rastrea2r

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

rastrea2r

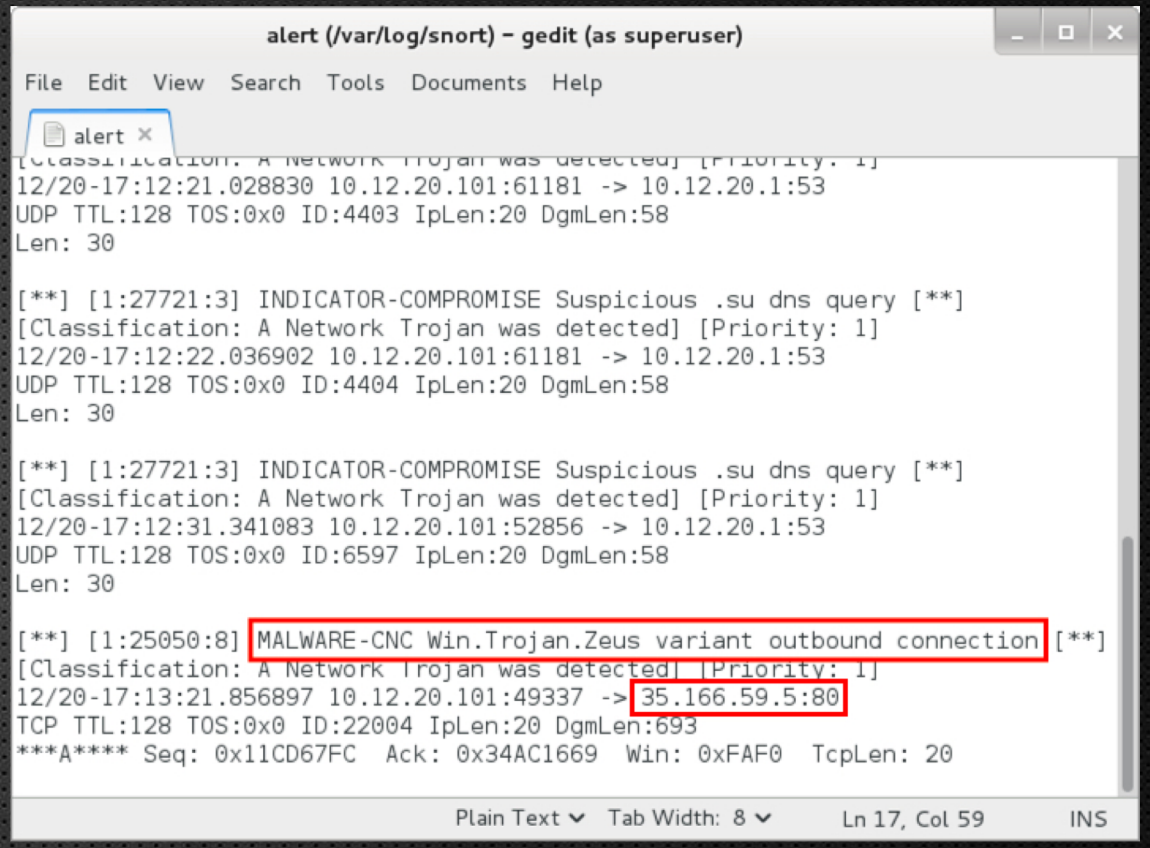
A DAY IN THE LIFE OF A SOC ANALYST

- 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?

rastrea2r

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?



TDS based Rig-V

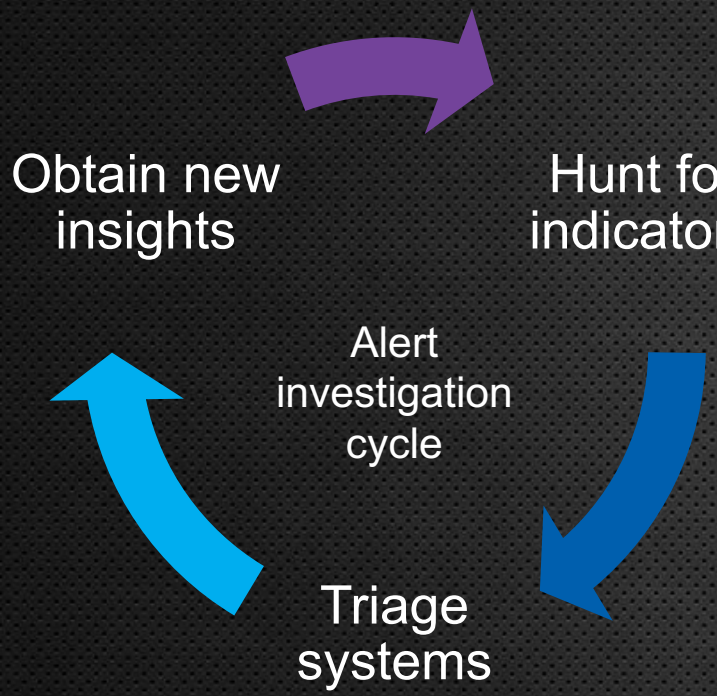
rastrea2r

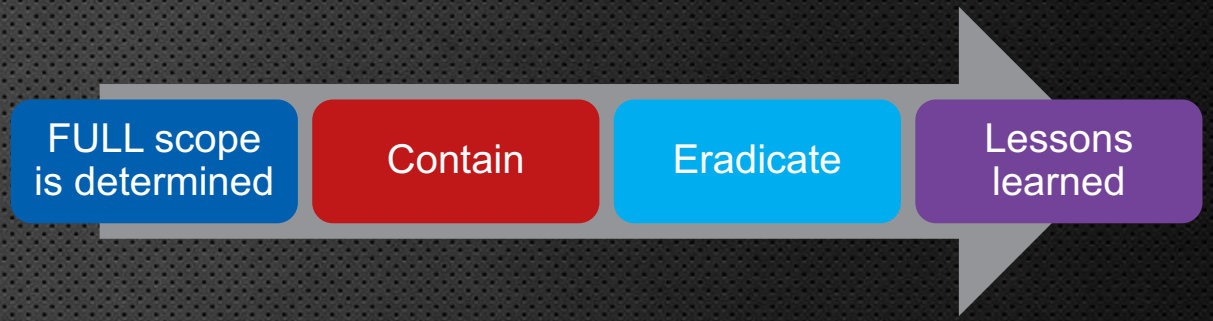
WHEN YOUR INCIDENT RESPONSE PROCESS IS SIMPLY…

REIMAGE THAT BOX !!!

