MINDCORE

SEGURIDAD TELECOM

TEST DE SEGURIDAD DE SEÑALIZACIÓN

El Riesgo

Los operadores de redes móviles son el blanco de ataques de señalización sofisticados que acarrean un impacto devastador para los servicios del suscriptor y la reputación del operador.

Los protocolos y tecnologías "legacy" de telecomunicaciones fueron concebidas sin considerar la ciberseguridad, a menudo permaneciendo desprotegidas y sin la visibilidad adecuada, convirtiéndose en un objetivo preferido de actores de amenaza y cibercriminales. A su vez, otros protocolos basados en IP a menudo carecen de autenticación, cifrado robusto y otros atributos de seguridad, dejándolos expuestos a múltiples amenazas tanto externas como internas.

Nuestra Solución

Mindcore lleva a cabo una revisión de seguridad exhaustiva de los enlaces de interconexión, a través de una serie de pruebas que simulan ataques sofisticados de hackers enfocados en tecnologías de telecomunicaciones.

Estas pruebas permiten identificar vulnerabilidades, configuraciones incorrectas y áreas de mejora, tomando como base las pautas de las guías GSMA FS.11, FS.19 y FS.20 sobre seguridad y monitoreo de los protocolos de señalización SS7, Diameter y GTP. Entre los principales objetivos de las pruebas de seguridad de señalización se encuentran los siguientes:

- Probar la seguridad y resiliencia de la red ante ataques sofisticados de señalización.
- Protección contra múltiples amenazas a los servicios, tales como fraude, interceptación y desvío de llamadas, captura de mensajes SMS y fuga de datos de ubicación.
- Validar la efectividad de las contramedidas implantadas en la red, tales como un firewall de señalización.
- Validar cumplimiento y adoptar las pautas de las guías GSMA FS.11, FS.19 y FS.20.

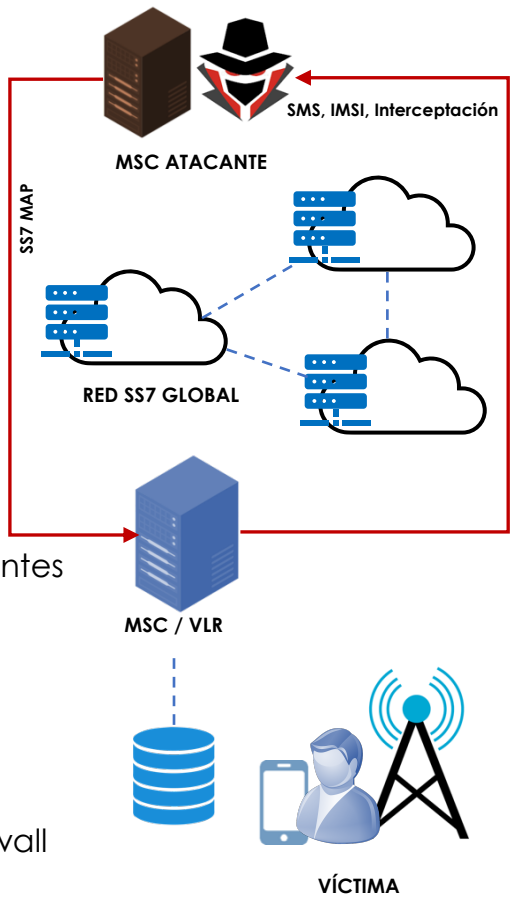
El Enfoque de Mindcore

La metodología de Mindcore para evaluar la seguridad en redes móviles se basa en una comprensión profunda de los servicios de roaming, los diversos mensajes de señalización parte de las especificaciones 3GPP, cuáles se intercambian regularmente entre determinados nodos de red, así como los distintos parámetros de estos mensajes.

Evaluación de vulnerabilidades SS7

Mindcore detecta vulnerabilidades a través de la conexión SS7 de cada nodo del operador de red móvil de una manera segura y sin afectar el servicio. Esta prueba permite obtener una visión realista de las vulnerabilidades que pueden ser explotadas por un adversario, como por ejemplo una agencia de gobierno extranjero o un atacante determinado.

