Enterprise Defense & Why You’re (Organization Is) Most Likely Doing it Wrong.

Tom Parker, April 2015
The Speaker..

• CTO FusionX
• Consultant > 15 Years
• Author (2004): Cyber Adversary Characterization
• Speaker/Trainer Blackhat Briefings/Training
  – Come learn how to own SCADA gear this summer!
• Columnist Dark Reading
What we do & topic relevance

• Our Perspective:
  – Conduct realistic, scenario based attacks
    • Typically for CXO / BOD Level
  – Identify customer ability to:
    • Detect, Protect, Respond
  – Provides first hand understanding of technical issues and common process level flaws
Todays Agenda

• Review of Threat Environment
  – Evolution 00’s - today

• Common Adversary TTP’s

• Key Issues in Enterprise Environments

• Addressing Gaps:
  – Increasing ROI on Existing Investments
Todays Environment

• 2014 estimated: $500B+ cost to Global Economy
• US “Hemorrhaging” Intellectual Property
• Enterprise IT is Losing Battles Daily
  – Just not the war (yet)
• Focus on Expense in Depth
  – And Compliance
Threat Time Line


2010: Stuxnet (Discovered) → 2010: Comment Crew Attacks → 2011: DuQu (Discovered) → 2011: Operation Shady Rat (Discovered)

2012: Flame (Discovered) → 2013: Comment Crew Report (Disclosed)
Adversary Evolution: Attackers Respond to Defense

• Attackers Forced to Evolve
  – Broad use of firewall products
    • Focus on ‘hard outer shell’
  – Microsoft focus on securing network services
  – Implementation of DEP/ASLR for Services
    • Resulting in less network attack surface

• Offensive vs. Defensive Evolution
Real-World Attacks Today

• Are not:
  – Nessus
  – Always sophisticated

• Are:
  – Fully Asymmetric
Process of Compromise: Non Linear

- Asset Discovery
- Asset Analysis
- Compromise
- Asset Data Mining
- Asset Value Analysis
Observe, Orient & Decide: Reconnaissance

• Careful Planning Pays Dividends
  – Surgical Compromise of Key Resources/Individuals
  – Reduced Likelihood of Detection
  – Increased Chances of Success

• Common Sources Include:
  – Social Networks
  – Search Engine Data Mining
  – Tech Forums
  – Paste Bin, Gist etc.
Act: Phishing & Drive-by Attacks

• Remains Tactic of Choice for Many Groups
• Often Provide High ROI for Attacker
  – Direct, internal network access
  – Immediate domain credentials / tokens
  – Access to large amounts of internal data
• Cannot Be Entirely Solved via User Education
• Cannot Be Entirely Solved via IT Controls
  – Even next-gen technologies (FireEye et al.)
Observe, Orient, Decide

• Information Repositories
  – Poorly Protected File Shares
  – Asset Management Systems

• Network Equipment
  – Pub SNMP etc.

• Broadcast Protocols
Act: Lateral Movement & Escalation

• Attackers <3 Flat Networks
  – Direct Access to Administrative Interfaces
  – Exploitation of Internal Network Services
  – Access to File Shares / Databases

• Secondary User Account Compromise
  – Targeting of Administrative Group Users
Act: Common Internal Targets

- Authentication Subsystems:
  - Domain Controllers
  - RAS Servers
  - Two Factor Systems (RSA SecurID Servers et al)

- Remote Access Devices:
  - SSL & B2B VPN Appliances
  - VDI Environments
Act: Common Internal Targets (Cont.)

• Internal Web Applications
  – Think HR, CRM, Management Apps
    • Often built on tech such as SAP, JD Edwards, E-Business
  – Typically less security scrutiny than ext. apps
    • Fewer controls between application tiers
    • Far less frequently tested & monitored

• Management Infrastructure
  – Frequently crosses over trust-zones
  – Patch & configuration management systems
Detect, Protect Respond

• Basic Enterprise Issues Hamper:
  – Detection: with confidence
  – Protection: effectively
  – Response: quickly enough, or at all
Detect: Key Issues

• Missed First Opportunities for Detection
  – Before primary attack even occurs

• Common Missed Opportunities
  – Domain Registration
  – Network Recon
  – Social Networks etc.
Detect: Key Issues

• There’s LOTS of Data within Enterprise
• Often Look to ‘Next-Gen’ Solutions
  – When the answer/data might already exist
• Data worthless without context
  – Asset context
  – Event context
Detect: Key Issues

• Common Monitoring Gaps:
  – Service & Privileged Account Usage
  – Industrial Control Systems Equipment
    • Often operated behind back of Enterprise IT
  – Enterprise Applications
    • Any monitoring often lacks application context
      – Generally focused around WAF technology
      – Versus application-level feedback to SIEM
  – Databases
    • Query auditing uncommon
    • DB logging infrequently tied to SIEM
Protect: Key Issues

• You can only protect what you know exists

• Unknown Unknowns
  – Poor Internal & External Asset Awareness
    • Sparsely Distributed Assets / Hosting
    • Domain Registration Tracking
    • Asset Management / Unmanaged Connectivity
  – Data Classification, Storage & Flows
    • Where your crown jewels are stored (incl. the copies)
    • How does it move around the environment
Protect: Key Issues

- Poor User Education wrt:
  - Social Media Usage
  - Use of Technical Forums
  - Use of Paste Bin et al.
Protect: Key Issues

• Basic Hygiene Issues
  – Poor network segmentation
  • Common IT resources leveraged across trust-zones
  – Excessive account privileges
  – Third party software patching
  – Insecure or non existent system base lines
  – Insecure remote access solutions (end points)
  – Over reliance on silver bullet solutions
    • FireEye, MIR et al.
Incident Response: Everyone Has a Plan

“Everyone has a plan ‘till they get punched in the mouth” – Mike Tyson
Compromise Time Line

• First 24 Hours of Internal Access **Critical**
  – For Both Attackers and Defenders
  – > 24 Hours == Non-trivial remediation
  – Will have established multiple C2 methods

• One week+:
  – Enterprise-wide compromise
  – Will likely know more about your own environment than your own staff
  – Significantly hinders future defensive efforts
Cost Of Response

Adversary Time On Network

Cost
Response: Key Issues

• Response Times Hampered By:
  – Poor knowledge of targeted assets
    • Allowing for effective triage/prioritization
  – Incomplete information on breach activity
    • Poor visibility / forensic data readily available
  – Inability to handle digital ‘fog of war’

• Response Plan Infrequently (Fully) Tested
  – Table-top exercises have limited value
Detect

• Users
  – Educate them
    • They might be your first line of detection
    • Ensure acceptable social network use is covered.
  – Develop a culture of self reporting
  – Educate them some more
  – Proactively monitor for infringements
    • Particularly social network / disclosures

• Monitor
  – New domains, SSL Certs, Web Sites
    • Via threat intel & other monitoring services
Detect

• Databases: Increase ROI
  – Leverage Table & Column ACL’s
    • Enabling detection of anomalous queries
  – Monitor Sensitive Fields
    • Such as via Oracle AUDIT Tables
  – Baseline Normal Query Activity
    • Such as Originating from App Server
    • Leverage SIEM for Deviations & Correlation Events
Detect

• Applications
  – Hook Applications to Understand Business Logic
    • Log business logic trespass attempts
    • Instrument Interface to SIEM
  – Stop Relying on that WAF!

• Identify & Track Priv. Account Activity
  – Reduce day-to-day use of priv. accounts.
  – Service account RDP’ing – probably not good.
Detect

• Industrial Control Systems
  – Everyone has them
    • HVAC, Energy Distribution Subs, Data Centers Power Management, Branch UPS Devices et al.
  – Find them, monitor them.

• Get Context
  – Develop Asset Risk / Scoring
    • Automate Prioritization Accordingly
Protect

• Get Asset Management Right
  – Don’t necessarily buy that list IT gave you.
  – Monitor Company-Branded Websites
  – Centralize Hosting / Reduce Attack Surface

• Mature Data Classification
  – Enforce adherence to data protection policy
  – Leverage e-Discovery tools to identify spillage
Protect

• Address Segmentation Issues
  – Identify & address problematic trust relationships

• Review Privilege Requirements

• Implement 3rd Party Patch Strategy
  – Proactively identify gaps

• Evaluate True Effectiveness of Security Products
  – Don’t believe (all) the marketing.
Respond

• Ensure your Responders Understand:
  – Your network
  – Have IR SME’s for Specialized Systems
  – Ensure access is provisioned to the right data
  – Train your team to operate under fog of war
  – Test & update your IR plan regularly
    • Not just table top exercises
Detect, Protect, Respond

• Find a Sparring Partner
  – (Don’t just go fight Mike Tyson)
  – Not nessus.

  – Engage in scenario based red teaming activities
    • Test your response times (let the SOC believe its real)
    • Test your business continuity processes
      – Legal, marketing, corporate communications
Wrapping Up

• Get back to basics
• Focus has to change from
  – Silver Bullet Solutions
  • No Solution Can Save you from Poor Hygiene
  – Compliance-centric Security
• Many solutions exist within the Enterprise
• Smart Money Matters, not Volume
  – Measure ROI
Questions?