rastrea2r

HUNTING & SMART INCIDENT RESPONSE



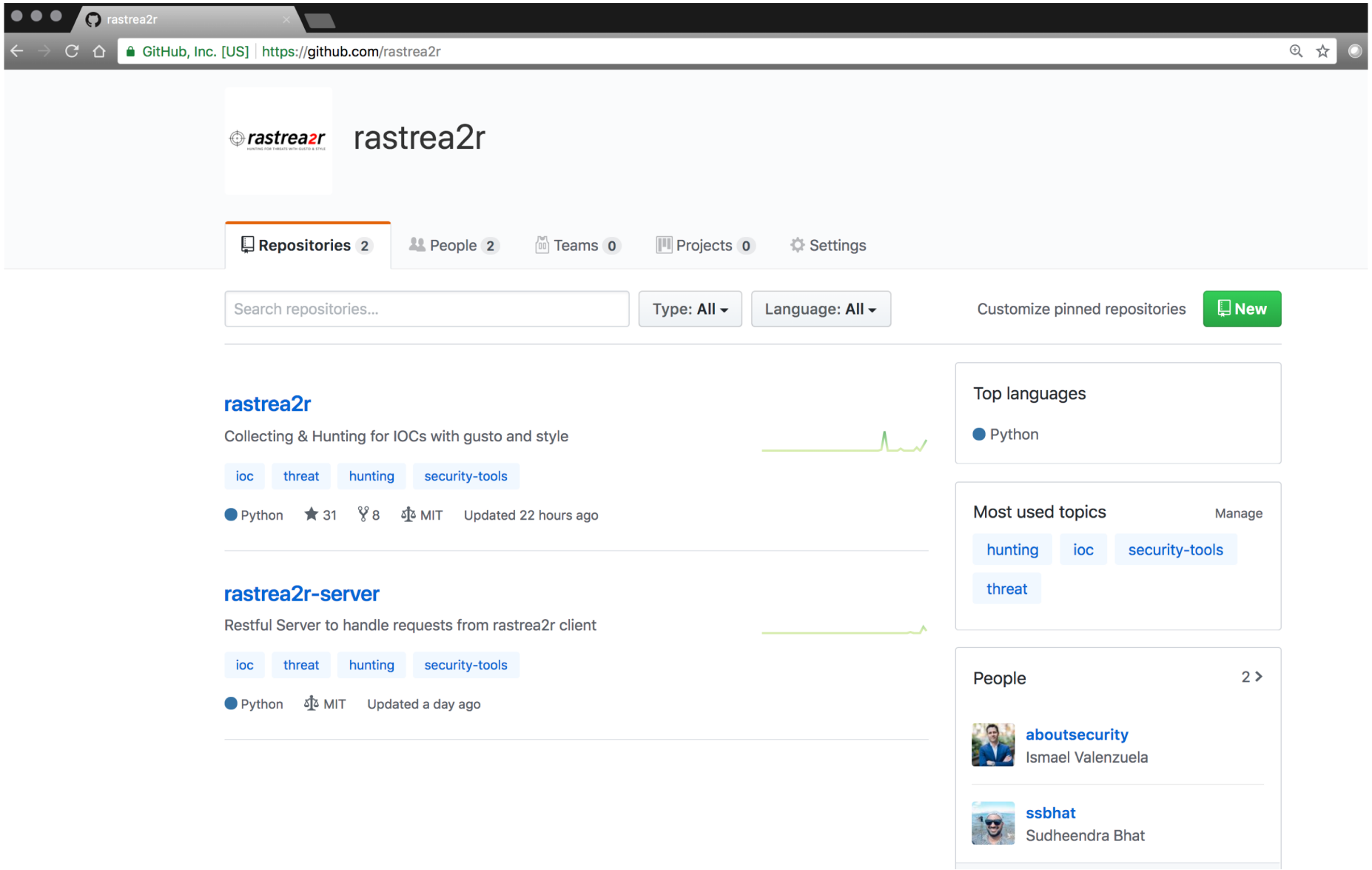


rastrea2r

SO HOW DO WE DO ALL OF THIS?

- **RASTREA2R** (PRONOUNCED *RASTREADOR*, *HUNTER* IN SPANISH):
  - 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 SYSINTERNALS, 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

rastrea2r


rastrea2r
GitHub, Inc. [US] | https://github.com/rastrea2r
rastrea2r
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
- ENHACED 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

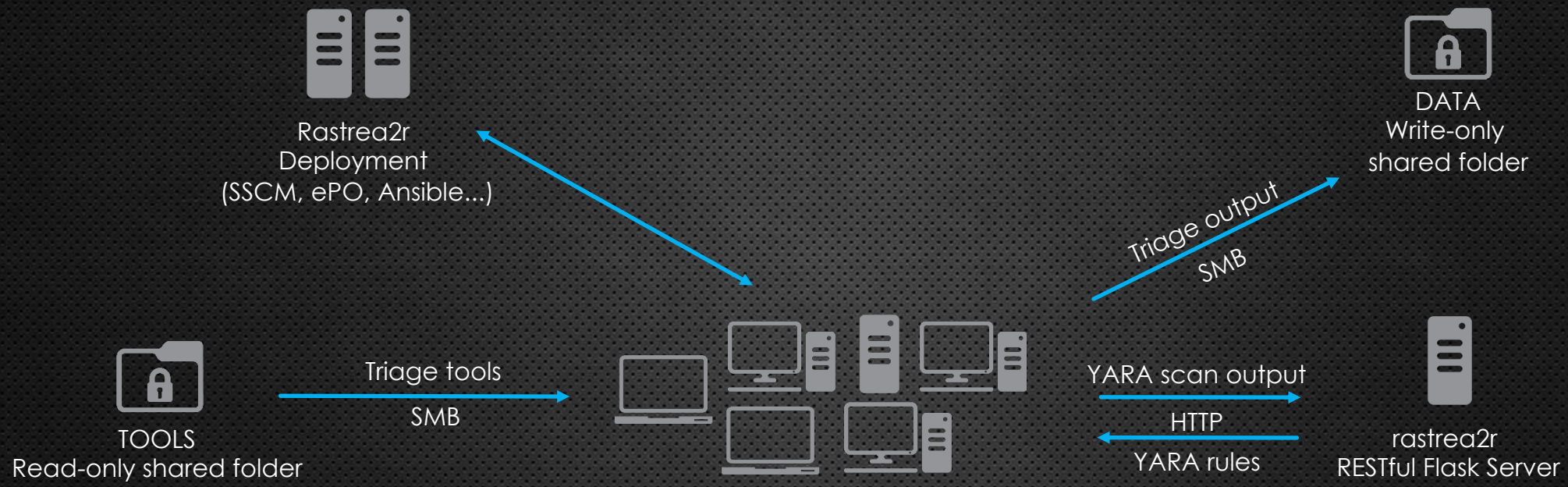
rastrea2r

CURRENT FUNCTIONALITY IN V1

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

rastrea2r

DEPLOYING RASTREA2R ON ENDPOINTS



rastrea2r

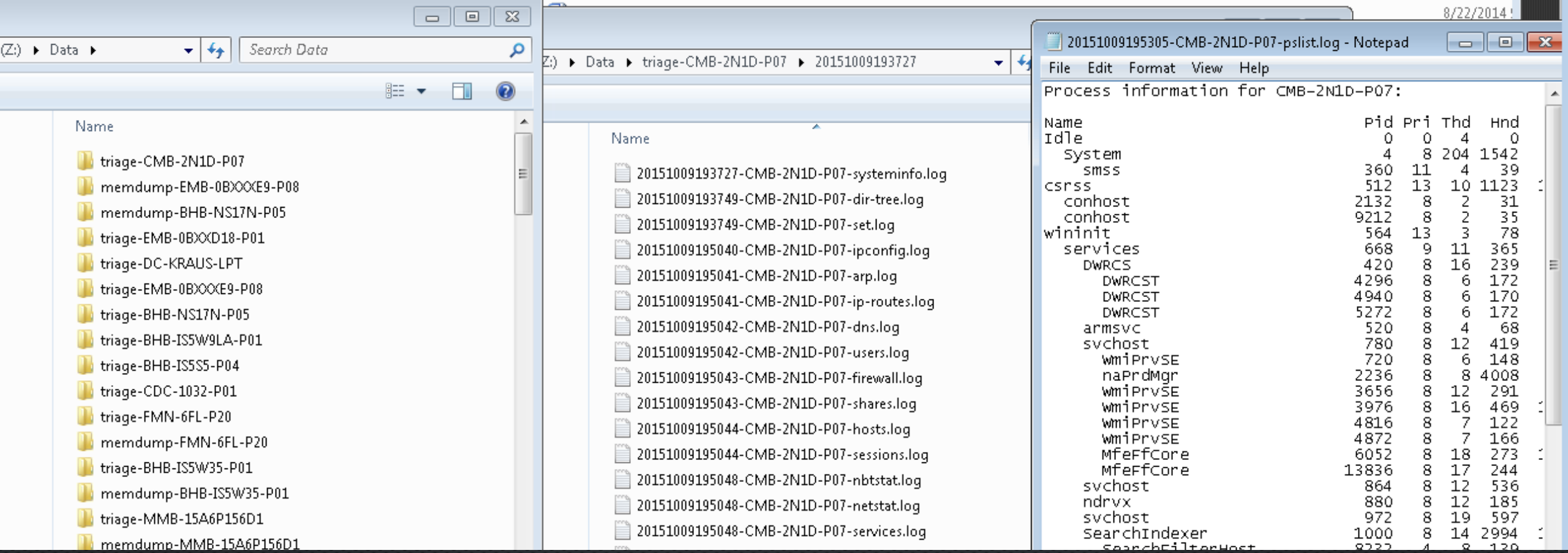
RASTREA2R COMMAND LINE & ARGUMENTS

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

rastrea2r



RASTREA2R IN ACTION – 15 MINUTES OF TRIAGE

rastrea2r

