Finger Pointing for Fun, Profit and War?

Tom Parker

tom.at.rooted.dot.net

Quick Introduction..

- Background & Recent Events
- Attribution – why do we care?
- Technical Analysis Today
- Technical Attribution 101
- Enhancing Existing Methodologies
- Non Technical Data Correlation & Augmentation

Media & “Cyber War” Love Affair

- WSJ “Wide Cyber Attack Is Linked to China”
- 60 Minutes “Sabotaging the System”
- Google/Adobe “Aurora Incident”
- Targeted SCADA Malware?

Cyber Conflict Lexicon

- Cyber War
- Adversary / Actor
- Attribution
- APT?

Attribution – Why do we care?

- LE/Actor Deterrents
- Actor Intelligence
  - Profiling Adversarial Technical Capabilities
  - Insight into State Sponsored Programs
  - Creating Linkage Between Actor Groups
  - Tracking the Supply Chain

Attribution: What are we looking for?

- The obvious – An individual or group of individuals name(s), street address, social networking page etc..
- However..
  - We often don’t care about this..
    - Doesn’t generally help develop countermeasures
    - Attributing to the actor/group level is often enough for profiling efforts

Attribution Continued..

- Attribution at actor group level
  - Differentiation between groups
  - Identification of group geography
  - Indications of sponsorship
    - Nation State (China, Russia or Korea?)
    - Organized Crime (RBN et al?)
    - Activist Group
    - Where worlds collide
      - Code sharing between groups

Conventional Analysis Data Sources

- Static and Runtime Binary Analysis
- Memory Forensics
- Vulnerability Exploitation & Payload Analysis
- Command & Control
- Post-Exploitation Forensics

Analysis Today Continued..

- What Happened?
- How did they get in?
- What did they exploit to get in?
- What was done once on the system?
- Are they still there?
- How can this be prevented in the future?

Automated Analysis Today

- Anti Virus:
  - Known Signature
  - Virus-Like Characteristics

- Sandbox / Runtime Analysis
  - What does the code do?

Analysis Today Continued..

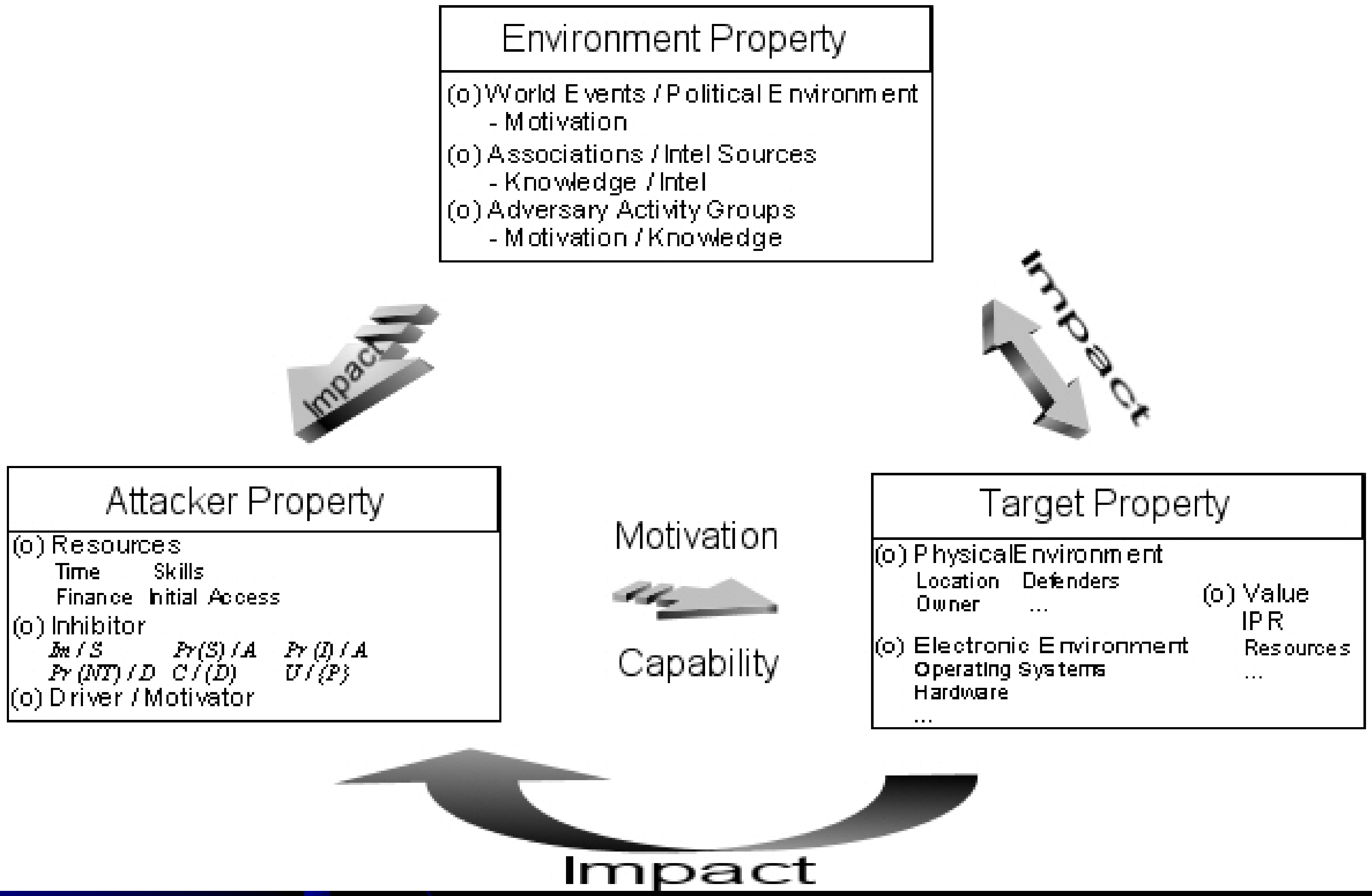
- Lots of R&D Associated with Modern AV/Analysis Technologies.
- Typically Designed to Provide End User with a one or a zero, and no exposure to any shades of grey.
- LOTS of useful metadata processed under the hood that we can make better use of.

