sustituyendo los sistemas contables financieros importados por nacionales; pero en cualquier variante la seguridad de los que tenemos en funcionamiento en nuestras empresas, unidades presupuestadas y demás instituciones es vital y es necesaria la certificación de los que se utilizan en el país.

"Por eso es importante este servicio que brinda, pues entre otras cuestiones verifica si cuentan con claves de acceso robustas (8 caracteres como mínimo) y requisitos de complejidad; la transmisión de las claves en texto claro en el proceso de autenticación; el acceso a las opciones del sistema en correspondencia con los perfiles de usuario; los mecanismos de seguridad que evitan la modificación, destrucción y pérdida de los ficheros y datos y el acceso a los mismos que esté compartimentado y controlado.

"Al igual el diseño sobre bases de datos robustas y los mecanismos de salva; mecanismos de alerta si se intenta modificar su código ejecutable; utilización de mecanismos de cifrado para proteger la información primaria que gestiona; el cambio periódico de la contraseña; el bloqueo de la cuenta de usuario tras varios intentos fallidos de conexión; las opciones de salva y restaura restringidas solo al usuario administrador del sistema; el registro de las acciones realizadas por los usuarios por al menos un año y si tiene implementados mecanismos de seguridad orientados a impedir la exportación de datos susceptibles de ser modificados sin emplear las funcionalidades del sistema.

Como se puede observar es riguroso el dictamen, hay aspectos que son invalidantes para obtener un resultado positivo y se realiza a partir de una lista de chequeo.

—Muy pocos países cuentan con un antivirus nacional. ¿Qué situación tiene hoy el Segurmática Antivirus?

—Aunque tenemos muchas insatisfacciones aún, nuestro antivirus continúa ganado usuarios en el panorama nacional y se trabaja en incrementar las computadoras protegidas tanto en las personas jurídicas como en las naturales.

"Al cierre del 2018 protegió el 12,1% del total de computadoras del país, 156591 máquinas de personas jurídicas y 15325 en las naturales. Se estima que al cierre del 2019 será un 13%.

En el caso de los equipos móviles protegidos con Segurmática Seguridad Móvil se inmunizó al cierre del 2018 apenas el 2% del total de los usuarios del servicio de datos móviles. Al concluir el 2019 se espera que sea un 2,3%. Como observamos es mucho el trabajo a realizar en esta actividad.

Por otro lado, se trabaja en el reconocimiento del malware a través de inteligencia artificial, en sistemas de telemetría para Android, que servirán de base para el antivirus en la nube, se incrementa el número de cadenas de identificación de programas malignos, se ha mantenido la generación de cuatro actualizaciones diarias, incluyendo además la identificación heurística y genérica, se han establecido alianzas con las universidades y se creó una unidad docente en la Universidad de Ciencias Informáticas (UCI)".

—¿Cuál es el sistema para recolectar las muestras de virus?

—Son diversas las vías. Como dijera Niurka Edith Milanés Sarduy, Directora General de la Empresa de Consultoría y Seguridad Informática, Segurmática, en entrevista concedida al Canal USB del sitio Cubadebate, el 3 de septiembre de 2019:

"No podemos acceder a sitios donde hay muestras frescas debido al bloqueo. Un ejemplo de ello es Virus Total, pues el .CU está bloqueado para descargas en ese repositorio, al ser de Google, y esto dificulta la

obtención de muestra diarias de malware. No obstante, tenemos un sistema de vigilancia tecnológica que busca constantemente dónde se publican las muestras de malware que más afectan a nivel internacional. Si pueden afectar a las redes nacionales, las muestras son introducidas rápidamente en la próxima actualización.

“Por otra parte, contamos con otras opciones como la OSRI, cuando le notifican alguna incidencia de programa maligno. O los propios usuarios reportan a través de nuestro correo virus@segurm [1]ática.cu, ya que tienen otro antivirus instalado en su PC.

“Ningún antivirus es cien por ciento seguro. Siempre hay algún programa maligno que se escapa. Y los atacantes cada día van usando mecanismos más sofisticados. Al cierre de julio pasado nosotros habíamos recibido por esa cuenta 301 reportes. Y este año tenemos 567 al cierre de igual periodo, lo que te dice que hemos crecido. El 50% se esos reportes lo resolvemos antes de siete días, muchos de manera inmediata. En dependencia de la complejidad puede demorar un poco más.

“Tenemos una base de datos de programas malignos de más de 4 Teras. A pesar de las limitaciones que te comenté anteriormente, tenemos el apoyo de muestras internacionales a las que podemos tener acceso desde Cuba”.

— ¿Qué se está proyectando desde el punto de vista de desarrollo tecnológico?

— Teniendo en cuenta que fortalecer la ciberseguridad es una prioridad, en los próximos años debemos incrementar los servicios orientados a brindar soluciones integrales de seguridad de las TIC y proteger de manera efectiva el ciberespacio nacional.

"En esta estrategia, Segurmática juega un papel muy importante por ser una de las contadas empresas de seguridad informática que tenemos hoy. Por tanto se están ejecutando acciones para la captación y retención de especialistas, intensificar la colaboración con universidades y centros de investigación para los proyectos de I+D+i, concretar inversiones en la infraestructura de red y desarrollo y dar solución a la certificación de drivers.

"Específicamente en lo referido a los productos se trabaja a corto y mediano plazos en el Segurmática Antivirus para Windows, versión 2.0; Segurmática Seguridad Móvil, versión 2.0 con funcionalidad de firewall; Seguridad Antivirus para Linux, versión 1.0 con interfaz gráfica; desarrollo de la protección de URL del motor Antivirus; desarrollo de driver MTP para control de dispositivos; prevención de fuga de datos (DLP); desarrollo de defensa proactiva y antiransomware (driver y servicio) para el motor Antivirus e incorporar motor de Android identificación de malware por inteligencia artificial, entre otras acciones.

"Todas permitirán la creación de una Suite de Seguridad para protección de red y navegación, que permitirá una mayor integración de los productos y servicios de Segurmática.

"Por último debemos referir que existe una proyección para potenciar el comercio electrónico en la empresa con la venta en línea a través de la tienda Superfácil de Citmatel y en las plataformas EnZona y Apklis, incluir las renovaciones como una opción en Transfermóvil e incorporar dentro de los productos la opción de comprar licencias", concluyó

Ataques que utilizan ingeniería social y recursos técnicos para robar credenciales de la identidad de consumidores. El término phishing proviene de la palabra inglesa fishing (pesca) haciendo alusión a que los usuarios (víctimas) “piquen el anzuelo” y den sus credenciales de acceso.

Links
[1] mailto:virus@segurm