Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 15

Integrantes

Juan Camargo

Diego Castellanos

Profesor

Daniel Esteban Vela Lopez

Bogotá 2024

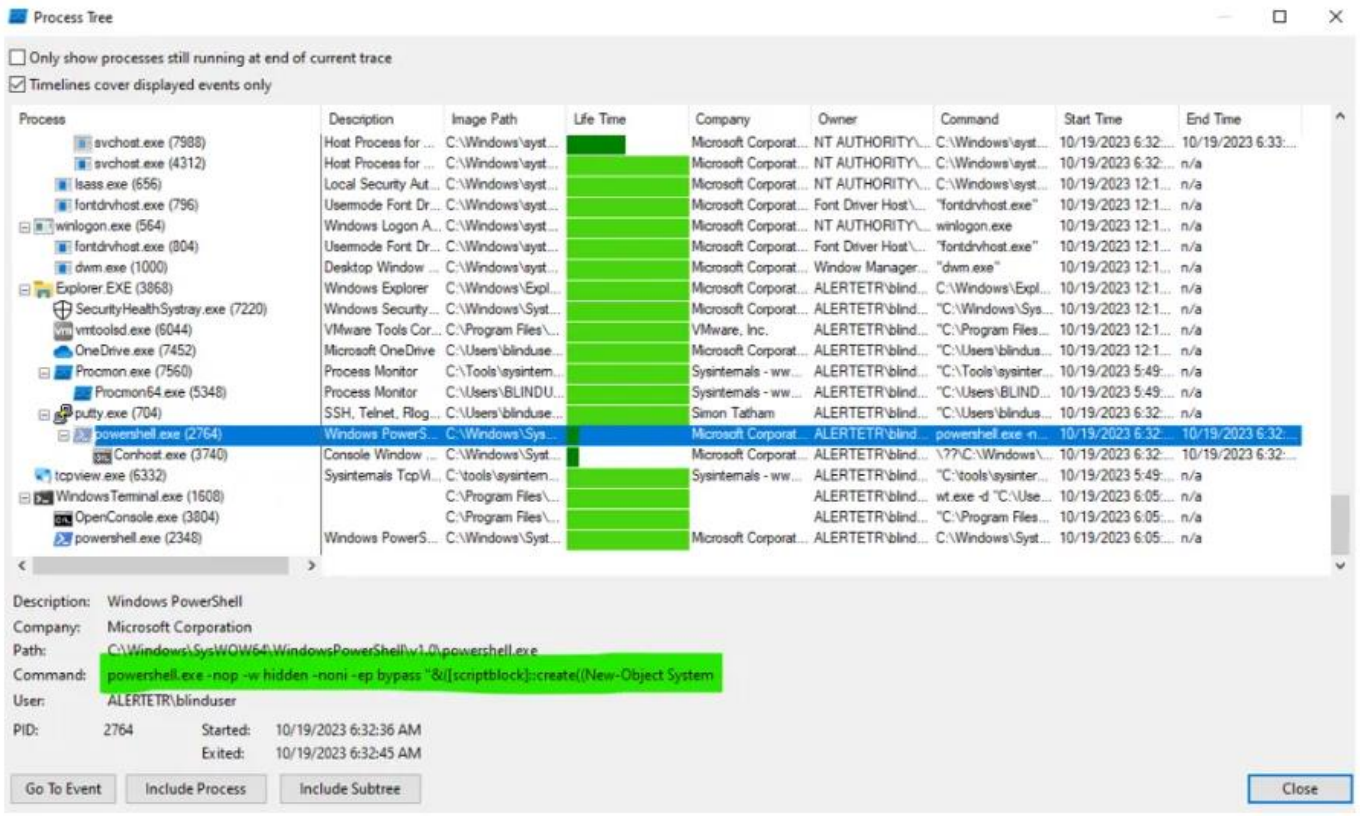
- Describe initial detonation. Are there any notable occurrences at first detonation? Without internet simulation? With internet simulation?

Con la simulación de Internet, se mostró una ventana emergente por un segundo y se cerró automáticamente.

Sin Internet, el proceso de simulación no consultó el dominio que estabamos mirando antes.

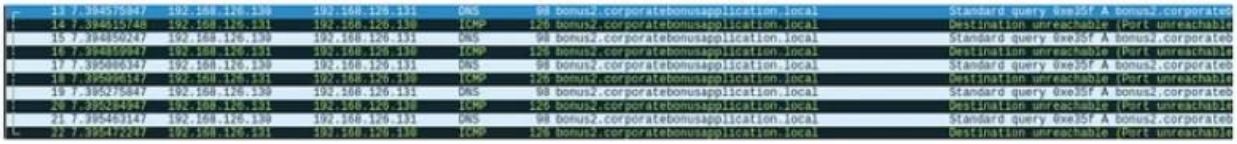
- From the host-based indicators perspective, what is the main payload initiated at detonation? What tool can you use to identify this?

Utilizando procmon Pudimos ver e identificar la carga útil principal, que es un script de PowerShell que se ejecutó después de la ejecución.



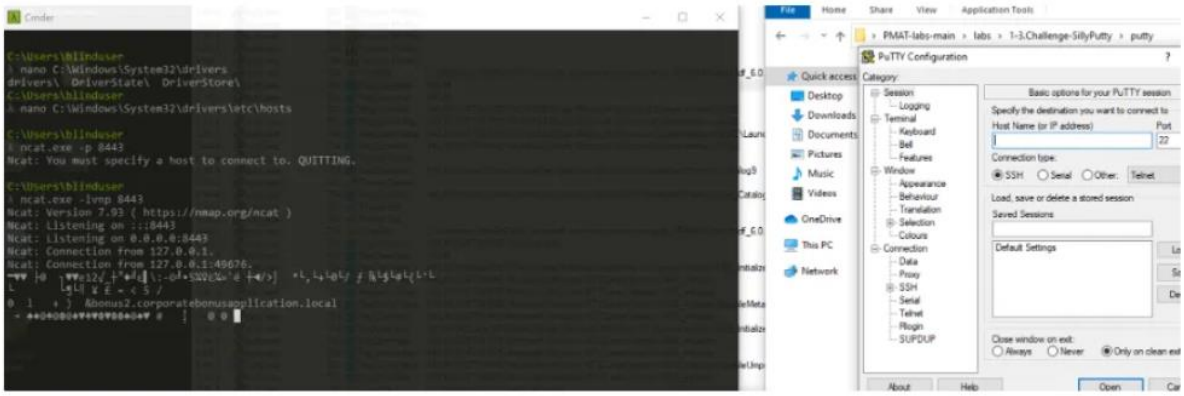
- What is the DNS record that is queried at detonation?

Wireshark registró el tráfico de consultas de registros DNS. La consulta fue el mismo dominio que se ha visto en las cadenas, que es bonus2.corporatebonusapplication. Local



- What is the callback port number at detonation?

8443 es el número de puerto. Esto lo supimos al cambiar el archivo etc/hosts y agregar el dominio solicitado para resolver a 127.0.0.1, que es localhost.



- What is the callback protocol at detonation?

Utilizamos el protocolo TCP en la detonación.

- How can you use host-based telemetry to identify the DNS record, port, and protocol?

Utilizando la salida de cadena se pueden extraer detalles del archivo como un script de Powershell que incluye el número de puerto.

- Attempt to get the binary to initiate a shell on the local host. Does a shell spawn? What is needed for a shell to spawn?

No funcionará porque no tenemos un certificado SSL válido.