

RASTREA2R

COLLECTING & HUNTING FOR IOCs WITH GUSTO AND STYLE!

AUTHOR: ISMAEL VALENZUELA (@ABOUTSECURITY)

CONTRIBUTORS: RYAN O'CONNOR (@_REMIXED) AND ROB GRESHAM (@RWGRESHAM)

[HTTPS://GITHUB.COM/ABOUTSECURITY/RASTREA2R](https://github.com/aboutsecurity/rastrea2r)

{ THE CHALLENGE};

- WORKING AS THREAT RESEARCHER FOR A LARGE HEALTHCARE AGENCY
- +50,000 ENDPOINTS CENTRALLY MANAGED BY McAFFEE EPO
- 700 EVENTS/SECOND (17 MILLION EVENTS/DAY)
- LITTLE OR NO FORENSICS IN PLACE. TRIAGE, EVIDENCE COLLECTION, AND ANALYSIS WAS MANUAL AND REACTIVE
- RESULTS OF THE TRIAGE PROCESS WERE DIFFICULT TO VALIDATE AND PROCESS
- INITIAL VECTOR OF COMPROMISE WAS DIFFICULT TO DETERMINE
- ATTACKS WERE DIFFICULT TO CLASSIFY BASED ON IMPACT TO THE BUSINESS
- CONTAINMENT WAS THE SAME ON ALL CASES (AV SCAN AND REIMAGE)
- NO LESSONS LEARNED

{ PROTOTYPING A SOLUTION: QUICK & DIRTY };

1. COLLECT HOST ARTIFACTS REQUIRED FOR TRIAGE (EVENT ANALYSIS) FROM ALL ENDPOINTS
2. WITHOUT DEPLOYING ADDITIONAL AGENTS TO THE ENDPOINT
3. CROSS-PLATFORM
4. MUST SUPPORT AUTOMATED, REMOTE RESPONSE
5. WITH MINIMAL FOOTPRINT, ADHERING TO FORENSICALLY SOUND PROCEDURES
6. TRIAGE USING BOTH NATIVE AND THIRD PARTY TOOLS
7. SUPPORT PROACTIVE HUNTING FOR ANY GIVEN IoCs
8. EXTENSIBLE TO INTEGRATE WITH WELL KNOWN IR AND FORENSICS OPEN SOURCE FRAMEWORKS

{ AUTOMATION == PYTHON };

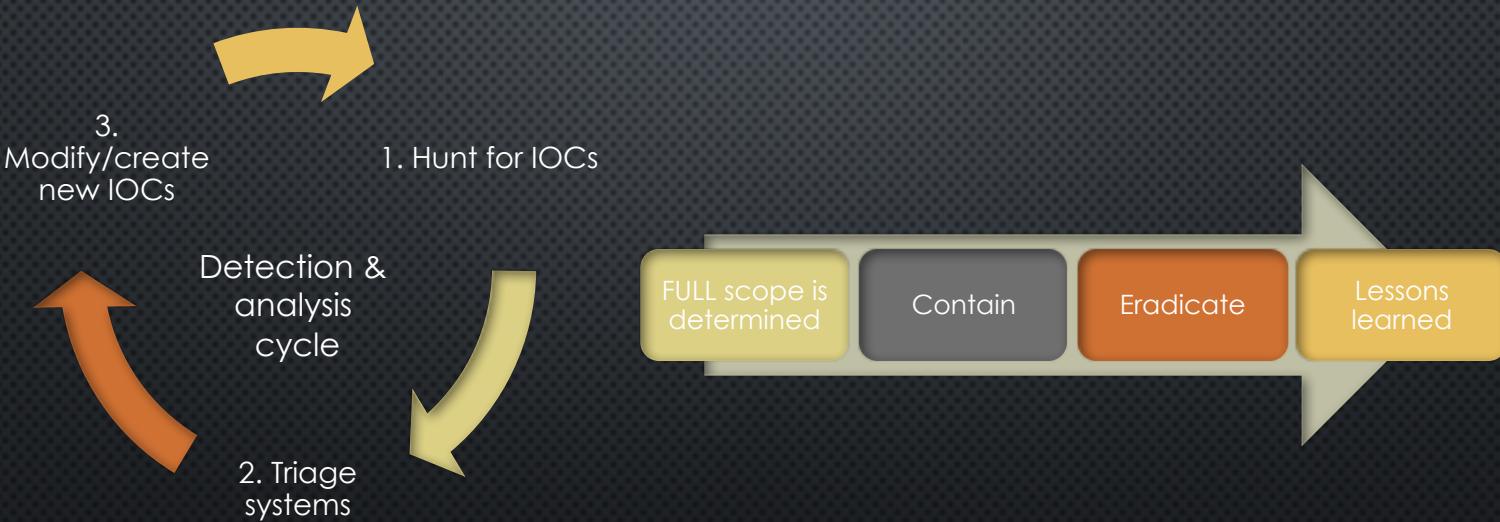
1. TONS OF LIBRARIES CREATED RELATED TO SECURITY AND COMPUTER FORENSICS
2. IDEAL TO CREATE QUICK PROTOTYPES OF APPLICATIONS OR ALGORITHMS
3. SUPPORTS THE DESIGN OF RESTFUL INTERFACES (CLIENT-SERVER SERVICES)
4. PYTHON LETS ME FOCUS ON CONCEPTS RATHER THAN CODE
5. WITH PYINSTALLER I CAN FREEZE (PACKAGE) PYTHON PROGRAMS INTO SMALL STAND-ALONE EXECUTABLES
6. ALSO... IT WAS NAMED AFTER THE GREAT MONTY PYTHON!



{ WHAT DO WE NEED TO AUTOMATE? };

- MALWARE DOESN'T EXIST IN A VACUUM:
 - THEY NEED TO RUN
 - THEY NEED TO COMMUNICATE
 - THEY NEED TO BE PERSISTENT
- HOW DO WE FIND "EVIDENCE"?
- TRADITIONAL FORENSICS TECHNIQUES ARE TOO TIME CONSUMING
- TRIAGING CAN BE USED TO IDENTIFY RELEVANT EVIDENCE QUICKLY AND GUIDE THE IR PROCESS
- LIVE FORENSIC ANALYSIS
- VOLATILE DATA
 - PROCESSES
 - NETWORK CONNECTIONS, ETC.
- NON VOLATILE DATA
 - PROGRAM EXECUTION (PREFETCH)
 - AUTORUN LOCATIONS
 - MASTER FILE TABLE (MFT), ETC.
- DUMP AND EXAMINE MEMORY
- SCAN WITH INDICATORS OF COMPROMISE (IOCs)

{ HUNTING & SMART INCIDENT RESPONSE };



{ HUNTING WITH YARA };



- “THE PATTERN MATCHING SWISS KNIFE FOR MALWARE RESEARCHERS (AND EVERYONE ELSE!)”
- [HTTP://PLUSVIC.GITHUB.IO/YARA](http://plusvic.github.io/yara)
- PATTERN MATCHING:
 - STRINGS, REGULAR EXPRESSIONS AND BINARY PATTERNS (HEX STRINGS)
- CLASSIFICATION:
 - ON INPUT: COMBINATION OF STRINGS & LOGIC, STORED IN A YARA RULE
 - ON OUTPUT: TAGS, METADATA
- CAN BE INTEGRATED IN YOUR PYTHON PROJECTS (BINDINGS)
- GREAT REPOSITORY:
[HTTP://YARARULES.COM/](http://yararules.com/)

@YARARULES

{ SO HOW DO WE DO ALL THIS? – RASTREA2R };

- **RASTREA2R** (PRONOUNCED RASTREADOR):

- [HTTPS://GITHUB.COM/ABOUTSECURITY/RASTREA2R](https://github.com/aboutsecurity/rastrea2r) (OPENSOURCE!)
- COMMAND LINE TOOL (COZ COMMAND LINE IS SEXY!)
- PYTHON / MULTIPLATFORM (WIN32/64, LINUX AND OSX)
- USES A REST API TO REPORT **YARA** SCANS
- WRAPPER TO SYSINTERNAL, SYSTEM COMMAND AND 3RD PARTY TOOLS
- EASY TO INTEGRATE WITH McAFFEE EPO (BUT ALSO DISTRIBUTABLE VIA SSCM, ETC.)
- PACKAGED BINARIES AVAILABLE ON GITHUB



{ CURRENT FUNCTIONALITY IN RASTREA2R V0.7 };

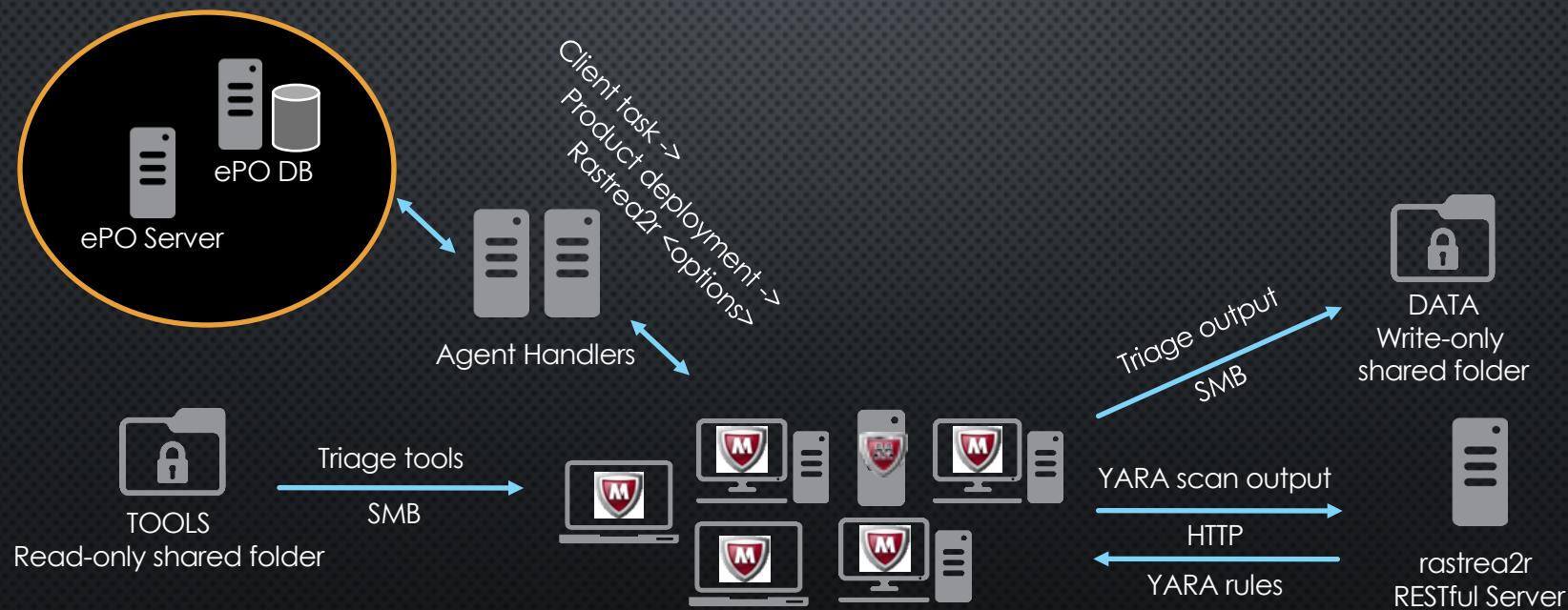
- **YARA-DISK:** YARA SCAN FOR FILE/DIRECTORY OBJECTS ON DISK
- **YARA-MEM:** YARA SCAN FOR RUNNING PROCESSES IN MEMORY
- **MEMDUMP:** ACQUIRES A MEMORY DUMP FROM THE ENDPOINT ** WIN ONLY
- **TRIAGE:** COLLECTS TRIAGE INFORMATION FROM THE ENDPOINT ** WIN ONLY

