



Aaron Telles Marin

Arquitecto de Preventa Regional de Ciberseguridad

Máster en Ciberseguridad con más de 20 años de experiencia en TI, Telecomunicaciones, Administración de Proyectos y Ciberseguridad.

Actualmente, se desempeña como Arquitecto de Preventa Regional de Ciberseguridad (Security Operations) para GBM, liderando la estrategia de seguridad cibernética en la región y ofreciendo soluciones avanzadas para proteger la infraestructura crítica de diversas organizaciones.



Defensa Activa.

Estrategias avanzadas para detectar y detener ataques con QRadar

Msc. Aarón Telles Marín.
Arquitecto regional de Prevención de
Ciberseguridad.
GBM Corporation



Panorama de las amenazas

Nueva dinámica

Una **nueva
dinámica** para
el panorama
de TI

Hasta **7x**

Mobilidad

5-7 veces el crecimiento
del tráfico móvil
empresarial hasta 2023¹

93%

Cloud

93% de las organizaciones
utilizará varias nubes para
2023

28B

IoT

28.5B dispositivos de red y
conexiones existirán para
el 2023

Hasta **70%**

Seguridad

50-70% del malware para
web será encriptado

La ocasión hace **al delincuente**

Oportunidad delictiva



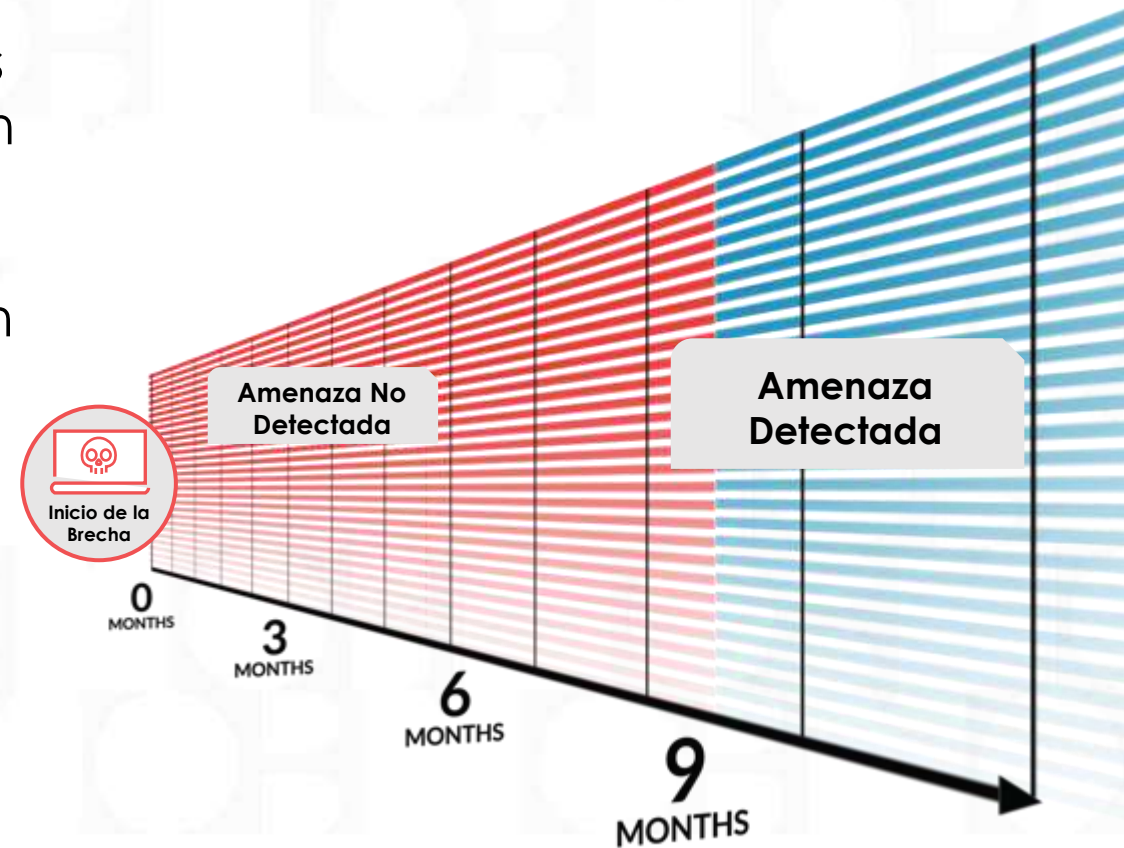
Por razones de salud y seguridad, haremos la transición al ciberdelito.

- El volumen de ataques ha crecido exponencialmente.
- Globalmente el fraude digital cuesta anualmente más de **\$4.2 trillones de dólares**.
- **97%** de los usuarios a nivel mundial no pueden identificar ataques de phishing.
- **1 de cada 3** Bancos reportaron haber sido víctimas de ataques
- Los defraudadores están evolucionando y explotando los canales digitales y acceso remoto.
- Con la pandemia se disparó el fraude electrónico por la menor presencia física en las oficinas, sucursales bancarias y comercios.
- El **48%** de las organizaciones tienen visibilidad limitada o nula cuando se trata de identificar el impacto de un ataque de phishing.

Impacto del modelo actual

Costo promedio de \$ 4.6 millones por brecha de seguridad

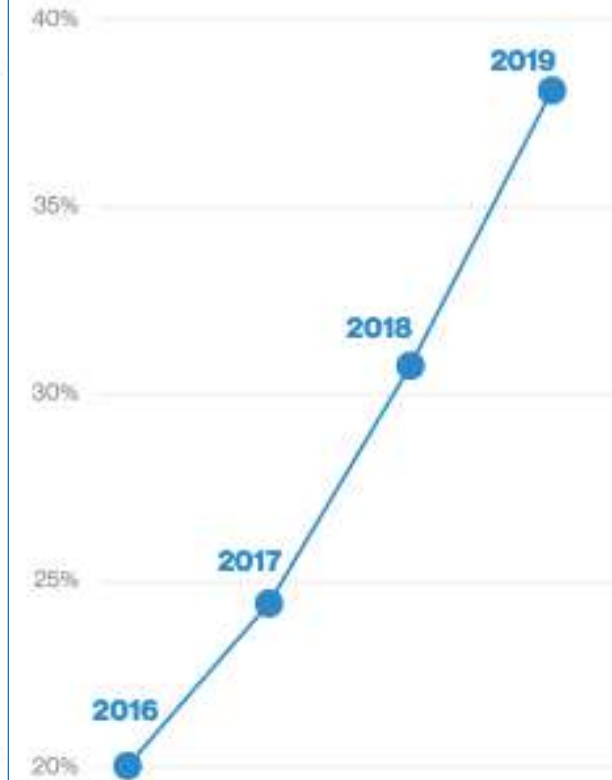
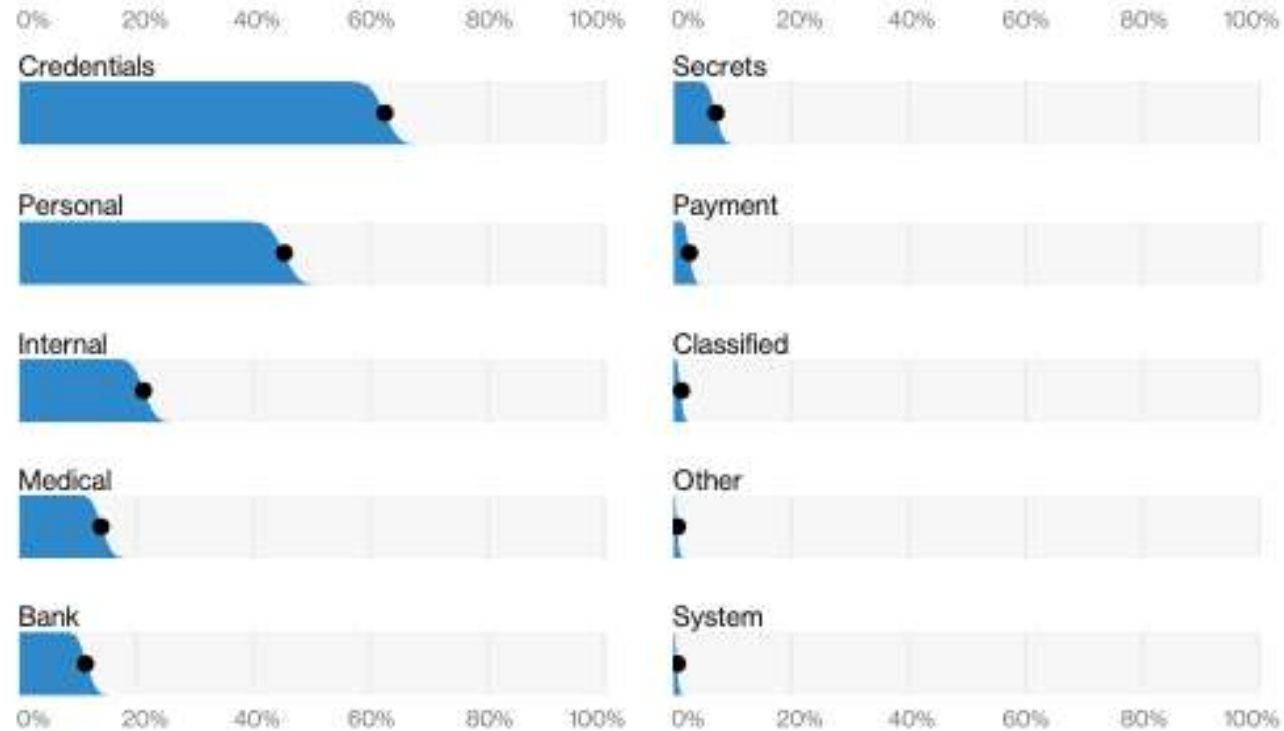
- El **97% de las organizaciones** que fueron víctimas de una brecha de seguridad; **3 de cada 4** tenían comunicaciones activas de **comando y control**.
- **280 días** promedio de días antes de la detección de la brecha.
- **32 días** para responder a una brecha de seguridad.
- El **53%** de las empresas se enteró de que fueron víctimas de una brecha de seguridad por una entidad externa.



