Security Alert Detection

ESQL - Suspicious PowerShell Download and Execute Pattern

Original Time: 2025-10-17T16:16:34.709Z

Alert Information

Alert UUID	e9541a2de77d94911abd6cf1150a3c1344aa1504
Rule Name	ESQL - Suspicious PowerShell Download and Execute Pattern
Original Time	2025-10-17T16:16:34.709Z
Event Action	creation

Host Information

Host Name	win-user-1
User Name	vagrant

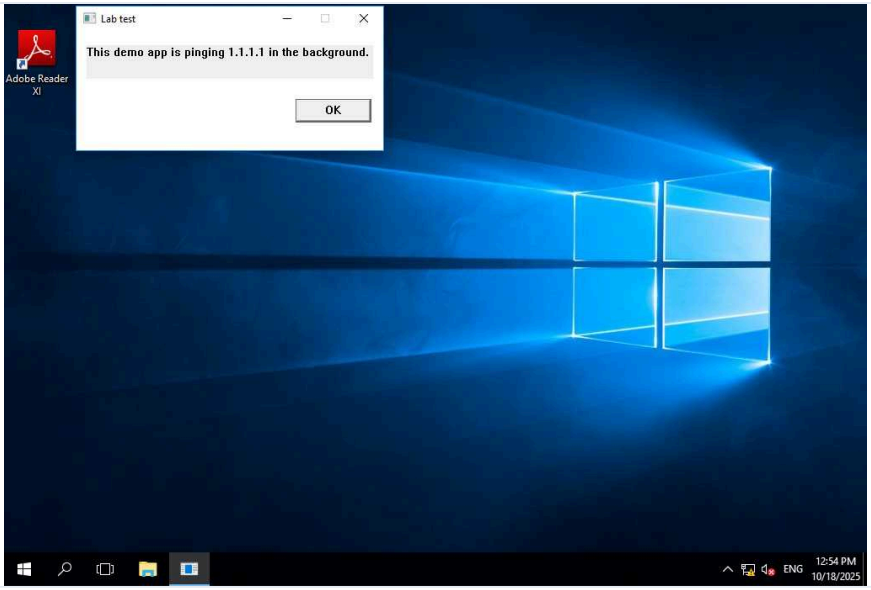
File Information

File Path	C:\Users\vagrant\AppData\Local\Temp\WinPingDemo.exe
File Name	WinPingDemo.exe

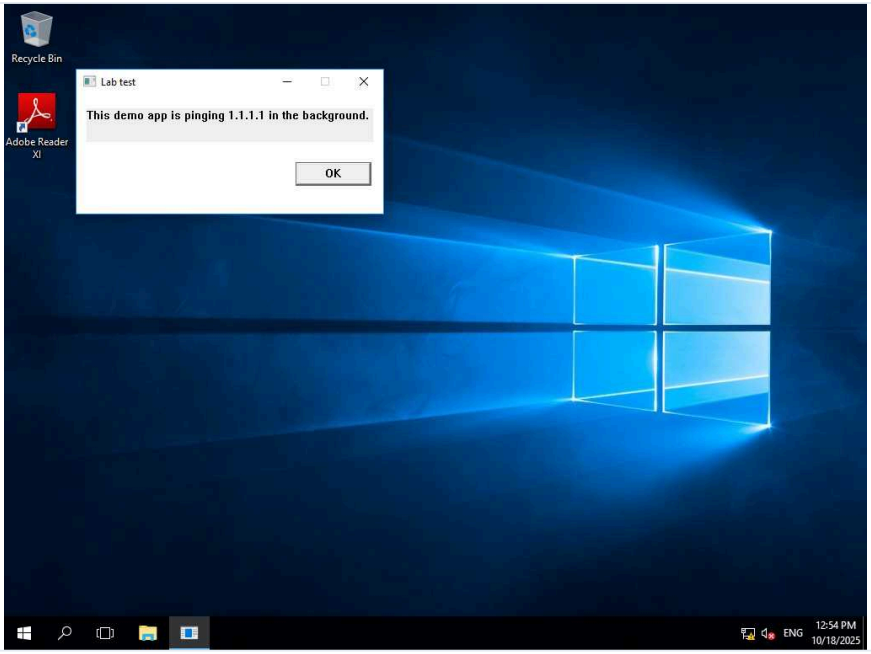
Process Chain (7 processes)

```
"C:\Users\ADMINI~1\AppData\Local\Temp\WinPingDemo.exe"
ping -n 1000 1.1.1.1
c:\windows\system32\svchost.exe -k netsvcs
c:\windows\system32\svchost.exe -k netsvcs -s BITS
c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -s SSDPSRV
c:\windows\system32\svchost.exe -k netsvcs -s wlidsvc
C:\Windows\System32\svchost.exe -k wsappx -s ClipSVC
```

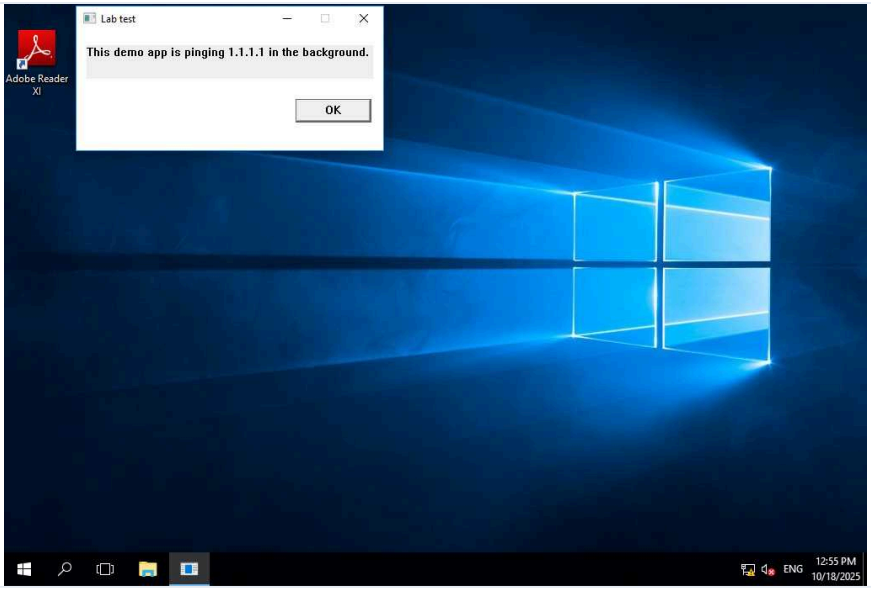
Evidence Screenshots (3 files)



27151.jpg



31376.jpg


Lab test
This demo app is pinging 1.1.1.1 in the background.
OK
Adobe Reader XI
ENG
12:55 PM
10/18/2025

43136.jpg