Threat Modeling: Concepts and Actions

Dr. Michael Blair and Chris Curry

Intro: Why do we do this?

- Analyze our attack surface
- Analyze our adversaries
- Implement security controls
- Test security controls
- Feed our Intelligence Lifecycle

Different Types of Threat Actor

Actor	Target
State-Sponsored Actor	Any and every computer
Organized Cybercriminals	Enterprises
Hacktivists	Government entities, corporations, individuals
Lone Wolf	Financial Institutions and their networks

Dispelling Notions

- We have the answers to criticality in your enterprise
  - BCDRs which lead to BIAs are essential
- We are not unique
  - From the eyes of an adversary, attack vectors maintain across enterprises.
- We are asking the wrong questions
- This is a technical problem that has to be solved

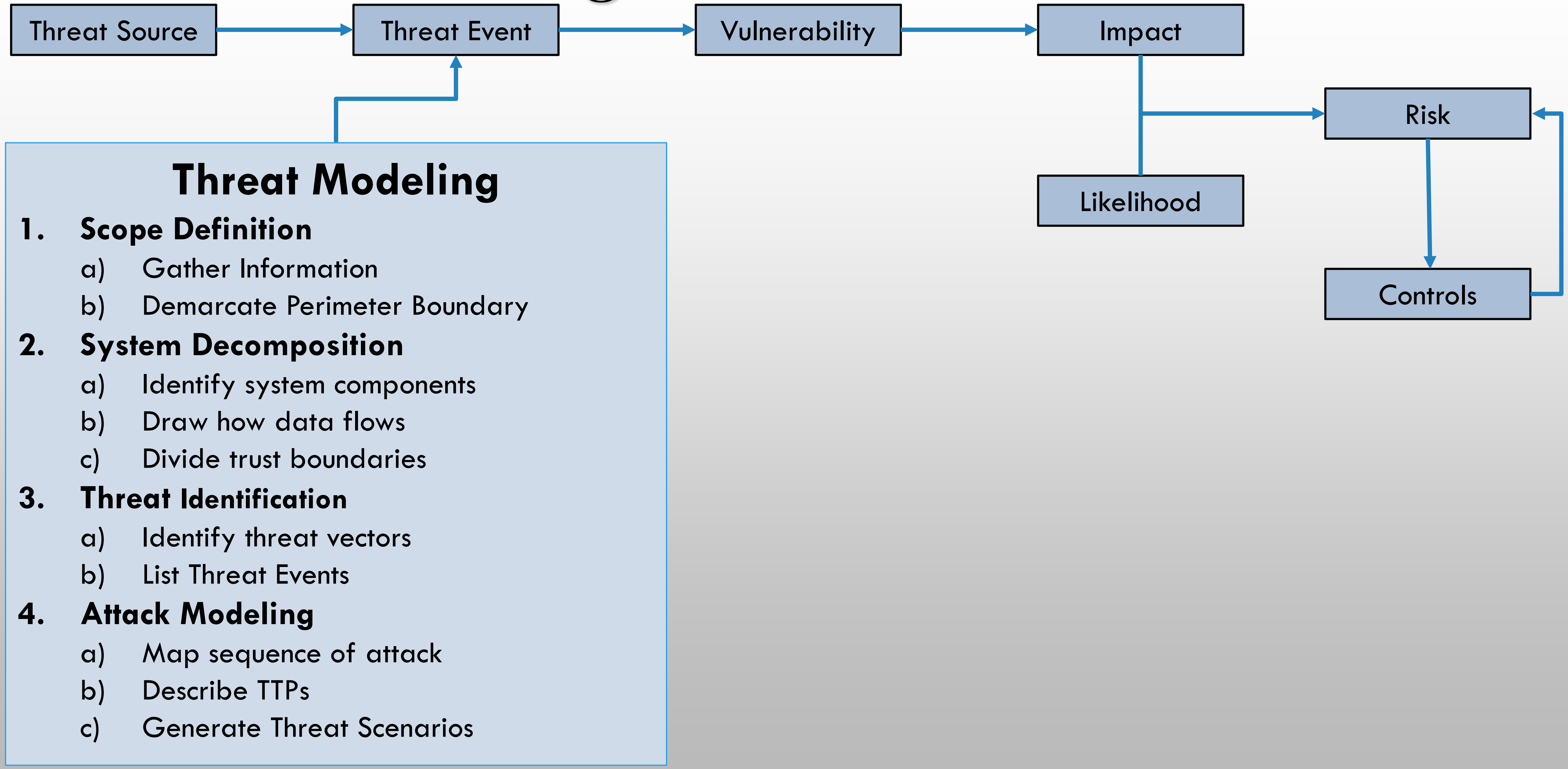
Priority Intelligence Requirements

- Must be specific; only answer one question
- Should focus on a single act or activity
- Should support a single decision

Generic Example: “What are the threats targeting financial institutions”

Specific Example: “What critical remote access technologies for financial institutions have been attacked in the past 4 months”