Las pruebas de seguridad SS7 realizadas por Mindcore cubren más de 35 diferentes tipos de vulnerabilidades usando cientos de combinaciones distintas de mensajes de señalización. Esto incluye las vulnerabilidades categoría 1, 2 y 3 de la guía FS.11 del GSMA Fraud and Security Group (FASG), así como otros escenarios de ataque no cubiertos por FS.11. Las vulnerabilidades probadas incluyen:



Vulnerabilidades Categoría 1 de GSMA

- Fuga de IMSI
- Fuga de información de ubicación

Vulnerabilidades Categoría 2 de GSMA

- Interceptación y desvío de llamadas
- Fraude de toll y facturación
- Fraude de USSD

Vulnerabilidades Categoría 3 de GSMA

- Interceptación y captura de mensajes SMS entrantes
- Fraude SMS de mayorista
- Captura de IMSI 3G

Otras vulnerabilidades no cubiertas por GSMA

- Falsificación ("spoofing") de SCCP
- Técnicas avanzadas de evasión (bypass) de firewall

MINDCORE

Acerca de Mindcore

Nuestra empresa cuenta con 40 años de experiencia acumulada en el área de la ciberseguridad, aplicada a diversos sectores y ambientes, tales como telecomunicaciones, banca, tecnología, gobierno, manufactura, entre otros.

Durante este período hemos trabajado con las empresas más avanzadas tecnológicamente en la evaluación, diseño e integración de soluciones de ciberseguridad, con un enfoque en la gestión de vulnerabilidades, amenazas y riesgos de la tecnología de información.

Nuestras áreas de especialización en seguridad de señalización y telecomunicaciones incluyen:

- Auditoría y remediación de vulnerabilidades de señalización de telecomunicaciones
- Selección, implementación y auditoría de firewalls de señalización de telecomunicaciones
- Diseño de arquitectura segura y auditoría de red móvil
- Selección, implantación, auditoría y solución de problemas complejos relacionados con la señalización en la mayoría de los nodos y protocolos en una red móvil, incluidos HLR, AuC, MSC, VLR, IN, SGSN, GGSN, USSD Gw, SMSC, OTA, tarjetas SIM, SBC, facturación y los siguientes protocolos: SS7 MAP, CAP, TCAP, Diameter, GTP
- Amplia experiencia con todos los aspectos de la tecnología multi-IMSI, incluyendo el perfil y seguridad de tarjetas SIM, claves de suscriptor AuC y algoritmos de autenticación GSM, perfiles y claves OTA, plataformas OTA y configuraciones de seguridad

Contamos con una vasta experiencia en pruebas de seguridad de señalización, habiendo ejecutado docenas de pruebas para grandes operadores en más de 40 países, incluyendo:

• Afghanistan • Algeria • Bahrain • Brasil • Bulgaria • Cambodia • Canada • Czechia • Grecia • Guam • Guatemala	• Hong Kong • Indonesia • Iran • Iraq • Jamaica • Japón • Jordania • Kuwait • Malasia • Maldives • Mali	• Mexico • Moldova • Montenegro • Marruecos • Myanmar • Oman • Palestina • Panamá • Perú • Polonia • Qatar	• Arabia Saudita • Senegal • Sri Lanka • Taiwan • Tunisia • Emiratos Árabes Unidos • Estados Unidos de América • Vietnam

El personal de nuestra empresa se encuentra entre el más capacitado de la región. El mismo cuenta con niveles de conocimiento y habilidades superiores, avalados por las certificaciones de mayor prestigio en materia de ciberseguridad, entre las cuales podemos mencionar las siguientes:

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CISA (Certified Information Systems Auditor)
- OSCP (Offensive Security Certified Professional)
- CEH (Certified Ethical Hacker)
- CCSK (Certificate of Cloud Security Knowledge)