

Incidente de ciberseguridad

Fecha: 01/05/2024

Problemática: Instituciones del Gobierno de Emiratos Árabes Unidos afectadas por Ciberataques

Correlativo: AC-0019

Institución / Sector: Público y Privado

SITUACIÓN

El grupo de actor de amenazas «TheFiveFamilies» se atribuyó los ciberataques dirigidos a servidores de distintas instituciones gubernamentales de Emiratos Árabes Unidos. Tras el incidente que interrumpió sus servicios tecnológicos el actor de amenazas exige una ciberextorsión para liberar la información cifrada.

RIESGOS

- Cifrado de Información
- Daños críticos a la infraestructura tecnológica
- Suplantación de identidad
- Campañas de censura y desprestigio

RECOMENDACIONES

- Implementar y/o reforzar la seguridad perimetral
- Emplear contraseñas seguras
- Cambiar contraseñas periódicamente
- Utilizar la autenticación de dos factores
- Nunca haga clic en enlaces o descargue archivos adjuntos de fuentes desconocidas.

Nivel de priorización

Prioridad
Urgente / No Urgente
No Urgente

Actualización
Seguimiento/Preventiva/Resiliente
Preventiva

Matriz de evaluación

Riesgo Alto/Medio/Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alto	Alto	Alto

ANEXO

```
07/20/2023 01:20 AM -@18- Sharik
07/20/2023 02:11 AM -@18- SharikAPIS
06/23/2023 10:04 PM -@18- SharikAPIS - Copy
04/29/2024 01:56 AM 2,787,829,768 Sharikcomm.tar
09/23/2022 11:08 AM -@18- SharikV2
09/23/2022 10:58 AM -@18- SharikV2-identityserver
09/23/2022 10:57 AM -@18- SharikV2-xconnect
04/29/2024 12:03 AM 2,787,829,768 SharikV2_connect.tar
09/07/2023 05:24 PM -@18- SharikWeb
10/18/2023 10:59 PM -@18- Slticorev18.3.1identityserver.dev.local
10/18/2023 11:06 PM -@18- Slticorev18.3.1sc.dev.local.zip
04/26/2024 07:59 PM -@18- TDRA Website
01/24/2023 03:00 PM -@18- TDRA Website 2
10/16/2022 09:56 AM -@18- TDRA Website 2-xconnect
12/22/2023 05:56 PM -@18- TDRA Website RC
10/14/2023 10:00 PM 750,346,407 TDRAwebv10.1.1sc.dev.local.zip
10/16/2023 05:19 PM -@18- TDRAwebv10.1.1xconnect.dev.local
12/13/2022 01:19 PM -@18- Text
09/16/2022 12:28 PM -@18- Thoughts RTA
06/01/2023 08:24 PM -@18- ThoughtIAADC
09/30/2022 01:52 PM -@18- ThoughtIA0
01/09/2023 11:15 PM -@18- ThoughtIAfari
08/30/2022 01:52 PM -@18- ThoughtIAPI
03/26/2024 11:26 PM -@18- ThoughtSIANS
10/09/2023 04:03 PM 158,190,428 ThoughtSIANS.zip
01/14/2024 07:56 PM -@18- ThoughtSDGE
07/11/2023 03:43 PM -@18- ThoughtSDOH
10/06/2024 02:52 PM -@18- ThoughtStethadMail
01/06/2024 02:35 PM -@18- ThoughtStethadMail - Copy
01/01/2023 08:00 PM -@18- ThoughtInnovation
09/27/2023 03:24 PM -@18- ThoughtInnovationDemo
11/07/2022 03:43 PM -@18- ThoughtInshires
07/05/2023 05:36 PM -@18- ThoughtSequenceV
04/01/2024 12:49 PM -@18- ThoughtSLC
09/30/2022 01:52 PM -@18- ThoughtTRA
04/01/2023 08:40 PM -@18- ThoughtWebsite_AADC-Innovates
07/22/2023 01:34 AM -@18- TicketsMarchAPI
09/22/2022 05:18 PM 9,723,233,348 U.A.E. Gov18.zip
09/22/2022 10:45 AM -@18- UAE5G5V2
09/22/2022 10:43 AM -@18- UAE5G5V2-xconnect
10/22/2024 01:49 PM -@18- UAE_BLS
10/22/2023 07:03 PM -@18- UCP_Test_Data
```

PYV From a few friends of ours! (Netrunners)

You have 6 days left to pay and get this btc Adress too a balance of 150 BTC.

If it doesnt reach the balance we will put all data for sale and start leaking some of it.

We've got something massive to share with you all. We've successfully breached UAE gov servers and let me tell you, the loot is beyond imagination. We've managed to acquire sensitive information not only from various ministries but also from other key entities in the UAE government. we've gained access to data from [Sharik.ae](#), [tdra.gov.ae](#), [fanr.gov.ae](#), Executive Council, Ministry of Cabinet Affairs, [U.AE](#), [Bayanat.ae](#), [Kidx.ae](#), [Sannif.ae](#), and [ThoughtsInnovation](#), [MOEModel](#), [rta.ae](#), [workinuae.ae](#) And some AI modules.

But wait, there's more... We've also secured employee data (phone mail and name) in:
Ministry of Interior
Ministry of Foreign Affairs & International Cooperation
Ministry of Health and Prevention
Ministry of Justice

REFERENCIAS

Fuente: https://twitter.com/_venarix_/status/1785802163676934195/photo/1