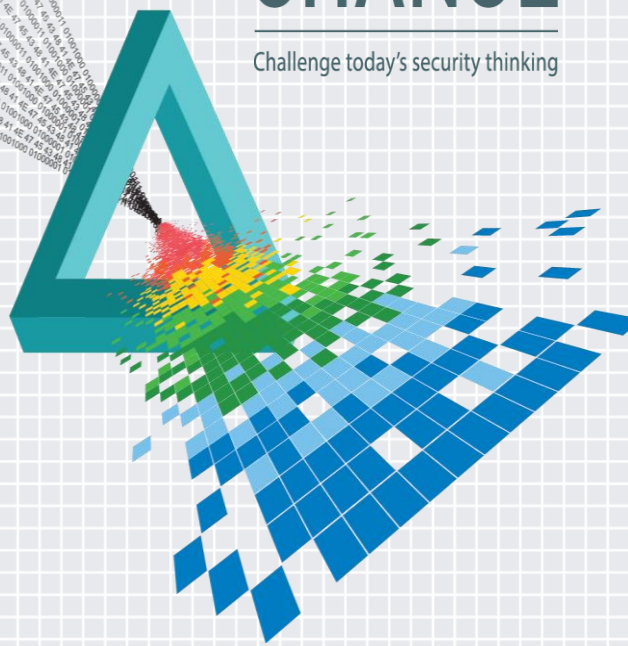
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: ANF-T09

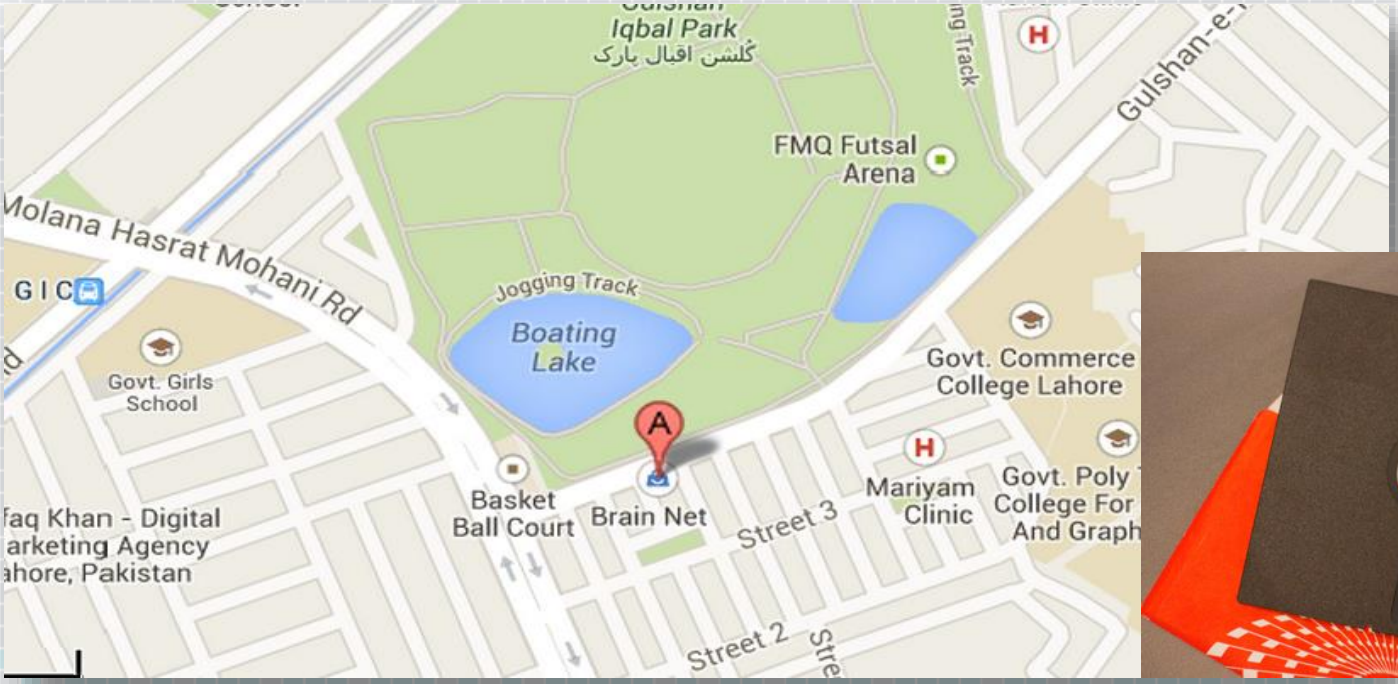
Detecting Unknown Malware: Security Analytics & Memory Forensics

Fahad Ehsan

Cyber Security Researcher

@memfors4all

Where it all Started



Welcome to the Dungeon (c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES 730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN PHONE :430791,44324
Beware of this VIRUS....Contact us for vaccination..... $#@%

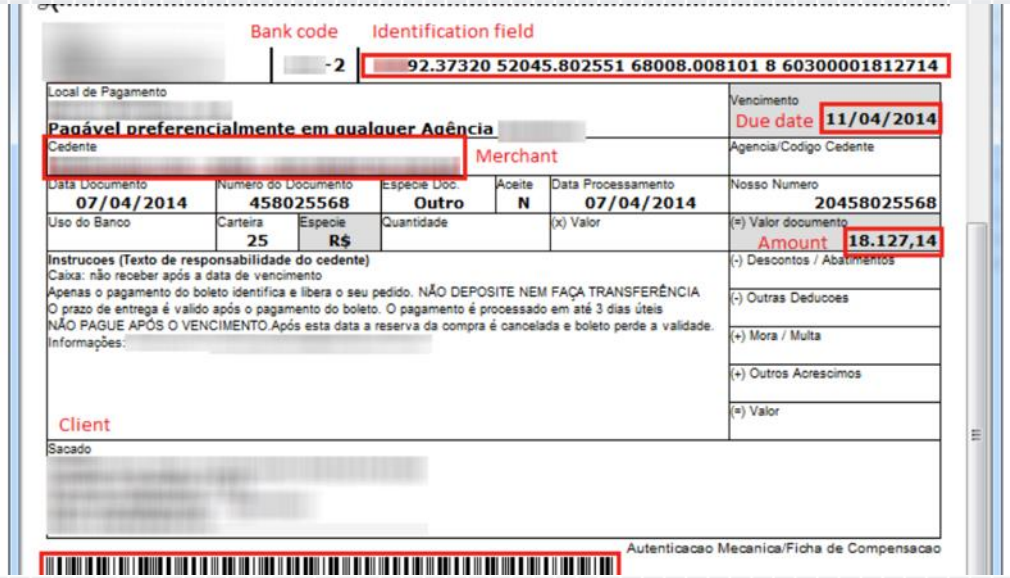
---

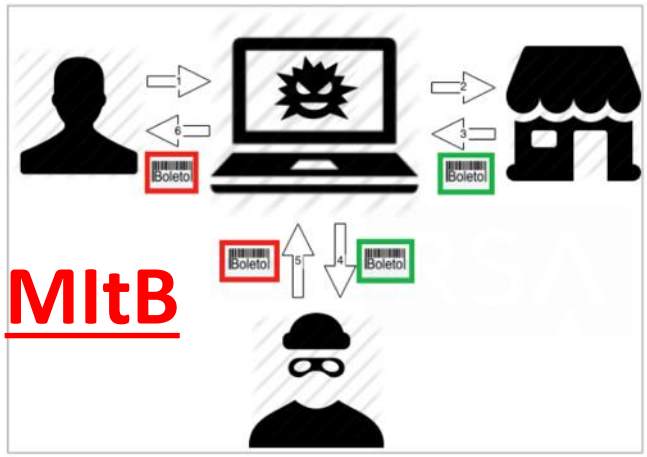
http://campaigns.f-secure.com/brain/virus.html

Bolware .. Boleto Fraud – $3.75 Billion

Country : Brazil (since 2013)
Total Victims: 192,227 (unique IPs)
Browsers : IE, Firefox , Chrome
Method :

- Create Dummy Exe (AvastSvc.exe)
- Code Injection into a legit Process
- Wait for Browser Launch
- Launch Injected code
- Create hooks in system APIs
- Create a copy and Add Registry Key





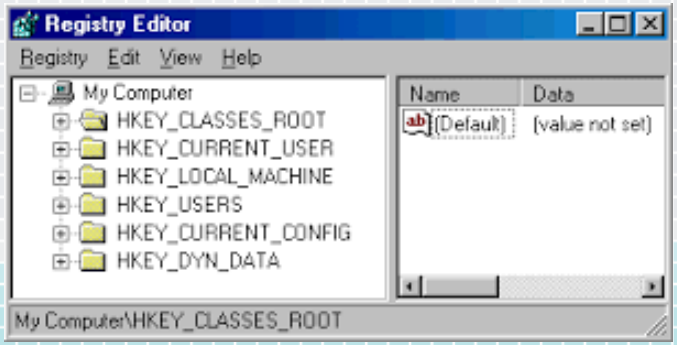
RegKey:
HKCU\Software\Microsoft\Windows\CurrentV
ersion\Run\76e35fb1

RSA

http://www.emc.com/collateral/white-papers/h13282-report-rsa-discovers-boleto-fraud-ring.pdf

Regin : Super Spyware – Nov 2014

- Cyber-espionage tool developed by a nation state. Affects GSM and all major OS.
- Regin takes its name from “IN REGistry”
- Recently detected by Symantec , Kaspersky
  - -Active since 2008
- Modular – Domino Affect
- Thought to be as complex as
- Stuxnet
- Targets found across the world, 14 countries and still counting



https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

2014 : Major Incidents

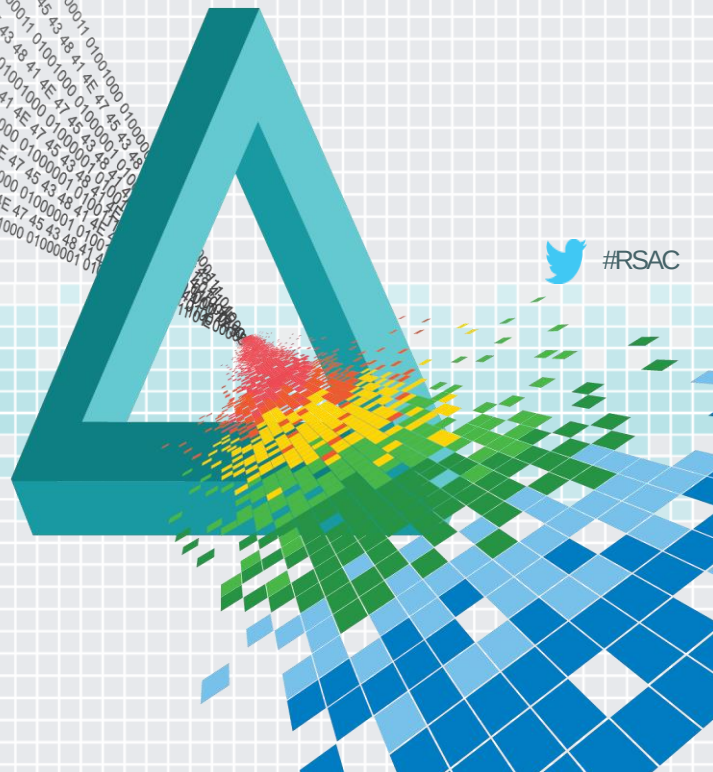
JPMorgan Chase & Co.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Agenda

- Unknown Malware
- Memory Forensics
- IOCs and Threat Intelligence
- Security Analytics
- My Solution
- Q & A



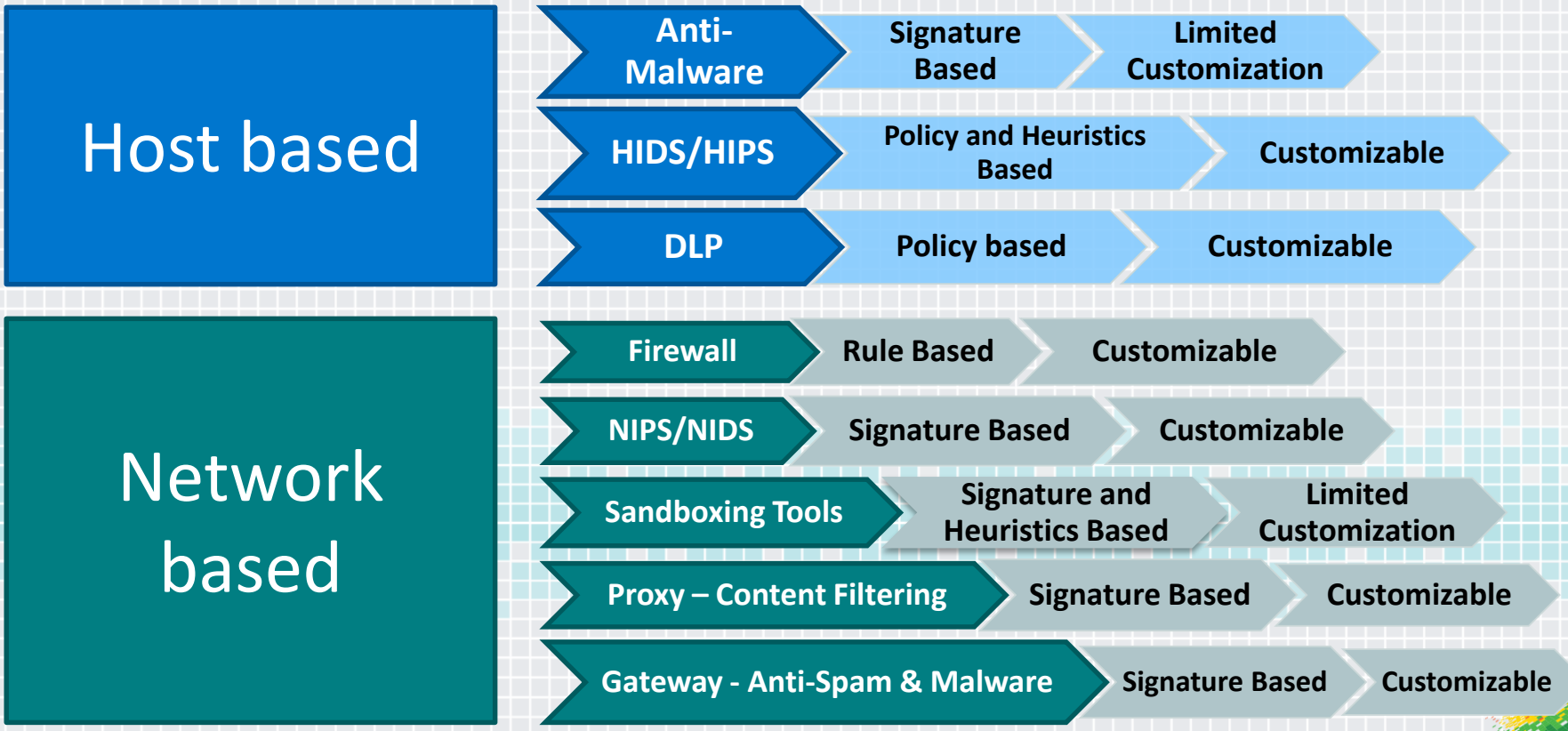
What is 'Unknown Malware'

All Malware is 'Unknown' at some point in its life. Rule and Signature based tools often fail to detect 'Unknown' malware.

