#### RSACONFERENCE 2014 ASIA PACIFIC & JAPAN

Share. Learn. Secure.

Capitalizing on Collective Intelligence

#### Memory Forensics & Security Analytics: Detecting Unknown Malware

SESSION ID: SEC-T09

#### Fahad Ehsan

Associate Director – Security Research and Analytics

**UBS AG** 



### 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...... \$#@%





## Bolware .. Boleto Fraud – \$3.75 Billion

3

#### Country : Brazil (since 2012) Total Victims: 192,227 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 Registry Entry

|   | Ban                          | k code          | Identificati                        | on field                     |   |                                    |
|---|------------------------------|-----------------|-------------------------------------|------------------------------|---|------------------------------------|
|   |                              | -2              | 92.373                              | 20 5204                      | 5.802551 68008.00   | 3101 8 60300001812714              |
| Local de Pagamento Pagamento Pagamento Cedente Merchant |                              |                 |                                     |                              | Vencimento<br>Due date 11/04/2014<br>Agencia/Codigo Cedente |                                    |
| Data Documento  | Numero do                    | Documento       | Especie Doc.                        | Aceite<br>N                  | Data Processamento<br>07/04/2014                            | Nosso Numero<br>20458025568        |
| Uso do Banco  | Carteira<br>25               | Especie<br>R\$  | Quantidade                          |                              | (x) Valor   | (=) Valor documento                |
| 2 prazo de entrega é valid<br>NÃO PAGUE APÓS O VEI      | o apos o paga<br>NCIMENTO Ap | rós esta data a | to. O pagamento<br>a reserva da com | e processad<br>pra é cancela | o em ate 3 días úteis<br>ida e boleto perde a validade.     | (+) Mora / Multa                   |
| Informações:  |                              |                 |                                     |                              |   | (+) Outros Acrescimos              |
| Informações:  |                              |                 |                                     |                              |   | (+) Outros Acrescimos<br>(*) Valor |



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

https://blogs.rsa.com/wp-content/uploads/2015/07/Bolware-Fraud-Ring-RSA-Research-July-2-FINALr2.pdf



#### Agenda

- Unknown Malware
- Memory Forensics
- IOCs and Threat Intelligence

4

**RSACONFERE** 

**ASIA PACIFIC & JAPAN** 

014

- 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' 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

#### STEP 9: By-Hand Memory Analysis



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 In-House / Government **Cyber Security** e.g. CERTs, Cyber Security Vendor **Briefings** Communities Research Forums, OpenIOC, Cybox Government briefings e.g. US-CERT, FBI Closed Open Open Forums e.g. facebook, **Source Peer** Forums IRC channels, Websites Discussions In-House/Vendor Research Threat E.g. Verizon, McAfee etc Intelligence Closed Source Peer Discussions

ASIA PACIFIC & JAPAN

#### Using Memory forensics with Security Analytics

The Security Analytics solution bring information together from multiple sources to detect 'Unknown' Malware.





### **Detecting Known Malware**

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





## **Detecting Known Malware : ZEUS**

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



RSACONFERENCE2014 ASIA PACIFIC & JAPAN

## **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



ASIA PACIFIC & JAPAN

## **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



**DB** and Analytics Server



### 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

| 901401231403  | E3 mild - dump complete   | 🔇 Back + 💿 - 🏂 🔎 Search 🍋 Folders 🔟 -  |   |   |  |
|---|---|--|---|---|--|
| e Edit View Fevorites Tools Help  | S:\Jed scripts<br>EdS:\Seminte\"Bun Helatilitu hat"   | Address 🔁 SilForenece/201401231603   |   |   |  |
| Bod:     Image: residence       Bod:     Image: residence       Stiglingspi(20)400232603       File:     Image: residence       Image: residence | <pre>"""" Usage: volcnd.hat "memory_dump" 'name-of repor<br/>"""" Usage: volcnd.hat "memory_dump" 'name-of repor<br/>"""" Gass directory; "S'Nape-S201402316331mage.ref<br/>""" Report file: "Log.tst<br/>""" Report file: "Log.tst<br/>""" Report file: "Log.tst<br/>"""" Analyze Running Report: Administrator<br/>"""" Analyze Running Report: Administrator<br/>"""" Analyze Running Neport: Administrator<br/>"""" Analyze Running Neport: Administrator<br/>"""" Analyze Running Neport: Administrator<br/>"""" Analyze Running Neport: Administrator<br/>""""" Analyze Running Neport: Administrator<br/>""""" Analyze Running Neport: Administrator<br/>""""" Analyze Running Neport: Administrator<br/>"""""" Analyze Running Neport: Administrator<br/>""""""""""""""""""""""""""""""""""""</pre> | File and Folder Tasks     8       Make a new folder     9       Publish this folder     9       Web     9       Share this folder     9       Other Places     8 | dunps<br>connections <sup>4</sup><br>Text Document<br>1 KB<br>connections <sup>4</sup><br>Text Document<br>1 KB | Connections<br>Text Document<br>1 KB<br>Connection<br>Text Document<br>2 KB<br>Connection<br>2 KB |  |
| Other Places 8  | Volatilitý Foundation Volatilitý Franework 2.3.1<br>command sochscan<br>Volatility Foundation Volatility Franework 2.3.1<br>Volatility Foundation Volatility Franework 2.3.1<br>command proview<br>Volatility Foundation Volatility Franework 2.3.1   | Details (8)  | mdS<br>Text Document<br>1 KB<br>societs   | Text Document.  |  |
| Details   |   |  | sodiscan<br>Tech Decument   | The Desarrent<br>2/5<br>Sodscarf<br>Text Desarrent<br>5/16  |  |



### **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



## So where do we go from here

- We learned today that a Memory Forensics tool can be developed using open source software
- We can automate many of the steps involved in Memory Forensics
- You don't need a fancy Analytics solution to get started with finding 'Unknown' Malware

#### STEP 9: By-Hand Memory Analysis Identify rogue processes 1 . Name, path, parent, command line, start time, SIDs 2 Analyze process DLLs and handles Review network artifacts 3 · Suspicious ports, connections, and processes Look for evidence of code injection 4 · Injected memory sections and process hollowing Check for signs of a rootkit 5 . SSDT, IDT, IRP, and inline hooks Dump suspicious processes and drivers 6 · Review strings, anti-virus scan, reverse-engineer



### **The Big Picture**

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









#### RSACONFERENCE 2014 ASIA PACIFIC & JAPAN



#### **Thank You**

