

CALDERA

Information Security Inc.



Contents

- About CALDERA
- Architecture
- Requirements
- Testing Setup
- Installing CALDERA
- Running CALDERA
- References



About CALDERA

- CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks
- Blueteam => what can you detect and how fast can you handle it



Architecture

Server

- · Planner Decision engine allowing CALDERA to chose actions
 - Attacker Model Actions available based on ATT&CK
 - World Model Representation of the environment
- Execution Engine Drives actuation of techniques and updates the database
- · Database Stores knowledge learned about the environment
- HTTP Server

Clients

- · Agent Client on endpoint systems used for communication
- RAT Remote access tool used during operations to emulate adversary behavior





Requirements

- CALDERA only supports Windows Enterprise networks that are configured as a Windows Domain
- At a minimum this will contain a Domain Controller running Windows Server 2008 R2 through 2016 and two Windows Enterprise computers joined to that domain
- Because the techniques and tactics currently built into CALDERA are unique to Windows domains
- The CALDERA server can be installed on either Linux or Windows



Testing Setup





- CALDERA Server Installation on Windows 10
- Download the zip from github and unzip it

Clone with HTTPS ⑦

Use Git or checkout with SVN using the web URL.

https://github.com/mitre/caldera.git

Open in Desktop

Download ZIP

Ê



- CALDERA Server Installation on Windows 10
- Download the zip from github and unzip it





- CALDERA Server Installation on Windows 10
- Install Python 3.5.4 or later



- CALDERA Server Installation on Windows 10
- Upgrade to setuptools 24.0 or later





- CALDERA Server Installation on Windows 10
- Install Visual C++ 2015 Build Tools





Information Security Confidential - Partner Use Only

- CALDERA Server Installation on Windows 10
- Install Visual C++ 2015 Build Tools





Information Security Confidential - Partner Use Only

- CALDERA Server Installation on Windows 10
- Install Python libraries

<u>C:\Users\User3\Downloads</u>caldera-master\caldera-master\caldera>pip3 install -r requirements.txt Collecting aiohttp==2.3.9 (†rom -r requirements.txt (line 1)) Using cached aiohttp-2.3.9-cp36-cp36m-win32.whl Collecting aiohttp-jinja2==0.14.0 (from -r requirements.txt (line 2)) Using cached aiohttp jinja2-0.14.0-py3-none-any.whl Collecting antlr4-python3-runtime==4.7 (from -r requirements.txt (line 3)) Using cached antlr4-python3-runtime-4.7.tar.gz Collecting asn1crypto==0.24.0 (from -r requirements.txt (line 4)) Using cached asn1crypto-0.24.0-py2.py3-none-any.whl Collecting async-timeout==2.0.0 (from -r requirements.txt (line 5)) Using cached async timeout-2.0.0-py3-none-any.whl Collecting certifi==2017.11.5 (from -r requirements.txt (line 6)) Using cached certifi-2017.11.5-pv2.pv3-none-anv.whl Collecting cffi==1.11.4 (from -r requirements.txt (line 7)) Using cached cffi-1.11.4-cp36-cp36m-win32.whl Collecting chardet==3.0.4 (from -r requirements.txt (line 8)) Using cached chardet-3.0.4-py2.py3-none-any.whl Collecting cryptography==2.1.3 (from -r requirements.txt (line 9)) Using cached cryptography-2.1.3-cp36-cp36m-win32.whl Collecting idna==2.6 (from -r requirements.txt (line 10)) Using cached idna-2.6-pv2.pv3-none-anv.whl



- CALDERA Server Installation on Windows 10
- Install MongoDB





- CALDERA Server Installation on Windows 10
- Install MongoDB





- CALDERA Server Installation on Windows 10
- Install OpenSSL

(https://slproweb.com/products/Win32OpenSSL.html)





- CALDERA Server Installation on Windows 10
- Add OpenSSL to PATH => C:¥WINDOWS¥system32>setx path "%path%;C:¥OpenSSL-Win32¥bin"



- CALDERA Server Installation on Windows 10
- Start MongoDB => If getting the following error (NonExistentPath: Data directory C:¥data¥db¥ not found., terminating manually) create the folder

