RSAConference2019
San Francisco | March 4–8 | Moscone Center

HACKING EXPOSED: LIVE
Bypassing ”NextGen”

Stuart McClure
President
BlackBerry | Cylance
@HackingExposed

Brian Robison
Chief Evangelist
BlackBerry | Cylance
@CylanceSecTech

Agenda

- Back to the Future hacks
- New ones: Playing in memory and in plain sight
- The BIG BANG in 5 seconds or less…
- What can I do???

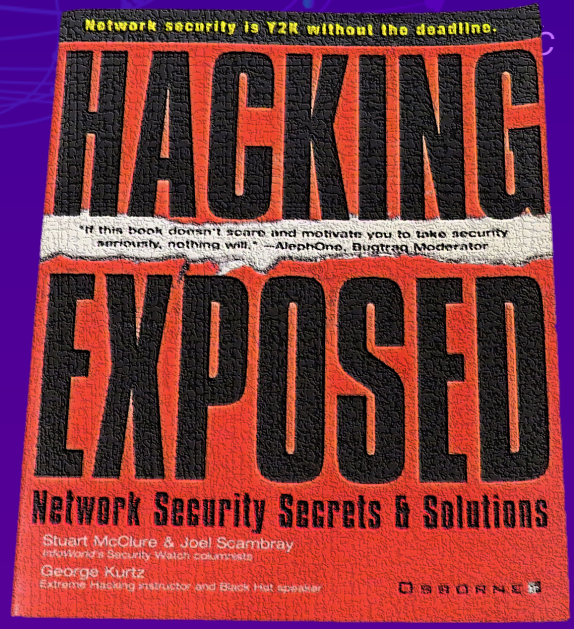
Where do these come from?

- Real-world customers who hired Cylance Professional Services
- Discovered “in-the-wild” attacks that bypassed Next Gen
  - Reverse engineered how those attacks bypassed
- Tracking on researchers dedicated to bypasses
  - Developed tools and techniques using available tech
- No product naming and shaming … just education

RSAConference2019

The “Simple” Methods

“Back to the Basics”



Flashback: Hacking Exposed - 1st Edition

1. File Pumping and Binary Padding
   - Performance or cloud upload not available
2. DLL Hijacking/Side Loading
   - Trusted execution – replace legitimate DLL with malicious code
   - Direct execution – RunDLL32
3. Command obfuscation or simply copying/renaming PowerShell
4. Unhooking
5. No “cloud” == BYPASS!

RSAConference2019

THE NEW “FUN” METHODS

RSAConference2019

FUN WITH MEMORY

DEMO TIME!

RSAConference2019

HIDING IN PLAIN SIGHT

DEMO TIME!

RSAConference2019

MORE FUN IN MEMORY

DEMO TIME!

RSAConference2019

THE ”BIG BANG” IN LESS THAN 5 SECONDS

DEMO TIME!

What can we do???

- Least privileged access to very powerful tools
- Continued education around dangers of attachments
- Do not rely on “white-listing”
- Use GPOs to enforce policies around DDE and Macros
- Signing approved internal scripts
- Do not rely on the “cloud”

RSAConference2019

THANK YOU!