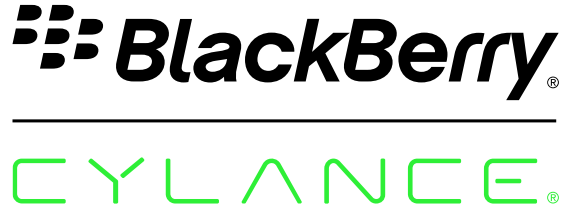


Protect Your Organization Against Retail Fraud and Data Theft

Sig Murphy
Senior Director
Professional Services
BlackBerry Cylance

Dave White
Principal Consultant
Incident Response and Forensics
BlackBerry Cylance

Ingrid Beierly
Senior Advisor
Cyber and Global Payment Security
Manatt, Phelps & Phillips, LLP

Sig Murphy

Senior Director

Professional Services

BlackBerry Cylance

- Formerly at Fidelis and the DoD Cybercrime Center (DC3; IA and CI)
- Husband, Father, Maker and Gamer (time allowing)

Dave White

Principal Consultant

Incident Response and Forensics

BlackBerry Cylance

- 17+ years conducting multifaceted computer and smartphone forensic investigations
- Previously worked with the FBI, DHS, and DOJ

Ingrid Beierly

Senior Advisor

Cyber and Global Payment Security

Manatt, Phelps & Phillips, LLP

- Focuses on payment data security, incident response and credit/debit/prepaid card fraud mitigation strategies
- Recognized, U.S. Secret Office and FBI, partnership to mitigate payment card fraud

