infosecurity® MEXICO

Presenting Virtual Edition

TREND MICRO™

DIRECTORIO DE EXPOSITORES

Organizado por Reed Exhibitions®

TREND MICRO™

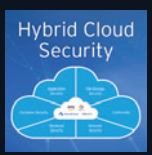
Ofrecemos soluciones líderes en la industria para proteger por capas workloads en nube, data centers, redes, correo y endpoints para asegurar este mundo cada vez más conectado.

Trend Micro Incorporated, líder mundial en soluciones de ciberseguridad, ayuda a hacer del mundo un lugar más seguro para el intercambio de información digital.

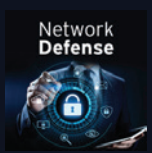
Nuestras innovadoras soluciones para consumidores, empresas y gobiernos brindan seguridad en capas para data centers, workloads en la nube, redes y endpoints.

Todos nuestros productos trabajan en conjunto para compartir la inteligencia de amenazas y proporcionar una defensa interconectada con visibilidad y control centralizados, lo que permite una mejor y más rápida protección

¿CÓMO PODEMOS AYUDARLE?



Plataforma de seguridad SaaS automatizada para containers físicos, virtuales y de nube, workloads serverless, apps nativas de nube y DevOps.



Detecta y previene amenazas conocidas y desconocidas y movimientos laterales en la red con dato de la Trend Micro ™ Zero Day Initiative™.

Protección de usuarios en cualquier dispositivo, aplicación, red y ubicación contra amenazas dirigidas, avanzadas y Ransomware.

www.trendmicro.com
marketing_la@trendmicro.com
/TrendMicroLATAM
@TrendMicroLATAM
/showcase/Trend-Micro-LATAM

Estimado visitante,

La pandemia del COVID-19 nos ha dejado una elevada curva de aprendizaje en todos los sentidos. Hablando de seguridad cibernética, este cambio acelerado hacia la virtualización ha incrementado los desafíos a los que nos ya nos enfrentábamos en nuestro día a día, donde hoy más que nunca, necesitamos continuar conectados para seguir avanzando.

*En este sentido, hemos creado el **Virtual Infosecutiry Mexico 2020,** un hub pensado en brindar, a nuestra comunidad de profesionales, nuevos espacios de colaboración y educación que les permita ir un paso delante de los retos emergentes.*

*Durante tres días, **vivirás un evento altamente interactivo** para establecer contacto con colegas, compartir mejores prácticas y escuchar a los expertos a través de **cyber talks, sesiones ask the expert, expert panels y keynote lectures,** todos enfocados en temas clave como inteligencia artificial, ciberseguridad en la nube, hacking ético, privacidad de datos, arquitecturas, factor humano, entre otros.*

*Además, podrás visitar los perfiles de nuestros expositores para ser asesorado en vivo acerca de **nuevas tecnologías y soluciones en seguridad cibernética.***

*Por supuesto, **que esperamos verlos a todos en nuestro evento presencial en mayo del 2021.** Sin embargo, estamos entusiasmados de organizar este evento de forma virtual, pues creemos que existen oportunidades únicas para los eventos virtuales que no debemos dejar pasar.*

¡Esperamos que lo disfrutes!

Juan Manuel Rodriguez
Director Infosecurity Mexico

Índice **Página**

La calidad, veracidad, confiabilidad y demás características de los productos anunciados son responsabilidad exclusiva de los expositores.
Para mayor información del tratamiento de datos personales, consulte nuestro Aviso de Privacidad Integral en el sitio web www.reedexpo.mx/aviso-privacidad
El presente directorio incluye los datos de expositores actualizados al 18 de septiembre de 2020.

infosecurity® MEXICO

Presenting Virtual Edition TREND MICRO

La verdadera comunidad se mantiene unida.

¡GRACIAS POR TU PARTICIPACIÓN EN NUESTRA PRIMERA EDICIÓN VIRTUAL!

Muy pronto nos volveremos a encontrar para hacer negocios cara a cara.

Gracias a las marcas que confiaron en nosotros:

PATROCINADORES

Presenting Edición Virtual: TREND MICRO

Leading Sponsorship: IBM

Premium Sponsor: S21sec

Digital Top Sponsors: GlobalSign, Excelerate Privitar, LexisNexis Risk Solutions, servicenow

Content Sponsor: totalsec

EXPOSITORES

CSI, Google Cloud, Check Point Software Technologies Ltd, (one) e-security, TRAPX Security

ORGANISMOS DE APOYO

AMECI, CETIC, ALAPSI, UDLAP Jenkins Graduate School, ASIS

MEDIOS DE APOYO

Revista MÁS SEGURIDAD, usecnetwork, Revista CONSULTORÍA

En alianza con

ISACA Mexico City Chapter

ISACA Guadalajara Chapter

infosecurity MEXICO

Presenting Virtual Edition

TREND MICRO

AGENDA

22.SEPT.2020

KEYNOTE

09:00 - 09:45 h

- **IMPLICACIONES LEGALES DEL T-MEC EN MATERIA DE CIBERSEGURIDAD**

IVONNE MUÑOZ TORRES

Directora General

IT Lawyers

CYBERTALK

10:00 - 10:45 h

- **LA NUEVA CARA DEL CIBERCRIMEN**

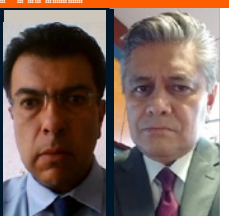
RAFAEL COSTA ABREU, *Director Planeación y Estrategia de Mercado*

ERNESTO MORENO, *Consultor, América Latina y el Caribe Soluciones de Prevención de Fraude e Identidad Digital*

