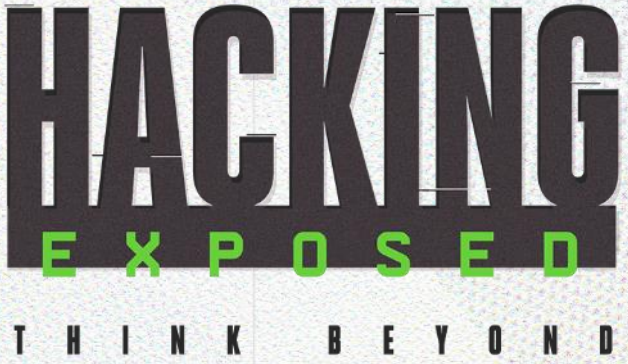
Cylance Webinar Series//
Presented:
March 21/22, 2019

Bypassing Next Gen



Presented By //
Stuart McClure, President
Brian Robison, Chief Evangelist

BlackBerry | CYLANCE

HOUSEKEEPING

- Audio will sound best streamed through your computer
- Please submit questions via the Q&A tool
- Links to the recording and presentation will be sent to you in the next few days
- Your feedback is essential, topics/ideas – brobison@cylance.com
- Need help with the webinar? Contact us at: webinars@cylance.com

BlackBerry | CYLANCE

HACKING EXPOSED
THINK BEYOND

SPEAKERS

Stuart McClure

President
BlackBerry | Cylance
@stuartmcclure
@hackingexposed

Brian Robison

Chief Evangelist
BlackBerry | Cylance
@CylanceSecTech

BlackBerry | CYLANCE

HACKING EXPOSED
THINK BEYOND

AGENDA

- Back to the Future Hacks
- New “Fun” Methods:
  - Leverage Trusted Execution - CACTUSTORCH and HTA
  - Hiding in Plain Sight - TrevorC2 with a Malicious Document
  - Playing with Memory - Self-Exploiter
- The BIG BANG!
- What can I do???

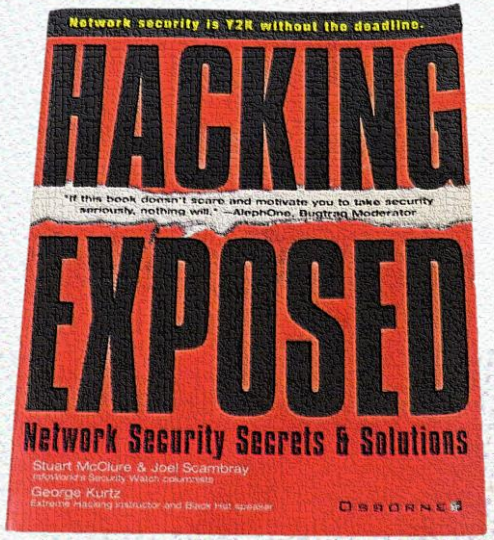
WHERE DO THESE COME FROM? . . . .

- 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 or shaming … just education

Back to the Future Hacks

BlackBerry | CYLANCE

“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!

BlackBerry | CYLANCE

HACKING EXPOSED
THINK BEYOND

HACKING EXPOSED

THINK BEYOND

New “Fun” Methods

BlackBerry | CYLANCE

HACKING EXPOSED

THINK BEYOND

Leverage Trusted Execution

CACTUSTORCH and HTA

BlackBerry | CYLANCE

CACTUSTORCH: BACKGROUND

- July 2017
- Author: Vincent Yiu (@vysecurity)
- Javascript and VBScript shellcode launcher.
- Spawns a 32-bit version of the binary specified and injects shellcode into it.
- Payload types supported: VBS, VBA, JS, JSE, WSF, HTA, VBE

