Reporte WannaCry Telefónica

Práctica integradora

Cáceres Zapata, Kevin Luis

Índice

Resumen ejecutivo

Este informe analiza el impacto que tuvo el ransomware **WannaCry** en la empresa **Telefónica España** en mayo de 2017.

Toda la información presentada fue recabada exclusivamente de fuentes públicas y oficiales, incluyendo reportes de **Microsoft, ENISA, NIST, Europol, CISA, CERT-EU** y análisis técnicos de proveedores de ciberseguridad.

WannaCry fue uno de los ataques más relevantes de la última década porque combinó dos factores:

- Su capacidad de propagarse automáticamente como un gusano.
- Su impacto global, que afectó tanto a empresas como a servicios críticos.

Telefónica fue una de las primeras grandes organizaciones europeas en verse afectada. La infección obligó a desconectar estaciones de trabajo de forma preventiva, generó interrupciones operativas y expuso la falta de preparación frente a un ataque de estas características.

Se identificaron riesgos principales en la organización:

1. **Uso de sistemas obsoletos y vulnerables** con el protocolo SMBv1 habilitado.
2. **Demora en la aplicación del parche MS17-010**, que hubiera mitigado el vector de ataque.
3. **Red corporativa poco segmentada**, que facilitó la propagación lateral.
4. **Backups accesibles desde la misma red**, con riesgo de ser cifrados.
5. **Falta de telemetría y detección temprana**, lo que impidió responder a tiempo.

Las recomendaciones propuestas incluyen controles técnicos y organizativos como la eliminación de SMBv1, la implementación de EDR y SIEM con capacidades de detección avanzada, la segmentación de red, políticas estrictas de respaldo, autenticación multifactor para accesos privilegiados y planes de respuesta a incidentes ensayados regularmente.

El objetivo del presente documento es no solo documentar lo ocurrido, sino también ofrecer medidas concretas para reducir la probabilidad de que incidentes de esta magnitud se repitan en el futuro.

Alcance y contexto

El alcance del presente reporte se limita al análisis del ataque de WannaCry en Telefónica España, considerando la infraestructura típica de una empresa de telecomunicaciones de gran porte.

Se incluyen observaciones basadas en fuentes oficiales y reportes de organismos internacionales, tales como **ENISA**, **NIST**, **Europol**, **CISA**, así como documentos técnicos de **Microsoft** y de proveedores de ciberseguridad privados.

Contexto internacional

El ataque de WannaCry no se limitó a Telefónica. Se estima que afectó a más de **200.000 equipos en 150 países** en cuestión de días. Entre los casos más notorios se encuentran:

- El **Servicio Nacional de Salud (NHS) del Reino Unido**, que tuvo que cancelar consultas médicas y cirugías por la indisponibilidad de sistemas.
- La automotriz **Renault**, que suspendió temporalmente la producción en varias plantas de Francia.
- La empresa de logística **FedEx** en Estados Unidos, que reportó retrasos significativos en la entrega de paquetes.

Estos ejemplos muestran que WannaCry trascendió el ámbito empresarial y afectó a sectores críticos como la salud, la industria y la logística.

Vector de ataque

WannaCry explotó la vulnerabilidad **MS17-010 (EternalBlue)** en el protocolo **SMBv1** de Windows. Este vector de ataque le permitió obtener ejecución remota de código y propagarse automáticamente sin intervención del usuario. A diferencia de otros ransomware de la época, WannaCry combinó el cifrado de archivos con la capacidad de gusano, lo que multiplicó exponencialmente su alcance.

Relevancia para Telefónica

Telefónica, como una de las principales operadoras de telecomunicaciones de Europa, se vio expuesta por la existencia de miles de estaciones de trabajo con SMBv1 habilitado y sin el parche MS17-010 aplicado. El ataque impactó principalmente a los equipos de usuario, pero generó gran repercusión mediática y obligó a la compañía a desconectar parte de su infraestructura para contener la propagación.

Metodología

La elaboración del presente reporte se realizó siguiendo un **enfoque estructurado y alineado con buenas prácticas internacionales**, de forma similar al reporte de ENISA aplicado a Microsoft 365/Azure.

Las fases metodológicas fueron las siguientes:

1. **Recolección de información**
   Se consultaron fuentes oficiales de Microsoft, alertas de CISA/US-CERT, reportes de ENISA, NIST y Europol, además de análisis técnicos de empresas de seguridad reconocidas como Symantec y Kaspersky.