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>
```

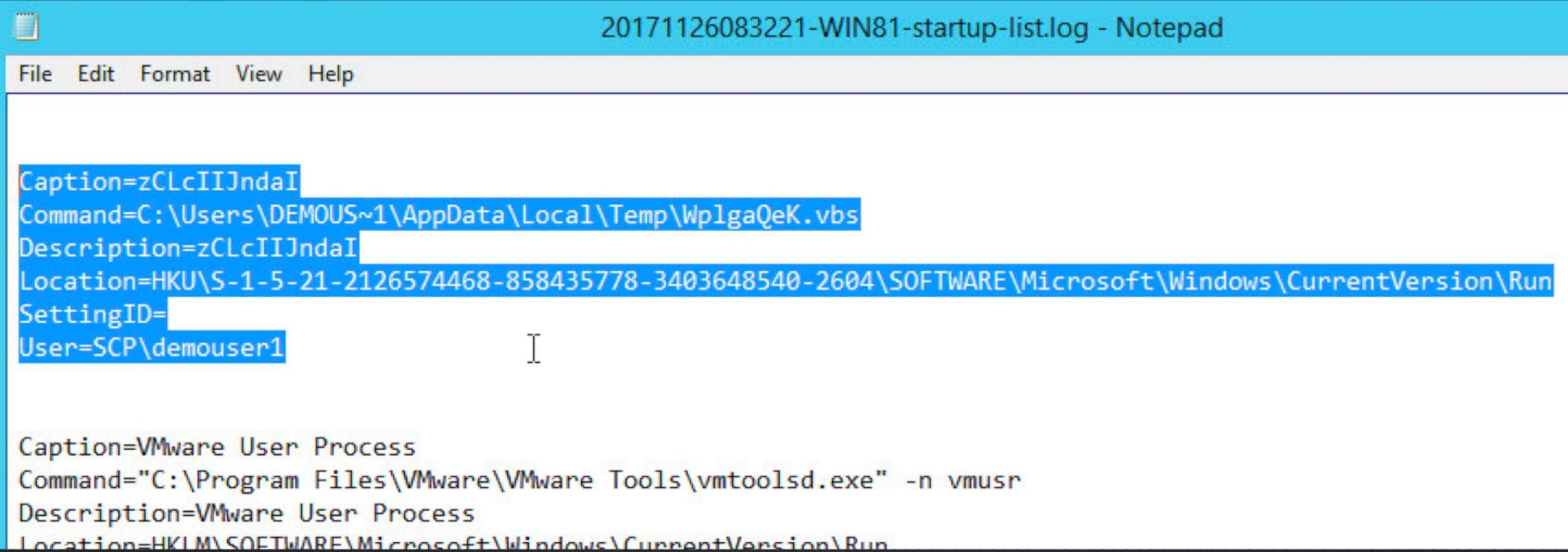
TRIAGING WITH RASTREA2R (SNAPSHOTS)

- EXAMPLE:
  - RASTREA2R.EXE TRIAGE *TOOLS.MYSERVER.COM DATA.MYSERVER.COM*

    *** TOOLS.MYSERVER.COM -> HAS A READ ONLY SHARED-FOLDER CALLED **TOOLS**

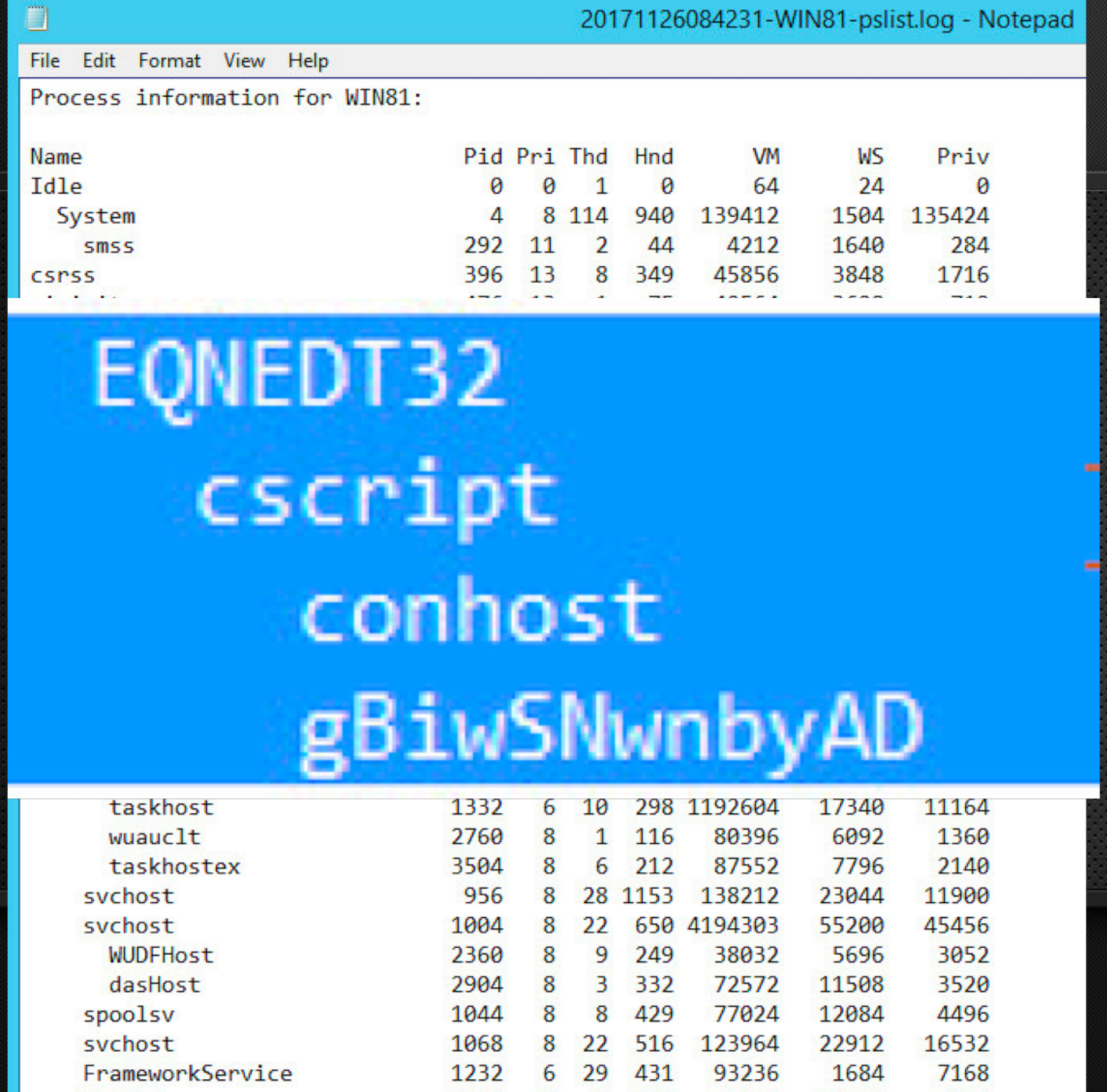
    *** DATA.MYSERVER.COM -> HAS A WRITE ONLY SHARED-FOLDER CALLED **DATA**

```
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
```

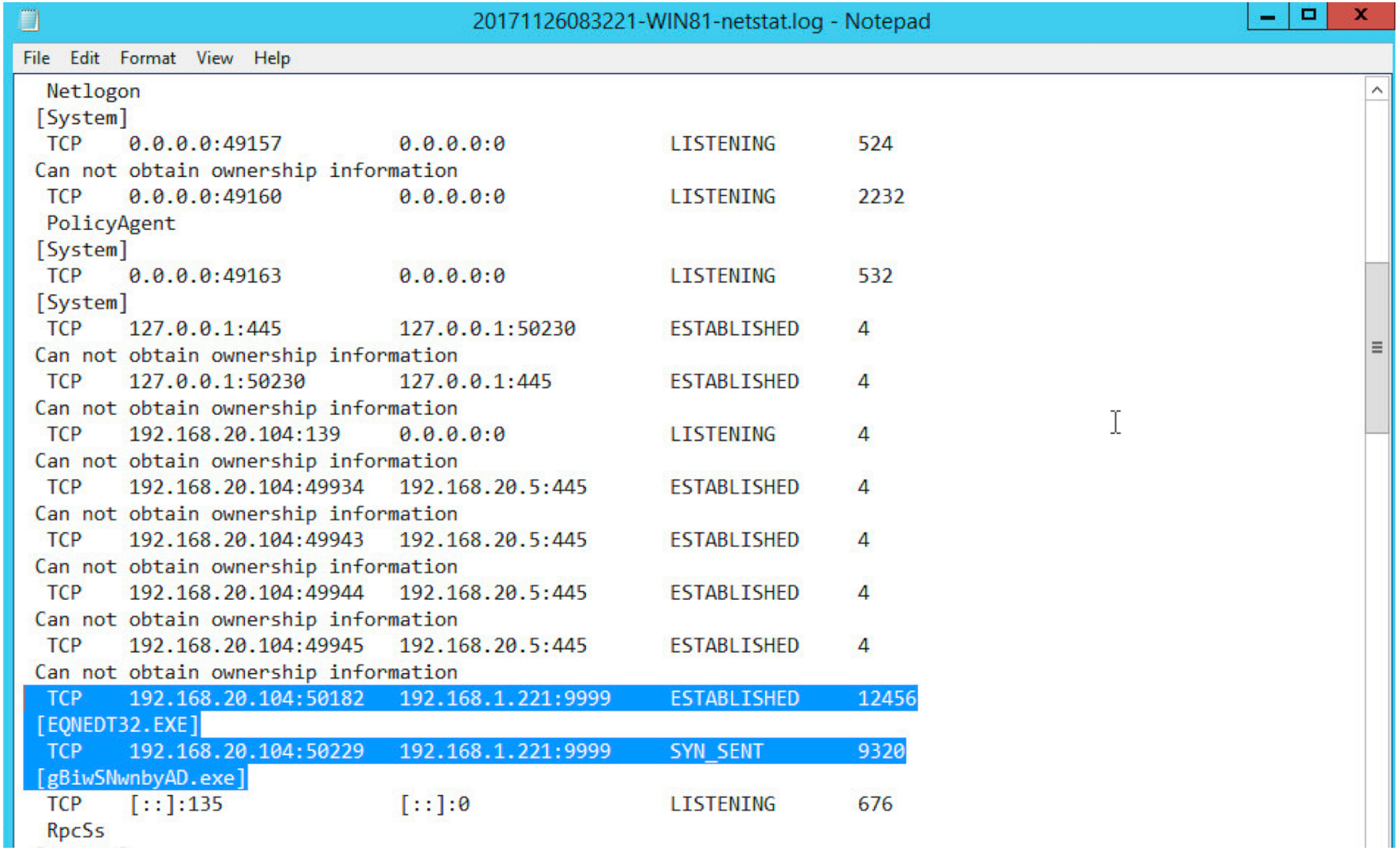


EVIDENCE OF PERSISTENCE - SYSINTERNALS STARTUP-LIST

rastrea2r


20171126084231-WIN81-pslist.log - Notepad
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

rastrea2r


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/Ix4UrfoN.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.dvtps.com/cfbc.htm?ifba=0&url=http%3A%2F%2Ftps10202.doubleverify.com%2Fevent.gif%3Fimpid%3D338cd6ba4b624974a2cd118f2f		11/26/2017 3:07	1		Internet Explorer 10/11 / Edge			177