Building our Threat Model



Threat Source

Threat Event

Vulnerability

Impact

Likelihood

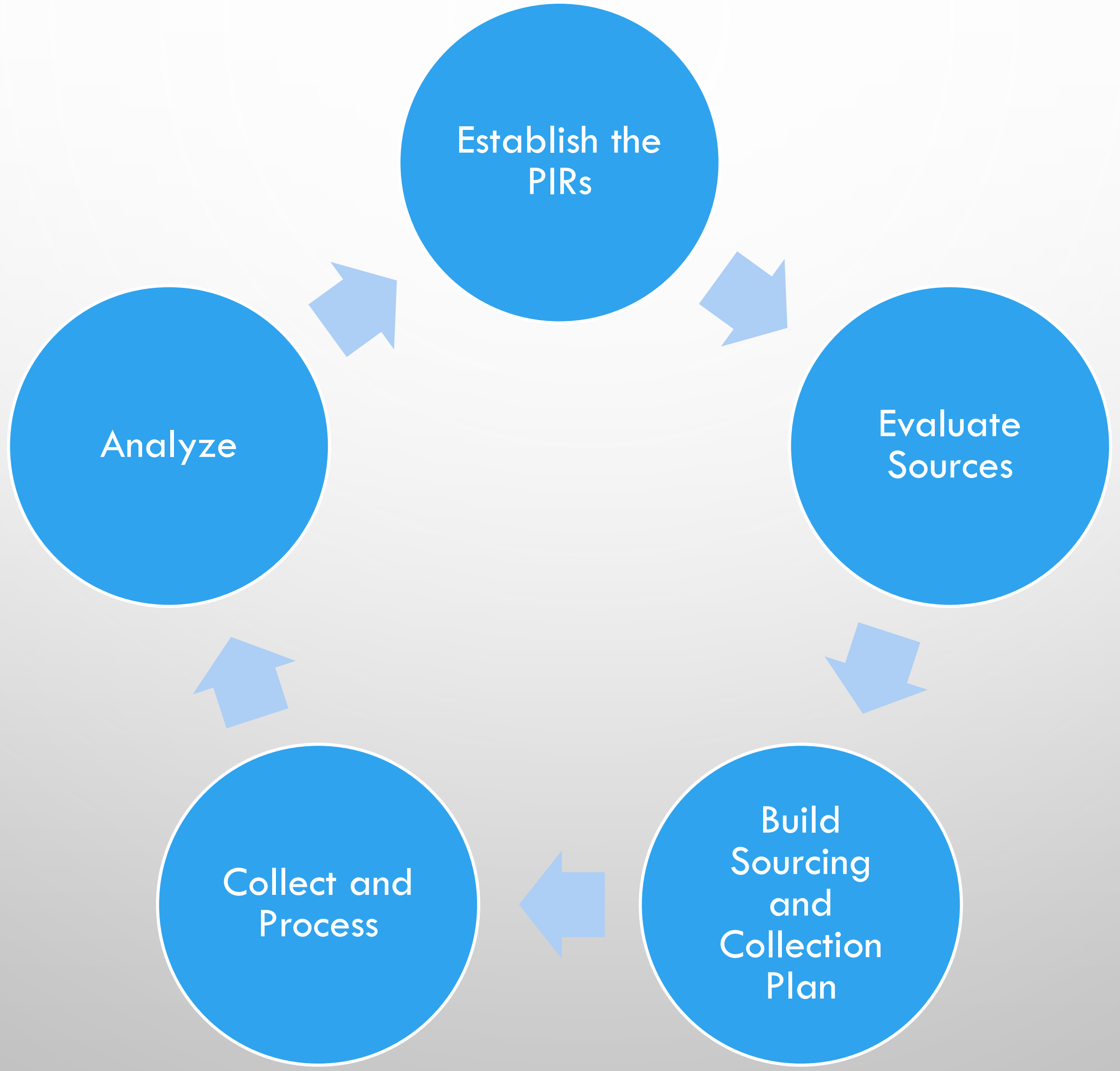
Risk

Controls

Threat Modeling

1. **Scope Definition**
   a) Gather Information
   b) Demarcate Perimeter Boundary
2. **System Decomposition**
   a) Identify system components
   b) Draw how data flows
   c) Divide trust boundaries
3. **Threat Identification**
   a) Identify threat vectors
   b) List Threat Events
4. **Attack Modeling**
   a) Map sequence of attack
   b) Describe TTPs
   c) Generate Threat Scenarios

The Modified Intelligence Lifecycle



Establish the PIRs

Evaluate Sources

Build Sourcing and Collection Plan

Collect and Process

Analyze

Enrichment with Threat Intelligence

- Creating a Collection Plan
  - Telemetry, Darknets/Honeypots, Tailored Feeds, Dumps, HUMINT, Paste Bins, News and Media platforms
- Utilize non-technical intelligence
  - Understanding geopolitical trends in areas where attacks may be launched
- Determine what networks require further hardening
  - i.e. DDOS attack prevention due to increased reporting
- Prioritize which vulnerabilities should be addressed in order of probability and severity of exploitation
- Dark Web Monitoring

Applying the Concepts

Threat Modeling for the:

EAST NORTHEAST WILMINGTON BANK

EST. 2022

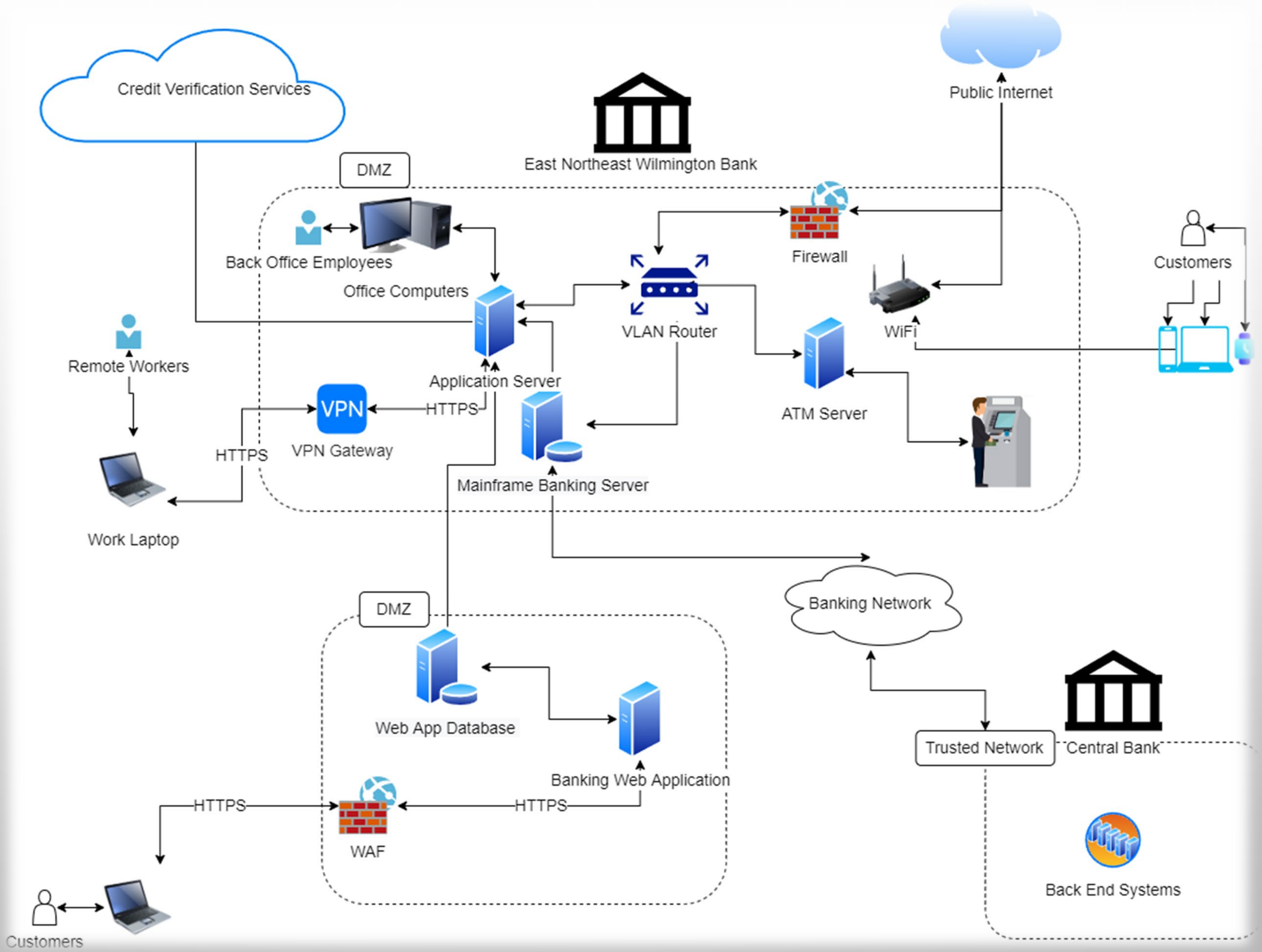
*This is a fictional bank

Business Impacts

1. Theft
2. Operational Costs
   a. Customer turnover
   b. Costs System downtown (Ransomware)
   c. Costs related to acquiring new business
1. Fines
2. Reputational Damage
3. Contractual

Attack Surface Analysis

1. Remote access gateways
2. Remote Employees
3. Web App
4. WiFi Access point
5. Back Office Employees
6. Web App Databases
7. Gateways to Third Party Networks

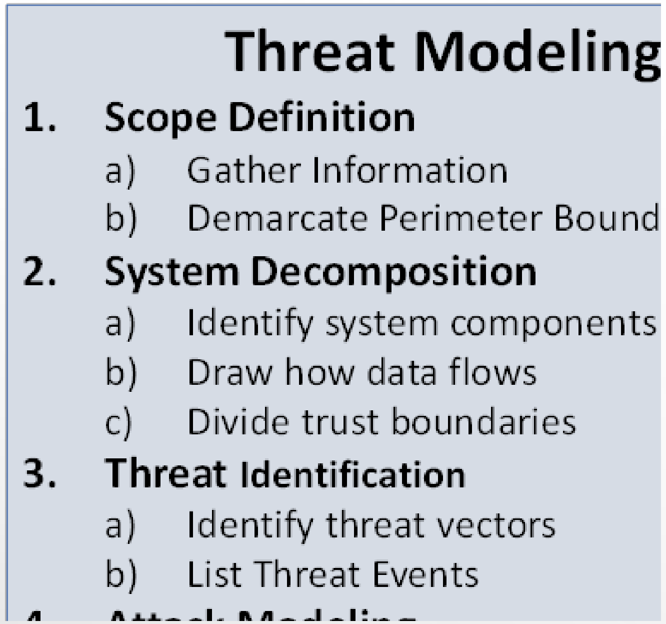


Framing the Impact

- Based on likelihood and severity

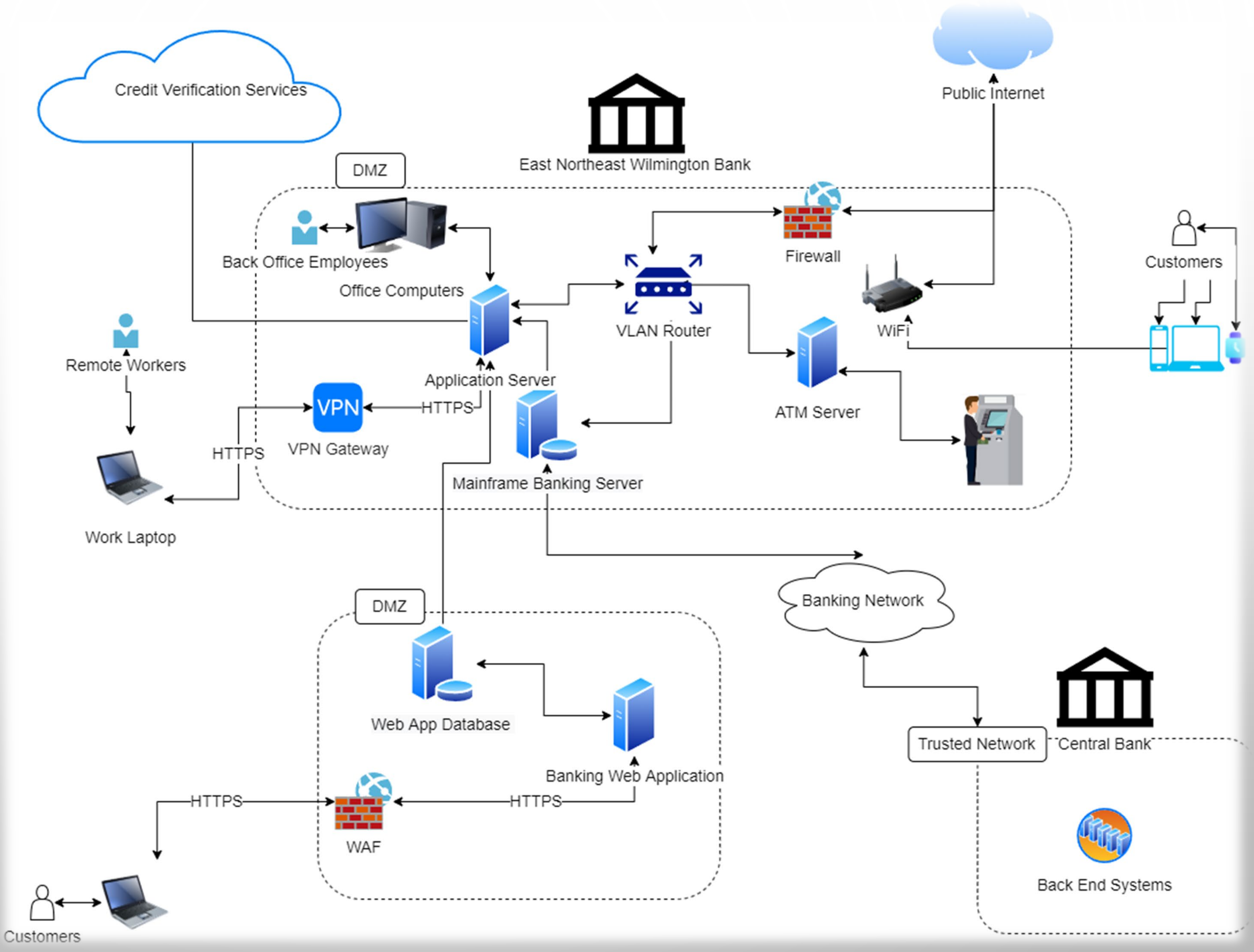
Impact	Likelihood	Severity
Corruption or destruciton of information systems	4	3
Data leakage/exfiltration	2	8
Interruption of technical operations	6	4
Fines and Penalties	4	3
Lost market share	4	8
Brand damage	3	9
Loss of trade licenses	2	9
Breach of Contract	1	5
Supply Chain Disruption		8