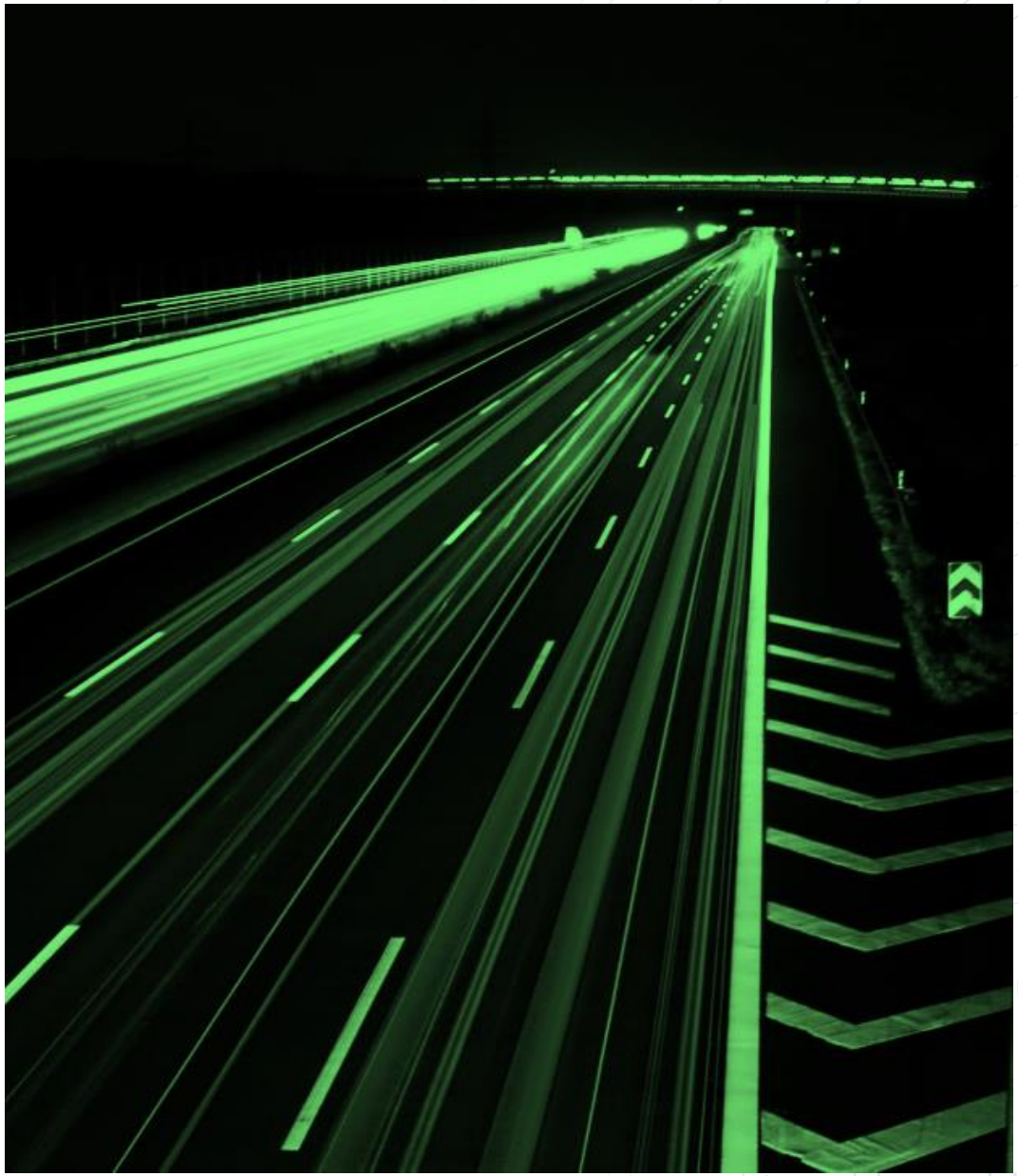
AGENDA

Payment Card Industry Threat Landscape

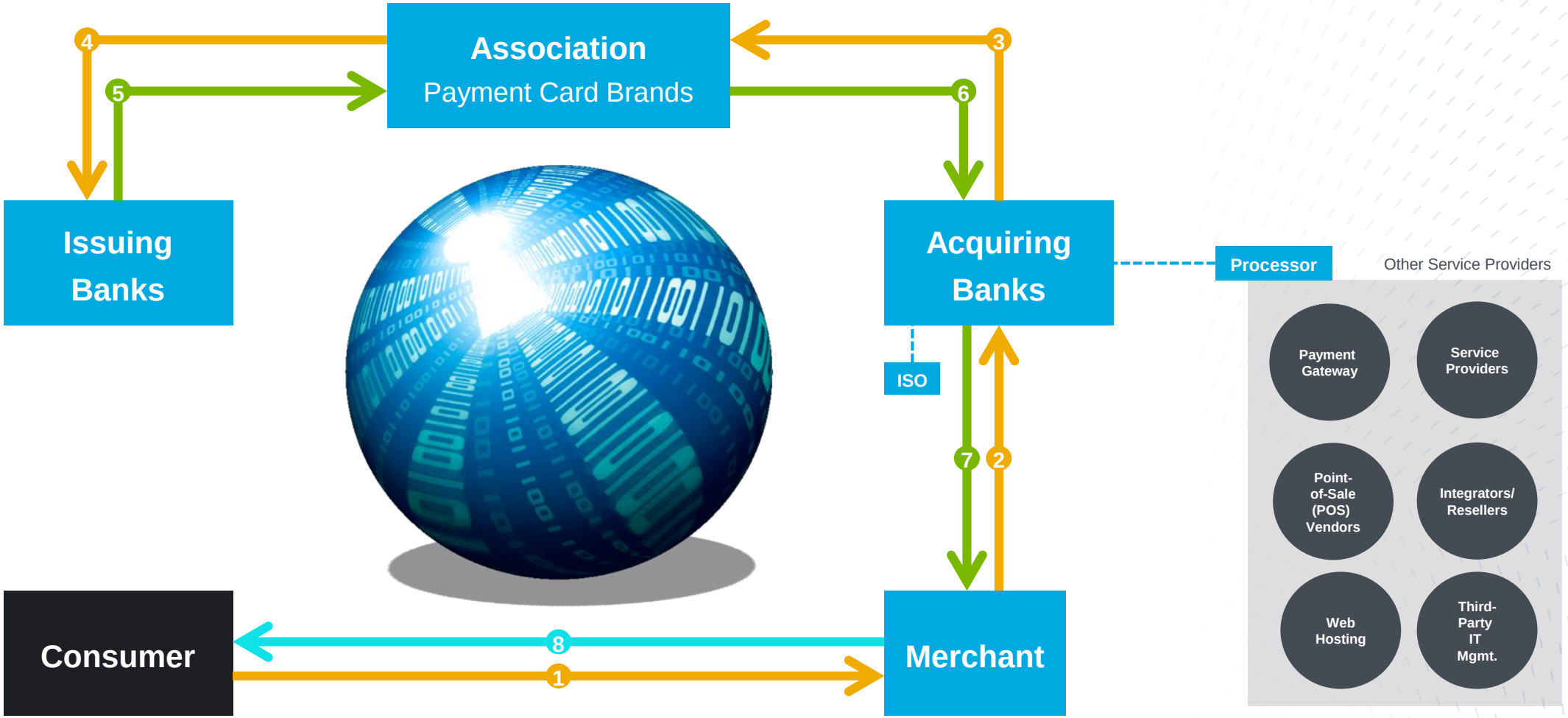
Common and Recent Types of Malware

How to Protect Your Customers and Your Organization

Q&A



Payment Processing Transaction Flow



BlackBerry | CYLANCE manatt

Payment Card Industry Threat Landscape

Card-Not-Present fraud involving insecure web applications

ATM targeted attacks

Account Takeover

Insecure 3rd party vendor remote access

RAM scrapper malware

BlackBerry | CYLANCE manatt

Common Point of Purchase

How do payment card brands get informed of a potential data breach?

Common Point of Purchase (CPP) reported by issuers or payment card brand internal analysis

- CPPs occur when multiple fraudulent transactions are identified by issuers or card brands and they have determined through their analysis that the transactions originated from a common location (i.e., merchant)
- An investigation is initiated to determine data elements at risk and exposure/window of intrusion
- Payment card brands will send out at-risk account numbers to the issuers for fraud monitoring and/or reissuance of credit/debit cards

PCI DSS fines:
Depending on the size of the data breach, the payment card brands can levy a fine on the acquirer from $5,000 to $500,000 per month until the entity is fully compliant.

