Número 97 | Diciembre 2024

NTT DATA

Radar

El magazine de ciberseguridad

Convergencia de la seguridad física y lógica en la ciberseguridad moderna

Por Enrique Bernao Rosado

La convergencia entre la seguridad física y lógica está transformando la ciberseguridad moderna, ya que ambas disciplinas, tradicionalmente aisladas, se están entrelazando para ofrecer una protección integral ante amenazas que pueden ser tanto físicas como digitales. Esta integración busca garantizar la seguridad de personas, bienes y datos, aprovechando las fortalezas de ambos enfoques para prevenir, detectar y responder a incidentes de seguridad.

Por dar algo de contexto, la seguridad física, engloba medidas para proteger el entorno físico, como edificios, oficinas o personas, contra accesos no autorizados, robos, sabotajes o desastres naturales.

Mientras que la seguridad lógica, incluye prácticas y herramientas para proteger la información digital y los sistemas contra accesos no autorizados, ciberataques y otras amenazas. La convergencia de ambas es crucial, ya que un enfoque aislado puede dejar vulnerabilidades explotables.

Integración de seguridad física y lógica

La convergencia de estos sistemas permite que las organizaciones tengan un enfoque de seguridad holístico, creando barreras más sólidas contra una gama amplia de amenazas. Veamos algunos ejemplos:

- **Control de Acceso Multifactorial:** Este tipo de control de acceso utiliza tanto factores físicos como lógicos para autorizar a una persona a entrar en un lugar o a un sistema. Este enfoque híbrido dificulta que una sola vulnerabilidad sea suficiente para burlar la seguridad.
- **Videovigilancia Inteligente:** Con el uso de cámaras conectadas a redes inteligentes y dotadas de algoritmos de inteligencia artificial, las organizaciones pueden monitorear áreas físicas en tiempo real y detectar comportamientos sospechosos.
- **Gestión de Identidad y Acceso (IAM) Centralizado:** En instalaciones grandes, la gestión de identidades que abarca tanto la seguridad física como la lógica permite que una organización controle el acceso de sus empleados de manera integral.
- **Dispositivos IoT en Seguridad Física:** Los dispositivos de IoT son cada vez más comunes en la seguridad física, como cámaras de vigilancia o cerraduras inteligentes. Sin embargo, al estar conectados a redes digitales, son susceptibles a ciberataques.

Riesgos y vulnerabilidades en la integración de iot y seguridad lógica

A medida que más dispositivos IoT se integran en sistemas de seguridad física, surgen nuevos desafíos en términos de ciberseguridad. Algunos de los principales riesgos incluyen:

- **Falta de actualizaciones de seguridad:** Muchos dispositivos IoT no se actualizan regularmente, lo que deja abiertas vulnerabilidades conocidas. Los atacantes pueden aprovechar estas brechas para acceder a la red o manipular el dispositivo.
- **Credenciales por defecto:** Algunos dispositivos IoT vienen con credenciales de fábrica que son fáciles de adivinar. Si no se cambian, un atacante podría utilizarlas para comprometer el dispositivo y obtener acceso a la red lógica.
- **Conectividad directa a Internet:** Si los dispositivos IoT están directamente conectados a Internet sin pasar por firewalls o redes privadas virtuales (VPN), pueden convertirse en puntos de entrada fáciles para atacantes externos.
- **Falta de segmentación de redes:** Muchos sistemas de IoT se encuentran en la misma red que otros activos críticos, lo cual facilita que, si un dispositivo es comprometido, el atacante tenga acceso a toda la infraestructura de la organización.

Mejores prácticas para una implementación segura

Para minimizar estos riesgos, es esencial adoptar una serie de buenas prácticas al integrar seguridad física y lógica:

1. **Autenticación Multifactorial (MFA):** Implementar autenticación multifactorial para todos los accesos, tanto físicos como lógicos, de manera que se reduzcan las probabilidades de acceso no autorizado.

2. **Actualización y parcheo constantes:** Mantener todos los dispositivos y sistemas actualizados con los últimos parches de seguridad es esencial para prevenir el aprovechamiento de vulnerabilidades conocidas.

3. **Segmentación de Redes:** Aislar los dispositivos IoT en redes separadas y aplicar firewalls robustos y protocolos de comunicación seguros ayuda a limitar el acceso de atacantes a la red principal en caso de que un dispositivo IoT sea comprometido.

4. **Uso de Redes Privadas Virtuales (VPN):** Al conectar dispositivos IoT o de seguridad física a la red, se debe considerar el uso de VPNs para añadir una capa extra de seguridad y cifrado en la transmisión de datos.

5. **Monitorización en tiempo real y respuesta a incidentes:** Implementar sistemas de monitoreo en tiempo real que detecten y respondan de forma automática a actividades sospechosas en redes y dispositivos IoT puede prevenir el escalamiento de incidentes de seguridad.

6. **Formación y Concienciación:** Invertir en la formación del personal es vital, ya que los errores humanos son una de las causas más comunes de brechas de seguridad. Los empleados deben entender los riesgos de la convergencia de seguridad física y lógica y saber cómo responder ante una posible amenaza.

Conclusión

La convergencia de la seguridad física y lógica es una evolución necesaria en la ciberseguridad moderna que busca proteger de forma integral a las organizaciones frente a amenazas complejas y multifacéticas.

Aunque esta integración aporta grandes beneficios, también plantea desafíos que deben abordarse con una estrategia bien planificada, centrada en buenas prácticas de seguridad y una combinación efectiva de tecnologías avanzadas.

A medida que la ciberseguridad evoluciona, la convergencia entre estos dos ámbitos será un pilar esencial para mantener la resiliencia de cualquier organización en el entorno actual.

Enrique Bernao Rosado
Cybersecurity Manager

Un relato de ataques, resiliencia y lecciones críticas

Cibercrónica por Alvaro Vela

El panorama de ciberseguridad del último mes se vio marcado por una oleada de ataques que pusieron a prueba la resiliencia de infraestructuras críticas, sectores corporativos y plataformas digitales. Desde sofisticadas campañas de ransomware hasta operativos globales para desarticular redes criminales, los eventos de este último mes ilustraron tanto las amenazas como las respuestas en el ámbito digital.

En octubre, uno de los primeros incidentes destacados fue el ciberataque a Wegmans, una conocida cadena de supermercados en Estados Unidos.

Este ataque, llevado a cabo el 3 de octubre, involucró ransomware que comprometió sistemas internos y expuso datos sensibles de clientes. Aunque los servicios se mantuvieron operativos, la intrusión evidenció vulnerabilidades críticas en la infraestructura tecnológica del sector retail.

Pocos días después, el 12 de octubre, Australia enfrentó un golpe significativo en su sistema sanitario. Varias clínicas en Victoria y Nueva Gales del Sur fueron blanco de un ataque cibernético que interrumpió servicios y buscó acceder a registros médicos. Si bien no se confirmó el robo de información crítica, las operaciones se vieron seriamente afectadas, subrayando la importancia de proteger los sistemas de salud en un entorno cada vez más digitalizado.

Hacia finales de mes, Europa fue escenario de una masiva campaña de phishing que afectó principalmente a instituciones financieras. Usando inteligencia artificial para replicar comunicaciones oficiales, los atacantes engañaron tanto a clientes como a empleados de alto rango, generando pérdidas millonarias.

Este tipo de ataques evidenció el uso de herramientas tecnológicas avanzadas para perpetrar fraudes con altos índices de éxito.

Mientras tanto, Canadá reportó, el 20 de octubre, un ataque de ransomware dirigido a su sector educativo.

Varias universidades vieron paralizadas sus plataformas de aprendizaje en línea, comprometiendo la continuidad académica y filtrando datos personales de estudiantes y profesores.

En Estados Unidos, el 25 de octubre, empresas del sector manufacturero sufrieron ataques a sus sistemas SCADA, lo que interrumpió temporalmente la producción.

Para finalizar el mes, el Reino Unido enfrentó una amenaza inusual: dispositivos IoT domésticos y empresariales fueron comprometidos y utilizados en una botnet masiva para lanzar ataques DDoS.

Noviembre comenzó con otro evento significativo: el 5 de noviembre, Amazon Web Services (AWS) sufrió un ataque DDoS masivo que afectó brevemente la disponibilidad de sus servicios globales.

Aunque no se comprometieron datos sensibles, el ataque destacó la necesidad de robustecer la protección de infraestructuras críticas en la nube.

El 13 de noviembre, un banco sudafricano informó una violación masiva en sus sistemas de banca en línea.

El incidente, causado por un ataque de malware, expuso información financiera de más de un millón de clientes. Este evento puso de manifiesto la creciente amenaza que enfrentan los sistemas financieros digitales en todo el mundo.

Más tarde, el 21 de noviembre, INTERPOL lideró una operación internacional que logró desmantelar redes de ransomware como LockBit, arrestando a 17 personas y recuperando claves de descifrado que permitieron mitigar el impacto en cientos de víctimas.

Este éxito demostró la efectividad de la cooperación internacional en la lucha contra el cibercrimen.

El ámbito del entretenimiento también fue afectado, cuando plataformas de videojuegos reportaron, el 10 de noviembre, intentos masivos de robo de credenciales.

Esto llevó a una oleada de alertas de seguridad y cambios masivos de contraseñas. A nivel industrial, el 18 de noviembre, se detectó una vulnerabilidad crítica en sistemas eléctricos de Sudamérica, la cual fue explotada sin causar daños mayores, pero dejando un claro mensaje sobre la urgencia de proteger estas infraestructuras críticas. futuro.

Finalmente, municipios en Japón y Corea del Sur fueron blanco de ataques con ransomware el 25 de noviembre, afectando servicios públicos esenciales y provocando filtraciones de documentos clasificados.

Estos eventos del pasado mes refuerzan la importancia de adoptar medidas de ciberseguridad proactivas. La sofisticación de los ataques, impulsada por herramientas avanzadas como la inteligencia artificial, y la creciente interconexión de sistemas resaltan la necesidad de estrategias robustas para proteger tanto a instituciones como a individuos. Ante un entorno cada vez más hostil, la inversión en prevención y la colaboración internacional son claves para enfrentar las amenazas digitales del

Alvaro Vela
Cybersecurity Expert Analyst

Replicación de Personalidad con IA: desafíos y oportunidades

Artículo por Carlos Moya Gamboa

La replicación de personalidad con Inteligencia Artificial (IA) es un área de investigación y desarrollo que ha generado mucho interés y debate en los últimos años. En este artículo, se presenta un experimento que busca replicar una personalidad utilizando dos enfoques distintos de IA. Analizaremos cómo los modelos de IA se desempeñan en esta tarea, destacando sus capacidades y limitaciones. El objetivo es proporcionar una visión general de este tema, ayudar a entender y aprovechar las posibilidades y mitigar los riesgos asociados con la replicación de personalidad con IA.

La integración de la IA en ciberseguridad ha permitido avances significativos en la protección de datos y la identificación de amenazas, gracias a la capacidad de las máquinas para aprender de grandes volúmenes de datos y detectar patrones.

Sin embargo, la idea de replicar personalidades humanas con IA representa un nuevo horizonte, impulsado por la creciente disponibilidad de datos personales y el avance en algoritmos de aprendizaje profundo.

La replicación de personalidades con IA tiene la capacidad de transformar cómo se perciben e interactúan los seres humanos con sí mismos y con otros, lo que puede tener implicaciones para la ciberseguridad. Esto debido a que puede ser utilizada para crear personalidades digitales que simulen a personas reales o incluso a personas ficticias, lo que puede crear confusiones y riesgos según el uso que se les dé.

Metodología

Para llevar a cabo el experimento de replicación de personalidad, se utilizaron dos enfoques distintos de inteligencia artificial. El primer enfoque se basó en la recopilación de datos del perfil digital disponible en internet. Para ello, se utilizaron campos como: nombre completo, edad, país de residencia, cédula de identidad y correo electrónico.

El segundo enfoque consistió en la recopilación de datos detallados sobre la personalidad del individuo, utilizando como base la teoría de los grandes rasgos de la personalidad (apertura a la experiencia, responsabilidad, extraversión, amabilidad y neuroticismo).