Building Our Threat Model



Threat Modeling

1. **Scope Definition**
   a) Gather Information
   b) Demarcate Perimeter Bound
2. **System Decomposition**
   a) Identify system components
   b) Draw how data flows
   c) Divide trust boundaries
3. **Threat Identification**
   a) Identify threat vectors
   b) List Threat Events
4. **Attack Modeling**

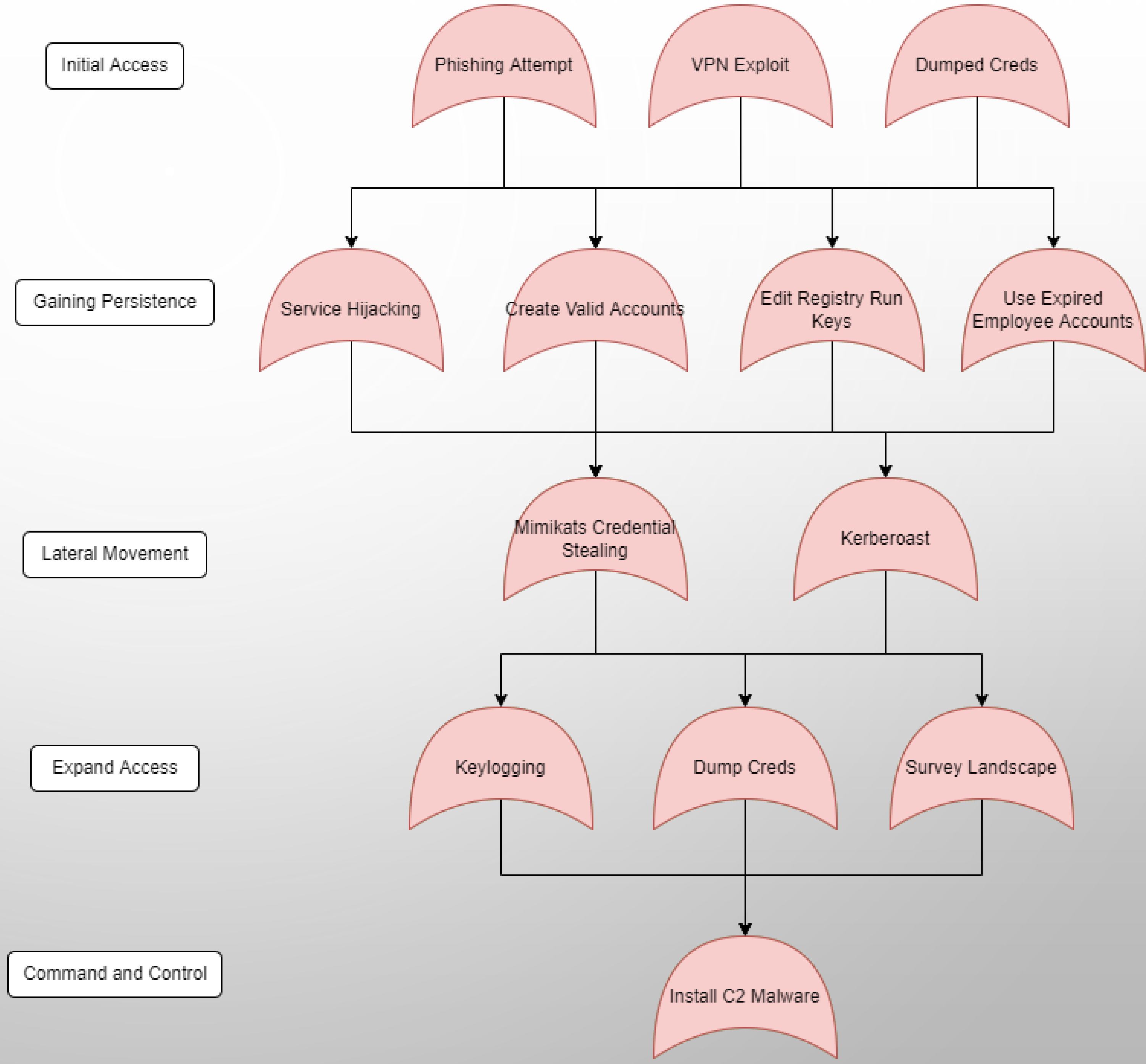


Adversarial Analysis

- Dark Web reporting indicated APT 25/Vixen Panda/Sushi Roll is actively targeting critical infrastructure in the Mid-Atlantic
  - In addition to being critical infrastructure, East Northeast Wilmington Bank conducts business with the Transportation System, Communications, and Critical Manufacturing Sectors
- Historical reporting indicates that APT25 exploits vulnerabilitie sin Pulse Secure VPN, which the East Northeast Wilmington Bank utilizes.

  https://www.fortiguard.com/threat-signal-report/4330/nickel-targeting-organizations-across-europe-north-america-and-south-america
- Additionally, they have used phishing attacks, and probe remote access endpoints as a way to gain initial access to the network.

Adversarial Analysis



Initial Access

Phishing Attempt

VPN Exploit

Dumped Creds

Gaining Persistence

Service Hijacking

Create Valid Accounts

Edit Registry Run Keys

Use Expired Employee Accounts

Lateral Movement

Mimikats Credential Stealing

Kerberoast

Expand Access

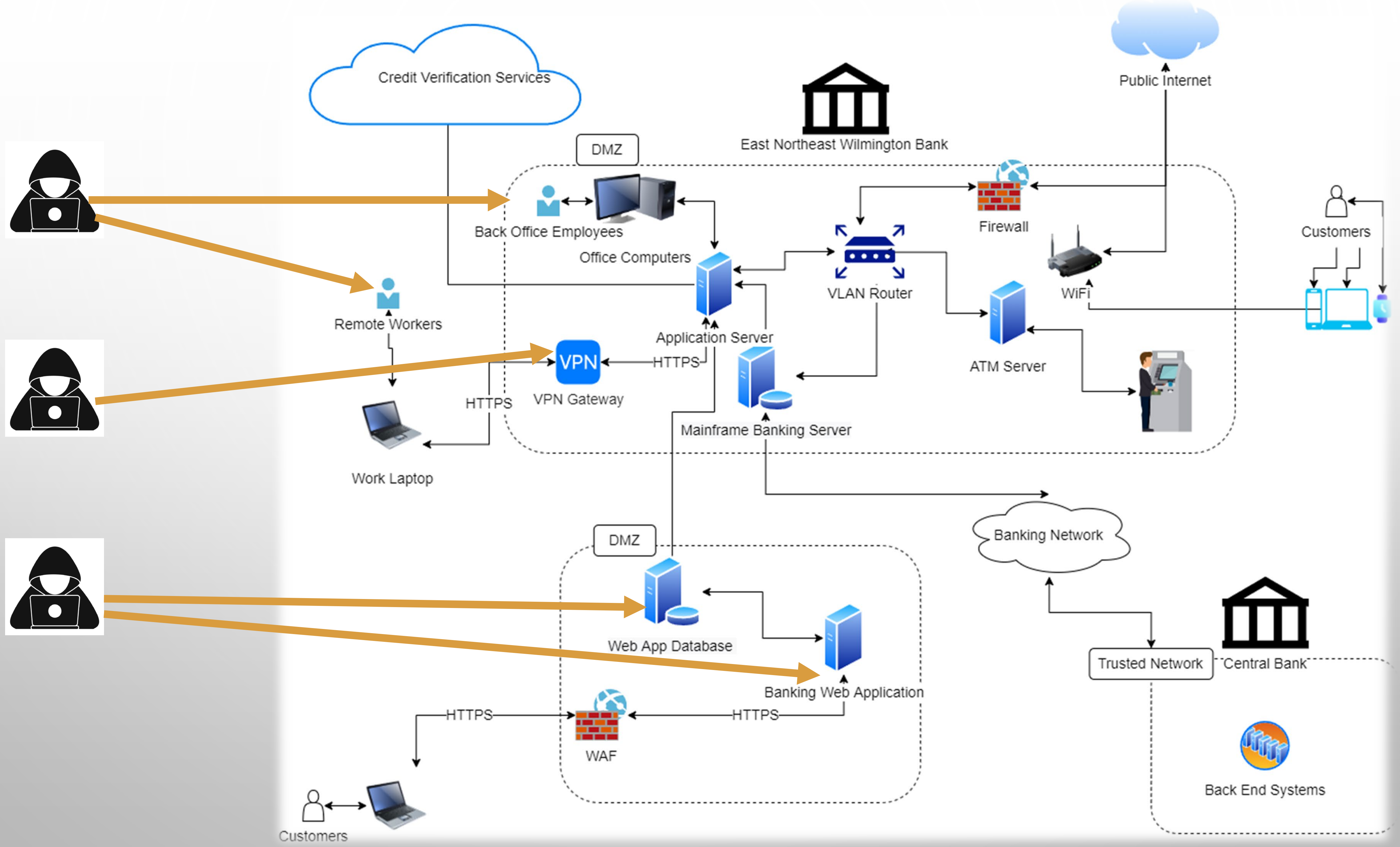
Keylogging

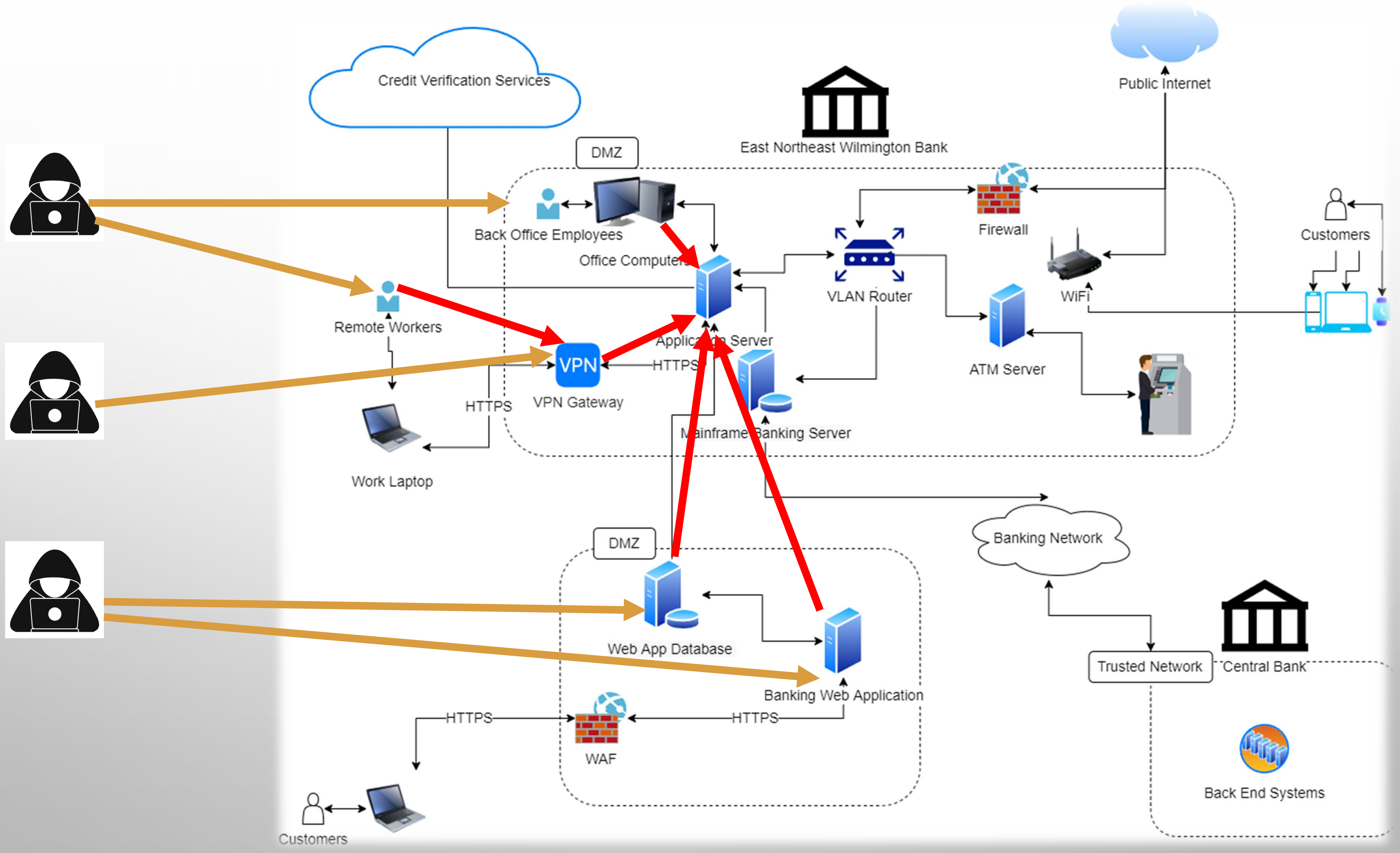
Dump Creds

Survey Landscape

Command and Control

Install C2 Malware

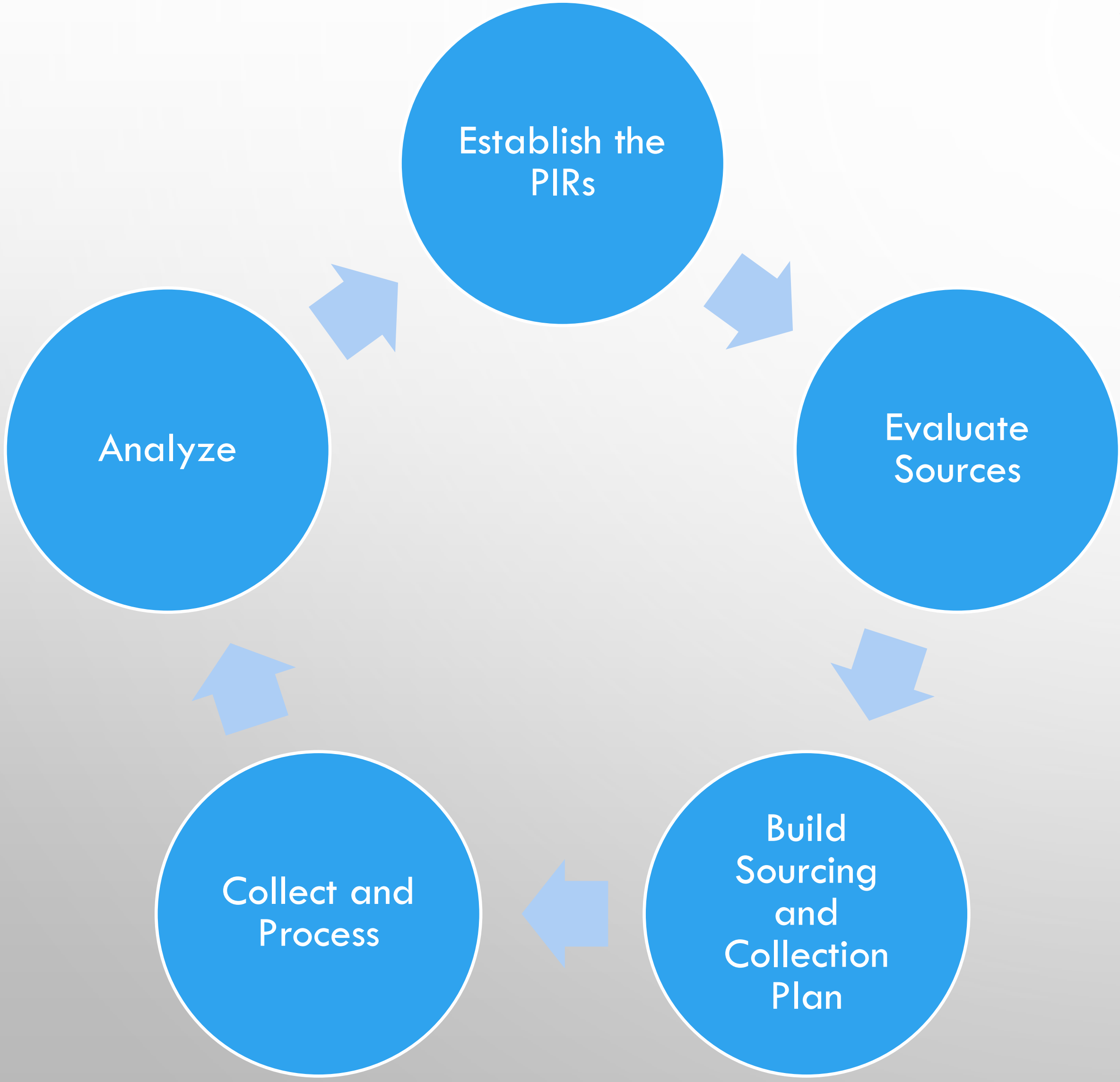

Credit Verification Services
Public Internet
East Northeast Wilmington Bank
DMZ
Back Office Employees
Office Computers
Firewall
Customers
VLAN Router
WiFi
Remote Workers
Application Server
HTTPS
VPN
VPN Gateway
ATM Server
HTTPS
Mainframe Banking Server
Work Laptop
Banking Network
DMZ
Web App Database
Banking Web Application
Trusted Network
Central Bank
HTTPS
WAF
HTTPS
Back End Systems
Customers


Credit Verification Services
Public Internet
East Northeast Wilmington Bank
DMZ
Back Office Employees
Office Computers
Firewall
Customers
VLAN Router
