Alerta

Técnica

Campaña activa de malware multivectorial

COLCERT AL-20260414 - 099

TIC

TLP:CLEAR

Resumen Ejecutivo

Se ha identificado una campaña de ciberataques activa y organizada que está afectando a entidades públicas y privadas en Colombia. **Esta campaña utiliza varios tipos de malware**, principalmente programas diseñados para robar información (infostealers) y herramientas de control remoto (troyanos de acceso remoto), **con el objetivo de obtener datos sensibles y tomar control de cuentas en la nube.**

El análisis realizado muestra que los atacantes están logrando evadir controles de seguridad tradicionales, incluso mecanismos como el Segundo Factor de Autenticación (MFA). Esto se logra mediante el robo de tokens de sesión de Azure AD, los cuales permiten acceder a servicios sin necesidad de ingresar usuario ni contraseña.

También se ha confirmado el compromiso de equipos de trabajo a través de medios físicos, como memorias USB, y medios digitales, como correos electrónicos dirigidos (spear phishing). Como resultado, los atacantes han obtenido credenciales completas de usuarios locales y de dominio, ampliando el alcance del compromiso.

Impactos principales identificados

Compromiso de identidades digitales: Obtención de sesiones activas de Microsoft 365, lo que permite acceder a servicios como OneDrive, SharePoint y Teams sin requerir credenciales adicionales.

Exfiltración de información confirmada: Transferencia de datos sensibles hacia servidores externos controlados por los atacantes, ubicados principalmente en Estados Unidos y Europa.

Mantenimiento del acceso en el tiempo: Creación de cuentas administrativas no autorizadas y de tareas automatizadas ocultas, utilizadas para conservar el acceso a los sistemas comprometidos incluso después de reinicios o cambios superficiales.

Contexto de la amenaza

La campaña identificada integra varias familias de malware con funciones complementarias, lo que sugiere la actuación de un actor con acceso a infraestructura de crimeware-as-a-service y un nivel técnico elevado. Los métodos utilizados para la entrega del malware, que incluyen correos electrónicos dirigidos (spear phishing) y el uso de dispositivos USB externos, incrementan significativamente la probabilidad de éxito del ataque al evadir controles de seguridad implementados de forma independiente.

Detalles de la Evolución Técnica

- Abuso de OAuth y Captura de Tokens (EvilTokens)
- Se ha confirmado el uso del kit PhaaS "EvilTokens" para capturar tokens Bearer de Azure AD mediante flujos de Device Code Grant. Esto permite a los atacantes acceder a M365, SharePoint y Teams eludiendo completamente el MFA (Multi-Factor Authentication).
- Malware Remoto y Persistencia (Remcos/Snake)
- La infraestructura utiliza servidores C2 en Psychz y Linode para distribuir Remcos RAT y Snake Keylogger. Se detectó la creación de tareas programadas denominadas SysUpdate y cuentas de respaldo (xavendnoe) para garantizar la persistencia en los sistemas afectados.
- Exfiltración por Múltiples Canales
- Los atacantes mimetizan su tráfico mediante protocolos legítimos. Se identificó exfiltración de datos biométricos vía Webhooks de Discord y transferencia de archivos críticos mediante SCP hacia servidores controlados en el extranjero.

NIVEL DE RIESGO

ALTO

COLCERT

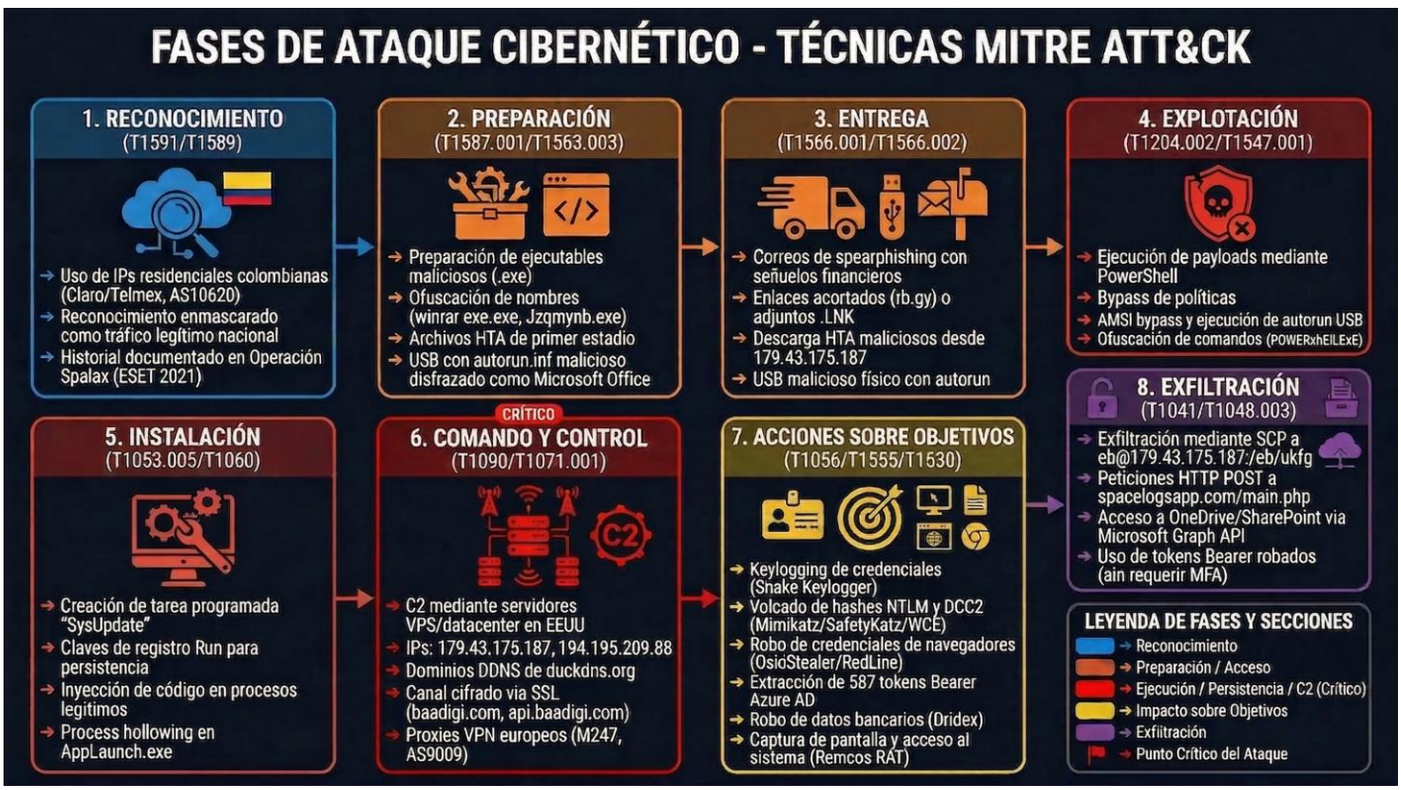
Mapeo táctico MITRE ATT&CK

A continuación, se presenta la tabla detallada de las Tácticas, Técnicas y Procedimientos (TTPs) identificadas en la campaña vinculada a chimaysl.com, mapeadas con el marco de MITRE ATT&CK.

Táctica	ID Técnica	Descripción Técnica Observada
Acceso inicial	T1566.001 / T1091	Spearphishing con enlaces acortados (rb.gy) y uso de medios extraíbles (USB) con autorun.inf malicioso
Ejecución	T1059.001	Uso intensivo de PowerShell ofuscado (ej. POWERshEll.ExE) con bypass de AMSI y políticas de ejecución.
Evasión de Defensa	T1548.002 / T1070	Bypass de UAC mediante ShimShady (Application Shimming) y auto-eliminación de artefactos tras la infección.
Acceso a credenciales	T1003.001 / T1539	Volcado de memoria LSASS con SafetyKatz y extracción de tokens de sesión web (Bearer tokens).
Comando y Control	T1071.001 / T1090	Uso de protocolos HTTPS/QUIC cifrados hacia infraestructura de Cloudflare y proxies europeos (M247).

Cadena de ataque (Kill Chain)

El flujo del ataque se divide en etapas críticas que permiten al atacante pasar de un compromiso local a una infiltración total en la nube institucional.



Familias de Malware identificadas

La campaña destaca por ser multivectorial, desplegando simultáneamente herramientas de control remoto y robo de información.

Malware	Tipo	Descripción Técnica Observada
Snake Keylogger / Noon	Infostealer	Captura de pulsaciones de teclado, robo de credenciales de navegadores (Chrome/Firefox) y exfiltración vía SMTP o Telegram.
Remcos RAT	Troyano de Acceso Remoto	Control total del sistema: acceso a cámara, micrófono, gestión de archivos y ejecución de comandos remotos. C2: 179.43.175.187.
Dridex	Banking Trojan	Especializado en el robo de credenciales bancarias mediante inyección web y facilitación de movimiento lateral en redes corporativas.
RedLine Stealer	Infostealer	Recolección de billeteras de criptomonedas, cookies de sesión, tokens de Discord y datos de autocompletado.
SafetyKatz / Mimikatz	Credential Dumper	Ejecución en memoria para volcar hashes NTLM y contraseñas en texto claro desde el proceso LSASS, evadiendo firmas de disco.

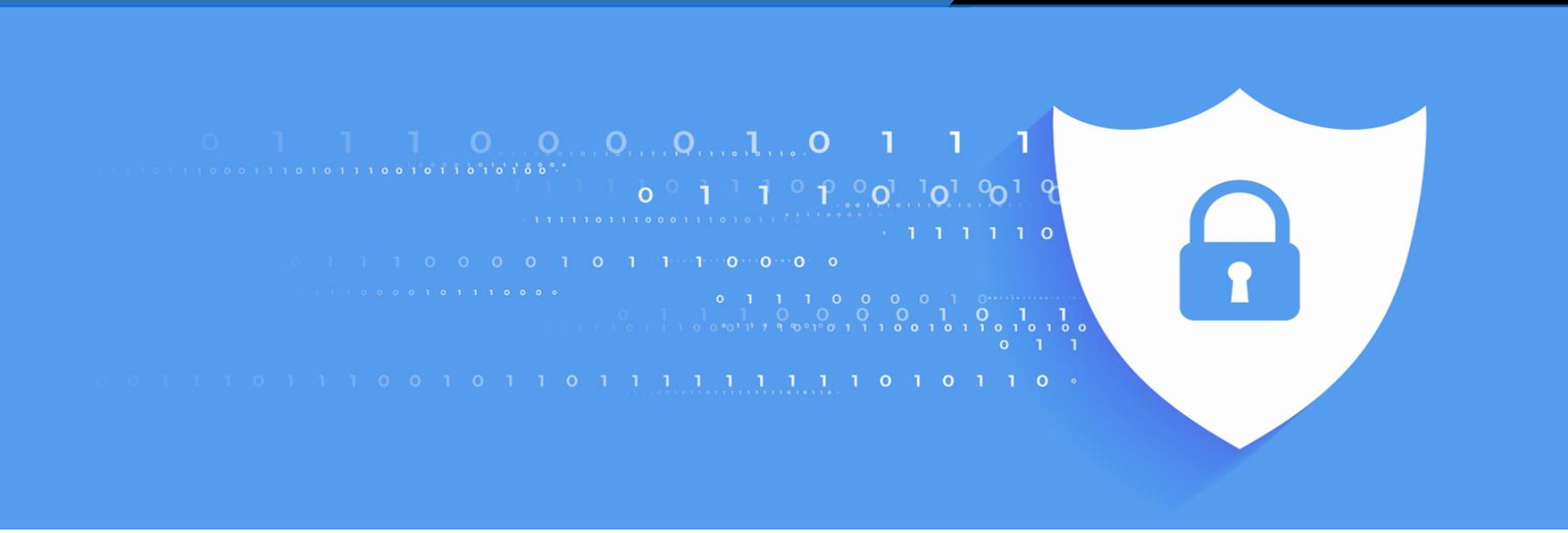
Indicadores de compromiso (IOCs)

Direcciones IP Maliciosas

Indicador (IP)	Función / Descripción Técnica	Descripción
179.43.175.187	TServidor C2 Primario (Remcos/Snake). RAT + servidor SCP de exfiltración. Descarga de 1zqmynb.exe y loaders HTA.	Psychz Networks (EE.UU.). Altamente activo
194.195.209.88	Distribución de Payloads (applauchh.exe). C2 Dridex banking trojan via PowerShell wget.	. Akamai/Linode. Aloja paneles de control maliciosos.
45.144.174.31	Proxy / Nodo de Anonimización. Clasificado como Alto Riesgo.	M247 Europe SRL.
181.53.13.247	Reconocimiento / C2 Enmascarado. Asociado a Operación Spalax.	Asociado a infraestructura de ataque.
104.21.42.149	Endpoint de Phishing (Cloudflare). Destino de tráfico C2 cifrado para chimaysl.com.	Infraestructura Cloudflare.
96.47.234.132	C2 secundario / descarga de tubw22.vbs (loader VBScript).	10_malware_artifacts.txt
23.95.52.140	C2 adicional — posible Cobalt Strike Team Server. Path / office/doc8 camufla tráfico como O365.	docx base + memdump
177.253.81.30	IP atacante Azure Portal: registro app OAuth maliciosa + creación cuenta licenciamiento + 74 mods GPO.	AuditLogs_2026-04-08.csv
200.10.164.43	IP adicional en sesiones interactivas en O365.	InteractiveSignIns.csv
198.12.89.24	Servidor payload Stage 2 (Vultr AS20473). Aloja cosse.exe (/312/) y C2 alternativo (/xampp/kvrmot).	Vultr Holdings, LLC

Dominios y URLs

Tipo	Indicador	Descripción	Confianza / Riesgo
URL	http://179.43.175.187/zqde/Jzqmynb.exe	Descarga Remcos RAT via PowerShell wget con obfuscación de mayúsculas (POWERShEll.ExE)	ALTA
URL	http://194.195.209.88/applauchh.exe	Descarga Dridex banking trojan via PowerShell wget	ALTA
URL	http://96.47.234.132/tubw22.vbs	Descarga VBScript loader	MEDIA
URL_SCP	scp://179.43.175.187/eb/ukfg	SCP → %appdata%\dnli.hta (HTA loader Stage 2) . Clave SSH pre-configurada.	ALTA
URL_SCP	scp://179.43.175.187/bb/mkt	SCP → %appdata%\ltq.hta (HTA loader alternativo)	ALTA
URL	http://198.12.89.24/312/cosse.exe	Descarga cosse.exe (payload Stage 2) desde servidor Vultr.	ALTA
URL	http://198.12.89.24/xampp/kvrmot	Panel de control o C2 adicional en XAMPP malicioso	ALTA
URL_C2	https://23.95.52.140/office/doc8	C2 Lumma Stealer. Path /office/doc8 camufla tráfico como comunicación de Office 365	ALTA
Dominio DDNS — C2	primeserver13.duckdns.org	Vinculado a 179.43.175.187. Subdominio dinámico — táctica C2 común para resistir bloqueos.	CRÍTICO — ALTA
Dominio DDNS — Phishing	accounting-invoices.duckdns.org	Temática financiera/contable. Señuelo para entidades con funciones de facturación o contratos.	ALTO — ALTA
Dominio DDNS — Distribución	privatemyhost.duckdns.org	Infraestructura de distribución de payloads desde 179.43.175.187.	ALTO — ALTA
Dominio DDNS — C2 alternativo	julytimeshow.duckdns.org	Canal C2 alternativo asociado a la misma infraestructura.	ALTO — MEDIA
Dominio C2 — SSL activo	baadigi.com / api.baadigi.com	Dominio de C2 con SSL Let's Encrypt activo. Cert. vence 21/04/2026. Vinculado a 194.195.209.88.	CRÍTICO — ALTA
Panel de control C2	admin.baadigi.com	Panel administrativo del C2. SSL activo hasta 21/04/2026. Monitorear crt.sh para renovación.	CRÍTICO — ALTA
Dominio exfiltración	spacelogsapp.com	Receptor de datos robados por applauchh.exe. Peticiones POST a /main.php y archivos falsos .jpg.	CRÍTICO — ALTA
Dominio infraestructura	yourtryinc.com / gragorian.com	Dominios asociados a 194.195.209.88. Infraestructura de soporte de la campaña.	ALTO — MEDIA
URL corta — Distribución	https://rb.gy/m7fdot	Redirige a bayfiles.com/x9nf68ycy8 → Vir.exe. Técnica de evasión de filtros de correo.	ALTO — ALTA
URL descarga — Payload	https://bayfiles.com/x9nf68ycy8	Vir.exe alojado en BayFiles. Nombre altamente sospechoso. 2 detecciones activas	ALTO — ALTA



Dominios C2 — Infraestructura de Ataque)

Tipo	Indicador	Descripción	Fuente	Confianza
Dominio_C2	smonstr.ru	C2/Loader TLD .ru – infraestructura rusa. Correlacionado campaña ingforever7	CTI / correlación externa	ALTA
Dominio_C2	snlyjkf3vs.ru	C2/Exfil TLD .ru – nombre generado algorítmicamente (posible DGA). Infraestructura de respaldo	CTI / correlación externa	ALTA
Dominio_C2	snovimgodomyap.ru	C2 TLD .ru – contiene frase rusa 'S Novym Godom' (Feliz Año Nuevo). Patrón APT28/APT29	CTI / correlación externa	ALTA
Dominio_C2	snitchlittle.info	C2/Phishing TLD .info – posible panel de control o landing page de phishing	CTI / correlación externa	MEDIA
Dominio_C2	check-up.co	Dominio correlacionado con infraestructura de la campaña. Posible redirector	CTI / correlación externa	MEDIA
Dominio_C2	baadigi.com	Dominio correlacionado con infraestructura de la campaña	CTI / correlación externa	MEDIA
Dominio_C2	accounting-invoices.duckdns.org	DDNS como C2 dinámico. Nombre simula tráfico financiero legítimo para evasión	CTI / correlación externa	MEDIA

Hashes de archivos (SHA-256)

Tipo	Indicador (Hash SHA-256 / Nombre)	Archivo / Nombre	Veredicto / Descripción	Confianza
Hash_SHA256	938f4e648e57b9ad6d41ea3fe8707c0f249ba2baa24a5af557b4f09d698b8145	Jzqmynb.exe	MALICIOSO — Noon/Remcos RAT (54/71 motores). Descargado desde 179.43.175.187/zqde/	ALTA
Hash_SHA256	0e72b4f27dad0e0746e3b2793e39af55936f6a0e112c9035decf92de51f7a622	applauchh.exe	MALICIOSO — OskiStealer / Agent Tesla / RedLine (37/69 motores). Descargado desde 194.195.209.88	ALTA
Hash_SHA256	b663321ab439cc53a329ee352c1b855d9998d3af95524a05795a88b42a9acf07	(payload asociado)	MALICIOSO — Variante infostealer. Asociado a 194.195.209.88	ALTA
Hash_SHA256	ed6f6f2144998175c846a99d2a0faab5bf7b6ace318f0fe2dc4bfeaf4700c1d8	(payload asociado)	MALICIOSO — Variante infostealer. Asociado a 194.195.209.88	ALTA
Hash_SHA256	fb47468a2cd3953c7131431991afcc6a2703f14640520102eea0a685a7e8d6de	(payload asociado)	MALICIOSO — Variante infostealer. Asociado a 194.195.209.88	ALTA
Hash_SHA256	b663321ab439cc53a329ee352c1b855d9998d3af95524a05795a88b42a9acf07	Winrar.exe	Variante de infostealer ofuscada	ALTA
Hash_SHA256	e857298fd2f8d1c7d48780769433f33e7b3ceaae5ea5a74c13ce8c10bcc7b690	cen.exe (1.4 MB)	Muestra en cuarentena MDE. Familia pendiente de sandbox	ALTA
Hash_SHA256	c613d3ed427c81b9b61ea145bf6a5faa63bf3e48c38e5f47e053f8571c248416	R729u_PRO.exe (114 KB)	Muestra en cuarentena MDE. Familia pendiente	ALTA
Hash_SHA256	80b26c00a67c38c49049dbb850d1f98eaa905e22b11c5270d96fbda2adda72a0	SE.exe (388 KB)	Muestra en cuarentena MDE. Posible herramienta de escalada	ALTA
Hash_SHA256	f682aadda9deb654885ae17909380a25f7cb1a43ac0934ac425ee8de4924c7f3	cmd.exe TROJANIZADO (344 KB)	Reemplaza binario legítimo del sistema operativo	ALTA
Driver	ad_driver.10.sys	ad_driver.10.sys	Controlador de kernel — instalado como servicio ad_driver10 desde %TEMP% de csepulveda. Hash SHA256 pendiente. NOTA: posiblemente driver legítimo de FTK Imager — verificar	MEDIA
Firma_AV	!#SCPT:Trojan:Win32/LummaStealer45.GPIM!MTB	—	Firma Lumma Stealer en strings del pagefile.sys de WSCANCIL6892	ALTA
Firma_AV	TrojanDownloader:PowerShell/SnakeKeyLogger.DF!MTB	—	SnakeKeyLogger variante PowerShell — keylogger + downloader.	ALTA
Firma_AV	Trojan:PowerShell/LummaStealer.AC!MTB	—	Lumma Stealer variante PowerShell (AC).	ALTA
Firma_AV	SCPT:Trojan:PowerShell/LummaStealer.AC101	—	Lumma Stealer variante AC101 — específica documentada en VirusTotal	ALTA
Archivo	(Hash SHA256 pendiente de sandbox)	cosse.exe	Binario Stage 2 descargado desde 198.12.89.24/312/. Hash SHA256 pendiente de sandbox	ALTA

Medidas preventivas de detección en registros

Microsoft Entra ID / Unified Audit Log

- ❑ **Filtrar por protocolo Device Code:** Buscar eventos UserLoggedIn donde el protocolo sea Device Code, con IPs originando desde ubicaciones anómalas o resoluciones vinculadas a los IoCs.
- ❑ **Token Replay:** Identificar el uso de tokens desde direcciones IP diferentes a las del inicio de sesión original.
- ❑ **Registro de dispositivos fraudulentos:** Alertar sobre eventos Add device o Register device en Entra ID en horarios inusuales o desde IPs no reconocidas.
- ❑ **Habilitar protección de Tokens (Token Protection):** Active esta funcionalidad para vincular criptográficamente los tokens al dispositivo del usuario, impidiendo que los atacantes usen los tokens robados desde su propia infraestructura (como las IPs de Cloudflare o Railway analizadas) .
- ❑ **Restringir el Consentimiento de Aplicaciones:** Configure las políticas de consentimiento para que los usuarios no puedan autorizar aplicaciones de terceros que soliciten permisos de alto privilegio (como Mail.Read o Notes.Read.All) sin la aprobación explícita de un administrador.

Registros de Red y DNS

- ❑ **Monitoreo DNS Wildcard:** Configurar alertas para cualquier consulta DNS hacia *.chimaysl.com.
- ❑ **Inspección TLS por SNI:** Dado el uso de Cloudflare como escudo, filtrar el campo SNI (Server Name Indication) en el tráfico TLS saliente buscando la cadena chimaysl.com.

Recomendaciones

❑ Revocar todas las sesiones activas en Microsoft Entra ID / Azure AD.

Para entidades con Microsoft 365: Revocar tokens en Entra ID (portal.azure.com → Usuarios → Revocar sesiones). Buscar accesos no autorizados a SharePoint/OneDrive/Teams. Monitorear logs de Azure AD para actividad de cuentas sospechosas (especialmente fuera de horario laboral). Los tokens Bearer tienen vida útil de 60-90 min; actuar antes de que expiren.

❑ Deshabilitar puertos USB en equipos sensibles.

Implementar política de restricción de dispositivos USB vía GPO o solución MDM en equipos de usuarios con acceso a información sensible. El vector USB confirmado en este incidente es altamente efectivo contra controles de red y correo.

❑ Buscar indicadores de compromiso en endpoints.

En todas las estaciones de trabajo: Buscar tarea programada "SysUpdate" y eliminar. Buscar archivos en AppData\Roaming con nombres similares a "winrar" y variantes. Revisar claves de registro Run/RunOnce para entradas sospechosas. Buscar procesos AppLaunch.exe con origen no legítimo (señal de process hollowing por applauchh.exe).

