OAC Boletín de Diciembre

"Al igual que nuestras experiencias en el dominio aéreo, el control del ciberespacio no es un estado permanente ni absoluto y se requiere una actividad constante para lograr un grado de ventaja"

Comodoro del Aire Tin Neal Hopes
Ministerio de Defensa UK

Se cierra el 2018, primer año del Observatorio Argentino del Ciberespacio (**OAC**), un detalle de los trabajos realizados y los boletines enviados puede ser encontrado en las URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php, micro-sitio de la página de la Escuela Superior de Guerra Conjunta. y http://www.ceptm.iue.edu.ar/index.php/category/antena-territorial-de-defensa-y-seguridad/observatorio-ciberespacio/ sitio del Centro de Estudios General Mosconi de prospectiva tecnológica militar de la Facultad de Ingeniería del Ejército.
Esperamos continuar en el 2019, en conjunto con la Antena Territorial de Defensa y Seguridad y el Centro Mosconi distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

Contenidos

CIBERDEFENSA y CIBERSEGURIDAD

RRHH en Ciberdefensa, los Ciberejercicios Locked Shields

Locked Shields es un ejercicio de ciberdefensa a 2 bandos que se realiza anualmente desde 2010, contiene desafíos técnicos y estratégicos , constituyendo hoy el ejercicio de ciberdefensa en tiempo real más grande y complejo del mundo.

https://ccdcoe.org/nato-ccdcoe-brings-improvement-through-practice.html

REPORTE

Ciberestrategia Nacional de los Estados Unidos de Norteamérica

En septiembre de este año el presidente de los EE.UU. publicó la Ciberestrategia Nacional, lo interesante del documento ya está en su título. No habla ni de seguridad ni de defensa, integra el ciberespacio como un todo que requiere una estrategia integral. En palabras del mismo Donald Trump: "*La Estrategia Cibernética Nacional demuestra mi compromiso con el fortalecimiento de las capacidades de ciberseguridad y protección de América contra las amenazas cibernéticas. Es un llamado a la acción para todos los estadounidenses y nuestras grandes empresas, que deben tomar las medidas necesarias para mejorar nuestra ciberseguridad nacional. Continuaremos liderando el mundo para asegurar un futuro cibernético próspero".*

El documento se divide en 4 grandes pilares, en los que se tratan los siguientes temas:

1. **Pilar I: Protección del pueblo estadounidense, la patria y su estilo de vida**
    - ***a. Redes Federales Seguras e Información***
        - i. Centralizar aún más la gestión y supervisión de la ciberseguridad civil federal
        - ii. Alinear las actividades de gestión de riesgos y tecnología de la información
        - iii. Mejorar la gestión de riesgos de la cadena de suministro federal
        - iv. Fortalecer la Ciberseguridad del Contratista Federal
        - v. Asegurar el liderazgo del gobierno en las mejores prácticas innovadoras
    - ***b. Asegurar infraestructura crítica***
        - i. Redefinir roles y responsabilidades
        - ii. Priorizar las acciones de acuerdo a los riesgos nacionales identificados
        - iii. Aprovechar a los proveedores de tecnología de la información y las comunicaciones como facilitadores de la ciberseguridad.
        - iv. Proteger nuestra democracia
        - v. Incentivar las inversiones en ciberseguridad
        - vi. Priorizar las inversiones nacionales en investigación y desarrollo
        - vii. Mejorar el transporte y la ciberseguridad marítima.
        - viii. Mejorar la ciberseguridad espacial
    - ***c. Combatir los delitos informáticos y mejorar los informes de incidentes***
        - i. Mejorar el reporte y respuesta a incidentes
        - ii. Modernizar las leyes de vigilancia electrónica y delitos informáticos.

iii. Reducir las amenazas de las organizaciones criminales transnacionales en el ciberespacio
iv. Combatir los delitos informáticos y mejorar los informes de incidentes
v. Mejorar el reporte y respuesta a incidentes
vi. Modernizar las leyes de vigilancia electrónica y delitos informáticos.
vii. Reducir las amenazas de las organizaciones criminales transnacionales en el ciberespacio
viii. Optimizar la captura de criminales ubicados en el extranjero
ix. Fortalecer la capacidad de las Naciones Unidas para hacer cumplir la ley para combatir la actividad cibernética criminal

2. **Pilar II: Promover la prosperidad estadounidense**
   a. ***Fomentar una economía digital vibrante y resistente***
      i. Incentivar un mercado de tecnología adaptable y seguro
      ii. Priorizar la innovación
      iii. Invertir en infraestructura de próxima generación
      iv. Promover el libre flujo de datos a través de las fronteras
      v. Mantener el liderazgo de Estados Unidos en tecnologías emergentes.
      vi. Promover la ciberseguridad de ciclo completo
   b. ***Fomentar y proteger el ingenio de Estados Unidos***
      i. Mecanismos de actualización para revisar la inversión extranjera y la operación en los Estados Unidos
      ii. Mantener un sistema de protección de propiedad intelectual fuerte y equilibrado
      iii. Proteger la confidencialidad y la integridad de las ideas americanas
      iv. Desarrollar una fuerza laboral de seguridad cibernética superior
   c. ***Construir y sostener el flujo de talentos***
      i. Ampliar la capacitación profesional y las oportunidades educativas para los trabajadores de América
      ii. Mejorar la fuerza laboral federal de seguridad cibernética
      iii. Utilizar la autoridad ejecutiva para destacar y recompensar el talento
3. **Pilar III: Preservar la paz a través de la fuerza**
   a. ***Mejorar la estabilidad cibernética a través de las normas de comportamiento responsable del estado***
      i. Fomentar la adhesión universal a las normas cibernéticas
   b. ***Desalentar el comportamiento inaceptable en el ciberespacio***
      i. Liderar teniendo como objetivo la Inteligencia Colaborativa.
      ii. Imponer consecuencias
      iii. Construir una iniciativa de disuasión cibernética
      iv. Contrarrestar en el ciberespacio, la mala influencia y las Operaciones de Información.
4. **Pilar IV: Avance de la influencia americana**

   Promover una Internet abierta, interoperable, confiable y segura
   a. ***Proteger y promover la libertad en internet***

i. Trabajar con países con ideas afines, industriales, academicas y sociedad civil
ii. Promover un modelo de gobernanza de internet de múltiples partes interesadas
iii. Promover una infraestructura de comunicaciones interoperable, confiable y conectividad de internet
iv. Promover y mantener mercados en todo el mundo, surgidos del ingenio de Estados Unidos

b. Construir una capacidad cibernética internacional

i. Mejorar los esfuerzos de creación de capacidad cibernética

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

– – –

EE.UU evalúa vulnerabilidades de sus propias agencias Ciberespaciales

AWARE es un software de monitoreo continuo de las agencias y le dará al Departamento de Seguridad Nacional una visión holística de la postura de ciberseguridad del gobierno, con una idea de cómo se encuentran en ciberseguridad básica y poder comparar su posición en relación con otras agencias del gobierno

https://www.defenseone.com/politics/2018/11/agencies-will-soon-have-cyber-hygiene-scoreand-will-know-where-they-rank/153136/?oref=d_brief_nl

– – –

CIBERFORENCIA

La contraseña del administrador en Linux, es amenazada

Dr WEB, ha descubierto un troyano dirigido a los usuarios de Linux (menos extendido que las cepas que se dirigen al sistema de Windows), pero se está volviendo tan complejo y multifuncional con un script de shell gigante de más de 1.000 líneas de código, que es ejecutado en un sistema Linux infectado, .lo que hace este script es encontrar una carpeta en el disco en la que tenga permisos de escritura para que pueda copiarse y luego utilizarla para descargar otros módulos.

https://vms.drweb-av.es/virus/?i=17645163

– – –

CIBERCONFIANZA

Algunos Vocablos propios del Ciberespacio

A continuación y desde diferentes fuentes, damos un resumen de los diferentes tipos de amenazas en el ciberespacio:

Malware: El término Malware es el acrónimo de malicious software y se utiliza para denominar a aquellos programas que tienen la capacidad de infiltrarse en un sistema, sin el consentimiento del usuario, con el fin de robar su información o provocar un funcionamiento incorrecto, entre otras acciones indeseables.

Al día de hoy, las plataformas más atacadas son Windows y Android (que, a su vez, son las plataformas más utilizadas). Como hemos mencionado anteriormente, los creadores de malware han visto en esta actividad un método de enriquecimiento.

Quizás otro obstáculo con el que chocan los creadores de malware para Linux/Unix tiene que ver con la usual capacitación media/alta de los usuarios de este tipo de plataformas, por lo que la Ingeniería Social (principal método de propagación en la actualidad) no resulta tan eficiente para con ellos.

Troyanos: Los troyanos son el subtipo de malware más frecuente y, debido a su complejidad, uno de los más peligrosos. El troyano intentará infiltrarse en un equipo aparentando ser un software inofensivo, al ejecutarse llevará a cabo acciones maliciosas sobre el sistema operativo de la forma más desapercibida posible. El objetivo es darle al atacante el control total sobre un equipo de forma remota (por eso también se los conoce como RAT – Remote Administration Tool, Herramienta de Administración Remota). Los troyanos más modernos cumplen este objetivo a tal punto que el control sobre el equipo sea igual a estar sentado frente al mismo.

Con esto en mente podemos imaginar que las funciones básicas de un troyano consistirán en permitirle al atacante obtener toda la información alojada en el equipo, administrar dispositivos, servicios y aplicaciones instaladas, bajar y subir archivos, así como borrar o editar los existentes. También grabar las teclas pulsadas, obtener capturas de pantallas o visualizar el escritorio de la máquina infectada en tiempo real, pudiendo controlar el mouse y el teclado. Ejecutar comandos, activar el micrófono y la webcam, entre muchas otras acciones que, por supuesto, no ocurrirán a la vista del usuario.

Ahora bien, para que un atacante pueda tomar el control de un equipo de esta manera, necesita crear una conexión entre su máquina y la que desee controlar. Los troyanos funcionan de esa manera, por eso constan básicamente de dos partes: cliente y servidor. El cliente estará en manos del atacante y será quien envíe las órdenes y peticiones de información al servidor, este último es el ejecutable que infecta al equipo (víctima) y responderá todas las solicitudes maliciosas del cliente (atacante).

¿Cómo operan los troyanos bancarios?

Una vez ejecutadas, las apps pueden bien mostrar un mensaje de error en el que afirman que han sido removidas debido a una incompatibilidad con el dispositivo de la víctima y luego proceden a esconderse de la vista del usuario, o bien la posibilidad es que ofrezcan la función que prometían (como mostrar el horóscopo).

Independientemente de cuál de las actividades antes mencionadas despliega cada una de estas apps, la principal función maliciosa está escondida en un payload cifrado ubicado en los assets de cada app. Este payload es codificado en base64 y luego cifrados con un cifrado RC4 utilizando una llave hardcodeada. La primera fase de la actividad del malware es tratar de instalarse por medio de un dropper que inicialmente corrobora si existe la presencia de un emulador o de una máquina virtual (sandbox). Si estos chequeos fallan, entonces descifra y libera un programa iniciador del sistema operativo junto con un paquete de datos que contiene el actual malware bancario. Algunas de las apps que analizamos contienen más de una etapa de estos paquetes cifrados.