LexisNexis RISK SOLUTIONS

EXPERT PANEL

11:00 - 11:45 h



- **RIESGOS Y MEJORES PRÁCTICAS DE SEGURIDAD EN LA NUBE**

ROBERTO HERNÁNDEZ, *Presidente, ISACA, Capítulo Ciudad de México*

RUBEN QUINTERO *VP, ISACA Capítulo Ciudad de México*

ISACA Mexico City Chapter

ASK THE EXPERT

12:00 - 13:00 h

- **DESAFÍOS DE CIBERSEGURIDAD EN LA TRANSFORMACIÓN DIGITAL**

JUAN PABLO CASTRO

Director de Innovación Tecnológica Trend Micro Latinoamérica

TREND MICRO

En alianza con

ISACA Mexico City Chapter

ISACA Guadalajara Chapter

infosecurity MEXICO

Presenting Virtual Edition

TREND MICRO

AGENDA

22.SEPT.2020

CYBERTALK

13:15 - 14:00 h

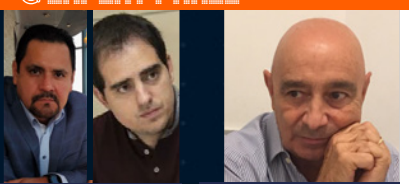
- **EL MITO DE LA PRIVACIDAD**

JORGE OSORIO BRETÓN

Cofundador y Director de Servicios de Consultoría

CSI Consultores en Seguridad de la Información

EXPERT PANEL



14:15 - 15:00 h

- **CIFRADO PARA LA GESTIÓN DE LA CIBERSEGURIDAD**

AMECI Asociación Mexicana de Ciberseguridad

MODERADOR: IGNACIO SOTELO
Presidente, AMECI

DR. ALFONSO MUÑOZ
Socio Fundador de CriptoCert

JORGE RAMIÓ
Socio Fundador de CriptoCert

KEYNOTE

15:15 - 16:00 h

- **CASB (CLOUD ACCESS SECURITY BROKER): UN NUEVO COMIENZO PARA EL GOBIERNO DE LA NUBE**

RAMSÉS GALLEGO

Security, Risk & Governance International Director, Micro Focus

ie Reinventing Higher Education

* Programa sujeto a cambios

En alianza con

ISACA Mexico City Chapter

ISACA Guadalajara Chapter

infosecurity MEXICO

Presenting Virtual Edition

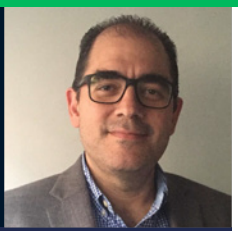
TREND MICRO

AGENDA

23.SEPT.2020

KEYNOTE

09:15 - 10:00 h



- **INVERSIÓN INTELIGENTE MEDIANTE EQUIPOS DE DEFENSA Y ATAQUE**

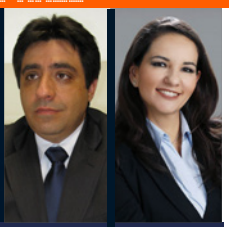
FEMSA

RHETT NIETO

Jefe de Seguridad TI, Femsa

EXPERT PANEL

10:15 - 11:00 h



- **LOS SECRETOS DEL CIBER CRIMEN Y SU RELACIÓN CON LA SOCIEDAD**

INTERPOL

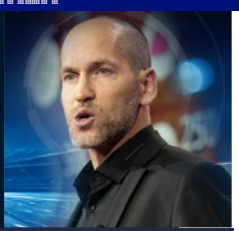
ADRIÁN EDUARDO ACOSTA

Digital Crime Officer

GABRIELA REYNAGA

CRISC, CISA, GRCP, COBIT 5 & COBIT 2019 Consejera en Ciberseguridad y CEO en Hollistics GRC,

CYBERTALK



12:00 - 12:45 h

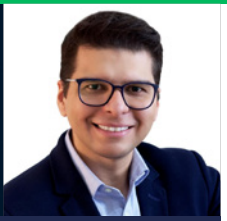
- **CISO DE CHECK POINT**

Check Point SOFTWARE TECHNOLOGIES LTD

JONATHAN FISCHBEIN

Director de Ciberseguridad

KEYNOTE



13:00 - 13:45 h

- **LOS DATOS DE RED: LA ÚNICA FUENTE CONFIABLE**

Gigamon

FELIX PARRA

Territory Account Manager

* Programa sujeto a cambios

infosecurity® MEXICO

Presenting Virtual Edition TREND MICRO

En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

AGENDA

23.SEPT.2020

CYBERTALK

14:00 - 14:45 h

- **CÓMO PROTEGER LAS JOYAS DE LA CORONA DE SU NEGOCIO CON SERVICENOW**

servicenow

WILLIANS MEDEIROS / ERICK CARRANZA

Consultores de Soluciones LATAM

ASK THE EXPERT

15:00 - 16:00 h

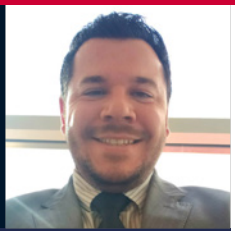
- **MEJORANDO LA CIBERSEGURIDAD CON LA AYUDA DE LA PSICOLOGÍA Y LAS NEUROCIENCIAS**

ULISES CASTILLO

M. en C. CISSP, CISM, CISA, MLP Director General TELMEX Scitum

Scitum | TELMEX está contigo

ASK THE EXPERT



16:15 -17:15 h

- **PROTECCIÓN DE REDES Y DISPOSITIVOS EN LA NUEVA NORMALIDAD DE LAS EMPRESAS**

S21SEC

JOSÉ FRANCISCO PANTOJA

Manager LATAM de Infraestructura

* Programa sujeto a cambios

infosecurity® MEXICO

Presenting Virtual Edition TREND MICRO

En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

AGENDA

24.SEPT.2020

ASK THE EXPERT

09:15 - 10:15 h

- **TELETRABAJAR DE MANERA SEGURA**

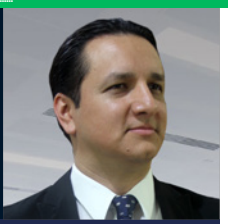
ANTONIO LOZANO MERINO

Responsable de Servicios de Ciberseguridad para Empresas de INCIBE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017