- https://github.com/mdsecactivebreach/CACTUSTORCH

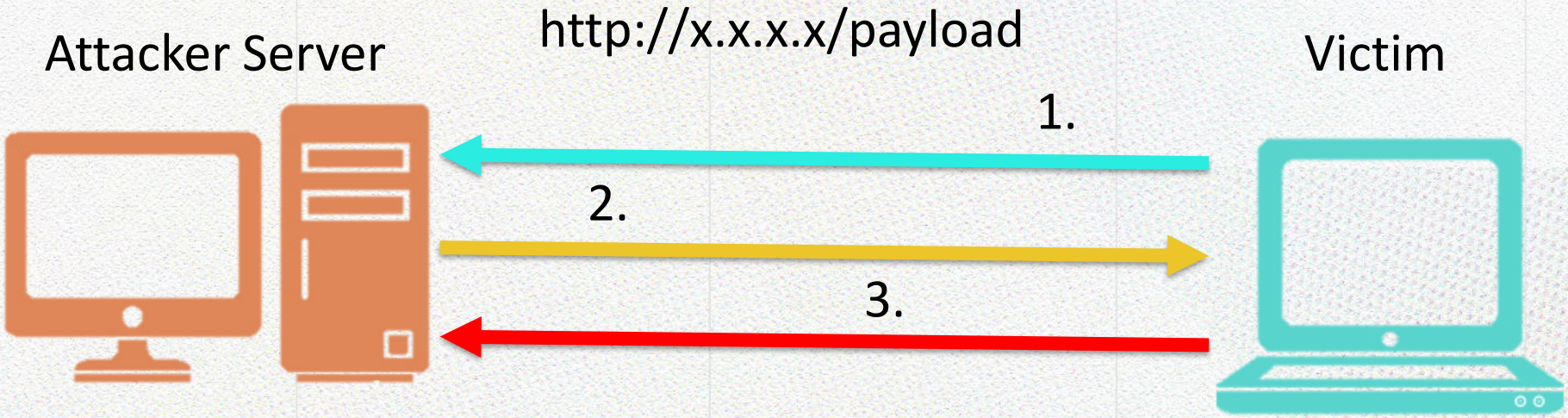
CACTUSTORCH: HOW IT WORKS…. . .

- Select binary “rundll32.exe”, “notepad.exe”, “calc.exe”, etc.
- Generate 32-bit raw shellcode (MSF, Cobalt Strike, other)
- Base64 encode the shellcode
- Copy this payload into the “code =” variable in Javascript/VBScript
- Run wscript.exe CACTUSTORCH.js/CACTUSTORCH.vbs via command line on target – or HTA file with MSHTA.exe
- Can easily infect Word docs using macros as well.

CACTUSTORCH: WHY DOES IT BYPASS?

- Very effective with HTA
  - Many NextGen technologies block JS, JSE, VBA etc.
  - Leverages trusted executable mshta.exe and wraps code with HTML
- Difficult to detect at the network layer
  - Obfuscated commands
  - HTTPS
- Generic Signatures detect MSF payload or post-execution

CACTUSTORCH: STEP BY STEP



A. Attacker hosts CACTUSTORCH file on webserver
B. MSF listener awaits the connection

1. Victim clicks on website
2. Victim downloads CACTUSTORCH HTA file
3. Victim runs payload and connects back to Attacker using HTA

BlackBerry | CYLANCE

HACKING EXPOSED THINK BEYOND

HACKING EXPOSED

THINK BEYOND

Leverage Trusted Execution – DEMO!

