Symantec

# ISTR20

## INTERNET SECURITY THREAT REPORT

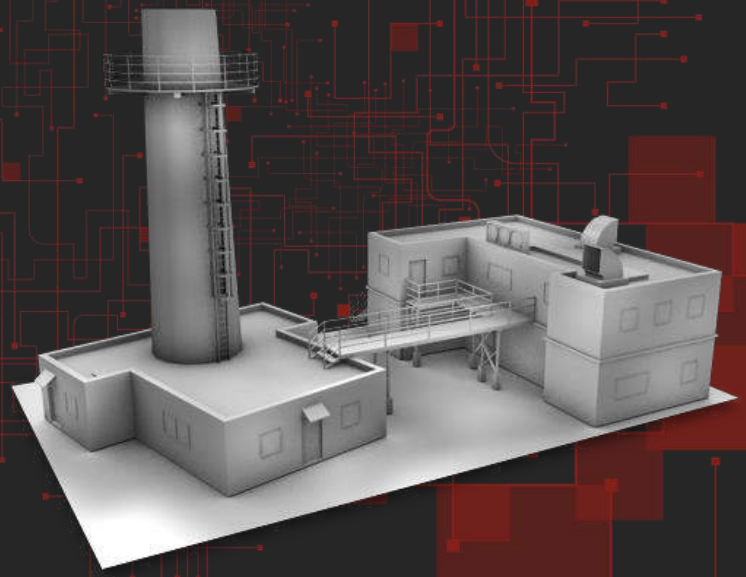
PRINCIPALES HALLAZGOS

AGOSTO, 2015

# Los cibercriminales evaden las defensas de maneras en que las compañías carecen de información para poder anticiparse

# Enemigos Actuales: Ejemplo - Dragonfly

- En 2014, Symantec reportó sobre la banda Dragonfly, cuyo objetivo era atacar el sector energético en Europa y los EEUU
- Utilizaron diversos métodos de ataque



