Alerta de Seguridad Informática (2CMV-00013-002)

Nivel de Riesgo: Alto

Tipo: Malware

Fecha de lanzamiento original: 05 de julio de 2019 | Última revisión 11 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha encontrado nuevos antecedentes en relación al caso 2CMV-00013-001.

En lo concreto, CSIRT ha podido identificar un segundo sitio que contiene un archivo con un malware bajo el nombre de “impuestos.exe”, con el Hash MD5 “349d6af6f1710decfcb42a6a6ce1c15e”.

Este malware es en realidad un Troyano que rastrea los datos ingresados con el teclado, aplicaciones instaladas y realiza captura de pantallas, entre otras acciones. Además deja la posibilidad de insertar nuevos malware a través de la comunicación con el servidor comando control, para así aumentar su vector de ataque insertando nuevos módulos de malware en el equipo infectado.

CSIRT pudo concluir que el archivo se conectaba a diferentes servidores comando control cada vez que se ejecutaba.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Archivo Adjunto

Archivo	:	impuestos.exe
MD5	:	349d6af6f1710decfcb42a6a6ce1c15e
SHA-1	:	817e215be884c50e0e115e106fd41fc9d5224359
SHA-256	:	1ce17200496c6ffbbfe6220fa147f7599edce5a4dfb27a0afe14e072ceca5eb6

Url's:

https[:]//incremento-avance-en-tarjeta-cl[.]gq/impuesto/impuestos[.]exe

http[:]//www[.]djcreview07[.]com/sh/?SH=MEgk2CqTNDVZyuqmd3CBEROWi1E70CRGmHI8VcMgV+lK9WwepqXXVqUluVRE77EGeeB4PQ==&rFQLM=_pd4lx8

http[:]//www[.]tuvanmoitruongvanlang[.]com/sh/?SH=2JmiDG2NtKn/mYtTMcIQpByNE/ZiEDR7ghsHCeUJK/G9b3WlmXnyY7XLJJfRt5UKp37zJQ==&rFQLM=_pd4lx8&sql=1

http[:]//www[.]firdesigns[.]com/sh/?SH=+N0C/HK6L8mCTLfVF9QKGJ9MctWTzRmaAz6PbiNNfFxG9q3vGqpauaYaEAMnPj7H0S5Sxw==&rFQLM=_pd4lx8&sql=1

http[:]//www[.]firdesigns[.]com/sh/

http[:]//www[.]tuvanmoitruongvanlang[.]com/sh/

Nuevos Antecedentes

htt[:]//camereco[.]com/wp-content/uploads/2019/05/impuestos[.]exe

0gc2t8[.]info/sh

15churchroad[.]com/sh

186528k[.]com/sh

34zhibo[.]com/sh

acebrezzoe[.]com/sh

alvota[.]com/sh

bada2l[.]com/sh

bjnbyj[.]com/sh

bolyex[.]com/sh

bolyex[.]com/sh/?rz=spxxblzh5xr4e&fx=vziv03thj62gwusngijjzsjx9t24uvj61xrlplfvpic1wakwv2e6r3ttql5wymazbqtsda==

borissovcoin[.]com/sh

broadciolpudd[.]win/sh

bzlouti[.]com/sh

chankiri[.]com/sh

darnitromance[.]com/sh

demureba[.]net/sh

destinydanes[.]com/sh

devfunlink[.]com/sh

djcreview07[.]com/sh

egoeffects[.]com/sh

emilyhenssen[.]com/sh

ezchoicepro[.]com/sh

feraserweb[.]live/sh

firdesigns[.]com/sh

further[.]design/sh

garnertautomotriz[.]com/sh

gomultitaxservice[.]com/sh

hangjv[.]com/sh

hollyelizabethfox[.]com/sh

hotelarabeluj-granada[.]com/sh

j1tnm1[.]info/sh

jetcharter360[.]com/sh

kitchenchoir[.]com/sh

lb41319[.]com/sh

leviathan[.]ltd/sh

maexinvent[.]com/sh

mendez-conseils-immo[.]com/sh

minitost[.]com/sh

neoconcerts.net/sh

niyniy.com/sh

pasta-linda.com/sh

plusgateway[.]net/sh

podscared[.]online/sh

prestigehm[.]net/sh

protocol[.]life/sh

purpsmoke[.]com/sh

rocketcityaxethrowing[.]info/sh

rodandwheelhouse[.]com/sh

sisiss[.]info/sh

snuff-bottles[.]com/sh

spydermangames[.]party/sh

tagpfm[.]com/sh

thereggaesoldiers[.]com/sh

topperdr[.]com/sh

touristinnhotel[.]com/sh

tuvanmoitruongvanlang[.]com/sh

useyanoggin[.]com/sh

vfxwarrior[.]com/sh

wallettop[.]com/sh

waylea[.]com/sh

worldtravellab[.]com/sh

xn--fiqy4bl9loxhtj8dffl[.]com/sh

zghzkj[.]com/sh

Detección de Sandbox

Kaspersky Lab

	Zone	Name
!	High	HEUR:Trojan.Win32.Generic
!	High	Trojan-Spy.Win32.Noon.sb
!	High	Backdoor.Win32.Androm
!	High	Trojan-Dropper.Win32.Injector
⚠	Medium	not-a-virus:AdWare.Win32.SpeedBit.sb

Proofpoint

Malware Generico

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob