Rising to the Challenge — Staying Ahead of the AML Curve

Welcome

Cybercrime…

…is any crime that involves a computer and a network.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

– National Research Council, "Computers at Risk", 1991.

Cybercrime…

… is much more efficient from a criminal perspective. More reward and (usually) lighter penalties.

"You know, you can do this just as easily online."

Cybercrime approaches are pervasive and driving bank fraud loss across almost all areas

Call Center

Online research → Defeat Knowledge Based Authentication

Credit / Debit Card

Malware compromise of payment systems → Full track data

Check

View check images → Counterfeit checks

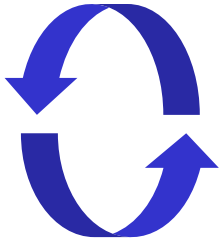
Online Account Takeover

Automated credential harvesting and utilization

Account takeover fraud occurs when a fraudster obtains credentials and uses them to gain control of an account. Broadly 2 approaches:

Social Engineering

- Branch
  - **Impersonate customer**
- Call Center
  - **Brute force**



Cybercrime (Technical Approach)

- Online
  - **Phishing**
  - **Malware**
  - **Mass Compromises**
  - **Internet Research**

Fraud rings often employ both approaches iteratively.

Account takeover fraud is perpetrated in multiple ways but all approaches require defeating authentication and then removing money from the bank

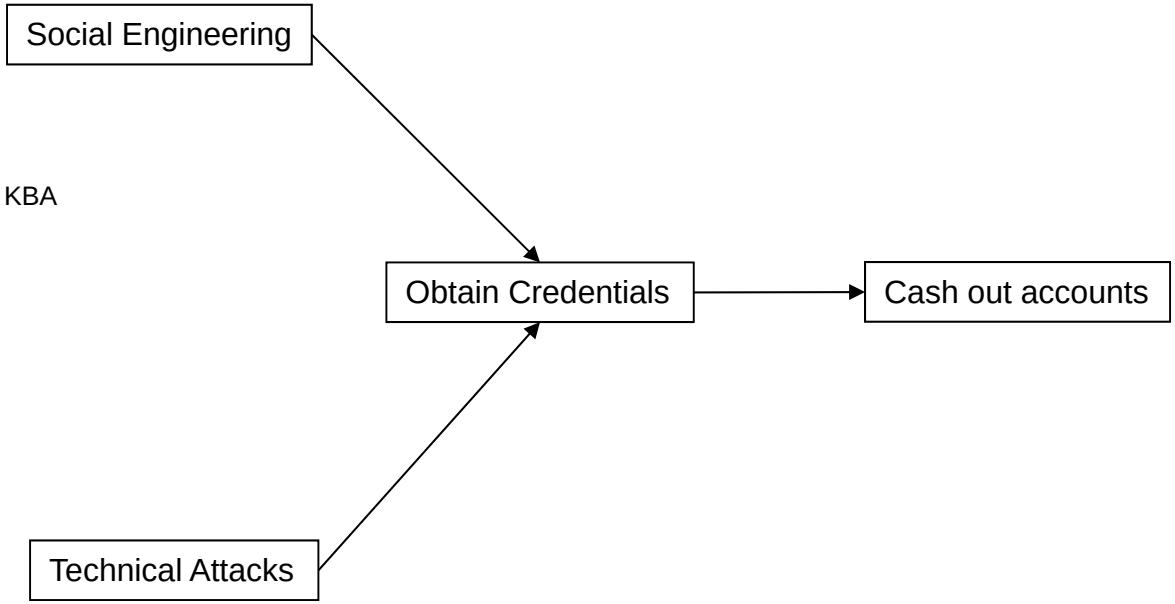
Auth controls

$Trans controls

Branch
- Impersonate customer
- Fake ID

Call Center
- Social engineering
- NPI / PR research to beat KBA
- Escalate → online access

Online
- Phishing
- Malware
- Mass Compromise
- Brute Force
- Credential Reset via phone



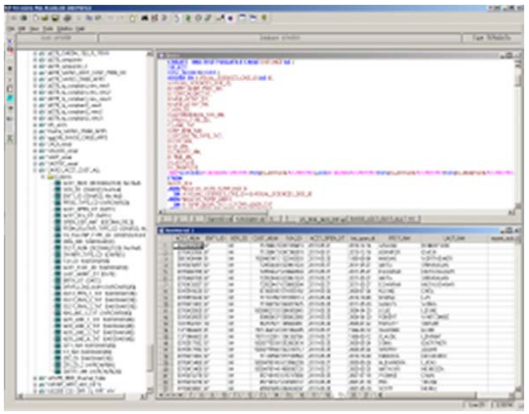
Method
- ACH
- Wire
- ATM / Debit
- Check
- BillPay
- Counter W/D

Defenses should be built that look holistically throughout the fraud attack cycle. Single focus "silo" defenses will struggle to mitigate risk.

Most account takeover fraud is perpetrated by organized criminal groups. It's important to look for these collusive networks.

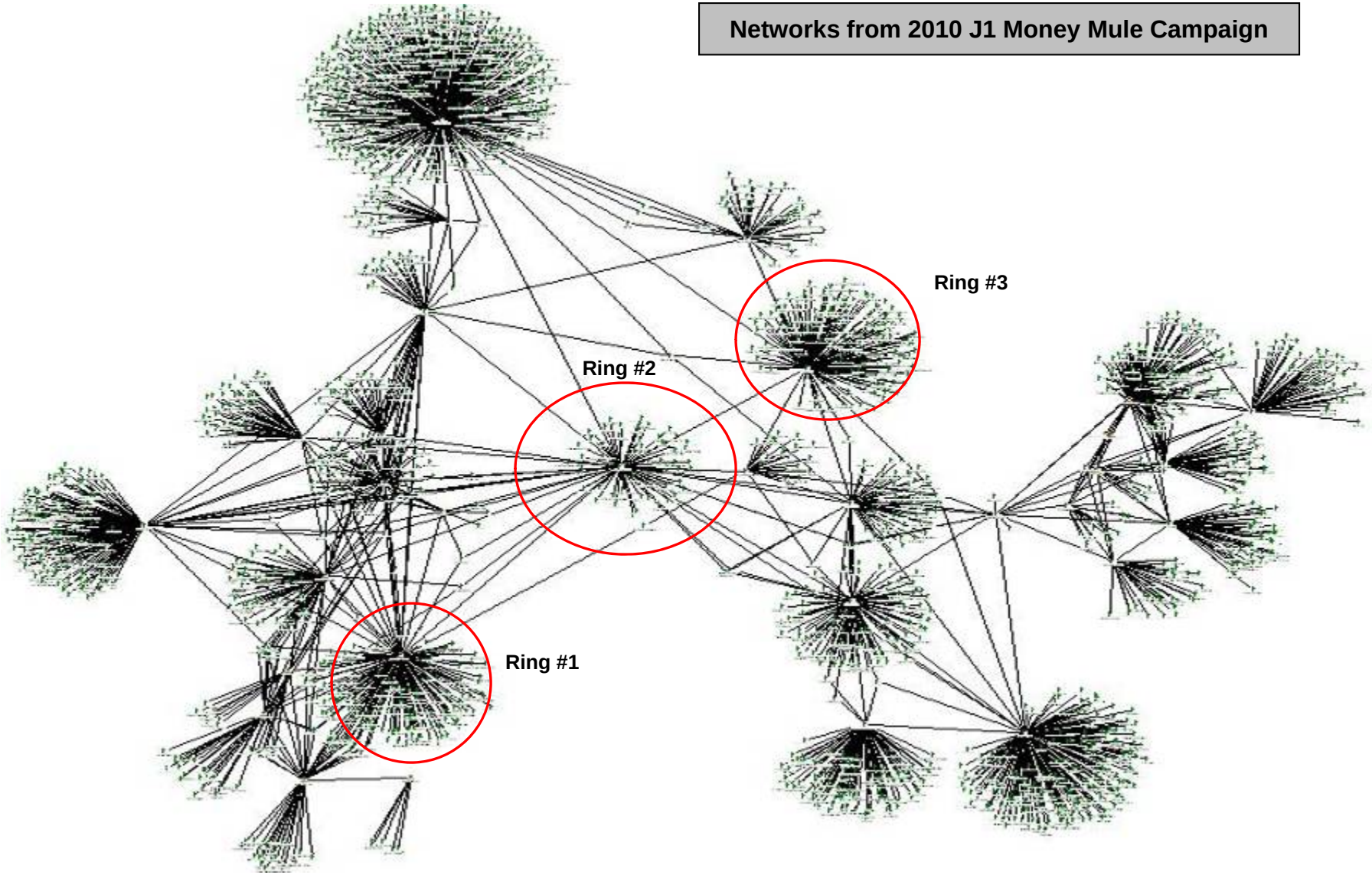
Identify fraud and leverage data sources to find related activity