# Métodos de Ataque

## Spear Phishing

Enviar un e-mail a una persona de interés

## Ataque Watering Hole

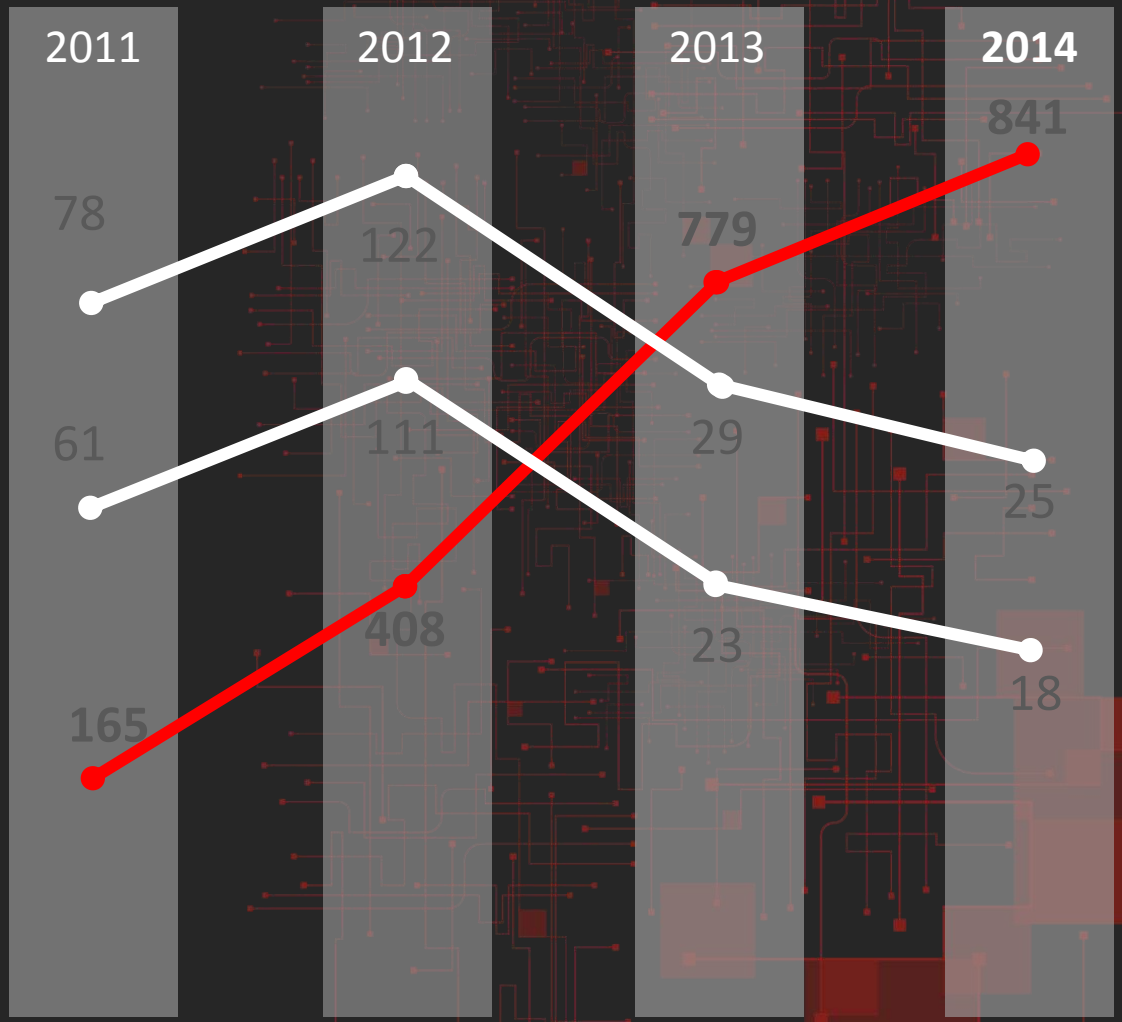
Infectar un sitio web, mentir y esperar

## Actualización Troyanizada

Infectar descargas de actualizaciones de software

# Campañas de Ataques Dirigidos

- **Incremento de un 8% en campañas de spear-phishing durante 2014**



# Índice de Amenazas sobre Ataques de Spear-Phishing, de Acuerdo con el Tamaño de la Organización


**40%** de incremento

**30%** de incremento

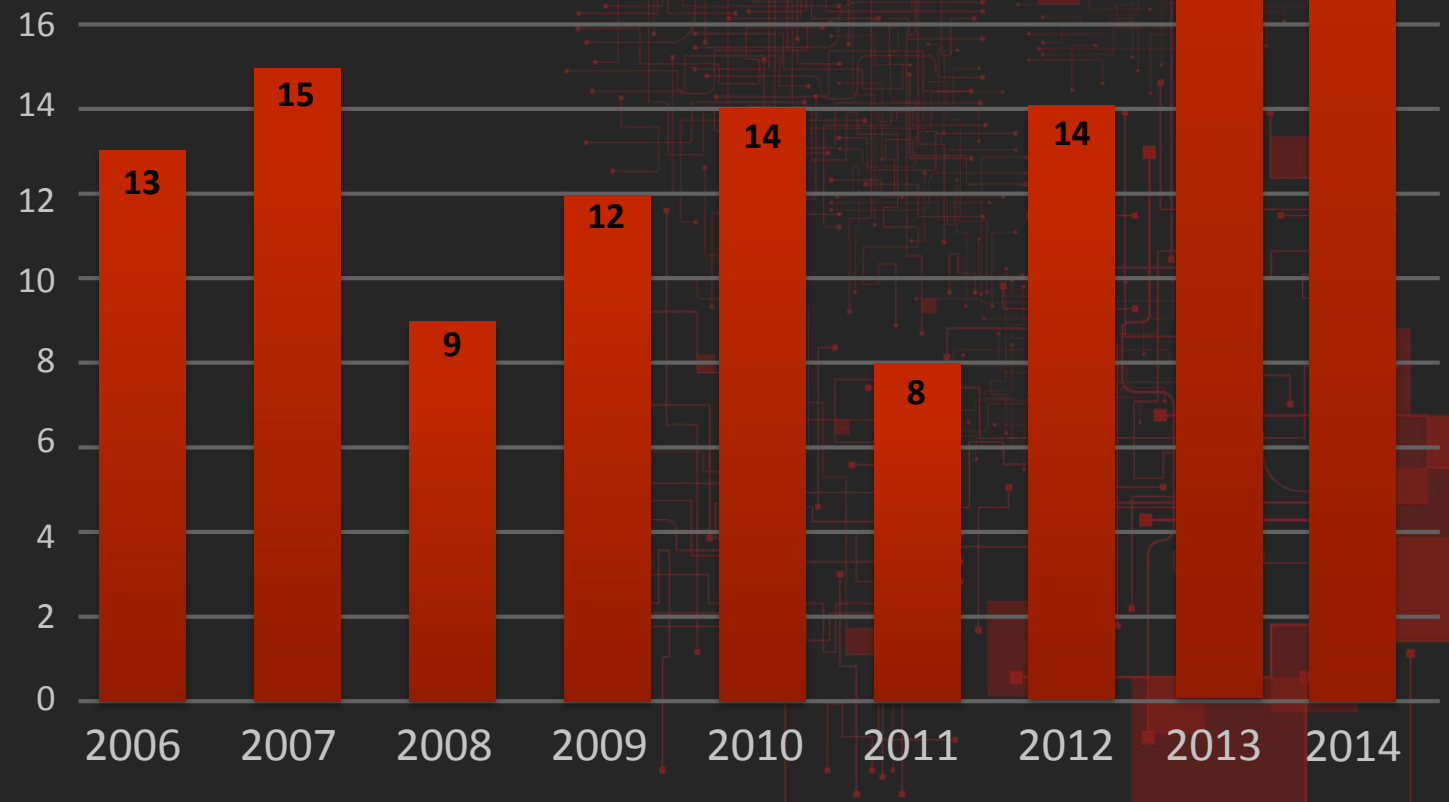
**26%** de incremento

- **5** de **6** grandes empresas son objetivos (**83%**)

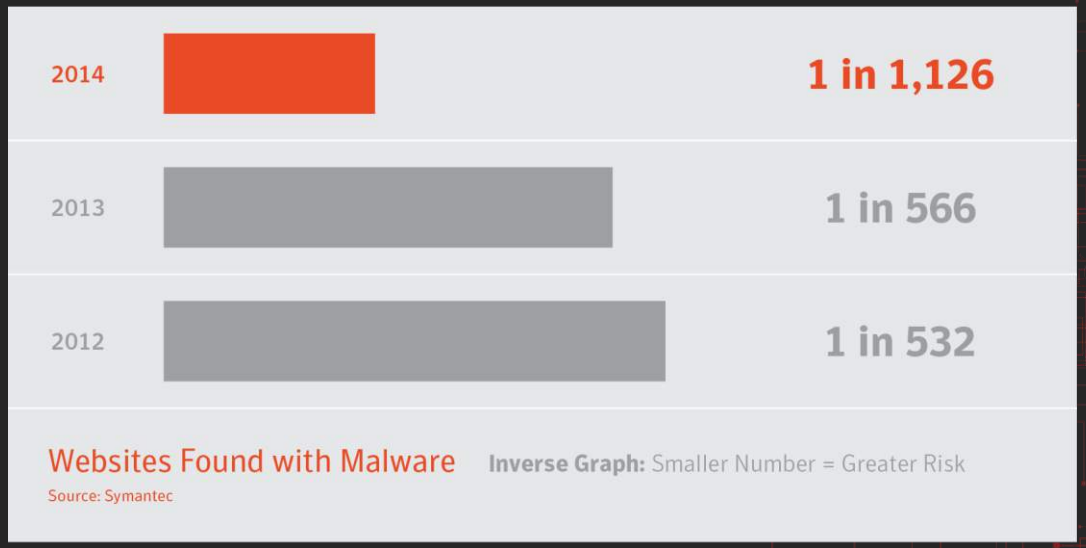
# Los agresores se mueven más rápido, las defensas no

# Vulnerabilidades día-cero

- Vulnerabilidades día-cero en su punto más alto
- El valor de la explotación día-cero impulsa un nuevo nivel de descubrimientos día-cero

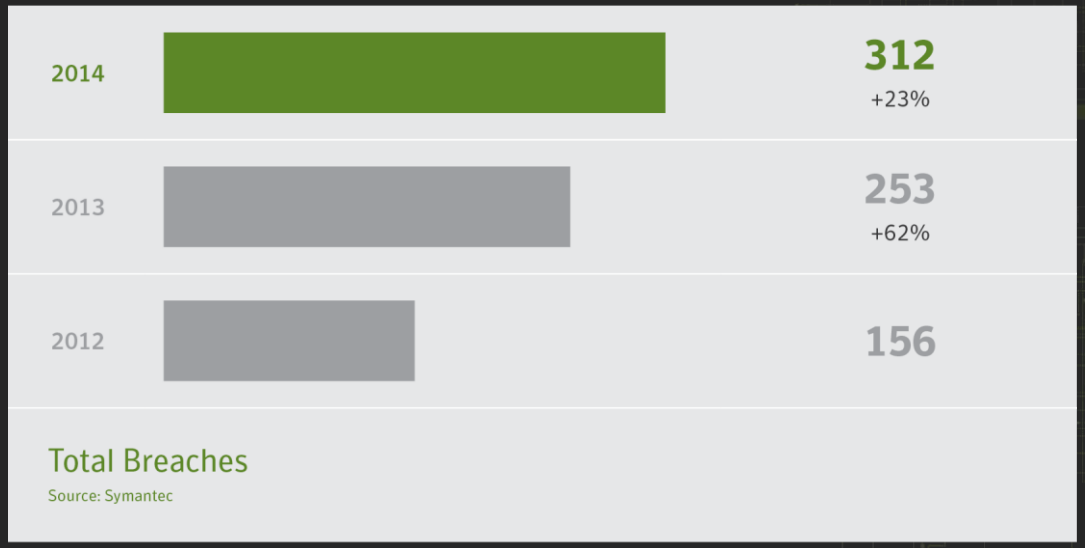


# Sitios web legítimos en los que se encontró malware




- Una caída dramática en el número de sitios web legítimos que albergan malware
- Impulsada por el cambio de tácticas de los atacantes, **no** por una mejor seguridad web.

