RADAR: Real-time Advanced Detection and Attack Reconstruction

Sadegh M. Milajerdi, Md Nahid Hossain, Kiavash Satvat, Sutanu Kumar Ghosh, Rigel Gjomemo, R. Sekar, V.N. Venkatakrishnan

Stony Brook University

THE UNIVERSITY OF ILLINOIS AT CHICAGO

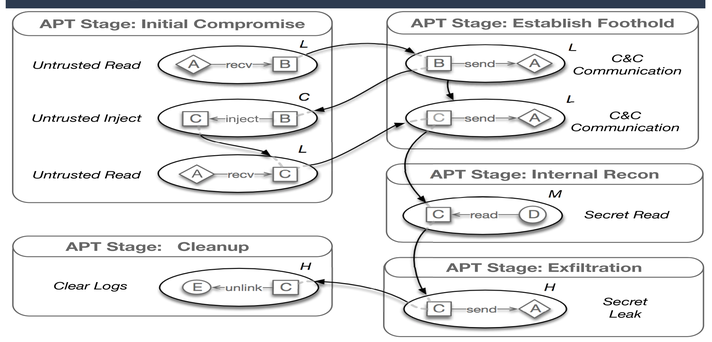
Approach

- Information-flow as a basis for alert correlation and campaign detection.
- Use alert correlation for attack campaign detection
- Use modeling of Tactics , Techniques, and Procedures to bridge semantic gap between APT stages and low-level system events
- Real-Time High-level attack reconstruction

Pay-Off

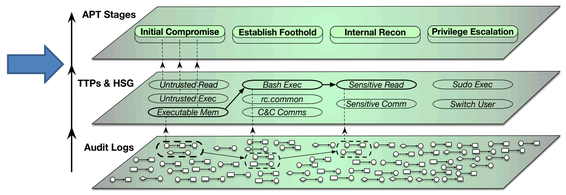
- Real time attack detection with high accuracy
- Very low rate of false positives
- Precise real-time high-level attack reconstruction
- Ability to focus detection on specific APT stages, if needed

High Level Attack Reconstruction

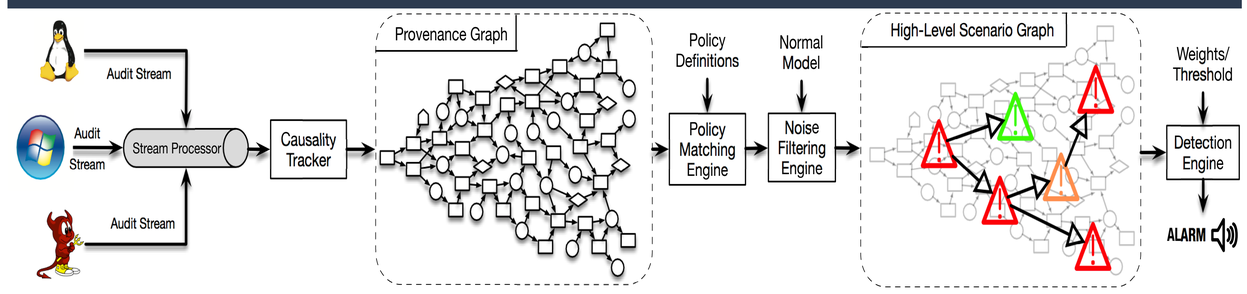


MITRE ATT&CK (Tactics, Techniques and Procedures)

Initial Access 10 items	Execution 33 items	Persistence 58 items	Privilege Escalation 28 items	Lateral Movement 17 items	Exfiltration 9 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	AppleScript	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Deployment Software	Data Compressed
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Distributed Component Object Model	Data Encrypted
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Exploitation of Remote Services	Data Transfer Size Limits
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Logon Scripts	Exfiltration Over Alternative Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Pass the Hash	Exfiltration Over Command and Control Channel
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Pass the Ticket	Exfiltration Over Other Network Medium
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Remote Desktop Protocol	Exfiltration Over Physical Medium
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Remote File Copy	Scheduled Transfer
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Remote Services	
	InstallUtil	Change Default File Association	File System Permissions Weakness	Replication Through Removable Media	
	Launchctl	Component Firmware	Hooking	Shared Webroot	
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	SSH Hijacking	
	LSASS Driver	Create Account	Launch Daemon	Taint Shared Content	
	Mshta	DLL Search Order Hijacking	New Service	Third-party Software	
	PowerShell	Dylib Hijacking	Path Interception	Windows Admin Shares	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Windows Remote Management	
	Regsvr32	File System Permissions Weakness	Port Monitors		