KEYNOTE

10:30 - 11:15 h



- **UN INGENIERO ANTISOCIAL… ENGINEERING!**

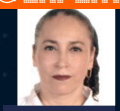
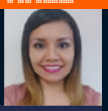
ARNULFO ESPINOSA

Presidente

ARES alliance

EXPERT PANEL

11:30 - 12:15 h

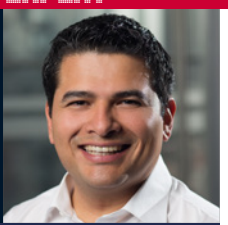

- **CHANGE & KNOWLEDGE MANAGEMENT EN CIBERSEGURIDAD**

- ROSA RAQUEL GARCÍA DE LEÓN
- GLORIA BEYDI PÉREZ
- MIGUEL A. ALVARADO
- EZEQUIEL CHÁVEZ
- EDILBERTO HILARIO

25 AÑOS Alapsi

ASK THE EXPERT

12:30 - 13:30 h



- **RESILIENCIA CIBERNÉTICA EN LOS TIEMPOS DE PANDEMIA**

DAVID RAMIREZ JOYA

Regional SE, LATAM

TRAPX SECURITY

* Programa sujeto a cambios

infosecurity MEXICO

Presenting Virtual Edition TREND MICRO

En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

AGENDA

24.SEPT.2020

CYBERTALK

13:45 - 14:15 h

- **CIBERSEGURIDAD FINANCIERA**

JESÚS CONSUELOS GARCIA

Cyber Security Senior Manager en Accentur y Vicepresidente de IAFCI

EXPERT PANEL



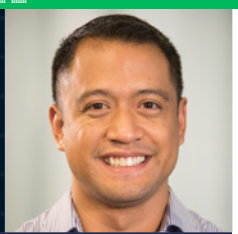

14:45 - 15:30 h

ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

- **GESTIONANDO RIESGOS**

- MODERADOR: ALBERTO FRIEDMANN
- FERNANDO GÓMEZ
- JOEL GÓMEZ
- GERARDO GALICIA

KEYNOTE



16:00 - 16:45 h

- **A FIREWALL AGAINST YOUR DEMONS: ACHIEVING A HACKERS MINDSET IN AN UNCERTAIN WORLD**

WILSON BAUTISTA

Founder

Jün Cyber

* Programa sujeto a cambios

GlobalSign®
GMO INTERNET GROUP

Los beneficios de una solución de firma digital todo en uno para lugares de trabajo remotos

- Ahorrar tiempo
- Eliminar las complejidades del flujo de trabajo
- Reducir costos
- Administrar múltiples usuarios
- Firmar electrónicamente con certificados digitales

GlobalSign® GMO INTERNET GROUP

e-Contract Service Agree By GlobalSign

CÓMO FUNCIONA EL ACUERDO

Visite https://www.globalsign.com/es/lp/agree-globalsign-pren para obtener más información

globalsign.com/es | contacto@globalsign.com
USA: 1-603-570-7060 | MX: 57-222-502-8962 | BR: 55-11-4680-6754

Juice Jacking,
la modalidad para el robo de datos

A las amenazas registradas hasta el día de hoy, se suma esta nueva modalidad de ataque cibernético que involucra cargadores de pared maliciosos o accesorios móviles comprometidos, conocido como Juice Jacking.

Las estaciones de carga de energía USB públicas son ahora el principal foco de preocupación para la seguridad pública y privada, por lo que las organizaciones deben comprender que mediante estos recursos pueden ser adjudicados ciertos datos por ciberdelincuentes como un conducto para implementar malware, robando así datos confidenciales.

¿Qué es Juice Jacking?

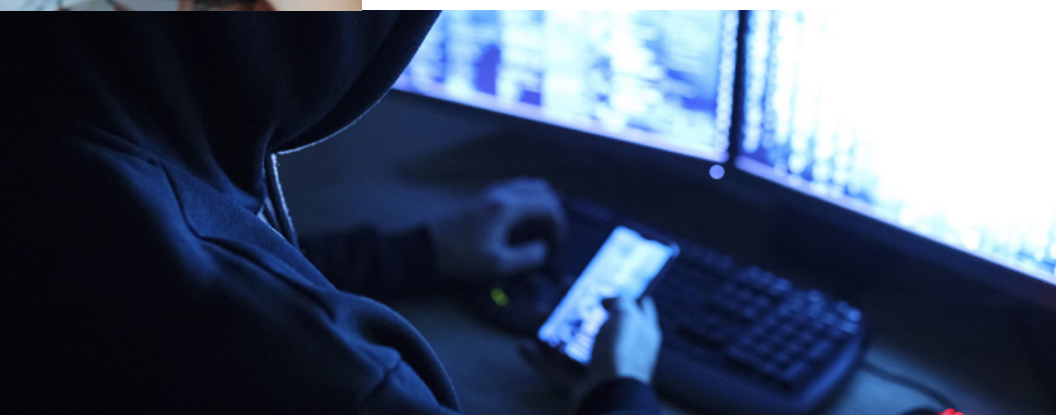
Los puertos de carga USB en lugares como aeropuertos, hoteles y otros sitios, se pueden reemplazar con versiones modificadas capaces de enviar malware a los dispositivos una vez que estén conectados. Un método aún más fácil es modificar un adaptador de CA o incluso un cable de carga para hacer lo mismo.

Esto funciona, por supuesto, porque el estándar USB está diseñado para transmitir electricidad y datos. En las estaciones de carga públicas, la gente está pensando en usar USB solo para cargar, pero los ciberdelincuentes pretenden usarlo para robar datos o para entregar malware.