Existen varios simuladores en línea que muestran datos cualitativos y cuantitativos de cada uno de los rasgos, basados en un cuestionario. En la Ilustración 1 se muestran los resultados obtenidos del sujeto de estudio en cada uno de ellos. Además, se incluyó información sobre vivencias personales, valores, intereses, hábitos, influencias culturales y sociales, formación académica y experiencia profesional.

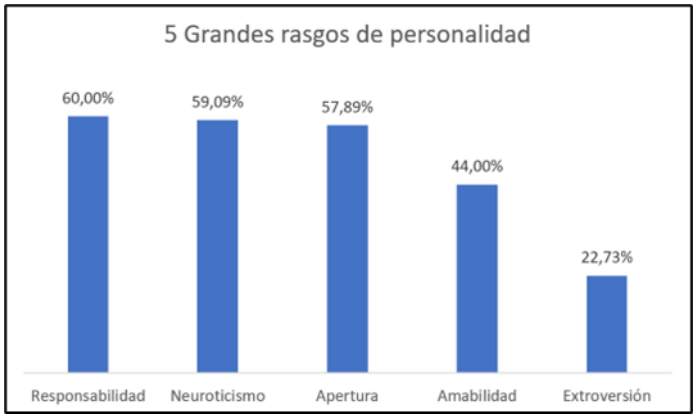


Ilustración 1 Resultados Teoría de los 5 grandes rasgos de la personalidad.

Se utilizaron dos modelos de IA distintos: ChatGPT-4, en su versión en línea y Mistral instructu v0 1 7B Q8_0 gguf, instalado en modo local, para evaluar su capacidad de replicar con precisión y complejidad la personalidad humana.
Resultados
Para evaluar la eficacia en la asimilación de personalidad del individuo, se consideraron los resultados cualitativos del Test de los 5 rasgos de la personalidad y el desempeño en tres entornos distintos: Una presentación en una video llamada para una entrevista de trabajo, una primera cita con una mujer y resolver un conflicto de trabajo con su jefe.

El análisis realizado se basa en el diálogo que tiene consigo mismo la IA en cada entorno y su desarrollo. Los criterios de evaluación fueron: Perfil digital, fluidez, adaptabilidad, coherencia e idioma.

Aspecto evaluado	ChatGPT 4.0	Mistral instructu v0 1 7B Q8_0 gguf
Test de los 5 rasgos de la personalidad	No mostró información cuantitativa al ingresar información cualitativa de cada rasgo; sin embargo, asimila la información provista de manera eficiente.	Al proporcionarle información cualitativa de cada uno de los rasgos, pudo reensamblar con bastante precisión los valores cuantitativos de estos.
Perfil digital	Aunque su política de privacidad limita la búsqueda, al utilizar técnicas de OSINT, puede determinar información confiable sobre el individuo, incluyendo perfiles de LinkedIn y documentos en repositorios como Clubensayos e Issuu.	La búsqueda no proporciona valores precisos del individuo. Identificó el perfil de LinkedIn correcto; sin embargo, los sitios en línea relacionados no proporcionan información legible.
Fluidez	Su dialecto es natural y se adapta a cada situación. Los diálogos propuestos se basan en la personalidad y situación planteadas.	Su respuesta es forzada. Busca utilizar las palabras provistas como información inicial y utilizarlas dentro del dialogo. Los diálogos no se basan por completo en la personalidad y situación planteada.
Adaptabilidad	Plantea preguntas y respuestas adaptadas a la situación. Inclusive genera nueva información que no ha sido ingresada previamente.	No cuenta con iniciativas de formular preguntas de temas no tratados en la información proporcionada. El dialogo entre situaciones mantiene la misma estructura, no es adaptable.
Coherencia	Sus respuestas se asemejan a la personalidad del individuo de estudio.	Los diálogos no se basan por completo en la personalidad y situación planteada.
Idioma	Mantiene con precisión el idioma utilizado.	Mezcla palabras entre inglés y español

Análisis

El experimento comparativo demostró que ChatGPT 4.0 cuenta con una notable capacidad para asimilar información cualitativa sobre los rasgos de personalidad y mantener una fluidez natural en los diálogos.

Su adaptabilidad y habilidad para formular preguntas pertinentes lo posicionan como una opción sólida para aplicaciones que requieren interacción humana fluida y coherente. Por otro lado, Mistral Instruct v0.1 7B Q8_0 gguf mostró fortalezas en la precisión de la información numérica de los rasgos de personalidad, pero presentó limitaciones significativas en términos de fluidez en el diálogo, adaptabilidad en las respuestas y búsqueda de información en línea.

Desafíos en la Replicación de Personalidad con IA

Uno de los mayores desafíos es la precisión de los datos del perfil digital, que a menudo puede ser incompleto o inexacto.

Replicar la complejidad de la personalidad humana también es un reto, dado que involucra aspectos sutiles y profundos de la psicología individual. Además, hay preocupaciones éticas y de privacidad sobre el uso de datos personales y el potencial para el mal uso de esta información.

Oportunidades

La capacidad de asimilar personalidades con IA ofrece beneficios significativos. En ciberseguridad, la replicación precisa de personalidades podría impulsar avances en la autenticación biométrica y el desarrollo de sistemas de seguridad más robustos y adaptables.

También tiene el potencial de mejorar la interacción humano-máquina y ofrecer nuevas perspectivas en la investigación psicológica y sociológica.

Conclusión

La replicación de personalidad con IA es una frontera emocionante en la ciberseguridad. Este experimento ha mostrado tanto el potencial como los desafíos de esta tecnología. Es crucial que los profesionales y las empresas del sector consideren tanto las oportunidades como las preocupaciones éticas y de privacidad.

Es fundamental abordar estas cuestiones de manera proactiva para garantizar que la replicación de personalidad con IA se desarrolle de manera ética y responsable, maximizando sus beneficios potenciales mientras se mitigan los riesgos asociados.

Carlos Moya Gamboa
Cybersecurity Analyst

Vulnerabilidades

Vulnerabilidad crítica en dispositivos NAS D-Link

Fecha: 6 de noviembre de 2024
CVE: CVE-2024-10914

CVSS: 9.8

CRÍTICA

Descripción

La vulnerabilidad crítica CVE-2024-10914, que afecta a varios dispositivos NAS (D-Link), permitirían a un atacante realizar inyección de código.

Esta vulnerabilidad afecta a la función cgi_user_add del script account_mgr.cgi. La manipulación del argumento "name" de esta función es lo que permite realizar la inyección de código.

El ataque podría ser lanzado de manera remota y aunque la complejidad del ataque parece elevada, el *exploit* ha sido publicado y podría ser explotado.

Solución

A la hora de redacción de esta publicación el fabricante no ha publicado ningún parche de seguridad para corregir esta vulnerabilidad.

Se recomiendan realizar la siguiente acción para mitigar la vulnerabilidad mientras se espera a recibir un parche desde el fabricante:

- Restringir el acceso al NAS a nivel de red únicamente a direcciones IP de confianza, para así minimizar la posible exposición del servidor.

Productos afectados

La vulnerabilidad afecta a las siguientes versiones:

- DNS-320: versión 1.00
- DNS-320LW: versión 1.01.0914.2012
- DNS-325: versión 1.01 y 1.02
- DNS-340L: versión 1.08

Referencias

- incibe.com
- cvedetails.com
- netsecfish.notion.site

TLP:WHITE

Vulnerabilidades

Vulnerabilidad en Palo Alto Networks Expedition

Fecha: 8 de noviembre de 2024
CVE: CVE-2024-5910

CVSS: 9.3

CRÍTICA

Descripción

Se ha publicado información sobre una vulnerabilidad de severidad crítica en Palo Alto Networks Expedition. La vulnerabilidad, CVE-2024-5910, fue descubierta un mes antes, pero se ha continuado la investigación por parte del fabricante, descubriendo nuevos ataques asociados.

La vulnerabilidad se debe a un error en la autenticación presente en la herramienta, y mediante su explotación un atacante podría hacerse con el control de la cuenta de administrador. Posteriormente, el atacante podría realizar ataques de inyección de código con los permisos de administrador obtenidos previamente.

Solución

El fabricante recomienda encarecidamente actualizar el producto a la versión 1.2.92 o posterior.

