Like what you hear? Tweet it using: #Sec360
AGENDA

• Introduction
• Retail Cyber Crime – How to detect CC data theft
• Protecting Other Critical Assets
• Fraud
• Security Analytics Platform
• Summary
TARGET BREACH BY THE NUMBERS (THANKS KREBS!)

• 40 million credit cards stolen

• 46% drop in profits

• $200 million – cost to financial institutions for reissuing credit cards

• What assets does your business have that could cost if compromised?

http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/
WHERE DOES CC DATA EXIST?

• Endpoints
  • POS Systems
  • Back-office Systems

• Network
  • Communications between POS and back-office or 3rd party payment processors

• These are the areas where attackers will focus, the attack surface
CREDIT CARD PROCESSING: NORMAL

Diagram showing the flow of data from POS systems through ports/protocols to a datacenter and then to 3rd party processing.
CREDIT CARD PROCESSING: COMPROMISED!

Like what you hear? Tweet it using: #Sec360
POS MALWARE: ENDPOINTS

- POS Systems
  - New process(es) running
  - Registry changes for persistence
  - Changes to the file system
  - Possibly different authentication activity

- Back-Office Systems
  - New process(es) running
  - Registry changes for persistence
  - Changes to the file system
  - Possible different authentication activity
POS MALWARE: NEW PROCESSES

• Where to look in the log data:
  • Some OS’s can audit process activity
  • Otherwise an endpoint monitoring solution can be used

• Strategies to detect new processes
  • Manual or Automated whitelisting
  • Peer Trending – compare prod systems to a “gold” standard
POS MALWARE: REGISTRY CHANGES

• Where to look in the log data:
  • Registry Monitoring solution should be used to audit registry changes
  • Specifically, look for changes in the autostart paths:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]

• Strategies to detect registry changes
  • Simple alarming
POS MALWARE: FILE SYSTEM CHANGES

• Where to look in the log data:
  • Certain OS’s can monitor for object-level changes
  • Ideally a FIM solution should be utilized

• Strategies to detect FIM activity
  • Simple alarming
POS MALWARE: CHANGE IN AUTHS

• Where to look in the log data:
  • Authentication logs
  • Endpoint monitoring solution

• Strategies to detect changes in authentication activity
  • Baseline
    • Who authenticates?
    • From where?
    • How often?
POS MALWARE: NETWORK

• CC data needs to be exfilled somehow

• Generally requires some sort of outbound network connection

• Data might be sent outbound directly from POS systems, or aggregated in compromised system and moved out from there
POS MALWARE: CHANGE IN NETWORK ACTIVITY

• Where to look in the log data:
  • Network Forensic Data (Layer 7)
  • Flow Data
  • Firewall Data
  • Any data describing end-to-end network activity

• Strategies to detect changes in network activity
  • POS systems communicating with a new host
    • Simple Whitelisting
    • Peer Trending
  • POS systems communicating over a new/unknown protocol
    • In the case of a compromised back-office system that the POS systems normally communicate with
  • Similar strategies should be applied to back-office systems
    • Communicating with a new host?
    • Communicating over new/unknown protocol?
    • Baseline/Trent bytes transferred
So far we’ve been talking about behavioral indicators:
  • New types of communication
  • Changes in the composition of processes running
  • Changes in the type of file system activity
  • Etc

Atomic indicators (lists of IPs, file hashes, etc) are easy to bypass
  • Get a new C&C Server
  • Repack/modify your malware
  • Etc

By utilizing behavioral indicators, any critical assets can be protected without having to completely understand the threat…for instance…
DOES THIS REALLY WORK?!?!?

• YES!!

• When testing with a large retail organization, on day one we found:
  • 6 types of malware running in the POS environment
  • Unauthorized file system modifications
  • An employee charging a smartphone on a POS system
  • Similar strategies can be used to protect other types of assets…
OLD SCHOOL APT: STUXNET

• 5 Network Propagation Routines
  • P2P over RPC
  • WinCC database default password
  • Network Shares
  • MS10-061 Print Spooler Zero-Day Vulnerability
  • MS08-067 Windows Server Service Vulnerability

• Network Propagation is Noisy
  • Probes for specific port on target machines
  • Can be identified in Flow data

• Removable Drive Propagation
  • LNK Vulnerability
  • AutoRun.Inf
OLD SCHOOL APT: STUXNET

• Similar to Propagation, Infection Itself Quite Noisy
• Creates files in system and app folders:
  - xutils\listen\xr000000.mdx
  - xutils\listen\s7p00001.dbf
  - xutils\listen\s7000001.mdx
  - GracS\cc.alg.sav
  …many more
• Modifies files in system and app folders:
  - Apilog\types\n  …many more
• Renames s7otbxdx.dll to s7otbxsx.dll and replaces original
  This is the heart of Stuxnet, the piece that intercepts and modifies data between WinCC/Step7 and certain PLCs.
• Added registry entries
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  "[random charaters.exe]"
OLD SCHOOL APT: STUXNET

• So systems infected by STUXNET, that were supposed to only be used to program/control certain PLCs:
  • Communicated over the network in new ways
  • Made changes to the file system
  • Made changes to the registry
  • Etc

• Monitoring the critical systems STUXNET attacked would have identified the infection
ANOTHER STRATEGY

• Sometimes we don’t know what type of behavioral change to look for

• Unknown changes can leave artifacts in the composition of the log data

• Build a baseline of the unique event *types* on a per-log-source basis

• If a new type of event is noticed in any log source’s stream, generate an alarm
MOVING OUTWARDS

- This approach really focuses on the “it’s when, not if” mentality, and is designed to help limit the scope of a breach.
- Ideally an attack is caught earlier in the kill chain, lifecycle, etc.
- Most successful attacks start with a spear phish and end up utilizing compromised hosts and credentials to pivot to the target assets.
- Multi-Dimensional Behavioral Analytics (MDBA) can be utilized to help detect compromised hosts/credentials before critical assets are accessed.
MDBA CONCEPT

• Utilize trending to identify when a host starts new processes, has new authentication activity, abnormal connections to other hosts, a change in the type of outbound connections initiated, etc.

• Any one of these changes for a given host might not be of much interest, but several of them changing within a small timeframe warrants investigation.
FRAUD

• Similar analytic capabilities can be utilized to detect fraud when applied to bank data
• A handful of use cases implemented at a customer:
  • Unusually large ATM withdrawal or ACH transfer
    • Trend and build up sum of each user’s withdrawals/transfers over 60 days, if they withdraw/transfer more in current day than the sum of last 60 days, generate an alarm
  • Loan Rate Change, Loan Issued, Loan Rate Change
    • All by the same loan officer...hooking up a friend/family member
  • ATM Withdrawals using the same card from disparate geographic locations
    • Just like VPN use cases, but for ATM withdrawals
  • Password Change, New ACH Payee, Large Transfer to new payee
    • Suspicious
• Not all necessarily indicate fraud, but they do put an account onto a watch list
SECURITY ANALYTICS PLATFORM

**Input**

FORENSIC DATA COLLECTION

- Log Data
- Application Data
- Vulnerability Data
- Event Data
- Flow Data
- Other Machine Data

FORENSIC DATA GENERATION

- Host Forensics
- Network Forensics
- File Integrity Monitoring
- DPI / Application ID
- Data & Process Monitoring
- Layer 7 Flow
- Network Connection Monitoring

**Analytics**

PROCESSING

- Time Normalization
- Data Classification
- Meta Data Extraction
- Context Infusion
- Risk Prioritization

REAL-TIME ANALYSIS

- Advanced Correlation
- Behavioral & Statistical Baselines
- Pattern Recognition
- Whitelist Profiling

FORENSIC ANALYSIS

- Search
- Indexing
- Persistence

**Output**

ACTIONABLE INTELLIGENCE

- Risk Prioritized Alerts
- Real-Time Dashboards
- Reports

ADAPTIVE CYBER DEFENSE

- Incident Response
- Workflow
- Case Management

Like what you hear? Tweet it using: #Sec360
SUMMARY

• Understand where your critical assets reside/move
• Utilize existing infrastructure to instrument behaviors on/around critical assets
  • Event logs
  • Syslogs
  • Application logs
  • Flow data
  • Etc
• Augment instrumentation with additional forensic visibility
  • Endpoint Monitoring
  • Network Monitoring
• Utilize behavioral analytics to understand when something changes in real-time
QUESTIONS?

David Pack
Director, LogRhythm Labs
david.pack@logrhythm.com
@LogRhythmLabs
http://blog.logrhythm.com