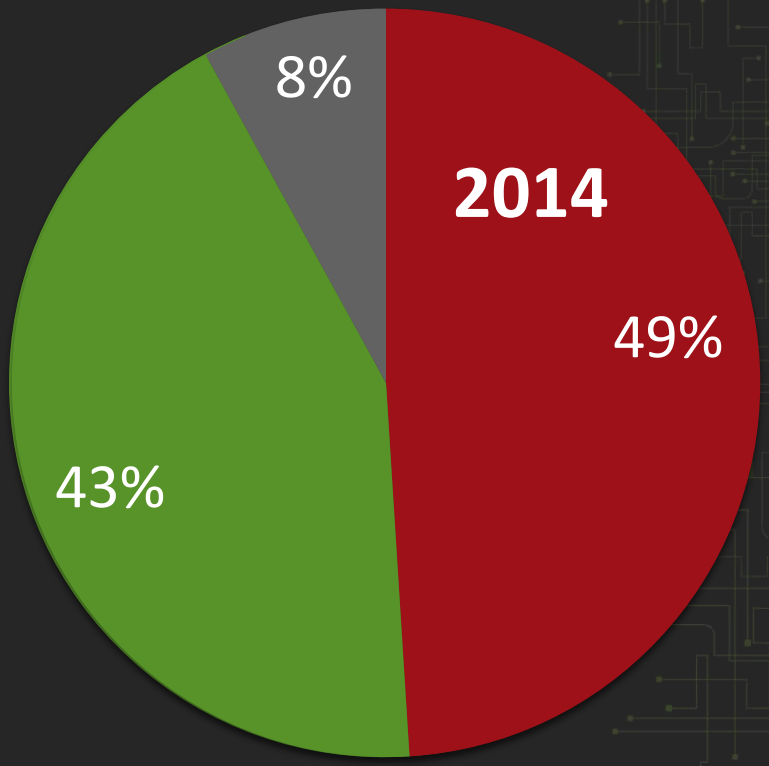
# Fugas totales




- **23%** de incremento en 2014

- **Menos "mega fugas" en 2014** 4 incidentes provocaron la exposición de más de 10 millones de identidades. (contra 8 en 2013)
- **1 de cada 5** compañías afectadas no reportaron la información sobre los datos expuestos. (1 de cada 6 en 2013)

# Principales causas de las fugas de datos




- Atacantes
- Expuestas accidentalmente/ robos o pérdida de dispositivos
- Robo interno

# 10 sectores con más fugas (número de incidentes)

| Rank | Sector | Number of Incidents | Percentage of Incidents (100%) |
|---|---|---|---|
| 1 | Healthcare | 116 | 37% |
| 2 | Retail | 34 | 11% |
| 3 | Education | 31 | 10% |
| 4 | Gov. & Public Sector | 26 | 8% |
| 5 | Financial | 19 | 6% |
| 6 | Computer Software | 13 | 4% |
| 7 | Hospitality | 12 | 4% |
| 8 | Insurance | 11 | 4% |
| 9 | Transportation | 9 | 3% |
| 10 | Arts and Media | 6 | 2% |

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

# 10 sectores con más fugas (identidades expuestas)

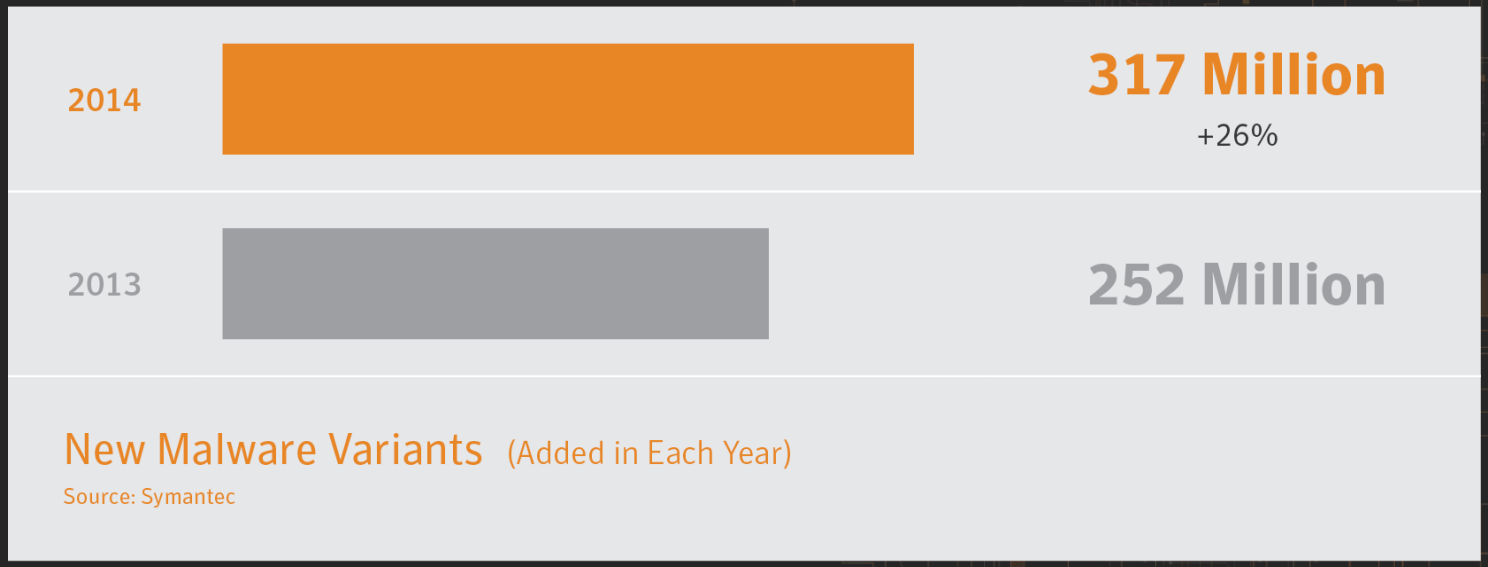
| Rank | Sector | Number of Identities Exposed | Percentage of Identities Exposed (100%) |
|---|---|---|---|
| 1 | Retail | 205,446,276 | 59% |
| 2 | Financial | 79,465,597 | 23% |
| 3 | Computer Software | 35,068,405 | 10% |
| 4 | Healthcare | 7,230,517 | 2% |
| 5 | Gov. & Public Sector | 7,127,263 | 2% |
| 6 | Social Networking | 4,600,000 | 1% |
| 7 | Telecom | 2,124,021 | .6% |
| 8 | Hospitality | 1,818,600 | .5% |
| 9 | Education | 1,359,190 | .4% |
| 10 | Arts and Media | 1,082,690 | .3% |

Top 10 Sectors Breached by Number of Identities Exposed

Source: Symantec

# El malware utilizado en ataques masivos se incrementa y adapta

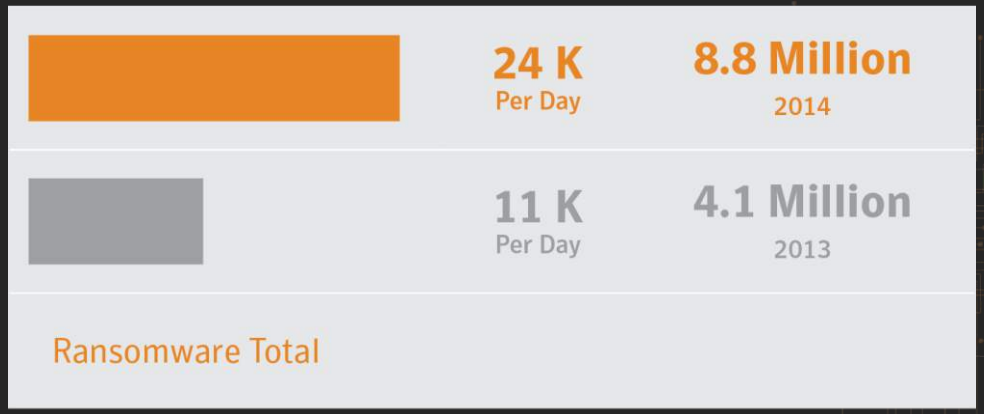
# Nuevas variantes de malware




- Casi 1 millón de nuevas amenazas creadas **diariamente** durante 2014

# La extorsión digital al alza: 45 veces más personas tuvieron sus dispositivos secuestrados en 2014

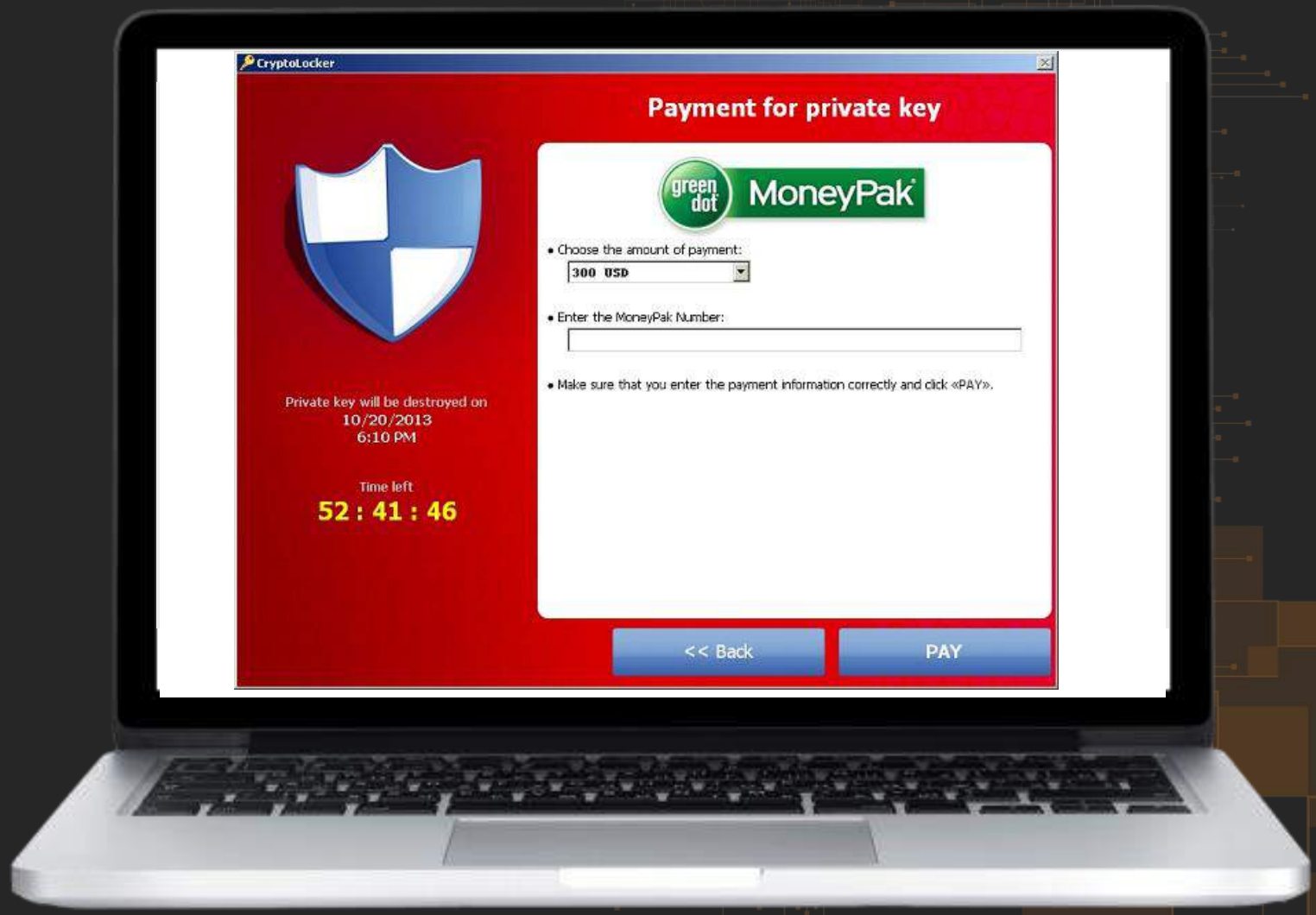
# Total de ransomware




- **113% de incremento** en 2014
- El ransomware continua siendo una amenaza que crece en contra de negocios y consumidores

