Information-Driven Cybersecurity

Why Do COTS-Based Architectures Fail to Protect Your Enterprise

4 June 2013

Bill Russell
Cybersecurity Strategist & Senior Architect
Where Has This Approach Gotten Us?

Chinese Domestic Aviation Circa 1983

Soviet AN-24 manufactured beginning 1963 – 40 sold to China

Chinese Y-7 manufactured beginning 1983
BEIJING — China’s military conducted a test flight of a new stealth fighter jet on Tuesday, overshadowing an important visit to Beijing by Defense Secretary Robert M. Gates aimed at improving defense ties — and apparently catching China’s civilian leadership off guard.

(New York Times, July 2011)
Chinese Unmanned Air Vehicle

Chinese made Pterodactyl 1 (2009)

U.S. made MQ-9 Reaper
Think There Is An Interest In Finance?

"China is the world's second-largest economy next to our own. They are a huge trading partner, and our two economies are incredibly intertwined"

Robert Mittelstaedt
Arizona State University

High-Speed Trading Algorithms

The Knife

The Boston Stumbler
The “Fan™” - Layered Cybersecurity Defensive Reference Model

Computer Network Defense
Defense-In-Depth
The Fan™

Layered Cybersecurity Defense Framework

OUTSIDE THREAT

PERIMETER SECURITY

Message Security (anti-virus, anti-malware)
Honeypot

NETWORK SECURITY

Application Security
Secure DMZs
Perimeter IDS/IPS
Perimeter Firewall
Virtual Network Security
Web Proxy Content Filtering
NAC/Endpoint Profiler
Inside Threats

ENDPOINT SECURITY

Content Security (anti-virus, anti-malware)
Endpoint Security Enforcement
Malware Analysis
Enterprise Message Security
Voice Over IP (VOIP) Protection

APPLICATION SECURITY

Desktop IDS/IPS
Static App Testing/Code Review
Dynamic App Testing
WAF
DLP
DAR/DIM/DIU Protection
Data Wiping Cleansing

DATA SECURITY

Enclave Firewall
Host IDS/IPS
Dynamic App Testing
Database Monitoring/Scanning
DLP
DLP
Database Secure Gateway (Shield)
Enterprise Right Management
Data Classification
FICAM
Data Integrity Monitoring
DLP
Data/Drive Encryption
DLP

Monitoring & Response

Mission Critical Assets

Acronyms & Abbreviations:

Acronyms & Abbreviations:

© 2013 Northrop Grumman Corporation

Approved for Public Release # 13-0985

DAR: Data At Rest
DIM: Data In Motion
DIU: Data In Use
DLP: Data Loss Prevention
IDP: Intrusion Detection and Prevention
FICAM: Federal Identity Credential and Access Management
NAC: Network Access Control
PKI: Public Key Infrastructure
SIEM: Security Information Event Management
USGCB: US Govt Configuration Baseline
Well funded adversaries have access to the same technologies as the defenders
COTS Security Technology Misses the Advanced Adversary

• A well architected defense-in-depth security approach based on COTS security technology defeats 80% of the threats

• Determined threat actors have access to all the COTS security products and test their attacks against those tools

• Openly available tools and online collaboration of hacktivists and criminals lower the barrier to entry for adversaries

• Advanced adversaries have state or criminal support including advanced exploits, collection management, and targeting

“Over the course of three months, attackers installed 45 pieces of custom malware. The Times … found only one instance in which … identified an attacker’s software as malicious and quarantined it…”

New York Times, 30 Jan 2013
Offense Always Has An Advantage

• Threat Technical Capabilities
  • Exploits – Development teams with State or criminal support
  • Internet distribution points to drop and pick up
  • Command and Control using Botnets
  • C2 Obfuscation using DDNS, FastFlux DNS
  • Process and attack strategy – intel teams, crash and attack teams, exploit teams, exfil teams

• Threat Intelligence Collection
  • Comprehensive target picture through open source collection
  • Your friends names, professions, and things they like
  • Everything and you post, share, like or link to
  • Social media systems not inclined to provide security

• Further Lowering of the Barrier to Entry
  • MetaSploit makes attacking easy for the uninitiated
  • Threat forums for collaboration and sharing of tools
  • Social Justice and Causes (Anonymous, WikiLeaks, Hacktivists) rallied against your enterprise:
  • Every employee is a possible vector

Threat Actors Only Need to Be Right One Time to Gain Access to the Enterprise
Good Guys Have Some Ways to Level the Field

- Behavioral analytics (Who talks and works with whom)
- Partnerships for threat information sharing
- Threat intelligence team augmentation

- Custom file analysis
- Custom monitoring of network traffic for C2 channels
- Organizational agility to respond to changing threat tactics

Defenders Have to Be Right Every Time… The Field Can Be Leveled by Leveraging Information Available Only to the Defender
So What Should I Do Now?

• Keep the COTS infrastructure that defeats the 80%

• Collect as much data as possible about what is happening on your network

• Play Cybersecurity as a team sport (InfraGuard, ISACs, FIRST)

• Train your employees for live threats (Not just CBTs)

• Look at the problem through a different lens (Not just the IT lens)
THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN