



*rastrea*2r

HUNTING FOR THREATS WITH GUSTO & STYLE

Ismael Valenzuela @aboutsecurity
Sudheendra Bhat @eaglesparadise

ABOUT US



Principal Engineer, leading Security Operations, Threat Hunting and DFIR at **McAfee**
SANS Certified Instructor for Cyber Defense and Digital Forensics curriculum
GIAC Security Expert (GSE #132), GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT,
GSNA, GMON, CISSP, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK.

<http://aboutsecurity.io>

Twitter: @aboutsecurity



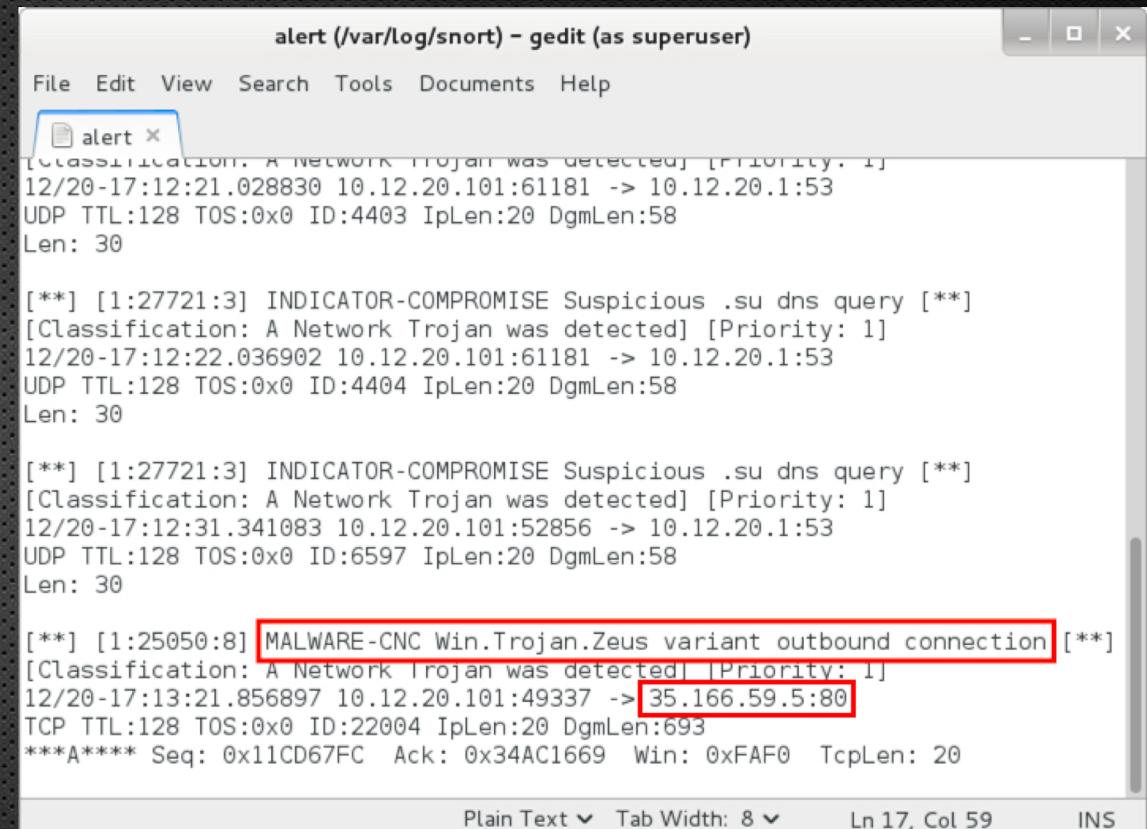
Sudheendra Bhat
Security Architect , Security Operations @ **McAfee**
Twitter: @eaglesparadise

A DAY IN THE LIFE OF A SOC ANALYST

- WHEN A SYSTEM IS REPORTED AS INFECTED OR IS ACTING SUSPICIOUSLY:
 - DO I HAVE ENOUGH CONTEXT TO DETERMINE WHAT TO DO NEXT?
 - SHOULD I SIMPLY DISCONNECT THE SYSTEM AND RE-IMAGE?
 - WHAT IF THE ATTACKER CAN DETECT MY RESPONSE AND CHANGE TACTICS?
 - IS THIS RANSOMWARE, A NON-TARGETED CAMPAIGN OR AN APT LIKE ATTACK?
 - IS IT POSSIBLE THAT THE SYSTEM HOLDS OTHER MALWARE THAT HASN'T BEEN DETECTED YET?
 - HOW CAN I COLLECT ENOUGH INFORMATION FROM THESE SYSTEMS (QUICKLY ENOUGH) TO DETERMINE THE BEST CONTAINMENT AND ERADICATION STRATEGY?
 - CAN THEY HELP ME TO PROFILE THE ATTACKER'S TECHNIQUES?
 - HOW CAN I PROACTIVELY SEARCH FOR INDICATORS OF COMPROMISE (IOC) ACROSS MY ENDPOINT?

A DAY IN THE LIFE OF A SOC ANALYST

- TRAFFIC BLOCKED TO A SUSPICIOUS IP
 - WHAT PROCESS IS GENERATING THIS TRAFFIC ON THE ENDPOINT? AND WHY?
 - IS THERE ANY OTHER MALICIOUS ACTIVITY ON THIS HOST THAT IS NOT BEING DETECTED?
 - HOW DO I RESPOND TO THIS? WHAT SHOULD I DO NEXT?



The screenshot shows a terminal window titled "alert (/var/log/snort) - gedit (as superuser)". The window contains several lines of text representing network traffic alerts. The last alert is highlighted with a red box:

```
alert (/var/log/snort) - gedit (as superuser)
File Edit View Search Tools Documents Help
alert x
[Classification: A Network Trojan was detected] [Priority: 1]
12/20/17:12:21.028830 10.12.20.101:61181 -> 10.12.20.1:53
UDP TTL:128 TOS:0x0 ID:4403 IpLen:20 DgmLen:58
Len: 30

[**] [1:27721:3] INDICATOR-COMPROMISE Suspicious .su dns query [**]
[Classification: A Network Trojan was detected] [Priority: 1]
12/20/17:12:22.036902 10.12.20.101:61181 -> 10.12.20.1:53
UDP TTL:128 TOS:0x0 ID:4404 IpLen:20 DgmLen:58
Len: 30

[**] [1:27721:3] INDICATOR-COMPROMISE Suspicious .su dns query [**]
[Classification: A Network Trojan was detected] [Priority: 1]
12/20/17:12:31.341083 10.12.20.101:52856 -> 10.12.20.1:53
UDP TTL:128 TOS:0x0 ID:6597 IpLen:20 DgmLen:58
Len: 30

[**] [1:25050:8] MALWARE-CNC Win.Trojan.Zeus variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
12/20/17:13:21.856897 10.12.20.101:49337 -> 35.166.59.5:80
TCP TTL:128 TOS:0x0 ID:22004 IpLen:20 DgmLen:693
***A*** Seq: 0x11CD67FC Ack: 0x34AC1669 Win: 0xF4F0 TcpLen: 20
```

Plain Text ▾ Tab Width: 8 ▾ Ln 17, Col 59 INS

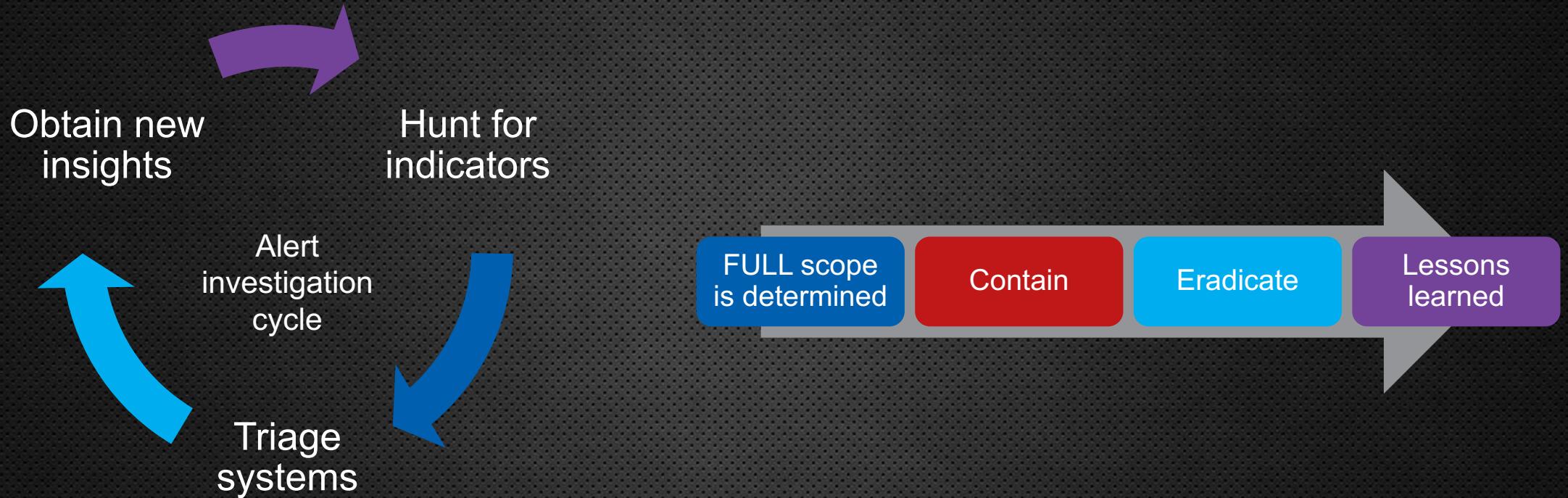
TDS based Rig-V



WHEN YOUR
INCIDENT
RESPONSE
PROCESS IS
SIMPLY...

