

# NSA Podría Estar Detrás Del Malware Regin

Durante más de 10 años, el [malware Regin](#) ha estado infectando grandes objetivos, como Gobiernos, grandes empresas y hasta personas. Ahora hay pruebas claras de que Regin y QWERTY (un **keylogger de la NSA** revelado por Edward Snowden) están relacionados con las mismas personas que **han desarrollado estas piezas de espionaje**.



Los expertos en seguridad de todo el mundo, publicaron que Regin es el programa de espionaje mas sofisticado jamas visto. El año pasado, Regin fue encontrado los [servidores](#) de Belgacom.

El objetivo de infectar estos [servidores](#) ha sido de nivel político, es una manera eficiente de recoger un montón de información de inteligencia sobre los aliados y adversarios de los bandos políticos en esta área del mundo.

En cuanto a la conexion de Regin con el **keylogger QWERTY**, se reduce a una comparación código. Investigadores de Kaspersky estudiaron minuciosamente una muestra QWERTY que obtuvieron de [Spiegel](#) y de inmediato encontró similitudes con Regin. Parte del **código del keylogger QWERTY** también está presente en un módulo de Regin. Kaspersky también encontró referencias a módulos de un determinado complemento de Regin dentro del código QWERTY.

<pre> 0001078C      lea     eax, [ebp+FileObject] 0001078F      push   eax                ; FileObject 00010790      push   100000h           ; DesiredAccess 00010793      lea     eax, [ebp+DestinationString] 00010796      push   eax                ; ObjectName 00010799      call   ds:IsGetDeviceObjectPointer 0001079C      test   eax, eax 0001079E      jnz    loc_10977 000107A1      cmp    [ebp+FileObject], eax 000107A4      jz     loc_10984 000107A7      cmp    [ebp+DeviceObject], eax 000107AA      jz     loc_10977 000107AD      push   [ebp+FileObject] 000107B0      call   IoGetBaseFileSystemDeviceObject 000107B3      test   eax, eax 000107B5      mov    [ebp+DeviceObject], eax 000107B8      jz     loc_10977 000107BB      mov    eax, dword_11900 000107BE      mov    ecx, [eax+4] 000107C1      mov    ecx, [ecx+0Ch] 000107C4      lea     edx, [ebp+var_4] 000107C7      push   edx 000107CA      push   eax 000107CB      call   dword ptr [ecx+20h] 000107CE      test   al, al 00010811 00010812 00010813 00010814 00010815 00010816 00010817 00010818 00010819 0001081A 0001081B 0001081C 0001081D 0001081E 0001081F 00010820 00010821 00010822 00010823 00010824 00010825 00010826 00010827 00010828 00010829 0001082A 0001082B 0001082C 0001082D 0001082E </pre>	<pre> 0001082B 0001082C 0001082D 0001082E 0001082F 00010830 00010831 00010832 00010833 00010834 00010835 00010836 00010837 00010838 00010839 0001083A 0001083B 0001083C 0001083D 0001083E 0001083F 00010840 00010841 00010842 00010843 00010844 00010845 00010846 00010847 00010848 00010849 0001084A 0001084B 0001084C 0001084D 0001084E 0001084F 00010850 00010851 00010852 00010853 00010854 00010855 00010856 00010857 00010858 00010859 0001085A 0001085B 0001085C 0001085D 0001085E 0001085F 00010860 00010861 00010862 00010863 00010864 00010865 00010866 00010867 00010868 00010869 0001086A 0001086B 0001086C 0001086D 0001086E 0001086F 00010870 00010871 00010872 00010873 00010874 00010875 00010876 00010877 00010878 00010879 0001087A 0001087B 0001087C 0001087D 0001087E 0001087F 00010880 00010881 00010882 00010883 00010884 00010885 00010886 00010887 00010888 00010889 0001088A 0001088B 0001088C 0001088D 0001088E 0001088F 00010890 00010891 00010892 00010893 00010894 00010895 00010896 00010897 00010898 00010899 0001089A 0001089B 0001089C 0001089D 0001089E 0001089F 000108A0 000108A1 000108A2 000108A3 000108A4 000108A5 000108A6 000108A7 000108A8 000108A9 000108AA 000108AB 000108AC 000108AD 000108AE 000108AF 000108B0 000108B1 000108B2 000108B3 000108B4 000108B5 000108B6 000108B7 000108B8 000108B9 000108BA 000108BB 000108BC 000108BD 000108BE 000108BF 000108C0 000108C1 000108C2 000108C3 000108C4 000108C5 000108C6 000108C7 000108C8 000108C9 000108CA 000108CB 000108CC 000108CD 000108CE 000108CF 000108D0 000108D1 000108D2 000108D3 000108D4 000108D5 000108D6 000108D7 000108D8 000108D9 000108DA 000108DB 000108DC 000108DD 000108DE 000108DF 000108E0 000108E1 000108E2 000108E3 000108E4 000108E5 000108E6 000108E7 000108E8 000108E9 000108EA 000108EB 000108EC 000108ED 000108EE 000108EF 000108F0 000108F1 000108F2 000108F3 000108F4 000108F5 000108F6 000108F7 000108F8 000108F9 000108FA 000108FB 000108FC 000108FD 000108FE 000108FF </pre>	<pre> lea     eax, [ebp+FileObject] push   eax                ; FileObject push   100000h           ; DesiredAccess lea     eax, [ebp+DestinationString] push   eax                ; ObjectName call   ds:IsGetDeviceObjectPointer test   eax, eax jnz    loc_10881 loc_10881 cmp    [ebp+FileObject], eax jz     loc_1088E cmp    [ebp+DeviceObject], eax jz     loc_10881 push   [ebp+FileObject] call   IoGetBaseFileSystemDeviceObject test   eax, eax mov    [ebp+DeviceObject], eax jz     loc_10881 mov    eax, dword_11508 mov    ecx, [eax+4] mov    ecx, [ecx+0Ch] lea     edx, [ebp+var_4] push   edx push   eax call   dword ptr [ecx+20h] test   al, al mov    edx, [ebp+DeviceObject] mov    edx, [edx+8] mov    ecx, [eax+4] push   dword ptr [edx+44h] mov    ecx, [ecx+4] mov    ecx, [ecx+0Ch] push   eax </pre>
---	---	--

50251.dll (Regin module)

20123.sys ("qwerty")

Sin duda esto es algo preocupante, ver como un organismo de espionaje como la NSA se ve involucrado en temas como **Malware para infectar entidades gubernamentales** y [servidores en general](#). Lo que finalmente queda por pensar es: ¿Dejarían de usar estas tácticas al ser expuestos? Sin duda no, no es raro pensar que ya están implementando alguna versión mejorada estos **sistemas de infección y espionaje**.