

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

UAC Bypass & Research with UAC-A-Mola



- Pablo González
- Telefónica Digital España (ElevenPaths)
- pablo@11paths.com



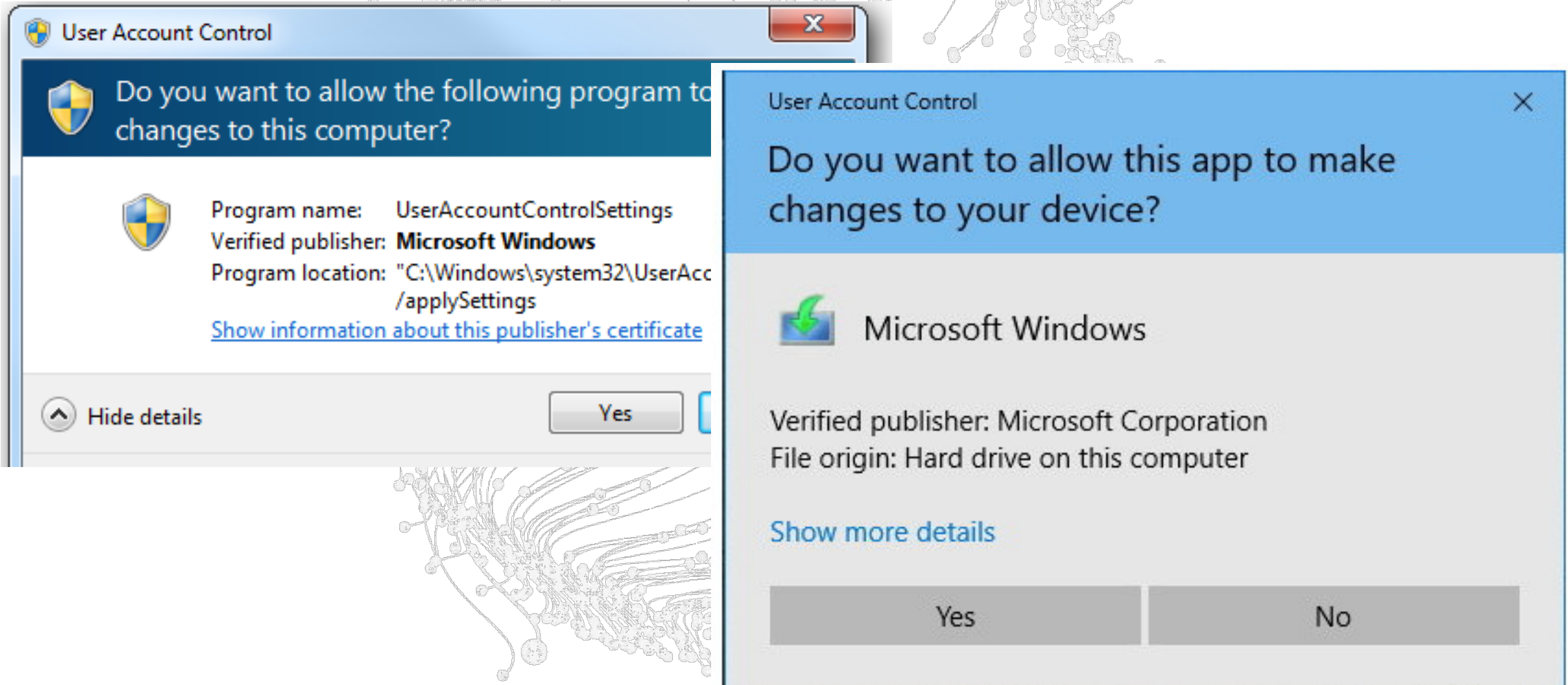
- Santiago Hernández
- Telefónica Digital España (ElevenPaths)
- santiago.hernandezramos@telefonica.com

Índice

1. ¿Qué es UAC?
2. ¿Cómo funciona?
3. ¿Qué es un bypass de UAC?
4. UAC-A-Mola
 - Arquitectura
 - Módulos
5. Resultados
6. PoC



¿Qué es UAC?



¿Cómo funciona?

Ante elevación de privilegio:

- Si user pert. grupo admins
- Si proceso está en integridad media
- Si UAC policy está por defecto

Entonces => proceso toma el token SYSTEM == High Integrity

svchost.exe	20,260 K	26,244 K	772 Host Proc...	Microsoft Corp...	
sihost.exe	4,496 K	5,752 K	2628 Shell Infra...	Microsoft Corp...	Medium
taskhostw.exe	6,036 K	5,404 K	2944 Host Proc...	Microsoft Corp...	Medium
cmd.exe	1,564 K	824 K	2840		High
conhost.exe	5,296 K	3,204 K	3592		High

¿Cómo funciona?

Hay más...

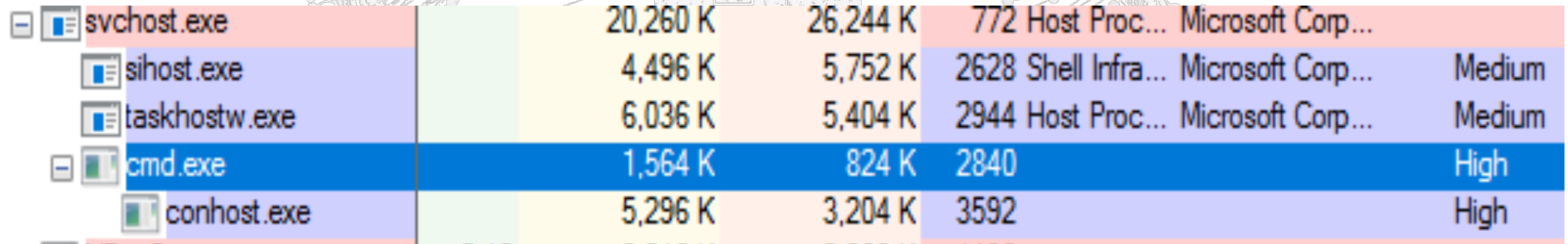
Binarios con manifest:

- Autoelevate True
- Binarios de confianza (firmados Microsoft)

```
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
    <requestedPrivileges>
      <requestedExecutionLevel
        level="requireAdministrator"
        uiAccess="false"
      />
    </requestedPrivileges>
  </security>
</trustInfo>
<asmv3:application>
  <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
    <autoElevate>true</autoElevate>
  </asmv3:windowsSettings>
</asmv3:application>
</assembly>
```

¿Qué es un bypass de UAC?

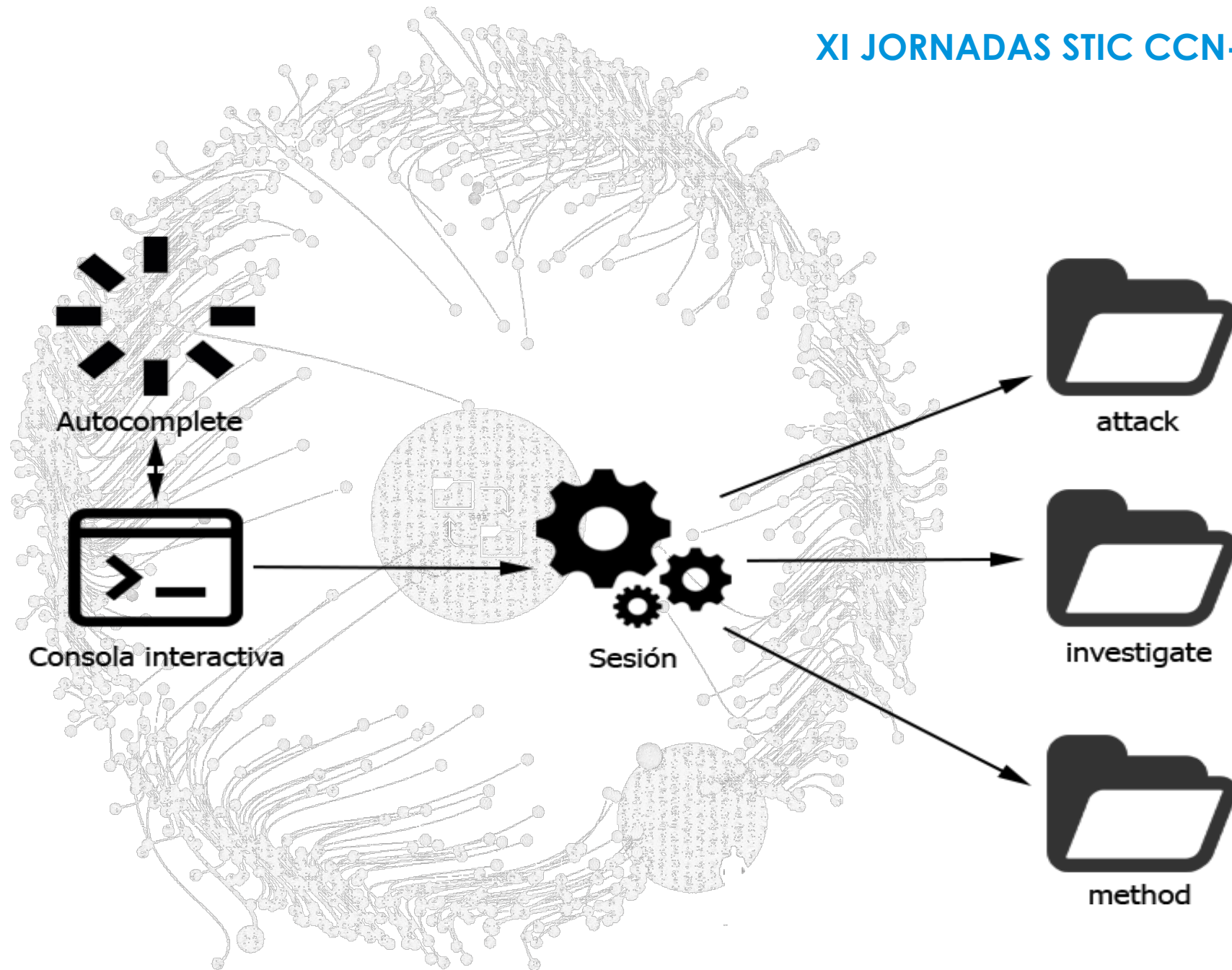
Vía para lograr ejecutar un proceso en un contexto de integridad ALTA (System) evitando que la pantalla de UAC salte



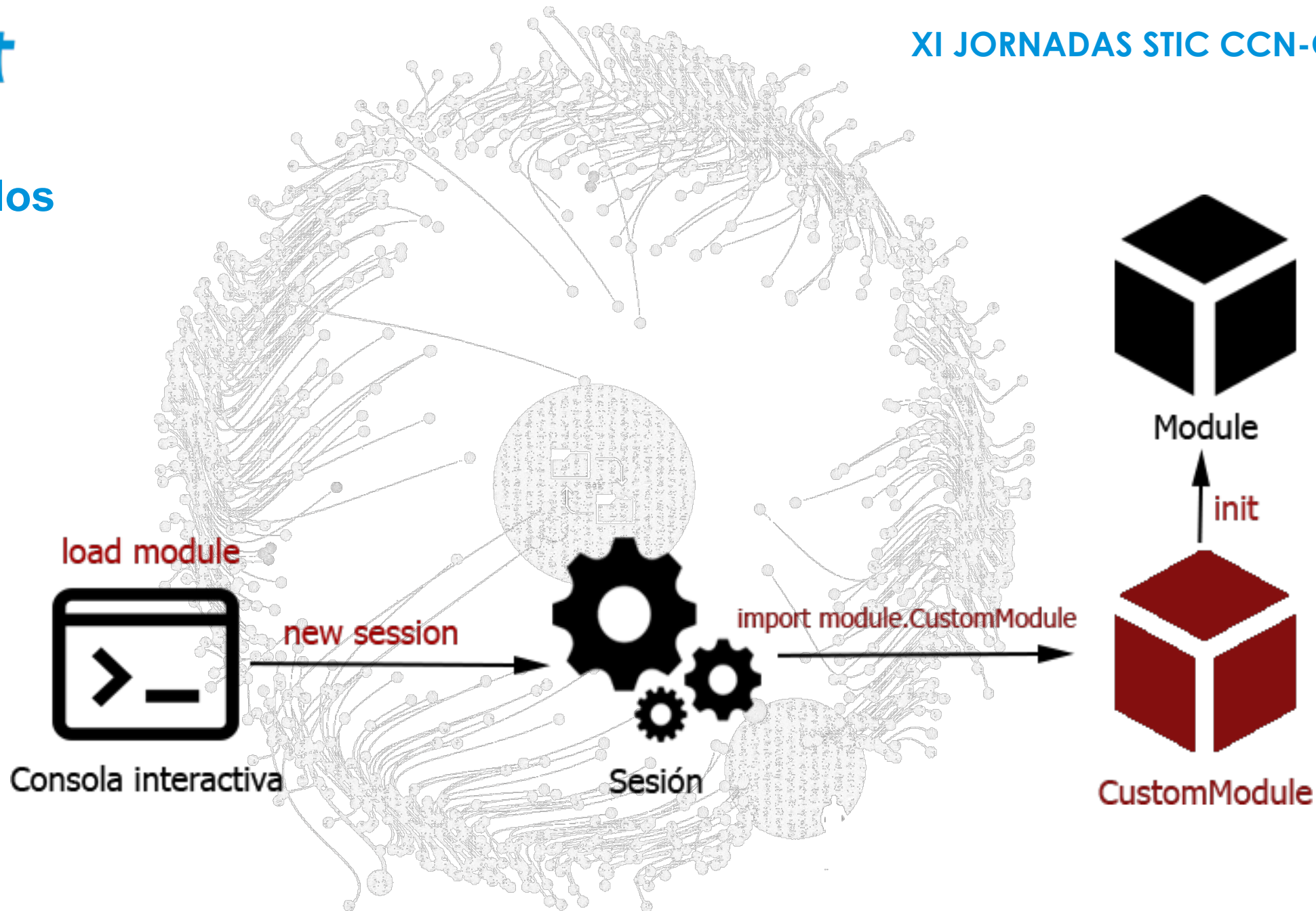
svchost.exe	20,260 K	26,244 K	772 Host Proc...	Microsoft Corp...	
sihost.exe	4,496 K	5,752 K	2628 Shell Infra...	Microsoft Corp...	Medium
taskhostw.exe	6,036 K	5,404 K	2944 Host Proc...	Microsoft Corp...	Medium
cmd.exe	1,564 K	824 K	2840		High
conhost.exe	5,296 K	3,204 K	3592		High



