Nro. Alerta:	EC-2023-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-feb-2023	**HACKERS CHINOS APUNTAN A ENTIDADES DIPLOMÁTICAS SUDAMERICANAS CON SHADOWPAD**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Backdoor - Filtración Información
Nivel de riesgo: Alto

II. ALERTA.

Microsoft atribuyó a un actor de ciber espionaje con sede en China una serie de ataques dirigidos a entidades diplomáticas en América del Sur.

El equipo de inteligencia de seguridad del gigante tecnológico está rastreando el grupo bajo el apodo emergente ***"DEV-0147"***, describiendo la actividad como: una "expansión de las operaciones de filtración de datos del grupo que tradicionalmente se dirigían a agencias gubernamentales y grupos de expertos en Asia y Europa".

III. INTRODUCCIÓN.

Se dice que el actor de amenazas utiliza herramientas de piratería establecidas, como: ***"ShadowPad"***, para infiltrarse en los objetivos y mantener el acceso persistente.

ShadowPad, también llamado ***PoisonPlug***, es un sucesor del troyano de acceso remoto PlugX y ha sido ampliamente utilizado por colectivos adversarios chinos con vínculos con el Ministerio de Seguridad del Estado (MSS) y el Ejército Popular de Liberación (PLA), según Secureworks.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-feb-2023	**HACKERS CHINOS APUNTAN A ENTIDADES DIPLOMÁTICAS SUDAMERICANAS CON SHADOWPAD**	V 1.1

Investigaciones adicionales mostraron que la fuente de estas solicitudes era un *software* de control de servidores producido por una compañía legítima y utilizado por cientos de clientes en industrias como las de servicios financieros, educación, telecomunicaciones, manufactura, energía y transporte. El hallazgo más preocupante era el hecho de que el proveedor no tenía intenciones de que el *software* realizara estas peticiones.

Hasta ahora, de acuerdo con la investigación de **Kaspersky Lab**, el módulo malicioso se ha activado en Hong Kong**,** mientras que **el *software* troyanizado ha sido detectado en varios países de América Latina, incluyendo: Brasil, Chile, Colombia, México y Perú.** Sin embargo, el módulo malicioso podría estar latente en muchos otros sistemas en todo el mundo, especialmente si los usuarios no han instalado la versión actualizada del software afectado.

ShadowPad es un ejemplo de lo peligroso y extenso que puede ser un ataque exitoso en la cadena de suministro. Con las oportunidades de alcance y recopilación de datos que da a los atacantes, lo más probable es que se reproduzca una y otra vez con algún otro componente de *software* ampliamente utilizado.

ShadowPad, es una puerta trasera plantada en el software, para el control de servidores que utilizan cientos de empresas en todo el mundo. Al activarse la puerta trasera, permite a los atacantes descargar módulos maliciosos o robar datos.

En julio de 2017, el equipo de Investigación y Análisis Global (**GReAT**) de **Kaspersky Lab** fue contactado por uno de sus socios, una institución financiera. Los especialistas en seguridad de la organización estaban preocupados por unas solicitudes sospechosas de **DNS** (servidor de nombres de dominio) originadas en un sistema que intervenía en el proceso de transacciones financieras.

Según Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para **Kaspersky Lab América Latina**, este ataque traspasa los mecanismos de seguridad, lo que le facilita a los atacantes acceso a máquinas de administración de la red, servidores, etc. “Los atacantes llegan a ser intrusos indetectables ya que con las mismas herramientas legitimas de administración del cliente troyanizado, pueden llegar a tener el control de sistemas críticos como servidores, estaciones de trabajo, archivos, etc. y extraer información, robar contraseñas, base de datos o simplemente espiar la actividad de sus víctimas”.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-feb-2023	**HACKERS CHINOS APUNTAN A ENTIDADES DIPLOMÁTICAS SUDAMERICANAS CON SHADOWPAD**	V 1.1

IV. VECTOR DE ATAQUE

Una de las herramientas maliciosas utilizadas por DEV-0147 es un cargador de paquetes web llamado ***"QuasarLoader"***, que permite implementar cargas útiles adicionales en los hosts comprometidos.

"Los ataques de DEV-0147 en Sudamérica incluyeron actividad posterior a la explotación que involucró el abuso de la infraestructura de identidad local para reconocimiento y movimiento lateral, y el uso de Cobalt Strike para comando y control (C&C) y filtración de datos", dijo Microsoft.

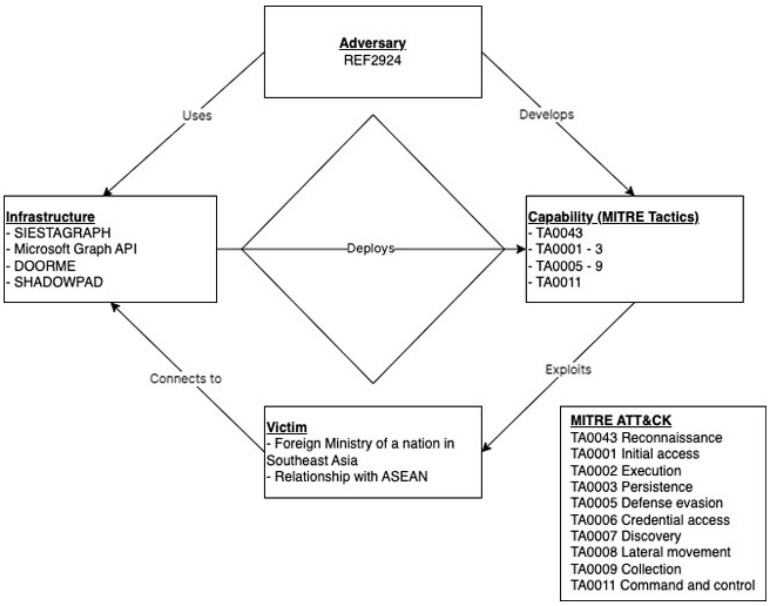

Fig.1. Diagrama de flujo de ataque con ShadowPad

DEV-0147 está lejos de ser la única amenaza persistente avanzada (APT), desarrollada en China que aprovecha ***ShadowPad*** en los últimos meses. En septiembre de 2022, NCC Group descubrió detalles de un ataque dirigido a una organización no identificada que abusó de una falla crítica en WSO2 **(CVE-2022-29464, puntaje CVSS: 9.8)** para soltar shells web y activar una cadena de infección que condujo a la entrega de ***ShadowPad*** para recopilación de inteligencia.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-feb-2023	**HACKERS CHINOS APUNTAN A ENTIDADES DIPLOMÁTICAS SUDAMERICANAS CON SHADOWPAD**	V 1.1

V. IMPACTO.

ShadowPad también ha sido empleado por actores de amenazas no identificados en un ataque dirigido a un ministerio de relaciones exteriores miembro de la ASEAN a través de la explotación exitosa de un Microsoft Exchange Server vulnerable y conectado a Internet.

Se ha observado que la actividad, denominada: REF2924, por Elastic Security Labs, comparte asociaciones tácticas con las adoptadas por otros grupos de estados-nación como Winnti (también conocido como APT41) y ChamelGang.

El conjunto de intrusión REF2924 representa un grupo de ataque que parece centrarse en prioridades que, cuando se observan en todas las campañas, se alinean con un interés estratégico nacional patrocinado.

El hecho de que los grupos de hackers chinos sigan usando ***ShadowPad*** a pesar de estar bien documentado a lo largo de los años sugiere que la técnica está teniendo cierto éxito.

VI. RECOMENDACIONES.

Es importante resaltar que hoy en día, una compañía de cualquier sector puede ser víctima de un ataque avanzado simplemente por usar un *software* comúnmente utilizado a nivel mundial. Esto hace que países de Latinoamérica, de una forma automática, lleguen a estar también en lista de objetivos potenciales de atacantes que operaran desde o fuera de la región".

Sin embargo, este caso muestra que las grandes empresas deben confiar en soluciones avanzadas capaces de vigilar la actividad de la red y detectar anomalías. Es aquí donde usted puede detectar la actividad maliciosa, incluso si los atacantes fueran lo suficientemente avanzados como para ocultar su *malware* dentro de un *software* legítimo".

Se recomendó a los usuarios actualizarse inmediatamente a la versión más reciente del software **NetSarang**, del cual se ha eliminado el módulo malicioso, y comprobar si en sus sistemas hay peticiones de **DNS** a dominios no habituales.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-feb-2023	**HACKERS CHINOS APUNTAN A ENTIDADES DIPLOMÁTICAS SUDAMERICANAS CON SHADOWPAD**	V 1.1

VII. DESCARGO DE RESPONSABILIDAD.

La información en la presente alerta; se proporciona solo con fines informativos. El EcuCERT de la ARCOTEL, no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.

Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT de la ARCOTEL.

La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS.

- https://thehackernews.com/2023/02/chinese-hackers-targeting-south.html
- https://www.infosecurity-magazine.com/news/chinese-shadowpad-infiltrate-south/
- https://unaaldia.hispasec.com/2020/02/shadowpad-la-nueva-variante-del-malware-winnti.html
- https://www.secureworks.com/research/shadowpad-malware-analysis
- https://www.adaptixnetworks.com/shadowpad-puerta-trasera-plantada-software/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec