
2015
AEGIS Policyholders' Conference
AEGIS


Tales of a Real-Life Hacker
Jon Miller
Vice President of Strategy
Former ethical hacker of energy company operations
Cylance
2015 PHC
AEGIS

CYLANCE

Failures of Modern Day Information Security Programs | Tales from a real life ethical hacker ...

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Introduction

Jon Miller

Vice President of Strategy

5 Years Internet Security Systems X-Force Penetration Testing Team

Accuvant Labs (7 years)

- Penetration Testing
- Reverse Engineering
- Weaponized Oday Sales

Cylance (1 Year)

- Internal Security
- Product Testing/Efficacy
- SPEAR Research Team

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Introduction

Stuart McClure
CEO/President and Founder

Leader of Cylance as CEO and Visionary.

Hacking Exposed
- Lead Author
- Creator
- Most Successful Security Book of All Time

Foundstone

WW-CTO McAfee

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Introduction

Ryan Permeh
Co-Founder and Chief Scientist

THE brain behind the mathematical architecture and new approach to security.

Eeye Retina, Securells

Code Red

Chief Scientist - McAfee

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

What is Cylance?

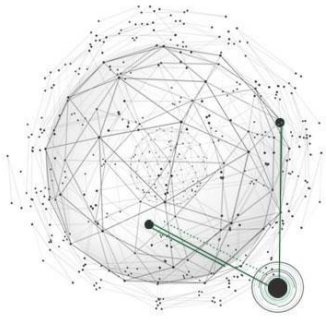
Detecting the Undetectable

First NG-Antivirus (MSFT, PCI, 3rd party testers)

Unlike Traditional A/V

- Signatures
- Cloud Hashing
- Dynamic Heuristics

Machine Learning Based Static Analysis



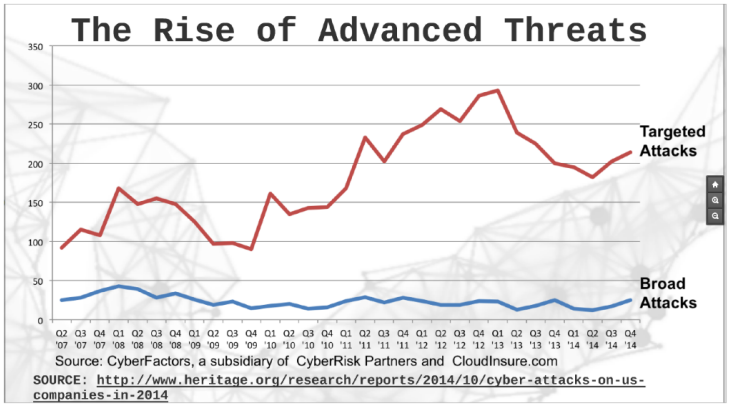
CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

What is the Problem?

The Rise of Advanced Threats



CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

What is the Problem?

The Rise of Advanced Threats

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

What is the Problem?

Adversaries

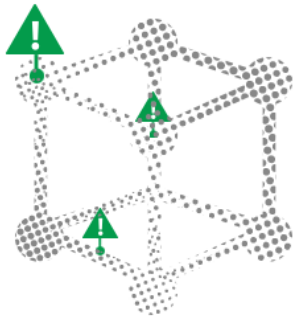
Traditional Adversaries

Nation State

- Intelligence
- Intellectual Property Theft
- Espionage

Organized Crime

- Financial Gain
- Identity Theft



CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

What is the Problem?

Adversaries

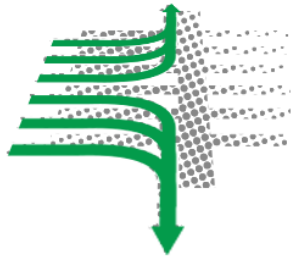
Next Generation Adversaries

Rogue Nation States

- Iran
- North Korea
- Syria

Individual and Terrorist Actors

- ISIS
- Anonymous
- Etc...



CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Operation Cleaver

Prevention is Everything

18-24 Month Long Iranian Offensive

- Solely Targeted at Global Critical Infrastructure companies
- Zh0up!n Exploit Team
- Phish based malware delivery, or MS08-067 external breach
- Public tools (psexec, mimikatz, cain + abel, etc)
- SQL injection, ASP Backdoors, cred harvesting
- Evolved into using their own Zeus variant (tiny_zbot)

CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Operation Cleaver

16 Countries Targeted

Canada
- Energy & Utilities
- Oil & Gas
- Hospitals

China
- Aerospace

England
- Education

France
- Oil & Gas

Germany
- Telecommunications

India
- Education

Israel
- Aerospace
- Education

Kuwait
- Oil & Gas
- Telecommunications

Mexico
- Oil & Gas

Pakistan
- Airports
- Hospitals
- Technology
- Airlines

Qatar
- Oil & Gas
- Government
- Airlines

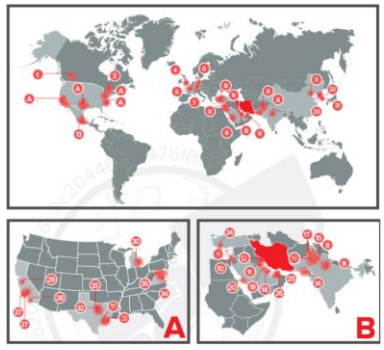
Saudi Arabia
- Oil & Gas
- Airports

South Korea
- Airports
- Airlines
- Education
- Technology
- Heavy Manufacturing

Turkey
- Oil & Gas

United Arab Emirates
- Government
- Airlines

United States
- Airlines
- Education
- Chemicals
- Transportation
- Energy & Utilities
- Military/Government
- Defense Industrial Base



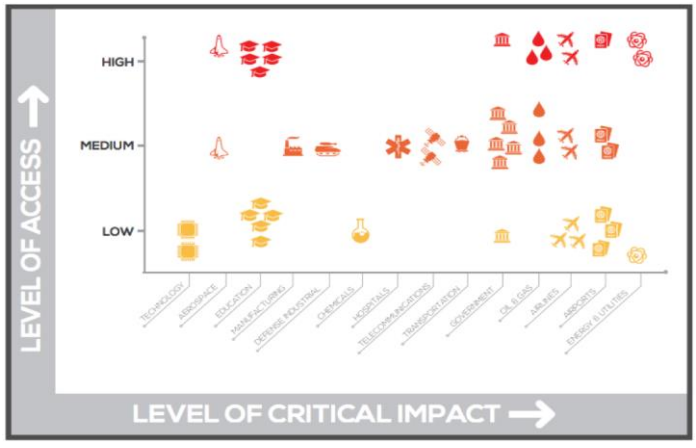
CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Operation Cleaver

Critical Industries Targeted



CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Operation Cleaver

Advanced Persistent Threat Campaign

Iranian Protection Takeaways

- No evidence of incursion into control systems
- Primarily Windows based vulnerabilities
- MS08-067 (2008 vuln, exploited up to 2014)
- SQL Injection
- Phishing (email and custom applications)
- Weak endpoint controls (av bypassed)
- Out of 53 companies disclosed, only ONE was aware of the breach and had remediated it.
- Skills advancing RAPIDLY

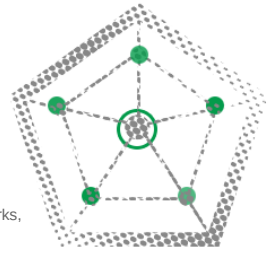
CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Energy Industry Vulnerabilities

- Outdated Systems, Protocols, and monitoring
- Security thru obscurity doesn't last forever
- The mixture of non-consumer based tech and consumer tech opens up vulnerabilities on networks discoverable by anyone with an internet connection, and IDA Pro.
- Frequent exceptions snowball over years to create large gaps in network based controls (PTP home connections into ICS networks, one-off access control exceptions)



CYLANCE

Introduction
What is Cylance
What is the Problem
Operation Cleaver
Vulnerabilities
Augmenting

www.cylance.com

Augmenting Existing Defenses

Close the gap between the capabilities of your attackers and your infosec risk.

Then get in front of it...

- New Technologies
- New Architectures
- Larger Investments
- 3rd Party Assessments
- Intelligence Sharing

CYLANCE

Questions


2015
AEGIS Policyholders' Conference
AEGIS