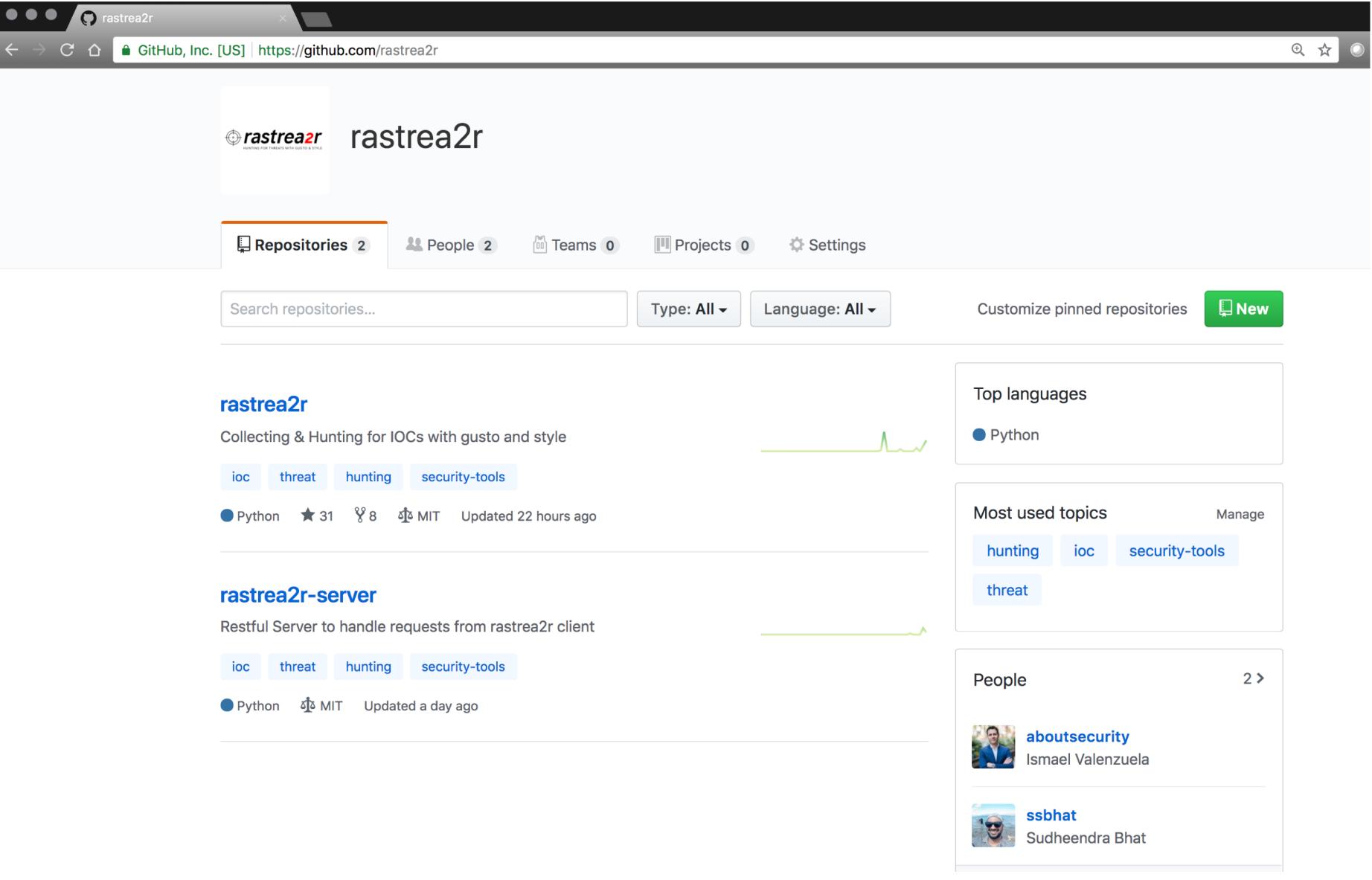
REIMAGE THAT BOX !!!

HUNTING & SMART INCIDENT RESPONSE



SO HOW DO WE DO ALL OF THIS?

- **RASTREA2R** (PRONOUNCED RASTREADOR, HUNTER IN SPANISH):
 - [HTTPS://GITHUB.COM/RASTREA2R/RASTREA2R](https://github.com/Rastrea2r/Rastrea2r) (OPENSOURCE!)
 - COMMAND LINE TOOL – COZ COMMAND LINE IS SEXY!
 - CROSS-PLATFORM (WINDOWS, LINUX AND OSX)
 - USES A RESTFUL API TO REPORT **YARA** SCANS
 - CAN RUN SYSINTERNAL, SYSTEM COMMAND AND OTHER 3RD PARTY TOOLS REMOTELY ON ENDPOINTS, INCLUDING CUSTOM SCRIPTS
 - EASY TO INTEGRATE WITH **AV** CONSOLES & ORCHESTRATION TOOLS (**SOAR**)
 - BUILT USING PYTHON (PACKAGED BINARIES AVAILABLE)
- CURRENT PROJECTS:
 - RASTREA2R CLIENT
 - RASTREA2R SERVER

A screenshot of a GitHub repository page for "rastrea2r". The page title is "rastrea2r" and the subtitle is "MONITORING FOR THREATS WITH GUSTO & STYLE". The main navigation bar includes "Repositories 2", "People 2", "Teams 0", "Projects 0", and "Settings". Below the navigation is a search bar with placeholder "Search repositories...", type and language dropdowns, and a "Customize pinned repositories" section with a "New" button. The first repository listed is "rastrea2r", described as "Collecting & Hunting for IOCs with gusto and style", with tags "ioc", "threat", "hunting", and "security-tools". It is written in Python, has 31 stars, 8 forks, and an MIT license, last updated 22 hours ago. The second repository listed is "rastrea2r-server", described as "Restful Server to handle requests from rastrea2r client", with tags "ioc", "threat", "hunting", and "security-tools". It is also written in Python, uses the MIT license, and was last updated a day ago. To the right of the repositories are three boxes: "Top languages" (Python), "Most used topics" (hunting, ioc, security-tools, threat), and "People" (aboutsecurity, Ismael Valenzuela, ssbhat, Sudheendra Bhat).

rastrea2r
MONITORING FOR THREATS WITH GUSTO & STYLE

Repositories 2 **People 2** **Teams 0** **Projects 0** **Settings**

Search repositories... Type: All Language: All Customize pinned repositories **New**

rastrea2r
Collecting & Hunting for IOCs with gusto and style

ioc threat hunting security-tools

Python ★ 31 8 MIT Updated 22 hours ago

rastrea2r-server
Restful Server to handle requests from rastrea2r client

ioc threat hunting security-tools

Python MIT Updated a day ago

Top languages
Python

Most used topics Manage
hunting ioc security-tools
threat

People 2 >

 **aboutsecurity**
Ismael Valenzuela

 **ssbhat**
Sudheendra Bhat

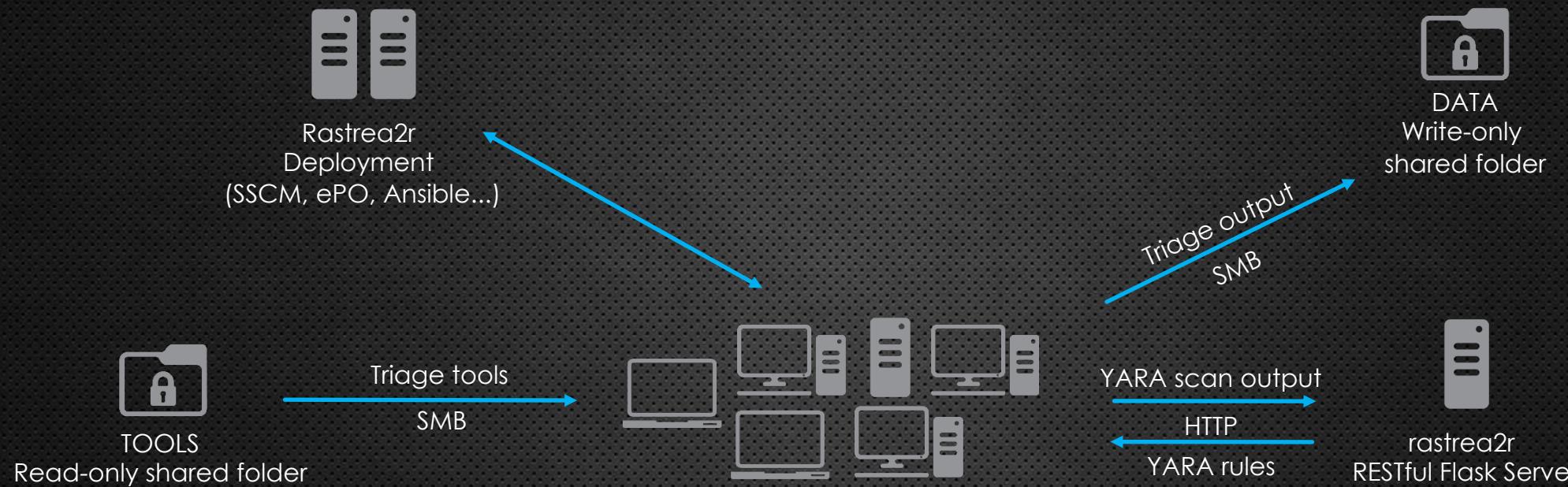
WHAT'S NEW @ BLACKHAT ARSENAL 2018

- MODULAR IMPLEMENTATION WITH SUPPORT FOR PYTHON 3.X
- SUPPORT FOR CUSTOM SCRIPT/COMMAND EXECUTION DURING TRIAGE
- BUILD AUTOMATION SCRIPTS TO HELP FOR EASIER DEPLOYMENT
- ENHANCED LOGGING & DEBUGGING CAPABILITIES
- TRAVIS (CONTINUOUS INTEGRATION) AND READTHEDOC.ORG INTEGRATION
- NEW RESTFUL IMPLEMENTATION OF RASTREA2R SERVER USING FLASK
 - SUPPORT FOR BASIC AUTHENTICATION
 - STRONG PASSWORD HASHING (STORED IN SQLITE DB)
 - SUPPORT FOR DIFFERENT LOGGING OPTIONS
 - RATE LIMITING FOR SAFETY
 - JSONIFIED ERROR HANDLING AND RESULT FORMAT

