Remote Access Toolkit Detection and Enrichment Platform (RATDEP)

Osric Nagle – Westwood High School – Austin, TX
Supervisors: Zachary Coker, Daniel Zhang – Signal and Information Sciences Laboratory – ARL:UT

Introduction

Advanced Persistent Threat (APT) groups are highly sophisticated hacking organizations that continue to threaten the cybersecurity landscape.

Often sponsored by nation states, APTs target defense contractors, financial institutions, and higher education facilities for sensitive data and personally identifiable information.

APTs utilize Remote Access Toolkits (RATs) to build exploitation payloads, obtain trusted command execution, establish backdoors, and exfiltrate data.

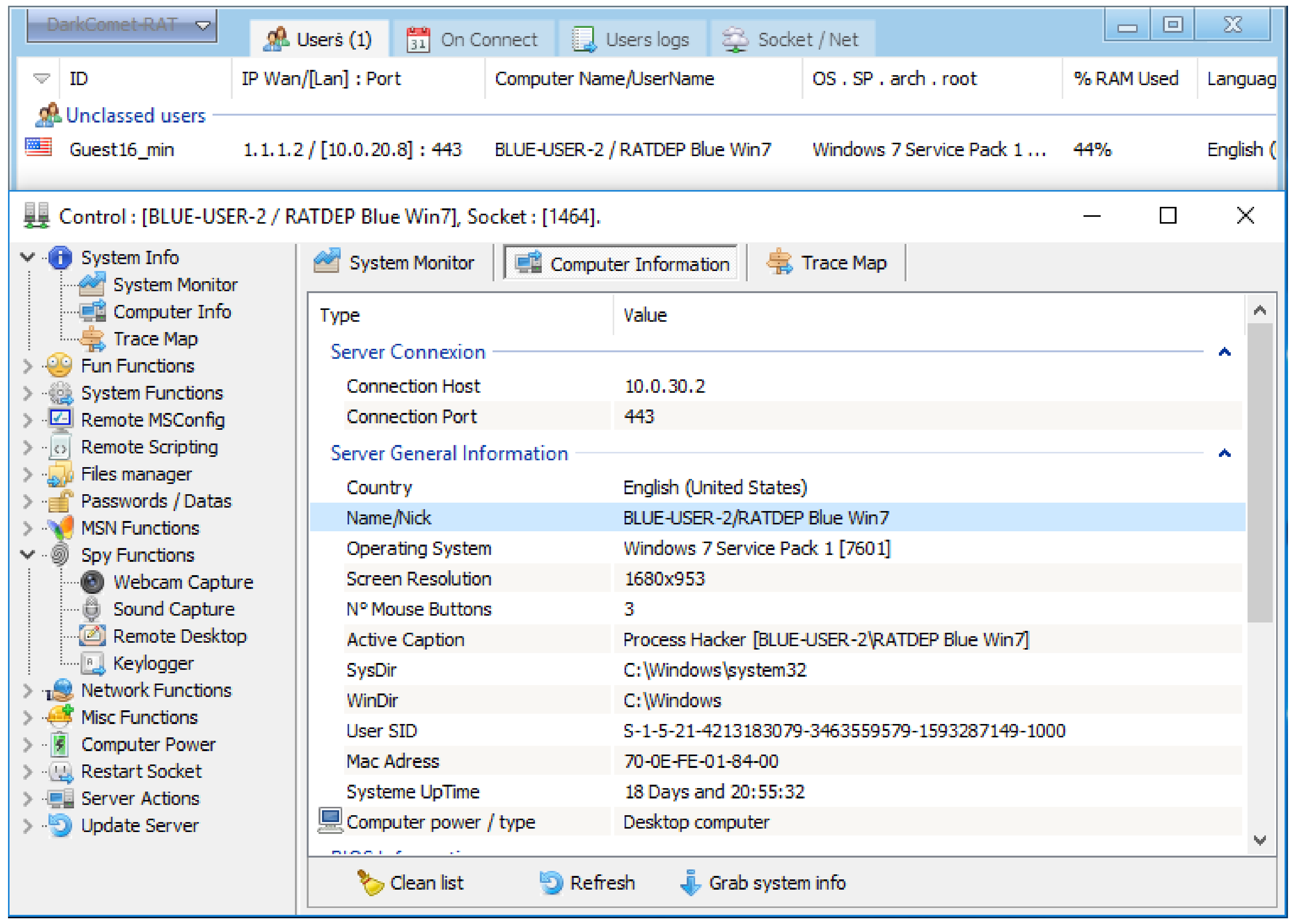
This research project is intended to explore the value of CASCADE as a tool to aggregate and analyze host-based logs for detecting RAT activity, versions, and families. In doing so, quicker identification and mitigation of RATs can occur, limiting potential damage to a targeted organization.

