RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO3-T10

Intelligence-Led Security: Confronting the Ever-Evolving Threat Landscape

Laura Galante
Director, Threat Intelligence

FireEye
@LauraLGalante

Glen Jones
Head of Payment System Cyber Intelligence

Visa

Intelligence Emerges in Info Sec

- A government function goes private
- Newest domain, minimal barrier to entry
- Private sector needs the same information advantage as governments

The Challenge: Build the capability and pioneer delivery

Dimensions of the Threat

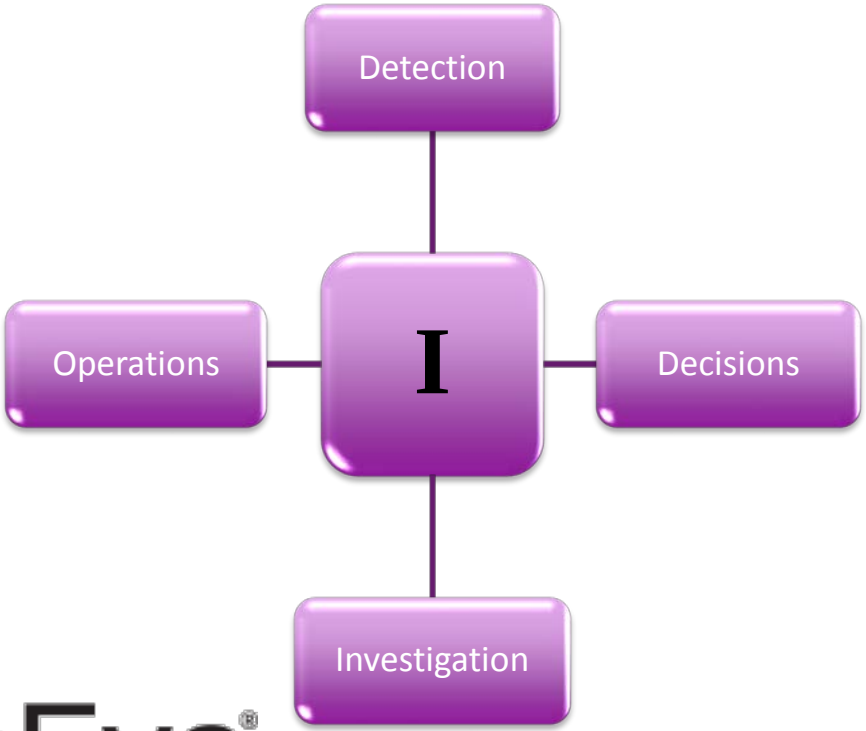
- IP Theft
- State Espionage
- Military Intelligence
- Network Destruction
- Insider Trading
- Regional Actors
- Advanced Recon
- Enterprise Criminals

FireEye®

Defining Intelligence

The evaluation and analysis of data: assessment based on observation and judgment

Intelligence-Led Security Operations



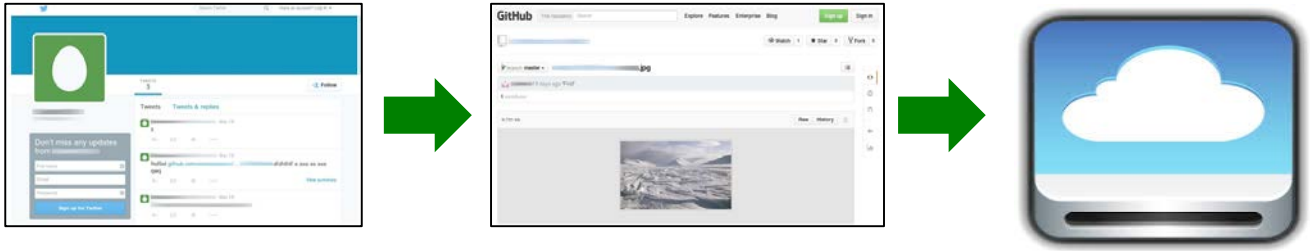
FireEye®

APT29: The Paradigm of an Advanced Actor

- Typical Targets: U.S. and European governments, policymakers
- Highly sophisticated, specialized malware
- Well resourced – extensive C2 infrastructure
- Conducts intrusions with extreme stealth
- Brazen and aggressive when discovered