In addition to PCI DSS fines, there is a liability assessment on data breaches involving counterfeit fraud.

Law enforcement investigation

Self-identification by merchant/service provider

BlackBerry | CYLANCE manatt

Current Challenges in Retail

1. Data is often stored in several disparate locations depending on its utility to the retailer.

2. Payment card handling standards and regulations currently ONLY require the data to be encrypted in transit – not where it is stored.

3. The data stores (customer information or intellectual property) are irresistible targets for cyber attacks who use these for financial motives.

TARGET

- **Cause**: Credentials stolen from a third-party vendor
- **Data store affected:** Up to 70M records
- **Cost:** $202 million

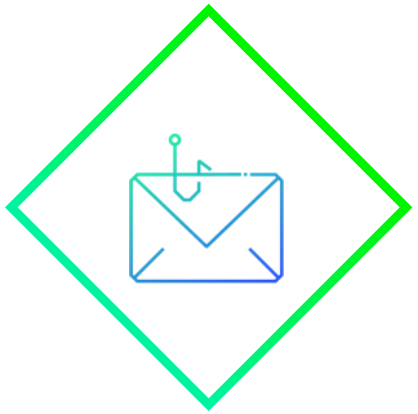
HOME DEPOT®

- **Cause**: Credentials stolen from a third-party vendor, RAM scraping malware
- **Data store affected:** More than 100M records
- **Cost:** $179 million

BlackBerry | CYLANCE manatt

Common Types of Malware

Usually Involved in Retail Data Breaches

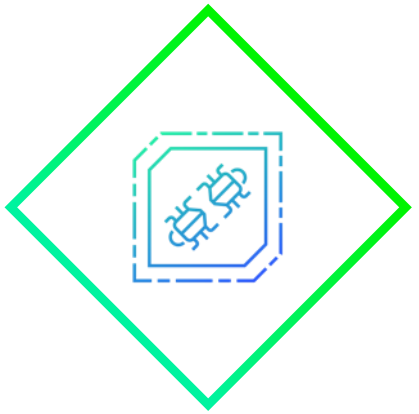


PHISHING EMAILS

- Contains malicious droppers or downloaders to infect systems with backdoor trojans
- Enables remote access and exploitation of networked corporate systems

PUPs

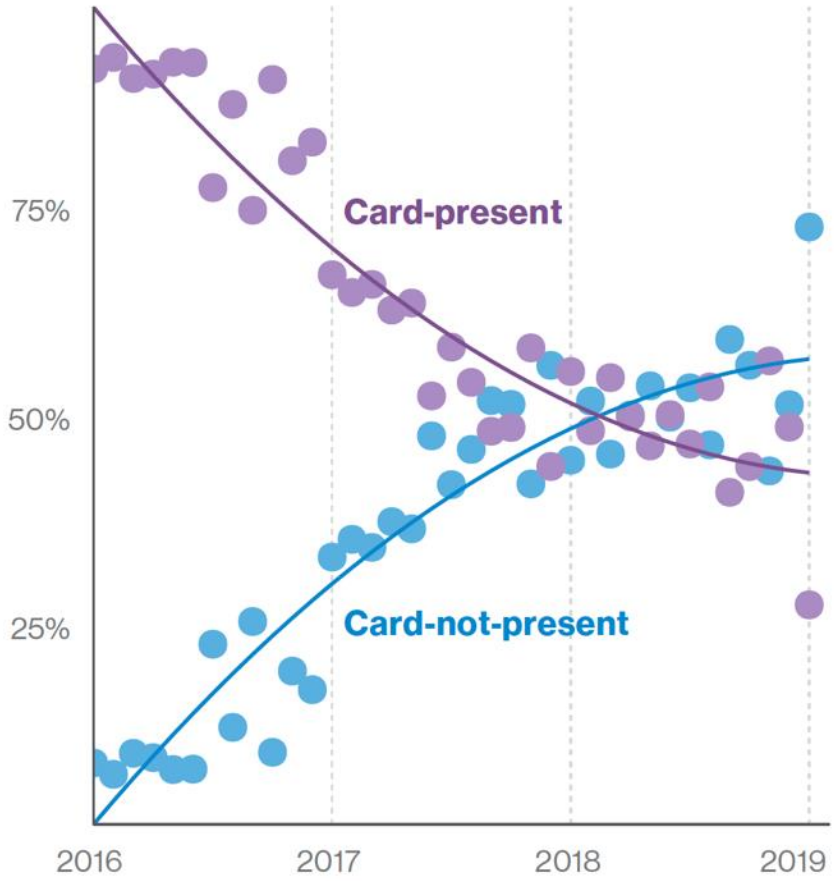
- Allow password hash collection or cracking, Active Directory or LDAP browsing, SQL server interaction, RAR/ZIP packaging, reconnaissance tools, etc.
- Establishes data harvesting and exfiltration methods



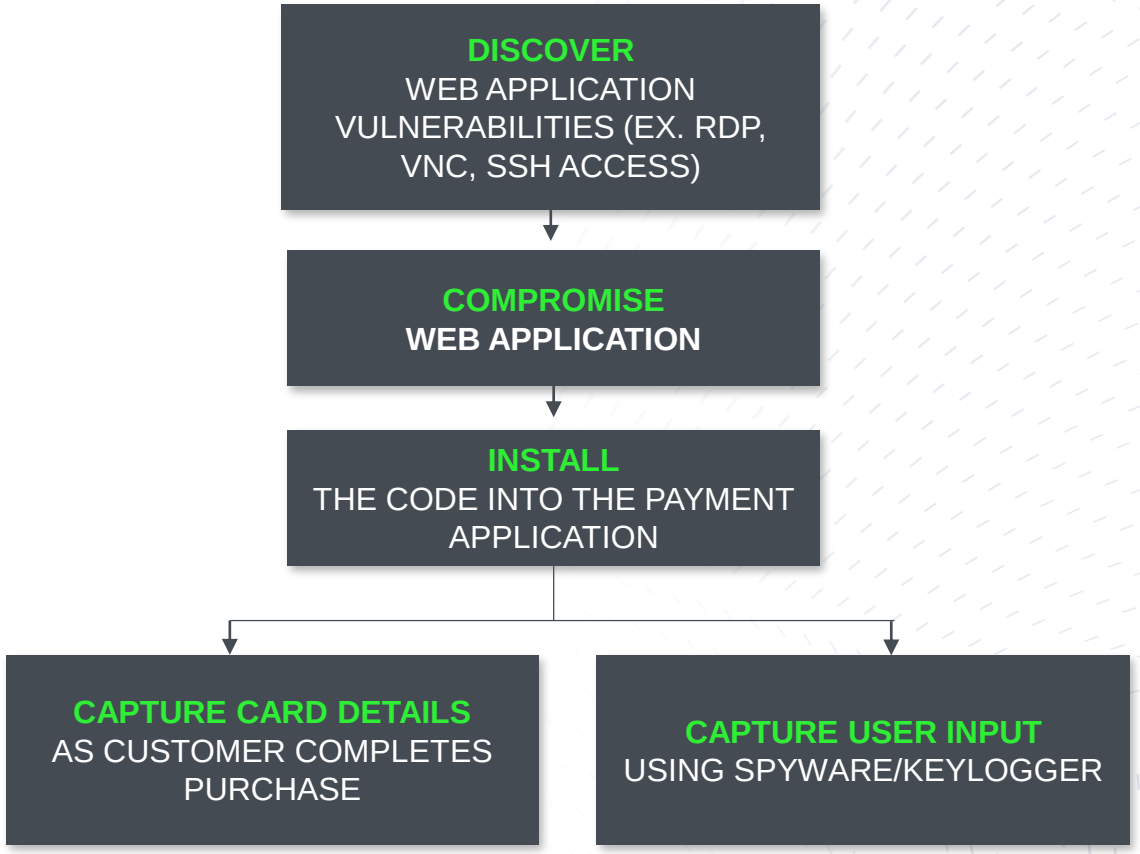
HARVESTORs

- Automated spread
- Often Polymorphic
- Packages up and exfils targeted data to the attackers
  - POS data
  - Banking info for Org
  - Personal banking info

Recent Types of Attacks in Retail



Source: Verizon 2019 Data Breach Investigations Report



BlackBerry | CYLANCE manatt

Recent Types of Attacks in Retail

"Magento confirmed…that its e-commerce platform suffered a malware attack that impacted around 5,000 of its Magento Open Source users.

A spokeswoman for Magento said the sites were infected with MagentoCore skimming malware that is designed to uncover simple passwords. MagentoCore is a malicious payment card data-stealing script that was designed to compromise websites that run on the Magento e-commerce platform."[1]

[1] https://www.digitalcommerce360.com/2018/09/05/magento-is-the-target-of-malware-attack/