Map fraud networks with manual and automated tools



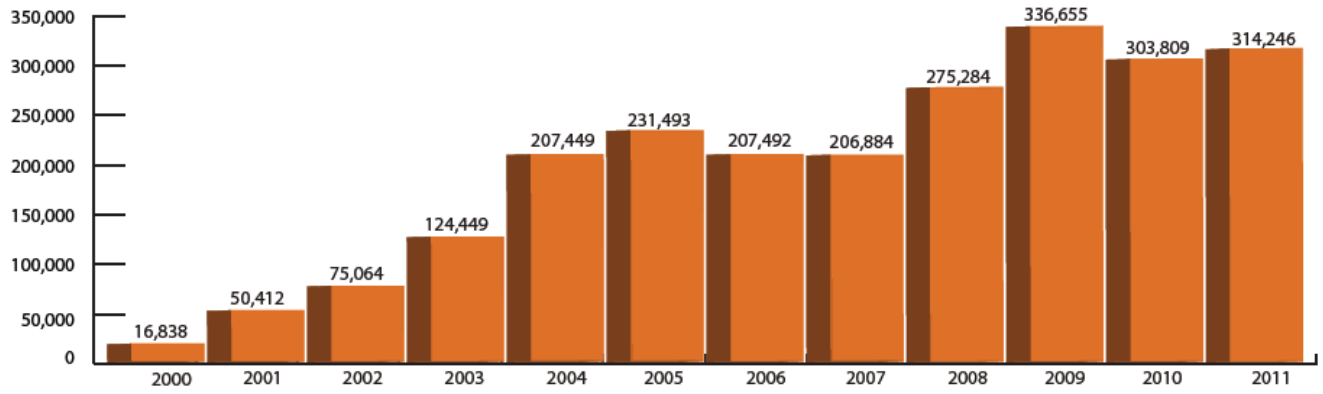
Design fraud ring specific logic and run until activity ceases

Criminal networks can be extensive. Understanding connections makes defense easier and collaboration with law enforcement more productive.



The level of online threats remains high with no signs of decreasing

Yearly Comparison of Complaints[3]

