

# Cyber Threat / Active Net-Defense

## FEDERAL SOLUTION BRIEF

### Challenge

The threat of crippling attacks on government telecommunications and computer networks continues to rise sharply, with daily attacks now in the millions. Well funded and highly motivated adversaries continue to launch large and sophisticated cyber attacks with severe implications. The speed in which these organizations create new and more sophisticated attack vectors to elude U.S. defenses provides a tremendous challenge for our Cyber Warriors.

The diversity and sheer number of services running through both agency networks and the critical infrastructure present an enormous challenge for the agencies that are deploying and supporting them. With the massive increase in voice, video, data, and other network services supporting mission-critical government operations and critical infrastructure, investment in research and development (R&D) is significant. This is aimed at improving the security of both existing deployed technologies, and new and emerging systems. Other investments are focused on developing new and enhanced technologies for the detection and prevention of, and the response to, cyber attacks on the nation's critical information infrastructure.

To deal with these challenges, federal agencies are requesting billions of dollars dedicated to cyber security, infrastructure protection and information security. The U.S. is looking to deploy government-wide network intrusion detection systems along with the enablement of active defense capabilities to limit and prevent malicious activities. Agencies continue to deploy intelligent application-aware systems to ensure secure, service delivery. These systems include deep packet inspection (DPI) gateways, firewalls and unified threat management systems (UTMs).

To help agencies and their cyber teams to meet their operational goals, they must be able to accurately account for the efficacy of their Cyber Threat and Active Net-Defense systems to ensure they can:

- Effectively develop, validate, optimize, and deploy IDS/IPS rules while maintaining the performance standard
- Re-create threat scenarios to identify nefarious activity (e.g. Beacons, exfiltration)
- Maintain and manage threat variants
- Maintain operational awareness
- Perform emulation-based development

### Solution

The Mu Dynamics Cyber Suite is a commercial off-the-shelf (COTS) Cyber Threat and Active Net-Defense analysis solution that supports the efforts of cyber organizations from the floor analysts to the operations support and mission execution teams.

The Mu Cyber Suite provides a robust platform to help agencies analyze the efficacy of the IDS/IPS rule sets and to validate their impact on the overall infrastructure. With its unique ability to statefully recreate any nefarious activity across protocols of the OSI layers 2-7, agencies can develop, verify/validate and optimize rule sets while preventing performance degradation, to support the threat analysis development cycle.

Additionally, Mu Dynamics provides the ability to create variants of attack vectors to perform variability modeling and simulation to enhance the development, verification and validation of those analytics. The Mu solution extends the capability of Active Net-Defense by providing analyst and mission operations teams the unique ability to recreate exfiltration strategies, posing as both internal and external threats.

The following section describes these use-cases in more detail.



### Select Mu Federal Customers includes:



U.S. Air Force Information Operations Center (AFIOC)



U.S. Army Information Systems Engineering Command Technology Integration Center (TIC)



U.S. Marine Corps Tactical Systems Support Activity (MCTSSA)



U.S. Food and Drug Administration (FDA)



Numerous intelligence agencies

# USE –CASE #1

## Malware “Beaconing” Detection

One of the most significant challenges network security is facing is “beaconing detection”. Most organizations are infested with surreptitious malware, and once a desktop or server is infected it periodically “phones home” for additional downloads or instructions, and ultimately it may infiltrate protected data. This nefarious behavior makes for many significant challenges.

Additionally, the beacons are becoming more sophisticated, while remaining buried within exploited protocols of applications.

By using real traffic captures, the Mu Cyber Suite can statefully reproduce and emulate beaconing profiles in the test lab to help agencies verify and validate threat analytics and sensors. High scale application loads can also be applied as background traffic to emulate “hiding in plain sight”.