CURRENT FUNCTIONALITY IN V1

- FAST TRIAGE (SNAPSHOTS)
- PREFETCH
- FORENSIC ARTIFACT COLLECTION
- WEB HISTORY
- MEMDUMP
- YARA DISK
- YARA MEM

DEPLOYING RASTREA2R ON ENDPOINTS



RASTREA2R COMMAND LINE & ARGUMENTS

C:\ Command Prompt

```
C:\Users\sbhat5\rastrea2r\src\dist>rastrea2r.exe -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.exe [-h] [-v]
                      {yara-disk,yara-mem,memdump,triage,web-hist,prefetch} ...
```

::Rastrea2r RESTful remote Yara/Triage tool for Incident Responders ::

positional arguments:

{yara-disk,yara-mem,memdump,triage,web-hist,prefetch}	modes of operation
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
triage	Collects triage information from the endpoint
web-hist	Generates web history for specified user account
prefetch	Generates prefetch view

optional arguments:

-h, --help	show this help message and exit
-v, --version	show program's version number and exit



Note: Currently OSX and Linux Versions support only yara-disk and yara-mem options

Z:\ Data ▶ triage-CMB-2N1D-P07 ▶ 20151009193727

Name
triage-CMB-2N1D-P07
memdump-EMB-0BXXXXE9-P08
memdump-BHB-NS17N-P05
triage-EMB-0BXXXXD18-P01
triage-DC-KRAUS-LPT
triage-EMB-0BXXXXE9-P08
triage-BHB-NS17N-P05
triage-BHB-IS5W9LA-P01
triage-BHB-IS5S5-P04
triage-CDC-1032-P01
triage-FMN-6FL-P20
memdump-FMN-6FL-P20
triage-BHB-IS5W35-P01
memdump-BHB-IS5W35-P01
triage-MMB-15A6P156D1
memdump-MMB-15A6P156D1

Name
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

20151009195305-CMB-2N1D-P07-pslist.log - Notepad

File Edit Format View Help

Process information for CMB-2N1D-P07:

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
DWRCS	4296	8	6	172
DWRCS	4940	8	6	170
DWRCS	5272	8	6	172
armsvc	520	8	4	68
svchost	780	8	12	419
wmiPrvSE	720	8	6	148
naPrdMgr	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	9232	4	8	120

RASTREA2R IN ACTION – 15 MINUTES OF TRIAGE

FORENSIC ARTIFACT ACQUISITION

- EXAMPLE:
 - RASTREA2R.EXE **COLLECT** 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:\Demo>rastrea2r collect -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r collect [-h] [-s] TOOLS_server DATA_server
```

positional arguments:

```
TOOLS_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
```

```
c:\Demo>
```

TRIAGING WITH RASTREA2R (SNAPSHOTS)

- EXAMPLE:
 - RASTREA2R.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\sbhat5\rastrea2r\src\dist>rastrea2r.exe triage -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.exe triage [-h] [-s] TOOLS_server DATA_server

positional arguments:
  TOOLS_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
```

Caption=zCLcIIJndaI
Command=C:\Users\DEMOUS~1\AppData\Local\Temp\WplgaQeK.vbs
Description=zCLcIIJndaI
Location=HKU\S-1-5-21-2126574468-858435778-3403648540-2604\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=SCP\demouser1

[

Caption=VMware User Process
Command="C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Description=VMware User Process
Location=HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

EVIDENCE OF PERSISTENCE - SYSINTERNALS STARTUP-LIST

File Edit Format View Help

Process information for WIN81:

Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
Idle	0	0	1	0	64	24	0
System	4	8	114	940	139412	1504	135424
smss	292	11	2	44	4212	1640	284
csrss	396	13	8	349	45856	3848	1716
...

EQNEDT32
cscript
conhost
gBiwSNwnbyAD

taskhost	1332	6	10	298	1192604	17340	11164
wuauclt	2760	8	1	116	80396	6092	1360
taskhostex	3504	8	6	212	87552	7796	2140
svchost	956	8	28	1153	138212	23044	11900
svchost	1004	8	22	650	4194303	55200	45456
WUDFHost	2360	8	9	249	38032	5696	3052
dasHost	2904	8	3	332	72572	11508	3520
spoolsv	1044	8	8	429	77024	12084	4496
svchost	1068	8	22	516	123964	22912	16532
FrameworkService	1232	6	29	431	93236	1684	7168

20171126083221-WIN81-netstat.log - Notepad

File Edit Format View Help

Netlogon

[System]

TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING 524

Can not obtain ownership information

TCP 0.0.0.0:49160 0.0.0.0:0 LISTENING 2232

PolicyAgent

[System]

TCP 0.0.0.0:49163 0.0.0.0:0 LISTENING 532

[System]

TCP 127.0.0.1:445 127.0.0.1:50230 ESTABLISHED 4

Can not obtain ownership information

TCP 127.0.0.1:50230 127.0.0.1:445 ESTABLISHED 4

Can not obtain ownership information

TCP 192.168.20.104:139 0.0.0.0:0 LISTENING 4

Can not obtain ownership information

TCP 192.168.20.104:49934 192.168.20.5:445 ESTABLISHED 4

Can not obtain ownership information

TCP 192.168.20.104:49943 192.168.20.5:445 ESTABLISHED 4

Can not obtain ownership information

TCP 192.168.20.104:49944 192.168.20.5:445 ESTABLISHED 4

Can not obtain ownership information

TCP 192.168.20.104:49945 192.168.20.5:445 ESTABLISHED 4

Can not obtain ownership information

TCP 192.168.20.104:50182 192.168.1.221:9999 ESTABLISHED 12456

[EQNEDT32.EXE]

TCP 192.168.20.104:50229 192.168.1.221:9999 SYN_SENT 9320

[gBiwSNwnbyAD.exe]

TCP [::]:135 [::]:0 LISTENING 676

RpcSs

PREFETCH

- EXAMPLE:
 - RASTREA2R.EXE **PREFETCH** 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**

Command Prompt

```
C:\Users\sbhat5\rastrea2r\src\dist>rastrea2r.exe prefetch -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.exe prefetch [-h] [-s] TOOLS_server DATA_server

positional arguments:
  TOOLS_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
```

WEB-HISTORY

- EXAMPLE:
 - RASTREA2R.EXE WEB-HIST –U SBHAT5 TOOLS.MYSERVER.COM DATA.MYSERVER.COM
 - *** -U -> USERNAME TO BE PROFILED
 - ***TOOLS.MYSERVER.COM -> HAS A READ ONLY SHARED-FOLDER CALLED **TOOLS**
 - *** DATA.MYSERVER.COM -> HAS A WRITE ONLY SHARED-FOLDER CALLED **DAT**

Command Prompt

```
C:\Users\sbhat5\rastrea2r\src\dist>rastrea2r.exe web-hist -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.exe web-hist [-h] [-u USERNAME] [-s] TOOLS_server DATA_server

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

optional arguments:
  -h, --help            show this help message and exit
  -u USERNAME, --username USERNAME
                        User account to generate history for
  -s, --silent          Suppresses standard output
```

RASTREA2R IN ACTION

The **web-history** plugin returns a CSV file with the browsing history for a user (or all users on the computer) from Firefox, Chrome, IE and Opera:

	A	B	C	D	E	F	G	H	I
127	https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&syslcid=1033&uilcid=1033&app=1&ver=15&build=15.0.4420&p=0&a=1&hm=1&sp=0	11/26/2017 2:17	2		Internet Explorer 10/11 / Edge				126
128	file:///192.168.20.5/data/webhistory-WIN81/20171126071638/20171126071638-WIN81-sha256-hashing.log	11/26/2017 2:20	1		Internet Explorer 10/11 / Edge				96
129	http://www.msn.com/?ocid=iehp	11/26/2017 3:07	4		Internet Explorer 10/11 / Edge				29
130	http://www.msn.com/?ocid=iehp	11/26/2017 3:07	21		Internet Explorer 10/11 / Edge				29
131	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&checkda=1&ct=1511654890&rver=6.7.6643.0&wp=lbi&wreply=https%3a%2f%2fwww.m	11/26/2017 3:07	1		Internet Explorer 10/11 / Edge				223
132	https://cdn3.doubleverify.com/bst2tv3.html	11/26/2017 3:07	4		Internet Explorer 10/11 / Edge				42
133	http://tpc.googlesyndication.com/sodar/lx4UrfoN.html	11/26/2017 3:07	3		Internet Explorer 10/11 / Edge				52
134	res://ieframe.dll/defaultbrowser.htm	11/26/2017 3:07	9		Internet Explorer 10/11 / Edge				36
135	https://cdn3.doubleverify.com/t2tv7.html	11/26/2017 3:07	4		Internet Explorer 10/11 / Edge				40
136	about:blank	11/26/2017 3:07	22		Internet Explorer 10/11 / Edge				11
137	http://acdn.adnxs.com/ib/static/usersync/v3/async_usersync.html	11/26/2017 3:07	4		Internet Explorer 10/11 / Edge				63
138	http://ul1.dvtos.com/cfhc.htm?ifha=0&nurl=https%3A%2F%2Ftnc10202.doubleverify.com%2Fevent%2Fimnid%3D233cd6ba4h624974a2rd118f2f	11/26/2017 3:07	1		Internet Explorer 10/11 / Edge				177
142	http://52.179.101.199/favicon.ico	11/26/2017 3:07	2		Internet Explorer 10/11 / Edge				64
		11/26/2017 3:07	2		Internet Explorer 10/11 / Edge				44
		11/26/2017 3:07	2		Internet Explorer 10/11 / Edge				39
		11/26/2017 3:08	3		Internet Explorer 10/11 / Edge				33
143	http://52.179.101.199/invoice.rtf	11/26/2017 3:08	1		Internet Explorer 10/11 / Edge				33
		11/26/2017 3:08	1		Internet Explorer 10/11 / Edge				33
		11/26/2017 3:12	4		Internet Explorer 10/11 / Edge				22
		11/26/2017 3:12	2		Internet Explorer 10/11 / Edge				22

FULL MEMORY DUMP

- EXAMPLE:
 - RASTREA2R.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 **DAT**

```
c:\Demo>rastrea2r.exe memdump -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.exe memdump [-h] [-s] TOOLS_server DATA_server

positional arguments:
  TOOLS_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
```

YARA DISK

- EXAMPLE:
 - RASTREA2R.EXE YARA-DISK "C:\PROGRAM FILES" HTTP://LOCALHOST EXAMPLE.YARA
 - *** "C:\PROGRAM FILES" -> PATH FOR DIRECTORY TO BE SCANNED
 - *** HTTP://LOCALHOST -> LOCATION OF THE RASTREA2R SERVER
 - *** EXAMPLE.YARA -> YARA RULE ON REST SERVER USED FOR MATCHING

Command Prompt

```
C:\Users\sbhat5\rastrea2r\src\dist>rastrea2r.exe yara-disk -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.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
```

YARA MEM

- EXAMPLE:
 - RASTREA2R.EXE YARA-MEM HTTP://LOCALHOST EXAMPLE.YARA
 - *** HTTP://LOCALHOST -> LOCATION OF THE RASTREA2R SERVER
 - *** EXAMPLE.YARA -> YARA RULE ON REST SERVER

Command Prompt

```
C:\Users\sbhat5\rastrea2r\src\dist>rastrea2r.exe yara-mem -h
DEBUG:root:Enabled Debug mode
usage: rastrea2r.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
```