2. **Análisis técnico del ataque**
   Se estudió el funcionamiento de WannaCry, incluyendo la explotación de EternalBlue, la propagación por SMBv1 y el proceso de cifrado de archivos en los equipos comprometidos.

3. **Mapeo a MITRE ATT&CK**
   Se relacionaron las tácticas y técnicas utilizadas con los identificadores oficiales de MITRE ATT&CK, para establecer trazabilidad con un marco de referencia reconocido.

4. **Revisión de controles de seguridad existentes**
   Se evaluaron las medidas que Telefónica tenía disponibles en 2017, identificando brechas que permitieron la propagación del ataque.

5. **Diseño de controles propuestos**
   Se definieron recomendaciones alineadas a ENISA, NIST SP 800-63B y Microsoft, orientadas a la prevención, detección y recuperación frente a ransomware.

6. **Evaluación de riesgo residual y priorización**
   Se analizaron los riesgos que permanecerían incluso después de aplicar los controles, y se estableció una priorización temporal de medidas inmediatas, a mediano y largo plazo.

7. **Elaboración de anexos técnicos**
   Se desarrollaron consultas de hunting (KQL), ejemplos de firmas IDS/IPS, fragmentos de políticas de red y backup en formato YAML/JSON, y un checklist de auditoría para verificar la correcta implementación de las medidas.

Este enfoque garantiza que las recomendaciones propuestas sean **concretas, verificables y aplicables** a entornos corporativos reales.

Hallazgos

El análisis del caso WannaCry en Telefónica puso de manifiesto múltiples debilidades que facilitaron la propagación del ataque y que son comunes en organizaciones de gran tamaño. Estos hallazgos se describen de manera narrativa, pero se resumen también en la siguiente tabla para mayor claridad:

Categoría	Hallazgo principal	Impacto observado
Inventario	Inexistencia de un inventario actualizado de activos vulnerables.	Dificultad para identificar rápidamente qué equipos eran críticos y vulnerables.
Gestión de parches	Retraso en la aplicación del parche MS17-010 publicado por Microsoft en marzo 2017.	Permitir que miles de equipos siguieran expuestos al exploit EternalBlue.
Protocolos inseguros	Mantenimiento del protocolo SMBv1 habilitado en estaciones de trabajo y servidores.	Explotación inmediata de la vulnerabilidad y propagación automática del gusano.
Segmentación de red	Infraestructura con diseño de red plano y sin microsegmentación.	Permitir un movimiento lateral rápido hacia otras áreas de la red corporativa.
Backups	Respaldos accesibles desde la misma red de producción.	Riesgo de cifrado de copias de seguridad y pérdida de capacidad de recuperación.

Categoría	Hallazgo principal	Impacto observado
Telemetría	Cobertura incompleta de EDR y correlaciones limitadas en el SIEM.	Falta de detección temprana de comportamientos anómalos de cifrado.
Preparación	Ausencia de simulacros de respuesta a incidentes y planes desactualizados.	Retrasos en la coordinación interna durante las primeras horas del ataque.

Estos hallazgos evidencian una combinación de factores técnicos y organizativos que contribuyeron a la magnitud del impacto.

Análisis y mapeo MITRE ATT&CK

Para comprender la dinámica del ataque se utilizó el marco **MITRE ATT&CK**, que permite mapear de forma estandarizada las tácticas y técnicas empleadas por WannaCry.

Táctica	Técnica utilizada	ID ATT&CK	Evidencia en WannaCry
Initial Access	Exploit Public-Facing Application (SMBv1)	T1190	Uso de EternalBlue para obtener acceso inicial a sistemas vulnerables.
Lateral Movement	Exploitation of Remote Services	T1210	Propagación automática hacia otros equipos por el puerto 445/TCP.
Execution	Command and Scripting Interpreter	T1059	Ejecución de binarios y scripts para activar el cifrado de archivos.
Defense Evasion	Masquerading / Disable Security Tools	T1036/1089	Intentos de detener servicios de seguridad y camuflar procesos maliciosos.
Impact	Data Encrypted for Impact	T1486	Cifrado de archivos en estaciones de trabajo y despliegue de notas de rescate.

El mapeo ATT&CK permite establecer una trazabilidad clara entre el comportamiento observado y las técnicas documentadas, facilitando el diseño de controles y detecciones.

Controles propuestos

En base a los hallazgos anteriores, se proponen controles alineados con **ENISA**, **NIST SP 800-63B** y con las capacidades disponibles en **Microsoft 365/Azure**. Estos controles se dividen en tres categorías: preventivos, detectivos y de recuperación.

Controles preventivos

- **Gestión de vulnerabilidades y parches:** establecer un proceso que asegure la aplicación de parches críticos en menos de 48 horas.
- **Eliminación de SMBv1:** deshabilitar el protocolo en todos los equipos y bloquear el puerto 445 en firewalls internos.
- **Inventario actualizado:** mantener un inventario dinámico de activos para identificar sistemas vulnerables.
- **Privilegios mínimos y autenticación fuerte:** aplicar el principio de menor privilegio y habilitar MFA en cuentas administrativas.
- **Hardening de sistemas:** uso de imágenes base seguras y auditorías periódicas de configuración.

Controles detectivos

- **EDR con detección de cifrado masivo:** herramientas como Microsoft Defender for Endpoint permiten detectar patrones de ransomware.
- **SIEM con correlaciones específicas:** Microsoft Sentinel u otros SIEM deben tener reglas de correlación para detectar escaneos SMB o procesos de cifrado inusuales.
- **Monitoreo de red:** detección de tráfico anómalo en el puerto 445/TCP, uso de honeypots y firmas IDS/IPS para EternalBlue.

Controles de recuperación

- **Backups inmutables y aislados:** aplicar la regla 3-2-1 y mantener al menos una copia offline o air-gapped.
- **Pruebas periódicas de restauración:** validar que los respaldos cumplen con RTO y RPO definidos.
- **Playbooks de respuesta:** guías claras para aislamiento de equipos, preservación de evidencias y comunicación interna.

Mapeo de controles a riesgos y ATT&CK

Control propuesto	Riesgo mitigado	Técnica ATT&CK	Norma de referencia
Parcheo inmediato (MS17-010)	Explotación de SMBv1	T1190/T1210	ENISA / NIST
Deshabilitar SMBv1 y bloquear 445	Propagación lateral automática	T1210	ENISA
Segmentación de red	Reducción del radio de propagación	T1210	ENISA
MFA y privilegios mínimos	Abuso de cuentas administrativas	T1078	NIST SP 800-63B
Backups inmutables y aislados	Pérdida de datos por cifrado	T1486	ENISA
EDR y SIEM con reglas específicas	Detección temprana de cifrado y escaneo SMB	T1059/T1486	ENISA / Microsoft
Playbook y simulacros de respuesta	Falta de coordinación y demora en contención	T1036/T1089	ENISA

Estos controles constituyen una estrategia de **defensa en profundidad**, que combina prevención, detección y capacidad de recuperación, asegurando resiliencia frente a ataques similares.

Actor atribuido: Lazarus Group

El ataque WannaCry ha sido atribuido a **Lazarus Group**, un actor de amenazas avanzado vinculado a Corea del Norte.
Este grupo se caracteriza por combinar motivaciones económicas con fines disruptivos y geopolíticos.

Característica	Detalle
Origen	Corea del Norte
Motivación	Económica (ransomware) y geopolítica (disrupción)
Historial	Ataques a SWIFT (2016), Sony Pictures (2014), campañas de ransomware 2017–2018
Técnicas utilizadas	Explotación de vulnerabilidades, malware wormable, evasión de controles, monetización vía Bitcoin
Relación con WannaCry	Uso de EternalBlue y propagación automática global

IoCs y señales de detección

La detección temprana de WannaCry depende de indicadores técnicos (IoCs) y señales de comportamiento en los registros de los sistemas.

Categoría	Indicador / Señal
Ficheros	`wannacry.exe`, `tasksche.exe`, extensión `.WNCRY`
Notas de rescate	`@Please_Read_Me@.txt`
Red	Tráfico inusual en puerto 445/TCP, dominio sinkhole: `iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com`
Hashes (SHA-256)	Publicados por CISA y Microsoft en 2017 (mantener actualizados)
Eventos Windows	4688 (creación de procesos), 4624/4625 (logons), 7045 (servicios instalados)

Estos IoCs deben integrarse en un **SIEM** para generar alertas automáticas y facilitar la caza proactiva de amenazas.

Plan de verificación de eficacia

Se recomienda un plan de pruebas periódicas para asegurar que los controles implementados son efectivos:

1. **Simulacros controlados de ransomware** → evaluar tiempo de detección (MTTD) y respuesta (MTTR).

2. **Pruebas de restauración de backups** → validar cumplimiento de RTO/RPO.

3. **Ejecución de hunting queries en SIEM** (ej. KQL en Sentinel).

4. **Validación de políticas de acceso condicional** → asegurar que bloquean protocolos inseguros.

5. **Revisión trimestral de configuración de EDR y firewalls**.

6. **Auditoría anual de cumplimiento de ENISA/NIST**.

KPIs sugeridos:
- MTTD $<$ 15 minutos.
- MTTR $<$ 4 horas.
- 95% de hosts parcheados en 48h.

Riesgo residual y priorización

Aunque los controles propuestos reducen significativamente el riesgo, persisten exposiciones residuales:

Riesgo residual	Descripción
Zero-day	Vulnerabilidades desconocidas sin parche disponible.
Sistemas legacy	Equipos antiguos que no permiten aplicar MS17-010 ni desactivar SMBv1.
Errores humanos	Fallos en despliegue de parches, backups o configuración de red.
Limitaciones operativas	Ventanas de mantenimiento, falta de cobertura 24/7 o recursos limitados.
Backups incompletos/no validados	Copias que no cumplen objetivos de recuperación.

Priorización temporal:

- **0–30 días:** deshabilitar SMBv1, aplicar MS17-010, aislar backups, ajustar reglas de EDR/SIEM.
- **1–6 meses:** migrar sistemas legacy, automatizar parcheo, ampliar telemetría SOC.
- **6–12+ meses:** implementar microsegmentación y realizar ejercicios regulares de respuesta a incidentes.

Conclusiones

- El ataque WannaCry a Telefónica evidenció cómo la falta de parches críticos puede derivar en un impacto global.
- La combinación de **parcheo inmediato, segmentación de red, EDR avanzado y backups inmutables** constituye la base para resistir ataques de ransomware.
- Marcos como **ENISA** y **NIST SP 800-63B**, junto con el mapeo de **MITRE ATT&CK**, permiten estructurar una defensa en profundidad.
- Si bien Telefónica logró contener el ataque, el incidente demostró la necesidad de planes de contingencia más sólidos y una gobernanza de seguridad proactiva.

En términos de lecciones aprendidas, WannaCry demostró que la gestión proactiva de vulnerabilidades y la actualización constante de sistemas no es opcional, sino un requisito crítico para la continuidad de negocio. Asimismo, la necesidad de segmentar redes, aislar respaldos y entrenar al personal en planes de contingencia se vuelve fundamental para reducir el impacto de futuros incidentes.

Como recomendación final, se propone institucionalizar una cultura de ciberresiliencia que combine controles técnicos robustos con procesos de mejora continua y capacitación de usuarios. Solo mediante este enfoque integral se puede asegurar que la organización esté preparada para enfrentar no solo amenazas similares a WannaCry, sino también las variantes más avanzadas de ransomware y otros ataques emergentes.

Referencias

- ENISA — WannaCry Ransomware (2017)
- NIST SP 800-63B — Digital Identity Guidelines
- Microsoft — MS17-010 Security Bulletin
- Europol — WannaCry overview and impact
- CISA / US-CERT — Indicators Associated With WannaCry Ransomware
- CERT-EU — Security Advisory SA2017-012
- Symantec (Broadcom) — WannaCry Threat Report
- Kaspersky — WannaCry Chronology and Technical Analysis
- Reuters — Telefónica and Spanish firms hit by ransomware attack

Anexos técnicos

Anexo A — Tabla de trazabilidad

Control aplicado	Riesgo mitigado	Técnica ATT&CK	Norma de referencia
Parche MS17-010	Explotación de SMBv1	T1190/T1210	ENISA / Microsoft
Deshabilitar SMBv1	Propagación lateral	T1210	ENISA
Segmentación de red	Movimiento lateral	T1210	ENISA
Backups offline/inmutables	Pérdida de datos por cifrado	T1486	ENISA

Anexo B — Ejemplos de queries KQL (Sentinel)

Detección de escaneos SMB:

```
DeviceNetworkEvents
| where RemotePort == 445
| summarize Attempts = count() by RemoteIP, DeviceId, bin(Timestamp, 5m)
| where Attempts > 50
```

Anexo C — Firma IDS/IPS

alert tcp any any -> any 445 (msg:“ETERNALBLUE MS17-010”; sid:2024217;)

Anexo D — Playbook de respuesta

1. Aislar host.
2. Notificar SOC.
3. Bloquear propagación en firewall.
4. Preservar evidencia.
5. Erradicar binarios.
6. Restaurar backups.
7. Reporte postmortem.

Anexo E — Política de backups (YAML)

backup: schedule: daily retention: 90d storage: offline verification: true

Anexo F — Política de red (JSON)

```
{
  "conditions": { "devices": { "requireCompliant": true } },
  "grantControls": { "operator": "AND", "builtInControls": ["blockLegacySMB","requireEDR"] }
}
```