CACTUSTORCH and HTA

BlackBerry | CYLANCE

HACKING EXPOSED

THINK BEYOND

Hiding in Plain Sight

TrevorC2 with Malicious Document

BlackBerry | CYLANCE

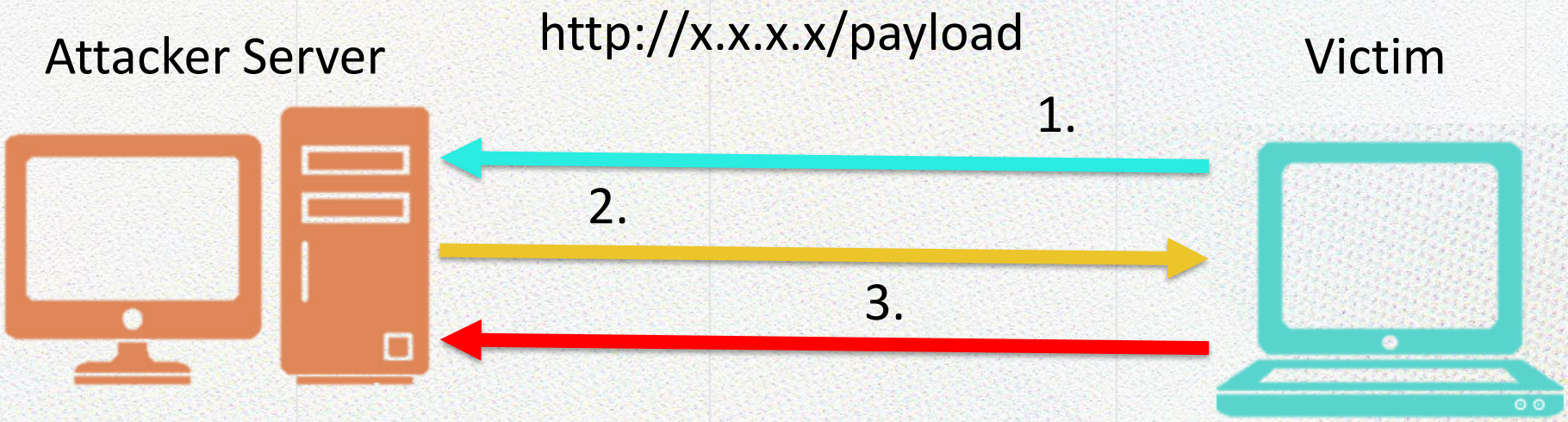
TREVORC2 WITH MALICIOUS DOCUMENT: BACKGROUND

- TrevorC2 tunnels C2 through a legitimate website
  - Clones any site upon launch
  - C2 commands are Base64 encoded with custom string
  - HTTPS is NOT required
  - Does NOT use POST for exfil
- https://github.com/trustedsec/trevorc2
- Malicious Document
  - Macros/VBA
  - Obfuscated VBA

TREVORC2 WITH MALICIOUS DOCUMENT: WHY DOES IT BYPASS?

- TrevorC2 – NO SHELLCODE! Native clients
- Malicious Documents
  - Macro/VBA Seen in the wild with APT32/OceanLotus
- Obfuscated Commands
- Lateral movement using WebDAV
- Executes directly in memory – no file on disk

TREVORC2 WITH MALICIOUS DOCUMENT: STEP BY STEP



A. Attacker hosts webserver with clients
B. TrevorC2 Server listener awaits
C. WebDAV server

1. Victim opens document/attachment
2. Macro/VB downloads client
3. Macro executes client and connects back to C2

BlackBerry | CYLANCE

HACKING EXPOSED THINK BEYOND

HACKING EXPOSED

THINK BEYOND

Hiding in Plain Sight – DEMO!

TrevorC2 with Malicious Document

BlackBerry | CYLANCE

HACKING EXPOSED

THINK BEYOND

Playing in Memory

”Self-Exploiter”

BlackBerry | CYLANCE

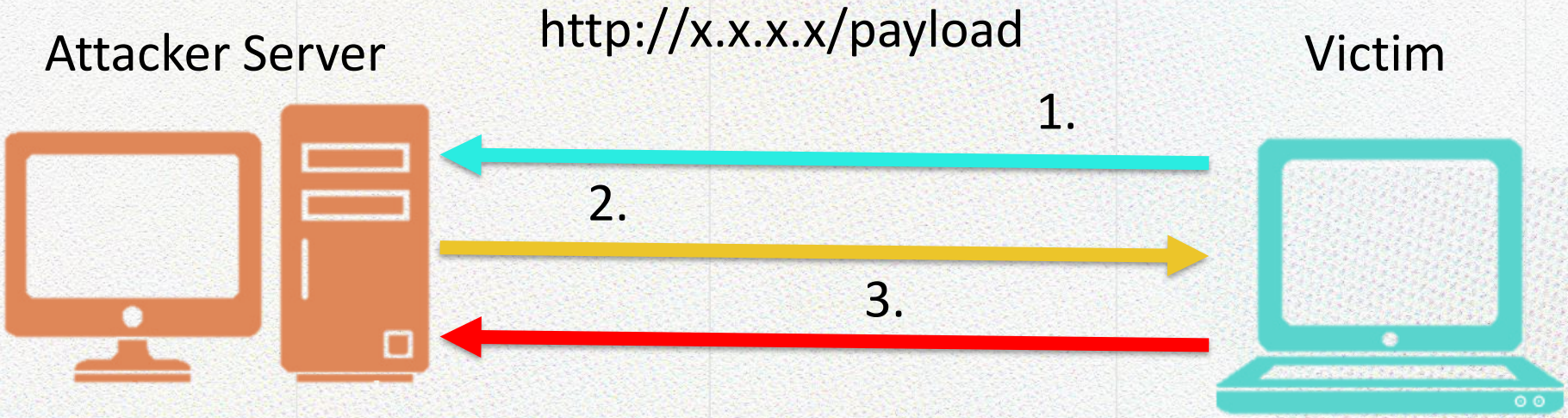
SELF-EXPLOITER: BACKGROUND . . .