Static and Runtime Binary Analysis

- What does the code “do”?
- How does it ensure persistence?
- What changes are made to the system

Attribution Research Intro

- Cyber Adversary Working Group (DC)
- RAND Conference
- Cyber Conflict Studies Association
- Blackhat Briefings (2003, 2004, 2006)
- Auditing the Hacker Mind (Syngress)



Environment Property

(o) World Events / Political Environment
- Motivation

(o) Associations / Intel Sources
- Knowledge / Intel

(o) Adversary Activity Groups
- Motivation / Knowledge

Attacker Property

(o) Resources
Time Skills
Finance Initial Access

(o) Inhibitor
Im / S *Pr(S) / A* *Pr (I) / A*
Pr (NT) / D *C / (D)* *U / (P)*

(o) Driver / Motivator

Target Property

(o) Physical Environment
Location Defenders
Owner ...

(o) Electronic Environment
Operating Systems
Hardware
...

(o) Value
IPR
Resources
...

Attack Inhibitors

- Payoff/Impact Given Success
- Perceived Probability of Success Given an Attempt
- Perceived Probability of Detection Given an Attempt
- Perceived Probability of Attribution Given Detection
- Perceived Consequences of Attribution
- Adversary Uncertainty Given the Attack Parameters

Attack Drivers

- Payoff/Impact Given Success
- Perceived Probability of Success Given an Attempt
- Perceived consequences of failure

Adversary attack fingerprints

- Key Attack Meta Data
  - Attack sources
  - Other Relevant Packet Data
  - Attack tools and their origins
- Attack methodology
  - Planning
  - Execution
  - Follow through

Attack tool meta data: Origins

- All attack tools have their origins..
- These can be put into two broad categories:
  - Public
    - Often simply prove a concept
    - Often not ‘robust’
    - Many contain backdoors
  - Private
    - Frequently more robust than public counterparts
    - Generally better written
    - May be based on private attack API’s

Attack tool meta data: Use

- How easy is it to use a given attack tool
- Prior technical knowledge required to use tool
- Prior target knowledge required to use tool
- Was it an appropriate tool to use for a given task?

Example Attack Scoring Matrix

Web Application Flaws	**Public**	**Private**
Proprietary Application Penetration:		
SQL Injection	3	5
Open Source Application Penetration:		
SQL Injection	3	5
Proprietary Application Penetration:		
Arbitrary Code Injection	2	4
Open Source Application Penetration:		
Arbitrary Code Injection	2	4
Proprietary Application Penetration:		
OS command execution using MSSQL Injection	3	5
Proprietary Application Penetration:		
OS command execution using SyBase SQL Injection	3	5
Proprietary Application Penetration:		
SQL Injection only (MS SQL)	4	6
Proprietary Application Penetration:		
SQL Injection only (IBM DB2)	6	8
Proprietary Application Penetration:		
SQL Injection only (Oracle)	6	8

Furthering the Toolset

- Large Bodies of RE/Analysis Research
  - Almost all geared around traditional IR
  - In most cases; not appropriate for attribution

Application of Current Tool Set To Attribution Doctrine

- Can be possible through..
  - Exploit /Payload Analysis
  - Known Tooling/Markings
    - Normally Requires Manual Effort to Identify
  - Binary Image Meta Data
    - Email Addresses
    - User Names
    - Etc..

Exploit Analysis

- Exploits often re-worked for malware
  - Improved Reliability
  - Specific host type/OS level targeting
  - Possible to automate coloration with knowledge base of public exploits
- ANI Exploit – Re-worked in malware to avoid IPS signatures for previous exploit

Exploit Reliability & Performance

- Crashes & Loose Lips Sink Ships
- Improved Performance
  - Advanced / Improved Shellcode
    - Re-patching Memory
    - Repairing Corrupted Heaps
  - Less Overhead
    - No Large Heap Sprays
    - Or Excessive CPU Overhead
  - Continued Target Process Execution

Exploit Failure

- Where possible – failure may be silent
- Exploit Self Clean-Up:
  - Java hs_err log files
  - System / Application Log files
  - *NIX Core files

Exploit Applicability

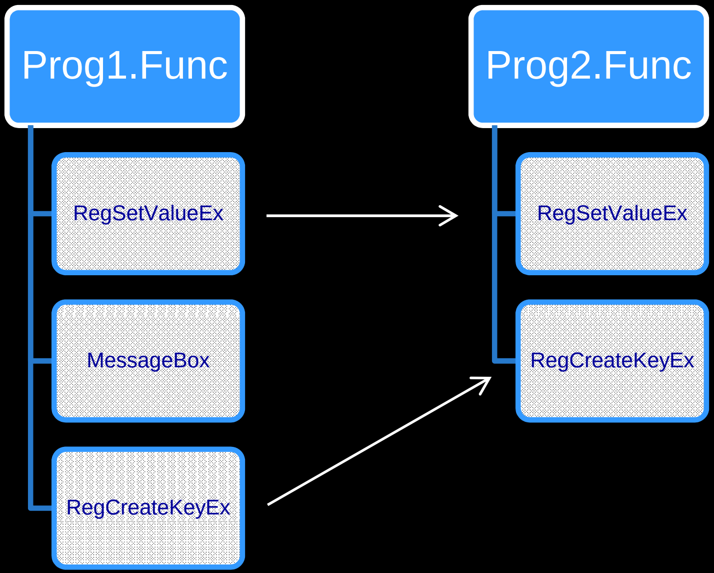
- Reconnaissance Performed
  - Execution based on SW (browser) version?
  - Operating System
    - Less likely to function on ASLR / DEP

Exploit Selection

- Lots of Attention Toward 0day
- 1+Day != Low End Adversary?
- Old Attacks Often Re-Worked
  - Bypass IDS/IPS Signatures
  - Improved Payloads Demonstrate Capability

Code Isomorphism

- Lots of Investment from Anti-Code Theft World
  - Small Prime Product
    - Create Large Prime # Per Function
    - Unique Prime # / Each Opcode
    - Resistant to Reordering
  - API Call Structure Analysis
  - Function Checksums
  - Variables / Constant Tracking



Code Isomorphism Cont..

- Seokwoo Choi, Heewan Park et al
  - **A Static Birthmark of Binary Executables Based on API Call Structure**
- Halvar Flake
  - **BinDiff**

Function Level Code Isomorphism Based Attribution

- Reuse of Code Functions
  - Useful for closed-source projects
  - Good for tracking malware ‘genomes’

- However..
  - Most malware based off of ‘kits’
  - In most cases - doesn't tell us much (or anything) about authors

BlackAxion

- Designed as Proof of Concept
- Utilizes int3 debugger breakpoints
  - Yes – you’re malware can detect me
- XML Model Defines Functions of Interest
  - Identification of API call context
  - Defines weighting of API calls

Further Development..