# Evolución del ransomware 2013

# Evolución del ransomware 2014 – Crypto ransomware



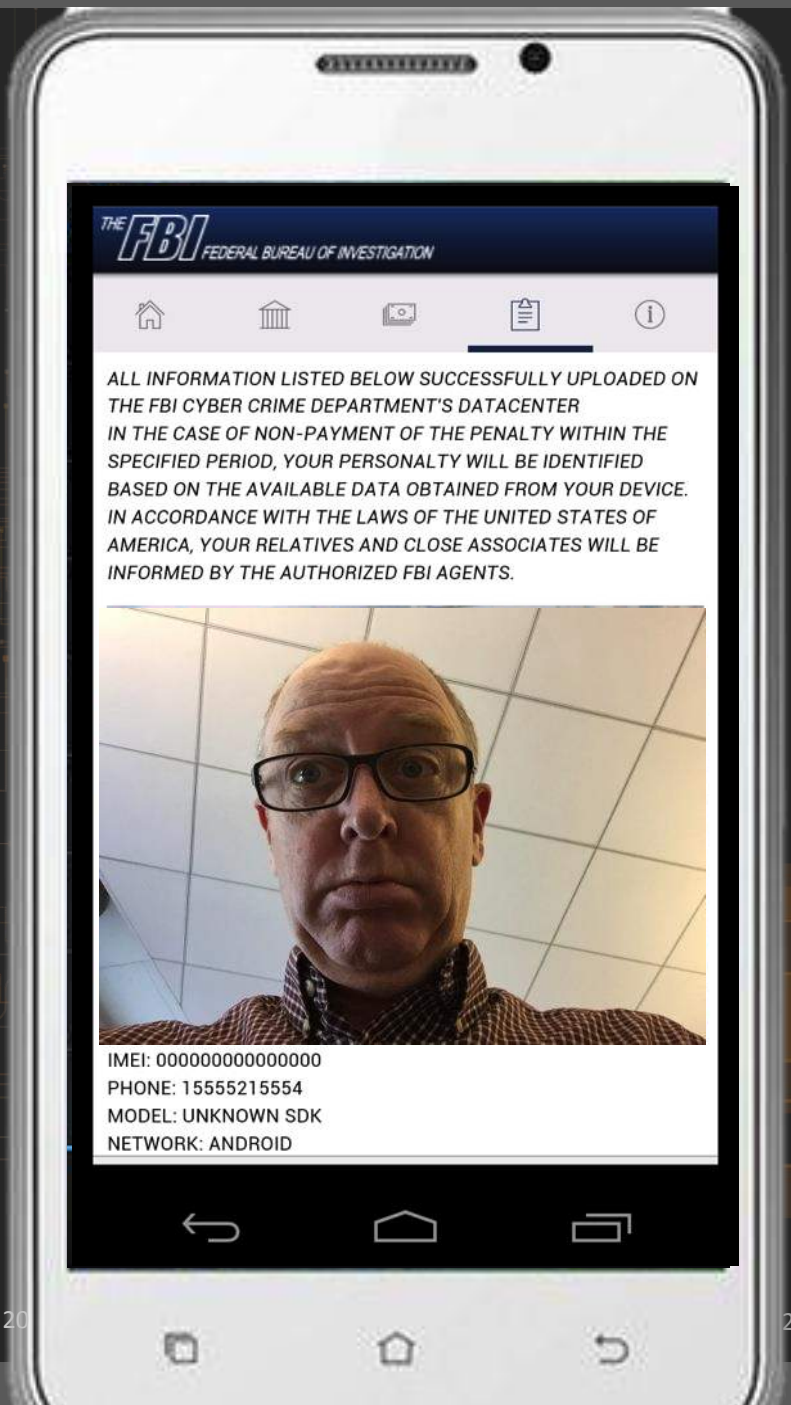
# Evolución del ransomware hacia el futuro

- El crypto-Ransomware continúa enfocándose en:
  - Archivos Office y PDF
  - Archivos y fotos personales
- El Crypto-Ransomware continua enfocándose en:
  - Drives mapeados
  - Almacenamiento adjunto
  - Almacenamiento en la nube (como drive mapeado)
- Pero encuentra nuevos objetivos
  - En 2014, Synolocker atacó drives NAS
  - En 2014, apareció el primer crypto-ransomware para teléfonos inteligentes

# Evolución del ransomware

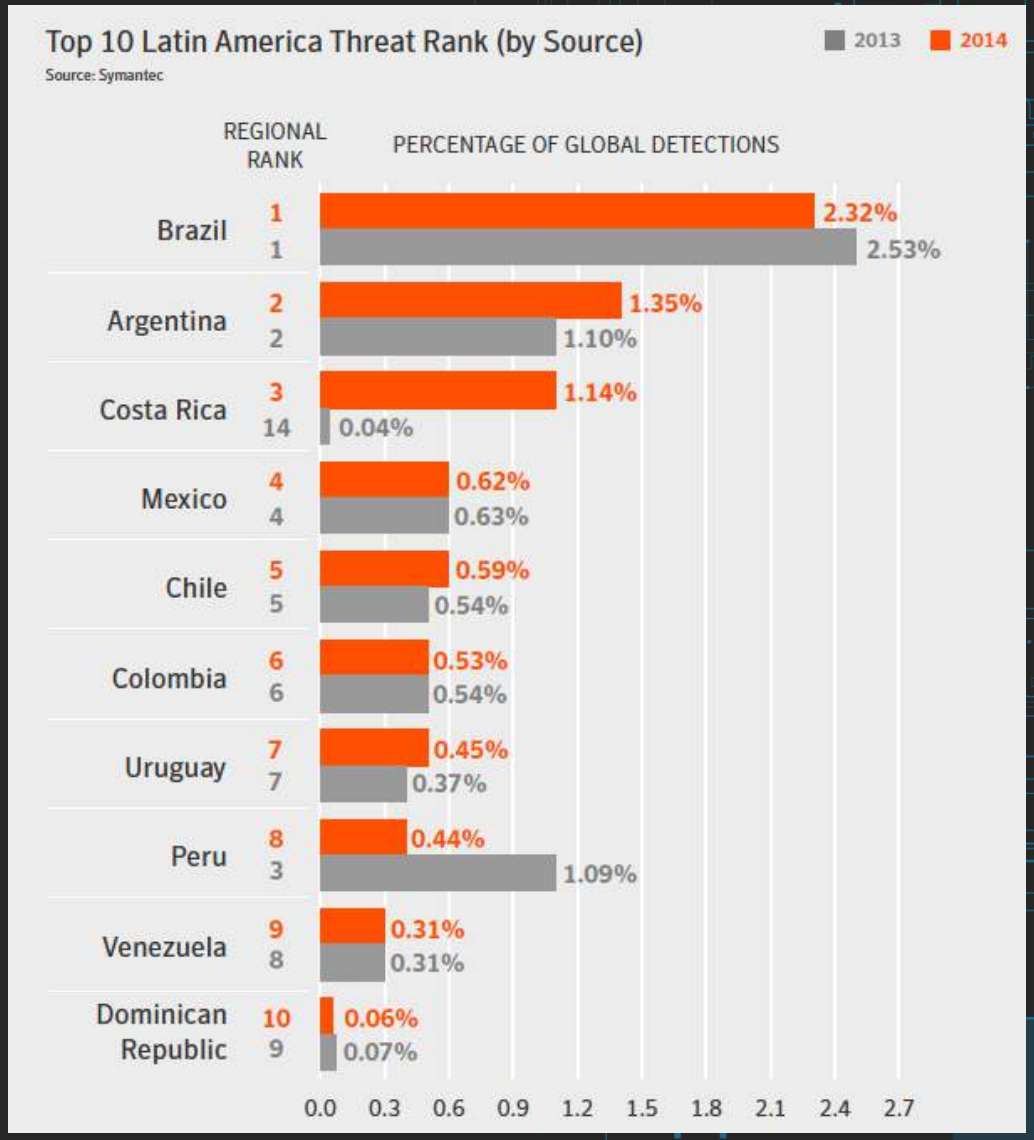
## Android.Simplocker Móvil

- Simplocker: primer crypto-ransomware para Android
- También son comunes los temas relacionados con agencias de la aplicación de leyes
- La cámara del dispositivo también es secuestrada



# Algunos datos de Colombia

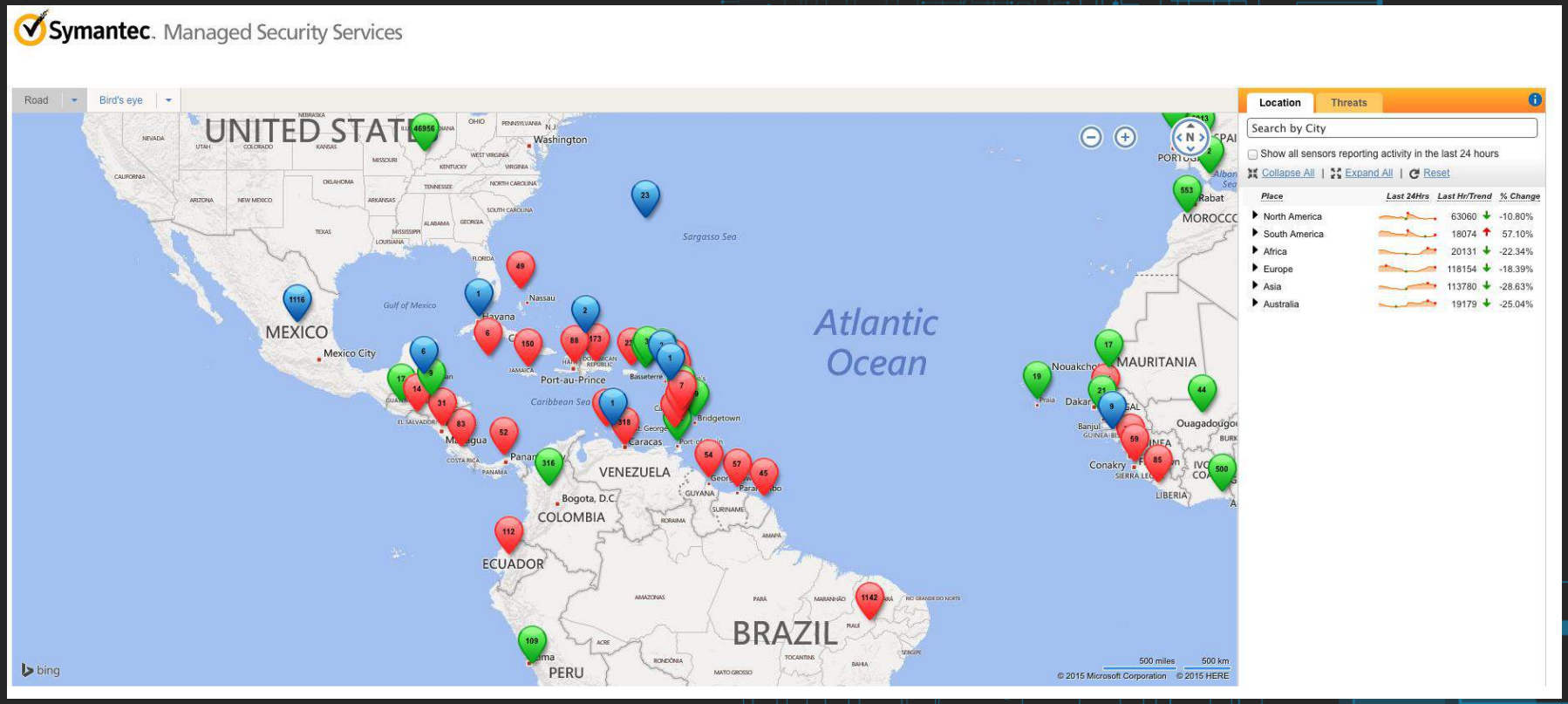
# Ranking Colombia - Global



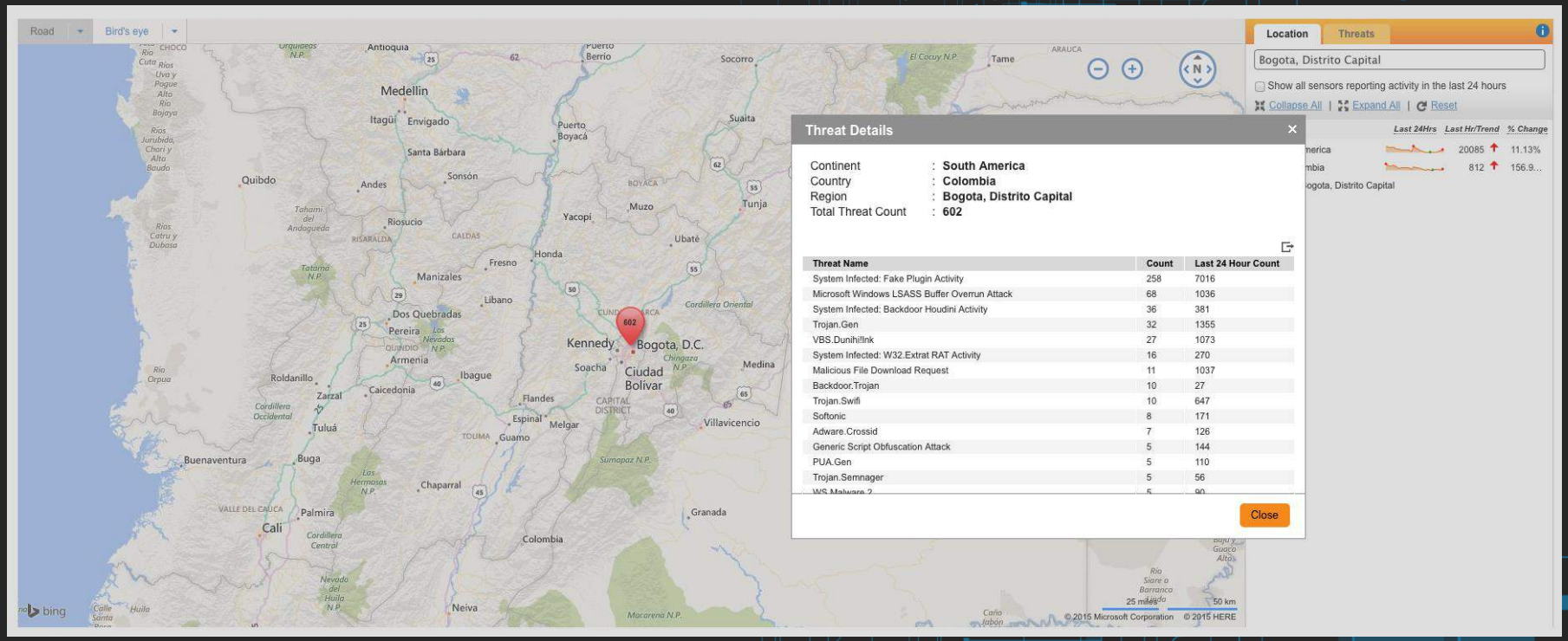
# Ranking Colombia - Global

| Threats (by Source)<br>Source: Symantec | 2014 Rank | 2014 Percentage | 2013 Rank | 2013 Percentage |
|---|---|---|---|---|
| Malicious Code | 53 | 0.24% | 43 | 0.32% |
| Spam | 19 | 1.55% | 17 | 1.85% |
| Phishing Hosts | 18 | 0.99% | 31 | 0.50% |
| Bots | 57 | 0.09% | 55 | 0.10% |
| Network Attacking Countries | 51 | 0.24% | 42 | 0.34% |
| Web Attacking Countries | 52 | 0.07% | 49 | 0.10% |

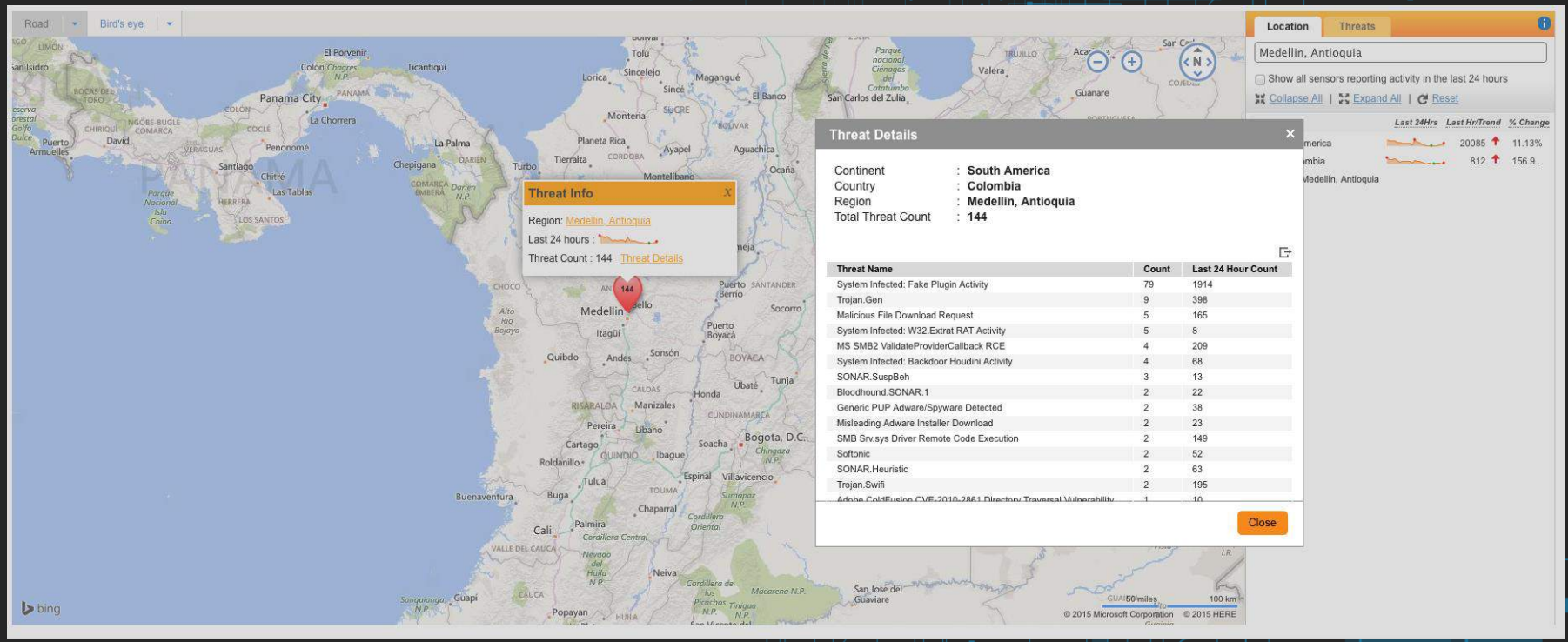
# Status en Symantec GIN (Global Intelligence Network)



# Status en Symantec GIN (Global Intelligence Network)



# Status en Symantec GIN (Global Intelligence Network)



Symantec

# ISTR20

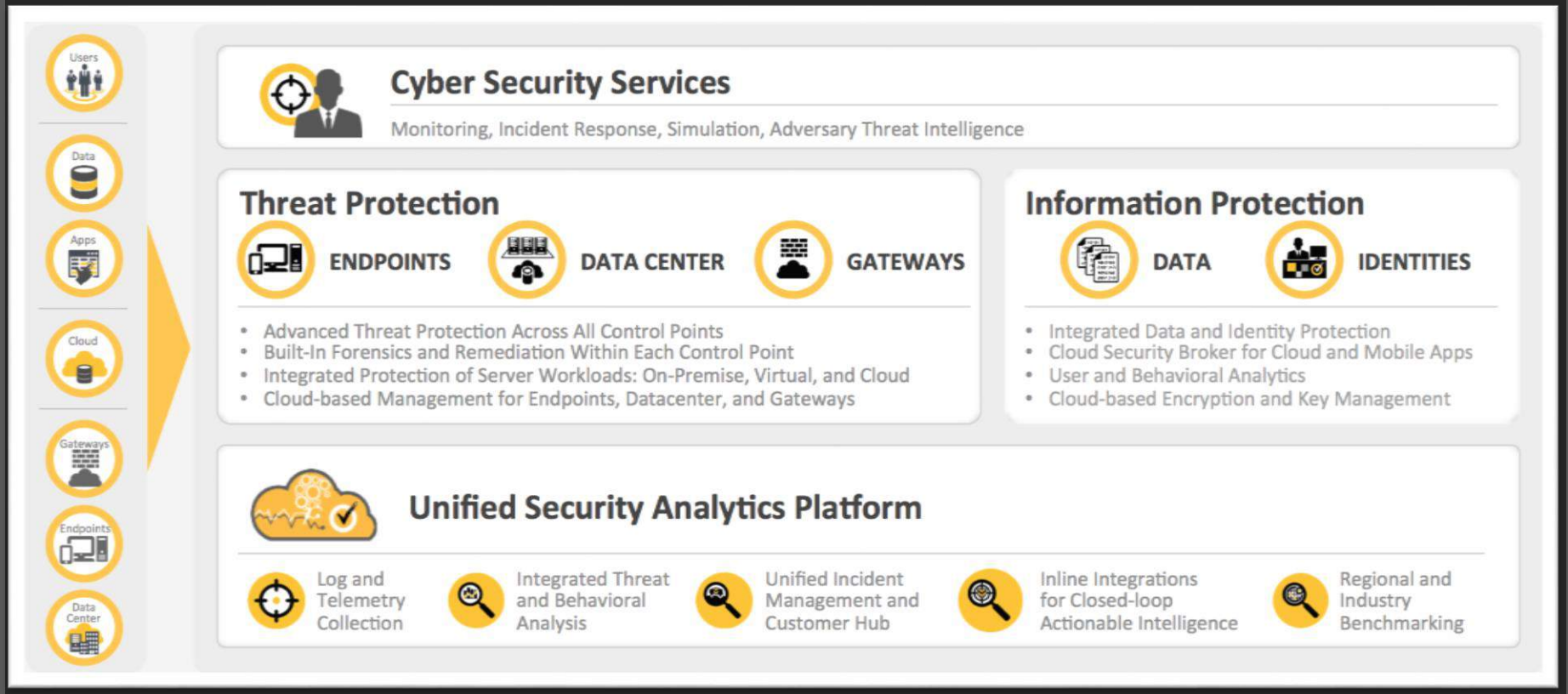
## INTERNET SECURITY THREAT REPORT

## Mejores Prácticas

# Mejores prácticas

| | |
|---|---|
| **Que no te sorprendan desprevenido** | Utiliza soluciones avanzadas de inteligencia ante amenazas para ayudarte a encontrar indicadores de riesgo y además responder rápidamente ante cualquier incidente. |
| **Adopta una fuerte política de seguridad** | Implementa seguridad con capas múltiples para endpoints, seguridad de red, encriptación, autenticaciones sólidas y tecnologías basadas en la reputación. Alíate con un proveedor de servicios de seguridad para expandir tu equipo de TI. |
| **Prepárate para lo peor** | La administración de incidentes garantiza que tu marco de seguridad esté optimizado, sea medible, repetible, y las lecciones aprendidas mejorarán tu postura en cuanto a la seguridad. Considera agregar honorarios para un experto que te ayude en momentos de crisis. |
| **Ofrece entrenamiento continuo** | Establece guías, políticas corporativas y procedimientos para proteger datos delicados en dispositivos personales y corporativos. Asesora constantemente a los equipos internos de investigación y lleva a cabo ejercicios de práctica para asegurarte de que cuentas con el conocimiento necesario para hacer frente a las amenazas cibernéticas de manera efectiva. |

# Symantec Enterprise Security | PRODUCT STRATEGY



# Symantec Threat Protection
## SUMMARY OF KEY CAPABILITIES

### Advanced Threat Protection

- Single platform
- Cloud-based payload detonation
- Cross-control point correlation and incident prioritization
- Closed-loop remediation
- Unified incident management

### Next Gen Forensics and Remediation

- Granular flight recorder
- Fine-grained remediation policies
- Known and unknown exploit detection
- Common management console with centralized activity logs
- Closed-loop remediation
- No new agent (easy upgrade)

### Server Workload Protection

- Integrated protection across on premise, virtualized, and cloud-based workloads
- Consistent application of lockdown, app control, and lockdown policies
- Common Management/orchestration as workloads move to and from cloud
- Support for VMWare (NSX/ESX) and Amazon, Azure, and OpenStack

**Cloud-based management with single extendable agent technology, self-service BYOD provisioning, and native encryption & key management**

Symantec.

# Symantec Information Protection
## SUMMARY OF KEY CAPABILITIES

### Cloud Security Broker

- Data and identity protection between mobile and cloud, with no perimeter
- Highly contextual protection by connecting user, device, location, and data loss prevention policies
- Cloud-based SSO with biometric authorization
- Scan and remediation of data already in cloud apps

### User and Behavioral Analytics

- Integrated analytics to track and profile behaviors and data flow
- Prioritized incident management
- Pre-built threat models and big-data analytics to quickly flag and detect incidents
- Industry and global intel correlation to detect coordinated attacks

Symantec.

# Symantec Cyber Security Services
## SUMMARY OF KEY CAPABILITIES

### Security Monitoring Services

- Key technology IP for log collection, analytics, and incident investigation
- Tailored to customer maturity/industry
- High-touch 24x7 service model
- Integration with next gen security infrastructure to detect advanced threats

### IR and Simulation Services

- Global team with extensive experience in forensics investigation
- Emergency/Retained/Managed options
- Integrated with SOCs to provide end to end service
- Realistic live fire training missions delivered as a SaaS solution

### Threat Intelligence Services

- Global Intelligence Network
- Early warning Portal
- Adversary threat intelligence
- Integrated IoCs from internal and external feeds

**Global team of 500+ threat and intel experts with unique knowledge of attack actors; Supported by Cloud-based Big Data analytics infrastructure**

Symantec.

# Cyber Security Services

**SERVICIOS DE SEGURIDAD ADMINISTRADOS**

- Expande tu grupo de seguridad con un equipo dedicado de analistas de seguridad altamente especializados para reducir gastos operacionales y mejorar la respuesta.
- Implementa una inteligencia global contra amenazas para reducir el impacto al negocio de ciberataques.
- Detecta rápidamente, evalúa y responde a ataques dedicados avanzados.

**INTELIGENCIA DEEPSIGHT**

- Prepara, detecta y responde a incidentes utilizando inteligencia contra amenazas y adversarios en tiempo real.
- Utiliza un análisis avanzado de ataques y las motivaciones y técnicas de los criminales para anticiparte y mitigar riesgos de ciberseguridad.
- Mantente informado sobre amenazas reales, desde las vulnerabilidades hasta las motivaciones y técnicas que utilizan los atacantes.

**RESPUESTA A INCIDENTES**

- Evalúa el impacto de un incidente de seguridad, contiene y erradica la amenaza con los servicios *Incident Response Emergency Services* y *Retainer Services*.
- Construye y afina tu programa de respuesta con servicios *Readiness Services* y al aplicar las lecciones aprendidas después de cada incidente.

**SIMULACROS DE SEGURIDAD**

- Fortalece la preparación ante amenazas mediante simulacros sobre los ataques sofisticados y de múltiples niveles que existen hoy.
- Prepara a tus equipos para combatir las más recientes herramientas y técnicas de ataque utilizando un entrenamiento con un entorno inmersivo e interactivo basado en la nube.
- Obtén información sobre el desempeño de tu equipo y las oportunidades para desarrollar los conocimientos individuales.

Proactivo  Reactivo  Monitoreo y administración

Symantec.

# ¡Gracias!

Felipe Silgado

Felipe_silgado@symantec.com

@SymantecLatam