HOLMES Architecture



EXTRACTOR: Extracting Attack Behavior Graphs from Threat Reports

Kiavash Satvat, Rigel Gjomemo, V.N. Venkatakrishnan

Stony Brook University

THE UNIVERSITY OF ILLINOIS AT CHICAGO

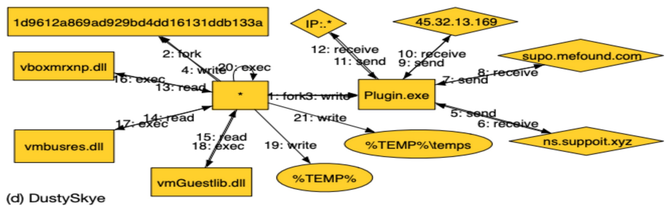
Problem

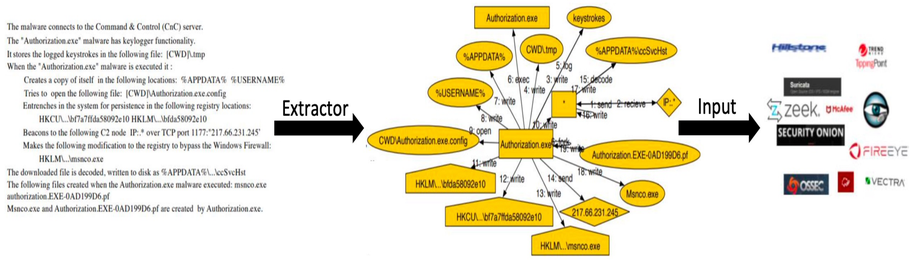
- Goal is to extract actionable provenance graphs of attack behavior from natural language CTI reports
- Actionable: Provenance graphs can be directly used to perform threat hunting
- Behavior: connected events and entities, not single IOCs

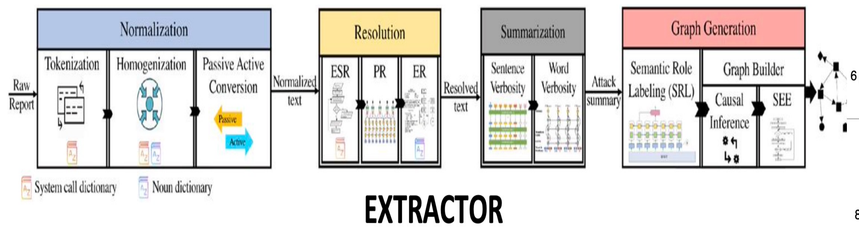
Approach

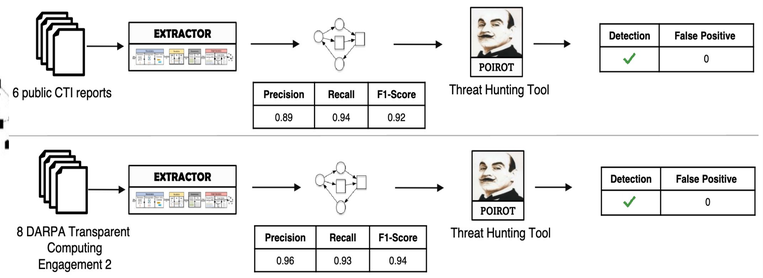
- CTI Language Complexities: Domain specific vocabulary, Ellipsis subjects and objects, Pronoun, Passive vs active
- Verbosity: Inter vs Intra verbosity
- Relationships Extraction (Subject, Verb, Object): Causality and flow of attack

Results Summary









Precision	Recall	F1-Score
0.89	0.94	0.92

Detection	False Positive
✓	0

Precision	Recall	F1-Score
0.96	0.93	0.94

Detection	False Positive
✓	0

Ostinato: Cross-host Attack Correlation through Attack Activity Similarity Detection

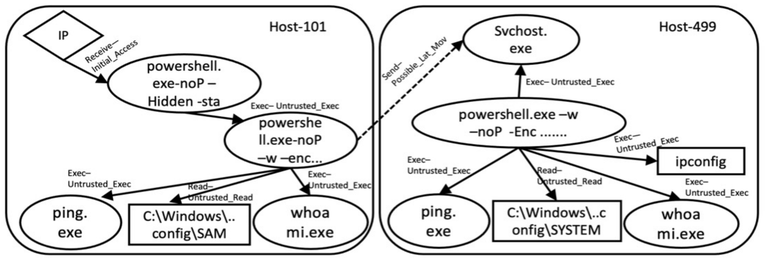
Sutanu Kumar Ghosh, Kiavash Satvat, Rigel Gjomemo, V.N. Venkatakrishnan

Stony Brook University

THE UNIVERSITY OF ILLINOIS AT CHICAGO

Problem

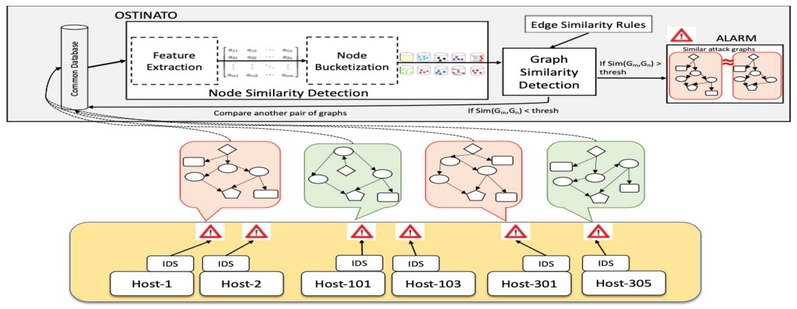
- How can we correlate alerts across hosts without relying on lateral movement detection in a network with hundreds of hosts?
- How can we obtain an additional suspicious signal related to correlation for SOC operators?



Approach

- Graph- and Similarity-based correlation from the attacker activities detected by the underlying IDS
- Identifying similar nodes: Node label content, Approximate node behavior
  - Usage of Feature Extraction and efficient Node Bucketization
- Identifying similar edges: Set of rules which matches edge similarity based on entity behavior
- Graph similarity algorithm: To compute the similarity between any pair of suspicious activities (graphs by IDS)
- Evaluated on OpTC-NCR2 dataset.

OSTINATO Architecture



Results Summary

- Correlated attacks in 21 distinct hosts missed by the underlying IDS
- Successfully correlated similar attacker behavior in Engagement-5 multi-host ssh campaign

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
June 1-2, 2022 | Alexandria, Virginia