HACKEAR PATRON ANDROID

El uso intensivo de los smartphone hace que puedas encontrar diferentes modelos, marcas y/o sistemas operativos. Como bien sabéis uno de los más extendidos sino el que más es Android.

El buque insignia de Google en smartphones tanto gamas altas como en las más bajas, posee ciertas medidas de seguridad para los dispositivos. Al igual que posee bugs que pueden alterar el funcionamiento de tu terminal.

Una de las medidas de seguridad que ofrece Android, además de colocar un PIN, password, o simplemente desbloquear el terminal deslizando el dedo (seguridad por llamarlo de alguna manera) es la del **patrón de desbloqueo.** Por ello hoy vamos a demostrar (aunque necesitamos una serie de circunstancias) como averiguar un patrón de desbloqueo.



Lo primero que necesitamos es nuestro terminal. Las pruebas se han realizado con un Nexus 4 con Android KitKat 4.4. Decir que también se necesita el dispositivo rooteado. Necesitamos algún tipo de explorador que pueda acceder a carpetas del sistema, en nuestro caso, hemos usado **Root Explorer**. Debemos acceder a la ruta /data/system . Una vez accedido a esa ruta debemos buscar el fichero *gesture.key* el cual debemos copiar a cualquier ruta que tengamos acceso desde nuestro ordenador. Nosotros los

hemos subido a la nube (Cuenta BOX, aunque podemos traspasarlo conectándolo al portátil).

Una vez realizada la subida, procedemos a descargarlo en nuestro equipo. Ahora procederemos a descargar un par de instrumentos que necesitamos para analizar el archivo.

- WinHex (o similar) <u>Descargar</u>
- Diccionario de Hashes <u>Descargar</u>

WinHex lo usaremos para analizar los valores Hexadecimales de *gestures.key* ya que los necesitaremos para consultarlos en el diccionario de hashes SHA-1. Abrimos el programa WinHex, arrastramos el fichero *gestures.key* hasta el programa, y veremos unos valores similares a estos o al menos con la misma construcción.

WinHex - [gesture.key]						
🚟 File Edit Search Navigati	ion View Tools Specialist	Options Window Help				
D 🖻 🖥 🎒 🗳 👘 🗠	🖹 🛍 🔤 🗤	ೆ 💥 🚧 → 🕀 😓 🔿	🔍 🎫 🥪 🖶 🖉	🕅 🕇 🕨 🛅 🔠 🧇		
Case Data gesture.key						
Fi <u>l</u> e E <u>d</u> it	Offset 0 1 2	3456789	ABCDEF			
	00000000 FB 84 A	. 2E 40 DD 71 73 1D 3A	45 9A 4F 55 AA 07	û∥i.@Ýqs :E∥OUª		
	00000010 7C 51 F	24		1098		

Debemosfijarnosenlosvaloresmarcados,concretamenteFB84A12E40DD71731D3A459A4F55AA077C51F524 estosvaloresvaloresdiferirándependiendodel patrónqueposeamos.Ahoraprocedemosa copiarestosvalorescon la combinación de teclasCtrl + Shift + C.CtrlC

Ahora, cuando hayamos descargado y descomprimido el Diccionario de Hashes, recomendamos abrir con el programa **Notepad++** para evitar bloqueos en el editor de texto de Windows. Veremos una pantalla con miles de números hexadecimales. Procedemos a buscar la secuencia que hemos copiado anteriormente. Lo vemos en la siguiente captura.

