Point-of-Sale (POS) Malware: Tactics and Strategies for Protecting Customer Payment Information

Bit9 and Carbon Black

Jeffrey J. Guy | 20 Feb 14
jjguy@bit9.com
@jjguy
Introduction

 prova Jeffrey J. Guy

• Background
  – 6 years USAF, USAF Red Team
  – 7 years ManTech, CNO R&D services
  – 2 years at Cb, now Bit9

• Director, Product Management at Bit9
  – Formerly Director of Operations at Carbon Black

Feb. 13, 2014

• Bit9 and Carbon Black merged to deliver single solution prevention, detection and response
Assume You Will Get Breached (Last 12 Months)

- Schnucks
- Drupal
- Ubisoft
- Adobe
- The Washington Post
- Yahoo!
- Target
- LivingSocial
- Evernote
- RentPath
- Apple
- MNSure
- Bit9
- Carbon Black
- Neiman Marcus
- GitHub
- Michaels
- National Security Agency
- United States Air Force
- United States Army
- United States Navy
- United States Marines
- United States Coast Guard
- National Security Agency
- United States Navy
- United States Coast Guard
The State of Information Security

Compromise happens in seconds
Data exfiltration starts minutes later
It continues undetected for months
Remediation takes weeks
At $341k per incident in forensics costs

THIS IS UNSUSTAINABLE
Endpoint security is evolving

Traditional Security

- **Prevention**: Provided by endpoint antivirus. Easily bypassed.
- **Detection**: Provided by endpoint antivirus. Efficacy limited to the opinion of your AV vendor’s signature database.
- **Response**: Usually by external consultants.

Emerging Model

*Prevention, detection and response as a single, integrated and continuous process.*
Protection = Prevention, Detection and Response

“Security...will shift to rapid detection and response capabilities linked to protection systems to block further spread of the attack.”

“Functions organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover.”
Prevention

Traditional Prevention

- Small local signature database of known-bad, wide-spread, well-known threats
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor’s global database, at the moment of compromise

Emerging Prevention

- Local database of known-good applications
- Tailored policies to your environment, not the world’s
- Lessons from network perimeter history: default-deny

Bit9 + Carbon Black
Detection

Traditional Detection

- Small local signature database of threat data
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor’s global database, at the moment of compromise
- Only action is block, thus requires high confidence

Emerging Detection

- Large global database of threat data
  - IOCs, VirusTotal, iSIGHT, US Cert, Bit9 Software Reputation Service and ATIs
- Efficacy is the consensus opinion of the industry’s collective intelligence
- Can block or flag for review, increasing overall utility
- True detection in depth
Response

Traditional Response

- Ad hoc, as-needed activity by expensive, external consultants
- Relies heavily on disk and memory artifacts for historical record
- Guidelines on IR prep (e.g., NIST 800-61, etc.) limit preparations to administrative measures

Emerging Response

- Even your entry-level staff can do IR in seconds
- Complete historical record of when/where/what/how
- Better, faster and cheaper than traditional IR
What Does This Mean for Your Security?

**Traditional Security Bottom Line**
- **Prevention**: dependent on AV signature of your one chosen vendor *at the moment of compromise*
- **Detection**: dependent on AV signature of your one chosen vendor
- **Response**: expensive and time-consuming forensics, limited to present and future

**Emerging Security Bottom Line**
- **Prevention**: likely never runs, defaultdeny
- **Detection**: consensus opinion of the industry’s collective intelligence
- **Response**: complete breadth and depth in seconds, including complete history
BlackPOS in Carbon Black – DEMO!

**Process Analysis**

f6f8df8d6c2197c7a3c8b35e7a11adec96fbd29c59c8d8ad6ce13d470eb8f052.exe.bin.exe on J-418D7A3CCFE64 - active for 1 days about 3 days ago

**Process Name (50+)**
- svchost.exe (92.7%)
- mscorwv.exe (1.5%)
- npen.exe (0.9%)

**Group (1)**
- default group (100.0%)

**Hostname (2)**
- xpsp3 (97.2%)
- j-8205e0c27e0c4 (2.8%)

**Parent Process (50+)**
- wscript.exe (63.0%)
- mscorwv.exe (1.5%)
- msieexec.exe (1.3%)

**Process Path (50+)**
- c:\windows\microsoft.net...
- d:\7ac9c61e417baa54...
- 8219c45e4723e8835e6c...

**Process MD5 (50+)**
- 5e7f396860d32b26bf0d...
- d37acaed61e417baa54...
- 8219c45e4723e8835e6c...

**Currently selected**
- cmd.exe
- ftp.exe

**Company**: Unknown
**Product**: Unknown
**Description**: Unknown
**Signed**: Unsigned
**Publisher**: Unknown

**Alliance Feeds** 3 hit(s) in 2 report(s)

**VirusTotal Scan Results for 7F1E4548790E7D936117694...**
- 2-18-2014
- Score: 43
  - 7F1E4548790E7D9361176949AB29F2
  - 7F1E4548790E7D9361176949A839F2

**VirusTotal Scan Results for C24B383D211C34DA8FFCC1...**
Security Lifecycle

Prevent

Prevention

Detect & Respond

Visibility

Response

Detection

Bit9

Carbon Black
Come Say “Hi” at RSA!

Jeffrey J. Guy
jjguy@bit9.com
@jjguy