OBTAINING HELP:

RASTREA2R_WIN32_v0.7.EXE -H

{ TRIAGE + HUNTING ON STEROIDS = RASTREA2R};

FORENSICALLY SOUND ARCHITECTURE AND COMMUNICATION FLOWS



{ TRIAGING WITH RASTREA2R };

- EXAMPLE:
 - RASTREA2R_WIN32_v0.7.EXE **TRIAGE** TOOLS.MYSERVER.COM DATA.MYSERVER.COM
 - *** TOOLS.MYSERVER.COM -> HAS A READ ONLY SHARED-FOLDER CALLED **TOOLS**
 - *** DATA.MYSERVER.COM -> HAS A WRITE ONLY SHARED-FOLDER CALLED **DATA**

```
C:\Users\user\Desktop\rastrea2r\client\rastrea2r_win32_v0.6>rastrea2r_win32_v0.6.exe triage -h
usage: rastrea2r_win32_v0.6.exe triage [-h] [-s] BIN_server DATA_server
```

positional arguments:

```
BIN_server    Binary tool server (SMB share)
DATA_server   Data output server (SMB share)
```

optional arguments:

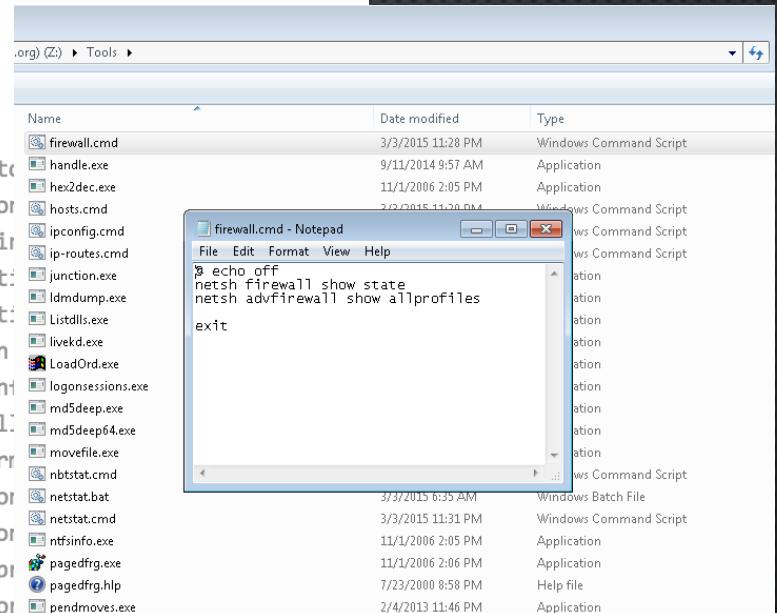
```
-h, --help      show this help message and exit
-s, --silent    Suppresses standard output
```

{ 3RD PARTY TOOLS & NATIVE WIN COMMANDS };

COPY THE TOOLSET TO THE READ-ONLY 'TOOLS' SHARE

""" Add your list of Sysinternal / third-party / BATCH files here """

```
tool=(  
    'systeminfo.cmd', # Gathers systeminfo  
    'set.cmd', # Gathers Set variables  
    'dir-tree.cmd', # Enumerates C:\ directory tree  
    'ipconfig.cmd', # Gathers IP information  
    'ip-routes.cmd', # Gathers IP routing information  
    'arp.cmd', # Gathers ARP table information  
    'dns.cmd', # Gathers DNS Cache information  
    'users.cmd', # Gathers User/local Admin information  
    'shares.cmd', # Gathers local shares information  
    'firewall.cmd', # Gathers local firewall information  
    'hosts.cmd', # Captures Host file information  
    'sessions.cmd', # Gathers Active Session information  
    'nbtstat.cmd', # Gathers NetBios Session information  
    'netstat.cmd', # Gathers Netstat with pinging  
    'services.cmd', # Gathers services information
```



{ 3RD PARTY TOOLS & NATIVE WIN COMMANDS };

The image shows a Windows file system browser window and two Notepad windows. The file system browser displays a folder structure under 'Data' for 'triage-CMB-2N1D-P07'. Inside this folder are several sub-folders and log files, including:

- 20151009193727-CMB-2N1D-P07-systeminfo.log
- 20151009193749-CMB-2N1D-P07-dir-tree.log
- 20151009193749-CMB-2N1D-P07-set.log
- 20151009195040-CMB-2N1D-P07-ipconfig.log
- 20151009195041-CMB-2N1D-P07-arp.log
- 20151009195041-CMB-2N1D-P07-ip-routes.log
- 20151009195042-CMB-2N1D-P07-dns.log
- 20151009195042-CMB-2N1D-P07-users.log
- 20151009195043-CMB-2N1D-P07-firewall.log
- 20151009195043-CMB-2N1D-P07-shares.log
- 20151009195044-CMB-2N1D-P07-hosts.log
- 20151009195044-CMB-2N1D-P07-sessions.log
- 20151009195048-CMB-2N1D-P07-nbtstat.log
- 20151009195048-CMB-2N1D-P07-netstat.log
- 20151009195048-CMB-2N1D-P07-services.log
- 20151009195049-CMB-2N1D-P07-process-list.log
- 20151009195050-CMB-2N1D-P07-tasklist.log

To the right, two Notepad windows are open:

- Process information for CMB-2N1D-P07:** This window contains a table of processes with columns: Name, Pid, Pri, Thd, and Hnd.
- 20151009195305-CMB-2N1D-P07-pslist.log - Notepad:** This window contains the raw text of the process list table from the previous window.

