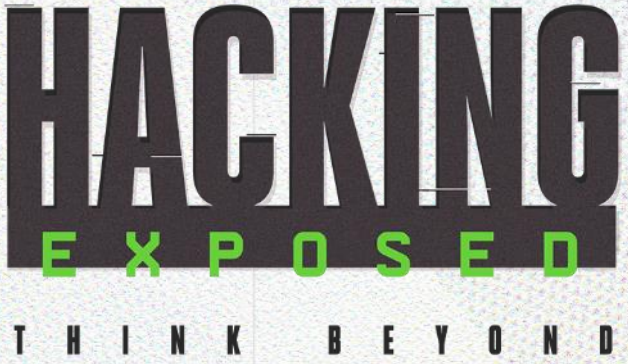
[redacted]

Cylance Webinar Series//

Presented:

June 28, 2018



[redacted] **Presented By //**

Stuart McClure, CEO Cylance, CNE, CCSE, [redacted]S

Brian Robison, Sr. Dir. of Security Tech[redacted]y

Evil Bob, Security Re[redacted]

HOUSEKEEPING

- Audio will sound best streamed through your computer
- Please submit questions via the Q&A box
- We will post additional resources in the chat box
- Your feedback is essential, please the polling questions at the end of the webinar
- Links to the recording and presentation will be sent to you in the next few days
- Need help? Contact us at: webinars@Cylance.com

HACKING EXPOSED
THINK BEYOND

SPEAKERS

Stuart McClure

CEO and co-Founder at Cylance

@stuartmcclure

@hackingexposed

Evil Bob

Security Researcher at Cylance

Brian Robison

Sr. Director of Security Technology at Cylance

@CylanceSecTech

HACKING EXPOSED

THINK BEYOND

Why “Think Beyond”?

Questioning the status quo…

THINK BEYOND

- *Apple and Steve Jobs' "Think Different"*
- More layers <> security
- Compliance <> security
- Predictive Prevention is possible
- Reimagine your endpoint, stack, architecture
- Don't "outsource" your decision making
- Threat centric prevention, before detect and respond

AGENDA

- **Bypassing Traditional AV and Endpoint Security**
  - Very Simple Methods
    - Mutation/Packing/Crypting
  - Injecting shell code directly into memory – AKA fileless
    - Non-malicious file
  - Using valid executables
    - Modifying the flow of application execution
- **One more thing…**

WHY IS IT SO EASY TO BYPASS

- Security industry is largely a “detect and respond” model
- Endpoint tools are primarily based on signatures for prevention
  - Requires sacrificial lamb
  - Requires humans
  - Requires constant updates with limited scope
- Even network security is largely signature based
  - Same issues as above
- URL/web security is the same
- Behavioral/heuristics requires bad code to run

- Serious hackers build their own tools to evade/bypass

Hands On

Time to bypass endpoint security for fun and profit

HACKING EXPOSED

THINK BEYOND

Mutation/Packing/Crypting

Mpress, upx, others [redacted]

MUTATION/PACKING/CRYPTING

- Simply changing the hash (MD5, SHA etc.) of a file can defeat signatures
- Can change file by 1-bit – create a unique hash
- Use off the shelf packers
  - Mpress
  - UPX
- Signatures are written to detect “packed” files

- Hiding the payload
  - AegisCrypter

HACKING EXPOSED

THINK BEYOND

DEMO

Mutation/Packing/Crypting

HACKING EXPOSED

THINK BEYOND

Injecting shellcode

Veil Framework and Shellter

DIFFERENT METHODS OF INJECTING SHELLCODE

- **Offensive security testing**
- **Directly inject shellcode into memory – no malicious file on disk**
  - By script
  - By non-malicious exe
- **Veil Framework**
  - Turn an arbitrary script or piece of shellcode into a Windows executable
  - Evade detection by common antivirus products
- **Shellter**
  - No additional code is added to the binary in terms of code caves or resource files
  - - Dynamically modifies the flow of an application to run shellcode on a system
  - - No additions to the binary in a predictable way, means no signature to queue off
  - - It only runs with standalone 32 bit binaries, but there are loads of them around, if you are struggling to find some, SysInternals has a few to choose from
  - - In stealth mode the original functionality of the application can be preserved
  - - There are ways to make legitimate binaries do malicious things

One more thing…

Putting it all together and weaponizing [redacted]

TREVOR C2

- Written by Dave Kenedy and Trusted Sec (you must give him a hug and a beer if you see him at a con)
- Uses legitimate website requests as the communication method for the C2 channel
- Evades traffic signatures for known C2 channels, via base 64 encoded cipher text
- Emulates the ability to create your own malware backdoors

- “Think beyond” well known tools for testing

COUNTERMEASURES

- **AI is NOT just a feature; it IS the future**
  - Generations of AI
  - AI to build sig
- **Detect and Respond is ok – but…**
  - Not scalable without an endpoint security solution that can PREVENT w/o signatures
    - By the numbers:
    - Traditional AV ~50-60% detection on unknown – leaves 50-40% for EDR/humans
    - AI AV (Cylance) - >99% prevention – leaves <1% for EDR/humans
  - Requires a prevention first strategy rather than reacting after a breach
- **Players????**
  - Cylance
  - Endgame
  - Invincea ?

HACKING EXPOSED

THINK BEYOND

QUESTIONS AND ANSWERS

Polling Questions

THANK YOU

CYLANCE