I. Aplicación utilizada

Monero.Criptomoneda.Miner

Control de aplicaciones

Monero.Criptomoneda.Miner

Descripción

Esto indica un intento de usar un minero de criptomoneda Monero.
Monero (XMR) es una criptomoneda de código abierto creada en abril de 2014. Es muy similar a Bitcoin. A partir de 2017, Monero es la sexta criptomoneda más comercializada, con una capitalización de mercado de más de $ 300,000,000.
Tenga en cuenta que los mineros de Monero Cryptocurrency a menudo están integrados en malware y se utilizan para la minería de botnet.

II. Logs registrados en FortiGate

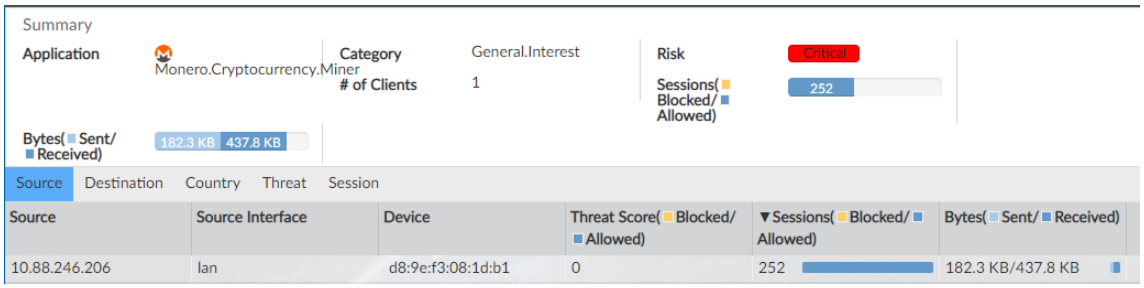
En la siguiente imagen se muestra información de los logs registrados en el equipo de Productivity Gurú, brindando información de Hora, Source, Destination, Aplication Name y Action. Se puede observar que las conexiones han sido permitidas.

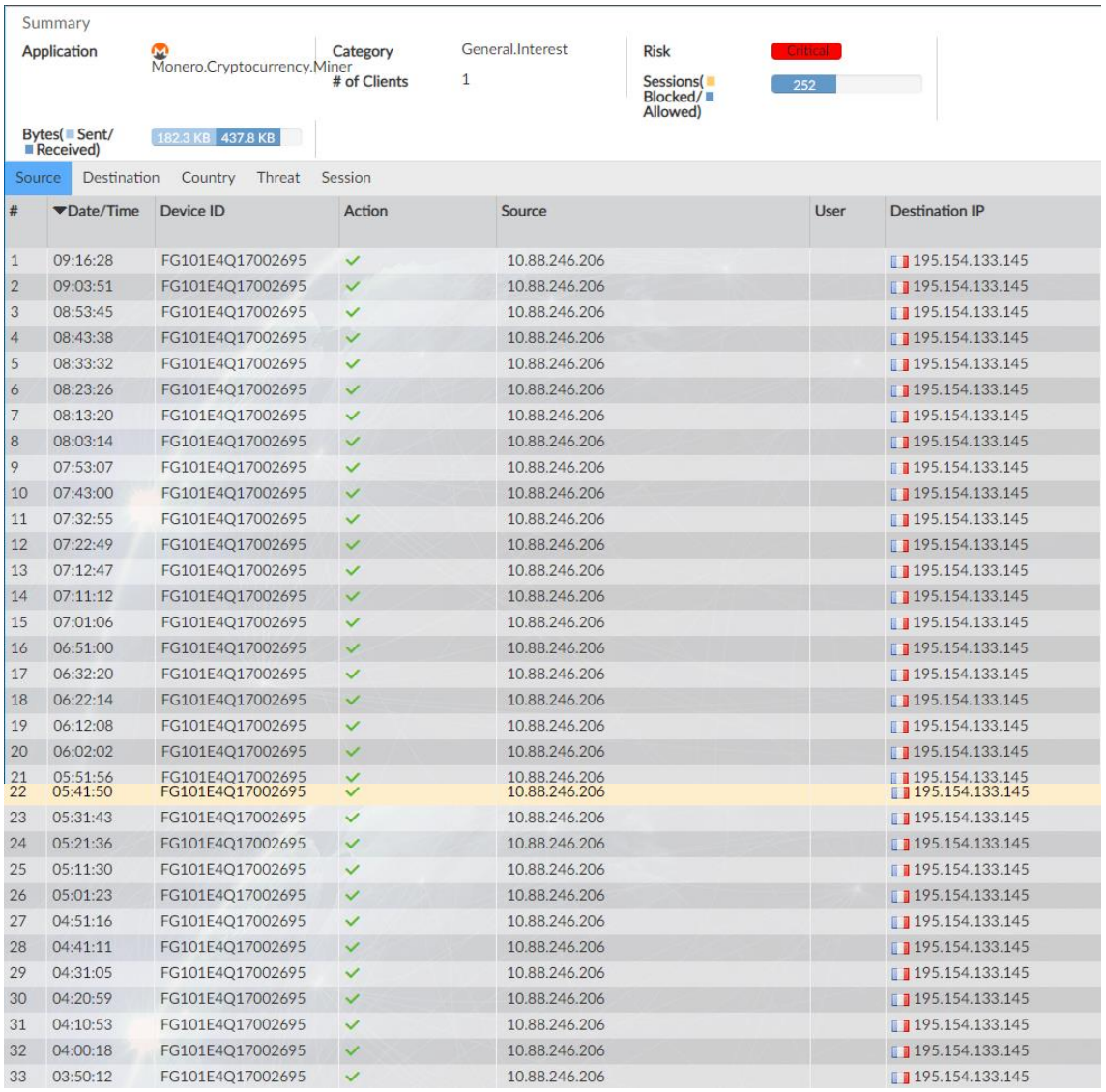
Application Name: Monero.Cryptocurrency.Miner | Add Filter