139			11/26/2017 3:07	2		Internet Explorer 10/11 / Edge			64
140			11/26/2017 3:07	2		Internet Explorer 10/11 / Edge			44
141			11/26/2017 3:07	2		Internet Explorer 10/11 / Edge			39
142	http://52.179.101.199/favicon.ico		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
144			11/26/2017 3:08	1		Internet Explorer 10/11 / Edge			33
145			11/26/2017 3:12	4		Internet Explorer 10/11 / Edge			22
146			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 Sever 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 Sever

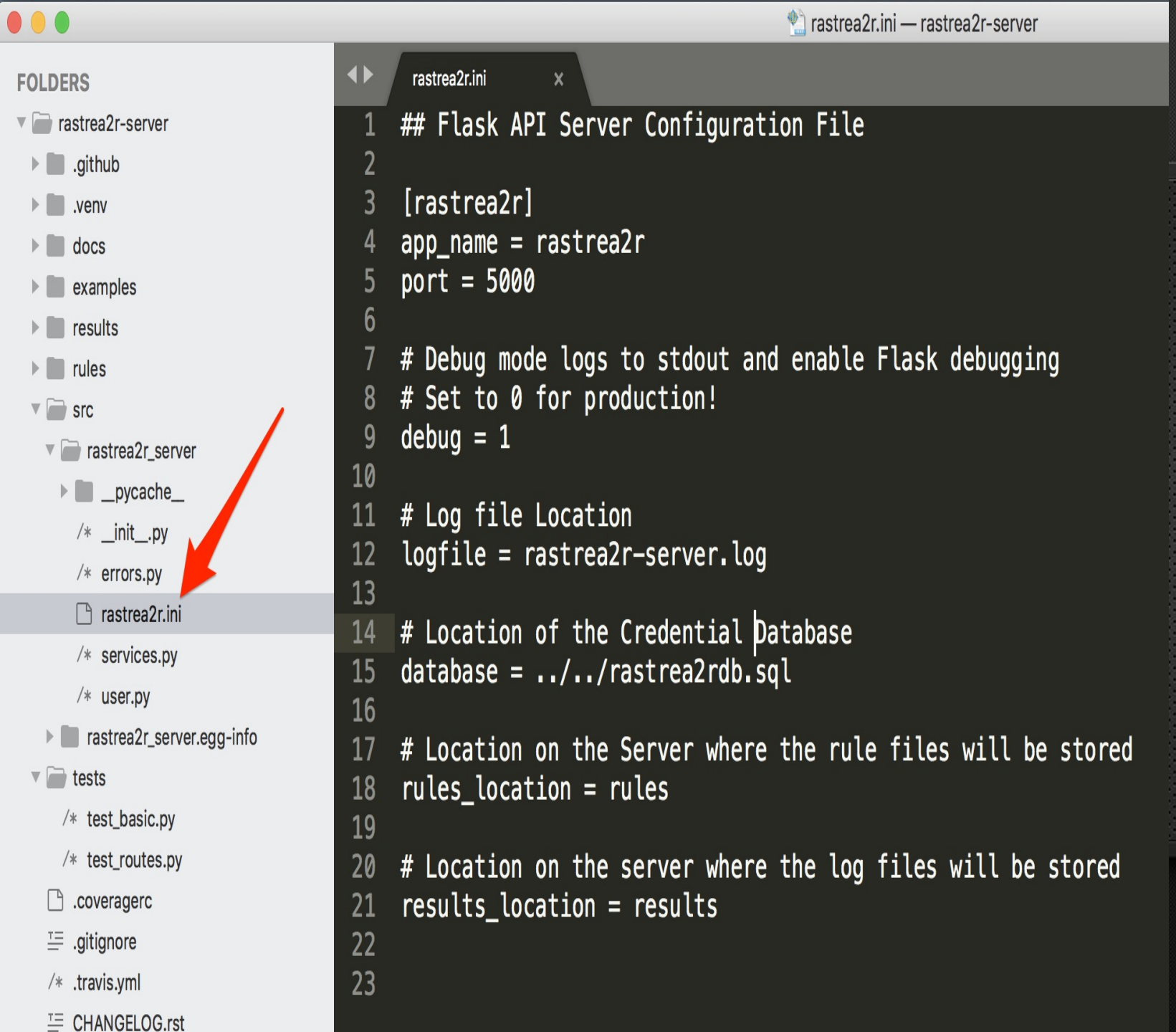
Command Prompt

