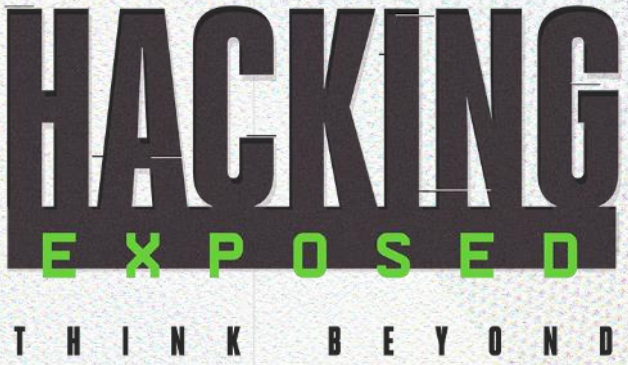
[redacted]

Cylance Webinar Series//
Presented:
March 29th, 2018

CYLANCE

VS



[redacted] **Presented By //**

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

[redacted]

Brian Robison, Sr. Dir. of Security Technology

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

Brian Robison

Sr. Director of Security Technology at Cylance

@CylanceSecTech

HACKING EXPOSED

THINK BEYOND

RSA 2018

HACKING EXPOSED: NEXTGEN AI POWERED

APRIL 18, 2018
3:00-3:45PM
MOSCONE WEST 2004

STOP BY OUR BOOTH IN THE NORTH HALL #3911
LIVE DEMOS + PROMO GIVEAWAYS!

Agenda

- Meltdown/Spectre exploitation
- Middle East targeting of nuclear power plants globally
- Adversarial AI

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

- Quick Recap of HE: DLLs
- Cylance VS HE: DLLs
- Cylance 101 and Tech to Prevent
- Hands On
- Q&A

HACKING EXPOSED
THINK BEYOND

Quick Recap of HE: DLLs

What did we do last time?

RECAP FROM LAST HACKING EXPOSED

- What is a DLL
- Are DLLs a Threat?
- Some Real World Examples Using DLLs
  - LSADUMP2
  - OPM
  - SHELL_CREW
  - Customer ?????
- Hands On!
  - Direct Execution Utilizing `rundll32.exe` – malicious Not-Petya
  - Exploiting the inherent trust with `rundll32.exe`
  - DLL Hijacking and Side-Loading Examples
- Weaponization
  - Hancitor
- What can we do?

HACKING EXPOSED

THINK BEYOND

Cylance VS HE: DLLs

What can Cylance do to protect me?

CYLANCE 101

CylancePROTECT®

- AI-Driven Malware Prevention
- Memory Exploit Prevention
- Script Management
- Device Policy Enforcement
- Application Control for fixed function devices

Pre-execution Prevention

CylanceOPTICS™

- AI-Driven Incident Prevention
- Dynamic Rule-Based Threat Detection
- Root Cause Analysis
- Smart Threat Hunting
- Aggressive Containment
- Automated Incident Response

Near Zero Latency Incident Prevention

CYLANCE TECH USED TO PREVENT DLL ATTACKS

CylancePROTECT

- AI/ML-based PE detection
  - Pre-Execution
    - Malicious DLL execution
  - Resident On Disk
    - BTD/File Watcher
- Script Control
  - PowerShell/JavaScript/VB
- Memory/Exploit Prevention

CylanceOPTICS

- Non-Malware Behavioral Prevention
  - RunDLL JavaScript Invocation
  - Fileless PowerShell Malware
  - PowerShell Download
  - MITRE ATT&CKs
    - Netsh DLL Persistence

Hands On

Hands on examples of techniques and Cylance prevention.

DIRECT EXECUTION - UTILIZING RUNDLL32.EXE

Part of the trusted base OS – can also be leveraged to execute scripts and download a hosted payload

- Execute malicious DLL by running it directly with RunDLL32.exe
- Malware Demo – Not-Petya/Petya-Like

- CylancePROTECT prevents the execution of the malicious code
- File Watcher will find the dll after being copied

HACKING EXPOSED

THINK BEYOND

DEMO

Direct Execution

EXPLOITING TRUST: RUNDLL32.EXE'S TRUSTED STATUS

Rundll32.exe can be used to execute script, download and execute code

- Using Metasploit to setup a dropper website
- Execute script using rundll32.exe to download dropper and execute directly into memory
  - No file to disk – bypasses AV as well as AppLocker/Software Restriction Policies

- CylancePROTECT Script Control will prevent the use of JavaScript and PowerShell
- If Script Control is disabled, CylanceOPTICS steps in a prevents the behavior

HACKING EXPOSED

THINK BEYOND

DEMO

Exploiting Trust

DLL HIJACKING/SIDE-LOADING

When programs require additional DLLs that get loaded at runtime and on demand; it's possible to take advantage of this and have a legitimate program load a malicious DLL.

- DLL hijacking demo
  - Build a malicious DLL using MSFVenom
  - Trick InternetExplorer into executing the DLL by replacing a legitimate DLL
  - Opens a reverse shell to Metasploit

- CylancePROTECT will detect the malicious DLL same result as direct execution

HACKING EXPOSED

THINK BEYOND

DEMO

Hijacking/Side-Loading

DLL PERSISTENCE TECHNIQUES MITRE ATT&CK

DLLs offer great persistence options because it's normal to see rundll32.exe and dlls listed in the registry.

- Netsh can be used as a persistence proxy technique, firewall control, pivoting, sniffing and as a wireless backdoor – ATT&CK ID T1128

- CylancePROTECT will detect the malicious DLL same result as direct execution
- CylanceOPTICS will detect the non-malware based behavior

HACKING EXPOSED

THINK BEYOND

DEMO

MITRE ATT&CK: DLL Persistence

HACKING EXPOSED

THINK BEYOND

Weaponization.

Bringing it all together.

DLL WEAPONIZATION

- Phishing and Social Engineering
  - Getting a user to reveal credentials
  - Tricking a user into opening an exe disguised as a folder or a document
  - Downloading seemingly benign programs and running them
  - Weaponized attachments like Hancitor (dll code executed directly into memory)
- Attackers placing malicious DLLs in packages of legitimate software
- Poorly written software that fails to validate dependencies

BONUS: HANCITOR

- Weaponized Word document
- Tricks user into enabling macros to see hidden content
- Macro code is very special
  - Wrote their own base64 decoder
  - Payload (Hancitor) was encoded and embedded within a secret form field in the VBA project
  - Uses native Windows API calls instead of VBA APIs to directly run the binary
  - No files dropped to disk
  - Makes a copy of a legitimate system DLL, executes and suspends the process
  - Replaces that code with the malicious code and resumes the process
  - Contacts C2 to obtain further RATs

HACKING EXPOSED

THINK BEYOND

DEMO

Hancitor

HACKING EXPOSED

THINK BEYOND

DEMO

One more thing…

CYLANCE

HACKING EXPOSED

THINK BEYOND

QUESTIONS AND ANSWERS

Polling Questions

HACKING EXPOSED

THINK BEYOND

THANK YOU

CYLANCE