HOW THEY'RE GETTING THE DATA OUT OF YOUR NETWORK

Eric Koeppen
IBM X-Force Advanced Research
erkoeppe[at]us[dot]ibm[dot]com
@PorkChop
(v1)

AGENDA

- Introduction
- Exfiltration Scenarios
  - Advanced Persistent Threat (APT)
  - Point of Sale (POS) Malware
  - Financial Malware
- Conclusion

How They're Getting The Data Out Of Your Network:

A Survey Of Methods Used For Exfiltration Of Sensitive Data, Recommendations For Detection And Protection

Introduction

Introduction

- Initial malware infection often just the first step.
- Data sent to external servers.
- Can have disastrous effects:
  - Initial loss of revenue
  - Company brand image
  - Customer loyalty
  - Competitive advantage (trade secrets)
  - Subsequent lawsuits

How They're Getting The Data Out Of Your Network:

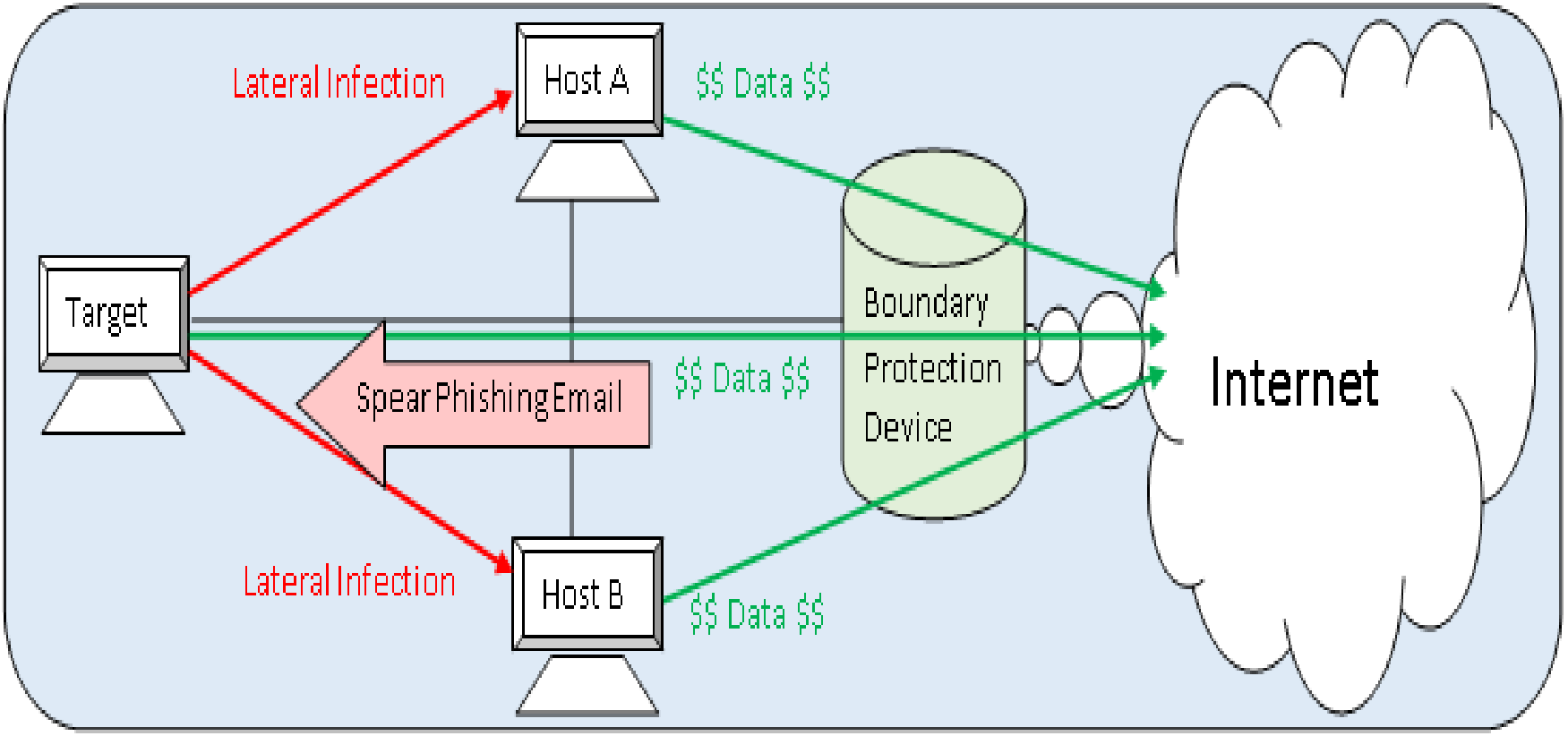
A Survey Of Methods Used For Exfiltration Of Sensitive Data, Recommendations For Detection And Protection