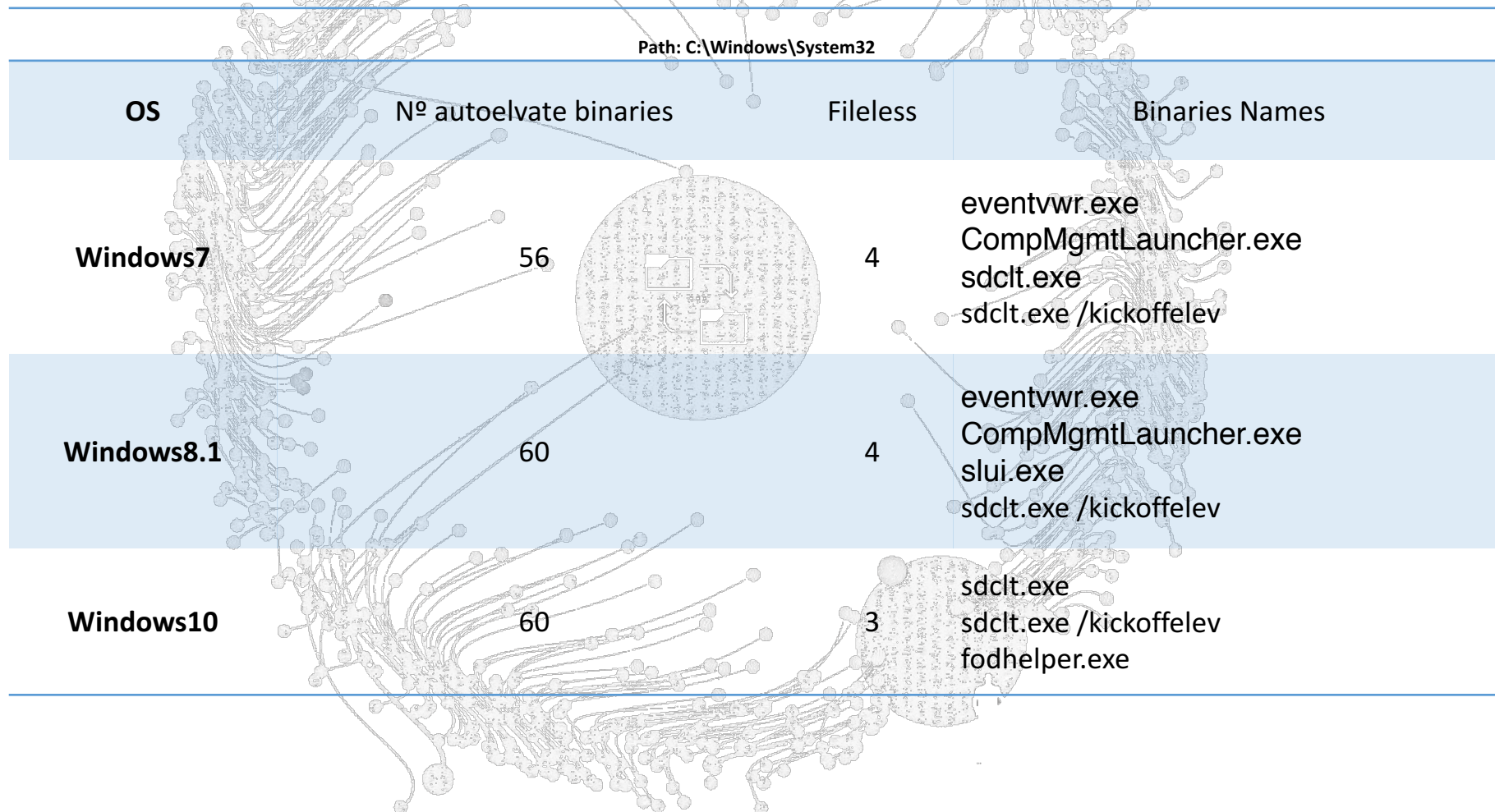
Arquitectura



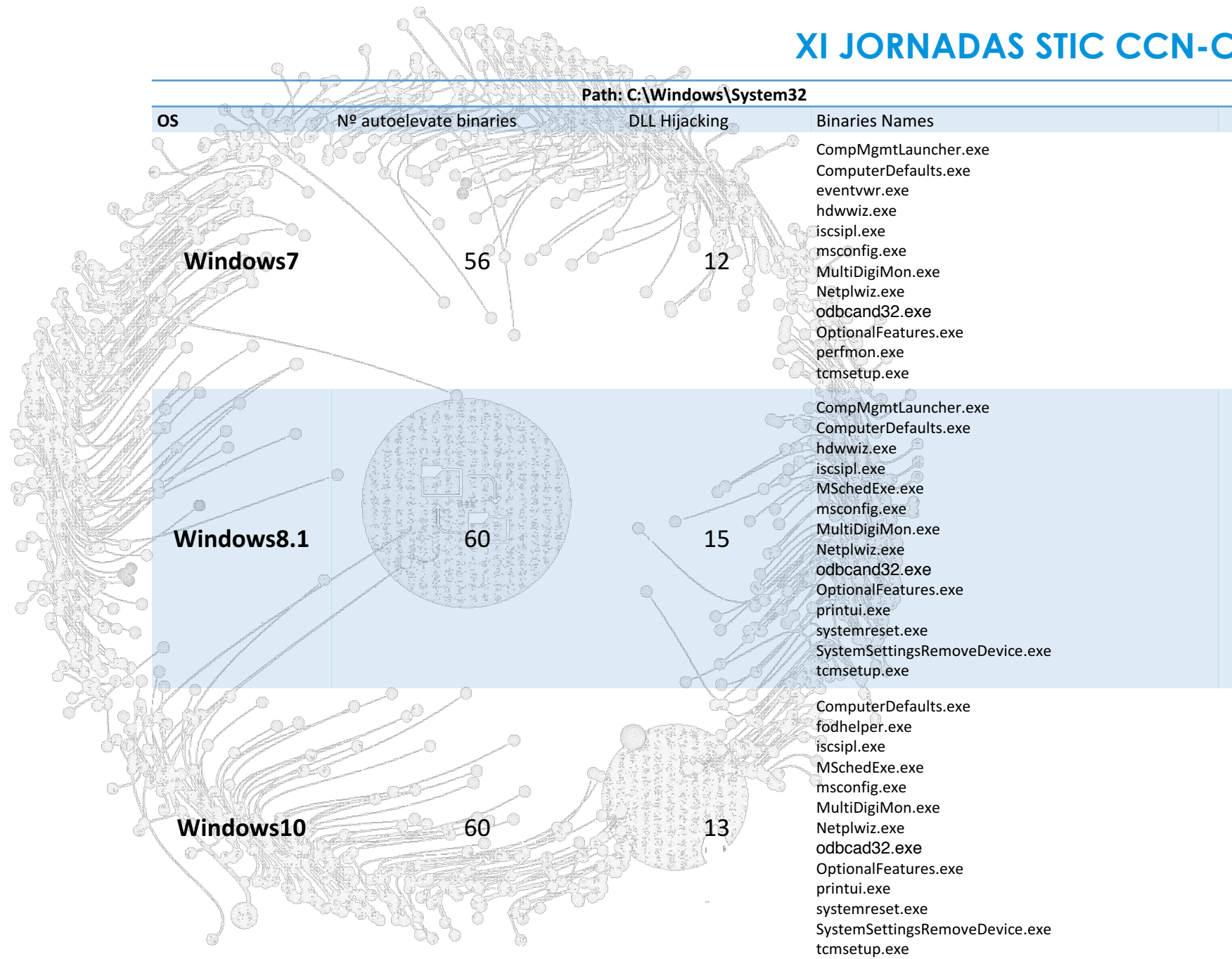
Módulos



Resultados



Resultados



PoC: uac-a-mola en acción



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