🔚 Andro	AndroidGestureSHA1.td 🗵						
7412	36915;02 05 08 00 04;9C1764C1A867C0138FB099BC87A8C2E1236EA633						
7413	36917;02 05 08 00 06;AAECACA43BFC2C91B85E9BB39A06DB4728DC522F						
7414	36918;02 05 08 00 07;B6A9EB4B91BCC1B15E45CB7C293D6CA4E6877AE3						
7415	36921;02 05 08 01 00;A4D623BA5DFC00B61040AC57EA966A6EB5C00F9F						
7416	36924;02 05 08 01 03;01EE54402072DF45429E57657DBC46F11647F8E9						
7417	36925;02 05 08 01 04;AC926BCDA120B67C2653F3CA399FA2099941A129						
7418	36927;02 05 08 01 06;BC7535752AC30900E03211FA773DC61C88003D06	Total III					
7419	36928;02 05 08 01 07;E8356D2D08CC5CE484F48B19320CAA55003453B3						
7420	36941;02 05 08 03 00;ED0413C0698A00C61BCD9ECC47EE2803F7719E54	Buscar Reemplazar Buscar en archivos Mark					
7421	36942;02 05 08 03 01;7983D39943FEB5F304CABDAF53F7F8F5F865D162						
7422	36945;02 05 08 03 04;5550AEEF61B549B3A83BA58A05B0BDC40137F624	Buscar: Buscar siguiente					
7423	36947;02 05 08 03 06;FB2B773BEB1D67315F076B1E2F4286FBB47B5712	Contar					
7424	36948;02 05 08 03 07;241CBB96CA83EB97BEE46C7A3554D30E51F155BF						
7425	36951;02 05 08 04 00;387F65252858197A7ACAD8244A1E73C7A8E90063	Buscar en todos los					
7426	36952;02 05 08 04 01;FB536D941435442A192B8B554881694671BF8173	al crivos apier tos					
7427	36954;02 05 08 04 03;DA567DE0319347314304B868F5CBD978A378F9B4	Buscar solo en el archivo					
7428	36957;02 05 08 04 06;B60D0FAA864D90FFA5B2A4961C0EC6E89E3FCFDB	Solo galabras completas					
7429	36958;02 05 08 04 07;FB84A12E40DD71731D3A459A4F55AA077C51F524	Coincidir mayúsculas/minúsculas					
7430	36971;02 05 08 06 00;845AA2906AB6D6D7B32476F47FA244F72CE4E098	Buscar en todo el documento					
7431	36972;02 05 08 06 01;51E3D204253FB88B1890831407EDFCD005ABB9BD	Modo de búsqueda Dirección 📝 Transparencia					
7432	36974;02 05 08 06 03;5813C434C572F9CB5D250E1BBDAFC67F43D0CFF6	Normal O Arriba O Al hacer dic sobre el arc					
7433	36975;02 05 08 06 04;461BEEC4F6A74E6AB86C3C10F2F96042287F20DF	Extendido (In, Ir, It, IO, Ix,) Abata Semare					
7939	36978;02 05 08 06 07;241804C16D8F08F2E509EE0E0EBF88CE361F6C00	Evenesión regular matches newline					
7435	36981;02 05 08 07 00;16D3C299663ED3680F1C9849EB75ABCC4F664FC4						
7437	36962;02 05 06 07 01;153622214B1D9442526156/9145/61EA4B1E4D/1						
7438	36984,02 05 08 07 04,00481F085749F24D77FC6C8F1C683B170FF807F5						
7430	36987:02 05 08 07 06:7DB4199162D7CB72CFFFFFA93914168B7826F508						
7440	37124.02 06 00 01 03:06624839350265733093333095653075412006506565						
7443	37125:02 06 00 01 04:50ADDB836A7DCF9A25DD60EF4F6369F2C8428510						
7442	37126:02 06 00 01 05:0D1A6E3530E8C96FBE0AFCCB6C6B33E16AE4F239						
7443	37128:02 06 00 01 07:FB4A7F16B5F7EC086028D3BA4587C0569D62EEBC						
7444	37129:02 06 00 01 08:CB8FA3C14B9707504E1E1A39DA473DFA7CB594A1						
7445	37142;02 06 00 03 01;0B3BC91CC7DDC10220AD260C152E0926B1E3EB2E						

Vemos como nos marca la secuencia en verde. Si nos fijamos en los números que le preceden 0205080407 podemos extraer el patrón. Por tanto y obviando el cero a la izquierda, nuestro patrón sería el 25847.

¿Cómo interpreto esta numeración? Muy sencillo, aquí os dejamos la equivalencia de los números respecto a la posición de los puntos del patrón.



Si lo probamos en nuestro dispositivo veremos que realmente se cumple siempre. Nosotros hemos modificado el patrón varias veces para testear que esto es real. Y en todas nos ha dado la secuencia correcta.

Esta forma de averiguar el patrón puede ser aprovechada por malware en tu teléfono aunque si no lo tienes rooteado no deberías estar expuesto a esto pero no tener rooteado el teléfono limita muchas funciones de tu smartphone.