Exfiltration Scenarios

Advanced Persistent Threat

- Operation ShadyRAT
  - Began 2006 and ran for 5 years
  - Targeted over 70 organizations
  - Government organizations & private companies
  - Multiple infection mechanisms
  - Moves laterally through network
  - Novel C2 (often used steganography)
  - Petabytes of data

ADVANCED PERSISTENT THREAT



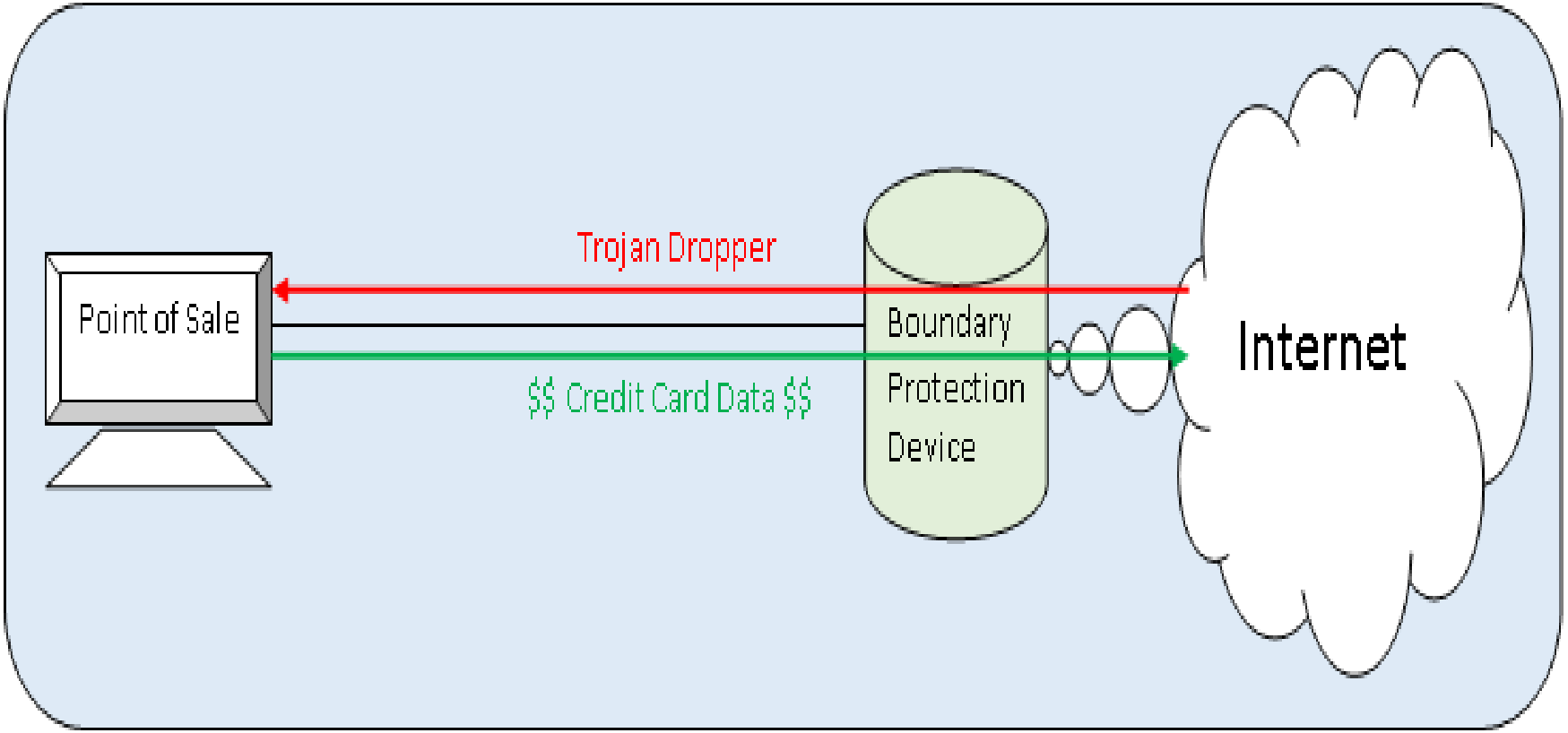
Advanced Persistent Threat

- Detection APT Exfiltration tactics
  - Data different for each site
    - Data types different
    - Data formats different
  - Various forms of C2
  - Initial connection uses predefined handshake

