ALERTA TÉCNICA

TLP:AMBER

MICITT-DGD-DRII-AT-115-2022

Alerta sobre indicadores de compromisos relacionados con la infraestructura de red de Trickbot y Ursnif

Se les comunica a los Directores (as) /Jefes (as) de Tecnologías de Información y a los enlaces de Ciberseguridad, para que tomen las medidas necesarias.

Trickbot es un malware altamente modular, capaz de realizar una serie de acciones en una red, como robar información o lanzar ransomware. Ursnif (también conocido como Gozi) se identifica como un troyano bancario, pero sus variantes también incluyen componentes (puertas traseras, software espía, inyectores de archivos, etc.) capaces de una amplia variedad de comportamientos.

Desde el CSIRT Nacional les compartimos la siguiente información de indicadores de compromiso (IoC) enviada por la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA por sus siglas en inglés) con los IoC relacionados con el malware de Trickbot correspondientes a la fechas del 11 al 14 de abril del 2022, y Ursnif correspondientes a la fechas del 12 al 14 de abril del 2022 para las instituciones de gobierno y de infraestructuras críticas.

Trickbot

IP Address	Country of Location	First Seen	Last Seen
103.87.48.54	India	30/12/2021	14/4/2022
45.221.8.171	Uganda	3/11/2021	14/4/2022
103.9.188.78	Cambodia	19/10/2021	14/4/2022
103.75.32.173	India	11/10/2021	14/4/2022
31.14.40.107	Romania	6/10/2021	14/4/2022
175.184.232.234	Indonesia	22/9/2021	14/4/2022
196.41.57.46	Tanzania	25/8/2021	14/4/2022
203.151.233.10	Thailand	15/8/2021	14/4/2022
103.146.232.5	India	8/2/2022	14/4/2022
179.43.169.178	Switzerland	20/10/2021	14/4/2022
177.190.76.82	Brazil	9/11/2021	14/4/2022
65.21.231.30	Germany	27/1/2022	14/4/2022
202.152.56.10	Indonesia	11/9/2021	14/4/2022
41.77.134.250	Mozambique	29/7/2021	14/4/2022
91.200.103.242	Germany	6/11/2021	14/4/2022
181.28.132.173	Argentina	20/11/2021	13/4/2022
190.131.243.186	Colombia	10/11/2021	13/4/2022
36.95.73.109	Indonesia	2/11/2021	13/4/2022
182.160.98.250	Bangladesh	22/9/2021	13/4/2022
96.9.69.207	Cambodia	2/11/2021	13/4/2022
190.152.2.86	Ecuador	29/7/2021	13/4/2022
150.129.55.108	India	29/9/2021	13/4/2022
95.217.109.26	Finland	25/2/2022	13/4/2022
5.9.144.234	Germany	1/2/2022	13/4/2022
5.9.66.153	Germany	15/11/2021	13/4/2022
51.89.202.111	Israel	29/7/2021	12/4/2022
139.255.41.122	Indonesia	24/9/2021	12/4/2022
195.39.233.29	Ukraine	22/9/2021	12/4/2022
65.108.110.26	Germany	8/3/2022	12/4/2022
5.9.88.113	Germany	25/1/2022	12/4/2022
37.187.27.125	France	12/4/2022	12/4/2022
65.108.3.252	Germany	12/4/2022	11/4/2022
78.46.149.254	Germany	15/9/2021	11/4/2022

Ursnif

Country of Location	IP Address	First Seen	Last Seen
Latvia	94.140.115.135	28/3/2022	14/4/2022
Kuwait	37.34.176.37	7/2/2022	14/4/2022
South Korea	211.59.14.90	26/1/2022	14/4/2022
South Korea	222.236.49.123	26/1/2022	14/4/2022
South Korea	222.232.238.243	27/1/2022	14/4/2022
South Korea	58.235.189.190	26/1/2022	14/4/2022
South Korea	222.236.49.124	26/1/2022	14/4/2022
South Korea	61.98.7.133	25/1/2022	14/4/2022
South Korea	1.248.122.240	26/1/2022	14/4/2022
South Korea	110.14.121.125	25/1/2022	14/4/2022
South Korea	175.126.109.15	25/1/2022	14/4/2022
South Korea	180.69.193.102	25/1/2022	14/4/2022
South Korea	116.121.62.237	25/1/2022	14/4/2022
South Korea	61.98.7.132	26/1/2022	14/4/2022
South Korea	110.14.121.123	25/1/2022	14/4/2022
Kuwait	37.34.248.24	27/1/2022	14/4/2022
Eritrea	196.200.111.5	20/1/2022	14/4/2022
South Korea	175.120.254.9	21/1/2022	14/4/2022
South Korea	175.119.10.231	24/1/2022	14/4/2022
Russia	213.183.53.118	17/2/2022	14/4/2022
South Korea	211.229.47.232	5/4/2022	14/4/2022
South Korea	203.228.9.102	3/2/2022	14/4/2022
Russia	37.140.241.20	24/1/2022	14/4/2022
Switzerland	185.189.149.186	12/4/2022	14/4/2022
Japan	162.133.73.151	6/4/2022	14/4/2022
Germany	81.169.145.94	14/4/2022	14/4/2022
Uzbekistan	195.158.3.162	7/4/2022	12/4/2022
South Korea	118.33.109.122	9/2/2022	12/4/2022
Russia	213.183.53.116	15/3/2022	12/4/2022
Pakistan	124.109.61.160	27/1/2022	12/4/2022
Netherlands	185.107.56.208	23/3/2022	12/4/2022
Netherlands	185.107.56.209	23/3/2022	12/4/2022
Netherlands	185.107.56.210	23/3/2022	12/4/2022
Russia	193.56.146.189	11/4/2022	12/4/2022
Germany	87.106.18.141	10/11/2021	12/4/2022
Bangladesh	27.147.183.45	24/1/2022	12/4/2022
Switzerland	185.189.149.215	12/4/2022	12/4/2022

Esta información no se puede utilizar en relación con ningún procedimiento judicial nacional o extranjero ni para ningún otro propósito legal, judicial o administrativo, es solo con fines preventivos en sus infraestructuras.

Recomendaciones

- Se recomienda incluir estos IoC a sus firewalls o sistemas de detección como medida de prevención.

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2022.04.23 20:24:14 -06'00'

Jorge Mora Flores
Director de Gobernanza Digital

Firmado digitalmente por ROBERTO PAULO LEMAITRE PICADO (FIRMA)
Ubicación: CSIRT-CR
Fecha: 2022.04.23 20:45:55 -06'00'

Roberto Lemaitre Picado
Coordinador CSIRT-CR