```
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

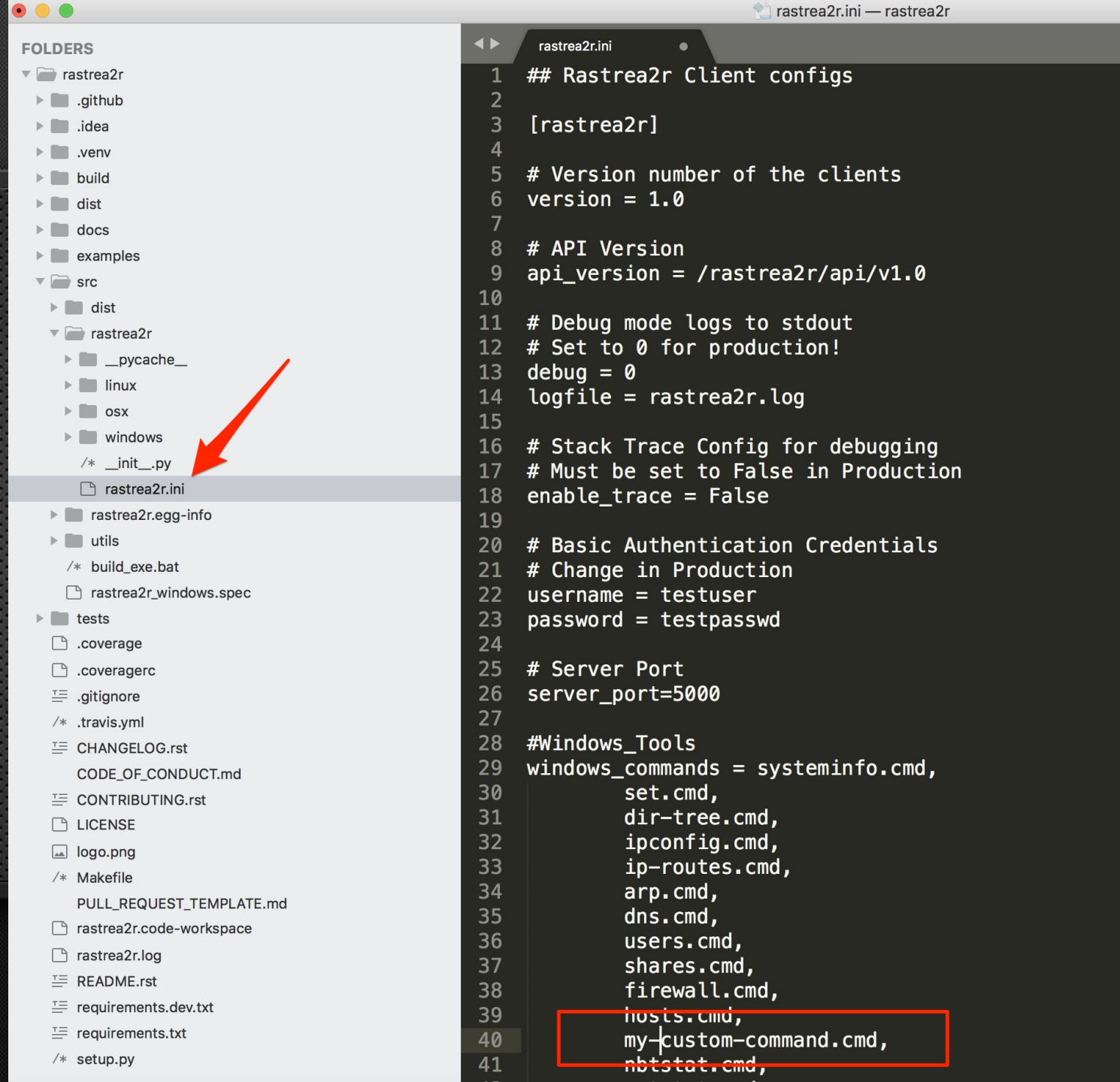
rastrea2r



RASTREA2R SERVER CUSTOMIZATIONS

rastrea2r

RASTREA2R CLIENT CUSTOMIZATIONS



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!

rastrea2r