ReSCIND Performer HSR Dataset Cover Sheet
Guarding Against Malicious Biased Threats (GAMBiT) HSR1

ReSCIND

Dataset Details

Dataset Title:	Guarding Against Malicious Biased Threats (GAMBiT) HSR1		
Dataset Citation:	GAMBiT HSR1 Dataset Citation TBD		
Data Format:	Available on S3 bucket, zip files	Data Size:	722.8 GB
Dates & Duration:	July 23, 2024 – September 14, 2024 Two 8-hour days per participant	Time Zone:	EST/EDT
How to access dataset:	Rachelle Thomas rthomas@bullsrungroup.com		
Point of contact for data questions:	Peggy Wu Peggy.Wu@rtx.com		

Description of Scenario

Objectives

This experiment was designed to identify and collect data around naturalistic attacker behaviors in a cyber range attack scenario to support the development of behavior classification methods.

Experiment Description

A two-day experiment was conducted with 19 red team participants, each attacking the network for the full duration. Attackers were provided guidance and access to the range in the beginning. Their further activities were self-paced. Key objectives were provided such as identify valuable targets and exfil important data. Participants were provided intermittent intelligence about the network, which they could choose to use. The cyber range contained 'triggers' or experimental stimuli, such as files with potential network user credentials that participants may or may not have encountered. Participants were asked to complete hourly and end of day surveys to describe their decision making and judgments throughout the day.

Experimental Results

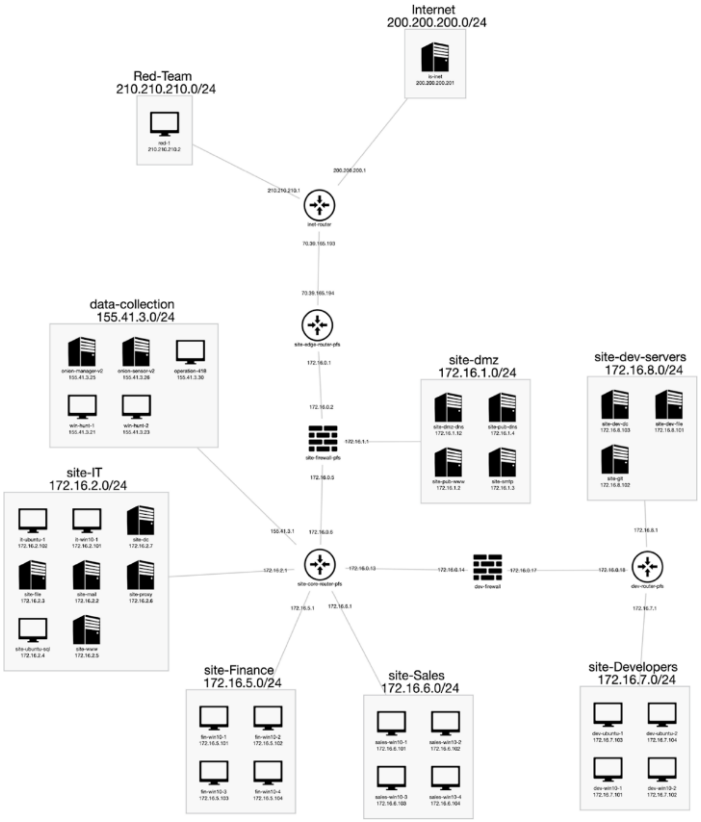
Analysis of cyber data, skills tests, self-reports, and operational notes found that higher-skilled individuals made more progress in cyber-attacks.

Cyber Environment

Experiment 1 used the SimSpace Cyber Force Platform to design and implement the GAMBiT cyber range, which simulated an enterprise business information system. This cyber environment comprised approximately 40 virtual devices organized into subnetworks, incorporating routers, switches, and user traffic commonly found in operational networks. Figure 1 illustrates the most recent network topology of the GAMBiT cyber range. Each participant operated within a designated cyber range and initiated all challenges using a virtual machine running Kali Linux.

The starting box was 10.10.0.5. Each participant had identical IP addresses within their assigned range, ensuring consistency across individual environments. The network included restricted subnets designated for managing the environment during the engagement, which were classified as no-strike targets. The experiment environment consisted of one range with seven triggers.

Image 1: Network topology for GAMBiT cyber range for Experiment 1, for reference only. Detailed network diagram and details about each host is included with the full dataset.



The following subnets were strictly off-limits and not to be scanned or accessed:

- 10.10.0.0/16
- 155.41.3.0/24
- 192.168.0.0/21
- 172.16.100.0/22
- 3.136.223.108

DATA

DATA SOURCES

Primary Data Sources

These data were collected directly from the cyber range experiment environment.

Category	Data Source	Examples of Select Data Features
Self Reports/Background Data *	Screening Questionnaire	Years of experience, type of cyber experience, team size, preferred OS, length of campaign.
	Demographics Questionnaire	Age, gender, native language, education level
Self Reports/Psychometric Data *	Cognitive Reflection Test (CRT)	3 multiple-choice items to assess the ability to override an intuitive but incorrect response and engage in more deliberate, analytical thinking. (Frederick, S. 2005)
	Big Five Inventory extra-short form (BFI-2)	15 items to indicate personality (Soto & John, 2017)
	General Risk Propensity Scale (GRiPS)	8 items on tendency to risky behaviors (Zhang et al., 2019)
	Adult Decision-Making Competence Scale (A-DMC)	Resistance to Framing Positive (7 items) & Negative (7 items) and Resistance to Sunk Cost (10 items) (Bruine de Bruin et al., 2007)
Self Reports/ Questionnaires	Applied Techniques	Hourly Stage reports (X.1-X.3): intended/applied MITRE ATT&CK techniques
	OPNOTES	CherryTree file with Operation Notes from participant.
Network Data	PCAP	Timestamps, source & destination packets & protocols, payloads
Network Data	NIDS - Suricata	Monitors network traffic for suspicious activities based on predefined rules

Kali Host Data	Keylog	Keylogger where each line records an individual keystroke. Particularly useful as it collects text that participants copy to their clipboard.
	Terminal histories	Bash and zsh histories, timestamps, order of commands

**Provide a citation for each psychometric assessment in the References section below.*

Derivative Data Sets

These datasets were created from aggregating, analyzing, curating, and labeling the source data.

Category	Data Source	Examples of Select Data Features
	Clean Log	Keylogger where each line records an individual keystroke. Particularly useful as it collects text that participants copy to their clipboard
		Result of running a post-processing script on Admin VM to remove certain keystrokes for better readability.

RESEARCH

Hypotheses

The GAMBiT HSR1 dataset was used to answer the following hypotheses:

[H1] Participant behaviors will be influenced by the presence of trigger associated with biases listed in table below.

[H2] Expert participants will perform better than open-division cyberattackers.

Bias	Descriptive Phrase	Indicators
Loss Aversion	Emotional weighting of outcomes.	Biased behaviors include prioritizing preserving what one already has instead of aiming for greater gains (endowment), such as focusing on found credentials
Base Rate Neglect	Statistical misjudgments	Biased behaviors include ignoring general statistics or probabilities such as access of valid admin credentials. Rational behaviors include testing account privileges.
Availability	Bias in memory and recall	Biased behaviors include making decisions based on what is easiest to remember or most recent in one's mind and overestimating the importance of rare but memorable events, such as recalling and attempting publicized Apache 2.4.50 vulnerability.
Confirmation Bias	Selective, belief driven data processing	Biased behaviors include seeking information that supports one's existing beliefs and dismissing evidence that does not align with one's initial assumptions, such as viewing failed attempts of found malformed SSH keys as "almost working" rather than as actual failures.
Sunk Cost	Effort-related persistence	Biased behaviors include continuing with a failing plan because one has already invested effort or resources, such as persisting in using commands despite repeated session termination, focusing on recovering their perceived process.

Publications

1. Shuo Huang, Frederick Jones, Nikolos Gurney, David Pynadath, Kunal Srivastava, Stoney Trent, Peggy Wu, and Quanyan Zhu (2024). PsybORG+: Modeling and Simulation for Detecting Cognitive Biases in Advanced Persistent Threats. In proceedings of 2024 IEEE Military Communications Conference (MILCOM). Washington, DC. Oct 28 to Nov 1, 2024.

References

1. Bruine de Bruin, W., Parker, A. M., & Fischhoff, B. (2007). Individual differences in adult decision-making competence. Journal of personality and social psychology, 92(5), 938.
2. Frederick, S. (2005). Cognitive reflection and decision making. Journal of Economic perspectives, 19(4), 25-42.
3. Soto, C. J., & John, O. P. (2017). Short and extra-short forms of the Big Five Inventory–2: The BFI-2-S and BFI-2-XS. Journal of Research in Personality, 68, 69-81.
4. Zhang, D. C., Highhouse, S., & Nye, C. D. (2019). Development and validation of the general risk propensity scale (GRiPS). Journal of Behavioral Decision Making, 32(2), 152-167.