31/03/2022

Alerta de Seguridad Digital

[TLP: GREEN]
[PAP: WHITE]

Modus Operandi Grupo Lapsus$

El surgimiento de nuevos actores de amenazas en el mundo de la ciberseguridad es cada vez más notable conforme incrementa la industria TI en el mundo; este boletín realiza un acercamiento del grupo conocido como ***Lapsus$***, el cual, desde el mes de marzo del presente año, ha comprometido compañías como NVIDIA y SAMSUNG.

Se presume que el grupo ***Lapsus*** opera directamente en sedes en América Latina, específicamente desde Brasil; recientemente en su foro en Telegram, cuestionan acerca de la preferencia de los asistentes de si exponer código fuente de Vodafone o de mercado Libre, las respuestas evidenciaron rápidamente la predilección por la empresa de telecomunicaciones Vodafone (Figura 1).

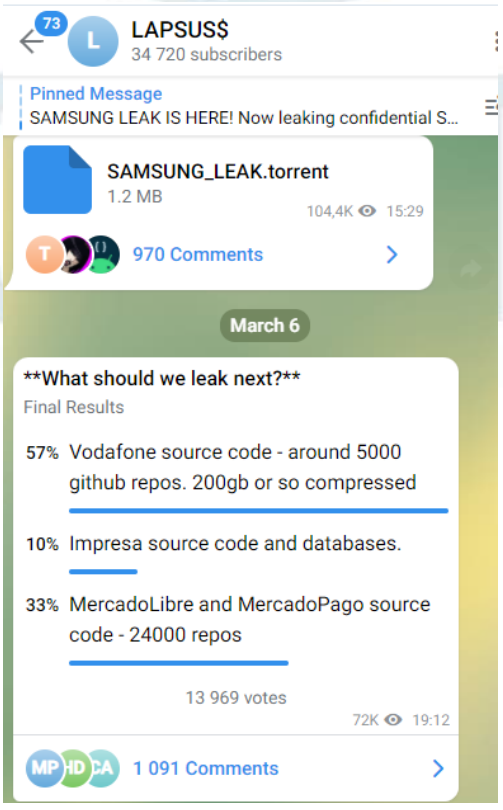

Figura 1. *Encuesta de ataque. Fuente: Grupo de Telegram de Lapsus$*

El modus operandi consiste en infiltrarse en redes objetivo ya sea a través de funcionarios con privilegios en la entidad blanco (ver figura 2), exfiltrar información sensible y proceder a extorsionar a la entidad para no publicar la información captada.

