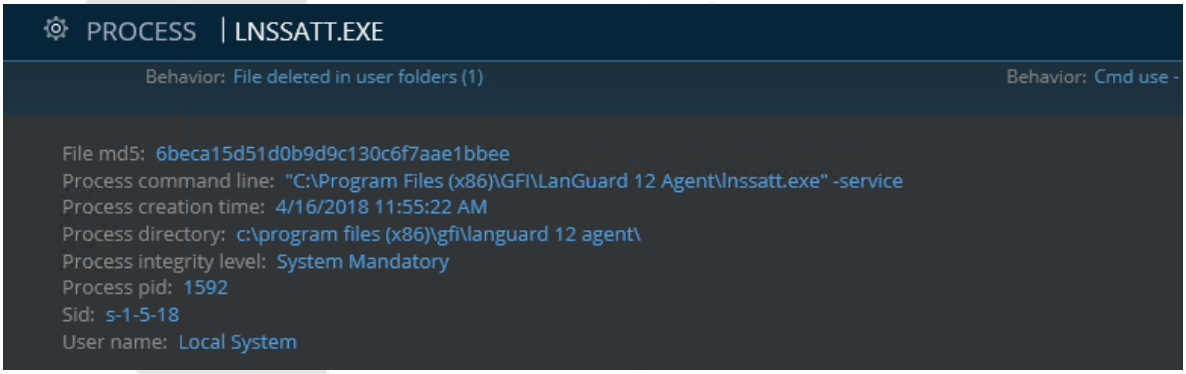
INCIDENT REPORT

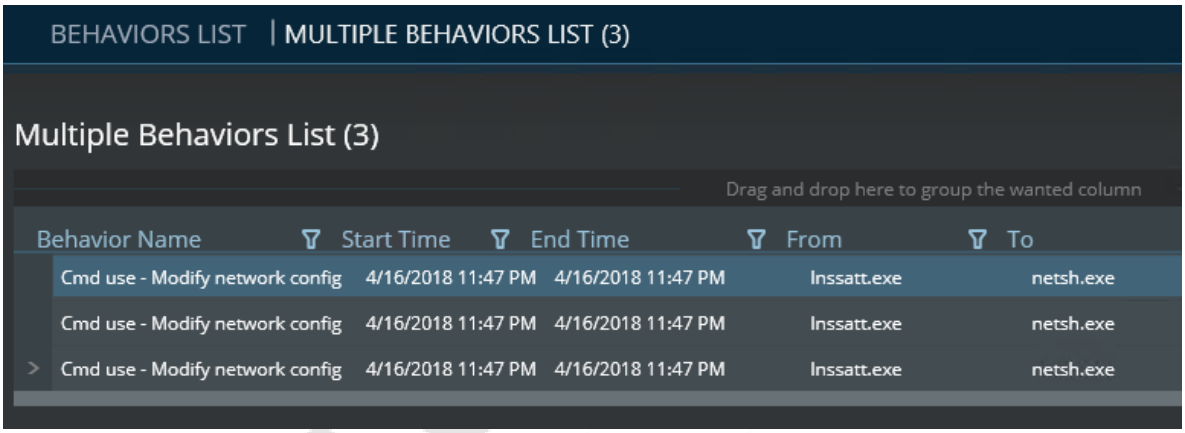
Organization	BANVIVIENDA
Service	MSS-EIR
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

