

Alerta ID:	117
Fecha del reporte:	30/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Campaña activa de phishing y robo de credenciales dirigida al sector salud
Herramienta de detección	N/A
Activo involucrado:	Sistema de autenticación de la organización
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una campaña activa de ataques de phishing dirigido (spear phishing) y distribución de malware tipo infostealer, cuyo objetivo principal es el robo de credenciales de acceso a sistemas críticos como VPN corporativas, correo institucional, plataformas de historia clínica electrónica (HCE) y servicios de autenticación centralizada.

El propósito de esta alerta es que las entidades del sector salud validen sus mecanismos de autenticación, la exposición de credenciales y la configuración de sus sistemas de correo electrónico y acceso remoto, con el fin de prevenir accesos no autorizados, compromiso de cuentas privilegiadas y afectación de la continuidad operativa de los servicios clínicos y administrativos.



Descripción:

Se ha identificado una campaña activa de phishing dirigido contra personal del sector salud, caracterizada por el uso de correos electrónicos, mensajes SMS y enlaces maliciosos que simulan ser comunicaciones legítimas de entidades médicas, aseguradoras o plataformas institucionales.

Los atacantes emplean técnicas de ingeniería social altamente dirigidas para inducir a las víctimas a ingresar sus credenciales en portales falsos que imitan servicios legítimos como VPN corporativas, Microsoft 365 o sistemas internos de autenticación.

Una vez capturadas las credenciales, estas son utilizadas para acceder de forma legítima a los sistemas corporativos, evitando mecanismos tradicionales de detección basados en malware o firmas. En muchos casos, la campaña se complementa con la instalación de malware tipo infostealer, diseñado para extraer credenciales almacenadas en navegadores, cookies de sesión, tokens de autenticación y datos sensibles del sistema.

Consecuencias de la explotación

La explotación exitosa de campañas de **phishing dirigido y robo de credenciales (credential harvesting)** en el sector salud puede generar un impacto sistémico, ya que el atacante no requiere vulnerar directamente la infraestructura tecnológica, sino que accede a ella mediante el uso de credenciales legítimas comprometidas.

1. Compromiso total de cuentas y acceso legítimo a sistemas críticos

El principal riesgo de esta campaña es el acceso no autorizado mediante credenciales válidas, lo que permite al atacante operar como un usuario legítimo dentro de la organización.



Esto incluye acceso a:

- VPN corporativas
- Correo institucional (Microsoft 365 / Exchange)
- Sistemas de historia clínica electrónica (HCE)
- Plataformas de laboratorio y diagnóstico
- Sistemas administrativos y financieros

Impacto clave:

El atacante evita controles tradicionales de seguridad al utilizar identidades válidas.

2. Compromiso de identidad digital y suplantación de usuarios

Una vez obtenidas las credenciales, el atacante puede:

- Suplantar personal médico o administrativo
- Acceder a sesiones activas sin detección inmediata
- Reutilizar tokens de autenticación o cookies de sesión
- Mantener acceso persistente sin necesidad de malware adicional

Impacto clave:

Se rompe el principio de confianza en la identidad del usuario dentro del sistema.

3. Acceso a información clínica y datos sensibles de pacientes

El acceso a sistemas internos permite la exposición directa de:

- Historias clínicas electrónicas (HCE)
- Resultados de laboratorio
- Imágenes diagnósticas



- Datos de aseguramiento y facturación
- Información personal identificable (PII)

Impacto clave:

Riesgo crítico de violación de confidencialidad de datos de pacientes.

4. Movimiento lateral dentro de la infraestructura hospitalaria

Con una sola cuenta comprometida, el atacante puede expandirse dentro de la red:

- Acceso a servidores internos vía SMB, RDP o VPN
- Escalamiento hacia Active Directory
- Acceso a múltiples sistemas clínicos interconectados
- Compromiso de otros usuarios mediante reutilización de credenciales

Impacto clave:

Un solo usuario comprometido puede escalar a compromiso de toda la red.

5. Persistencia del atacante en el entorno

El uso de credenciales válidas permite al atacante:

- Mantener acceso incluso después de reinicios del sistema
- Acceder desde múltiples ubicaciones geográficas
- Reutilizar sesiones activas sin levantar alertas inmediatas
- Evadir controles basados en detección de malware

Impacto clave:

Alta dificultad de detección por ausencia de indicadores de malware tradicionales.