#	Date/Time	Source	Destination	Application Name	Action
1	10:08:23	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
2	09:58:17	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
3	09:48:11	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
4	09:38:06	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
5	09:28:00	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
6	09:15:23	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
7	09:05:16	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
8	08:55:10	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
9	08:45:04	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
10	08:34:58	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
11	08:24:51	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
12	08:14:45	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
13	08:04:38	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
14	07:54:32	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
15	07:44:25	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
16	07:34:19	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
17	07:24:13	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
18	07:22:43	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
19	07:12:36	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
20	07:02:30	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
21	06:43:51	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
22	06:33:45	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
23	06:23:39	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
24	06:13:33	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
25	06:03:27	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
26	05:53:20	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
27	05:43:13	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
28	05:33:07	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
29	05:23:00	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
30	05:12:54	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
31	05:02:48	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
32	04:52:41	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
33	04:42:34	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
34	04:32:28	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
35	04:22:22	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
36	04:11:48	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
37	04:01:41	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
38	03:51:34	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
39	03:41:29	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
40	03:37:58	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
42	03:17:45	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
43	03:07:39	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
44	02:57:32	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
45	02:45:06	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
46	02:35:00	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
47	02:24:53	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
48	02:14:47	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
49	02:04:40	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass
50	01:45:05	10.88.246.206	195.154.133.145 (roro2016.linkpc.net)	Monero.Cryptocurrency.Miner	pass

III. Logs registrados en Analyzer

Se muestran los logs registrados en el Analizador de RealNet. Mostrando información como: Source, Source Interface, Device, Threat Score, Sessions y Bytes, así como el nombre de la aplicación, la categoría a la que pertenece y el nivel de riesgo.