WiFi
Remote Workers
Application Server
ATM Server
VPN
HTTPS
VPN Gateway
HTTPS
Mainframe Banking Server
Work Laptop
Banking Network
DMZ
Web App Database
Trusted Network
Central Bank
Banking Web Application
HTTPS
HTTPS
WAF
Back End Systems
Customers

Putting our Threat Model to Action

1. Security Mitigations
    1. Properly segment networks
    2. Eradicate lines of communication between segments
    3. Ensure persistent logs and sensor placement on hosts as well as networked architecture
    4. Drop traffic to known Ips and domains associated with APT 25
2. Threat Hunting
    1. Observe VPN logs
    2. Observe Exchange Server logs
    3. Analyze authentication failures, and rapid authentications in a short time
    4. Focus on gateways into the network where client aided attacks may take place
3. Adversarial Emulation
    1. Emulated phishing attacks
    2. Automate SQL injection attacks
    3. Red Team engagement against VPN gateways
    4. Security Assessments / Vulnerability assessment against externally facing entities
    5. Test for possibility of API misuse in Web App and Enterprise Application
4. Architecture
    1. Audit current systems; search for hidden remote end points i.e. test websites; unused accounts
    2. Remove local admin rights and review password policy
    3. Require MFA for remote and on-site employees

Feeding The Intelligence Lifecycle



- PIRs
  1. Phished emails with similar remote access attachment
  2. Wide spread failed authentication attempts using dumped passwords
  3. Firewall logging anomalous TCP/IP traffic originating from inside the trusted network

- Sources
  - Internal: WAF Logs, Web Application Logs, Endpoint Security, Router Logs, VPN Logs, Vulnerability Scans
  - External: Threat Data Feeds, Paste Bins, Dark Web, HUMINT

- Data is collected, filtered, organized, and delivered to a common repositor for analysis
- Analysis is conducted to confirm or deny the validity of our security controls threat assumptions, and logging
- Analysis will uncover if we need to modify our PIRs and/or sources