6. Exfiltración de información sensible y filtración de datos



El atacante puede extraer información de forma silenciosa, incluyendo:

- Bases de datos clínicas completas
- Credenciales de otros sistemas internos
- Información de pacientes y personal médico
- Documentos administrativos y financieros

Impacto clave:

Posible fuga masiva de datos sensibles del sector salud.

7. Impacto regulatorio y cumplimiento normativo

La exposición de datos personales puede generar:

- Incumplimiento de la Ley 1581 de 2012 (Protección de datos en Colombia)
- Sanciones por parte de la Superintendencia de Industria y Comercio (SIC)
- Obligaciones de notificación de incidentes de seguridad
- Investigaciones regulatorias y auditorías forenses

Impacto clave:

Riesgo legal y sancionatorio para la entidad de salud.

8. Interrupción operativa de servicios críticos

El compromiso de credenciales puede derivar en:

- Bloqueo de accesos a sistemas clínicos
- Interrupción de servicios de atención médica digital
- Caída de plataformas de laboratorio o diagnóstico
- Retrasos en procesos administrativos y asistenciales



Impacto clave:

Afectación directa a la continuidad del servicio de salud.

9. Pérdida de confianza institucional y reputacional

La materialización de este tipo de incidentes puede provocar:

- Pérdida de confianza de pacientes y usuarios
- Afectación de la reputación institucional
- Impacto en relaciones con aseguradoras y aliados estratégicos
- Incremento de auditorías externas y supervisión regulatoria

Impacto clave:

Daño reputacional prolongado en el sector salud.

Modo de explotación del ataque

La explotación de esta campaña se basa en una cadena de ataque progresiva que combina **ingeniería social, robo de credenciales y uso de accesos legítimos**, permitiendo a los atacantes evadir controles tradicionales de seguridad y operar como usuarios válidos dentro de la infraestructura hospitalaria.

FASE 1 – RECONOCIMIENTO Y PERFILAMIENTO DEL OBJETIVO

El atacante inicia con la identificación de personal del sector salud mediante técnicas de inteligencia de fuentes abiertas (OSINT) y filtraciones de datos previos.

Se priorizan usuarios con acceso a:

- VPN corporativa
- sistemas de historia clínica electrónica (HCE)



- Active Directory
- correo institucional
- plataformas administrativas y clínicas

MITRE ATT&CK:

- T1589 – Gather Victim Identity Information
- T1592 – Gather Victim Host Information

FASE 2 – INGENIERÍA SOCIAL Y ENTREGA DEL ATAQUE

Se ejecuta una campaña de **phishing dirigido (spear phishing)** mediante:

- correos electrónicos fraudulentos
- mensajes SMS (smishing)
- mensajes de WhatsApp corporativo simulado
- enlaces a portales falsos de autenticación

Los señuelos suelen simular:

- resultados de laboratorio
- alertas médicas urgentes
- acceso a portales institucionales
- notificaciones de EPS o aseguradoras

MITRE ATT&CK:

- T1566.001 – Spearphishing Attachment
- T1566.002 – Spearphishing Link



FASE 3 – CAPTURA DE CREDENCIALES (CREDENTIAL HARVESTING)

El usuario es redirigido a portales falsos que imitan servicios legítimos como:

- VPN corporativa (Fortinet / Cisco / Palo Alto)
- Microsoft 365 / Outlook Web Access
- portales internos hospitalarios

Al ingresar sus credenciales:

- estas son enviadas en tiempo real al atacante
- se almacenan en infraestructura controlada por el adversario
- pueden ser reutilizadas inmediatamente

MITRE ATT&CK:

- T1056 – Input Capture
- T1556 – Credential Access via Web Portals

FASE 4 – ACCESO INICIAL CON CREDENCIALES VÁLIDAS

El atacante utiliza las credenciales robadas para autenticarse en los sistemas reales de la organización:

- acceso a VPN corporativa
- ingreso a correo institucional
- autenticación en Active Directory
- acceso a portales internos de salud

MITRE ATT&CK:

- T1078 – Valid Accounts



Riesgo clave:

No se detecta como intrusión porque el acceso es “legítimo”.

FASE 5 – RECONOCIMIENTO INTERNO DEL ENTORNO

Dentro de la red, el atacante realiza reconocimiento interno:

- identificación de servidores críticos
- enumeración de usuarios y grupos AD
- mapeo de recursos compartidos (SMB)
- exploración de sistemas clínicos

MITRE ATT&CK:

- T1087 – Account Discovery
- T1018 – Remote System Discovery
- T1069 – Permission Groups Discovery

FASE 6 – MOVIMIENTO LATERAL

El atacante se desplaza dentro de la infraestructura usando:

- SMB (acceso a archivos compartidos)
- RDP (acceso remoto a servidores)
- WinRM (administración remota)
- reutilización de credenciales internas

Esto permite expandir el compromiso hacia:

- servidores clínicos
- bases de datos de pacientes



- sistemas administrativos
- Active Directory

MITRE ATT&CK:

- T1021 – Remote Services
- T1550 – Use Alternate Authentication Material

FASE 7 – ESCALAMIENTO DE PRIVILEGIOS Y DOMINIO

Si se obtienen credenciales privilegiadas, el atacante puede:

- comprometer Active Directory
- escalar a Domain Admin
- modificar políticas de seguridad (GPO)
- crear usuarios persistentes ocultos

MITRE ATT&CK:

- T1068 – Privilege Escalation
- T1558 – Kerberos Ticket Abuse
- T1078 – Valid Accounts

FASE 8 – IMPACTO FINAL

Una vez consolidado el acceso, el atacante puede ejecutar:

- exfiltración de bases de datos clínicas
- robo masivo de credenciales
- despliegue de ransomware



- interrupción de servicios hospitalarios
- eliminación de copias de seguridad

MITRE ATT&CK:

- T1041 – Exfiltration Over C2 Channel
- T1486 – Data Encrypted for Impact

Vulnerabilidades asociadas

La campaña de phishing dirigido y robo de credenciales analizada no se basa en la explotación de vulnerabilidades de software específicas (CVE), sino en el abuso de técnicas de ingeniería social, credenciales válidas y debilidades en controles de identidad y monitoreo, las cuales están ampliamente documentadas en el marco MITRE ATT&CK.

1. Ingeniería social y acceso inicial**MITRE ATT&CK: T1566 – Phishing****Descripción**

Los atacantes utilizan correos electrónicos, SMS o mensajes de mensajería instantánea para engañar a los usuarios y dirigirlos a portales falsos de autenticación.

Debilidades asociadas

- Falta de filtros avanzados de correo (ATP / anti-phishing)
- Ausencia de verificación de dominios
- Baja concienciación del usuario final
- Ausencia de validación de urls seguras

2. Captura de credenciales (Credential Harvesting)

MITRE ATT&CK: T1056 – Input Capture

Descripción

Robo de credenciales mediante formularios falsos que simulan sistemas legítimos (VPN, Microsoft 365, portales clínicos).

Debilidades asociadas

- Falta de MFA en sistemas críticos
- Reutilización de contraseñas
- Ausencia de detección de páginas de phishing
- Sesiones sin protección adicional (token replay)

3. Uso de credenciales válidas

MITRE ATT&CK: T1078 – Valid Accounts

Descripción

El atacante utiliza credenciales legítimas robadas para autenticarse en sistemas corporativos sin levantar alertas inmediatas.



Debilidades asociadas

- Ausencia de autenticación multifactor (MFA)
- Falta de detección de login anómalo (geolocalización / dispositivo)
- Credenciales sin rotación periódica
- Cuentas privilegiadas sin control PAM

4. Descubrimiento del entorno interno**MITRE ATT&CK: T1087 / T1018 / T1069****Descripción**

Una vez dentro de la red, el atacante realiza reconocimiento del entorno para identificar activos críticos.

Debilidades asociadas

- Falta de segmentación de red
- Visibilidad limitada en siem
- Ausencia de monitoreo de enumeración de ad
- Permisos excesivos en usuarios estándar

5. Movimiento lateral en la red**MITRE ATT&CK: T1021 – Remote Services****Descripción**

El atacante se desplaza dentro de la infraestructura utilizando servicios legítimos como RDP, SMB y WinRM.

Debilidades asociadas

- RDP expuesto o sin restricción
- Falta de segmentación entre redes clínicas y administrativas
- Credenciales reutilizadas entre sistemas
- Ausencia de jump servers o bastion hosts

6. Escalamiento de privilegios

MITRE ATT&CK: T1068 / T1558

Descripción

Uso de credenciales adicionales o abuso de configuraciones débiles para escalar privilegios dentro del dominio.

Debilidades asociadas

- Privilegios excesivos en Active Directory
- Mala configuración de delegación de permisos
- Ausencia de tiering model (Tier 0/1/2)
- Cuentas administrativas sin MFA

7. Persistencia del atacante

MITRE ATT&CK: T1098 – Account Manipulation



Descripción

El atacante crea o modifica cuentas para mantener acceso prolongado al entorno comprometido.

Debilidades asociadas

- Falta de auditoría de creación de usuarios
- Ausencia de alertas en cambios de privilegios
- Cuentas inactivas no eliminadas
- Monitoreo insuficiente de active directory

8. Evitación de detección**MITRE ATT&CK: T1071 – Web Protocols****Descripción**

Uso de tráfico HTTPS legítimo para ocultar actividad de comando y control o exfiltración.

Debilidades asociadas

- Falta de inspección SSL/TLS
- Ausencia de análisis de comportamiento (UEBA)
- SIEM sin correlación avanzada
- Falta de detección de anomalías en tráfico saliente

Recomendaciones de detección y mitigación

Para reducir el impacto de campañas de **phishing dirigido y robo de credenciales (credential harvesting)** en el sector salud, es fundamental implementar controles de detección temprana, correlación en SIEM y fortalecimiento de controles de identidad y correo electrónico.

DETECCIÓN EN SIEM (SOC – MONITOREO AVANZADO)

Detección de accesos anómalos

Configurar alertas para:

- Inicios de sesión desde ubicaciones geográficas inusuales
- Accesos simultáneos desde diferentes países o IPs
- Logins exitosos después de múltiples intentos fallidos
- Acceso a sistemas clínicos fuera de horario laboral

MITRE ATT&CK:

- T1078 – Valid Accounts

Detección de comportamiento sospechoso en identidad

Monitorear:

- cambios de contraseña no autorizados
- uso de cuentas privilegiadas desde dispositivos no registrados
- autenticaciones desde dispositivos nuevos o no confiables
- reutilización de sesiones o tokens



Detección de movimiento lateral temprano

Alertas sobre:

- múltiples accesos RDP/SMB entre servidores
- autenticaciones repetidas en distintos sistemas internos
- uso de credenciales de un usuario en varios hosts simultáneamente

MITRE ATT&CK:

- T1021 – Remote Services

Detección de phishing activo

- dominios recién creados relacionados con la organización
- URLs similares a portales oficiales (typosquatting)
- redirecciones sospechosas desde correos electrónicos
- acceso a páginas de login no corporativas

SEGURIDAD EN CORREO ELECTRÓNICO (EMAIL SECURITY)

Controles recomendados:

- Implementar filtros avanzados anti-phishing (ATP)
- Bloquear dominios no verificados o recién creados
- Activar análisis de URLs en tiempo real (URL rewriting)
- Sandboxing de archivos adjuntos sospechosos
- Validación SPF, DKIM y DMARC obligatoria



Objetivo: prevenir la entrega del phishing antes del usuario.

MITIGACIÓN EN IDENTIDAD (IAM / MFA)

Controles críticos:

- Implementar MFA obligatorio en:
 - VPN
 - correo institucional
 - sistemas clínicos
 - Active Directory (administración)
- Aplicar autenticación basada en riesgo:
 - ubicación
 - dispositivo
 - comportamiento
- Bloquear autenticaciones heredadas (legacy authentication)

MITRE ATT&CK:

- T1078 – Valid Accounts (reducción de impacto)

ENDURECIMIENTO DE ACCESO A SISTEMAS CRÍTICOS

- restringir acceso a VPN por geolocalización
- permitir acceso solo desde dispositivos gestionados (MDM)
- implementar Zero Trust Network Access (ZTNA)
- uso de bastion hosts para accesos administrativos

DETECCIÓN DE INFESTEALERS (SI APLICA)