C:\Program Files\MongoDB\Server\3.6\bin:	mongod.exebi	nd_ip 127.0.0.1replSet caldera
2018-02-05T04:55:10.463-0800 I CONTROL	[initandlisten]	MongoDB starting : pid=8784 port=27017 dbpath=C:\data\db\ 64-bit
host=DESKTOP-IHQN9S5		
2018-02-05T04:55:10.463-0800 I CONTROL	[initandlisten]	targetMinOS: Windows 7/Windows Server 2008 R2
2018-02-05T04:55:10.467-0800 I CONTROL	[initandlisten]	db version v3.6.2
2018-02-05T04:55:10.467-0800 I CONTROL	[initandlisten]	git version: 489d177dbd0f0420a8ca04d39fd78d0a2c539420
2018-02-05T04:55:10.468-0800 I CONTROL	[initandlisten]	OpenSSL version: OpenSSL 1.0.1u-fips 22 Sep 2016
2018-02-05T04:55:10.469-0800 I CONTROL	[initandlisten]	allocator: tcmalloc
2018-02-05T04:55:10.470-0800 I CONTROL	[initandlisten]	modules: none
2018-02-05T04:55:10.471-0800 I CONTROL	[initandlisten]	build environment:
2018-02-05T04:55:10.472-0800 I CONTROL	[initandlisten]	distmod: 2008plus-ssl
2018-02-05T04:55:10.472-0800 I CONTROL	[initandlisten]	distarch: x86_64
2018-02-05T04:55:10.472-0800 I CONTROL	[initandlisten]	target_arch: x86_64
2018-02-05T04:55:10.473-0800 I CONTROL	[initandlisten]	<pre>options: { net: { bindIp: "127.0.0.1" }, replication: { replSet:</pre>
"caldera" } }		
2018-02-05T04:55:10.474-0800 I STORAGE	[initandlisten]	exception in initAndListen: NonExistentPath: Data directory C:\d
ata\db\ not found., terminating		
2018-02-05T04:55:10.475-0800 I CONTROL	[initandlisten]	now exiting
2018-02-05T04:55:10.482-0800 I CONTROL	[initandlisten]	shutting down with code:100



- CALDERA Server Installation on Windows 10
- Start MongoDB => If getting the following error (NonExistentPath: Data directory C:¥data¥db¥ not found., terminating manually) create the folder

PS C:\data\db> pwd Path ----C:\data\db



- CALDERA Server Installation on Windows 10
- Start MongoDB

C:\Program Files\MongoDB\Server\3.6\bin>mongod.exe --bind ip 127.0.0.1 --replSet caldera 2018-02-05T05:02:33.807-0800 I CONTROL [initandlisten] MongoDB starting : pid=4024 port=27017 dbpath=C:\data\db\ 64-bit host=DESKTOP-IHON9S5 2018-02-05T05:02:33.807-0800 I CONTROL [initandlisten] targetMinOS: Windows 7/Windows Server 2008 R2 2018-02-05T05:02:33.811-0800 I CONTROL [initandlisten] db version v3.6.2 [initandlisten] git version: 489d177dbd0f0420a8ca04d39fd78d0a2c539420 2018-02-05T05:02:33.812-0800 I CONTROL [initandlisten] OpenSSL version: OpenSSL 1.0.1u-fips 22 Sep 2016 2018-02-05T05:02:33.812-0800 I CONTROL 2018-02-05T05:02:33.813-0800 I CONTROL [initandlisten] allocator: tcmalloc 2018-02-05T05:02:33.814-0800 I CONTROL [initandlisten] modules: none 2018-02-05T05:02:33.814-0800 I CONTROL [initandlisten] build environment: [initandlisten] distmod: 2008plus-ssl 2018-02-05T05:02:33.815-0800 I CONTROL 2018-02-05T05:02:33.815-0800 I CONTROL [initandlisten] distarch: x86 64 2018-02-05T05:02:33.816-0800 I CONTROL [initandlisten] target arch: x86 64 2018-02-05T05:02:33.816-0800 I CONTROL [initandlisten] options: { net: { bindIp: "127.0.0.1" }, replication: { replSet: "caldera" } }



- CALDERA Server Installation on Windows 10
- Install CraterMain.exe => It should be placed in: (C:¥Users¥User3¥Downloads¥caldera-master¥calderamaster¥dep¥crater¥crater¥CraterMain.exe) on the computer that the CALDERA server is installed on





• Start the CALDERA server

C:\Users\User3\Downloads\caldera-master\caldera-master\caldera>openssl req -new -x509 -days 3652 -nodes -out conf/cert.
pem -keyout conf/key.pem
Generating a 2048 bit RSA private key
+++
writing new private key to 'conf/key.pem'
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HOME
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
C:\Users\User3\Downloads\caldera-master\caldera-master\caldera>python caldera.py
DEBUG:app.server:Planner has started
DEBUG:asyncio:Using selector: SelectSelector
INFO:app.server:Creating new user: admin
DEBUG:asyncio:Using selector: SelectSelector
INFO:app.server:Serving on 0.0.0.0:8888



