Adversary Emulation using CALDERA

Pralhad Chaskar (@c0d3xpl0it)

Terms to know

- MITRE
- Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
- CALDERA

About MITRE

The MITRE Corporation's mission-driven team is dedicated to solving problems for a safer world. We are a not-for-profit company that operates multiple federally funded research and development centers (FFRDCs).

At MITRE, we work across the whole of government, through our FFRDCs and public-private partnerships, to tackle difficult problems that challenge the safety, stability and well-being of our nation. Our unique vantage point allows us to provide innovative, practical solutions for some of our nation's most critical challenges in defense and intelligence, aviation, civil systems, homeland security, the judiciary, healthcare, and cybersecurity.

Adversarial Tactics, Techniques & Common Knowledge

Welcome to ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

Windows Technique Matrix

Main page
Help
Contribute
References

Tactics
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Techniques
- Technique Matrix
- All Techniques
- Windows
- Linux
- macOS

Groups
- All Groups

Software
- All Software

Tools
- Printable version
- Permanent link

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Vulnerability	Execution through API	Browser Extensions	Data Encrypted	Connection Proxy
Application Shimming	AppInit DLLs	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Execution through Module Load	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Application Shimming	Component Firmware	Exploitation of Vulnerability	Network Share Discovery	Pass the Hash	Graphical User Interface	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	Bypass User Account Control	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	InstallUtil	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Browser Extensions	DLL Search Order Hijacking	DLL Search Order Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	LSASS Driver	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Change Default File Association	Exploitation of Vulnerability	DLL Side-Loading	Input Capture	Process Discovery	Remote File Copy	Mshta	Data from Removable	Exfiltration Over Physical Medium	Domain Fronting

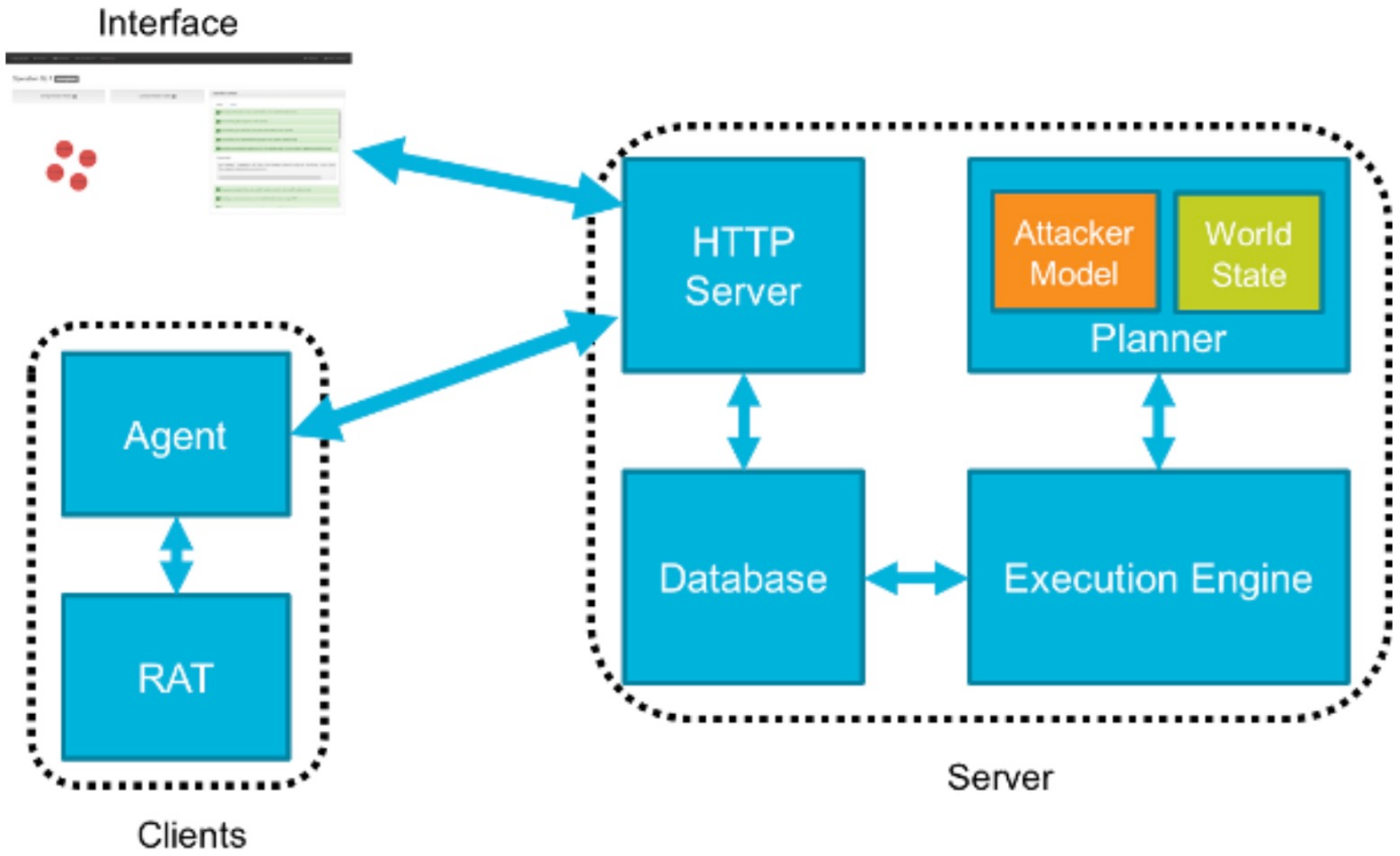
CALDERA

- CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. It generates plans during operation using a planning system and a pre-configured adversary model based on the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™) project.
- These features allow CALDERA to dynamically operate over a set of systems using variable behavior, which better represents how human adversaries perform operations than systems that follow prescribed sequences of actions.

Who needs CALDERA ?

- For Defenders who want to generate real data that represents how an adversary would typically behave within their networks.
- Defenders can get a glimpse into how the intrinsic security dependencies of their network allow an adversary to be successful

Architecture



mitre / caldera

An automated adversary emulation system

adversary-emulation caldera security-automation red-team mitre mitre-attack security-testing

21 commits | 1 branch | 0 releases | 3 contributors

dm-mitre committed on Jan 19 Documentation on how to add a Step. Latest commit e5f3e80 on Jan 19

caldera	Documentation on how to add a Step.	a month ago
docs	Documentation on how to add a Step.	a month ago
scripts	initial commit	3 months ago
.gitignore	initial commit	3 months ago
AUTHORS	initial commit	3 months ago
LICENSE	Update License so autodetect works	3 months ago
LICENSE-3RD-PARTY	initial commit	3 months ago
NOTICE	initial commit	3 months ago
README.md	Update README.md	a month ago
SECURITY.md	initial commit	3 months ago
build.py	initial commit	3 months ago


Start
DEMO

Reference

- https://github.com/mitre/caldera
- https://www.mitre.org/research/technology-transfer/open-source-software/caldera
- https://www.sprocketsecurity.com/blog/getting-started-with-mitre-caldera
- https://holdmybeersecurity.com/2018/01/13/install-setup-mitre-caldera-the-automated-cyber-adversary-emulation-system/