Monitorear endpoints para:

- robo de credenciales almacenadas en navegadores
- extracción de cookies de sesión
- ejecución de procesos inusuales en perfiles de usuario
- conexiones salientes hacia dominios desconocidos

Indicadores típicos:

- tráfico HTTPS a dominios sin reputación
- ejecución de archivos temporales en AppData
- procesos de navegador inyectados

HARDENING DE ENDPOINTS

- deshabilitar almacenamiento de contraseñas en navegadores
- restringir ejecución de archivos descargados por correo
- activar EDR con detección de comportamiento
- bloquear ejecución de scripts no firmados
- habilitar logging avanzado en endpoints

INTELIGENCIA Y BLOQUEO PROACTIVO

- integrar feeds de threat intelligence (phishing domains)
- bloquear dominios recién creados (NRD filtering)
- actualizar listas de IOC en firewall y proxy
- correlacionar eventos con campañas activas de phishing



La principal debilidad explotada en estas campañas no es tecnológica, sino de identidad y comportamiento del usuario, por lo que la mitigación efectiva depende de la capacidad de detectar accesos anómalos, bloquear phishing antes de la interacción del usuario y asegurar que las credenciales robadas no puedan ser utilizadas sin validación adicional.

Recomendaciones de prevención y mitigación

Para reducir la exposición a campañas de phishing dirigido, robo de credenciales e instalación de infostealers, las organizaciones del sector salud deben implementar un enfoque de defensa en profundidad, combinando controles tecnológicos, de identidad y de concienciación del usuario:

FORTALECIMIENTO DE LA IDENTIDAD (IAM)

- Implementar MFA obligatorio en todos los sistemas críticos:
 - VPN corporativa
 - correo institucional
 - historia clínica electrónica (HCE)
 - plataformas administrativas
- Eliminar autenticación heredada (legacy authentication).
- Aplicar políticas de acceso condicional basadas en:
 - ubicación geográfica
 - dispositivo confiable
 - nivel de riesgo del usuario

Objetivo: evitar uso de credenciales robadas sin validación adicional

PROTECCIÓN DE CORREO ELECTRÓNICO



- Implementar filtros avanzados anti-phishing (ATP).
- Bloquear dominios recién creados o sospechosos (NRD filtering).
- Activar validación obligatoria de:
 - SPF
 - DKIM
 - DMARC
- Habilitar análisis de URLs en tiempo real (URL rewriting).
- Aislar adjuntos en entornos sandbox.

SEGURIDAD DE ACCESO A VPN Y PORTALES

- Restringir acceso a VPN por:
 - geolocalización
 - dispositivos registrados (MDM)
- Implementar Zero Trust Network Access (ZTNA).
- Deshabilitar accesos sin MFA en VPN y portales clínicos.
- Monitorear intentos de login anómalos en tiempo real.

ENDPOINT HARDENING (ESTACIONES DE TRABAJO)

- Bloquear almacenamiento de contraseñas en navegadores.
- Restringir ejecución de archivos descargados desde correo.
- Activar EDR con protección comportamental.
- Implementar control de scripts (PowerShell restringido).
- Habilitar logging avanzado en endpoints (Sysmon).

PROTECCIÓN CONTRA INFOSTEALERS



- Monitorear procesos de navegador con comportamiento inusual.
- Detectar accesos a perfiles de usuario y robo de cookies.
- Bloquear conexiones a dominios no reputados.
- Revisar tráfico HTTPS anómalo desde estaciones de trabajo.

INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE)

- Integrar feeds de phishing activo y dominios maliciosos.
- Bloquear dominios recién registrados (NRD).
- Actualizar listas IOC en firewall, proxy y SIEM.
- Correlacionar campañas activas de phishing sector salud.

CONCIENCIACIÓN Y FACTOR HUMANO

- Realizar campañas periódicas de simulación de phishing.
- Capacitar al personal clínico y administrativo en:
 - identificación de correos falsos
 - validación de enlaces
 - manejo seguro de credenciales
- Promover cultura de “verificación antes de hacer clic”.
- Establecer canal de reporte rápido de correos sospechosos.

GESTIÓN DE CREDENCIALES

- Aplicar rotación periódica de contraseñas críticas.
- Evitar reutilización de credenciales entre sistemas.
- Monitorear credenciales filtradas en bases externas.