- Exploits an intentional (~1990's tech) buffer overflow (via strcpy)
- Stack is marked as executable via VirtualProtect API
- Shellcode executes after it is jumped to via JMP ESP/RSP

SELF-EXPLOITER: WHY DOES IT BYPASS?

- Next Gen Fails:
  - to detect the stack smashing
  - to detect the forced RWX change
  - to detect the shellcode executing

SELF-EXPLOITER: STEP BY STEP . . .



A. Attacker hosts self-exploiter exe file on webserver
B. MSF listener awaits the connection

1. Victim clicks on website
2. Victim downloads self-exploiter exe
3. Victim runs exe, memory exploited, connects back to Attacker

BlackBerry | CYLANCE

HACKING EXPOSED THINK BEYOND

HACKING EXPOSED

THINK BEYOND

Playing in Memory – DEMO!

”Self-Exploiter”

BlackBerry | CYLANCE

HACKING EXPOSED

THINK BEYOND

The “Big Bang”

Stuart’s Challenge to Brian…

BlackBerry | CYLANCE

A LIFETIME TO BUILD YOUR CAREER. FIVE SECONDS TO LOSE IT!

- Use a previous method to:
  - Exfiltrate some sensitive data
  - Destroy the evidence/system

BlackBerry | CYLANCE

HACKING EXPOSED
THINK BEYOND

A LIFETIME TO BUILD YOUR CAREER. FIVE SECONDS TO LOSE IT!

- Use a previous method to:
  - Exfiltrate some sensitive data
  - Destroy the evidence/system

- BONUS POINTS!!!!
  - “Dwell time” < 5 seconds
  - Windows 10 v1809 fully “protected?”

A LIFETIME TO BUILD YOUR CAREER. FIVE SECONDS TO LOSE IT!

- Use a previous method to:
  - Exfiltrate some sensitive data
  - Destroy the evidence/system
- BONUS POINTS!!!!
  - “Dwell time” < 5 seconds
  - Windows 10 v1809 fully “protected?”

1. Exfil all files on the desktop
2. Destroy the MBR and reboot

HACKING EXPOSED

THINK BEYOND

The “Big Bang” – DEMO!

Stuart’s Challenge to Brian…

BlackBerry | CYLANCE

A lifetime to build your career…

LESS THAN five seconds to lose it!

BlackBerry | CYLANCE

WHAT CAN WE DO???

- Least privileged access to very powerful tools/users as local admins
- System hardening, firewalling to prevent C2 communication
- 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”

WHAT'S NEXT?

- Hacking Exposed Webinars
- Next webinar 3/28 - Cylance vs. Hacking Exposed: Bypassing NextGen
  - www.cylance.com/webinars

- Follow Us
  - Stuart McClure @HackingExposed
  - Brian Robison @CylanceSecTech

BlackBerry | CYLANCE

HACKING EXPOSED
THINK BEYOND

HACKING EXPOSED

THINK BEYOND

[redacted] QUESTIONS [redacted] AND ANSWERS

[redacted]

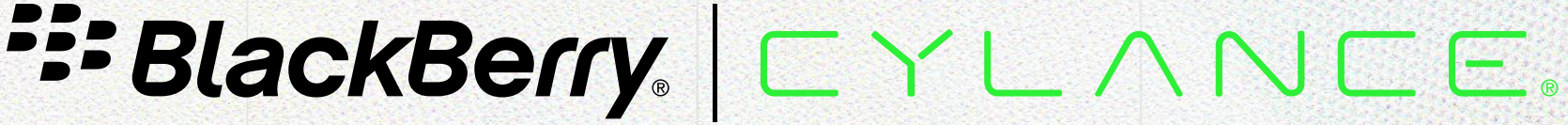
BlackBerry | CYLANCE

HACKING EXPOSED

THINK BEYOND

THANK YOU

BlackBerry | CYLANCE


BlackBerry®
CYLANCE®