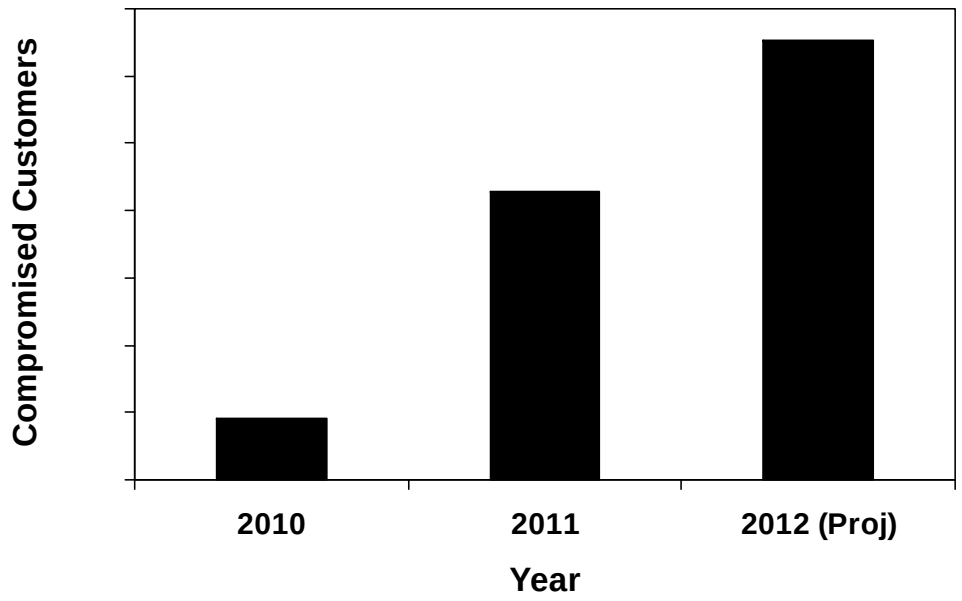


[1]Methodology of evaluating loss amounts: FBI IC3 Unit staff reviewed for validity all complaints that reported a loss of more than $100,000. Analysts also converted losses reported in foreign currencies to dollars. The final amounts of all reported losses above $100,000 for which the complaint information did not support the loss amount were excluded from the statistics.

[2]Complaint category statistics that are based on the perceptions of the complaints are not typically accurate for statistical purposes. The statistics pulled from the complaints themselves, however, are considerably more accurate as they are categorized and grouped through the IC3 automated system. IC3 does not verify complaint data.

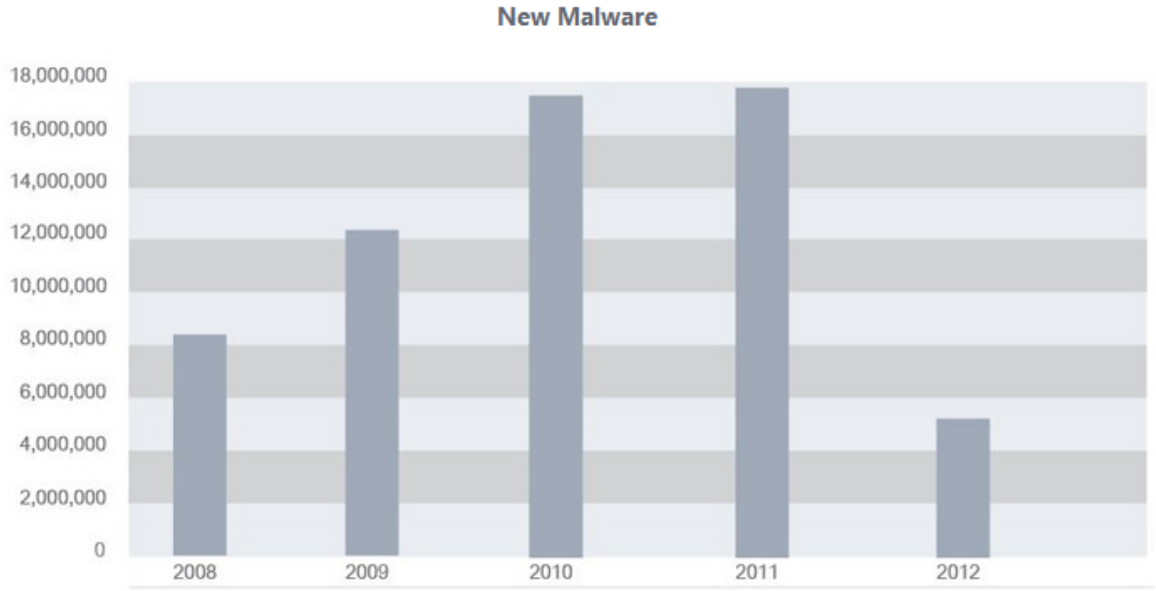
[3]IC3 started in May 2000.

Capital One has seen a ramp in attacks targeting the commercial platforms



Cybercriminals continue to create new malware and obfuscate existing code to make detection algorithms less effective

The Malware Challenge



Growth in malware presents serious challenges for the anti-malware industry. There are about a million new malware samples presented a month. This graph shows the number of new samples added to AV-Test.org's malware collection over the last 5 years.

Source: www.av-test.org, March 2012

Key takeaways…

- **Cybercrime is increasingly prevalent but often hidden by approach**

- **Most cybercrime is organized and sizable (“isolated” events rarely are)**

- **It’s most efficient to fight account takeover fraud holistically.**