- Deshabilitar cuentas inactivas o sin uso.

El éxito de estas campañas no depende de vulnerabilidades técnicas del sistema, sino de la explotación del usuario y el robo de identidad digital, por lo que la prevención debe centrarse en fortalecer la autenticación, reducir la superficie de ataque y aumentar la capacidad de detección temprana en todos los niveles de la infraestructura.

Recomendaciones de respuesta ante compromiso

En caso de sospecha o confirmación de compromiso asociado a campañas de phishing dirigido o robo de credenciales, es fundamental activar de inmediato el plan de respuesta a incidentes para contener el acceso no autorizado, evitar la propagación y proteger la información clínica y administrativa:

CONTENCIÓN INMEDIATA

- Bloquear inmediatamente las cuentas sospechosas o comprometidas.
- Revocar sesiones activas en:
 - VPN corporativa
 - correo institucional
 - sistemas clínicos y administrativos
- Forzar cierre de sesión en todos los dispositivos.
- Bloquear direcciones IP o ubicaciones asociadas a actividad anómala.
- Aislar estaciones de trabajo sospechosas de infección por infostealer.

Objetivo: detener el acceso del atacante de forma inmediata.

PRESERVACIÓN DE EVIDENCIA



- No apagar equipos comprometidos sin previa recolección de evidencia.
- Capturar:
 - logs de autenticación (AD / VPN / correo)
 - historial de accesos
 - registros del SIEM
- Extraer evidencia de endpoints:
 - procesos activos
 - conexiones de red
 - sesiones abiertas

Objetivo: garantizar trazabilidad del incidente para análisis forense.

ANÁLISIS Y VALIDACIÓN DEL COMPROMISO

- Identificar cuentas utilizadas en accesos no autorizados.
- Verificar accesos exitosos desde ubicaciones o dispositivos inusuales.
- Revisar uso de credenciales en múltiples sistemas simultáneamente.
- Analizar si hubo acceso a sistemas críticos (HCE, AD, VPN).

MITRE ATT&CK:

- T1078 – Valid Accounts
- T1041 – Exfiltration

ERRADICACIÓN DE LA AMENAZA

- Forzar cambio de credenciales en todas las cuentas comprometidas.



- Revocar tokens de sesión y cookies activos.
- Eliminar accesos persistentes en sistemas afectados.
- Bloquear dominios utilizados en campañas de phishing.
- Revisar y eliminar malware tipo infostealer en endpoints.

RECUPERACIÓN DE SISTEMAS

- Restaurar accesos seguros a los sistemas críticos.
- Verificar integridad de:
 - Active Directory
 - sistemas clínicos (HCE)
 - plataformas administrativas
- Reintegrar estaciones de trabajo solo tras validación de seguridad.
- Monitorear actividad post-incidente en SIEM.

ANÁLISIS DE IMPACTO

- Determinar alcance del compromiso:
 - usuarios afectados
 - sistemas accedidos
 - datos potencialmente expuestos
- Evaluar posible exfiltración de información sensible.
- Identificar si hubo movimiento lateral dentro de la red.

NOTIFICACIÓN Y ESCALAMIENTO

- Informar al equipo CSIRT / SOC inmediatamente.
- Escalar a líderes de TI e infraestructura.



- Notificar a áreas legales y de cumplimiento si aplica.
- En caso de datos personales:
 - notificar a la SIC (Colombia) según Ley 1581 de 2012

LECCIONES APRENDIDAS Y MEJORA CONTINUA

- Ajustar reglas de detección en SIEM basadas en el incidente.
- Fortalecer controles de MFA en sistemas críticos.
- Mejorar filtros de correo anti-phishing.
- Capacitar nuevamente al personal afectado.
- Revisar políticas de gestión de credenciales.

El compromiso por phishing no se limita a una sola estación de trabajo, sino que puede escalar rápidamente a un **compromiso de identidad institucional**, por lo que la respuesta debe enfocarse en la contención de credenciales, la visibilidad de accesos y la recuperación segura de los sistemas críticos del sector salud.