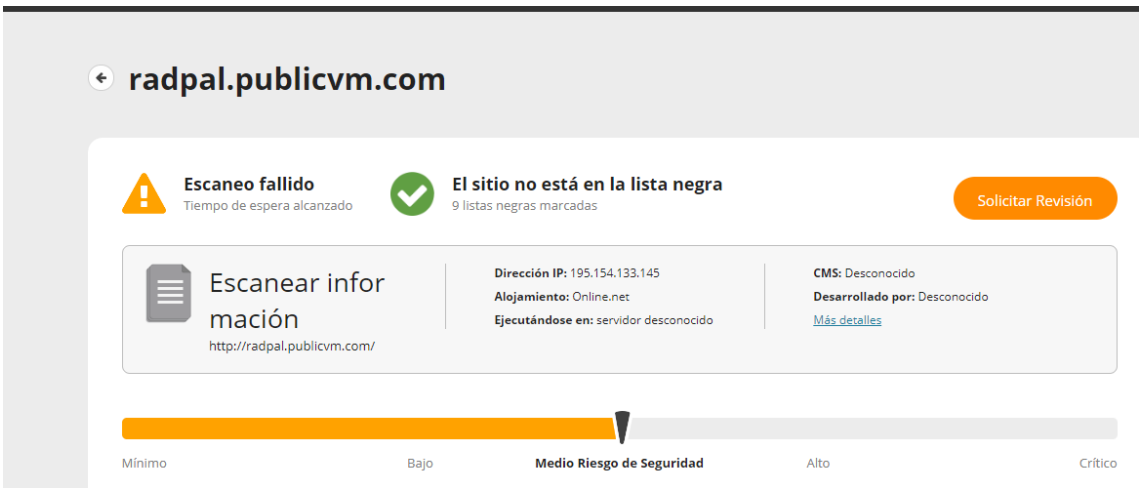


#	Date/Time	Device ID	Action	Source	User	Destination IP
1	09:16:28	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
2	09:03:51	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
3	08:53:45	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
4	08:43:38	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
5	08:33:32	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
6	08:23:26	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
7	08:13:20	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
8	08:03:14	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
9	07:53:07	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
10	07:43:00	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
11	07:32:55	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
12	07:22:49	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
13	07:12:47	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
14	07:11:12	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
15	07:01:06	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
16	06:51:00	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
17	06:32:20	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
18	06:22:14	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
19	06:12:08	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
20	06:02:02	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
21	05:51:56	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
22	05:41:50	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
23	05:31:43	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
24	05:21:36	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
25	05:11:30	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
26	05:01:23	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
27	04:51:16	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
28	04:41:11	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
29	04:31:05	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
30	04:20:59	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
31	04:10:53	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
32	04:00:18	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145
33	03:50:12	FG101E4Q17002695	✓	10.88.246.206		195.154.133.145

IV. Escaneo de Sitios Web

En base a la información obtenida del equipo de Productivity Gurú se han mostrado 3 sitios web diferentes hacia donde se están realizando las conexiones, los cuales se escanearon con diferentes herramientas, pero los resultados no son los esperados ya que los sitios no pueden ser escaneados. Adjunto evidencias.

1. **radpal.publicvm.com**



radpal.publicvm.com

URL: http://radpal.publicvm.com
Submission: On March 06 via manual (March 6th 2019, 4:42:19 pm)

We could not scan this website!

Error text of the first response:

net::ERR_ABORTED

This can happen for multiple reasons:

- The site could not be contacted (DNS or generic network issues)
- The site uses insecure TLS (weak ciphers e.g.)
- The site requires HTTP authentication

Screenshot During scan

2. **roro2016.linkpc.net**

Búsqueda de filtros web

roro2016.linkpc.net

Presentar una URL para comprobar su Clasificación

5.6 +

FortiOS Version

Categoría: Sitios web maliciosos

Los sitios que alojan software que se descarga de forma encubierta en la máquina de un usuario para recopilar información y monitorear la actividad del usuario, y los sitios que están infectados con software dañino o destructivo, específicamente diseñados para dañar, interrumpir, atacar o manipular sistemas informáticos sin el consentimiento del usuario, como virus o troyano.

roro2016.linkpc.net

Escaneo fallido
Tiempo de espera alcanzado

El sitio está en la lista negra
por McAfee

Solicitar limpieza

Escanear infor
mación
http://roro2016.linkpc.net/

Dirección IP: 195.154.133.145
Alojamiento: Online.net
Ejecutándose en: servidor desconocido

CMS: Desconocido
Desarrollado por: Desconocido
Más detalles

Mínimo | Bajo | Medio | Alto | **Crítico Riesgo de seguridad**

roro2016.linkpc.net

URL: http://roro2016.linkpc.net
Submission: On March 06 via manual (March 6th 2019, 4:06:00 pm)

Screenshot During scan

We could not scan this website!