Adicionalmente, recomiendan que los accesos por red a la herramienta se encuentren restringidos únicamente a los usuarios, equipos y redes autorizados.

Productos afectados

Esta vulnerabilidad afecta a las siguientes versiones:

- Palo Alto Networks Expedition: las versiones comprendidas entre la 1.2 y la 1.2.91.

Referencias

- bleepingcomputer.com
- security.paloaltonetworks.com

Parches de seguridad de noviembre de Android

Fecha: 4 de noviembre de 2024
CVE: CVE-2024-38408 y 44 más

Crítica

Descripción

Android ha publicado su actualización mensual de seguridad donde solucionan una vulnerabilidad de severidad crítica y múltiples de severidad alta. Las vulnerabilidades más importantes son:

- CVE-2024-38408: esta vulnerabilidad se debe a un problema de cifrado en componentes Qualcomm.
- CVE-2024-43093: vulnerabilidad de escalada de privilegios en el *framework* del sistema operativo que podría permitir a un atacante obtener acceso no autorizado a los directorios "Android/data", "Android/obb" y "Android/sandbox“, así como a sus subdirectorios .

Productos afectados

La actualización de seguridad de noviembre incluye parches para los siguientes recursos:

- Android Open Source Project (AOSP): versiones 12, 12L, 13, 14 y 15 (framework y system)
- Componentes de Kernel, Kernel LTS, Imagination Technologies, MediaTek y Qualcomm
- Actualizaciones del sistema Google Play.

Solución

Se recomienda actualizar los productos afectados a la versión publicada por el fabricante lo antes posible.

Referencias

- source.android.com
- incibe.es

TLP:WHITE

Actualizaciones de Cisco para vulnerabilidad critica URWB

Fecha: 6 de noviembre de 2024
CVE: CVE-2024-20418

Crítica

Descripción

Cisco ha publicado un parche para mitigar la vulnerabilidad de severidad crítica CVE-2024-20418. Esta vulnerabilidad afecta al punto de acceso "Ultra Reliable Wireless Backhaul" (URWB).

Esta vulnerabilidad es debida a un pobre manejo de *inputs* en la interfaz web de gestión de los equipos vulnerables. Un atacante podría explotar la vulnerabilidad mediante el envío de paquetes HTTP específicamente diseñados para la explotación de esta vulnerabilidad.

Una explotación satisfactoria de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario en el equipo con máximos privilegios.

Productos afectados

La vulnerabilidad parcheada afecta a los siguientes productos (con sus versiones correspondientes) y que utilicen URWB:

- Catalyst IW9165D Heavy Duty Access Points
- Catalyst IW9165E Rugged Access Points and Wireless Clients
- Catalyst IW9167E Heavy Duty Access Points

Solución

Se recomienda encarecidamente que todas las instalaciones que se ejecuten en una versión afectada se actualicen lo antes posible según el boletín de seguridad de Cisco.

Referencias

- incibe.es
- sec.cloudapps.cisco.com

TLP:WHITE

Eventos

I Foro Madrid CyberStartup
4 de diciembre

Desde el Ayuntamiento de Madrid, en su centro de innovación Aravaca Innovation Lab (AIL), se va a celebrar el I Foro Madrid CyberStartup, un evento destinado a las Startups de Madrid Innovation que permitirá a pymes y emprendedores dedicados a la ciberseguridad conocer las últimas tendencias y desafíos del sector. En este espacio dedicado al aprendizaje y el *networking* se tratarán temas como el marketing, los Modelos de Lenguaje Extensos (LLM) o el desarrollo de la Tecnología Blockchain, brindándose así una oportunidad para compartir la visión de cada uno sobre el futuro de la ciberseguridad.

Enlace

II Congreso Internacional de Ciberseguridad y Fraude Digital
4 de diciembre

World Compliance Association organiza este congreso donde se reunirán diferentes expertos en ciberseguridad, peritos judiciales, responsables de ciberseguridad empresarial (CISO, CTO), funcionarios de la administración pública y representantes policiales y de gestión, entre otros, para debatir, realizar talleres prácticos sobre problemas y soluciones reales, compartir e intercambiar conocimientos y buenas prácticas y desarrollar estrategias efectivas para enfrentar las posibles amenazas y fraudes digitales que puedan darse en los ámbitos públicos y privados como la protección ciudadana, empresarial, de las Administraciones Públicas y sobre la Seguridad Nacional y la Era de la inteligencia.