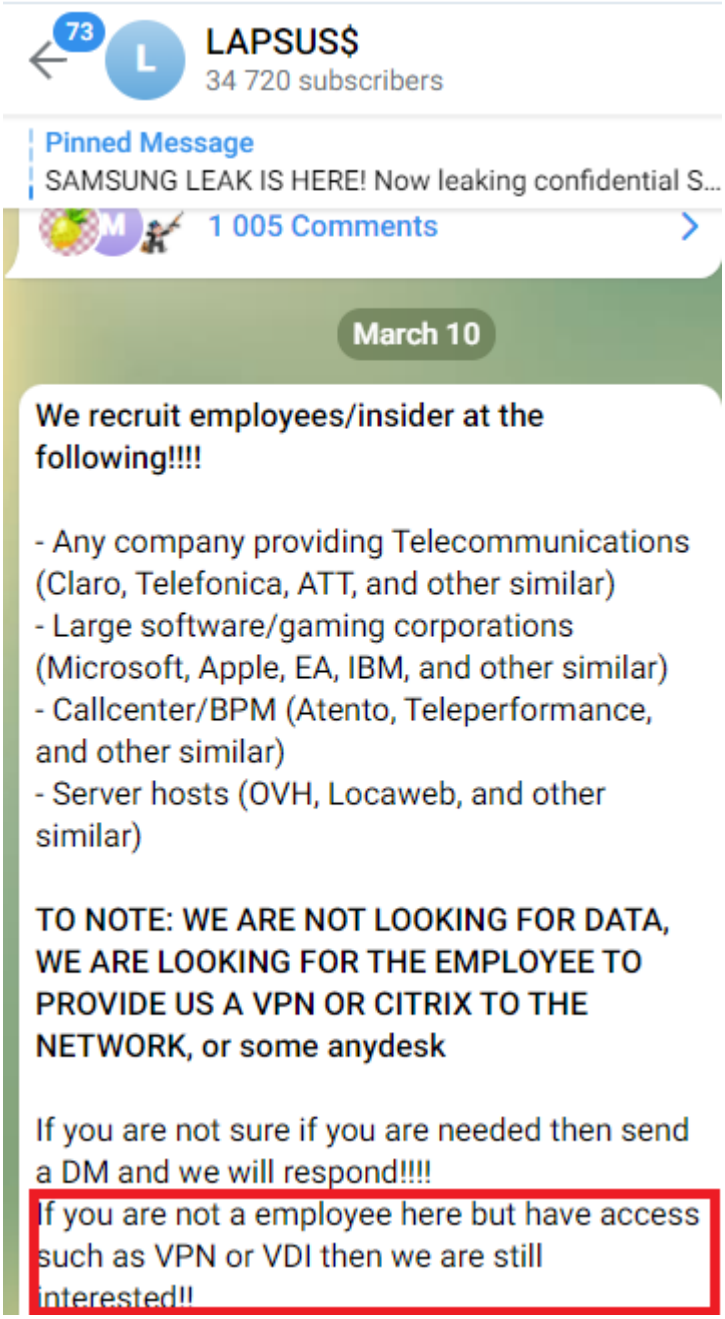

Figura 2. *Próximos objetivos de Lapsus, búsqueda de insiders con acceso a VPN corporativa. Fuente: Grupo de Telegram de Lapsus$*

Historial delictivo

Aunque este grupo ha estado en la mira desde el año 2020, se materializaron sus intenciones en el año 2021 al atribuirse el ataque hacia el ministerio de salud de Brasil; en esta oportunidad, afectaron entidades y servicios en línea, borrando datos de vacunación de covid-19 e interrumpiendo la emisión de certificado digital de vacunación para los ciudadanos.

Hacia finales del año 2021, Lapsus$ toma el control de una de las cuentas verificadas en Twitter de Expresso, uno de los periódicos más renombrados en Portugal para autoproclamarse presidente del país. También enviaron mensajes de correos electrónicos phishing a los suscriptores del periódico, informado acerca de la supuesta muerte del presidente de Portugal.

Figura 3. *Comprometimiento de una cuenta de Twitter. Fuente: Twitter.*

Realiza también un ataque a Impresa, desfigurando varios sitios web y situando la nota de rescate en cada página de inicio informando acerca de la presunta toma de control sobre la cuenta de Amazon Web Services (AWS) de Impresa.

Figura 4. *Defacement y nota de rescate en Impreso.*

Perfil del grupo

- Exfiltración de datos sensibles, eliminación de máquinas virtuales y alteración de registros DNS A.
- Primer enfoque en lugares de habla portuguesa, pero ha escalado hacia otros objetivos a nivel mundial.
- Inicialmente ha realizado sus ataques con ransomware en donde no solo cifra la información exfiltrada, sino que sustrae datos confidenciales.
- Compromete la red al realizar una primera intrusión a través de credenciales legítimas de VPN.
- Se cree que las sedes principales se encuentran en América del Sur y Europa.
- Enfoque en organizaciones gubernamentales y medios de comunicación masivos.
- Establecimiento de contacto con funcionarios y exempleados de las entidades objetivo para comprar acceso a la red corporativa.

Herramientas usadas en la campaña

- **MMIKATS**: Su principal función es exfiltrar credenciales a través de la inyección de procesos en Windows, particularmente se enfoca en la extracción de credenciales del Servicio Windows
- Local Security Authority Subsystem (LSASS), escalado de privilegios y manipulación de servicios.
- **METASPLOIT**: Framework de explotación que incluye prueba de vulnerabilidad, enumeración de red, generación y ejecución de payload y evasión de defensa, muy usado para desarrollar cargas útiles de etapa para descargar y ejecutar puertas traseras.
- **DOUBLEJUMP**: Utilería pública que explota la vulnerabilidad *CVE-2022-21919* encargada de escalar privilegios en entornos Windows.

- **PROCESSHACKER**: Monitoreo y controla recursos de sistema; muy similar al administrador de tareas.

A continuación, se detallan las tácticas, técnicas y procedimientos de esta campaña.

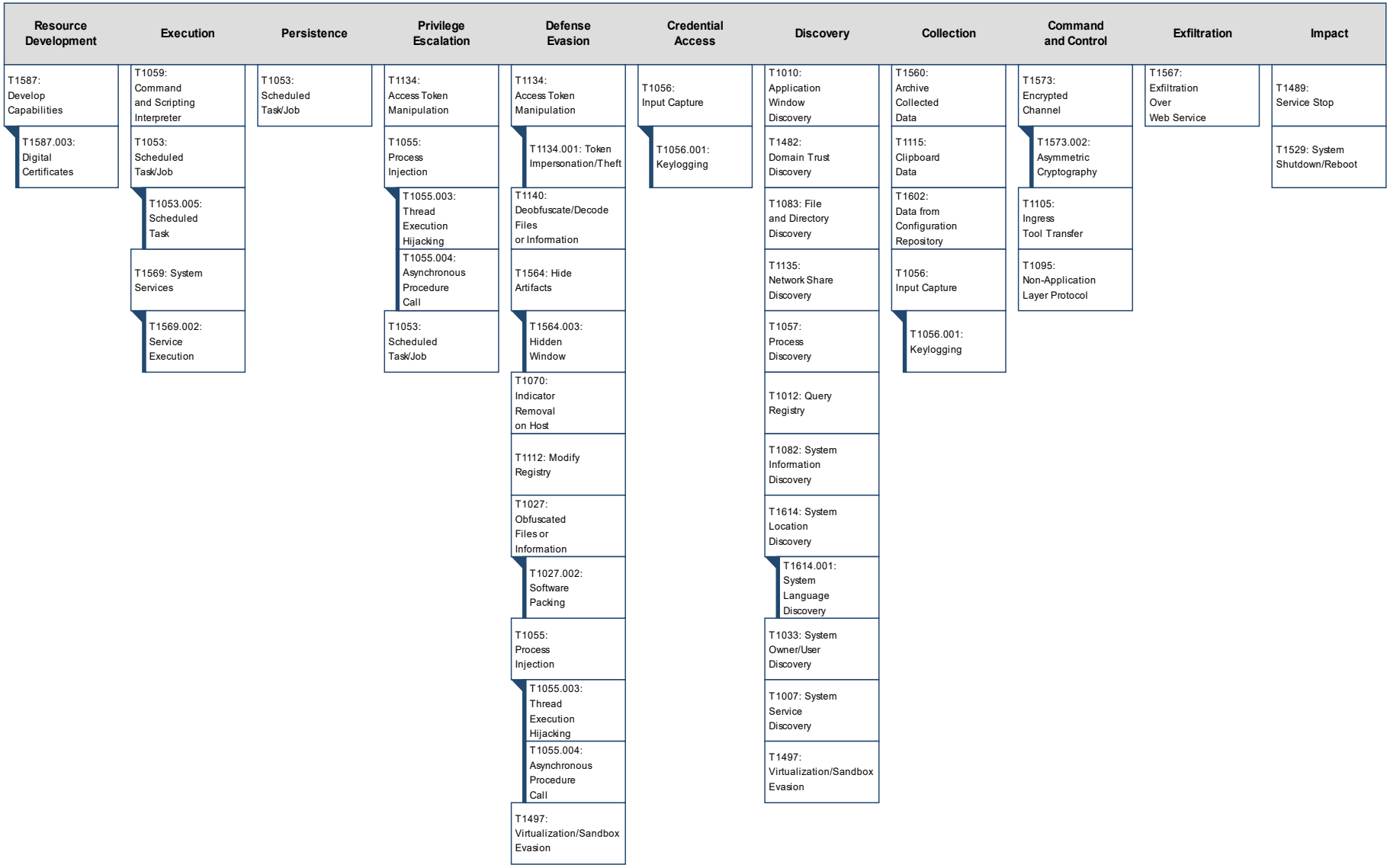

Diagrama 1. *ATT&CK grupo Lapsus. Fuente: MITRE ATT&CK®*

Recomendaciones

- Realizar periódicamente la evaluación de la postura de seguridad de los servicios expuestos hacia internet frente a los mecanismos de autenticación para los usuarios.
- Implemente copias de seguridad periódicas y actualizadas de modo que haya disponibilidad sobre la última versión de los datos. Salvaguarde dichas copias de seguridad de modo que no puedan ser modificadas o manipuladas.
- Implemente la segmentación de red, de manera que no se pueda acceder a los equipos de red desde todos los equipos.
- Parchee sistemas operativos, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.
- Bloquee los Indicadores de compromiso (IOC) mencionado en esta alerta en sus dispositivos perimetrales.
- Si es contactado por el grupo, por favor no cancele el rescate estipulado, ya que esto patrocina las actividades maliciosas de los ciberdelincuentes. Por favor contacte inmediatamente a colCert y Csirt Gobierno para dar trámite al incidente.
- Implemente una política organizacional en donde se deba cambiar constantemente las credenciales de las diferentes **plataformas y VPN** a cargo del personal.
- Al desvincularse un empleado o funcionario de la entidad, por favor realice inmediatamente la eliminación del perfil; así mismo si el colaborador cambia de rol dentro de la organización.
- Realice un seguimiento desde las primeras etapas de desarrollo de un aplicativo, programa o sitio web, esto con el fin de evitar brechas de seguridad.

- **Referencias**

[1] MITRE ATT&CK®

Contáctanos

Si tienes alguna consulta técnica comunicarse con ColCERT/CSIRT Gobierno a través de los siguientes canales:

Bogotá: 601 344 22 22
Línea Gratuita Nacional: 018000952525 Op 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT

Hechos QUE CONECTAN