That Point of Sale is a PoS

Charles Henderson
Vice President – Managed Security Testing
Trustwave
@angus_tx

David Byrne
Senior Security Associate
Bishop Fox
Agenda

- POS Architecture
- Breach Investigations
- Testing Techniques
- Penetration Test Findings
PoS Attacks: Theory vs. Reality

- Most breaches involve very simple vulnerabilities
- Future breaches are likely to leverage more complex vulnerabilities as merchants become more secure
- Many merchants have very immature security programs
PoS Purchasing: Security Is Not A Criteria
Point of Sale Architecture
Hardware

- Standard PC workstation
- Specialized peripherals
  - Card reader and PIN pad
  - Barcode scanner
  - Touch screen – much less “specialized” than it used to be
  - Expanded keyboard
  - Scale
  - Customer display
Hardware

◆ Interfaces
  ◆ USB
  ◆ RS-232 – becoming less common
  ◆ TIA-485/RS-485 – rare in 2015
  ◆ Ethernet – some PIN pads and printers can connect directly to network
Client Operating System and Software

- Windows dominates
- Some Linux
- Occasional use of network boot with no local storage
- Even large retailers use off the shelf packages that are customized to the client
Application Servers

- Many separate systems:
  - Transaction records (purchases, refunds, etc.)
  - Payment card processing
  - Promotions
  - Customer tracking
  - Gift cards

- May be from entirely different vendors; more likely to see custom software in larger merchants
Application Servers

- In larger environments, typically implemented as middleware services: XML web services, etc.
- Small environments (isolated stores) likely to store all data on register.
Remote Administration

- Major source of compromise
- Registers will almost always have remote administration services
- Small organizations typically outsource administration
- Large chains will still not have on-site technical support
Breach Investigations
Attacks Become More Efficient

- Physical Modifications (External)
- Physical Modifications (Internal)
- Drive-By Malware
- Scalable Malware
Physical Attacks (Internal)
Physical Attacks (Internal)
Physical Attacks (Internal)
Forensics Case Study One: Vendor Negligence

- Same administrator password for nine years
- Attackers most likely discovered merchant in breach of other merchant using same vendor

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Administrator [500]</td>
</tr>
<tr>
<td>Full Name</td>
<td></td>
</tr>
<tr>
<td>User Comment</td>
<td>Built-in account for administering the computer/domain</td>
</tr>
<tr>
<td>Account Created</td>
<td>Xxx Xxx XX XX:XX:XX 2004</td>
</tr>
<tr>
<td>Last Login Date</td>
<td>Xxx Xxx XX XX:XX:XX 2013</td>
</tr>
<tr>
<td>Pwd Reset Date</td>
<td>Xxx Xxx XX XX:XX:XX 2005</td>
</tr>
<tr>
<td>Pwd Fail Date</td>
<td>Xxx Xxx XX XX:XX:XX 2014</td>
</tr>
<tr>
<td>Login Count</td>
<td>261</td>
</tr>
</tbody>
</table>

Password does not expire
Normal user account
Forensics Case Study Two: Vendor Negligence

- Attacker installs memory-scraping malware
- Data was *manually* retrieved by attacker; memory dumps left on PoS disk
- Malware easily discovered during investigation using current AV

Scan type: Quick scan
Objects scanned: 191441
Time elapsed: 12 minute(s), 40 second(s)

Files Detected: 2
C:\WINDOWS\system32\Searcher.dll (Trojan.Clicker) -> Quarantined and deleted successfully.
C:\WINDOWS\system32\QOS.dll (Trojan.Agent) -> Quarantined and deleted successfully.
Forensics Case Study Three: Vendor Negligence

- Back of house server configured for remote management utilizing pcAnywhere
- Null Administrator password
- Administrator password had not been changed in nine years
- Malware easily discovered during investigation using current AV
Forensics Case Study Four: Origin of Malware

- Multiple workstations in CHD environment used to browse pornographic websites, download torrents, and video chat
- Keylogger installed by attacker also logged use of machines with CHD being used to play Guitar Hero 3, Call of Duty, and other games

Key Pressed:
```
bxcvbxcvbxcvbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

b{Esc}bbxcvbxcvcvcvbvbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb

b{Esc}bbvbvbvbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
```

- CHD being used to play Guitar Hero 3, Call of Duty, and other games
- Keylogger installed by attacker also logged use of machines with CHD being used to play Guitar Hero 3, Call of Duty, and other games

```
xcvbxcvcbxvcbxvcbxvcbxvcbxvcbxvcbxvcbxvcbxvcbxv
```

- CHD being used to play Guitar Hero 3, Call of Duty, and other games
- Keylogger installed by attacker also logged use of machines with CHD being used to play Guitar Hero 3, Call of Duty, and other games
Backoff Malware

- Self-propagates through weak remote access authentication
- Command and control features
- Memory scraping for payment card data
- Automatic data exfiltration
- Keylogging
- New infections look for old versions of Backoff to remove
Testing Strategies
Multiple Testing Perspectives

- Remote (routed) network access
  - Vulnerable network services
- Local network access
  - Proper protocol encryption
  - Endpoint authentication (i.e., no MitM)
  - Identification of second-tier application servers
Multiple Testing Perspectives

- Momentary physical access
  - Introduction of malicious device – key-logger, network adapter, USB attacks, IEEE 1394 DMA, etc.

- Prolonged physical access
  - Hard drive encryption
  - Local storage of sensitive data (i.e., payment card numbers)
  - Analysis of application binaries
  - Monitoring and modification of key peripherals (i.e. PIN pad)
Multiple Testing Perspectives

- Console interaction
  - Execution of unauthorized and malicious programs
  - Escalation of system privileges
  - Modification of PoS application
  - Monitoring of network and peripheral communication
  - Memory dumps
Physical Security

- Quality of locks
- Exposed network cables, drops
Penetration Testing Results
Physical Security

- This is not good physical security
- Easy access to USB, Ethernet, etc
Physical Security

- This is not a good lock
166816 (Z66816)

- Since 1990, this has been the default password for all products from a major vendor
- Publically documented in a 1994 alt.2600 FAQ (featuring terms like “sysop” and company names like “Northern Telecom”)
- 90% of the terminals of this brand we test for the first time still have this code
Improper Use of Symmetric Keys

- Symmetric algorithms: one key for both encryption and decryption
- Asymmetric algorithms: decryption & encryption keys separate
- Using symmetric algorithms for payment card data invites abuse
Operating System Security

- Most POS deployments are overly reliant on passwords
  - Very difficult to secure OS passwords on endpoint
- AV scanning isn’t perfect, but still important
- Easy to introduce custom malicious executables
- No drive encryption
  - Simplifies offline attacks
  - Allows stolen devices to be used for analysis
  - Devices get stolen
Authentication Fail

- Single set of authentication credentials across enterprise
- Automatic Windows login and local enforcement of POS user authentication – no authentication against networked application services
Running as administrator

- Vendors often claim that this is a requirement.
- Lies, nothing but lies.
- Windows and Unix-like operating systems have never worked this way.
- Simply an excuse for lazy programmers
PIN Pad Debug Triggered
Plaintext Network Traffic

Note the protocol. This is not IP.
Running Unauthorized Programs

- This is how malware infections start
Network Communication Security Flaws

- Plaintext communication
- Failure to authenticate endpoints
  - SSL is next to useless without certificate verification
Encryption Insanity

- Symmetric encryption used for transmission of payment cards
- Point-to-point-to-point encryption (one too many points)*
- XOR to protect passwords; programmers are always amazed that we can reverse this

* Note: The addition of more points does not enhance security posture.
PIN Pad Security

- Default configuration often insecure
- Can almost always be reprogrammed from register
  - Convenient way of implementing management across enterprise
  - Some code is cryptographically signed
  - Configuration is almost never signed
  - Attacker may be able to disable security controls such as end-to-end encryption
PAN Abuse

- Coupon printer using PAN to track customers
- PAN returned to PoS for truncation
- Purchase history stored for tracking fraud – 37 million numbers
- Adding drives to register store growing debug transaction logs
Card Numbers in RAM
Symlink to Access Filesystem
Apply:
PoS Security Program
Implement a PoS Security Program

- Always verify the security claimed to be implemented by vendors
- Top priorities:
  - Ensure no payment card data is stored on registers
  - Enforce strong authentication policies
  - Don’t run PoS user interface as “administrator”
  - Stay current on patches and AV signatures
Implement a PoS Security Program

◆ Secondary priorities:
  ◆ Evaluate security of data communication (encryption, certificate checks, etc.)
  ◆ Pen test application servers for application vulnerabilities
  ◆ Lock down client execution environment

◆ Final efforts:
  ◆ Use strong authentication (key/certificate-based)
  ◆ Implement end-to-end encryption with asymmetric keys