Amenaza al auge

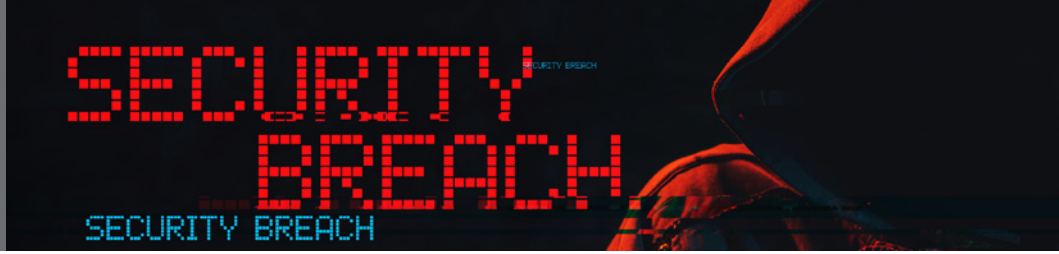
Actualmente, el FBI, e incluso el Better Business Bureau (BBB), han advertido a la población sobre los peligros del robo de jugos. Sin embargo, algunos expertos en seguridad descartan la amenaza, alegando que todas las noticias a su alrededor provienen de investigadores éticos que demuestran hacks de prueba de concepto y que no han aparecido casos conocidos de extracción de jugo en la naturaleza. Además, los teléfonos inteligentes modernos alertan a los usuarios cuando se transfieren datos.

Aun así, cada amenaza es teórica hasta que ocurre un incidente, y cuando nos enteramos de un nuevo ataque en la naturaleza, los datos ya habrán sido robados. También vale la pena señalar que los ciberdelincuentes centran cada vez más sus esfuerzos en los ataques contra los viajeros de negocios.



Cómo prevenir la extracción de jugo

- Evitar usar estaciones de carga públicas que ofrezcan puertos USB.
- Utilizar adaptadores de carga y cables propios para enchufar los dispositivos a las estaciones eléctricas públicas.
- Portar una batería móvil certificada de alta calidad para no tener que depender de las oportunidades de energía.
- No usar la PC de otra persona para cargar los dispositivos móviles.
- Utilizar una llave de bloqueo de datos USB, que es un producto que desactiva la transferencia de datos.



Algunos puntos más importantes para derrotar la extracción de jugo

Para evitar la extracción de jugo es necesario capacitar a ejecutivos y empleados sobre la clasificación de herramientas y procesos, para que sean capaces de transmitir datos evitando cualquier interferencia de malware, integrando un enfoque más amplio de la ciberseguridad.

Hoy por hoy, una de las tácticas más usadas para robar datos es simplemente implementando un punto de acceso Wi-Fi honeypot, que permite atacar dispositivos móviles en cualquier área.

Un método de prevención es usar un bloqueador de datos, el llamado "condón USB", aunque esta vía es poco conveniente ya que se tiene que adquirir, llevarlo, recordar usarlo y luego sufrir los tiempos de carga más lentos que estos dispositivos suelen causar, además de que generalmente están disponibles para conexiones USB 2, pero no suelen funcionar con conexiones USB 3 más rápidas.

Por lo general, muchos métodos anti-zumo implican el uso de cables y adaptadores autorizados. Los cables baratos, no autorizados o de imitación pueden reducir el rendimiento de la batería e incluso poner los dispositivos en riesgo de dañarse. Los cables y adaptadores defectuosos también representan un riesgo de incendio, por lo que el uso de cables y adaptadores de carga conocidos y de buena reputación siempre es una buena práctica.

Conclusión

Podremos concluir que esta práctica de Juice Jacking es un ataque raro o no practicado actualmente, sin embargo, está lleno de potencial para los ciberdelincuentes y espías ya que ciertas estrategias implementadas son fáciles de disuadir, por lo que es crucial integrar medidas contra el robo de jugo en los planes generales de ciberseguridad.

Fuentes

https://securityboulevard.com/2020/02/juice-jacking-how-hackers-can-steal-your-info-when-you-charge-devices/

https://timesofindia.indiatimes.com/blogs/tastefully-contemporary/beware-of-juice-jacking-a-new-way-to-steal-your-data/

https://www.informationsecuritybuzz.com/articles/the-ins-and-outs-of-juice-jacking-attacks/

Caso de éxito DLP – ICT- ICE

El reto

Diseñar una estrategia de protección de datos integral, flexible y funcional, que permitiera a su vez lograr la identificación de la información crítica de **TV Azteca,** manteniendo como premisa el gestionar el uso y manejo de la información, evitando afectar la operación diaria de sus usuarios.

¿Cómo lograrlo?

Implementando la herramienta de Prevención de **Perdida de datos (Data Lost Prevention, DLP)** e integrando módulos dedicados a la Clasificación y Encripción de información en medios removibles, para desarrollar un **esquema de protección de datos** robusto, capaz de:

1.- Monitorear la actividad de más de **4000 usuarios** y restringir el uso de información crítica, mediante la configuración de políticas y reglas de negocio funcionales.

2.- Clasificar la información diaria de más de **2000 usuarios** por su grado de importancia, contribuyendo con esto a la identificación de información crítica para **TV Azteca.**

3.- Proteger la información enviada a medios removibles mediante su encripción, limitando su uso solo a usuarios autorizados.

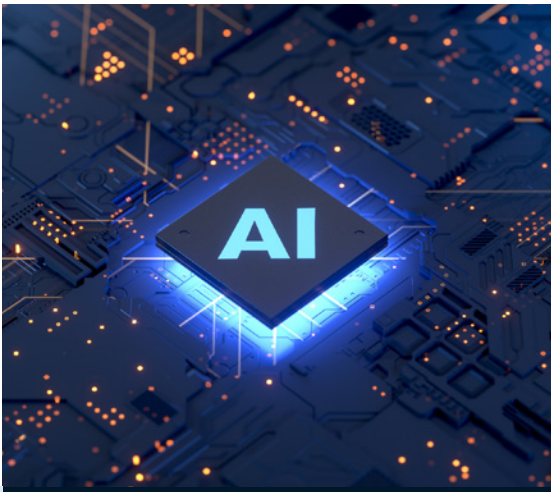
Conclusión

Gracias al análisis efectivo y puntual sobre las necesidades de **TV Azteca, Totalsec** logró desarrollar un esquema de protección de datos que no únicamente involucra la implementación de herramientas para su funcionamiento, sino que su visión los llevó a integrar de manera simultánea un esquema de concientización con los usuarios, haciéndolos participes en la identificación y clasificación de información de acuerdo a su uso.

Machine learning y AI

A través de algoritmos, las empresas aprenden con la ayuda de AI y machine learning cuáles son nuestras preferencias y qué nos atrae para ofrecernos productos y servicios basados en los datos personalizados, gustos y necesidades.

De la misma manera, los profesionales de la ciberseguridad se enfrentan constantemente a una enorme cantidad de amenazas a analizar y priorizar a diario.



Preguntamos a nuestra comunidad de profesionales qué opinaban acerca del uso de AI y machine learning en la ciberseguridad, a lo cual el 46% respondió que estas tecnologías tienen gran impacto para detectar y defenderse contra ataques, sin embargo, el 39% respondió que estas tecnologías son útiles para automatizar algunos procesos de seguridad, pero su impacto en general es limitado.

Lo cierto es que los ciberdelincuentes están empleando métodos de ataque cada vez más sofisticados y en constante evolución, sin embargo, como mencionó el Exsecretario de Defensa de los Estados Unidos, Donald Rumsfeld, no es suficiente perseguir lo conocido, son las incógnitas conocidas y las incógnitas desconocidas las que van a causar el mayor daño. Es decir, luchar contra el enemigo de ayer puede funcionar cuando las amenazas de hoy son las mismas que las de ayer, pero no cuando cambian constantemente, dando lugar a nuevas creadas por piratas informáticos e inteligencia artificial.

Sin duda, no existe una solución mágica que proporcione una protección al 100%. Podemos ayudarnos de diferentes herramientas, pero es imprescindible seguir aprendiendo y evolucionando para poder combatir en esta guerra cibernética.

S21SEC

Nuestros expertos pueden solucionar cualquier problema en relación a incidentes de ciberseguridad para que tu negocio siga su curso.

S21sec es una empresa internacional de ciberseguridad con años en el mercado en América y Europa.

ÁREAS DE ESPECIALIZACIÓN DE S21SEC


SOC


Integración


Consultoría


Ciberinteligencia


Red Team & Forensic

CYBERSECURITY YOU CAN TRUST

- Amplia experiencia en ciberseguridad
- Certificaciones específicas
- Portafolio completo de soluciones de ciberseguridad
- Metodología y herramientas propias

marketing@s21sec.com

DIRECTORIO DE EXPOSITORES

CHECK POINT SOFTWARE TECHNOLOGIES

Somos el mayor proveedor de redes de seguridad cibernética a nivel mundial. Brindamos soluciones líderes en la industria y protegemos a los clientes contra ataques cibernéticos con una incomparable tasa de captura de malware y contra otros tipos de amenazas avanzadas. Ofrecemos una completa Arquitectura de Seguridad (desde las redes hasta los dispositivos móviles) además de servicios de gestión de seguridad completos e intuitivos. Hoy protegemos a más de 100,000 organizaciones de todos los tamaños.

Montes Urales No. 415 Piso 3 B
Lomas Virreyes, Lomas de Chapultepec
Miguel Hidalgo, Ciudad de México
México, CP: 11000
Tel: +52 55 5540-5435
www.checkpoint.com

/checkpointsoftware
@checkpointsw
/check-point-software-technologies
/CPGlobal

CSI CONSULTORES DE SEGURIDAD DE LA INFORMACIÓN

Empresa 100% mexicana con personal altamente capacitado para brindar los servicios de: análisis de vulnerabilidades estático y dinámico, pruebas de penetración, programas de concientización, auditorías de cumplimiento, implementación de mejores prácticas, análisis forense y prevención de fraudes, entre otros. Somos la mejor empresa de Consultoría en Seguridad de la Información.

Coyoacán, Ciudad de México
México, CP: 04420
Tel: +52 55 8582-0941
E-mail: info@csinfo.com.mx
www.csinfo.com.mx

/csiconsultoresenseguridad
@consultores_csi
/csi-consultores-en-seguridad-de-la-información/

DIGITAL TOP SPONSOR

Empresa de servicios de identidad que ofrece soluciones de PKI escalables basadas en la nube que permiten a las empresas llevar a cabo transacciones comerciales, comunicaciones, entrega de contenidos e interacciones sociales de forma segura. Sus soluciones confiables de identidad y seguridad permiten que organizaciones aseguren las comunicaciones en línea, administren millones de identidades digitales verificadas y automaticen la autenticación y el cifrado.

2 International Dr. No. 150
Portsmouth, New Hampshire
Estados Unidos, CP: 03801
Tel: 57-222-502-8962
E-mail: contacto@globalsign.com
www.globalsign.com/es

/GlobalSignSSL
@globalsign
/globalsign-seguridad-digital/
Da clic aquí

GOOGLE CLOUD PLATFORM (GCP)

Google Cloud Platform (GCP), ofrecido por Google, es un conjunto de servicios de computación en la nube que se ejecuta en la misma infraestructura que Google usa internamente para su producto de usuario final.

Montes Urales No. 445
Lomas - Virreyes, Lomas de Chapultepec
Miguel Hidalgo, Ciudad de México
México, CP: 11000
Tel: 800-083-5649
E-mail:
sales-team-google-cloud-mexico@google.com
www.cloud.google.com

@googlecloud
/googlecloud

DIGITAL TOP SPONSOR

LexisNexis® RISK SOLUTIONS

Nuestras soluciones de gestión fraude e identidad combinan información de identidad física y digital transformandola con tecnología avanzada de toma de decisiones y autenticación para ofrecer una visión precisa del riesgo de identidad del cliente. Además, permiten que su negocio aumente la efectividad y precisión del análisis de decisiones, verificación y autenticación de identidad y dispositivos, e investigaciones. Concéntrese en la experiencia de su cliente y combata eficazmente el fraude.

Paseo de la Reforma No. 243 Piso 15
Edificio Mapfre
Cuauhtémoc, Ciudad de México
México, CP: 06500
Tel: +52 55 4755-0043
E-mail: alexander.peeters@lexisnexisrisk.com
www.risk.lexisnexis.com/fraude

/lexisnexis-risk-solutions-business-services/

ONE eSECURITY

Especialista líder en el mercado en servicios y tecnología de Digital Forensics and Incident Response (DFIR). Nuestros servicios están dirigidos a clientes que necesitan rápida respuesta y soporte cuando ocurre una brecha de seguridad. Cubrimos todo el ciclo de vida de la respuesta a incidentes, desde los servicios de preparación hasta las evaluaciones y el análisis de brechas de su plan de respuesta a incidentes, plan de gestión de crisis y plan de continuidad del negocio, desarrollando y mejorando sus capacidades de ciberseguridad.

Av. Paseo de la Reforma No. 342 Piso 25
Of. 2640 Torre New York Life
Ciudad de México
México, CP: 06600
Tel: +52 55 2881-6666
E-mail: info@one-esecurity.com
www.one-esecurity.com/

@One_eSecurity
/one-esecurity/

DIRECTORIO DE EXPOSITORES

PREMIUM SPONSOR

Somos una empresa líder internacional con presencia en Europa y América Latina. Nos caracterizamos por contar con más de 500 especialistas certificados en ciberseguridad.

/S21sec_ @S21sec /s21sec

Río Pánuco No. 108
Cuauhtémoc, Ciudad de México
México, CP: 06500
Tel: +52 55 7822-0127
E-mail: marketing@s21sec.com
www.s21sec.com

DIGITAL TOP SPONSOR

Es una plataforma en la nube, la cual contiene numerosas aplicaciones para la optimización de las operaciones y la creación de experiencias tanto para empleados como para clientes.

/servicenow @ServiceNow_EMEA
/servicenow /servicenowinc

Paseo de los Tamarindos No. 90 Piso 19,
Arcos Bosques Torre 2
Bosques de las Lomas
Cuajimalpa, Ciudad de México
México, CP: 05120
Tel: +52 55 852-63466
E-mail: marketinglatam@servicenow.com
www.servicenow.es/

STATE OF TEXAS MEXICO OFFICE

La oficina del Estado de Texas en México brinda asistencia integral en comercio a empresas de Texas interesadas en exportar productos y servicios a México, al tiempo que facilita las oportunidades de inversión a empresas mexicanas mediante alianzas internacionales de desarrollo. Para este evento, contamos con la participación de empresas en el sector de ciberseguridad, provenientes del Estado de Texas y la ciudad de San Antonio; esta última cuenta con la segunda concentración más grande de profesionales de ciberseguridad en Estados Unidos.

José María Castorena
Cuajimalpa, Ciudad de México
México, CP: 11270
Tel: +52 55 5514-8100
E-mail: contact@texasinmexico.com
www.gov.texas.gov/business

/TexasInMexico

@TexasInMexico

Da clic aquí

DIRECTORIO DE EXPOSITORES

CONTENT SPONSOR

totalsec
Expertos en Ciberseguridad

Somos una empresa de Grupo Salinas con un equipo de profesionales de ciberseguridad y seguridad de la información, con experiencia de más de 15 años protegiendo a nuestros clientes en los sectores financieros, retail, telecomunicaciones, medios de comunicación, sector gobierno, pymes y más.

Periférico Sur No. 4121
Fuentes del Pedregal
Tlalpan, Ciudad de México
México, CP: 14140
Tel: +52 55 1720-7777
E-mail: contacto@totalsec.com.mx
www.totalsec.com.mx

/TotalsecMx/ **@TotalsecMx** **/totalsec** **Da clic aquí**

TRAPX SECURITY

TRAPX SECURITY

Empresa israelita creadora de la tecnología basada en el engaño que detecta, analiza y derrota los ataques de ransomware. Su oferta denominada DeceptionGrid 6.1 es una plataforma que protege los activos contra una multitud de ataques, incluidos internos malintencionados, movimientos laterales, amenazas persistentes avanzadas, día cero y ciberdelincuentes. La solución sirve a los mercados de proveedores de servicios de seguridad, salud, manufactura, financieros, venta minorista, gobierno, tecnología y administración.

Av. Patriotismo 229 Pisos 7 y 8
Ciudad de México
www.trapx.com

/TrapXDeception

@ rapXSecurity

/trapx

PRESENTING EDICIÓN VIRTUAL

TREND MICRO™

Líder mundial en soluciones de ciberseguridad, ayudamos a hacer del mundo un lugar más seguro para el intercambio de información digital. Nuestras innovadoras soluciones para consumidores, empresas y gobiernos brindan seguridad en capas para data centers, workloads en la nube, redes y endpoints. Todos nuestros productos trabajan en conjunto para compartir la inteligencia de amenazas y proporcionar una defensa interconectada con visibilidad y control centralizados, lo que permite una mejor y más rápida protección. Con más de 6,000 empleados en más de 50 países.

Av. Insurgentes Sur No.730 Piso 3
Del Valle
Benito Juárez, Ciudad de México
México, CP: 03100
Tel: +52 55 3067-6000
E-mail: marketing_la@trendmicro.com
www.trendmicro.com

/TrendMicroLATAM

@TrendMicroLATAM

/trend-micro-latam

Da clic aquí

ASOCIACIONES Y ALIADOS

ALAPSI, A.C. (ASOCIACIÓN LATINOAMERICANA DE PROFESIONALES DE SEGURIDAD INFORMÁTICA, A.C.)

Más de 25 años promocionando el conocimiento de seguridad de la información y ciberseguridad en instituciones privadas, educativas, gubernamentales y sociedad en general, mediante diplomados, seminarios, cursos, talleres y preparación para certificaciones internacionales ISO, ISACA, ISC2, NIST, mejores prácticas, otros.

Ciudad México
E-mail: contacto@alapsi.org
www.alapsi.org

ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

ASIS International es la organización más grande de Profesionales de la seguridad en el mundo, cuenta con 38,000 miembros y tiene presencia en 149 países, en los 5 continentes. ASIS Capítulo México, existe hace más de 25 años.

Ciudad México
E-mail: info@asis.org.mx
www.asis.org.mx

/asis-international-chapter-mexico

AMECI MÉXICO

Empresa mexicana que se especializa en capacitación en diversos nivel y especialidades, diagnóstico y determinación de riesgos, corrección de problemas de seguridad informática y servicios de análisis de vulnerabilidades en infraestructuras de TIC y remediación y mitigación de hallazgos.

Ciudad México
www.ameci.org

CETIC

Es una agrupación organizada de empresarios del sector de las tecnologías de información y comunicaciones con la finalidad de representar a sus asociaciones afiliadas ante instituciones académicas, de gobierno y otras cámaras y asociaciones empresariales. Con ello, busca impulsar y fortalecer el posicionamiento de los productos y servicios de los asociados e integrarlos en soluciones que permitan el progreso económico de todos los sectores en general.

Ciudad México
www.cetic.com.mx/inicio

ASOCIACIONES Y ALIADOS / MEDIOS

ALIADO ESTRATÉGICO

ISACA Mexico City Chapter

Asociación global que brinda a los profesionales de TI conocimientos, credenciales, capacitación y comunidad en auditoría, gobernanza, riesgo y privacidad.

Ciudad México
www.isaca.org

ISACA Guadalajara Chapter

Asociación global que brinda a los profesionales de TI conocimientos, credenciales, capacitación y comunidad en auditoría, gobernanza, riesgo y privacidad.

Guadalajara
www.isaca.org

UDLAP JENKINS GRADUATE SCHOOL

UDLAP JENKINS GRADUATE SCHOOL

Institución académica de alto nivel que ofrece diversos programas de maestría y educación continua en forma de diplomados, cursos y talleres para quienes buscan aplicar en sus actividades profesionales las máximas de excelencia, innovación, liderazgo y creatividad.

Ciudad México
E-mail: informes@udlapjenkins.mx
www.udlapjenkins.mx

MEDIOS

REVISTA CONSULTORÍA

REVISTA CONSULTORÍA

La única revista digital e impresa especializada en los principales temas de este importante sector. Por su amplio concepto, reúne en su contenido los diferentes campos de la consultoría, infraestructura y obra, sustentabilidad, pymes, negocios, recursos humanos, tecnología, etc., con temas escritos por especialistas y dirigido a empresarios, funcionarios y altos ejecutivos que requieren de información práctica, profesional y objetiva de este rubro. Su periodicidad es mensual y editamos 3 suplementos y una edición especial durante el año.

Ciudad México
www.revistaconsultoria.com.mx

Revista MÁS SEGURIDAD
Servicios informativos de y para la industria

REVISTA MÁS SEGURIDAD

Es una publicación especializada con 12 años de existencia y distribución en México y Latinoamérica, a través de las versiones impresa y digital, newsletter semanal, portal de noticias, RRSS y podcats.

Ciudad México
www.revistamasseguridad.com.mx

edición méxico usecnetwork International magazine

REVISTA USECNETWORK

Revista impresa y digital técnica en seguridad.

Ciudad México
www.usecim.net/

Caso de éxito
Correlación Grupo Salinas

En Grupo Salinas, al ser una empresa con presencia en todo el país, requerían contar con una herramienta que pudiera contener gran cantidad de información y que fuera consultada de una manera rápida. Anteriormente, contaban con una tecnología SIEM, sin embargo, era compleja y poco intuitiva para los usuarios, lo que resultaba en una pobre explotación de los datos ahí almacenados.

Asimismo, dentro de sus planes estaba el incrementar la cantidad de tecnologías de seguridad que reportarían al SIEM y el modelo de licenciamiento no era el adecuado para la estrategia que se manejaría.

Actualmente, con el servicio de CSOC de Totalsec y su herramienta de SIEM, se tienen 50 diferentes tecnologías reportando sus logs, dando un aproximado de 20,000 millones de logs al mes, se generan un aproximado de 400 incidentes de seguridad al mes.

"En Ciberseguridad hace años nos preocupábamos de detectar eventos relevantes ya que habían ocurrido. Hoy, nuestras metas son detectar de manera temprana, pronosticar y prevenir.

El Servicio de CSOC de Totalsec ha sido la clave que nos ha llevado de la simple gestión de datos a verdaderamente extraer conocimientos de ellos. Un gran avance en el camino entre los datos duros y la sabiduría."

Julio César López Santana
Director de Network Security & Analytics, Grupo Salinas

En los últimos meses del servicio, se ha convertido en la principal herramienta en el proyecto de Threathunting de Grupo Salinas.

"El Servicio del CSOC de Totalsec nos ayuda para realizar análisis más avanzados utilizando la correlación de eventos de todas las herramientas que envían Logs, además de que podemos generar dashboards que nos ayudan operativamente a identificar de manera más rápida y sencilla algún evento relevante que debe de ser atendido de manera inmediata."

Iván Sánchez Moreno
Gerente SOC, Grupo Salinas

APTs como medida de disuasión contra ataques cibernéticos.

Actualmente la diversidad en ataques cibernéticos ha hecho de la ciberseguridad uno de los principales temas de interés tanto de las empresas como de la sociedad. Entre aquellas amenazas que resultan más preocupantes, se encuentra el APT o Advanced Persistent Threat.

En este artículo aprenderás qué son las APT, cómo funcionan, sus características y sus fases. Además, verás los ejemplos reales de APT que se utilizaron para llevar a cabo ataques, así como contrarrestar ciertos riesgos a tus dispositivos.

Una APT se define como un ataque centralizado en un objetivo específico con el fin de comprometer el sistema y robar información; utiliza diferentes herramientas para obtener acceso a su objetivo y ampliar el ataque.

