RSAConference2019
San Francisco | March 4–8 | Moscone Center


SESSION ID: SEM-M03H

# Combatting the Scourge of Fileless Attacks

**Stuart McClure**

President
BlackBerry | Cylance
@HackingExposed

**Brian Robison**

Chief Evangelist
BlackBerry | Cylance
@CylanceSecTech

# Fileless attacks

- Goal is to avoid the use of malware or other more “visible” tools
  - Use whitelisted/allowed applications
  - Existing software “live off the land”
  - Non-malware executables
  - Vulnerabilities/Exploit Memory
  - Scripts/PowerShell/VBScript/JavaScript – HIGHLY obfuscated
- Initial Vector
  - Most common vector == Email
    - Macro -> PowerShell -> Download (malware) or directly into memory

# Weaponizing Documents

- Embedding malware in document
- DDE
  - Different file types (.iqy)
  - Control the error messages
    - Not the normal “yellow” warning
- VBScript Macro
  - Standard “Enable Macros” warning
  - User’s are trained

RSAConference2019

# Demo: Weaponizing Documents

# Combatting Fileless Attacks

- Gauge the effectiveness of existing solutions:
  - Add fileless attack simulations to your existing exercises
- Utilize GPOs to enforce policies around Macros/DDE
- Look for solutions that “go beyond”:
  - Beyond on-disk malware detection
  - Prevent the malicious use of PowerShell/macros/memory-exploits
  - Don’t rely on behavioral detection only – usually too late
- Implement and continually re-verify
  - Continual education and testing improvements

RSAConference2019

# THANK YOU!