¿Usas escritorio remoto? Entonces deberías estar preocupado…

Siempre hemos oído hablar de los ataques informáticos más convencionales como los ataques de monitorización o los ataques DDOS, sin embargo, los piratas informáticos suelen buscar cualquier oportunidad para tratar de conseguir acceso pleno a un servidor o equipo informático. En esta ocasión, vamos a hablar sobre los escritorios remotos de Windows y su protocolo RDP (Remote Desktop Protocol), con el cual los piratas tendrán la posibilidad de acceder y obtener acceso a tu equipo remotamente.

Este problema se está dando cada vez más en las empresas. Según una reconocida marca de antivirus, el 40% de las organizaciones medianas y grandes analizadas son objeto de este tipo de ataques todos los meses. Para sacar beneficio de este tipo de ataque, los piratas informáticos acceden al mercado negro para vender las claves robadas, tal como podemos observar en la siguiente tabla la comparación de precios según el sistema operativo y región a la que pertenezca:

	United States	European Union	Asia	Africa
Windows XP	$3 USD	$5 USD	$5 USD	$5 USD
Windows Vista	$5 USD	$7 USD	$6 USD	$6 USD
Windows 7	$8 USD	$8 USD	$7 USD	$7 USD
Windows 8	$9 USD	$10 USD	$9 USD	$9 USD
Windows 10	$9 USD	$10 USD	$9 USD	$8 USD
Windows 2003 Server	$3 USD	$5 USD	$3 USD	$3 USD
Windows 2008 Server	$7 USD	$7 USD	$6 USD	$6 USD
Windows 2012 Server	$8 USD	$9 USD	$8 USD	$7 USD

Precios de acceso a ordenadores. Obtenido de la darkweb

Los ataques que hemos estado viendo últimamente en los laboratorios de **Dolbuck** involucran una piratería cibernética en el RDP, y ataques de ransomware.

Ya que una vez iniciada la sesión como un usuario regular, a menudo con derechos de administrador llegan incluso a desactivar cualquier antivirus instalado y se carga y ejecuta manualmente el software de secuestro de datos, más conocido como **ransomware**. Por ejemplo, las cepas de rescate ACCDFISA, SamSam y CrySiS (también conocidas como Dharma) se han propagado casi exclusivamente a través de RDP durante estos últimos años.

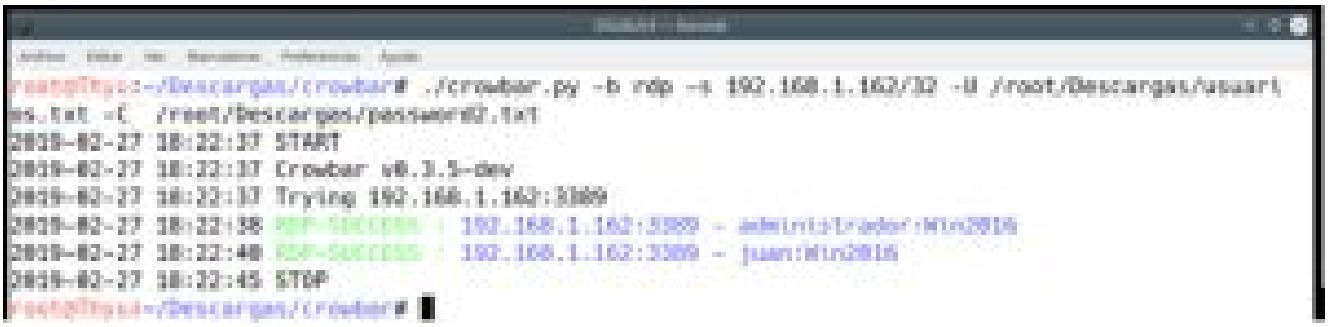
Además, se ha notado un cambio en los métodos de ejecución preferidos de múltiples cepas de **ransomware**, incluyendo Rapid y GlobeImposter, que ahora se entregan principalmente a través de ataques RDP.

A modo de prueba, en los **laboratorios de Dolbuck** hemos reproducido como sería uno de estos ataques.

En la siguiente captura se puede apreciar como identificamos las máquinas de una red que utilizan RDP.

```
root@Thyu:/home/dolbuck#
root@Thyu:/home/dolbuck# nmap -T4 -A -v 192.168.1.1/24 | grep 3389
Discovered open port 3389/tcp on 192.168.1.2
Discovered open port 3389/tcp on 192.168.1.162
Discovered open port 3389/tcp on 192.168.1.169
```

Para luego utilizar ataques de fuerza bruta por diccionario para acceder a ellos.



Una vez dentro simplemente se ejecuta el código malicioso para secuestrar la información y pedir rescate por ella en Bitcoins.

Así que ten cuidado si utilizas RDP, ya que posiblemente tu máquina pueda ser víctima el día de mañana de estos piratas informáticos.

Desde Dolbuck se recomienda utilizar VPN o escritorio remoto pero con filtrado de IPs.