Medico
Governmental
Case
The Speaker
Mohamed Abdelghani

- Digital forensics expert at EG-CERT
- 10+ year of experience in the field of information security.
- ENCE, ACE, eRCE, CFCE.
Agenda

- About Medico
- Medico case
- Incident Response
- Data Acquisition
- Initial Access
- Discovery
- Persistence
- Memory Analysis
- Attack Vector
- Lesson Learned
About Medico
Facts

- Medico funding.
- How it raise money.
- Great scattering.
- Affect the economic conditions of the country.
- The pharmaceutical industry
- Evolve to cope with environmental changing.
- Cheaper and more accessible.
Suddenly

- Production line stopped.
- The control to Machines within same subnet had been cut off.
- Loss of control and loss of view.
- Case was reported.
- The IT manager announced EMERGENCY.
Figuring out the problem

- After little investigation
  - Files and folders are Encrypted.
  - Connections eliminated with some of the servers.
  - Money is required in bitcoin to regain the access to the system.
Informing the rescue team

- Due to lack of expertise at Medico, the EG-CERT was informed.

Requirements
- Investigation with Team members related to the encrypted servers.
- Full diagram for the existing system
Incident Response
Incident Response Process

Preparation
Understanding and preparing.

Containment
How intruders hacked the network and moved from one system to another

Recovery
Restoring affected systems back into business

Identification
Identify compromised systems.

Eradication
Actions required to mitigate the current incident

Follow up and lesson learned
Involved Parties

- IT manager
- System Administrators
- Network Administrators
- Developing team
- SCADA Team
Topology

- VLAN IDs: Internal_73, External 11
- VLAN ID: SCADA_1
- VLAN ID: Internal_71

- DC: IP: 10.10.71.40
- Backup: IP: 10.10.71.40
- Financial: IP: 10.10.73.65, 11.22.11.22
- SCADA: IP: 10.10.67.22
Data Acquisition
Data Acquisition

Physical

Logical

Custom-Content Image
Data Acquisition (CONT’D)

- Custom content image in addition to memory
Triage

- Prioritize Immediately
- Save Crucial Time
- Avoid Evidence Pile Up
Data Acquisition (CONT’D)

- File Knowledge / Deleted File
  - Thumbs.db
  - Recycle Bin
  - OpenSaveMRU

- Program Execution
  - Recent Apps
  - LastVisitedMRU
  - UserAssist
Data Acquisition (CONT’D)

- File/ Folder Opening
  - Shellbags ➔ UsrClass.dat, NTUSER.dat
  - *.lnk
  - Prefetch

- Account Usage
  - RDP Usage ➔ Security.evtx
Data Acquisition (CONT’D)

- **External Device/ USB Usage**
  - USB drive letter ➔ SYSTEM
  - Volume serial no. ➔ SOFTWARE

- **Browser Usage**
  - History, cache, cookie ➔ User/AppData
Initial Access
Ransomware VIA RDP

- Ransomware ID: Striker
Attacker INFO

- Public vs Private
  - 10.10.73.65
  - 11.22.11.22
- External Attacker
Discovery
Event Viewer

- Event Viewer
- Eternal Blue
- Virustotal Check
Persistence
Persistence

- Modification to the cooperate repos.
- Backdoor was installed on the webserver.
- Reverse connection had been made with unused machine in the network.
Source code files

- Integrity Check
Memory Analysis
Why Memory Analysis

- Identify Rogue Processes
- Analyze Process DLLs and Handles
- Review Network Artifacts
- Look for Evidence of Code Injection
- Check for Signs of a Rootkit
- Extract Processes, Drivers, and Objects
### Domain Controller

- spoolsv.exe

<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>Thds</th>
<th>Hnds Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>82</td>
<td>451</td>
</tr>
<tr>
<td>256</td>
<td>4</td>
<td>2</td>
<td>29</td>
</tr>
<tr>
<td>384</td>
<td>364</td>
<td>7</td>
<td>167</td>
</tr>
<tr>
<td>2300</td>
<td>384</td>
<td>2</td>
<td>50</td>
</tr>
<tr>
<td>424</td>
<td>364</td>
<td>3</td>
<td>110</td>
</tr>
<tr>
<td>372</td>
<td>316</td>
<td>3</td>
<td>74</td>
</tr>
</tbody>
</table>

Volatility Foundation Volatility Framework 2.6

```
Volatility Foundation Volatility Framework 2.6

0x13ff3bba0 TCPv4 :49212 :4448 ESTABLISHED 1100 spoolsv.exe
```

```
PS D:\presentation\Volatility_2.6_Win64_standalone\Volatility_2.6_Win64_standalone> Volatility 2.6 Win64 standalone\Volatility 2.6 Win64 standalone
```

```
Volatility Foundation Volatility Framework 2.6

0xfffffa8032c9f080:spoolsv.exe
  1100  468  13  335  15:40:21 UTC+0000
  2492 1100  0 ------ 16:20:05 UTC+0000

0xfffffa8031e00000:svchost.exe
  1752  468  9  310  15:40:27 UTC+0000

0xfffffa8032e8f410:svchost.exe
  1136  468  17  292  15:40:21 UTC+0000

0xfffffa80325c30b0:SearchIndexer.exe
  1652  468  13  658  15:40:21 UTC+0000

0xfffffa8032848b0:lsass.exe
  476  372  7  606  15:40:19 UTC+0000

0xfffffa803288870:sm.exe
  484  372  9  135  15:40:19 UTC+0000

0xfffffa8031e03e00:explorer.exe
  1356 1032 23  835  15:49:31 UTC+0000

0xfffffa8031e0f0b0:mme.exe
  1080 1356 12  295  15:50:02 UTC+0000

0xfffffa80325c0b30:cmd.exe
  2302 1356 1  42  15:57:12 UTC+0000
```
## Attack Vector

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial access and Execution</td>
<td>The initial access was done using weakly configured RDP</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Logged on the server using Admin Account</td>
</tr>
<tr>
<td></td>
<td>Used SMB vulnerability which has system level user</td>
</tr>
<tr>
<td>Credential Access</td>
<td>Dumping Domain Accounts</td>
</tr>
<tr>
<td>Discovery</td>
<td>Scan for all active IPs on the network</td>
</tr>
<tr>
<td>Lateral movement</td>
<td>Gathering Domain Admin Credentials</td>
</tr>
<tr>
<td>Persistence</td>
<td>Placing backdoors on webserver</td>
</tr>
<tr>
<td>Impact</td>
<td>Production Stopped, Data Leakage</td>
</tr>
</tbody>
</table>
Lesson Learned
Lesson Learned

✓ Complex Password
✓ Service account privileges
✓ EDR (Endpoint Detection and Response)
✓ SIEM
✓ Regular Security Audit to Infrastructure
✓ Consider RDP in restricted Admin Mode
Lesson Learned (Cont’d)

- Enable command line and PowerShell auditing and logging
- Security Awareness
- Create hash repository for your applications
- Incident Response Readiness Plan
- Forensic Readiness Plan
THANKS!

For more information, please contact:
mabdelghani@egcert.eg