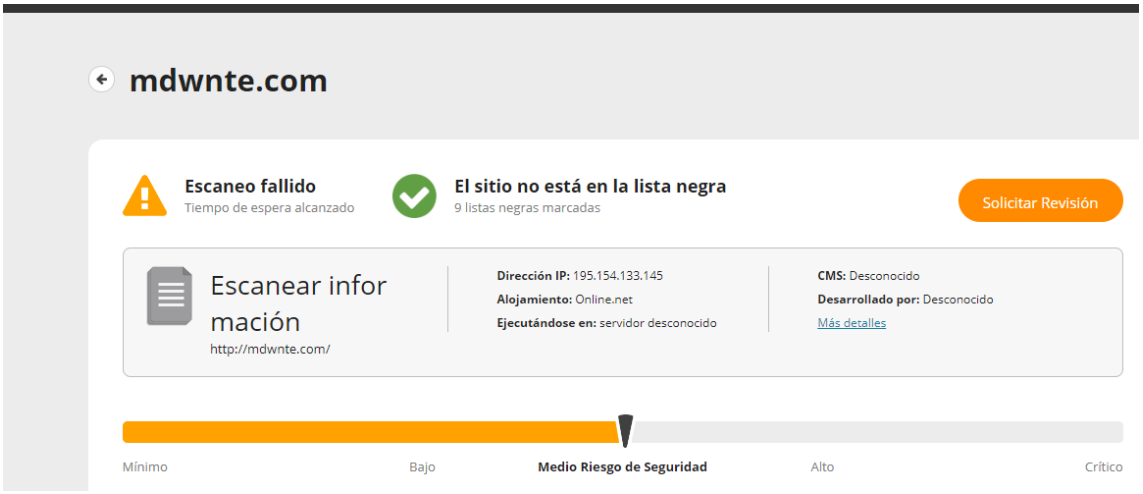
Error text of the first response:

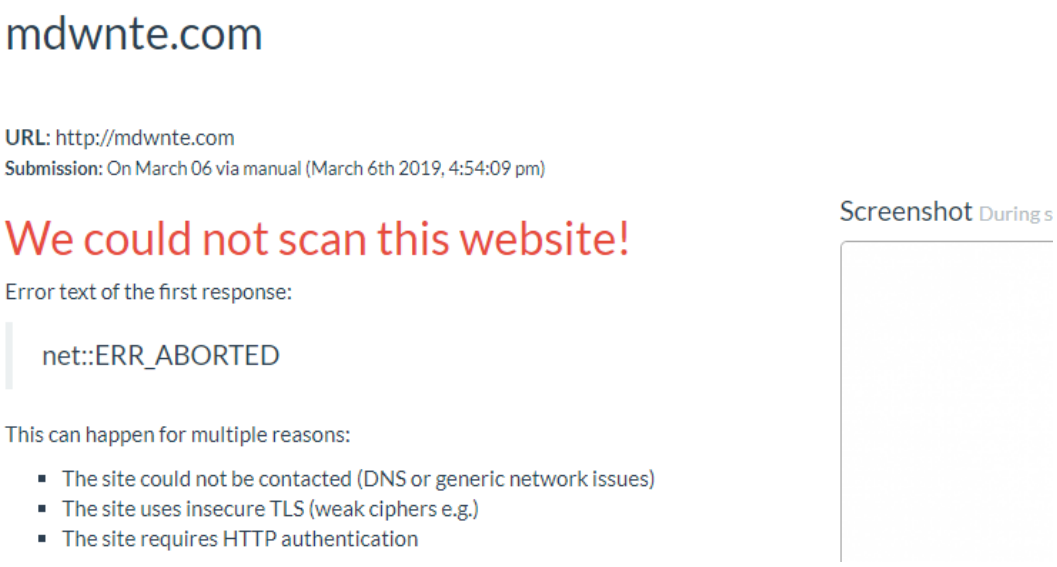
> net::ERR_ABORTED

This can happen for multiple reasons:

- The site could not be contacted (DNS or generic network issues)
- The site uses insecure TLS (weak ciphers e.g.)
- The site requires HTTP authentication

3. mdwnte.com





V. Conclusiones

En las imágenes se puede ver las conexiones realizadas desde las 0:00 hrs, así como la direccion IP que está realizando dichas conexiones de igual manera, durante la actualización de logs en el equipo de Productivity Gurú, se han mostrado 3 sitios distintos los cuales están apuntando a una misma dirección IP. En la investigación de dichos sitios los resultados fueron insatisfactorios ya que estos no pueden ser escaneados sin embargo si se muestra información con el nivel de riesgo que tienen y las razones por la cuales no se puede escanear el sitio.

VI. Recomendaciones

- Analizar el equipo con un antimalware para descartar cualquier tipo de amenaza.
- Aislar el dispositivo de red interna e internet mientras se realiza el análisis, para evitar posibles infecciones de Malware.
- Bloquear la aplicación.

Para cualquier duda o aclaración estaremos atentos para apoyarle.Nuestro Servicio de Productivity Gurú: https://realnetguru.mx/seguridad/productivityguru/