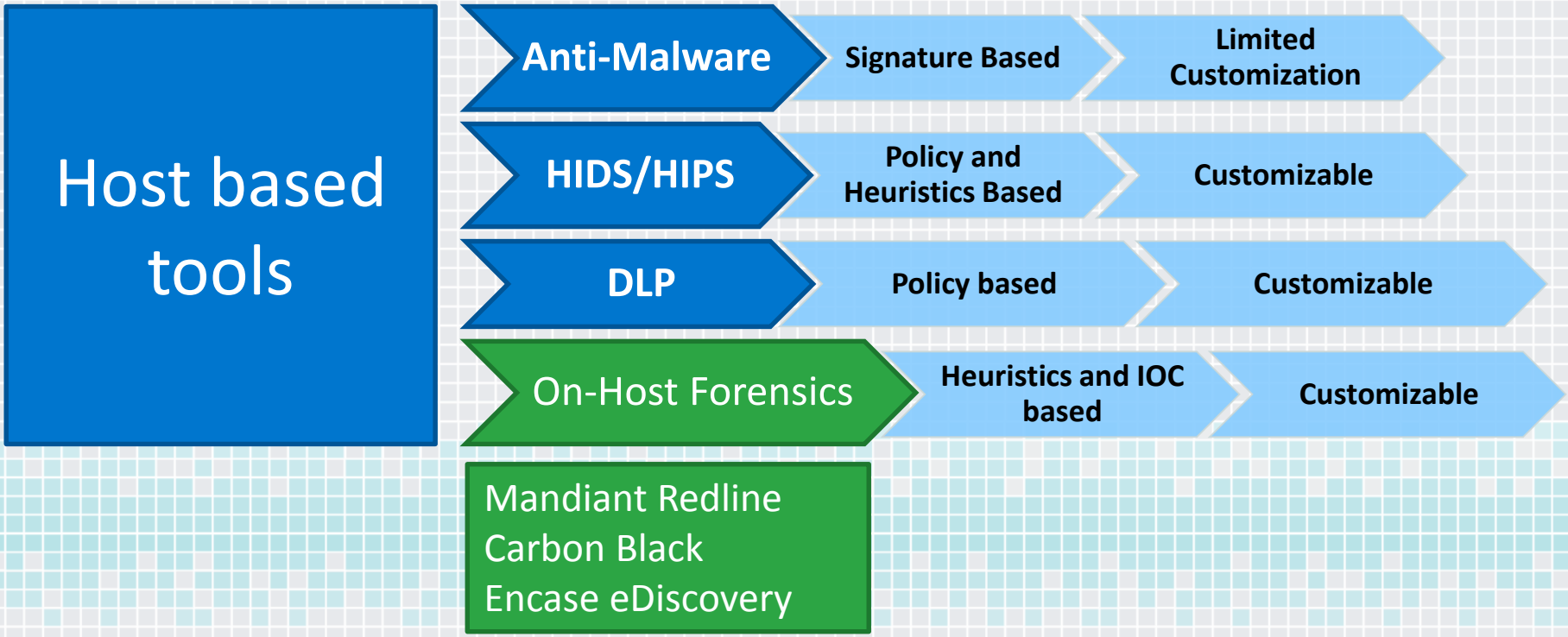
- Any malware that is not detected by traditional and modern security tools at any given time.
- The bottle neck is generally the time taken by the vendors to update the signatures and contents.
- Unknown Malware can target a specific environment, which makes it even more difficult to detect e.g. stuxnet
- 'Unknown Malware' generally target Zero-Vulnerabilities, as there is little protection available against such vulnerabilities.

Common Enterprise Security Tools

Most of the tools found in enterprise today are signature or rule based.



Latest Host Based Tool : On-Host Forensics



Memory Forensics

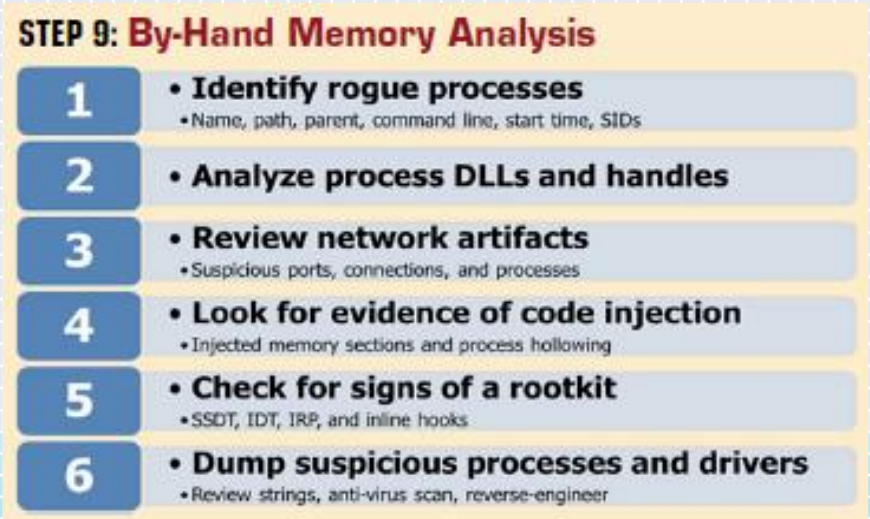
Forensic Analysis of the Memory dump taken from an infected computer. Traditionally, this is done manually with the help of tools.

- Memory dump taken from a live system
- Identify artifacts in memory which can be malicious or stealthy
- Techniques
- In enterprises, generally used for Incident Response
- The findings can be helpful for future investigations
- Build internal repository of known malware and build defenses against them

How Memory Forensic Tools work

In most cases, a successful malware infection leaves a trail of evidence and symptoms in the memory

- Audits and collects running processes , drivers from memory, registry data, tasks, network connections etc
- Analyze data, which is collected from the Memory, this maybe based on heuristics or other techniques
- Perform Indicator of Compromise (IOC) analysis.
- It is any artifact residing in the memory or on the system, e.g. Registry Key, File Hash, Connection, Process, Files

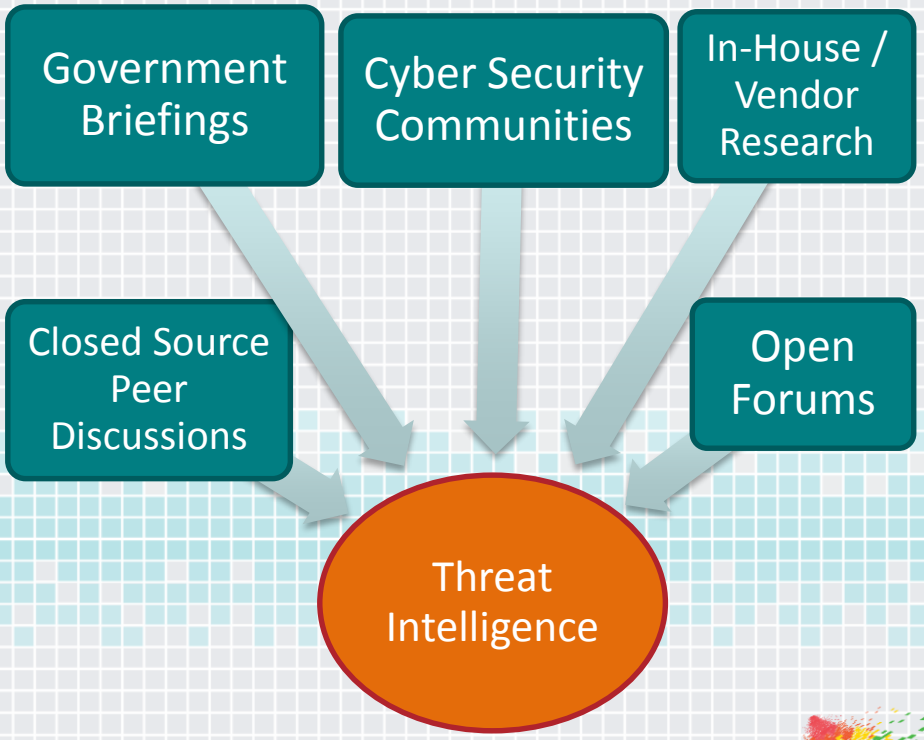


Source : SANS Website

Threat Intelligence

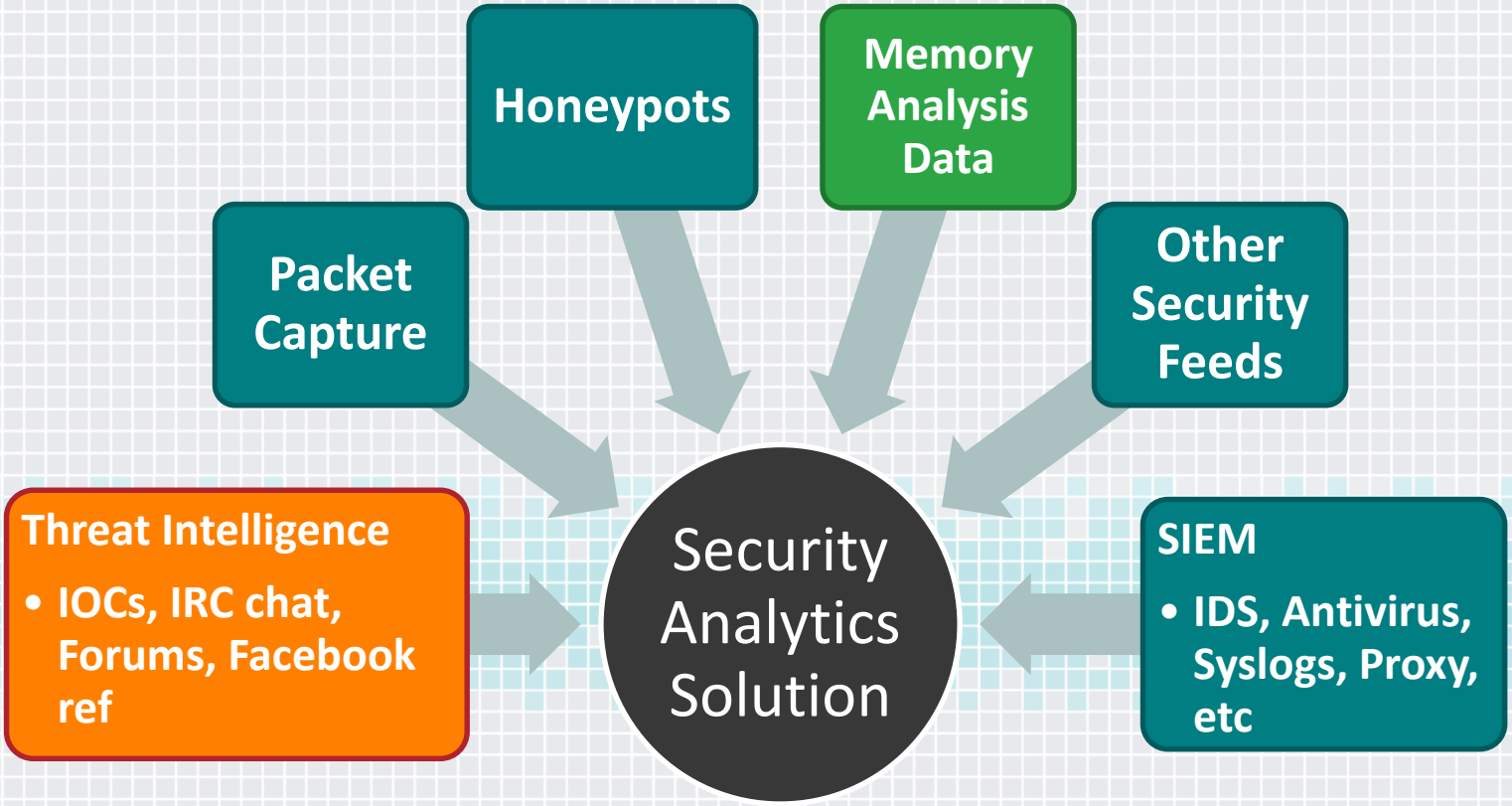
It is a source of information which provides early warnings on emerging threats applicable to your environment.

- TI can be gathered from multiple sources
- Cyber Security Communities e.g. CERTs, Cyber Security Forums, OpenIOC, Cybox
- Government briefings e.g. US-CERT, FBI
- Open Forums e.g. facebook, IRC channels, Websites
- In-House/Vendor Research E.g. Verizon, McAfee etc
- Closed Source Peer Discussions



Using Memory Forensics with Security Analytics

The Security Analytics solution brings information together from multiple sources to detect Malware.



Detecting Known Malware

Both IOCs and Signatures have similar limitations, both require somebody to report. You need something smarter.

IOCs

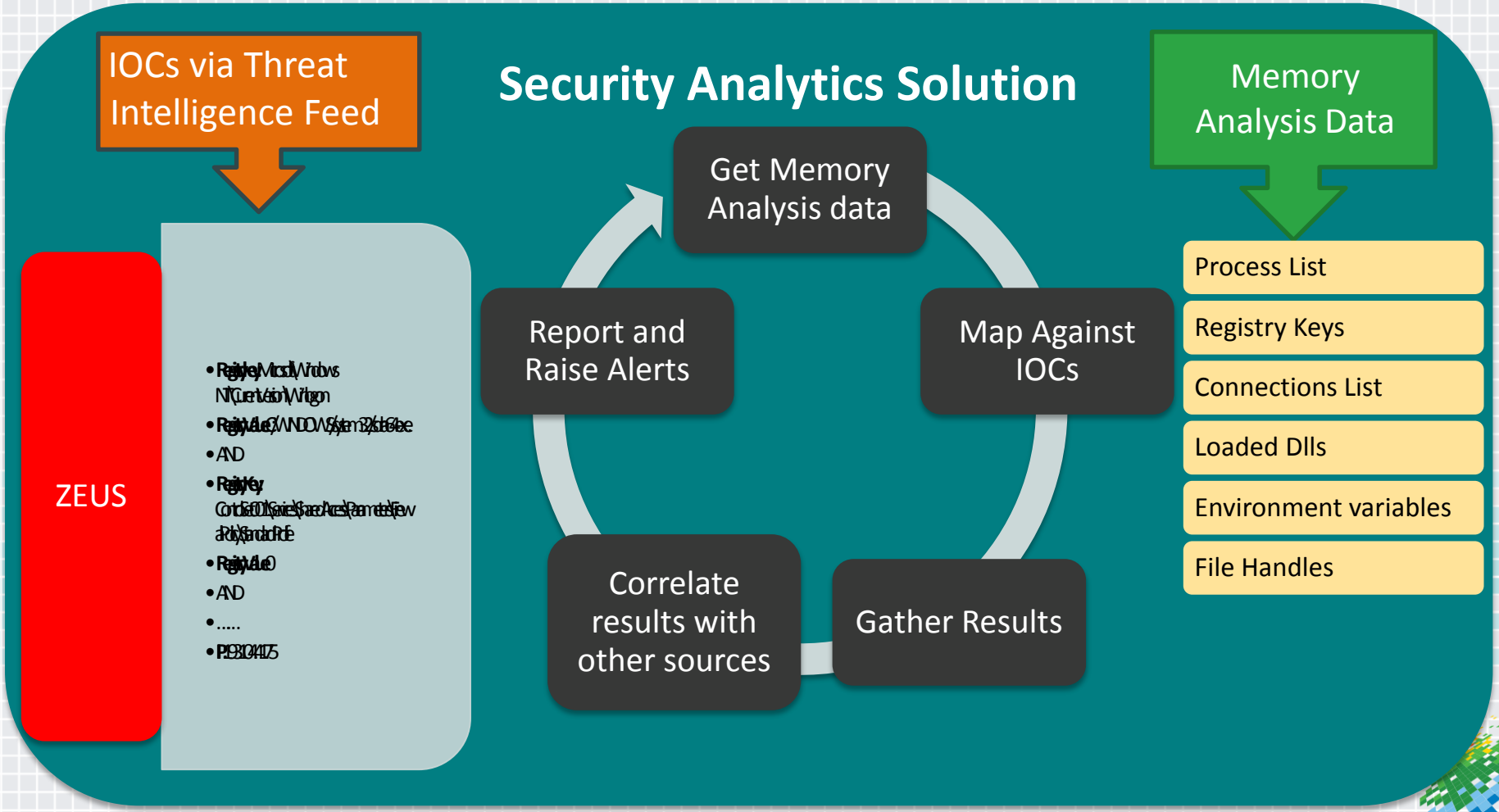
- Open Format
- Low turnaround time
- Can be incomplete / experimental
- May requires internal research
- Can be customized
- Somebody needs to report

Signatures

- Vendor Specific
- Depends on the Vendor
- Independently validated by Vendor
- Environment independent
- Limited Customization
- Somebody needs to report

Detecting Known Malware : ZEUS

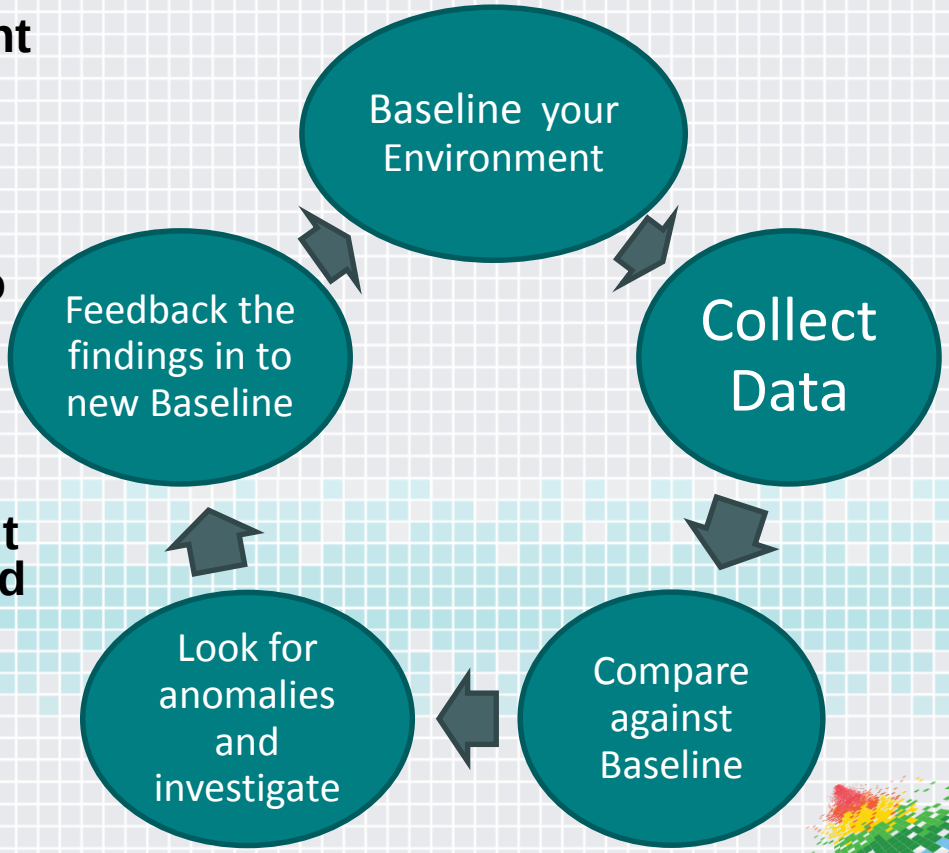
If any of the criteria in the IOC is met, the host is likely to be infected with Zeus.



Understand your Environment

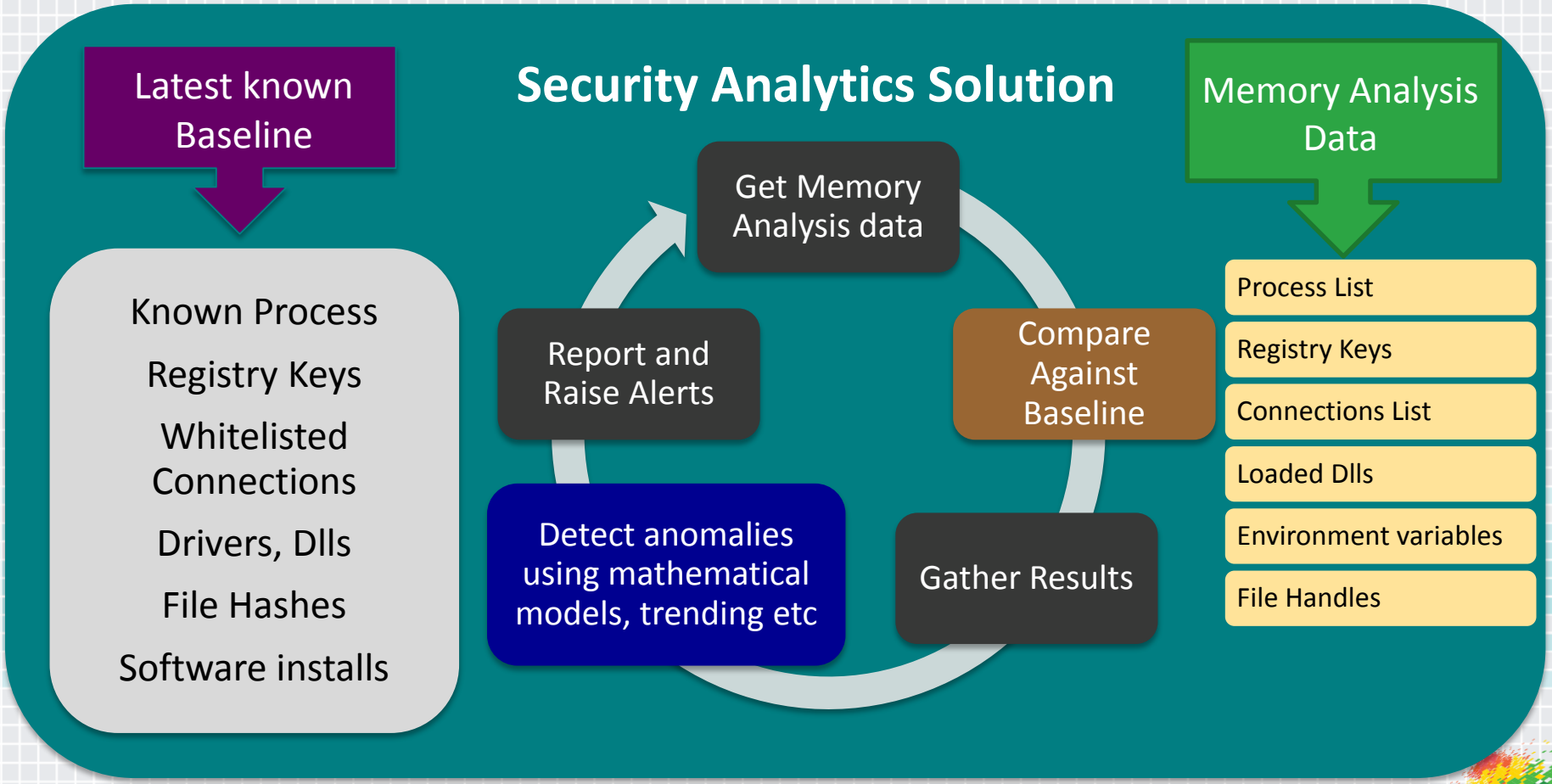
One of the ways to detect 'Unknown' Malware is by baselining your environment

- Compare your current environment with a known old state.
- Statistical analysis of your environment
- Use Security Analytics Solution to do massive historical analysis
- Identify anomalies in your environment
- Build strong research and incident response capabilities to detect and respond to 'Unknown' Malware



Detecting Unknown Malware

Security Analytics can be used to detect anomalies by doing comparisons against last known baseline.



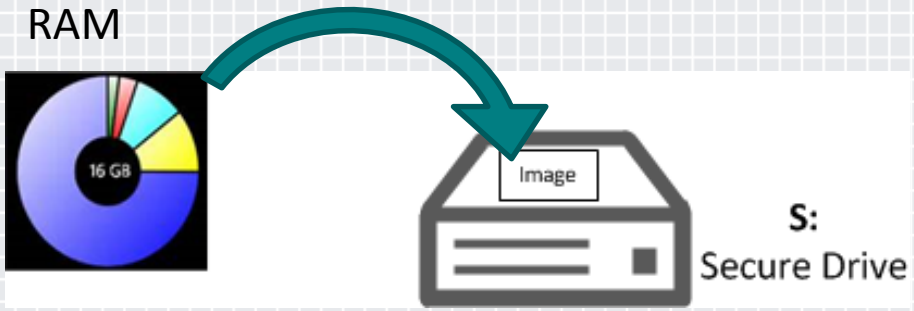
The Solution

- Based on an Open source Toolkit and relatively cheap solutions
- Volatility is a well known open source memory Analysis tool
- Has built in Malware detection capabilities
- Supports Windows, Linux, Android, Mac OS etc
- Can help in capturing Indicators of compromise (IOC) by listing memory contents as text or dumping files
- Items like processes, connections, registry keys etc can be dumped to disk

The Solution

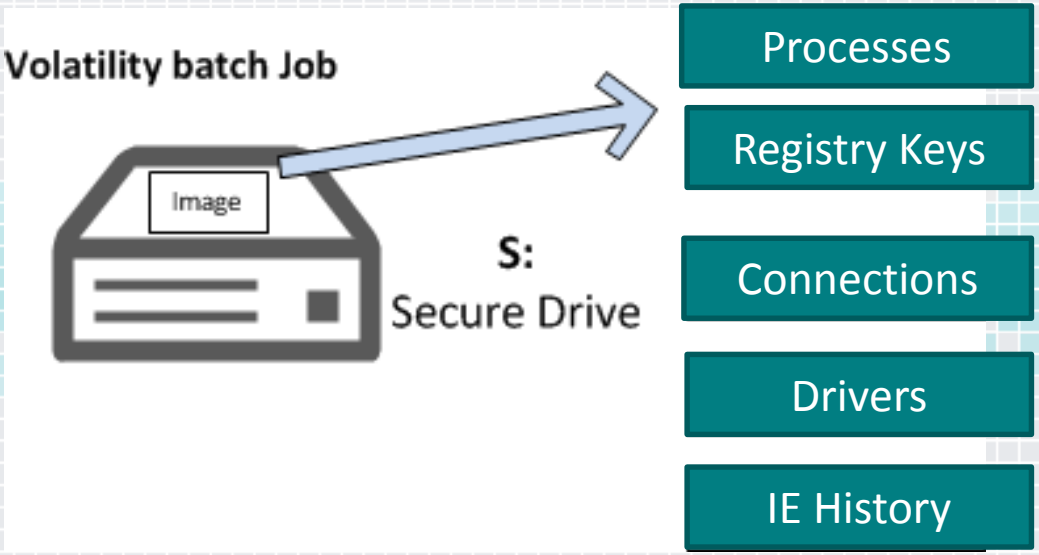
Step 1

Dump memory to a Secure Drive. The Secure Drive is Hidden from the user.



Step 2

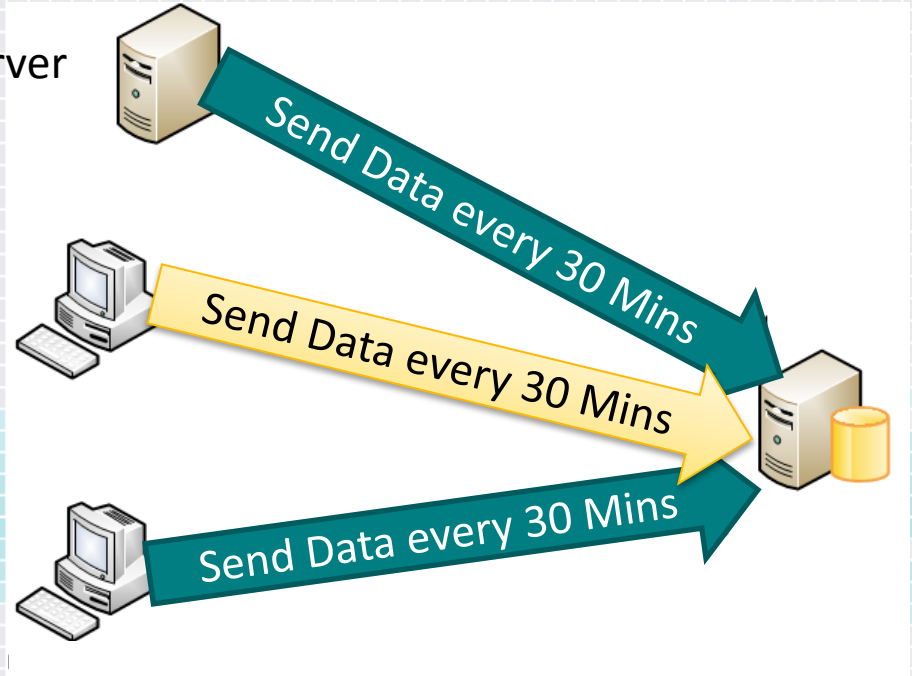
Run Volatility to extract contents of the memory



The Solution

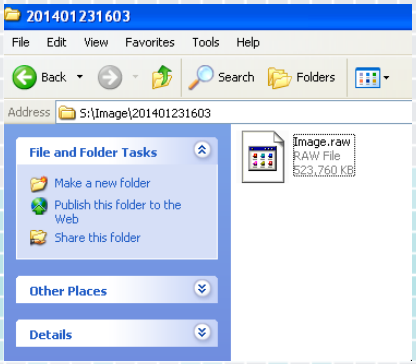
Step 3

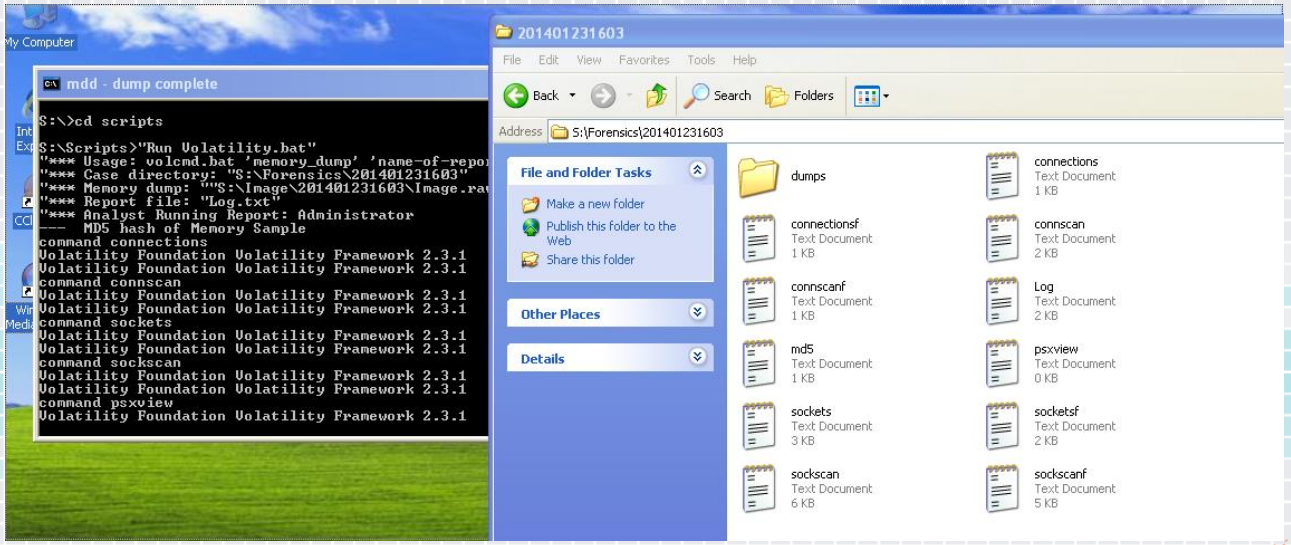
Send data to a central server every 30 mins



Lab Setup

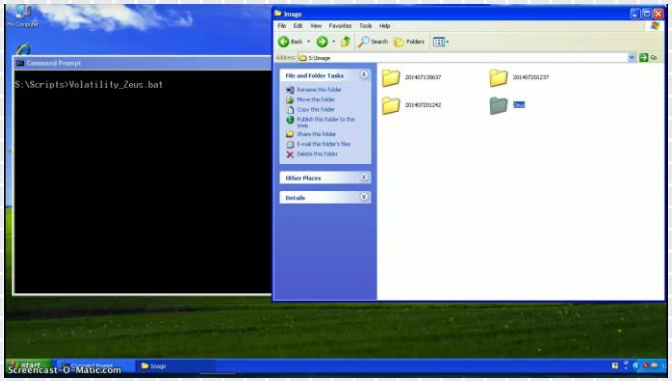
- A Windows XP Client – 1 GB RAM – Running Volatility
- Windows 7 Running SQL Server
- This is our POC Security Analytics Engine
- Sample IOCs loaded in the Security Analytics solution
- The server receives memory analysis data from the Client and processes it





The Demo

- Detect known malware using IOC



- Detecting ‘Unknown’ Malware

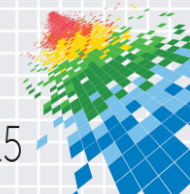
Pros and Cons

Benefits

- Cost
- Provides vital information from clients which may not be available from any other source e.g. registry key, active processes
- Open source tool, which is flexible. The scripts can be changed to suit the environment and scale in the future.
- Can be integrated with external Intelligence feeds to detect emerging threats

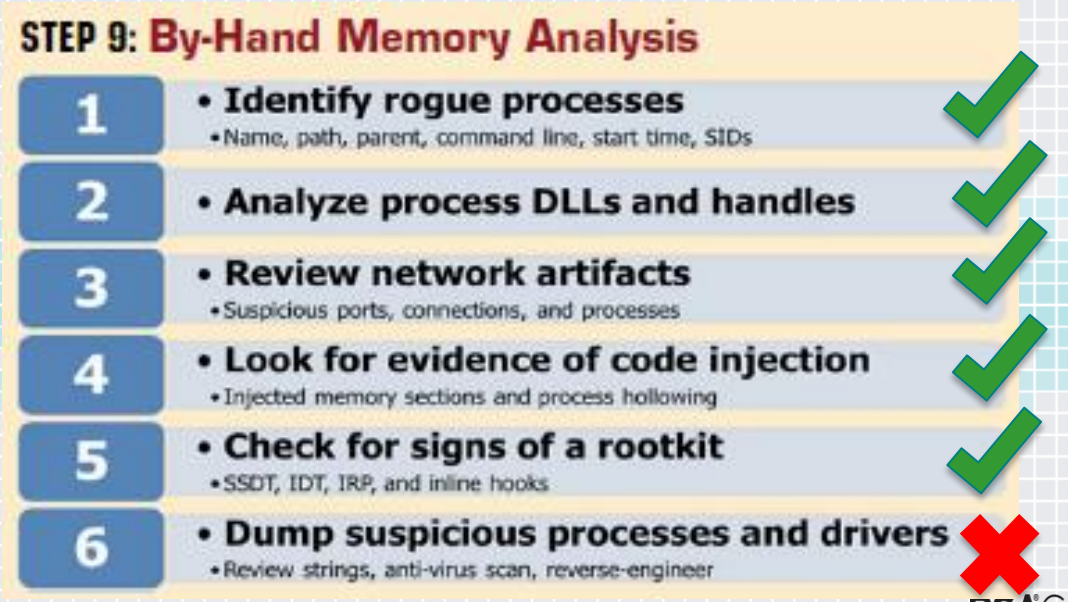
Concerns

- Can be resource intensive, consumes CPU during advanced analysis
- Based on open source tools with limited support
- Data Privacy



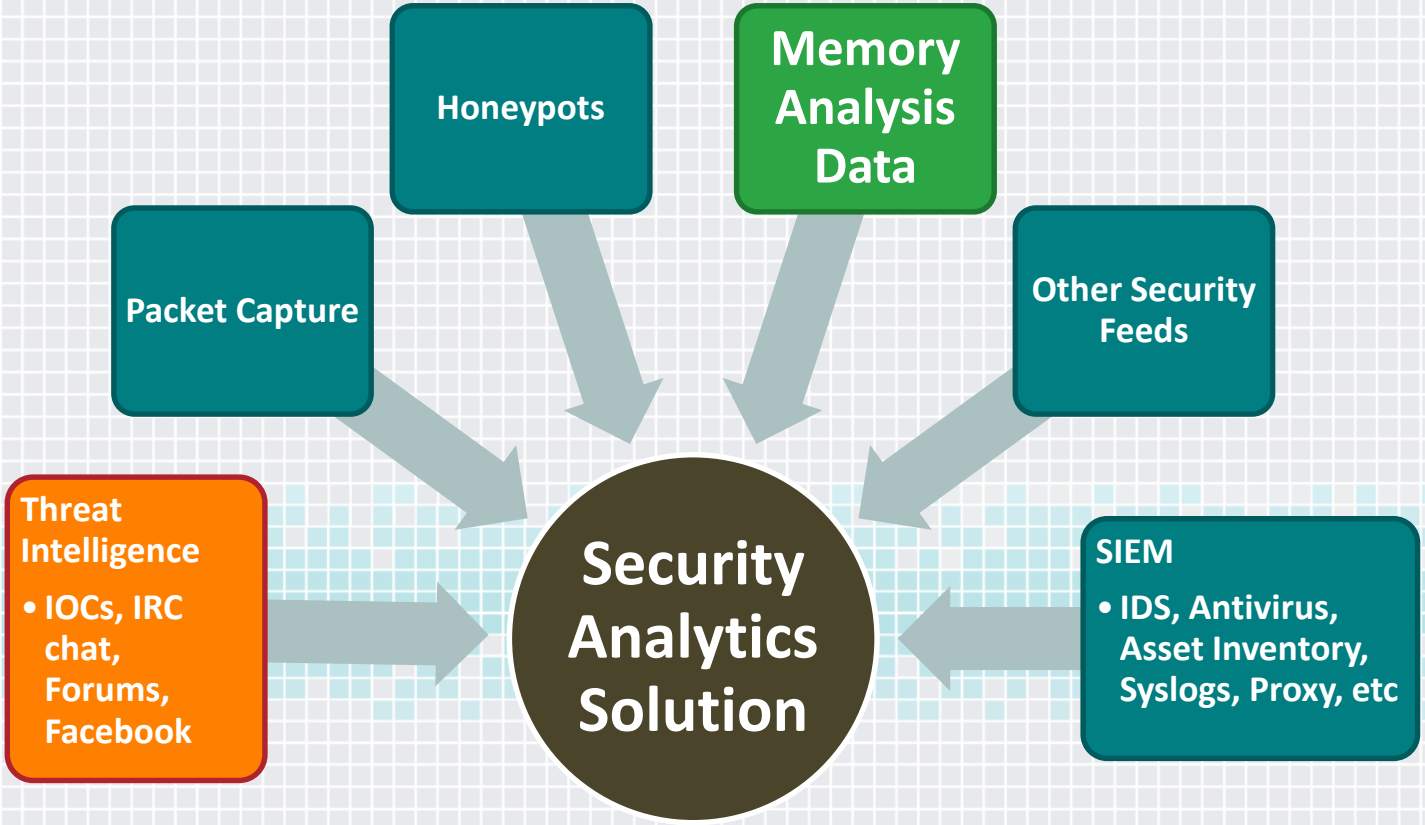
So where do we go from here

- We learned today that a Memory Forensics tool can be developed using open source software
- You can start small and scale as you learn more about your own environment
- You don't need deploy a fancy Analytics solution to get started with finding 'Unknown' Malware



The Big Picture

Memory Forensics is a growing field and it will play a vital role as Security Analytics Solutions mature.

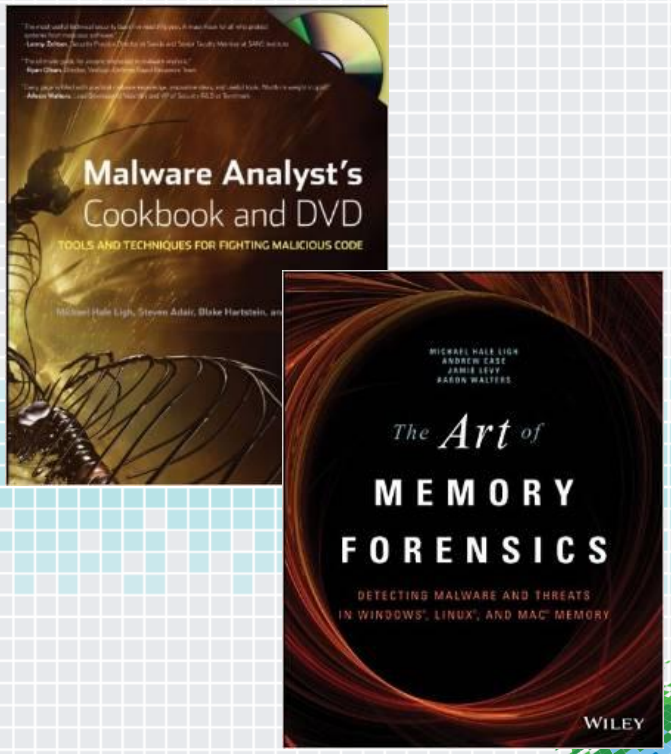


Credits

- Lenny Zeltser – @lennyzeltser
  - http://zeltser.com/
- Jamie Levy – Volatility project
  - http://gleeda.blogspot.se/
- **Malware Analyst's Cookbook**

  by Michael Ligh , Steven Adair , Blake Hartstein, Matthew Richard
- **The Art of Memory Forensics**

  by Michael Ligh , Andrew Case , Jamie Levy , AAron Walters



Thank You

Questions?

Fahad Ehsan

CyberSecurity Researcher

fahade@gmail.com

Twitter : @memfors4all

GitHub Location: https://github.com/MemForsKing/memfors4all