FireEye®

End-to-End Traffic in Legitimate Services



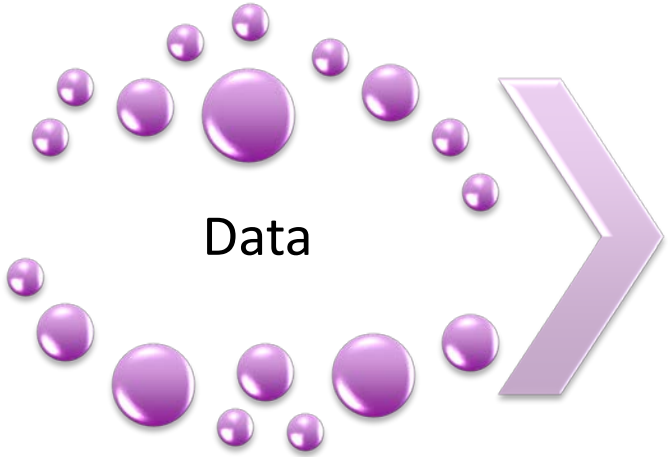
Twitter to GitHub to Cloud Drive

FireEye®

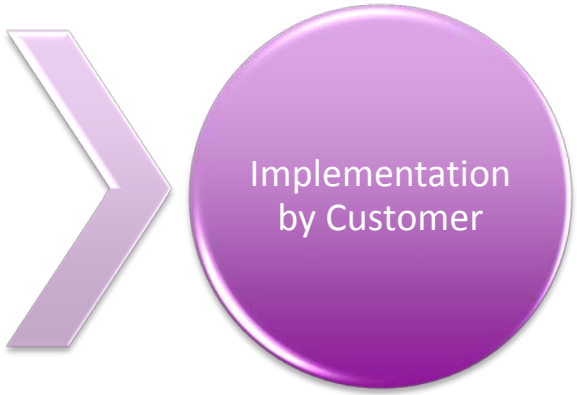
Late 2015…Targeting Morphs

FireEye®

From Collection to Action



Analysis



FireEye®

Visa's Approach to Threat Intelligence

Glen Jones
Head of Payment System Cyber Intelligence
Visa

Visa Security Pillars

Remove sensitive data

Devalue Data

Render data useless for criminals, reducing incentive for payment breaches

- Tokenization
- EMV

Protect Data

Safeguard payment data

- Encryption
- PCI

Prevent fraud

Harness Data

Identify fraud before it occurs and increase confidence in approving good transactions

- Risk-Based Authentication
- One-time Passcode
- Dynamic CVV2
- Breach Response

Empower Consumers

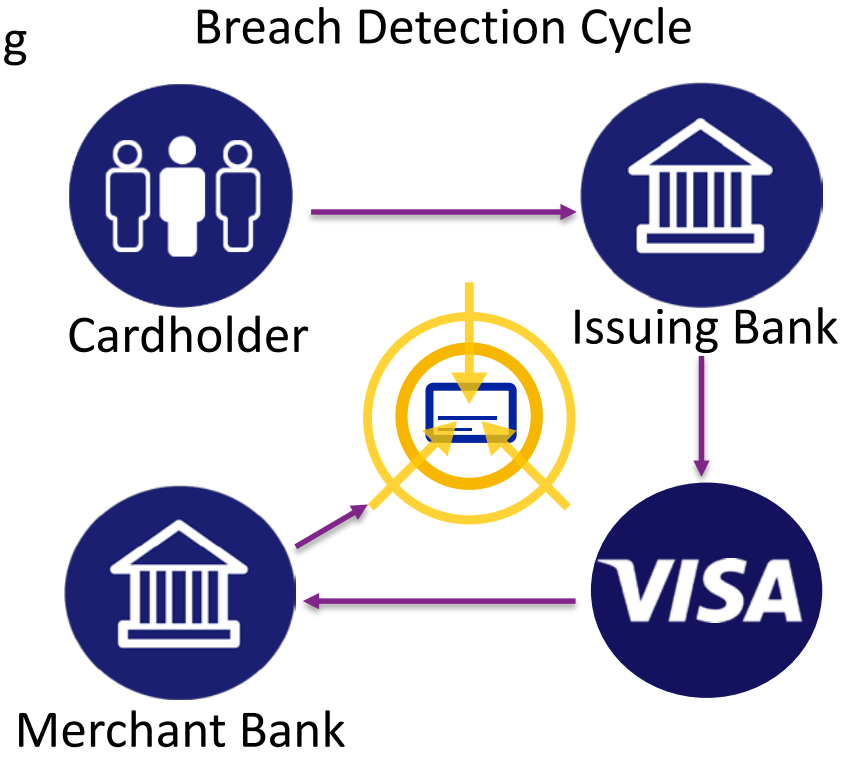
Engage cardholders as an underutilized resource in fighting fraud

- Transaction Alerts
- Spend Controls
- Geolocation

Transactional Threat Intelligence

- Intelligence comes from recognizing fraud patterns, predicting fraud activity
- Cardholders report fraud to their bank
- Banks report fraud to Visa (CPP)
- Visa reports fraud to other banks
- Breach found, stopped

One major limitation: **What if there's no fraud?**



An Improved Approach to Threat Intel

- Combine cyber threat with transaction-based intelligence
- Goal is to identify the **breach** before the **fraud** ever begins
- We believe in actionable intelligence, but "actionable" is a buzzword
- Makes all the difference when we make the call (literally) on a suspected breach

"You're breached...now go find the needle in the haystack"

vs.

"You're breached…and here's exactly what to look for…"

VISA

Case Study: Breached Retailer

- Payment data breach at a large nationwide retail merchant
- Cards go up for sale on a dark market site
- A number of counterfeit transactions occur
- You didn't know there was fraud until your bill arrived
- Your bank didn't know until you told them

Impact: breach went undetected for months

VISA

Case Study: Breached Restaurant

- Point of Sale (POS) malware recovered from a retailer breach in early 2014, analyzed and indicators were extracted, including a hard-coded IP address
- Mandiant's malware analysis was distributed by Visa to a wide set of targeted merchants
- One of those merchants plugged IOCs into their Intrusion Detection System and immediately discovered a matching IP address
- Encrypted traffic to that IP for the last 12 weeks
- Traced it back to a credit switch in the merchant's processing environment

Impact: Breach was detected, although no payment card data was ever sold, no fraud had occurred, none of the normal warning signs were present.

VISA

Evolving Payment System Crime

- We expect attack techniques to evolve along with security
  - Intruders will use your own accounts and tools against you
  - Highly customized, difficult to detect malware
  - Stolen data combined in ways that perpetuate fraud
- Fraudsters will get even more savvy with payment data monetization
  - Payment data will be sold in ways designed to thwart bank fraud detection (by ZIP code, for example)
  - Mixing in old data to “water down” fraud detection
  - They'll hold on to data for months or longer before selling on dark markets

VISA

Key Takeaways

- Predictability of threat actors has changed, requiring the approach to change
- Prepare to be attacked
- Don’t rely on one type of intelligence
- “Actionable” intel should trigger some sort of action
- Cybercriminals are cooperating, we need to do the same