Descripción

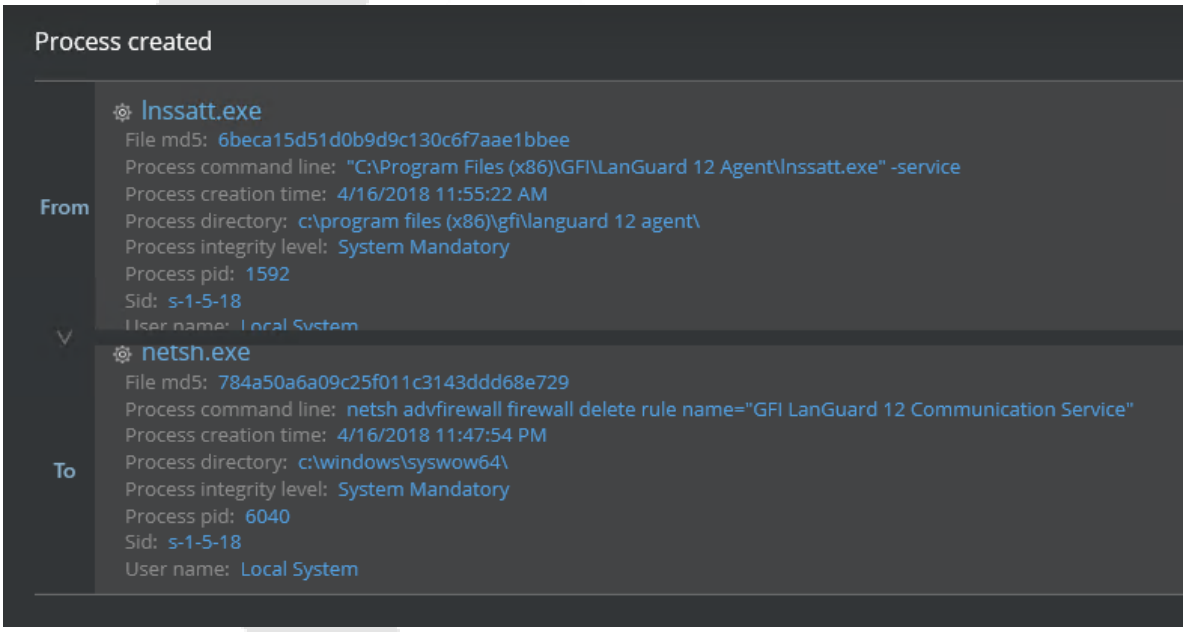
Desde el servidor con agente BPVBLBE2, se detectó un servicio con nombre “lnssatt.exe” y asociado al ID de proceso 1592, iniciado el día 16/04/2018 a las 11:55 AM, eliminó automáticamente una regla de advfirewall de aplicativo “GFI LanGuard 12 Communication Service”, esto sucedió de manera automática a las 11:47 PM. Este programa utilizo la herramienta netsh de Windows para modificar la regla de Windows Firewall a través de comando de consola como se evidencia en las siguientes imágenes. También se registró que este proceso elimino un archivo con nombre “scanorder.txt” de manera automática a las 5:22 PM del mismo día.



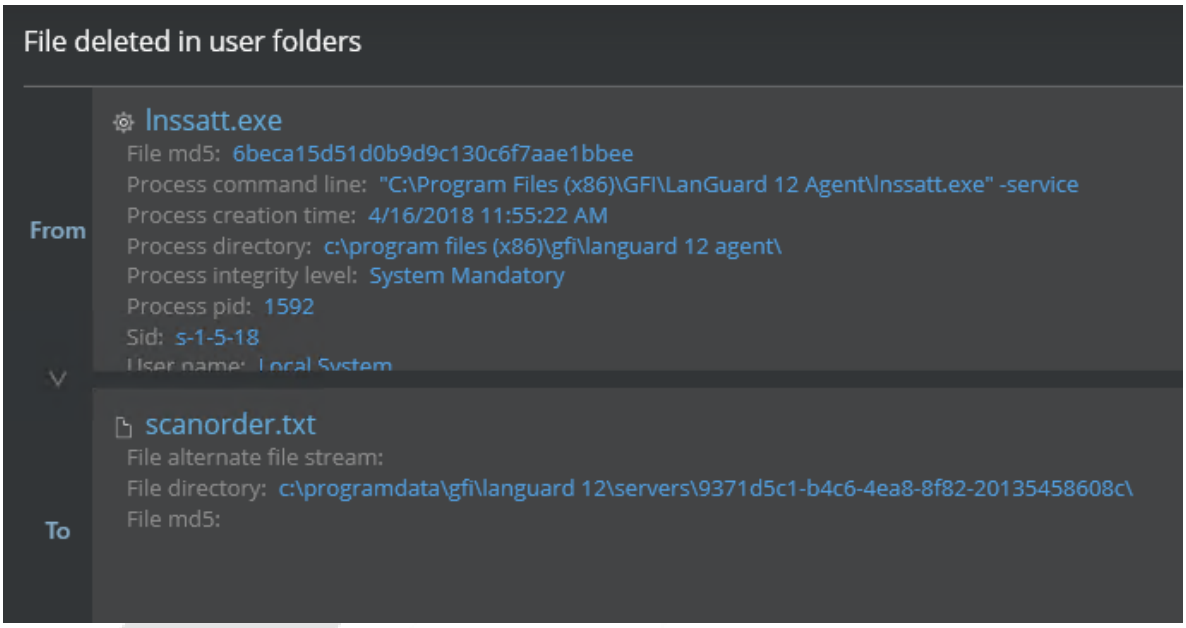
Aquí se muestra cuando se creó el proceso mencionado anteriormente.