Name	Pid	Pri	Thd	Hnd
Idle	0	0	4	0
System	4	8	204	1542
smss	360	11	4	39
csrss	512	13	10	1123
conhost	2132	8	2	31
conhost	9212	8	2	35
wininit	564	13	3	78
services	668	9	11	365
DWRCS	420	8	16	239
DWRCSST	4296	8	6	172
DWRCSST	4940	8	6	170
DWRCSST	5272	8	6	172
armsvc	520	8	4	68
svchost	780	8	12	419
WmiPrvSE	720	8	6	148
naPrvMgr	2236	8	8	4008
WmiPrvSE	3656	8	12	291
WmiPrvSE	3976	8	16	469
WmiPrvSE	4816	8	7	122
WmiPrvSE	4872	8	7	166
MfEffCore	6052	8	18	273
MfEffCore	13836	8	17	244
svchost	864	8	12	536
ndrvx	880	8	12	185
svchost	972	8	19	597
SearchIndexer	1000	8	14	2994
SearchFilterHost	8232	4	8	139
SearchProtocolHost	10508	4	10	331
svchost	1044	8	16	492
svchost	1177	8	16	492

{ MEMORY DUMPS WITH RASTREA2R };

- EXAMPLE:
 - RASTREA2R_WIN32_V0.7.EXE **MEMDUMP** TOOLS.MYSERVER.COM DATA.MYSERVER.COM
 - *** TOOLS.MYSERVER.COM -> HAS A READ ONLY SHARED-FOLDER CALLED **TOOLS**
 - *** DATA.MYSERVER.COM -> HAS A WRITE ONLY SHARED-FOLDER CALLED **DATA**

```
C:\Users\user\Desktop\rastrea2r\client\rastrea2r_win32_v0.6>rastrea2r_win32_v0.6.exe memdump -h
usage: rastrea2r_win32_v0.6.exe memdump [-h] [-s] BIN_server DATA_server

positional arguments:
  BIN_server    Binary tool server (SMB share)
  DATA_server   Data output server (SMB share)

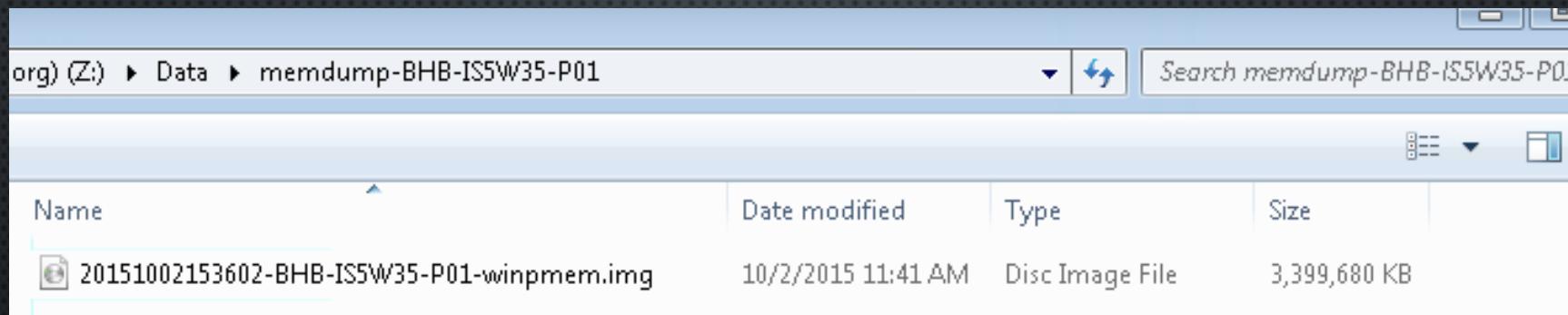
optional arguments:
  -h, --help      show this help message and exit
  -s, --silent    Suppresses standard output
```

{ MEMORY DUMPS WITH RASTREA2R };