❑ Fortalecer la seguridad de Microsoft 365 y Azure AD.

Implementar o revisar: Acceso Condicional con requisitos MFA para todos los usuarios. Política de vida útil de tokens reducida (recomendado: 1 hora o menos para tokens de acceso). Habilitación de Microsoft Defender for Identity para detección de Pass-the-Hash y Pass-the-Ticket. Revisión de permisos de aplicaciones de terceros en el tenant.

❑ Implementar controles contra USB y medios extraíbles.

Definir política corporativa de control de acceso a dispositivos USB con excepciones aprobadas. Evaluar soluciones de DLP (Data Loss Prevention) para endpoints. Capacitar a usuarios sobre el riesgo de USB encontrados o recibidos sin solicitar.

Fuentes

COLCERT-20260203-092: Alerta — Sofisticación de Phishing con robo biométrico – IoCs.

https://www.colcert.gov.co/800/articles-426289_COLCERT_AL__20260203__092_Alerta_sofisticacion_de_Phishing_con_robo_biometrico__IoCs.pdf

ColCERT AL-20251215-088: Alerta — Campaña de Kits de Phishing en Colombia (Tycoon 2FA, EvilProxy, Mamba).

https://www.colcert.gov.co/800/articles-425747_COLCERT_AL20251201__087_Alerta_vulnerabilidad_en_chat_externo_de_Microsoft_Teams.pdf

Microsoft Security Blog. (2026, 6 de abril). Inside an AI-enabled device code phishing campaign.

https://www.microsoft.com/en-us/security/blog/2026/04/06/inside-an-ai-enabled-device-code-phishing-campaign/

Sekoia.io TDR. (2026). EvilTokens Launches New Phishing Service Targeting Microsoft Accounts.

https://blog.sekoia.io/eviltokens-launches-new-phishing-service-targeting-microsoft-accounts/

The Hacker News. (2026, 25 de marzo). Device Code Phishing Hits 340+ Microsoft 365 Orgs Across Five Countries via OAuth Abuse.

https://thehackernews.com/2026/03/device-code-phishing-hits-340-microsoft.html

Proofpoint Threat Research. (2025, 22 de diciembre). Phishing Attacks Exploit OAuth Device Codes to Breach Microsoft 365 Accounts.

https://www.proofpoint.com/us/blog/threat-insight/phishing-attacks-exploit-oauth-device-codes-breach-microsoft-365-accounts

KnowBe4 Threat Labs. (2026, 23 de febrero). Threat Actors Target Microsoft 365 Accounts In OAuth Token Theft Operation.

https://blog.knowbe4.com/threat-actors-target-microsoft-365-accounts-in-oauth-token-theft-operation

Barracuda Networks Blog. (2025, 22 de enero). Threat Spotlight: kit de phishing Tycoon 2FA actualizado para evadir la inspección.

https://es.blog.barracuda.com/2025/01/22/threat-spotlight-tycoon-2fa-phishing-kit

Barracuda Networks Blog. (2025, 19 de marzo). Threat Spotlight: Un millón de ataques Phishing como servicio en dos meses.

https://es.blog.barracuda.com/2025/03/19/threat-spotlight-phishing-as-a-service-fast-evolving-threat

MITRE Corporation. MITRE ATT&CK® Framework — Enterprise Matrix.

https://attack.mitre.org/

Google Threat Intelligence / VirusTotal. Telemetría global para validación de reputación de infraestructura y atribución de tácticas de actores de amenaza.

MITRE Corporation. (s.f.). MITRE ATT&CK Framework.

https://attack.mitre.org

ESET. (2021). Operación Spalax: ataques de malware dirigidos en Colombia. ESET Research.

https://www.welivesecurity.com/la-es/2021/01/12/operacion-spalax-ataques-malware-dirigidos-colombia/

ESED-SL. (2020). Snake Keylogger: qué es, cómo funciona y cómo de peligroso es. ESED Security Lab.

https://www.esedsl.com/blog/snake-keylogger