Methodologies

We created a malware lab to test RAT activity by building a network of attacker (red) and victim (blue) virtual machines within two ESXi servers. Each victim Windows VM was configured to collect Sysmon logs and forward them to the central logging server, which ran the ELK stack and CASCADE:

- System events create Sysmon log entries
- Winlogbeats forwards log entries to Logstash
- Logstash stores and converts log entries to the Cyber Analytic Repository (CAR) data model
- Elasticsearch aggregates logs and Kibana presents the data
- CASCADE analytics identify suspicious events and creates a visualization of captured activity

Offensive cyber operations were designed to evaluate CASCADE and identify needed analytics. Each operation plan emulated real-world APT activity by using specific malware samples, penetration testing tools, and methodologies attributed to that group.

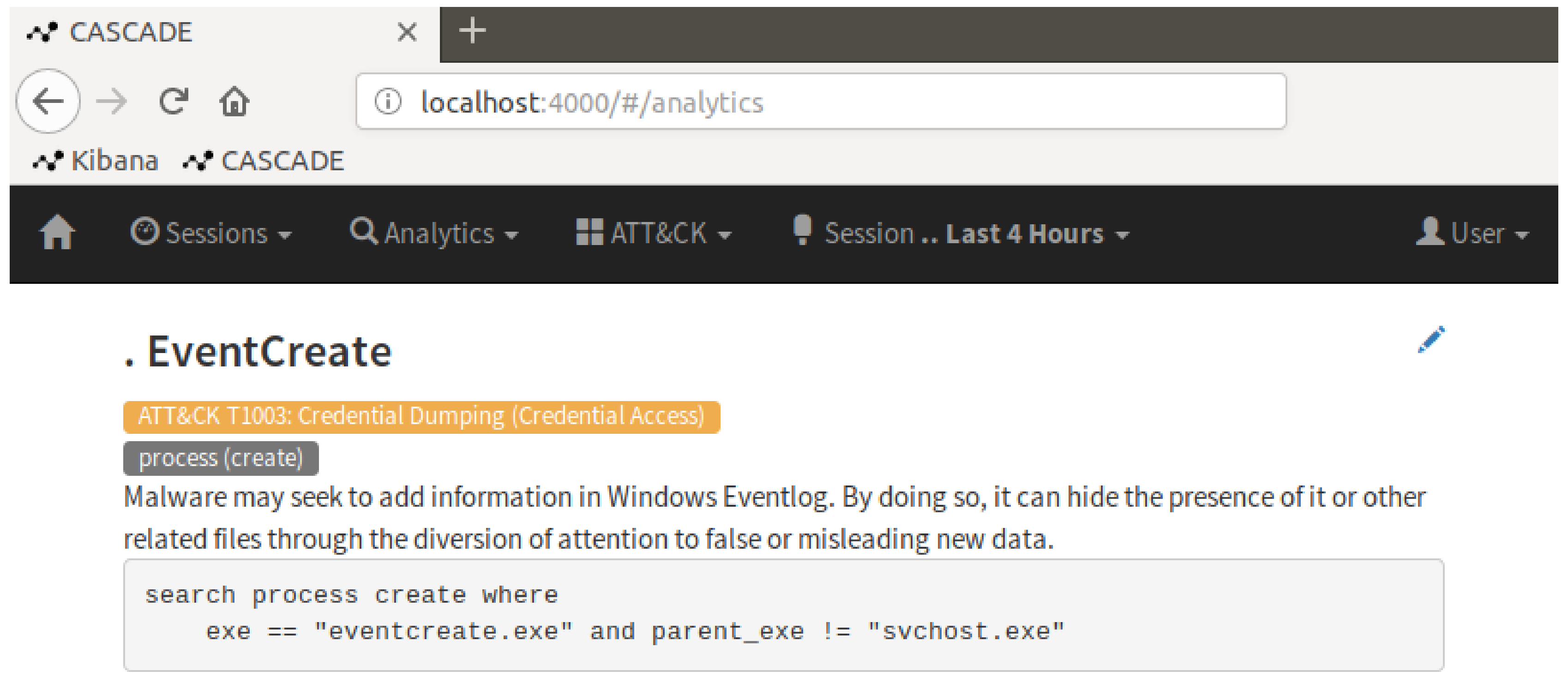


ID	IP Wan/[Lan] : Port	Computer Name/UserName	OS . SP . arch . root	% RAM Used	Languag
Unclassed users					
Guest16_min	1.1.1.2 / [10.0.20.8] : 443	BLUE-USER-2 / RATDEP Blue Win7	Windows 7 Service Pack 1 ...	44%	English (

Control : [BLUE-USER-2 / RATDEP Blue Win7], Socket : [1464].

Type	Value
Server Connexion	
Connection Host	10.0.30.2
Connection Port	443
Server General Information	
Country	English (United States)
Name/Nick	BLUE-USER-2/RATDEP Blue Win7
Operating System	Windows 7 Service Pack 1 [7601]
Screen Resolution	1680x953
N° Mouse Buttons	3
Active Caption	Process Hacker [BLUE-USER-2\RATDEP Blue Win7]
SysDir	C:\Windows\system32
WinDir	C:\Windows
User SID	S-1-5-21-4213183079-3463559579-1593287149-1000
Mac Adress	70-0E-FE-01-84-00
Systeme UpTime	18 Days and 20:55:32
Computer power / type	Desktop computer

Attacker uses DarkComet RAT to gather victim system information



. EventCreate

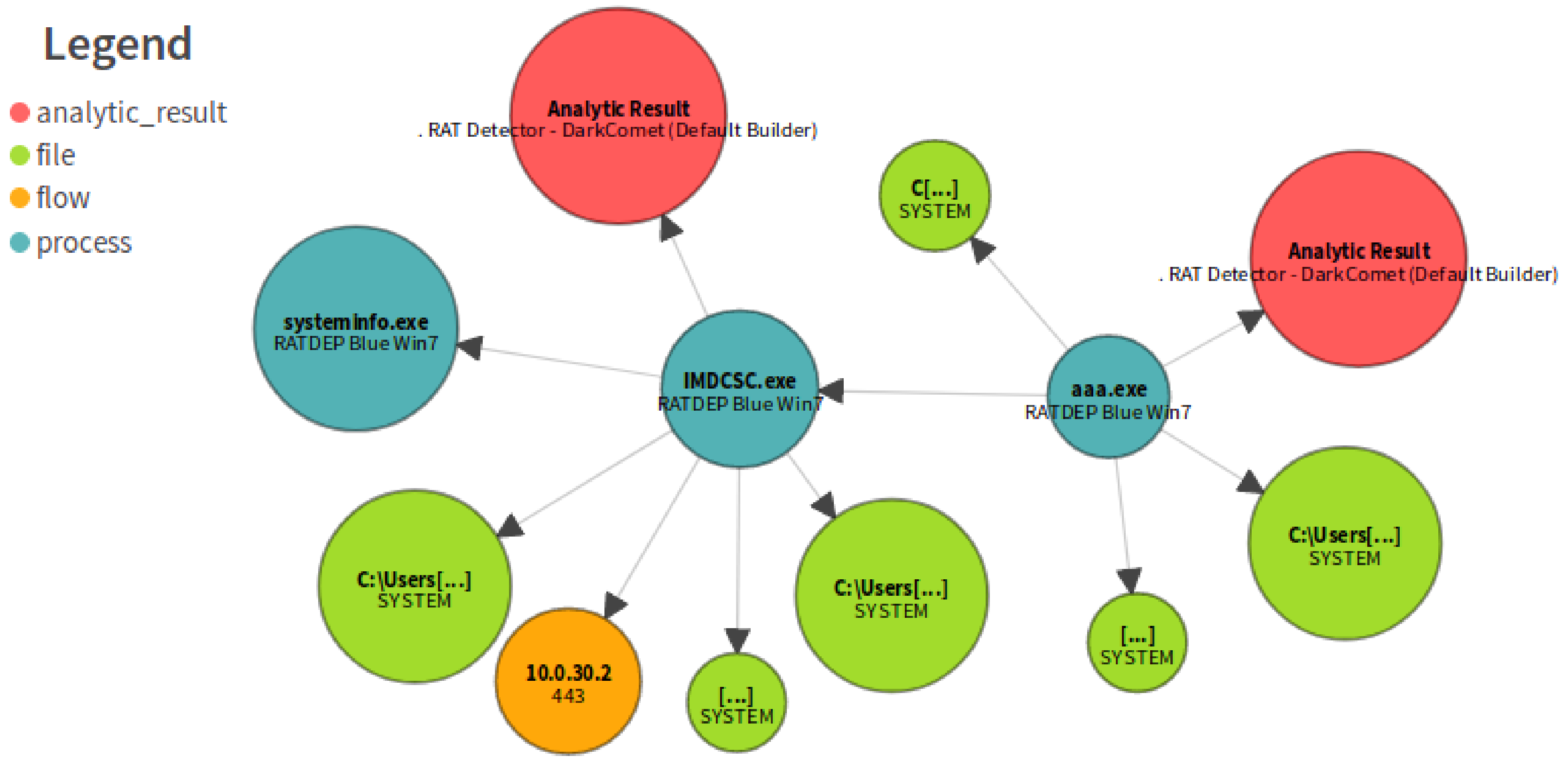
ATT&CK T1003: Credential Dumping (Credential Access)

process (create)