- Login to the Caldera server => username: admin
- password: caldera





- Login to the Caldera server => username: admin
- password: caldera





- CALDERA Agent Installation
- The CALDERA Agent or cagent, is installed on every computer participating in the Adversary Emulation
- It should be accessible over the network to the CALDERA server
- Install the Visual C++ Redistributable for Visual Studio 2015





- CALDERA Agent Installation
- Download the latest release of cagent(<u>https://github.com/mitre/caldera-agent/releases</u>)
- Place cagent.exe in the desired installation location (the recommended location is C:¥Program Files¥cagent¥cagent.exe)

C:\Program	Files>	cd cage	ent	
C:\Program Volume in Volume Ser	Files\ drive rial Nu	cagent> C has n mber is	dir 10 label. 20EA-5461	
Directory	of C:\	Program	n Files∖cagent	
02/05/2018	06:22	PM	<dir></dir>	
02/05/2018	06:22	PM	<dir></dir>	
02/05/2018	06:15	PM	8,645,543	3 cagent.exe
	1	File(s)	8,645,54	13 bytes
	2	Dir(s)	40,916,103,10	58 bytes free



- CALDERA Agent Installation
- In the same directory, place the conf.yml file which can be downloaded from the CALDERA server by navigating to https://192.168.10.101:8888/conf.yml

conf - WordPad								
View								
ourier New • 11 • A A*	- * 11 * A' 本 律律 田 * 語 * 🔛 🧭 🏧 👬 And At Police			C:\Program	C:\Program Files\cagent>dir			
ι <u>I</u> <u>abs</u> × _i x ⁱ <u>∠</u> • <u>A</u> •		Picture Paint Date and Insert	Select all	Volume in drive C has no label. Volume Serial Number is 20EA-5461				
Font	Paragraph	Insert	Editing					
+ 1	· · · · · · · · · · · · · · · · · · ·	1 • • • 1 • • • 1 • • • 2 • • •	3					
	url_r verif	root: https://192.168. Fy_hostname: false	10.101:8888	Directory	of C:\Progra	am Files\cager	it	
	cert:	BEGIN CERTIFICATE		02/05/2018	06:31 PM	<dir></dir>		
	MIID	nDCCAmygAwIBAgIJAP+zbx	VuF9qWMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV	02/05/2018	06:31 PM	<dir></dir>		
	BAYT	AkpQMQ0wCwYDVQQIDAR0QV	JEMRAwDgYDVQQHDAdLQVNISUJEMQ0wCwYDVQQR	02/05/2018	06:15 PM	8,645,5	43 cagent.exe	
	DARIT	C01FMRgwFgYDVQQDDA9ERVI	NLVE9QLU11UU45UzUwHhcNMTgwMjA1MTMzNDEx	02/05/2018	06:28 PM	1,4	45 conf.yml	
	WhoNB	4jgwMjA1MTMzNDExWjBXMQ	swCQYDVQQGEwJKUDENMAsGA1UECAwETkFSQTEQ		2 File(s	5) 8,646,	988 bytes	
	MA4GA	AlueBwwHS0FTSElcgTENMA	sGA1UECgwESE9NRTEYMBYGA1UEAwwPREVTS1RP		2 Dir(s)	38,504,660,	992 bytes free	



- CALDERA Agent Installation
- In an Administrator command prompt install cagent with "cagent.exe --startup auto install"

C:\Program Files\cagent>cagent.exe --startup auto install Installing service cagent Service installed



- CALDERA Agent
- In an Administrator command prompt start cagent with "cagent.exe start"

C:\Program Files\cagent>c Starting service cagent	agent.exe start		
Command Prompt			
C:\Users\Gaku2>tasklist /	fi "pid eq 300"		
Image Name	PID Session Name	Session#	Mem Usage
		==========	=======
cagent.exe	300 Services	0	35,856 K



- CALDERA Agent
- Agents that are connected to the CALDERA server are visible by checking the Debug>Connected Agents tab

CALDERA	🌢 Threat 🗸	A Networks -	😽 Operations 🗸	💠 Debug 🗸	
		Connecter	d Agents		
		IP	oleu. z		Hostname
		192.168.10.1	109		agent1.switch.nes
		192.168.10.1	111		agent2.switch.nes



- CALDERA Agent Installation
- Send remote commands to the remote host (Agent)





References

• CALDERA documentation https://caldera.readthedocs.io/en/latest/

 MongoDB https://www.mongodb.com/download-center#community

OpenSSL
https://slproweb.com/products/Win32OpenSSL.html

Caldera Crater
https://github.com/mitre/caldera-crater/releases

• Caldera Agent https://github.com/mitre/caldera-agent/releases

