Un malware de botnet con una década de antigüedad, está controlando actualmente más de 450 mil computadoras en todo el mundo y ha cambiado recientemente sus operaciones de infectar máquinas con ransomware o cripto mineros a abusar de ellas al enviar correos electrónicos de extorsión sexual a millones de personas inocentes.

La extorsión por correo electrónico está creciendo significativamente, con un gran número de usuarios quejándose al recibir una gran cantidad de correos electrónicos que intentan extorsionar a las personas amenazando con publicar contenido íntimo que supuestamente los hackers tienen en su poder.

Hasta ahora, no estaba claro cómo los estafadores enviaban tantos correos electrónicos sin ser incluidos en lista negra de los proveedores de correo, los investigadores de CheckPoint finalmente encontraron el bloque que faltaba en este juego.

En su último informe compartido con THN, la firma de seguridad con sede en Tel Aviv reveló que una botnet, llamada Phorpiex, se actualizó recientemente para incluir un bot de spam diseñado para utilizar computadoras comprometidas como servidores proxy para enviar más de 30 mil correos electrónicos de sextortion por hora, sin el conocimientos de los propietarios de las computadoras infectadas.

Funcionamiento del spam bot Phorpiex

El módulo del spambot de Phorpiex descarga la lista de direcciones de correo electrónico desde su servidor remoto de comando y control y utiliza una implementación simple del protocolo SMTP para enviar correos electrónicos de extorsión.

Entre una variedad de mensajes enviados, es común ver algunos como el siguiente:

> *Hey, I know your password is: XXXXXXXX*
>
> *Your computer was infected with my malware, RAT (Remote Administration Tool),*

> *your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more – Google: «Drive-by exploit».*
>
> *My malware gave me full access and control over your computer, meaning, I got access to all your accounts (see password above) and I can see everything on your screen, turn on your camera or microphone and you won't even notice about it.*
>
> *I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!*
>
> *After that I removed my malware to not leave any traces.*
>
> *I can send the video to all your contacts, post it on social network, publish it on the whole web, including the darknet, where the sick people are, I can publish all I found on your computer everywhere!*
>
> *Only you can prevent me from doing this and only I can help you out in this situation.*
>
> *Transfer exactly 900$ with the current bitcoin (BTC) price to my bitcoin address.*
>
> *It's a very good offer, compared to all that horrible shit that will happen if I publish everything!*
>
> *My bitcoin address is: 1LfYcbCsssB2niF3VWRBTVZFExzsweyPGQ*
>
> *Copy and paste my address, it's (cAsE-sEnSEtiVE)*
>
> *I give you 2 days time to transfer the bitcoin!*
>
> *As I got access to this email account, I will know if this email has already been read.*

> *If you get this email multiple times, it's to make sure you read it, my mailer script has been configured like that and after payment you can ignore it.*
> *After receiving the payment, I will remove everything and you can life your live in peace like before.*
>
> *Next time update your browser before browsing the web!*

En muchas ocasiones, la contraseña que muestran es la real del usuario víctima, que ha sido obtenida en ataques cibernéticos a empresas, aunque por lo general, es una contraseña vieja.

> *«Luego, se selecciona aleatoriamente una dirección de correo electrónico de la base de datos descargada, y un mensaje se compone de varias cadenas codificadas. El bot de spam puede producir una gran cantidad de correos electrónicos no deseados, hasta 30,000 por hora. Cada campaña de spam individual puede cubrir hasta 27 millones de víctimas potenciales»*, dicen los investigadores.

> *«El spam bot crea un total de 15,000 hilos para enviar mensajes de spam desde una base de datos. Cada hilo toma una línea aleatoria del archivo descargado. El siguiente archivo de base de datos se descarga cuando finalizan todos los hilos de spam. Si consideramos los retrasos, podemos estimar que ese bot puede enviar unos 30,000 correos electrónicos en una hora»*, agregaron.

Para intimidar a los destinatarios inocentes, los delincuentes detrás de las campañas de sextortion también agregan una de las contraseñas de las víctimas en el campo de asunto, lo que hace que sea más convincente que el pirata informático tenga en realidad información privada del usuario.

Como se mencionó, estas combinaciones de direcciones de correo y contraseñas fueron

seleccionadas de varias bases de datos comprometidas anteriormente, por lo que las contraseñas podrían ser antiguas y relacionadas con cualquier servicio en línea.

> *«La base de datos descargada es un archivo de texto que contiene hasta 20,000 direcciones de correo electrónico. En varias campañas, observamos de 325 a 1363 bases de datos de correo electrónico en un servidor de C&C. Por lo tanto, una campaña de spam cubre hasta 27 millones de víctimas potenciales. Cada línea de este archivo contiene correo electrónico y contraseña delimitados por dos puntos»,* dijeron los investigadores.

Esta misma campaña impulsada por una botnet similar o en su caso, la misma, también ha sido nombrada como ataques de malware *«Save Yourself»* por otros equipos de investigadores.

En más de cinco meses, los piratas informáticos detrás de la campaña han obtenido más de 11 BTC, lo que equivale aproximadamente a 88 mil dólares. Aunque la cifra no es muy alta, los investigadores afirman que los ingresos reales obtenidos por los estafadores podrían ser mayores, ya que no monitorearon las campañas de sextortion en años anteriores.

Finalmente, si recibes correos de este tipo, no debes preocuparte, ya que son una estafa para obtener dinero. Sin embargo, debes tener cuidado con tu información personal almacenada en la nube.