En esta imagen se evidencian los eventos reportados, en donde desde el proceso lnssatt.exe se inicia netsh 3 veces seguidas con diferencia de segundo entre ellos.



El comando específico que se utilizó en los 3 eventos se muestra en la imagen anterior, así como fecha y hora en que sucedió.



Este evento lo incluimos porque ocurrió dentro de la ventana de tiempo en que se creó el proceso y se utilizó la herramienta netsh. Se eliminó automáticamente un archivo con nombre sospechoso.
Es posible que esto forme parte de algún proceso normal y debidamente autorizado, sin embargo, de no ser así, se recomienda tomar las acciones necesarias para que esto no siga sucediendo.

Cabe destacar que Netsh es una herramienta que se puede utilizar tanto para mostrar información sensitiva de la red, como también para modificar configuraciones de varios contextos de red, es por esto que sólo servicios explícitamente autorizados deben tener privilegios suficientes para ejecutarla, la lista completa de comandos a continuación:

```
PS C:\Windows\system32> netsh
netsh>/?

The following commands are available:

Commands in this context:
..            - Goes up one context level.
?             - Displays a list of commands.
abort         - Discards changes made while in offline mode.
add           - Adds a configuration entry to a list of entries.
advfirewall   - Changes to the `netsh advfirewall' context.
```

alias - Adds an alias.
branchcache - Changes to the `netsh branchcache' context.
bridge - Changes to the `netsh bridge' context.
bye - Exits the program.
commit - Commits changes made while in offline mode.
delete - Deletes a configuration entry from a list of entries.
dhcpclient - Changes to the `netsh dhcpclient' context.
dnsclient - Changes to the `netsh dnsclient' context.
dump - Displays a configuration script.
exec - Runs a script file.
exit - Exits the program.
firewall - Changes to the `netsh firewall' context.
help - Displays a list of commands.
http - Changes to the `netsh http' context.
interface - Changes to the `netsh interface' context.
ipsec - Changes to the `netsh ipsec' context.
ipsecdosprotection - Changes to the `netsh ipsecdosprotection' context.
lan - Changes to the `netsh lan' context.
namespace - Changes to the `netsh namespace' context.
netio - Changes to the `netsh netio' context.
offline - Sets the current mode to offline.
online - Sets the current mode to online.
popd - Pops a context from the stack.
pushd - Pushes current context on stack.
quit - Exits the program.
ras - Changes to the `netsh ras' context.
rpc - Changes to the `netsh rpc' context.
set - Updates configuration settings.
show - Displays information.
trace - Changes to the `netsh trace' context.
unalias - Deletes an alias.
wfp - Changes to the `netsh wfp' context.
winhttp - Changes to the `netsh winhttp' context.
winsock - Changes to the `netsh winsock' context.

The following sub-contexts are available:
advfirewall branchcache bridge dhcpclient dnsclient firewall http interface ipsec ipsecdosprotection lan namespace netio ras rpc trace wfp winhttp winsock

Según documentación oficial de Microsoft.

Nota: en caso de ser un comportamiento normal favor notificarnos.

Estamos a sus órdenes para apoyarlos con cualquier consulta.

GLESEC OPERATION CENTER – GOC.