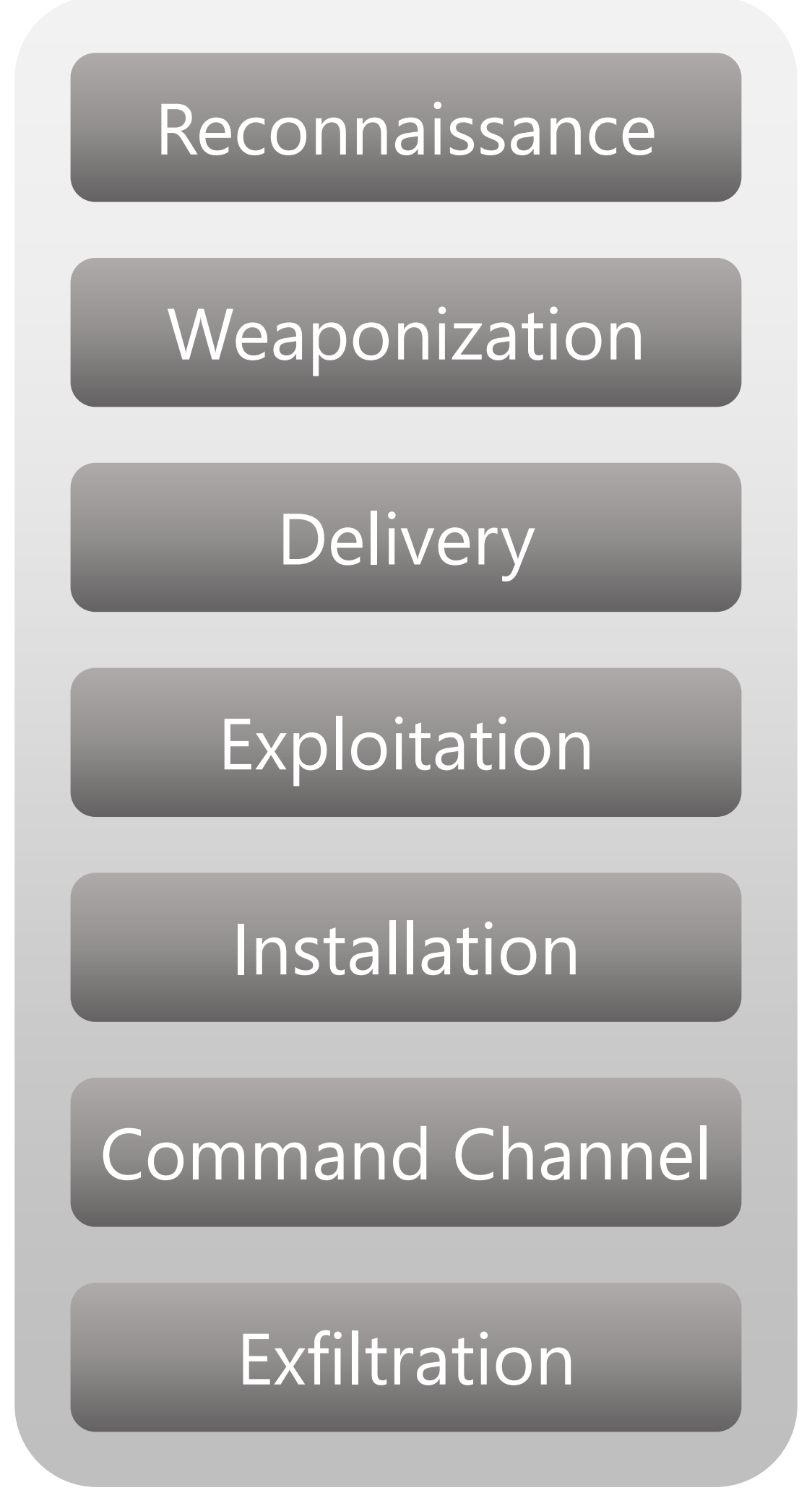
Malware may seek to add information in Windows Eventlog. By doing so, it can hide the presence of it or other related files through the diversion of attention to false or misleading new data.

```
search process create where
    exe == "eventcreate.exe" and parent_exe != "svchost.exe"
```