BlackBerry | CYLANCE manatt

Protecting Your Organization

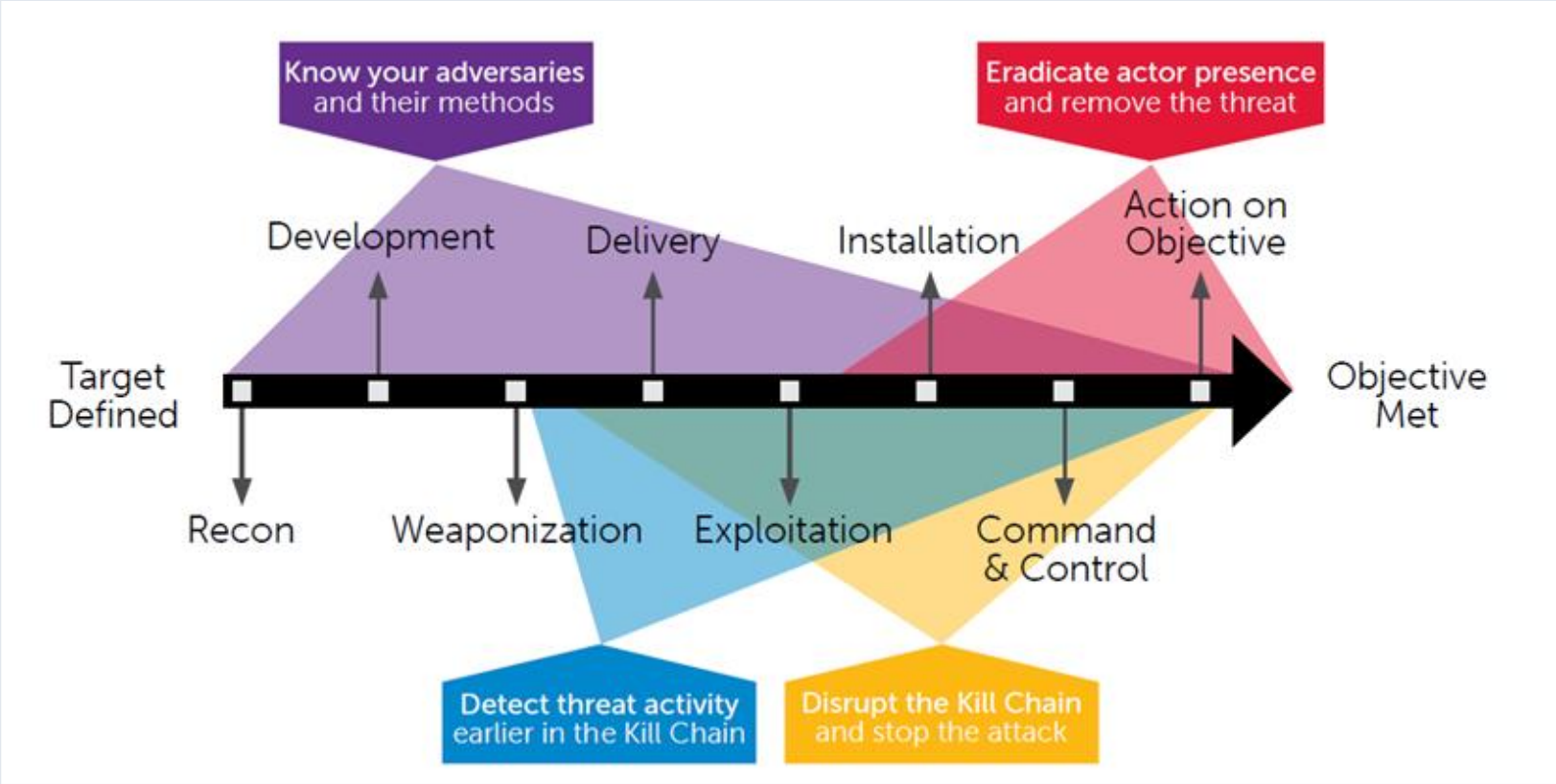
Preventing Retail Fraud and Data Theft

WHAT YOU CAN DO

The (Traditional) Cyber Kill Chain

Phases

1. Reconnaissance
2. Development
3. Weaponization
4. Delivery
5. Exploitation
6. Installation
7. Command and Control
8. Action on Objective



What To Do If You Are a Victim

- **Engage counsel <u>immediately</u>**
  - PCI Requirements
    - Number of systems
    - Compromised accounts
    - Etc.
  - Prepping for card brand discussions
  - IR plan (counsel -> IR Plan)

BlackBerry | CYLANCE manatt

Thank You!

Ingrid Beierly
Senior Advisor
Cyber and Global Payment Security
Manatt, Phelps & Phillips, LLP
ibeierly@manatt.com

Dave White
Principal Consultant
Incident Response and Forensics
BlackBerry Cylance
dwhite@cylance.com

Sig Murphy
Senior Director
Professional Services
BlackBerry Cylance
smurphy@cylance.com