Características de los ataques APT

1. **Troyanos de puerta trasera generalizados.**

   Los ataques APT dependen de troyanos de puerta trasera, porque los atacantes necesitan volver a los sistemas en los que han establecido una entrada principal para filtrarse en dicho software.

2. **Flujos de información.**

   Se establece el uso de VPNs por parte de los atacantes, mediante el uso del HTTPS. por lo que un buen punto de partida para identificar dicho malware, es saber cómo se ve normalmente tu flujo de información.

3. **Paquetes de datos inesperados.**

   Estos paquetes de datos pueden ser tu información que se filtra a los atacantes. Debes estar atento a grandes cantidades de información que está donde no debería estar, especialmente si está comprimida.

4. **Campañas enfocadas de spear phishing.**

   Se emplean correos electrónicos que comúnmente tienen un archivo de documento infectado generado por enlaces URL maliciosos o código ejecutable malicioso, por lo que rastrear el sistema infectado podría llevarte al punto cero del ataque APT.

Fases de una APT

1. Conocer el objetivo; la información recopilada puede ayudar a promover el ataque.
2. Encontrar una entrada y enviar malware personalizado; se puede lograr mediante phishing o usando otros medios.
3. Obtener el punto de apoyo; engañar a un usuario para que ejecute el malware en su sistema, dentro de la red objetivo.
4. Ampliando el alcance del ataque.
5. Encontrar y robar información; esto puede implicar la elevación de privilegios.
6. Mover y cubrir pistas; puede ser necesario mover o expandir los puntos de entrada para avanzar en el ataque.

3 ejemplos reales de APT

GhostNet

Este grupo de ciberataques APT, con sede en China, utilizó spear Phishing, así como archivos adjuntos maliciosos para obtener acceso a los sistemas en más de 100 países a partir de 2009. Entre las muchas técnicas de ataque que GhostNet utilizó fueron el audio y la captura de pantalla para obtener información sobre los objetivos.

Sykipot APT

El grupo de ataque Sykipot es conocido en parte por crear la familia de malware Sykipot APT. Este malware personalizado aprovechó vulnerabilidades en productos de Adobe y usó ataques de spear phishing para efectuar exploits de día cero sobre sus víctimas.

Mettel

Este grupo de ataque, junto con otros incluidos Carbanak y GCMAN, se dirigió a instituciones financieras. Mettel usó malware personalizado para infectar cajeros automáticos. Cuando los cajeros automáticos se liquidaron al final del día, el malware hizo transacciones de los cajeros automáticos. Esto demuestra que los ataques APT pueden robar dinero e información.

¿Cómo protegerse de las APTs?

1. Las APTs son programas diseñados con base a las características del objetivo, por lo que un antivirus o antimalware convencional no suelen ser efectivos, ya que se suelen basar en buscar patrones conocidos de otros virus que tienen en la base de datos. En este sentido, la mejor recomendación es disponer de mecanismos de seguridad y software actualizado tanto en equipos de usuario como servidores (Windows, Linux, macOS) para que los atacantes no puedan aprovechar vulnerabilidades y así infectarlos.

2. Es indispensable concienciar a todos y cada uno de los empleados de la importancia de la seguridad en la organización e implementar mejores prácticas, mediante protocolos, reglas y procedimientos.

3. Utilizar políticas de contraseñas robustas y que éstas se cambien con frecuencia.

4. Instalar un firewall (cortafuegos) corporativo, que aísla la red de la organización del exterior y, bien configurado, puede llevar a detectar los APTs a través de los ataques realizados, ya que se puede llegar a controlar lo que entra y lo que sale de la red, monitorizando el flujo de los datos de entrada y salida, aunque muchos cibercriminales usan los puertos 80 y 443 (http y https) para sus conexiones,

lo que hace que despierten menos sospechas.

5. Realizar un análisis del tráfico para detectar anomalías o intrusos en la red utilizando IDS Sistemas de Detección de Intrusos, para localizar y evitar que atacantes realicen ARP spoofing, Rogue DHCP server o ataques de otro tipo.

6. Instalación de HIDS (sistemas de detección de intrusos basados en host – Host based intrusion detection systems), que son agentes que se instalan individualmente en cada equipo y monitorizan el estado del sistema, alertando de posibles amenazas.

7. Instalación de herramientas que reduzcan la probabilidad de que se exploten las vulnerabilidades provenientes de spear phishing y fallos en aplicaciones para infectar al atacante. Herramientas como EMET (Enhanced Mitigation Experience Toolkit y la guía de usuario de EMET) permiten reducir las probabilidades de que un atacante ejecute código malicioso a través en un cierto programa.

8. Utilizar herramientas como Honeypoto, que son sistemas especialmente diseñados para ser atacados, pero cuyo objetivo es ser un señuelo para que se detecte la intrusión. Honeynets es un equivalente, pero son auténticas redes de señuelos falsos, IOC (indicadores de compromiso) por las que, a través de unos esquemas XML, pueden llegar a detectarse ataques de APT, etc.

Conclusión

A partir de dicha información podremos catalogar a las APT como una especie de "suite" de Malware ya que combina una amplia variedad del mismo, desde un malware preexistente hasta un malware personalizado, así como algunos métodos de trabajo adecuados para lanzar ataques dirigidos que pueden continuar durante un período de tiempo prolongado ya que tienden a persistir después de los intentos iniciales de detección y mitigación, convirtiéndolos en grandes riesgos de malware junto al ransomware.

Fuentes

http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO12_2020GABSAN_Submarinos.pdf

https://www.incibe-cert.es/blog/apt-amenaza-oculta

https://neuronamagazine.com/atacantes-aprovechan-herramientas-legitimas-en-el-30-de-los-ciberincidentes-exitosos/

https://www.gb-advisors.com/es/advanced-persistent-threat-atp-seguridad/

infosecurity®
MEXICO

SAVE THE DATE

26-27 mayo

Centro Citibanamex

EDICIÓN PRESENCIAL

www.infosecuritymexico.com