Conclusiones

La presente alerta de ciberseguridad evidencia una evolución significativa en las campañas dirigidas contra el sector salud, en las cuales el principal vector de ataque no corresponde a la explotación de vulnerabilidades técnicas tradicionales, sino al compromiso de la identidad digital de los usuarios mediante técnicas de phishing dirigido (spear phishing) y robo de credenciales.

Estas campañas demuestran un alto nivel de sofisticación, al combinar ingeniería social avanzada, suplantación de portales legítimos y el uso posterior de credenciales válidas para



acceder a sistemas críticos como VPN corporativas, correo institucional, plataformas de historia clínica electrónica (HCE) y servicios de autenticación centralizada.

El análisis permite concluir que el principal riesgo no radica únicamente en la obtención inicial de credenciales, sino en la capacidad del atacante para operar dentro del entorno como un usuario legítimo, lo que facilita el movimiento lateral dentro de la infraestructura hospitalaria, el acceso a información sensible y la posible escalación hacia sistemas de mayor criticidad como Active Directory.

En este contexto, el impacto potencial es alto debido a la interconexión de los sistemas del sector salud, lo que permite que un único compromiso de identidad pueda escalar hacia la afectación de múltiples servicios clínicos, administrativos y financieros, generando interrupciones operativas, fuga de información sensible y afectación de la continuidad del servicio de salud.

Asimismo, se identifica que la ausencia o debilidad en controles como la autenticación multifactor (MFA), la falta de segmentación de red, la limitada visibilidad en los sistemas de monitoreo (SIEM) y la baja concienciación del usuario final, incrementan significativamente la superficie de ataque y facilitan la ejecución exitosa de este tipo de campañas.

Se concluye que la mitigación efectiva de esta amenaza requiere un enfoque integral basado en defensa en profundidad, centrado en la protección de la identidad digital, el fortalecimiento de los controles de acceso, la implementación de monitoreo continuo y la capacidad de respuesta rápida ante incidentes de seguridad.

Finalmente, se recomienda a las organizaciones del sector salud fortalecer sus estrategias de ciberseguridad bajo el modelo de Zero Trust, priorizando la autenticación robusta, la detección temprana de accesos anómalos y la educación continua del personal, con el fin de reducir la probabilidad de compromiso y garantizar la protección de la información sensible de los pacientes.



Fuentes:

- MITRE ATT&CK Framework – Base de conocimiento oficial de técnicas de ataque utilizadas en campañas de phishing, robo de credenciales, movimiento lateral y compromiso de identidad en entornos corporativos y de salud.
o <https://attack.mitre.org/>
- CISA Cybersecurity Alerts & Advisories – Publicaciones oficiales sobre campañas activas de phishing, robo de credenciales, amenazas dirigidas a infraestructura crítica y recomendaciones de mitigación para entornos corporativos.
o <https://www.cisa.gov/news-events/cybersecurity-advisories>
- CISA Zero Trust Maturity Model – Guía oficial para la implementación de arquitecturas Zero Trust en organizaciones críticas, incluyendo el sector salud, con enfoque en identidad, acceso y segmentación.
o <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>
- Microsoft Security Intelligence & Defender Reports – Reportes oficiales sobre campañas de phishing, infostealers, robo de credenciales y ataques dirigidos a Microsoft 365, Active Directory y entornos Windows.
o <https://www.microsoft.com/en-us/security>
o <https://www.microsoft.com/en-us/security/security-insider>
- ENISA Threat Landscape (ETL) – Informes de inteligencia sobre amenazas globales que afectan sectores críticos como salud, incluyendo phishing, ransomware, robo de identidad





Alerta Vulnerabilidad

Campaña activa de phishing y robo de credenciales

CSIRTSALUD-AL-20260630-117

TLP: CLEAR

y ataques a infraestructuras digitales.
o <https://www.enisa.europa.eu/publications>

- ENISA Cybersecurity Guidelines for Health Sector – Lineamientos específicos de seguridad para el sector salud en Europa, enfocados en protección de datos, continuidad operativa y gestión de incidentes.
o <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health>

- Verizon Data Breach Investigations Report (DBIR) – Análisis global de incidentes de seguridad que confirma que el phishing y el uso de credenciales válidas son los vectores más comunes de compromiso inicial.
o <https://www.verizon.com/business/resources/reports/dbir/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