CUSTOMIZING RASTREA2R

A MODULAR, COMMUNITY READY PLATFORM





FOLDERS

rastrea2r-server

.github

.venv

docs

examples

results

rules

src

rastrea2r_server

pycache

/* _init_.py

/* errors.py

rastrea2r.ini

/* services.py

/* user.py

rastrea2r_server.egg-info

tests

/* test_basic.py

/* test_routes.py

.coveragerc

.gitignore

.travis.yml

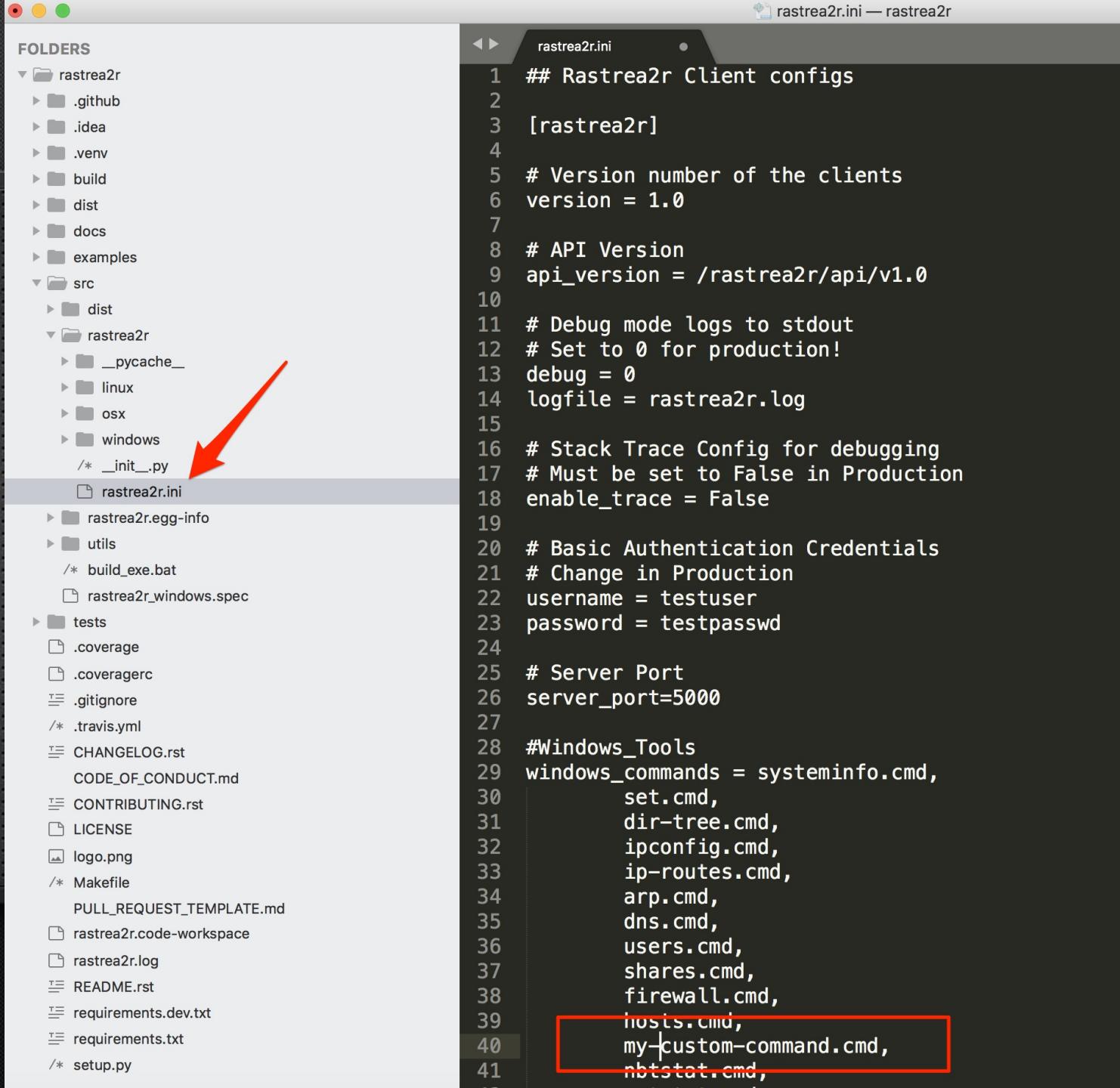
CHANGELOG.rst

rastrea2r.ini

```
1 ## Flask API Server Configuration File
2
3 [rastrea2r]
4 app_name = rastrea2r
5 port = 5000
6
7 # Debug mode logs to stdout and enable Flask debugging
8 # Set to 0 for production!
9 debug = 1
10
11 # Log file Location
12 logfile = rastrea2r-server.log
13
14 # Location of the Credential Database
15 database = ../../rastrea2rdb.sql
16
17 # Location on the Server where the rule files will be stored
18 rules_location = rules
19
20 # Location on the server where the log files will be stored
21 results_location = results
22
23
```

RASTREA2R SERVER CUSTOMIZATIONS

RASTREA2R CLIENT CUSTOMIZATIONS



The image shows a file explorer window on a Mac OS X system. The left pane displays the project structure:

- rastrea2r (folder)
 - .github
 - .idea
 - .venv
 - build
 - dist
 - docs
 - examples
 - src (folder)
 - dist
 - rastrea2r (folder)
 - __pycache__
 - linux
 - osx
 - windows
 - /* __init__.py
 - rastrea2r.ini
 - rastrea2r.egg-info
 - utils
 - /* build_exe.bat
 - rastrea2r_windows.spec
 - tests
 - .coverage
 - .coveragerc
 - .gitignore
 - /* .travis.yml
 - CHANGELOG.rst
 - CODE_OF_CONDUCT.md
 - CONTRIBUTING.rst
 - LICENSE
 - logo.png
 - /* Makefile
 - PULL_REQUEST_TEMPLATE.md
 - rastrea2r.code-workspace
 - rastrea2r.log
 - README.rst
 - requirements.dev.txt
 - requirements.txt
 - /* setup.py

```
rastrea2r.ini
1 ## Rastrea2r Client configs
2
3 [rastrea2r]
4
5 # Version number of the clients
6 version = 1.0
7
8 # API Version
9 api_version = /rastrea2r/api/v1.0
10
11 # Debug mode logs to stdout
12 # Set to 0 for production!
13 debug = 0
14 logfile = rastrea2r.log
15
16 # Stack Trace Config for debugging
17 # Must be set to False in Production
18 enable_trace = False
19
20 # Basic Authentication Credentials
21 # Change in Production
22 username = testuser
23 password = testpasswd
24
25 # Server Port
26 server_port=5000
27
28 #Windows_Tools
29 windows_commands = systeminfo.cmd,
30         set.cmd,
31         dir-tree.cmd,
32         ipconfig.cmd,
33         ip-routes.cmd,
34         arp.cmd,
35         dns.cmd,
36         users.cmd,
37         shares.cmd,
38         firewall.cmd,
39         iosts.cmd,
40         my-custom-command.cmd,
41         nbtstat.cmd,
```

WHAT'S COMING – STAY TUNED!

- ABILITY TO CREATE BASELINES AND ANALYZE THEM...
- INIT METHOD TO INITIALIZE THE RASTREA2R TOOLS DOWNLOADS
- UNIFIED SINGLE RASTREA2R CLIENT FOR ALL PLATFORMS
- DOCKERIZED DEPLOYMENTS
- SUPPORT FOR HTTPS IN RASTREA2R SERVER
- ABILITY TO STORE THE SCAN AND TRIAGE RESULTS TO AWS CLOUD (S3 BUCKETS)
- INTEGRATION WITH ELK STACK WITH DASHBOARDS FOR MONITORING / HUNTING
- LDAP SUPPORT FOR RASTREA2R SERVER
- MORE DOCUMENTATION, VIDEOS AND TUTORIALS
- HELP US TO IDENTIFY NEW USE CASES & TOOLS TO INTEGRATE!