MEMORY DUMPS OF ANY MANAGED HOST PIPED OVER SMB USING WINPMEM

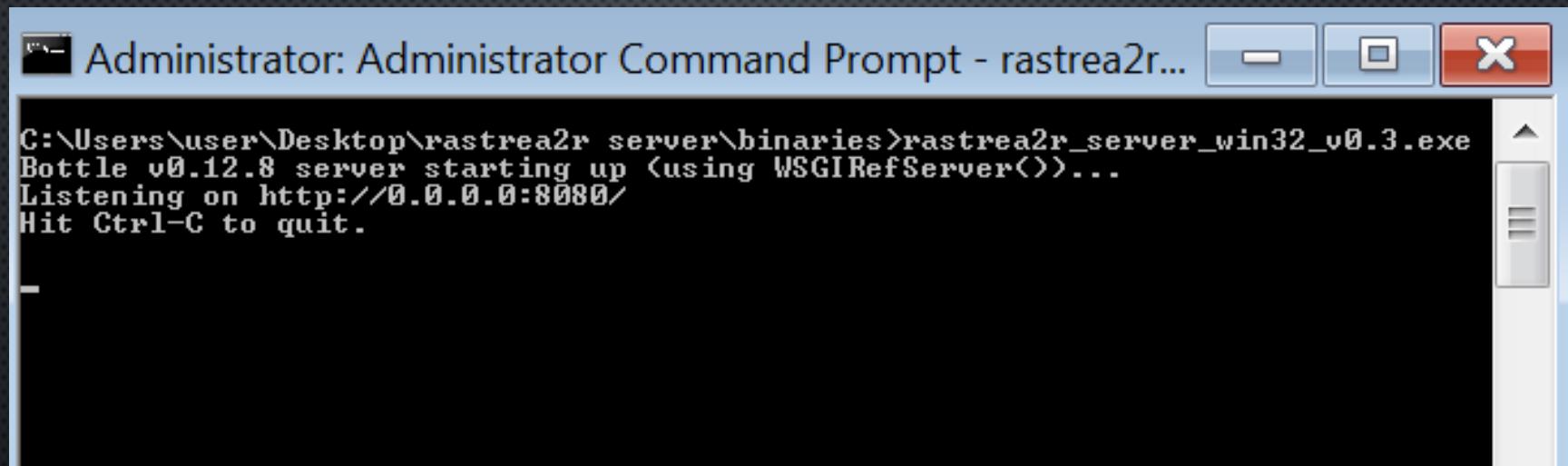
Full memory dump on RAW format:

- Ready to be parsed with memory analysis tools like volatility



{ STARTING THE RASTREA2R SERVER };

LISTENING ON ALL INTERFACES ON PORT 8080



An Administrator Command Prompt window titled "Administrator: Administrator Command Prompt - rastrea2r...". The window contains the following text output:

```
C:\Users\user\Desktop\rastrea2r_server\binaries>rastrea2r_server_win32_v0.3.exe
Bottle v0.12.8 server starting up (using WSGIRefServer())
Listening on http://0.0.0.0:8080/
Hit Ctrl-C to quit.
```

{ HUNTING WITH RASTREA2R };

*** CLIENT / SERVER ARCHITECTURE USING A RESTFUL API

*** YARA RULES MUST BE STORED ON THE SAME DIRECTORY AS THE SERVER

```
C:\Users\user\Desktop\rastrea2r client\rastrea2r_win32_v0.6>rastrea2r_win32_v0.6.exe yara-mem -h
usage: rastrea2r_win32_v0.6.exe yara-mem [-h] [-s] server rule
```

```
positional arguments:
  server      rastrea2r REST server
  rule        Yara rule on REST server
```

```
optional arguments:
  -h, --help    show this help message and exit
  -s, --silent  Suppresses standard output
```

```
C:\Users\user\Desktop\rastrea2r client\rastrea2r_win32_v0.6>rastrea2r_win32_v0.6.exe yara-disk -h
usage: rastrea2r_win32_v0.6.exe yara-disk [-h] [-s] path server rule
```

```
positional arguments:
  path        File or directory path to scan
  server      rastrea2r REST server
  rule        Yara rule on REST server
```

```
optional arguments:
  -h, --help    show this help message and exit
  -s, --silent  Suppresses standard output
```

{ HUNTING FOR IOCS IN MEMORY WITH YARA };

Example:

- rastrea2r_win32_v0.7.exe yara-mem *localhost ransomware.yar*

```
Scanning running processes in memory

['cmdline': [], 'exe': None, 'pid': 0, 'name': 'System Idle Process']
Failed scanning process ID: 0
['cmdline': [], 'exe': None, 'pid': 4, 'name': 'System'}
Failed scanning process ID: 4
['cmdline': ['C:\Program Files\VMware\VMware Tools\vmtoolsd.exe', '-n', 'vmuser'], 'exe': 'C:\Program Files\VMware Tools\vmtoolsd.exe', 'pid': 120, 'name': 'vmtoolsd.exe'}
['cmdline': ['C:\Program Files\Microsoft Office\Office15\lync.exe'], 'exe': 'C:\Program Files\Microsoft Office\Office15\lync.exe', 'pid': 148, 'name': 'lync.exe'}
['cmdline': ['C:\SystemRoot\System32\snss.exe'], 'exe': 'C:\Windows\System32\snss.exe', 'pid': 304, 'name': 'snss.exe'}
['cmdline': ['C:\Program Files\McAfee\Common Framework\naPrdMgr.exe', '-Embedding'], 'exe': 'C:\Program Files\McAfee\Common Framework\naPrdMgr.exe', 'pid': 320, 'name': 'naPrdMgr.exe'}
['cmdline': ['C:\SystemRoot\system32\csrss.exe', 'ObjectDirectory=\Windows', 'SharedSection=1024,12288,512', 'Windows=On', 'SubSystemType=Windows', 'ServerDll=basesrv,1', 'ServerDll=winsrv:UserServerDllInit', 'me': 'csrss.exe'}
['cmdline': ['wininit.exe'], 'exe': 'C:\Windows\System32\wininit.exe', 'pid': 444, 'name': 'wininit.exe'}
['cmdline': ['C:\SystemRoot\system32\csrss.exe', 'ObjectDirectory=\Windows', 'SharedSection=1024,12288,512', 'Windows=On', 'SubSystemType=Windows', 'ServerDll=basesrv,1', 'ServerDll=winsrv:UserServerDllInit', 'me': 'csrss.exe'}
['cmdline': ['C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe'], 'exe': 'C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe', 'pid': 492, 'name': 'sqlwriter.exe'}
['cmdline': ['C:\Windows\system32\services.exe'], 'exe': 'C:\Windows\System32\services.exe', 'pid': 500, 'name': 'services.exe'}
['cmdline': ['C:\Windows\System32\lsass.exe'], 'exe': 'C:\Windows\System32\lsass.exe', 'pid': 516, 'name': 'lsass.exe'}
['cmdline': ['C:\Windows\System32\lsm.exe'], 'exe': 'C:\Windows\System32\lsm.exe', 'pid': 528, 'name': 'lsm.exe'}
['cmdline': ['winlogon.exe'], 'exe': 'C:\Windows\System32\winlogon.exe', 'pid': 572, 'name': 'winlogon.exe'}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'DcomLaunch'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 740}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'RPC$'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 744}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'imgsvc'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 748}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'LocalServiceNetworkRestricted'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 752}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'LocalSystemNetworkRestricted'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 756}
['cmdline': ['C:\Program Files\skPartnerNetwork\Toolbar\apnmcp.exe'], 'exe': 'C:\Program Files\skPartnerNetwork\Toolbar\apnmcp.exe', 'pid': 760}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'LocalService'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 764}
['cmdline': ['C:\Windows\System32\svchost.exe', '-k', 'netsvcs'], 'exe': 'C:\Windows\System32\svchost.exe', 'pid': 768}
['cmdline': ['C:\load'], 'exe': 'C:\Program Files\Microsoft\Common Framework\McTray.exe', 'pid': 1020, 'name': 'McTray.exe'}
['cmdline': ['C:\Program Files\McAfee\Common Framework\UpdateUI.exe', '/StartedFromRunKey'], 'exe': 'C:\Program Files\McAfee\Common Framework\UpdateUI.exe', 'pid': 1024, 'name': 'UpdateUI.exe'}
['cmdline': ['C:\Program Files\VMware\VMware Tools\vmtoolsd.exe'], 'exe': 'C:\Program Files\VMware Tools\vmtoolsd.exe', 'pid': 1028, 'name': 'vmtoolsd.exe'}
['cmdline': ['C:\Windows\System32\cmd.exe'], 'exe': 'C:\Windows\System32\cmd.exe', 'pid': 1324, 'name': 'cmd.exe'}
['cmdline': ['C:\Windows\System32\cmd.exe'], 'exe': 'C:\Windows\System32\cmd.exe', 'pid': 1328, 'name': 'cmd.exe'}
Administrator: Administrator Command Prompt - rastrea2r...
C:\Users\user\Desktop\rastrea2r server\binaries\rastrea2r_server_win32_v0.3.exe
Bottle v0.12.8 server starting up <using WSGIRefServer()>...
Listening on http://0.0.0.0:8080/
Hit Ctrl-C to quit.

Pulling ransomware.yar
127.0.0.1 - - [09/Oct/2015:21:25:37] "POST /getrule HTTP/1.1" 200 2588
```

{ HUNTING FOR IOCS ON DISK WITH YARA };

Example:

- rastrea2r_win32_v0.7.exe yara-disk c:\users\user localhost ransomware.yar

```
all of <$s*> and filesize < 600
}
rule BackdoorFCKG: CTB_Locker_Ransomware
{
meta:
author = "ISG"
date = "2015-01-20"
reference = "https://blogs.mcafee.com/mcafee-labs/rise-backdoor-fckq-ctb-locker"
description = "CTB_Locker"
strings:
$string0 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
$string1 = "RNDBAAAAAAA"
$string2 = "keme132.DLL"
$string3 = "klospad.pdb"
condition:
3 of them
}
```

Scanning c:\users\user

'filename': 'c:\\users\\user\\Desktop\\rastrea2r_server\\binaries\\ransomware.yar', 'hostname': 'WIN-M4BNKTI076D', 'module': 'yaradisk', 'rulename': BackdoorFCKG}

```
C:\Users\user\Desktop\rastrea2r_server\binaries>rastrea2r_server_win32_v0.3.exe
Bottle v0.12.8 server starting up (using WSGIRefServer())
Listening on http://0.0.0.0:8080/
Hit Ctrl-C to quit.
```

```
Pulling ransomware.yar
```

```
127.0.0.1 - - [09/Oct/2015 21:25:37] "POST /getrule HTTP/1.1" 200 2588
127.0.0.1 - - [09/Oct/2015 21:26:40] "POST /putpid HTTP/1.1" 200 0
127.0.0.1 - - [09/Oct/2015 21:26:46] "POST /putpid HTTP/1.1" 200 0
```

```
Pulling ransomware.yar
```

```
127.0.0.1 - - [09/Oct/2015 21:31:35] "POST /getrule HTTP/1.1" 200 2588
127.0.0.1 - - [09/Oct/2015 21:33:28] "POST /putfile HTTP/1.1" 200 0
```

{ TRIAGING WITH ‘RASTREA2R’ FROM MCAFEE EPO CONSOLE };

CLIENT TASKS -> PRODUCT DEPLOYMENT -> RASTREA2R TRIAGE/MEMDUMP

The screenshot displays the McAfee EPO Console interface. On the left, the 'System Properties' tab is selected, showing details for the system 'BHB-NS17N-P05'. The 'Communication Type' section lists various tasks such as 'Deploy Agents', 'Modify Policies on a Single System', and 'Run Client Task Now'. The 'Run Client Task Now' dialog is open in the center, listing tasks under 'Product' (McAfee Agent) and 'Task Type' (McAfee Agent statistics, McAfee Agent Wakeup (Windows only), Mirror Repositories (Windows only), Product Deployment, Product update). A task named 'Rastrea2r - Triage' is selected. On the right, the 'Running Client Task Status' panel shows the task has been initiated on 10/7/15 at 5:17:24 PM. The status bar indicates the task is running.

Modularity:

- A specific task is created for each combination of command line switches

{ ANALYZING THE RESULTS (~5 MINUTES) };

A FOLDER IS CREATED PER SYSTEM, THEN PER COLLECTION SET (TIMESTAMP)

Name	Date modified	Type
triage-BHB-NS17N-P05	10/7/2015 5:18 PM	File folder
memdump-BHB-NS17N-P05		File folder
triage-BHB-IS5W9LA-P01	10/7/2015 5:18 PM	File folder
triage-BHB-IS555-P04		File folder
triage-DC-KRAUS-LPT		File folder
triage-CDC-1032-P01	10/5/2015 2:02 PM	File folder
triage-FMN-6FL-P20	10/2/2015 3:11 PM	File folder
memdump-FMN-6FL-P20	10/2/2015 2:34 PM	File folder
triage-BHB-IS5W35-P01	10/2/2015 11:51 AM	File folder
memdump-BHB-IS5W35-P01	10/2/2015 11:36 AM	File folder
triage-MMB-15A6P156D1	10/2/2015 9:30 AM	File folder
memdump-MMB-15A6P156D1	10/2/2015 9:21 AM	File folder
triage-CMB-4W11-P03	9/30/2015 1:36 PM	File folder
triage-ENY-2205-P03	9/30/2015 12:58 PM	File folder
triage-KBR-6W-NS-P00	9/30/2015 10:28 AM	File folder
triage-9B-NS_13D1	9/30/2015 10:20 AM	File folder
triage-EMB-07XXBF0-P02	9/30/2015 10:05 AM	File folder
triage-QPB-05XXXNS-P08	9/30/2015 9:40 AM	File folder
triage-KBS-CS15-P07	9/29/2015 11:18 AM	File folder
memdump-KBS-CS15-P07	9/29/2015 11:12 AM	File folder
triage-55W-EOC-P12	9/29/2015 8:51 AM	File folder
triage-QMB-01XEX32-P01	9/28/2015 3:19 PM	File folder
triage-BEB-RD140ED-P01	9/25/2015 12:20 PM	File folder
memdump-BEB-RD140ED-P01	9/25/2015 11:52 AM	File folder
triage-BHB-PL4E17E-P02	9/25/2015 11:48 AM	File folder
triage-KBT-M208-P01	9/25/2015 11:46 AM	File folder
memdump-KBT-M208-P01	9/25/2015 11:38 AM	File folder

→

Name	Date modified
20151006203053	10/6/2015 4:45 PM

{ ANALYZING THE RESULTS };

	20151006204120-BHB-IS5W9LA-P01-firewall.log	10/6/2015 4:41 PM	Text Document 4 KB
	20151006204121-BHB-IS5W9LA-P01-hosts.log	10/6/2015 4:41 PM	Text Document 1 KB
	20151006204121-BHB-IS5W9LA-P01-sessions.log	10/6/2015 4:41 PM	Text Document 6 KB
	20151006204133-BHB-IS5W9LA-P01-nbtstat.log	10/6/2015 4:41 PM	Text Document 1 KB
	20151006204133-BHB-IS5W9LA-P01-netstat.log	10/6/2015 4:41 PM	Text Document 11 KB
	20151006204134-BHB-IS5W9LA-P01-process-list.log	10/6/2015 4:41 PM	Text Document 214 KB
	20151006204134-BHB-IS5W9LA-P01-services.log	10/6/2015 4:41 PM	Text Document 44 KB
	20151006204135-BHB-IS5W9LA-P01-tasklist.log	10/6/2015 4:42 PM	Text Document 179 KB
	20151006204205-BHB-IS5W9LA-P01-at-schtasks.log	10/6/2015 4:42 PM	Text Document 16 KB
	20151006204208-BHB-IS5W9LA-P01-startup-list.log	10/6/2015 4:42 PM	Text Document 8 KB
	20151006204214-BHB-IS5W9LA-P01-psinfo.log	10/6/2015 4:42 PM	Text Document 1 KB
	20151006204214-BHB-IS5W9LA-P01-zRemote.log	10/6/2015 4:42 PM	Text Document 1 KB
	20151006204216-BHB-IS5W9LA-P01-diskext.log	10/6/2015 4:42 PM	Text Document 1 KB
	20151006204216-BHB-IS5W9LA-P01-logonsessions.log	10/6/2015 4:42 PM	Text Document 6 KB

{ THAT SOUNDS HIGHLY SUSPICIOUS... };

```
Caption=ConnectionCenter
Command="C:\Users\BHB-NS17N-P05\AppData\Local\citrix\ICA client\concentr.exe" /startup
Description=ConnectionCenter
Location=HKU\S-1-5-21-2250110424-2442967196-2465209428-110119\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=CORP\BHB-NS17N-P05
```

```
Caption=MSConfig
Command="C:\Users\BHB-NS17N-P05\mvsbsihj.exe"
Description=MSConfig
Location=HKU\S-1-5-21-2250110424-2442967196-2465209428-110119\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=CORP\BHB-NS17N-P05
```

```
Caption=RTHDVCPL
Command=C:\Program Files\Realtek\Audio\HDA\RtHDVCpl.exe -s
Description=RTHDVCPL
Location=HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=Public
```

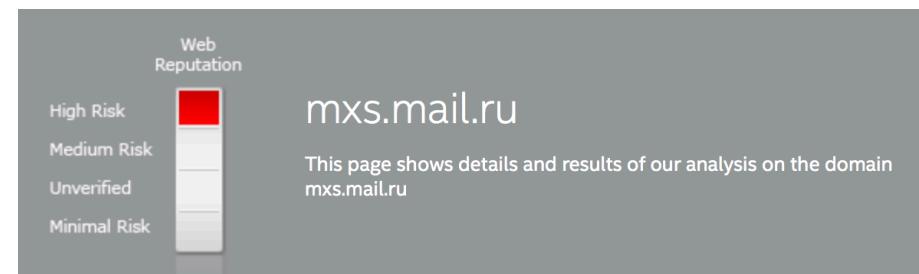
```
Caption=IMSS
Command="C:\Program Files\Intel\Intel(R) Management Engine Components\IMSS\PIconStartup.exe"
Description=IMSS
Location=HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=Public
```

mail.ru

```
Record Name . . . . : mail.ru
Record Type . . . . : 15
Time To Live . . . . : 4
Data Length . . . . : 8
Section . . . . : Answer
MX Record . . . . : mxs.mail.ru
          10
          0
```

```
Record Name . . . . : mxs.mail.ru
Record Type . . . . : 1
Time To Live . . . . : 4
Data Length . . . . : 4
Section . . . . : Additional
A (Host) Record . . . : 217.69.139.150
```

```
Record Name . . . . : mxs.mail.ru
Record Type . . . . : 1
Time To Live . . . . : 4
Data Length . . . . : 4
Section . . . . : Additional
A (Host) Record . . . : 94.100.180.150
```



b-0.19-43000408.9851081.1644.1f0a.2f4a.410.0.9ape7qnbhhzejna5s1525sn3wb.avts.mcafee.com

```
Record Name . . . . : b-0.19-43000408.9851081.1644.1f0a.2f4a.410.0.9ape7qnbhhzejna5s1525sn3wb.avts.mcafee.com
Record Type . . . . : 1
Time To Live . . . . : 3061
Data Length . . . . : 4
Section . . . . : Answer
A (Host) Record . . . : 127.129.0.128
```

{ WHAT ABOUT THAT FUNKY BINARY? };

ALWAYS CHECK HASHES. BAD GUYS USE VIRUSTOTAL TOO!

MVSBSIHJ.EXE

- LOW AV DETECTION AT THE TIME OF SUBMISSION (CHECKED WITH PESTUDIO)
- INJECTS ITSELF INTO SVCHOST.EXE
- CHECKS NETWORK STATUS
- DOWNLOADS A SECOND PAYLOAD WITH SPAMBOT CAPABILITIES
- IN ADDITION TO SENDING SPAM IT CAN DOWNLOAD ADDITIONAL PLUGIN COMPONENTS FROM C&C SERVERS:
 - DDoS ATTACKS
 - SNIFF TRAFFIC AND STEAL CREDENTIALS
 - READ MESSAGES ON TWITTER, SKYPE, FACEBOOK, ETC.
 - BITCOIN MINING, ETC.

Type	Size	Blacklisted (5)	Value
ascii	14	x	VirtualAllocEx
ascii	18	x	CreateRemoteThread
ascii	11	x	SendMessage
ascii	8	x	VBA6.DLL
ascii	15	x	DllFunctionCall
ascii	40	-	!This program cannot be run in DOS mode.
ascii	5	-	.text
ascii	6	-	'.data
ascii	5	-	.rsrc
ascii	12	-	MSVBVM60.DLL
ascii	5	-	'2@x;
ascii	24	-	= Filmwissenschaften

{ WHAT NEXT? };

1. CREATE A NEW YARA RULE BASED ON THIS SAMPLE
2. SCAN THE ENVIRONMENT AND TRIAGE INFECTED SYSTEMS
3. TUNE THE YARA RULE BASED ON FINDINGS
4. REPEAT, RINSE AND STOP ONCE THE **FULL** SCOPE IS DETERMINED
5. CONTAIN & ERADICATE
6. CONDUCT MEMORY ANALYSIS AND FULL DISK FORENSICS TO DETERMINE **ROOT CAUSE**

```
RULE SYSTEMXYZ-SPAMBOT
```

```
{
```

```
STRINGS:
```

```
$STRING0 = "FFFFF."
```

```
$STRING1 = "AVVWSH"
```

```
$STRING2 = "AWAVAUATVWSH"
```

```
$STRING3 = "FFFFFF."
```

```
$STRING4 = ".RELOC"
```

```
CONDITION:
```

```
4 OF THEM }
```

{ THE RESULTS };

WHERE ARE WE NOW?

- ABILITY TO TRIAGE AND COLLECT EVIDENCE FROM THOUSANDS OF ENDPOINTS CENTRALLY MANAGED BY McAFFEE ePO **IN MINUTES**
- TRIAGE AND EVIDENCE COLLECTION IS **AUTOMATED**, WITH **PROACTIVE** HUNTING OF IOCS BASED ON FBI TLPs, VENDOR REPORTS, INTERNAL IR INVESTIGATIONS AND OTHER THREAT INTELLIGENCE FEEDS
- RESULTS OF THE TRIAGE PROCESS CAN BE **VALIDATED** BY TRAINED ANALYSTS
- WORKING ON AUTOMATING EVIDENCE/ARTIFACTS PROCESSING AND ANALYSIS
- INITIAL VECTOR OF COMPROMISE CAN BE DETERMINED ON MOST CASES

THANK YOU!

@ABOUTSECURITY

[HTTP://BLOG.ISMAELVALENZUELA.COM](http://blog.ismaelvalenzuela.com)

[HTTPS://GITHUB.COM/ABOUTSECURITY/](https://github.com/aboutsecurity/)