- DETOURS Hooks
- Kernel Hooks

DEMO / CASE STUDY

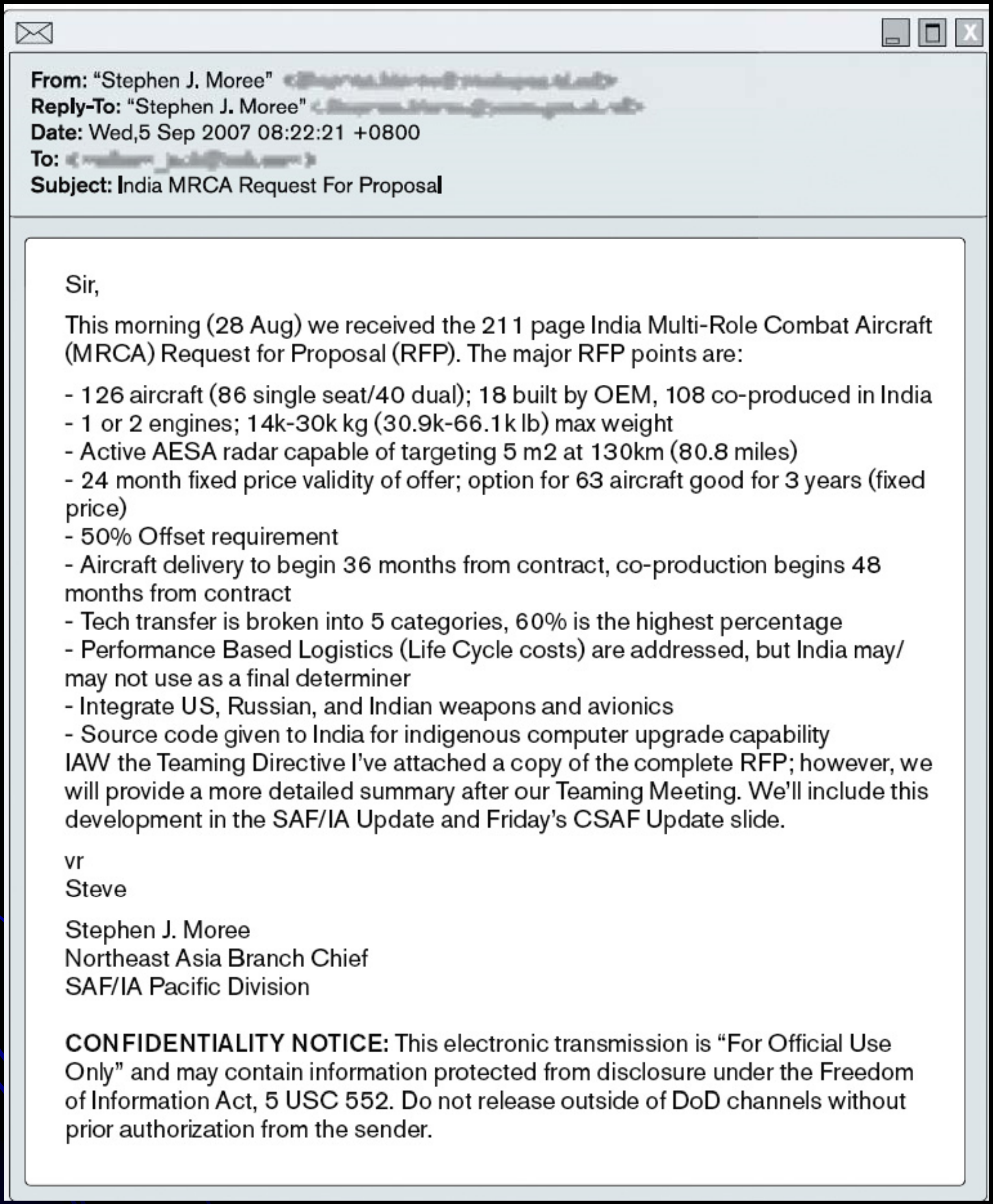
When code analysis #fails

- Other meta data:
  - C&C Channel Hosts Correlation
  - Check-In Server Identification
  - Post-Incident Artifacts
    - Auxiliary Tools / Code Utilized
    - Data Exfiltrated
    - Secondary Targets Attacked

When code analysis #fails

- Meta Data Relationship Analysis Tools
  - Maltego
  - Palantir

- IRC / Chat Forums



From: “Stephen J. Moree” [redacted]
Reply-To: “Stephen J. Moree” [redacted]
Date: Wed,5 Sep 2007 08:22:21 +0800
To: [redacted]
Subject: India MRCA Request For Proposal

Sir,

This morning (28 Aug) we received the 211 page India Multi-Role Combat Aircraft (MRCA) Request for Proposal (RFP). The major RFP points are:

- 126 aircraft (86 single seat/40 dual); 18 built by OEM, 108 co-produced in India
- 1 or 2 engines; 14k-30k kg (30.9k-66.1k lb) max weight
- Active AESA radar capable of targeting 5 m2 at 130km (80.8 miles)
- 24 month fixed price validity of offer; option for 63 aircraft good for 3 years (fixed price)
- 50% Offset requirement
- Aircraft delivery to begin 36 months from contract, co-production begins 48 months from contract
- Tech transfer is broken into 5 categories, 60% is the highest percentage
- Performance Based Logistics (Life Cycle costs) are addressed, but India may/may not use as a final determiner
- Integrate US, Russian, and Indian weapons and avionics
- Source code given to India for indigenous computer upgrade capability

IAW the Teaming Directive I’ve attached a copy of the complete RFP; however, we will provide a more detailed summary after our Teaming Meeting. We’ll include this development in the SAF/IA Update and Friday’s CSAF Update slide.

vr
Steve

Stephen J. Moree
Northeast Asia Branch Chief
SAF/IA Pacific Division

CONFIDENTIALITY NOTICE: This electronic transmission is “For Official Use Only” and may contain information protected from disclosure under the Freedom of Information Act, 5 USC 552. Do not release outside of DoD channels without prior authorization from the sender.

Questions?