Megatron

Cyber Deception Framework

Megatron is an Air Force Research Laboratory (AFRL)-sponsored cyber deception framework as well as a catalog of deception techniques usable in that framework.

There is an asymmetry in cyber warfare which currently greatly benefits attackers over defenders. Specifically, attackers need only find a single vulnerability among a target's attack surface at a single point in time while defenders must defend the whole attack surface at all times. The application of deception to cyber defense is one of the few remaining areas of research with the potential to reduce this asymmetry.

Assured Information Security · 315.336.3306 · **WWW.AINFOSEC.COM**

AFRL THE AIR FORCE RESEARCH LABORATORY LEAD DISCOVER DEVELOP DELIVER

ais

Megatron

Cyber Deception Framework and Catalog

OVERVIEW

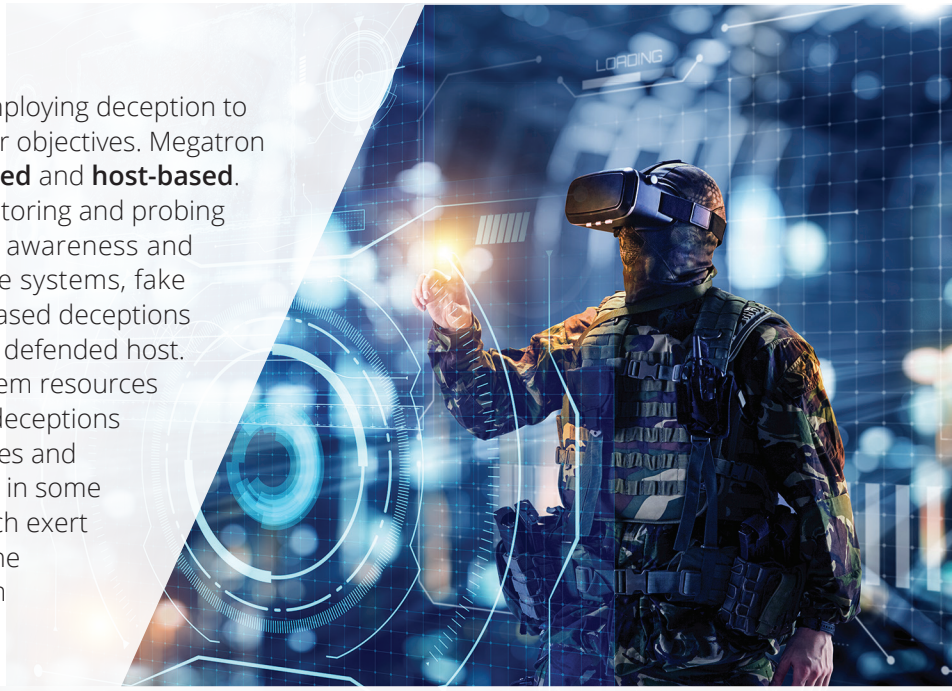
Deception can take many forms to reduce the asymmetry benefitting attackers. For example, data deceptions can place misleading yet highly realistic documents throughout a system on which sensitive documents reside. If attackers exfiltrate those documents, the fake nature of the data within them may cause attackers to waste resources if they put stock in them or to spend extra time and effort determining which ones are real and which are fake. They may also take the form of tripwires meant simply to alert defenders to the presence of attackers. Tripwires might be authentications to fake accounts for which there is no authorized use, access to specific files or interaction with dummy processes. Historically, attackers could count on replies from their network probes being genuine, even if they weren't illuminating. With deception, defenders can insert "honey" assets throughout the network, or items with no real purpose other than to serve as bait to attackers which notify administrators when they have been touched or accessed. This causes attackers to be discovered more often during their learning phase and to proceed with copious levels of caution when aware of deceptions.

KEY BENEFITS

- **Protect Critical Resources**
  Keep your organization's sensitive assets and knowledge out of attacker's hands.
- **Protect Production Systems**
  Deceptions can be applied not just to honeypot systems, but to those in production.
- **Mix & Match Deceptions**
  Create custom deception operations using hand-selected deception techniques.
- **Monitor Attackers**
  Megatron tracks attackers and monitors their activities.

Research Benefits

Megatron has been exploring various ways of employing deception to degrade attackers' effectiveness at achieving their objectives. Megatron deceptions fall into two categories: **network-based** and **host-based**. Network-based deceptions target attackers monitoring and probing the network as they attempt to gain situational awareness and to map out their next moves. Examples are fake systems, fake services, fake network vulnerabilities, etc. Host-based deceptions target attackers who have gained execution on a defended host. These attackers run applications and invoke system resources to view assets and to cause effects. Host-based deceptions intercept application requests to system resources and modify the returned data to mislead the attacker in some way. For example, Megatron has deceptions which exert total control over the list of running processes, the contents of the file system, the amount of system resources (CPU, RAM, disk, etc.), the contents of things like the Windows registry and others.

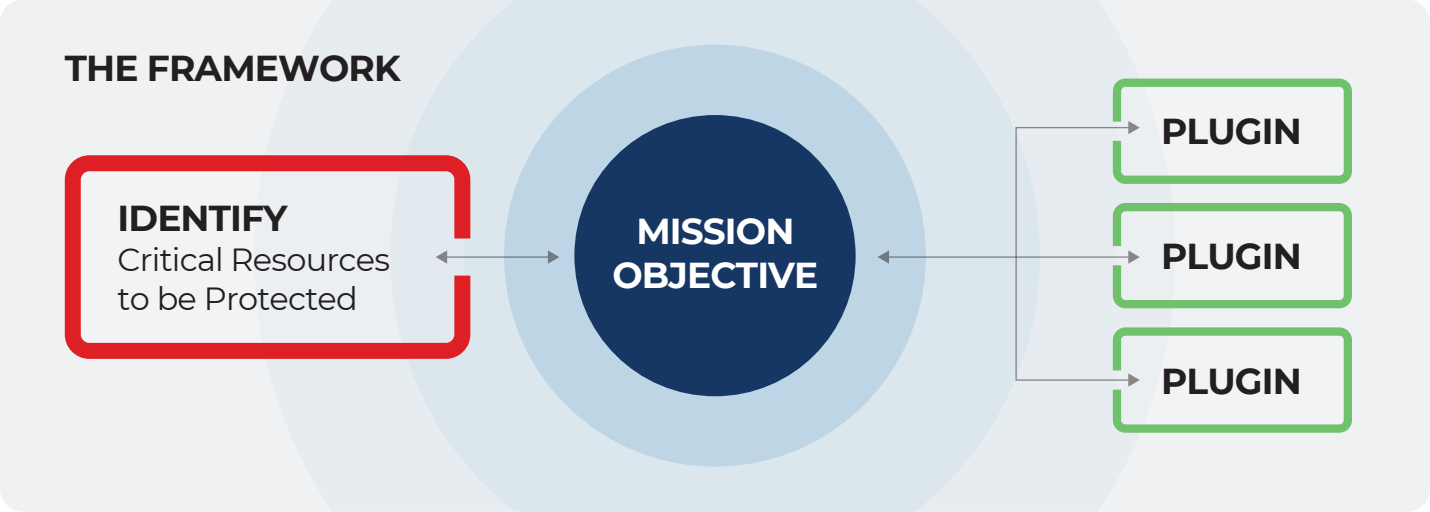


Below is a representative list of deceptions currently supported:

	TOOL NAME	DESCRIPTION
HW ARTIFACTS	**Windows Hardware Spoof**	Via the registry, hides entries in the installed hardware and drivers lists, such as mice, keyboards and network cards. (Essentially anything that appears in the list in the Windows Device Manager).
	CPU Spoof	Spoofs CPU utilization statistics, e.g., making it arbitrarily high or low.
	Memory Protect	Corrupts memory reads between processes.
FILE SYSTEM	**File Corrupt**	Checks file being written against a set of YARA rules. Matches are corrupted by replacing random bytes with random values.
	File Filter	Restricts access to files of a certain extension to a certain set of executables. Other executables are denied access.
	File Hide	Hides a file in the file system. Removes file from listings and reports the file as not existing when accessed.
	File Replace	Replaces a guest file with the content of one on the guest.
	File Change Cache	Protects a file from being overwritten, but caches changes to return in future attempts at reading the file.
	Fake File Delete	If a file is deleted, pretends to remove the file by removing it from listings and deny access, while leaving the file intact.
	File Redirect	If a protected file is accessed, the deception redirects the access to another file on the file system.
	File Trigger PoC	Reveals hidden text in the process list when there is an attempt to delete a certain file.
	File Tracker	Records processes that access numerous files.
OS ARTIFACTS	**Application Spoof**	Modifies the displayed information for installed applications, such as install date, icon and size. Can also remove entries.
	Registry Intercept	Intercepts and modifies registry events. Currently protects keys against being deleted and can replace data returned from queries.
	Fake Process Stop	If a process is stopped, pretends to have stopped the process by removing it from listings, while leaving the process intact.
	Event Log Modify Spoof	Protects the event log from being cleared.
	Password Protect	Protect/deceive attacks against password and hash extraction from memory.
	Process Hider	Hides a process from the process list.
NETWORK ACTIVITY	**Fake Network Nodes**	Fake the presence of multiple network nodes and services on the network.
	Netstat Spoof	Modifies output of the netstat command.
	Brute-Force Sesame	Detects attempts to brute force an SSH login on a Linux machine, and limits the offending address access to only fake accounts/limited accounts with weak passwords. These accounts can be logged into, but are merely fake accounts.
	Fake Device	Python script that listens for connections for certain devices, and pretends they exist by responding to ARP requests, scans, and connection attempts.
	FakeSMB	Fake presence of a Windows SMB share with complete file system.

The Framework

Megatron also consists of a framework for designing, deploying and managing deception operations. A deception operation is built around a mission objective, the identification of critical resources to be protected, and the selection of individual plugins – sensors and deceptions – which mislead attackers and prevent them from accessing the critical resources. A deception operation utilizes many deceptions – chosen by operators – which can coordinate their activities and share information using the Megatron message-passing infrastructure.



Third-Party Participation

A major design goal with the framework was to be able to accept plugins, such as sensors and deceptions, from third-parties. In this way, operators can import deceptions and capabilities from anyone with a useful contribution to deception. Megatron supports this by having established a public API which can be implemented by any third-party deception, and which gives Megatron the ability to de-conflict the plug-in with others already in the framework and to make it available for new deception operations.

FOR MORE INFORMATION

bd@ainfosec.com

Assured Information Security
315.336.3306
WWW.AINFOSEC.COM

About Assured Information Security (AIS)

AIS is a cyber and information technology company that plays a leading role in supporting critical cyber operations for the United States Department of Defense and Intelligence Community. AIS employs expert engineers and research scientists across the United States.