Datos comprometidos

Datos comprometidos

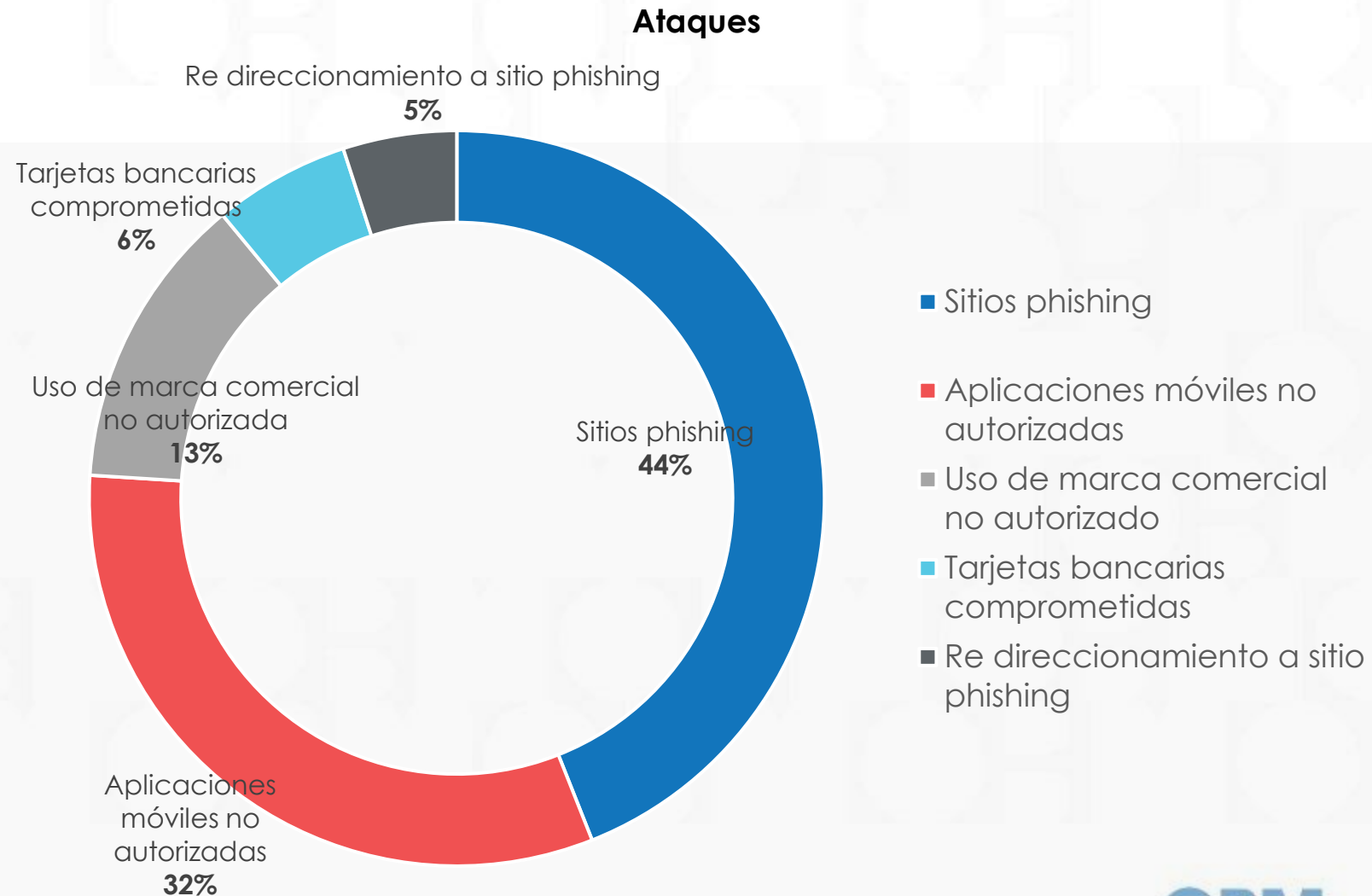
Principales variedades de datos comprometidas en infracciones de phishing (n=619).



Cuántas campañas de test de phishing son reportadas al menos una vez.

Ataques más vistos

Centroamérica y Caribe



Evolución de la Seguridad

Transforme su capacidad de detectar, responder y contener ciberataques avanzados.

Donde muchas compañías están hoy.

Cierre de la brecha

Donde muchas compañías quieren estar.

Brecha



Seguridad por Diseño

Continuo Incremento
Postura de Seguridad

Remediaciones

Actualización de
Políticas



Básico

Contraseñas / AD

Gestión de Parches

Respaldos



Perímetro

Firewalls

SPAM / Filtrado Web

WAF / Proxy



Defensa en Profundidad

Endpoint (AV, AEP)

DLP / Inspección SSL

Anti-DDoS / IPS / CASB



Detección y Respuesta

Log Agregación &
Correlation

Human / Threat
Intelligence

Incident Detection &
Response



Qradar SIEM.
Velocidad, escala y precision.

IBM Security

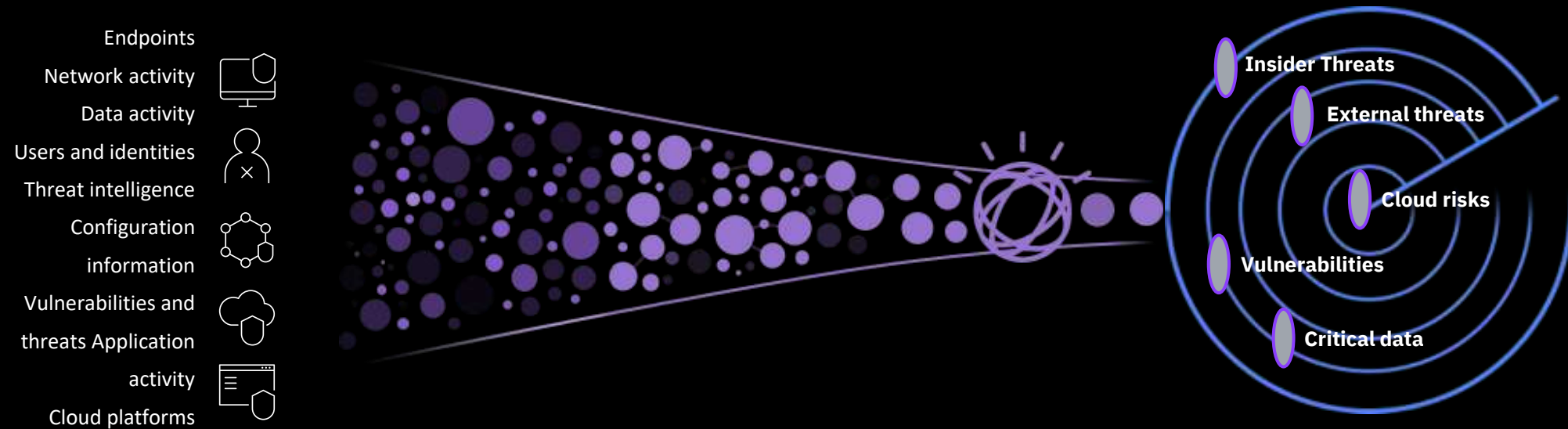


 NO MORE RANSOM





Visibilidad Detección Investigación Respuesta





Qradar SIEM.
Veamos el Qradar.

IBM Security



 NO MORE RANSOM



Muchas gracias



www.gbm.net | mercadeo@gbm.net | [f](#) [t](#) GBM Corp

Contacte a GBM en su país y marque la extensión 3840 (Contact Center)

GT (502)2424-2222 | ES (503)2505-9600 | HN (504)2232-3219/09 | NI (505)2255-6630
CR (506)2284-3999 | PA (507)300-4800 | RD (809)566-5161 | MI +1(305)597-3998