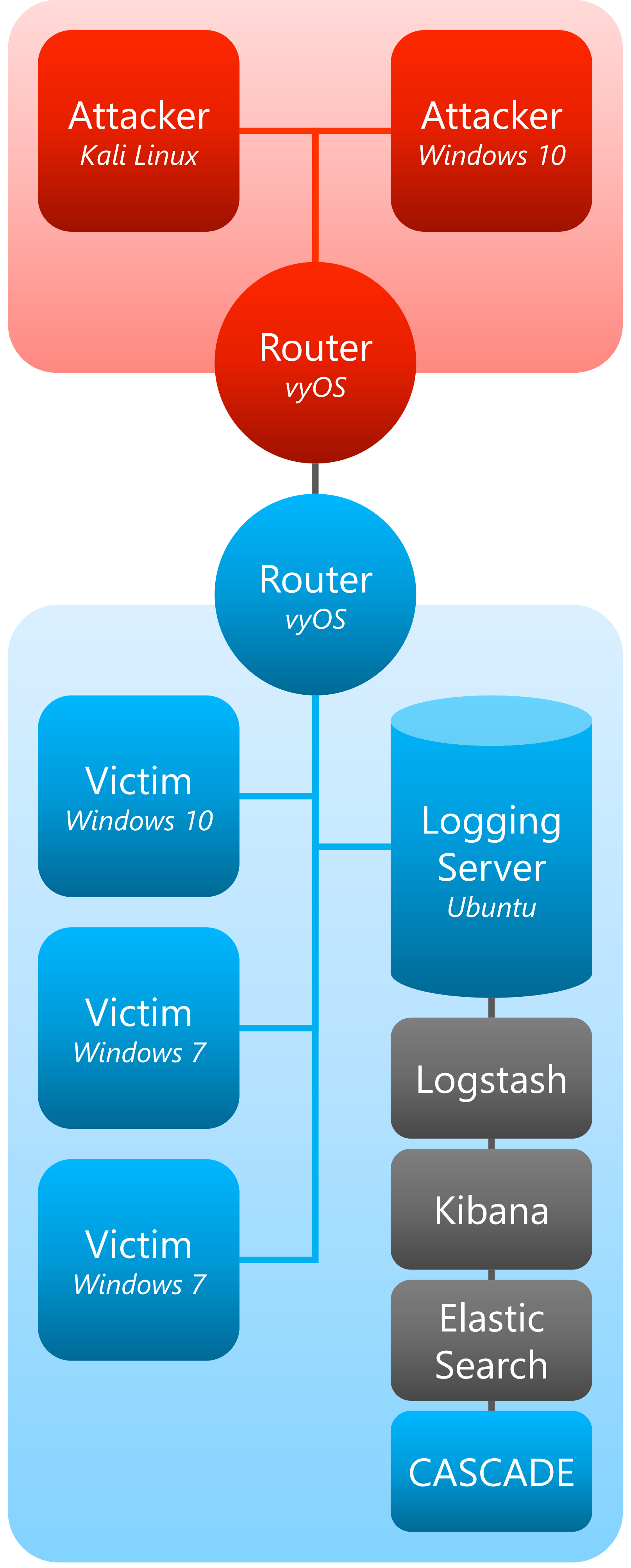
Creating an analytic to detect false entries to the Windows event log



CASCADE event graph links exploitation, callouts and command execution



The Cyber Kill Chain was used to conduct APT-like operations



RATDEP malware lab network topology and associated processes

Findings

Initially, CASCADE had limited success in detecting RAT activity and linking the suspicious events to steps on the cyber kill chain.

To increase CASCADE's detection rate, we built 14 new analytics in correspondence with the CAR data model, which organizes activity into a tripartite coordinate of object, action, and field.

By comparing Sysmon logging fields, CASCADE was able to build out relationships between processes, file touches, and network events, greatly reducing the time necessary to link the exploitation, installation, and exfiltration phases.

CASCADE analytics search for instances of activity that match phases of the Cyber Kill Chain, and provide an aggregated confidence score across several adversarial tactics and techniques.

Some of these analytics were also created to identify activity unique to specific RATs that had known, publicly available exploits.

Using CASCADE, we were able to detect the presence of Gh0st RAT and Darkcomet on a victim machine.

Conclusion

Based on our findings, it is clear that CASCADE is an effective tool at identifying all stages of RAT activity. Its rapid, structured analysis of Sysmon data minimizes the amount of time between RAT infiltration and detection. With more development and refinement, CASCADE can be successfully deployed in many public and private sector organizations to help prevent and respond to APT activity.

Future work could include: 1) completion of more operations and analytics to increase the effectiveness of CASCADE and/or 2) further research on classifying RATs into families and additional study into RAT exploitation.

This work was supported by the Cyber Information Assurance and Decision Support (CIADS) division within the Signal and Information Sciences Laboratory (SISL).