¿Cómo se interpretan los términos?:

***Payload**: las vulnerabilidades o errores presentes en cualquier software pueden ser aprovechadas para producir efectos inesperados en los equipos, una vez descubierto ese fallo se desarrollaban pequeños programas (**exploits**) para forzar de forma específica ese error en el sistema.*

***Exploit:** es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.*

***Assets:** activo, recurso Elemento del sistema que se requiere para ser protegido por la política de seguridad de un sistema de información, destinado a ser protegido por una contramedida, o necesario para la misión de un sistema. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, recursos físicos y recursos humanos.*

***Cifrado RC4:** Dentro de la criptografía **RC4** o **ARC4** es el sistema de cifrado de flujo más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.*

***Hardcodeada**: término del mundo de la informática hace referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente en el código fuente del programa, en lugar de obtener esos datos de una fuente externa como un fichero de configuración o parámetros de la línea de comandos, o un archivo de recursos.*

***Dropper**: es un software diseñado para instalar algún tipo de malware (virus, puertas traseras, etc.) en el sistema operativo donde ha sido ejecutado. El código malicioso puede estar contenido dentro del propio programa para evitar ser detectado por el antivirus o descargarse automáticamente desde Internet cuando el dropper se ejecuta.*

***Sandbox:** Primeramente, definiremos **qué es un sandbox**. Tomando el origen de la palabra traduce algo así como caja de arena. Es como esas cajas de arena cerradas para que los niños jueguen. Sólo que en informática una **caja de arena o sandbox** no es otra cosa que una zona de la memoria completamente aislada del resto de la memoria disponible, con el objetivo de ejecutar un programa o aplicación para verificar si contiene malware o software malicioso, sin poner en riesgo al sistema operativo y por ende a nuestra computadora o dispositivo móvil.*

***Loader:** Programa de utilidad encargado de transferir programas de la memoria auxiliar a la memoria central para su ejecución.*

La funcionalidad del payload final es la de suplantar apps bancarias instaladas en el dispositivo de la víctima, interceptar y enviar mensajes SMS, y descargar e instalar aplicaciones adicionales elegidas por el operador. La funcionalidad más significativa es que **de manera dinámica el**

malware puede suplantar la identidad de cualquier aplicación instalada en el dispositivo de la víctima.

Esto lo consigue mediante la obtención del código HTML de estas apps instaladas en el dispositivo y utilizando ese código para superponerse a la aplicación legítima con falsos formularios una vez que la app legítima es ejecutada, dándole a la víctima muy pocas chances de notar que hay algo sospechoso.

Para evitar ser víctima de este malware bancario recomendamos:

- Solo descargar apps de Google Play. Si bien esto no asegura que la app no es maliciosa, este comportamiento maligno es más común en tiendas de terceras partes, donde difícilmente se eliminen por más que sean descubiertas; a diferencia de lo que pasa en Google Play que se eliminan rápidamente cuando son reportadas.
- Asegúrese de revisar el número de descargas, la valoración y los comentarios existentes sobre la app antes de descargarla de Google Play si el sistema es Android.
- Preste atención de cuáles son los permisos que otorga a las apps que instala.
- Mantenga su dispositivo Android actualizado y utilice una solución de seguridad para móviles que sea confiable. Los productos de ESET detectan y bloquean esta amenaza como Android/TrojanDropper.Agent.CIQ.
- Realice las operaciones bancarias a través de las páginas oficiales de las entidades asegurándose que en la barra de direcciones figure HTTPS, que la identifica como una página segura; y evite el uso de equipos ajenos, preferentemente no por conexiones inalámbricas o servicios de WiFi abiertos.
- Chequee la vigencia del certificado de seguridad de la página; haciendo clic sobre el candado que figura en la barra de direcciones del navegador que desplegará la información.
- No responder a supuestos mensajes que dicen ser de la entidad bancaria solicitando datos aludiendo que los han perdido, esto no es la práctica usual en dichos casos.
- No descargar archivos o acceder a links en los que no estemos familiarizados con la fuente emisora.