Stuxnet Redux: Malware Attribution & Lessons Learned

Blackhat DC 2011

Taking the guesswork
out of cyber attribution

Tom Parker

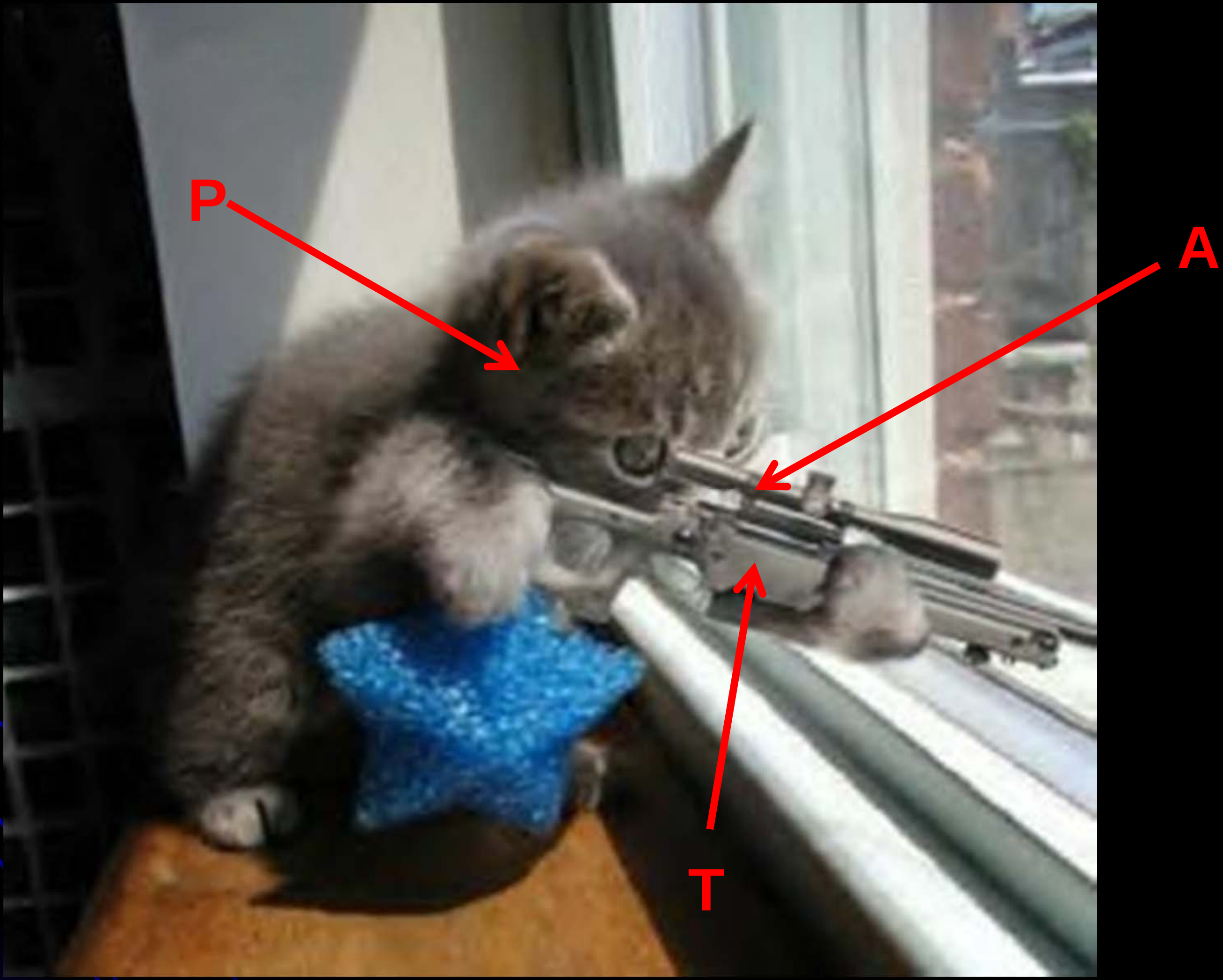
tom.at.rooted.dot.net

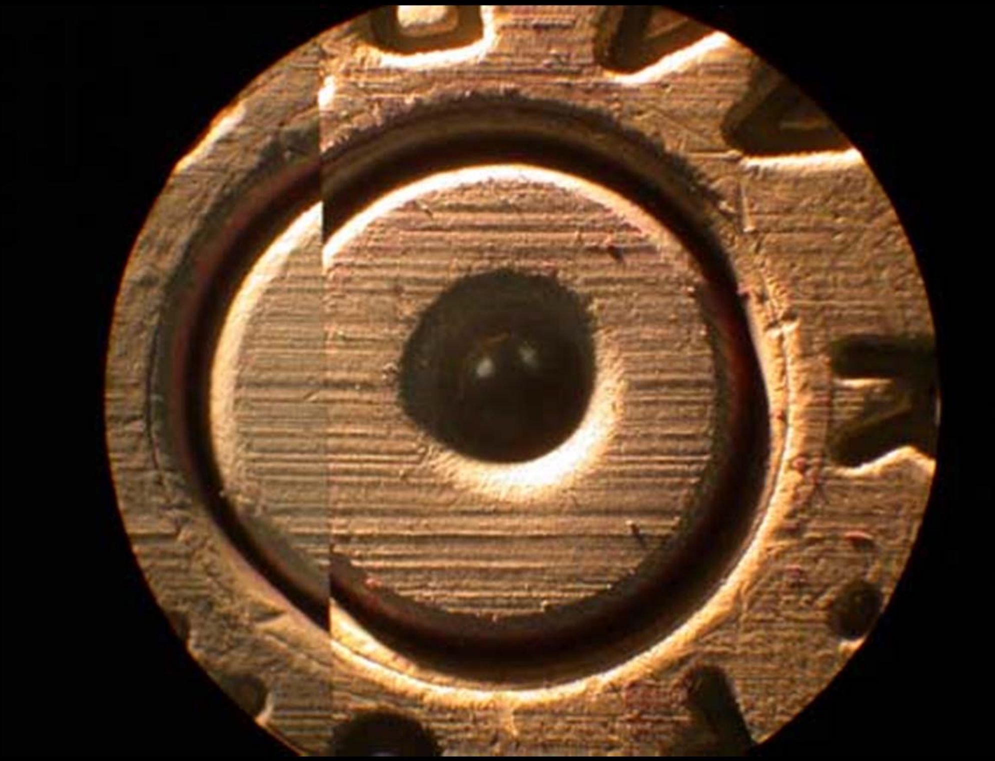
Media & “Cyber War” Love Affair

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

Cyber Conflict Lexicon

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


P
A
T



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
- Differentiating Between Actors
  - State Sponsored or Crimeware?

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

Automated Analysis Today

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

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

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?

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.

Existing Attribution Research

- 2000 RAND Conference
- Numerous CARC working group meetings
- 2004 Syngress Publication
- Focus on:
  - Theoretical attack profiling
    - Who do we have to care about?
  - Post event/forensic approach
    - Forensic actor profile

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
- Clear Need for Reduction in Guesswork
  - Less art, more science
  - Use of Common Attribution Models

Adversary Profiling Today

- Lots of science behind criminal profiling
  - Linguistics & Behavioral Analysis
- Warm Touch

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

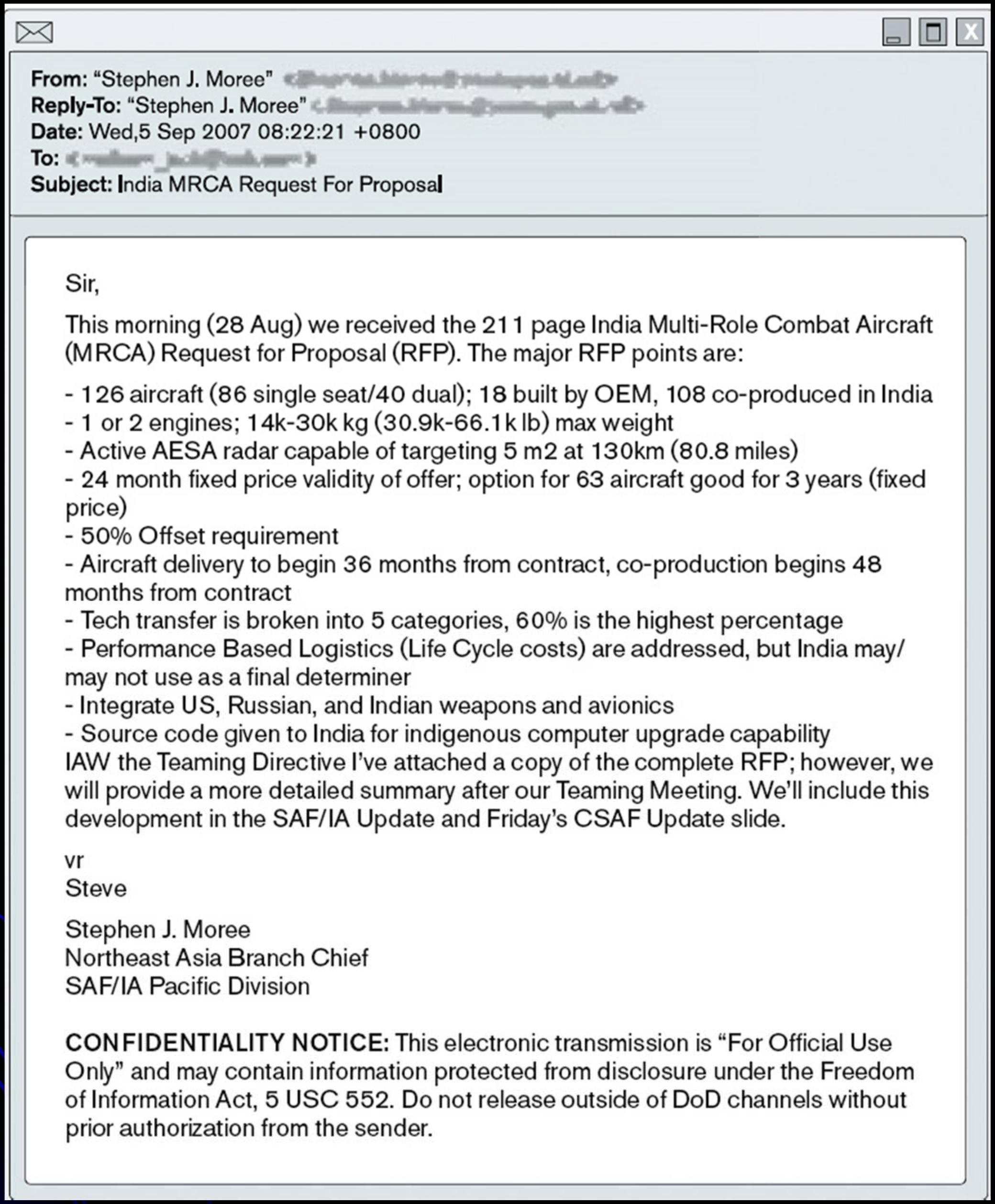
- Where possible – failure may be silent
- Exploit Self Clean-Up:
  - Java hs_err log files
  - System / Application Log files
  - *NIX Core files

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



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.

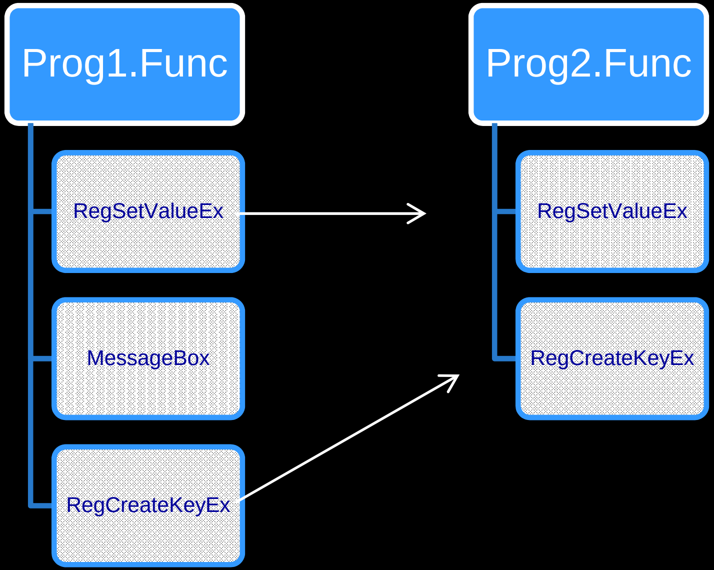
vr
Steve

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.

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 & VxClass**
- Others..

Function Level Code Isomorphism Based Attribution

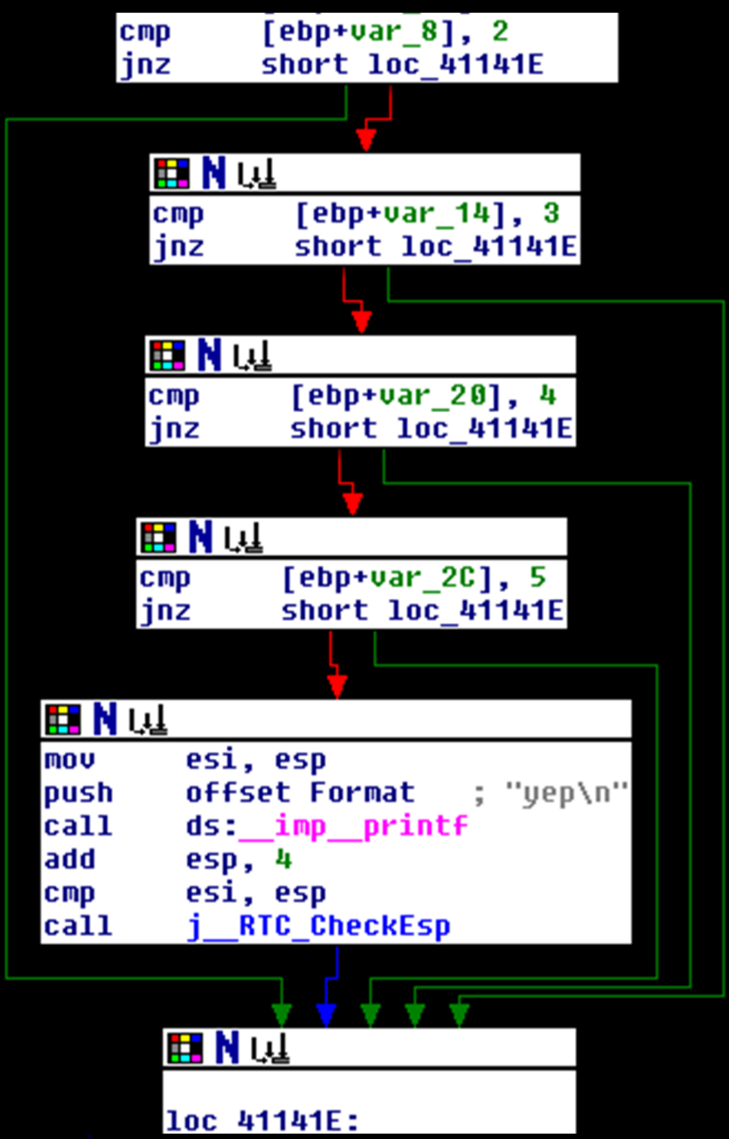
- Reuse of Code Functions
  - Useful for closed-source projects
  - Good for tracking malware ‘genomes’

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

Code Quality

- Nested Statements
  - Compiler Optimization May Interfere
- Unclosed File Handles
- Memory Leaks
- Unused Variables
- Function Redundancy
- Debug Strings Present

Nested Conditionals



```
cmp     [ebp+var_8], 2
jnz     short loc_41141E
```

```
cmp     [ebp+var_14], 3
jnz     short loc_41141E
```

```
cmp     [ebp+var_20], 4
jnz     short loc_41141E
```

```
cmp     [ebp+var_2C], 5
jnz     short loc_41141E
```

```
mov     esi, esp
push    offset Format   ; "yep\n"
call    ds:__imp__printf
add     esp, 4
cmp     esi, esp
call    j__RTC_CheckEsp
```

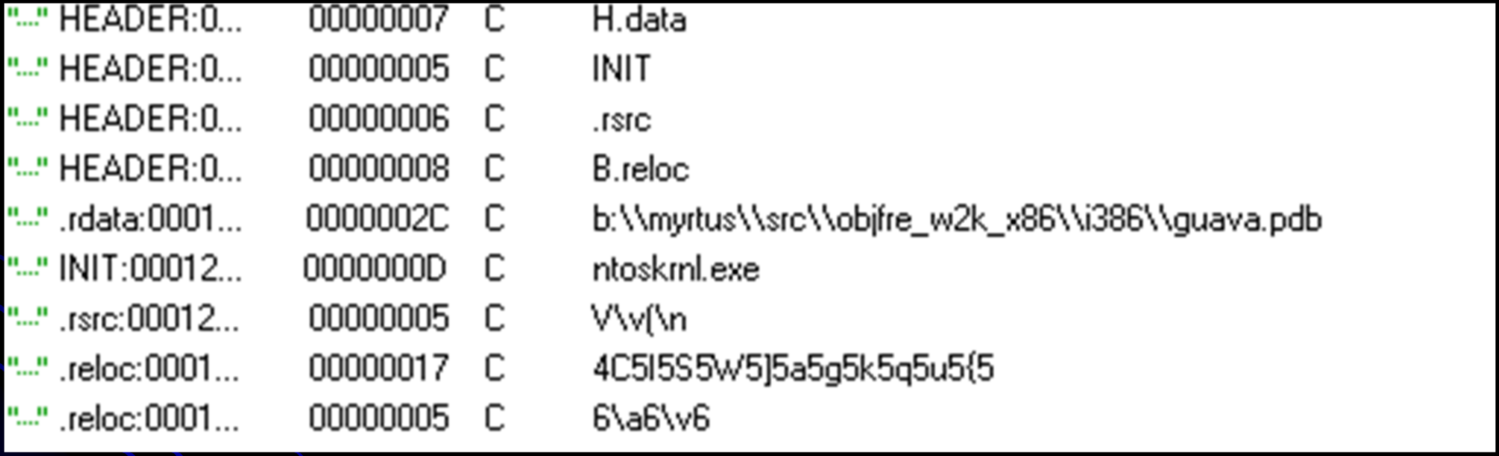
```
loc_41141E:
```

Debug Symbols

- Can indicate developer knowledge
  - Aware of tool markings assoc with compiler
- PDB Locations may provide details of:
  - User Names
  - Operating System (Users VS Docume~1)

Stuxnet PDB References

- Likely Forged
- However…



```
"..." HEADER:0...     00000007   C       H.data
"..." HEADER:0...     00000005   C       INIT
"..." HEADER:0...     00000006   C       .rsrc
"..." HEADER:0...     00000008   C       B.reloc
"..." .rdata:0001...  0000002C   C       b:\\myrtus\\src\\objfre_w2k_x86\\i386\\guava.pdb
"..." INIT:00012...   0000000D   C       ntoskrnl.exe
"..." .rsrc:00012...  00000005   C       V\v(\n
"..." .reloc:0001...  00000017   C       4C5I5S5W5]5a5g5k5q5u5{5
"..." .reloc:0001...  00000005   C       6\a6\v6
```

Stuxnet PDB Contiued

- b:\\myrtus\\src\\objfre_w2k_x86\\i386\\guava.pdb
- Myrtaceae Family:
  - Myrtle
  - Clove
  - Guava ← Stuxnet / mrxnet.sys
  - Feijoa
  - Allspice
  - Eucalyptus

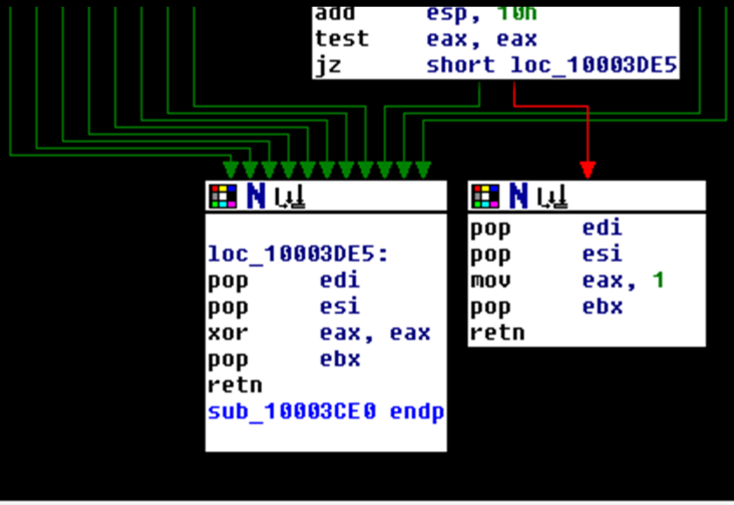
Future Automation

- Automation Vital for Scale
  - Too much badness, not enough analysts
  - Analyst time better spent on edge cases
  - LOTS of repetition in most current efforts; ex:
    - Isomorphic analysis
    - Cataloguing and identification of tool markings

BlackAxon

- Designed as Proof of Concept
- Utilizes int3 debugger breakpoints
  - Yes – you're malware can detect me
- User Sets the Rules
  - No preconceived notion of 'badness'
- XML Model Defines Functions of Interest
  - Identification of API call context
  - Defines weighting of API calls

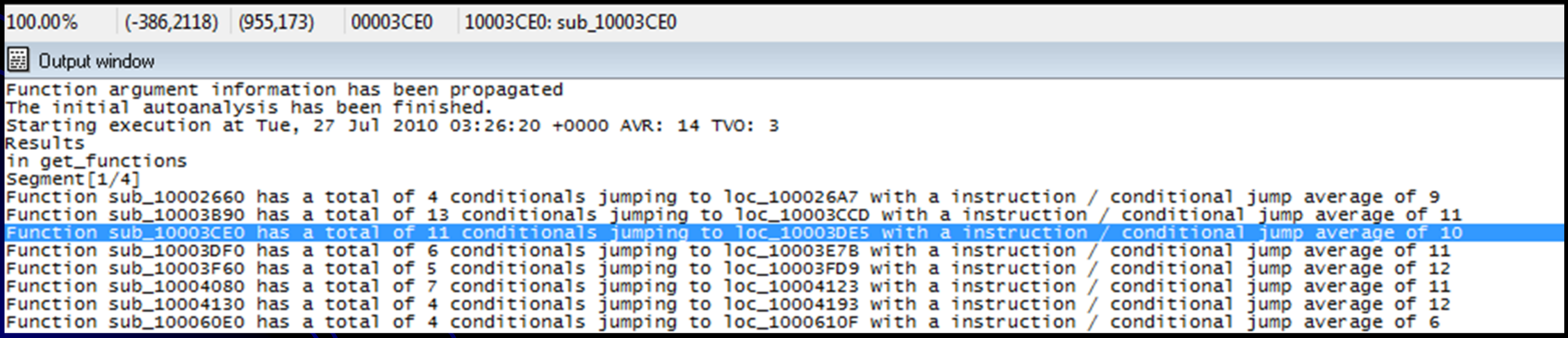
Stuxnet (Dropper) Example



```
add     esp, 10h
test    eax, eax
jz      short loc_10003DE5
```

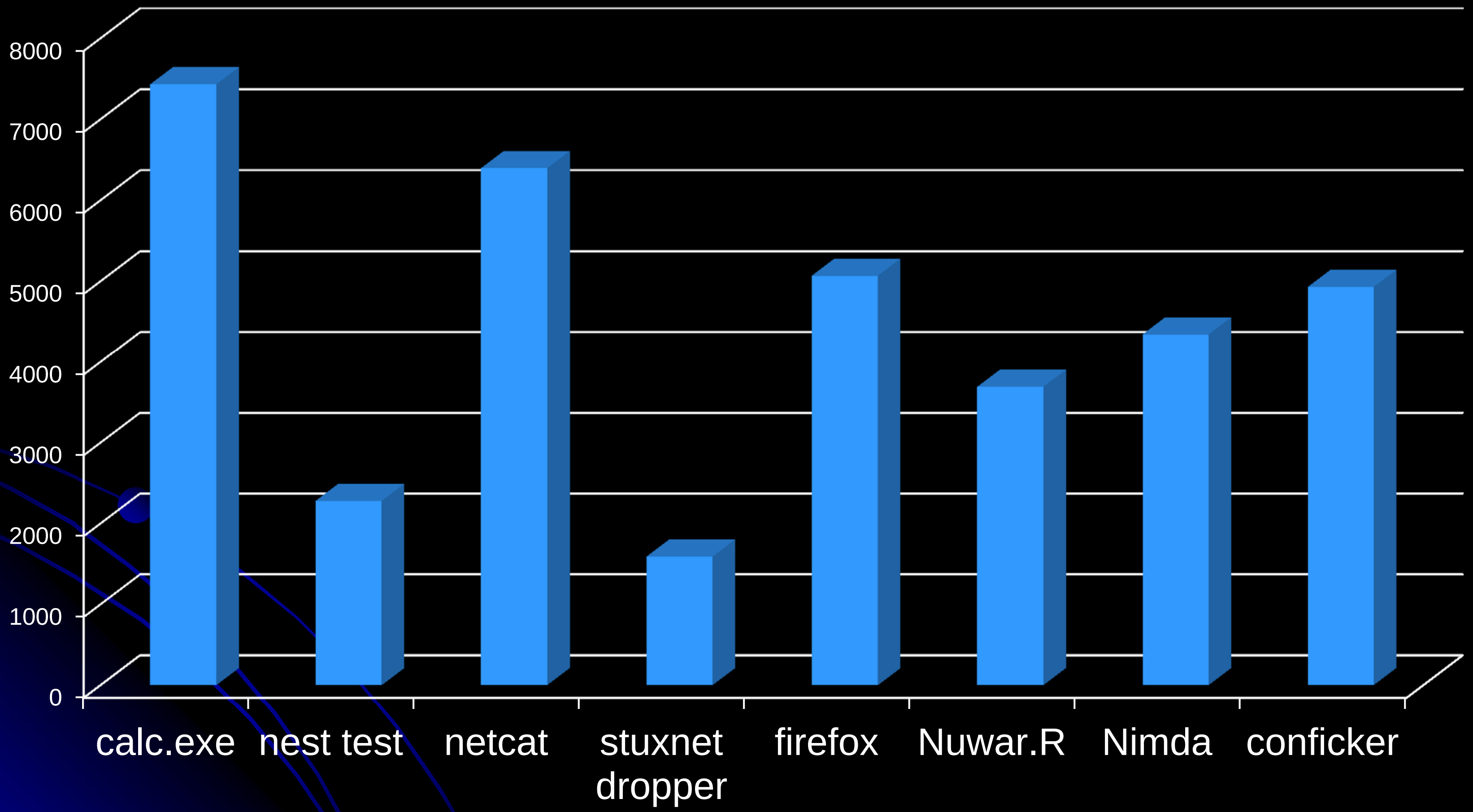
```
loc_10003DE5:
pop     edi
pop     esi
xor     eax, eax
pop     ebx
retn
sub_10003CE0 endp
```

```
pop     edi
pop     esi
mov     eax, 1
pop     ebx
retn
```

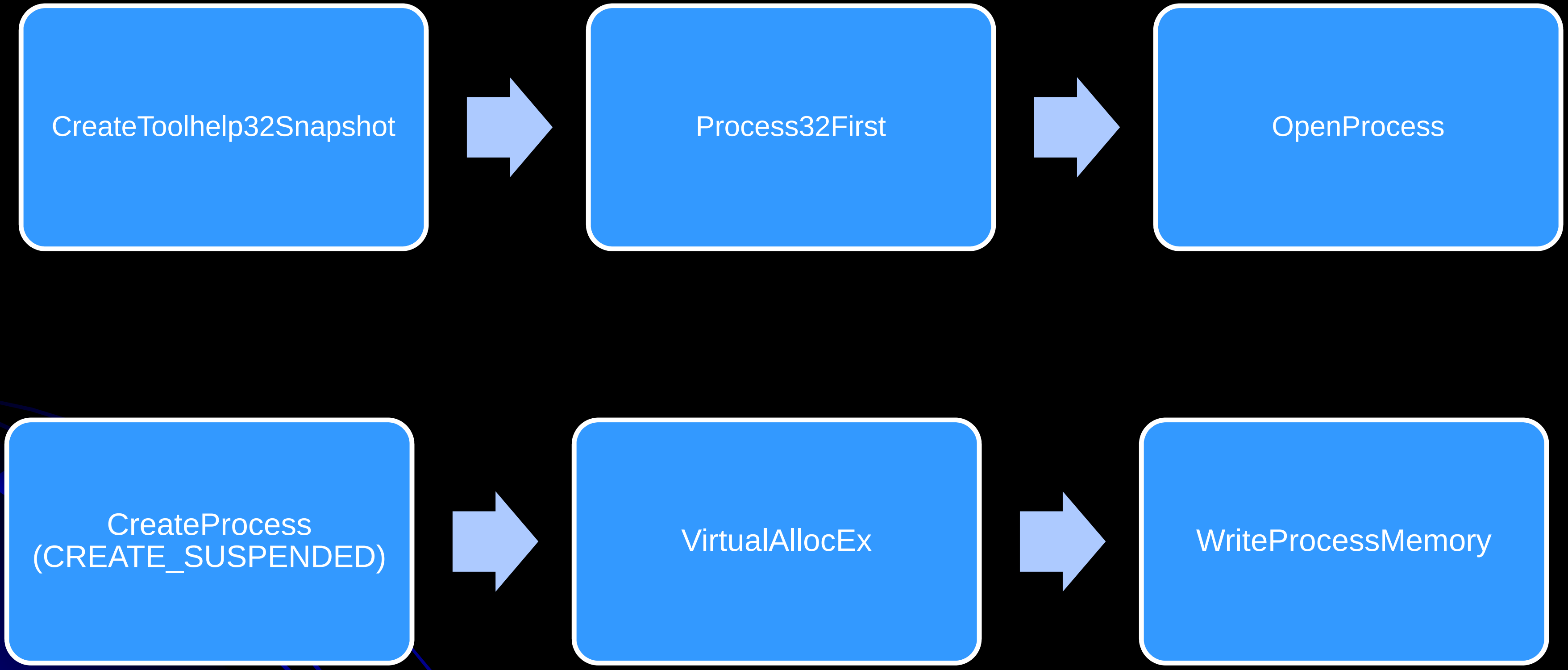


```
Function argument information has been propagated
The initial autoanalysis has been finished.
Starting execution at Tue, 27 Jul 2010 03:26:20 +0000 AVR: 14 TVO: 3
Results
in get_functions
Segment[1/4]
Function sub_10002660 has a total of 4 conditionals jumping to loc_100026A7 with a instruction / conditional jump average of 9
Function sub_10003B90 has a total of 13 conditionals jumping to loc_10003CCD with a instruction / conditional jump average of 11
Function sub_10003CE0 has a total of 11 conditionals jumping to loc_10003DE5 with a instruction / conditional jump average of 10
Function sub_10003DF0 has a total of 6 conditionals jumping to loc_10003E7B with a instruction / conditional jump average of 11
Function sub_10003F60 has a total of 5 conditionals jumping to loc_10003FD9 with a instruction / conditional jump average of 12
Function sub_10004080 has a total of 7 conditionals jumping to loc_10004123 with a instruction / conditional jump average of 11
Function sub_10004130 has a total of 4 conditionals jumping to loc_10004193 with a instruction / conditional jump average of 12
Function sub_100060E0 has a total of 4 conditionals jumping to loc_1000610F with a instruction / conditional jump average of 6
```

Nest Analysis



API Call Hit/Context Tracing: Persistence



CreateToolhelp32Snapshot

Process32First

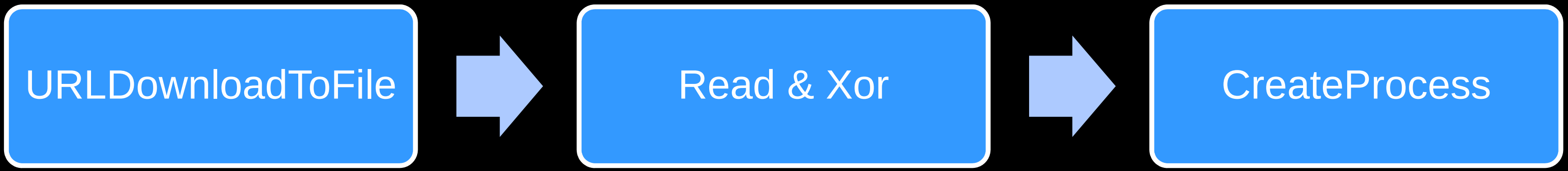
OpenProcess

CreateProcess (CREATE_SUSPENDED)

VirtualAllocEx

WriteProcessMemory

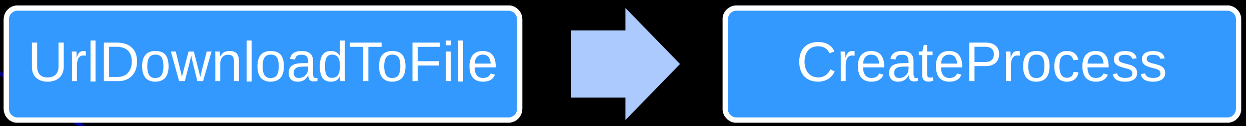
API Call Hit/Context Tracing: Persistence



URLDownloadToFile

Read & Xor

CreateProcess



UrlDownloadToFile

CreateProcess

Further Development..

- DETOURS Hooks
- Kernel Hooks

Digital Evidence Forgery

- Always a Possibility
- Requires Knowledge of ‘What’ to Forge
- Cost of Forgery May Outweigh ROI

When code analysis #fails

- Code Analysis Can be Inconclusive
- Out of Band Data Useful to Support Hypothesis
  - 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

- Some automation available
  - Meta Data Link Analysis:
    - Maltego
    - Palantir
    - Analysts Desktop
- Alternate data sources include..
  - Social Networking / Chat
  - Whois databases
  - Website Archives (archive.org)
  - DNS record archives (dnshistory.org)

Say Nay?

“Budgets will get cut when politicians find out that most of those ‘APT’ attacks are not actually state sponsored”

“Technical analysis useless because of code sharing/reuse”

“Attack analysis tools should only be used by people with a high degree of technical skills”

“Short code segments – there’s only a few ways to achieve certain functionality”

Stuxnet, stuxnet, stuxnet

- Lots of speculation of origins

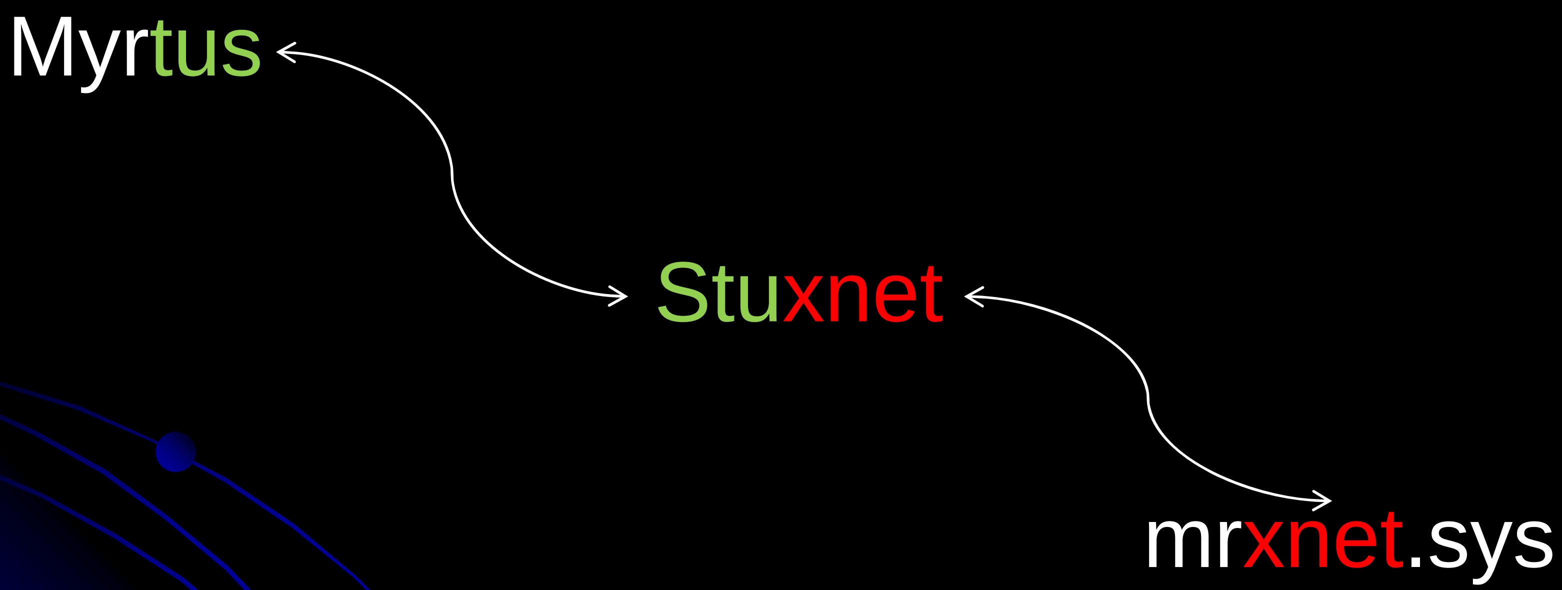
  .. and possible targeting

- Some great analysis performed..
  - Symantec Stuxnet Dossier
  - Langer Communications blog
  - DHS ICS-CERT
  - ISIS Report

Stuxnet Public Disclosures

- June 17th – VirusBlokAda Discovery
- June 24th – VirusBlokAda White Paper
- July 7th – Microsoft Malware Sigs Released
- July 15th – Let the media circus commence!
- July 16th – Microsoft Issue Advisory 2286198
- August 2nd ‘Lnk’ Vulnerability Patched

What the Stux?

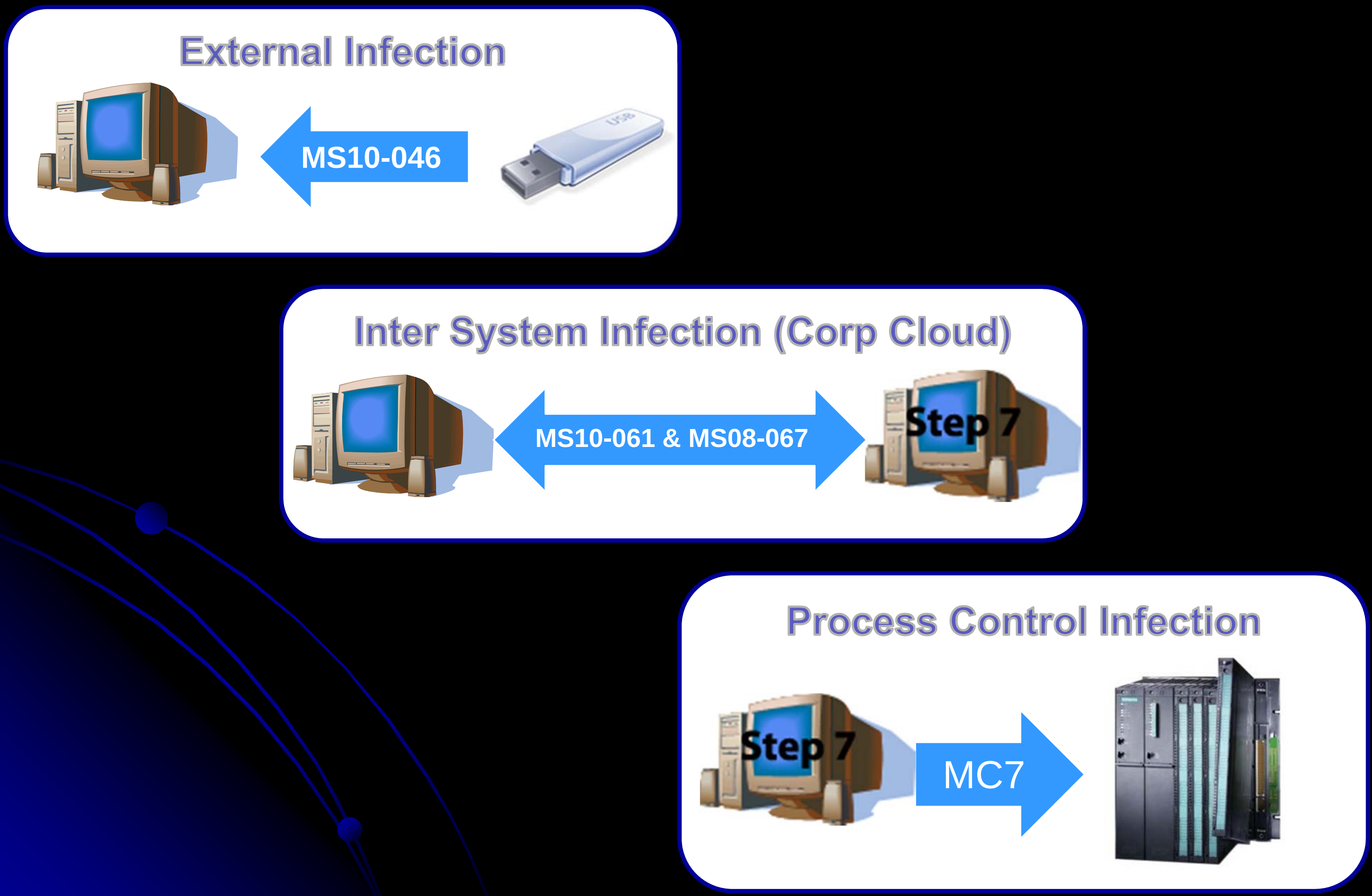


Myrtus

Stuxnet

mrxnet.sys

Stuxnet Infection



External Infection

MS10-046

Inter System Infection (Corp Cloud)

MS10-061 & MS08-067

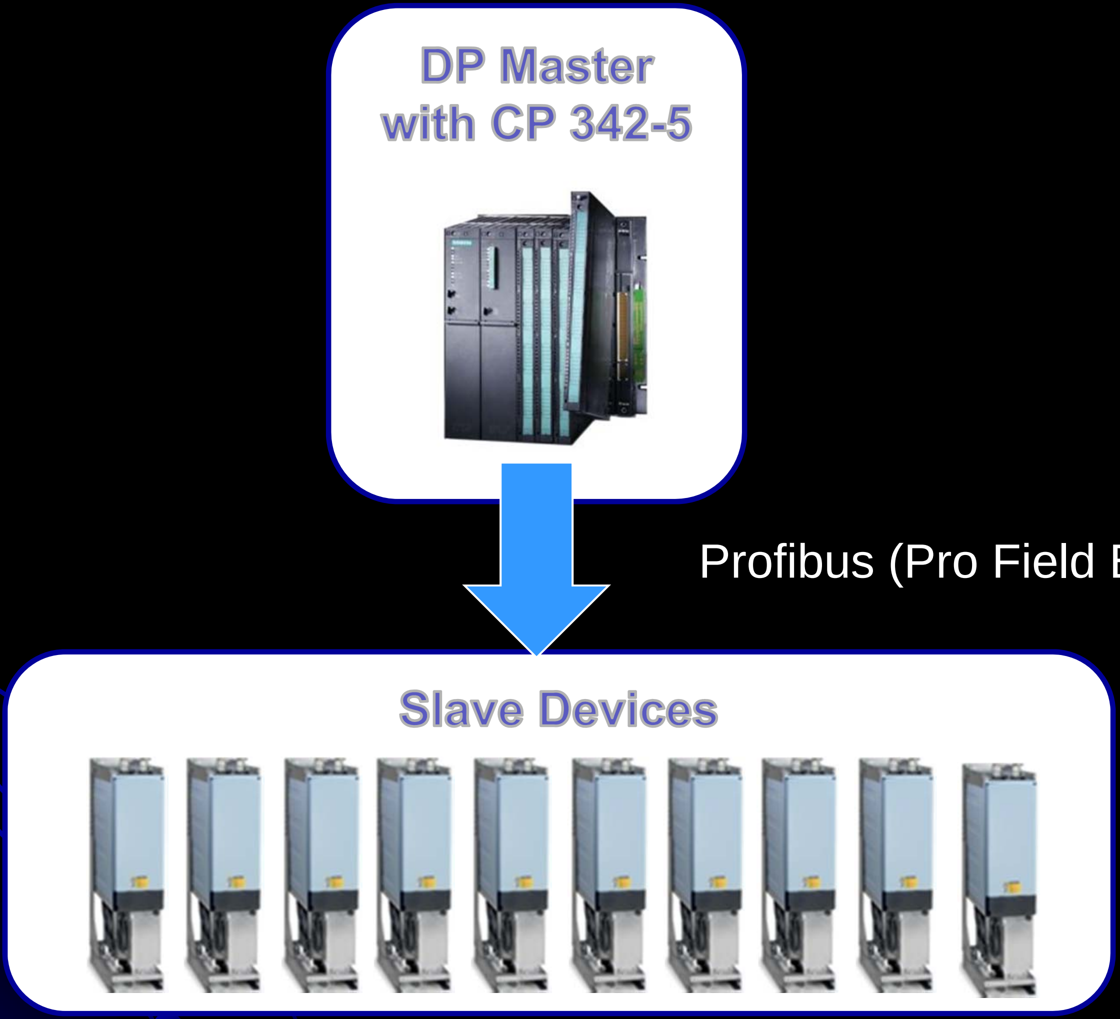
Step 7

Process Control Infection

Step 7

MC7

Stuxnet Infection



DP Master with CP 342-5

Profibus (Pro Field Bus) Comms

Slave Devices

Stuxnet Attribution & Targeting

- Several Popular Targeting Theories:
  - Israel targeting Bushehr Nuclear Plant
  - Israel targeting Natanz Enrichment Facility
- And Attribution
  - Disgruntled Siemens Employee(s)
  - Nation State
  - Organized Crime
  - Lone actor

Developing Stuxnet..

- PLC Programming (MC7 & STL)
- Plant Process Specific Knowledge
- Insider, Target-Specific Knowledge
- Step7 & WinCC Program Suite Internals
  - S7P/TMP/MCP Files
  - Internal Step7 API's
- Windows Kernel/Rootkit Development
- Exploit/shellcode development
- Anti-Virus/Security Product Subversion R&D
- Dropper, C&C & Persistence Components

Resources Required

- Access to hardware & software
  - including frequency converters
  - and probably centrifuges
- Propagation Method
- Stolen Certificates

Stuxnet 0days?

MS10-046 (LNK Vulnerability)	Almost two years old
MS08-067 (Server Service)	Patched for two years
MS10-061 (Print Spooler)	Disclosed over one year ago
MOF ‘Feature’	Not a vulnerability?
WinCC DBMS Password	Original work
Step7 Project Files	Original work
MS10-073 (Kbd Privilege Escalation)	Original work

However…

- Vulnerabilities chosen were
  - Unlikely to fail
    - If they did – failure should not result in a GPF
    - With exception of MS08-067..
  - Comparatively silent in exploitation
  - Creative exploitation (i.e. MOF)

The Dichotomy of Stuxnet

- Costly due to:
  - Maintenance for at least eighteen months and as long as four years
  - R&D invested into R&D PLC Payload, Step7 Subversion & Delivery Framework
- However..
  - Trivial C&C Channel
  - Lots of prior art re-use
  - We’re talking about it right now..

C&C #FAIL?

- Trivial C&C Mechanism
  - More indicative of crime-ware
- Two points of failure for control
  - (Updates a required feature)
- Vulnerable to C&C Hijacking
  - No use of server-side cert validation

Story so far: who was the target?

- Still difficult to say – however:
  - Unlikely to be Power Generation
  - Power Transmission / Distribution Unlikely
  - Oil Cracking & Refining Unlikely

- Likely targets:
  - Manufacturing (incl Chemical Manufacturing)
  - Nuclear Enrichment

Who it was not..

- Disgruntled employee / lone actor
  - Skill requirements preclude work of an individual acting alone
- Western State advanced IO capabilities
  - Too much technical inconsistency
  - Large amount (and risk) of collateral damage
- Greenpeace?

We now know that..

- Stuxnet Targeted Specific Components
  - Almost exclusively utilized in enrichment
- Frequencies referenced indicative of enrichment
  - Specifically 807Hz – 1210 Hz
- Iran was beyond reasonable doubt the target
  - Supported by previous theories
  - and.. IAEA Safeguards & ISIS Report
  - Iran has admitted an impact on operations

Stuxnet Timeline

- September 24th 2007 – Timestamp from MC7
- June 17th 2010 – VirusBlokAda Discovery
- June 24th 2010 – VirusBlokAda White Paper
- July 7th 2010 – Microsoft Malware Sigs Released
- July 15th 2010 – Let the media circus commence!
- July 16th 2010 – Microsoft Issue Advisory 2286198
- July 16th 2010 – Realtek Cert Revoked
- July 17th 2010 – Variant Discovered with J-Micron Cert
- July 22nd 2010 – J-Micron Cert Revoked
- August 2nd 2010 ‘Lnk’ Vulnerability Patched
- September 14th 2010 – Microsoft Patch MS10-061
- October 12th 2010 – Microsoft Patch MS10-073
- November 15th (approx.) – Iran halts Natanz enrichment
- November 23rd 2010 – Statement by Ali Akbar Salehi
- November 29th 2010 – Iran officially admits stuxnet impact

Actor Profile..

- Small(er), technically astute nation state
- Basic IO Capabilities
- Full time staff of operators
- Presently reliant on external assistance
  - Good connections to acquire it..
- Compartmented approach to operations
- Good HUMINT Capabilities
- Access to restricted centrifuge technology

Fail #1 Chinese Theory

- Various theories linking stuxnet to China
    - J-Micron & Realtek Taiwan locations
        - RealTek subsidiary in China
    - Vacon also located in China

Fail #2: Espionage VS Siemens

- Goal: To disrupt deal with Rosatom
- Suspect: Areva

Fail #3: Greenpeace Theory

- Goal: Disrupt NPP / Enrichment Activities
- Suspect: Greenpeace

Scenario #1 – Broken Arrow*

- PLC Components likely to be older than primary assembly (pre-2008)
- Digitally signed rootkit & load point components recyclable
- Technical skills of component developers in excess of operators

- However – highly targeted nature makes this less likely

Scenario #2 – A Joint Effort

- Payload Components Developed Under Contract (Private or Public Partnership)
  - PLC work most likely of western origin
- End-User Developed C&C + Entry Vector
- Repackaged by End-User
- Digital code signature could be either party
- End-User localized access to target site

Stuxnet Countermeasures

- PCN / Corp Network System Co-Mingling
- System Baselines
  - LPD Bug Required Guest Account
  - Unrequired Services on PLC Dev Systems
  - Host Based Firewalls & HIPS
- Default Passwords/Accounts
  - Siemens WinCC SQL DB
  - In the US – a likely violation of NERC CIP

Could Stuxnet have been worse?

- Absolutely..
  - Vastly Improved C&C
  - Greater Propagation Discipline
  - Possible Supply Chain Influence
  - Improved Frequency Converter Targeting
  - PLC OS Rootkit?

Lessons Learned

- Stuxnet should not have been a game changer
  - If it was… you already lost

- Simple countermeasures would have reduced impact
  - Even those mandated in the US by NERC CIP-002 – 009

- Control Systems world is far behind many others
  - Security Assurance
  - Compliance

Closing thoughts..

- Lots still unconfirmed (un-confirmable?)
- Extent of success unknown
  - Likely a set back for end-user/actor
- Just the tip of the iceberg
  - Control systems <u>are</u> vulnerable
  - Investments **<u>are</u>** being made to attack them
- Stuxnet could have been much worse

Questions?