Enlace

CyberThreat 2024
9-10 de diciembre

En esta conferencia anual de dos días, organizada por el Centro Nacional de Ciberseguridad de Reino Unido (NCSC) y el instituto SANS, se contemplan tanto disciplinas ofensivas como defensivas, incidiendo sobre todo en los aspectos más técnicos, mediante diferentes ponencias y actividades como CTF, resolución de problemas en equipo y desafíos «Hackathon» para ampliar los conocimientos y capacidades de los asistentes para defenderse de las ciber amenazas.
Asimismo, se fomenta el intercambio de experiencias, conocimientos, herramientas y técnicas para impulsar el desarrollo y crecimiento del talento y así afrontar el problema que supone la falta de habilidades en ciberseguridad.

Enlace

Black Hat Europe 2024
9-12 de diciembre

Black Hat Europe 2024 cuenta con un programa de cuatro días de formaciones prácticas y cursos para todos los niveles, siendo los días 11 y 12 los que recogen la conferencia principal con sesiones informativas sobre las últimas investigaciones, desarrollos y tendencias en ciberseguridad.
El evento también ofrece demostraciones de herramientas de código abierto en Arsenal, programas exclusivos para CISOs y otros profesionales ejecutivos, así como “Business Halls” y diferentes espacios de actividades para conocerse, descubrir nuevos recursos y competir en dinámicas prácticas y creativas.

Enlace

Recursos

➢ GoIssue

GoIssue se trata de una herramienta de phishing que ha surgido y presenta un nuevo peligro para los usuarios de GitHub. Esta herramienta no solo proporciona una serie de plantillas a utilizar para el diseño de phishing, sino que además extrae correos electrónicos de los repositorios de GitHub, obteniendo posibles víctimas de ataque de phishing. Junto con las funcionalidades de proxy y administración de tokens, esta herramienta presenta todas las características necesarias para diseñar una campaña de phishing hacia todos los usuarios que tengan su correo electrónico expuesto en los repositorios de GitHub.

Enlace

➢ BitLocker Decryptor – ShrinkLocker Ransomware

La empresa de ciberseguridad Bitdefender ha lanzado una nueva herramienta para desencriptar datos comprometidos por el ransomware ShrinkLocker. La ejecución de este ataque causaba la encriptación del dispositivo a través de BitLocker, utilizando contraseñas pseudoaleatorias que impedían su recuperación a través de fuerza bruta y eran a su vez enviadas a un servidor controlado por el atacante. Ante la amenaza que ha supuesto este ransomware, Bitdefender ha lanzado esta nueva herramienta gratuita de descifrado que permite recuperar los datos afectados por ShrinkLocker.

Enlace

➢ Azure Storage Explorer

Esta herramienta de Azure está siendo un nuevo método utilizado por atacantes a la hora de la exfiltración de datos a grandes escalas. Esta aplicación de Microsoft presenta una interfaz gráfica que permite administrar el almacenamiento de Azure, trabajando con diferentes componentes como: recursos compartidos, blobs o discos administrados. Esta herramienta está siendo utilizada principalmente para copiar y transmitir grandes cantidades de archivos desde un dispositivo comprometido a un contenedor controlado por el atacante. Además, dado que se trata de un programa legítimo de Microsoft, existe una baja posibilidad de que los controles de red bloqueen la conexión a esta herramienta, siendo uno de los motivos principales por los cuales está siendo cada vez más utilizada por atacantes.

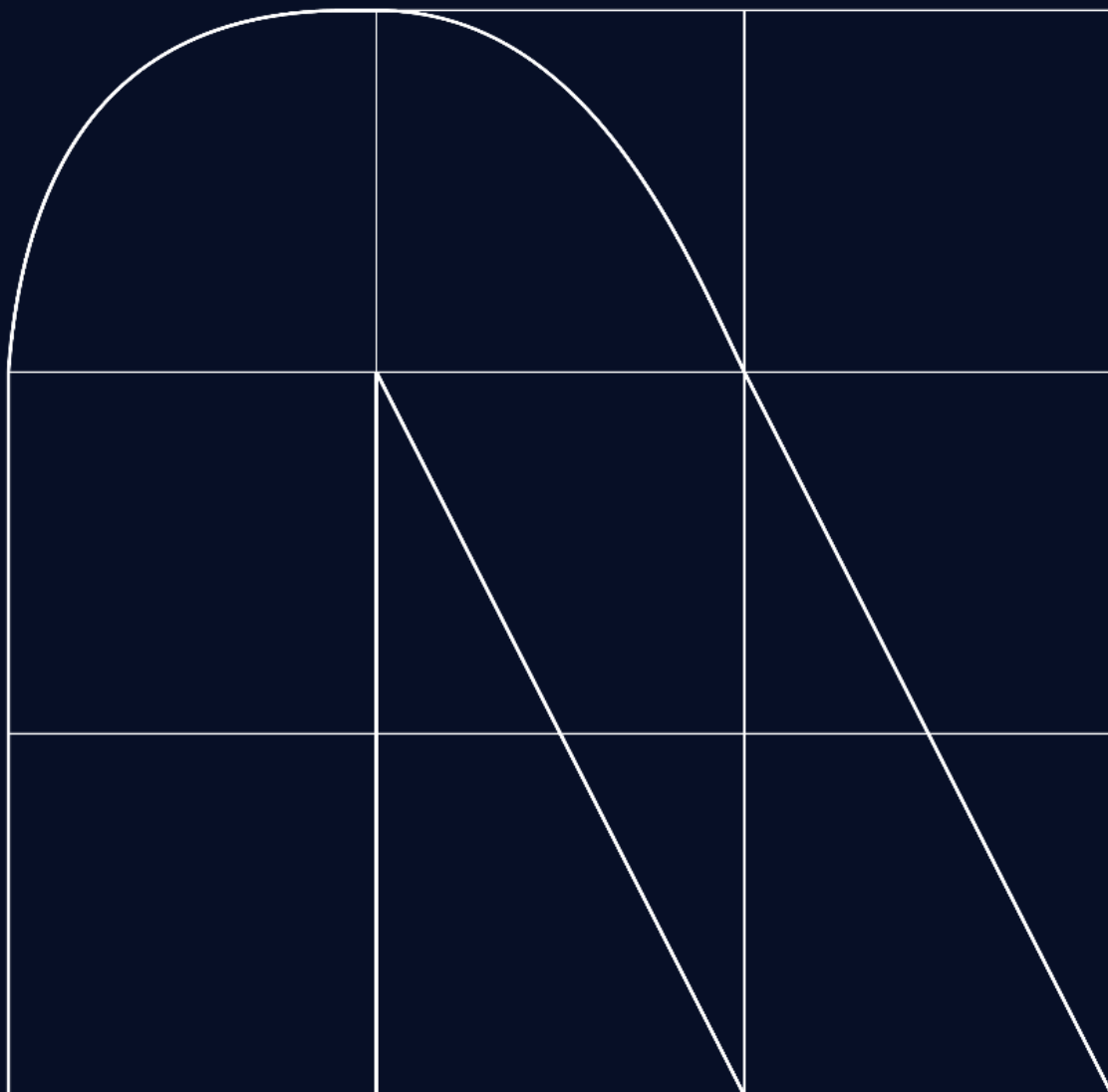
Enlace

➢ GolgdenJackal

GolgdenJackal es un grupo Advanced Persisten Threat (APT) que ha logrado, entre otras cosas, comprometer sistemas gubernamentales aislados en Europa. Este ataque se logró gracias a la explotación de un malware especialmente desarrollado, donde se aplican diversas herramientas comunes (USB) así como personalizadas. Existe múltiples estudios sobre este grupo y sus ataques, entre ellos este artículo que ofrece un kit de herramientas de las metodologías y procedimientos implementados por este equipo a la hora de comprometer sistemas aislados.

Enlace

Suscríbete a RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com