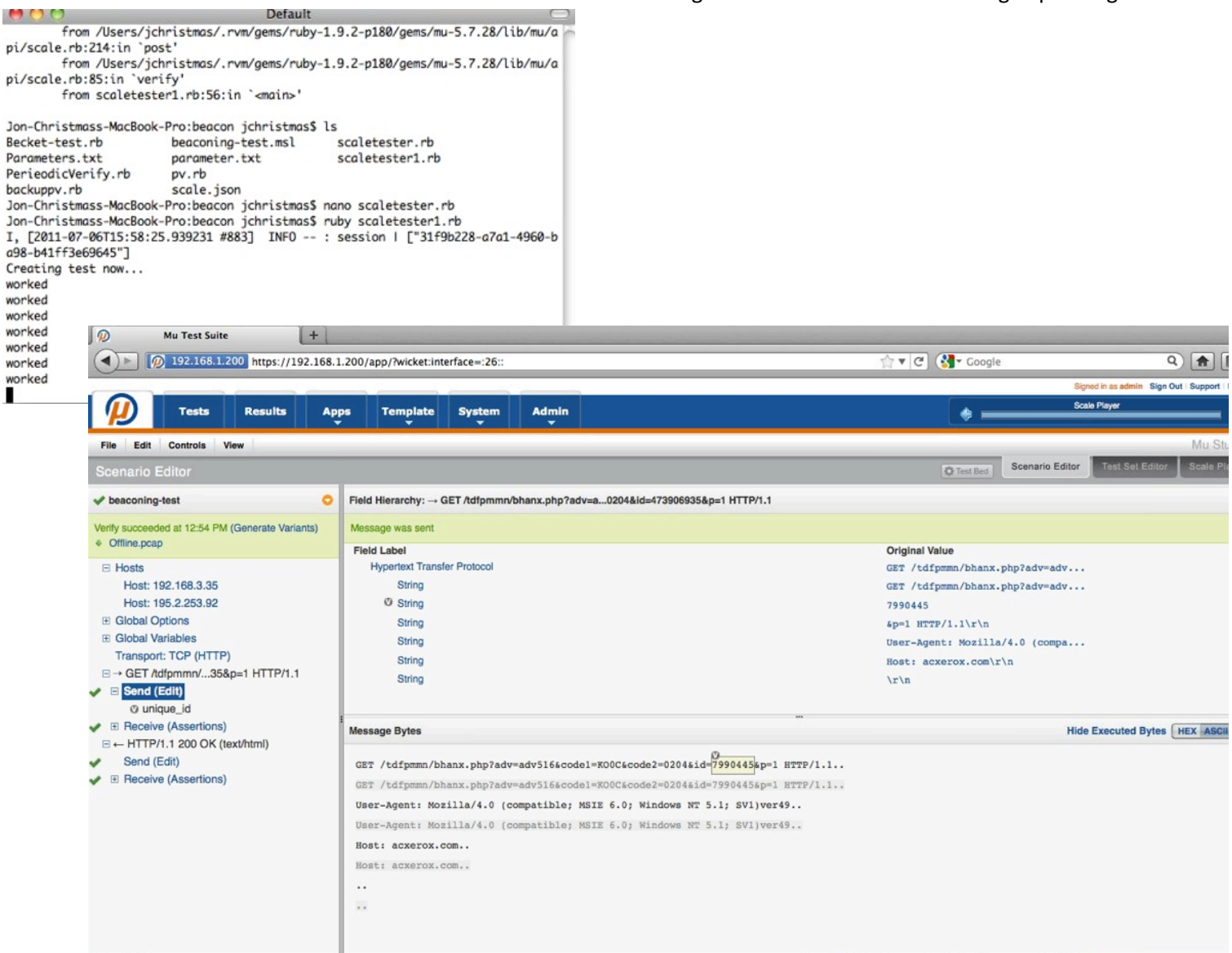


Fig. 1 - Mu Cyber Suite recreates beaconing profiles from real traffic captures to aid in detection validation



# USE –CASE #3 Exfiltration Detection

Exfiltration, or exportation, of data is usually accomplished by copying sensitive data from the trusted system via a network channel, or via remote access to applications.

The Mu Cyber Suite allows agencies to take a proactive approach to testing exfiltration analytics by using the agencies own service traffic to auto-generate tens of thousands of unique, relevant and stateful transactions using standard protocols from across the OSI Layers.

These protocols can be manipulated and exploited (e.g. leveraging the trusted reserved bits in MODBUS or optimization mechanisms like HTTP pipelining) to carry out the sensitive data as part of their interaction with applications, industrial control systems and other services.

By generating such real-life scenarios, analysts can exercise their exfiltration detection and threat analytics capabilities to take a proactive stance against this method of security exploitation.

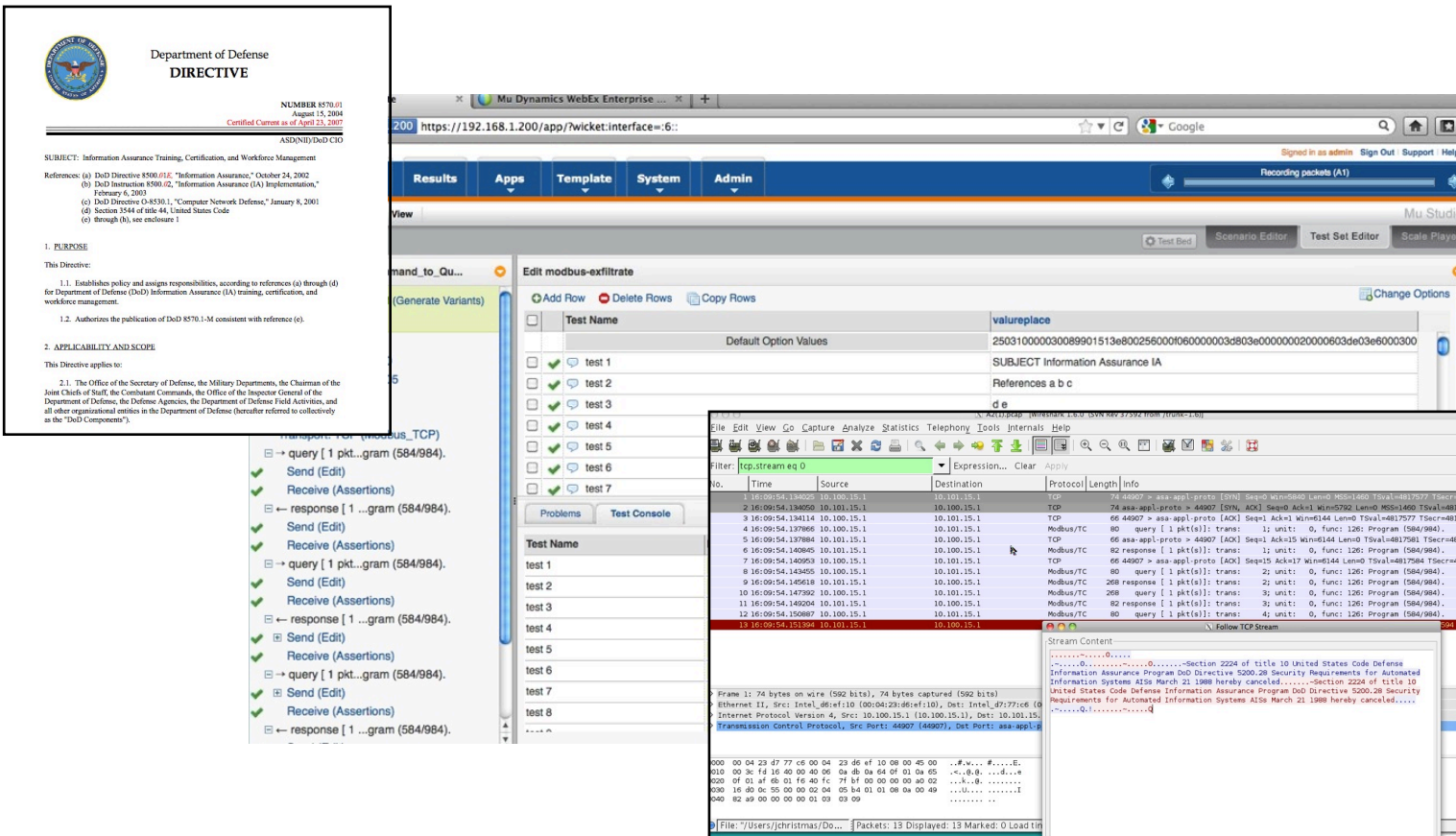


Fig. 3 - Mu Cyber Suite recreates stateful protocol transactions using exploits to exercise exfiltration detection capabilities

**Federal Sales Contact:**

Greg McDermott

e: [gmcdermott@mudynamics.com](mailto:gmcdermott@mudynamics.com)

o: 703-780-4272

c: 703-459-8813

Mu Dynamics solutions are available through a variety of procurement vehicles and resellers, including access to several government contract vehicles such as NASA SEWP and GSA Schedule 70.

Address : 686 W. Maude Avenue, Suite #104  
Sunnyvale, CA 94085

Phone: 866-276-4640