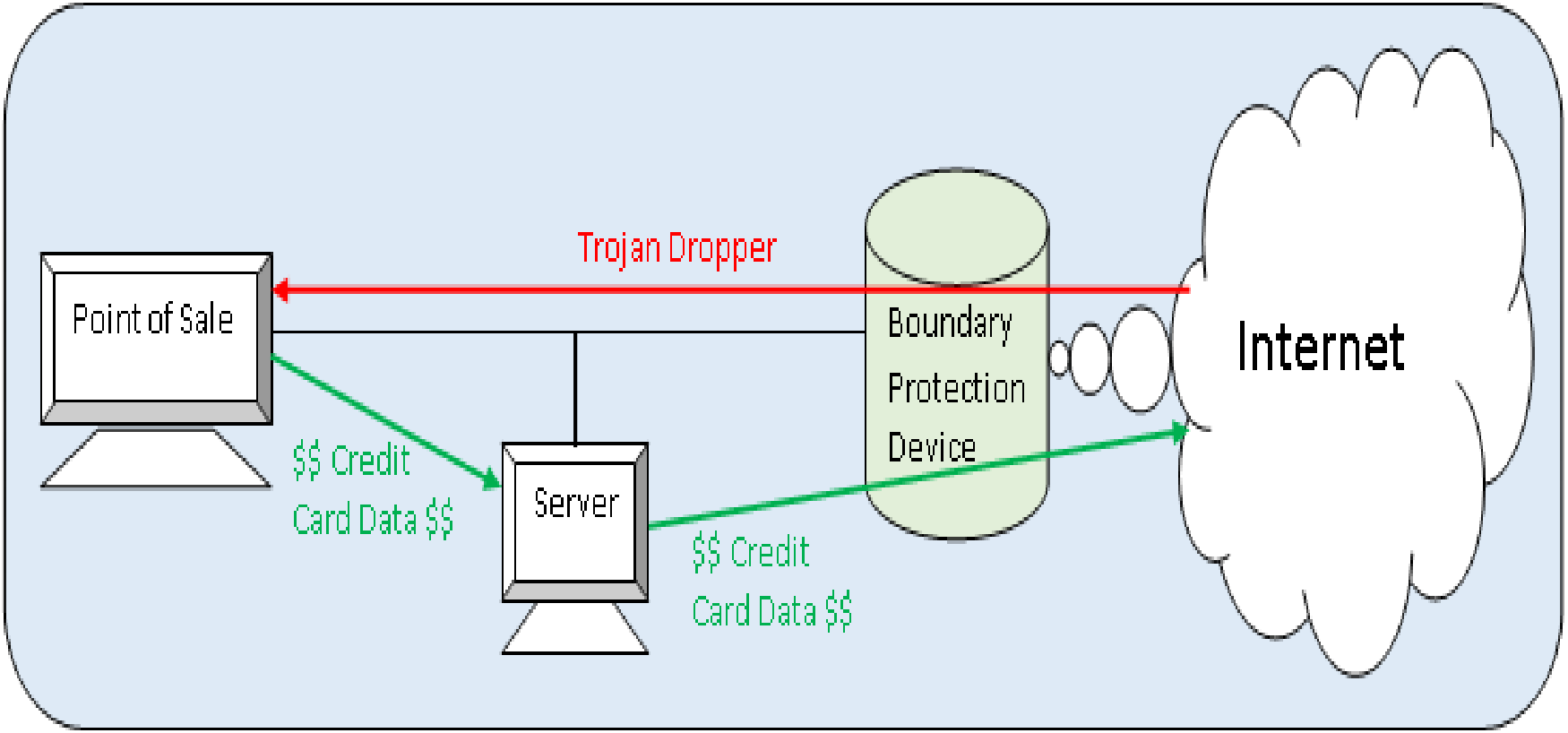
Point of Sale Malware

- BlackPOS – the Target attack
  - Customer data compromised
    - 40 million accounts
    - PII data for 70 million
  - Initial infection by Trojan
  - Periodic memory scraping to collect info

Point of Sale Malware (Scenario 1)



POINT OF SALE MALWARE (SCENARIO 2)



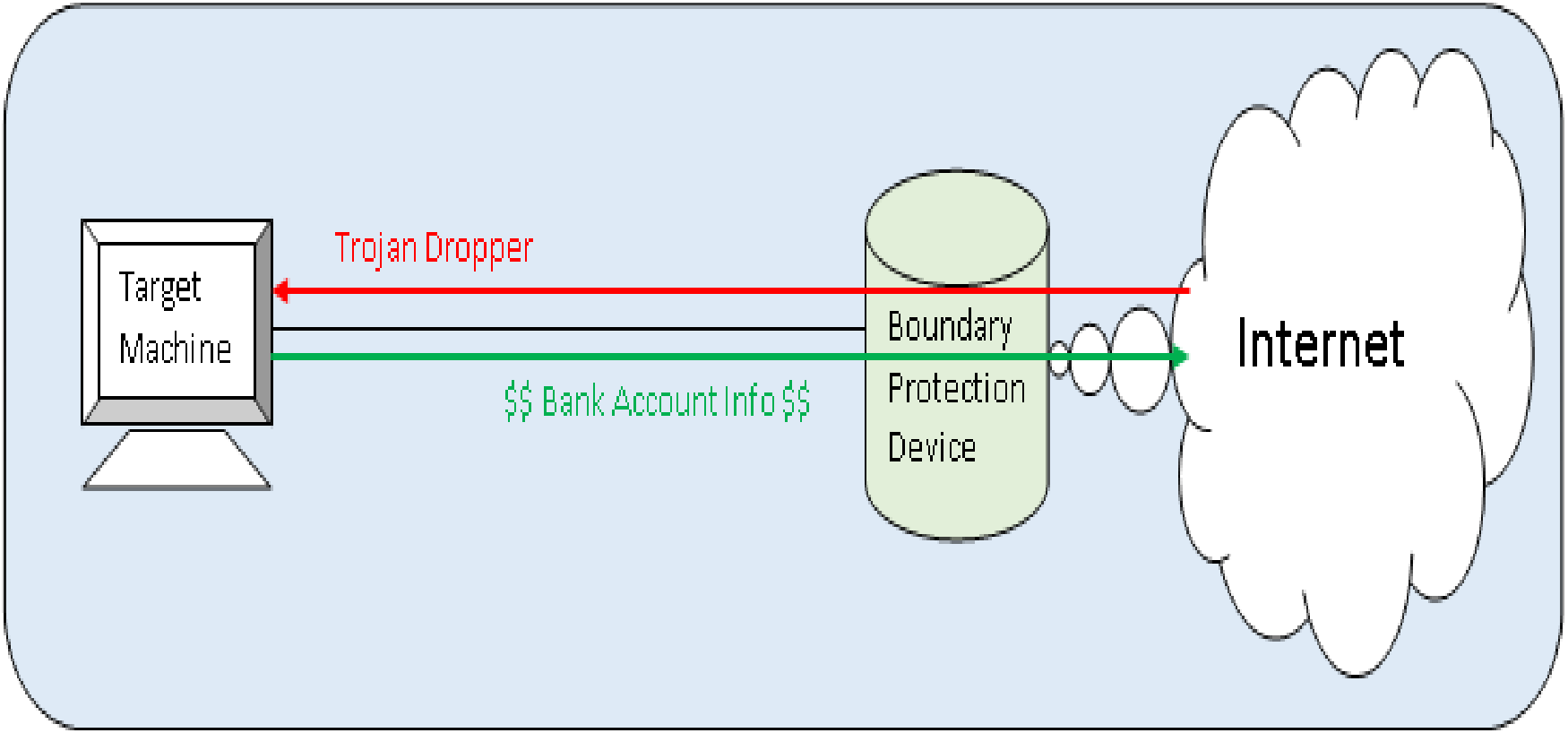
Point of Sale Malware

- Detection POS Malware Exfiltration
  - Leverages different transport protocols/methods
    - HTTP Posts, HTTP Gets, HTTPS, FTP, SMB/NetBIOS, NFS, etc
  - Data usually known format:
    - Track 1 & 2 credit card information
  - Various data encoding techniques:
    - Some samples use Ascii or UUencoding
    - Some samples use minor obfuscation
    - Some samples use encryption

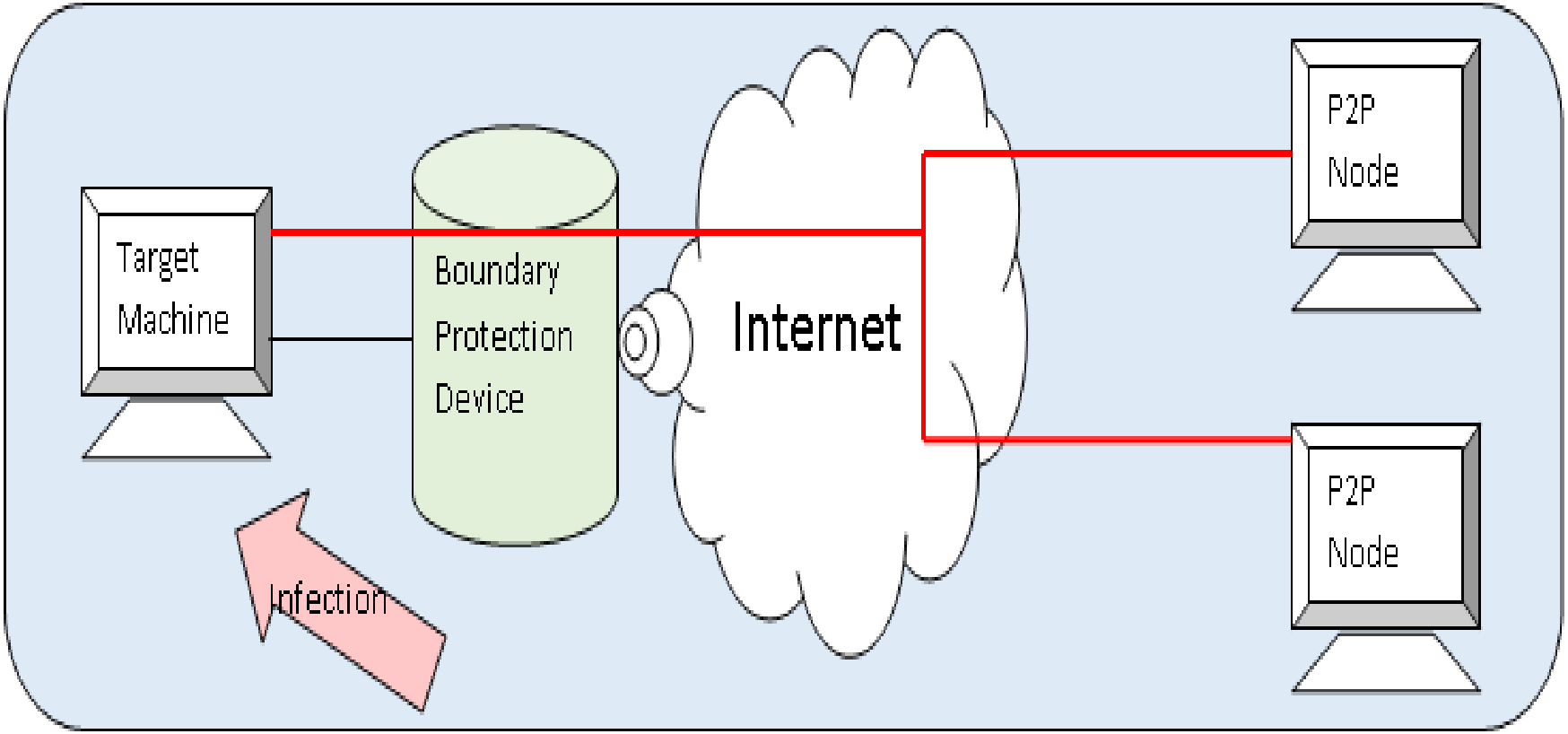
Financial Malware

- Zeus Banking Trojan
  - Many variants
  - Has been around for years
  - Gameover Zeus variant has accounted for over $100 million in theft since 2011
  - Various techniques:
    - Mock up web pages for stealing bank info
    - Parsing cookie files for local data-containing files
    - Steal digital certificates, local private keys
    - Stealing FTP client info and mail client settings
    - Parses registry keys for valuable information

FINANCIAL MALWARE (SCENARIO 1)



FINANCIAL MALWARE (SCENARIO 2)



Financial Malware

- Detection Zeus Banking Trojan Exfiltration
  - Constantly updating their techniques
  - Payload messages hashed, signed, and encrypted with RC4 encryption
  - Can detect the presence of P2P botnet on the network (Game Over P2P variant)
    - Detect P2P keep-alive messages

How They're Getting The Data Out Of Your Network:

A Survey Of Methods Used For Exfiltration Of Sensitive Data, Recommendations For Detection And Protection

Conclusion

Conclusion

- Changing landscape
- Detection based on knowing:
  - Which data is being targeted
  - What are typical formats for that data
  - How that data is being encoded
- When data is encrypted, monitor traffic patterns
- Common practices can go a long way:
  - Monitor logs
  - Keep patches up to date
  - Lock down acceptable communication
  - Educate users

Thank You!

Eric Koeppen
IBM X-Force Advanced Research
erkoeppe[at]us[dot]ibm[dot]com
@PorkChop