DUY TÂN UNIVERSITY

International School

Capstone Project 1

CMU-CS 450 AIS

Project Proposal

Version 1.0

Date:29/08/2022

Command And Control Attack Simulation & Log Analysis

Submitted by

Mentor : Le Van Tinh

Khoa, Pham Anh

Huy, Tran Minh

Trung, Nguyen Huy

Khoa, Tran Van

Approved by

Proposal Review Panel Representative:

Name	Signature	Date

Capstone Project 1- Mentor:

Name	Signature	Date

PROJECT INFORMATION

Project acronym	C2 AS & LA		
Project Title	Command And Control Attack Simulation & Log Analysis		
Start Date	18 Aug 2022	**End Date**	10 Dec 2022
Lead Institution	International School - Duy Tan University		
Project Mentor	Tinh, Le Van M. Sc		
Scrum master / Project Leader & contact details	Khoa, Pham Anh Email: khosasuke@gmail.com Tel: 0905648553		
Partner Organization			
Project Web URL			
Team members	Name	Email	Tel
25211116624	Huy, Tran Minh	minhhuytran2015@gmail.com	0935010972
25211109733	Trung, Nguyen Huy	huytr.work@gmail.com	0968580247
25211100051	Khoa, Tran Van	Tranvankhoa.1998@gmail.com	0522909360

REVISION HISTORY

Version	Date	Comments	Author	Approval
1.0	30 JUN 04	Initial Release	SE CONOPS Team	
1.1	30 SEP 04	Updates to incorporate comments in preparation for use with Pilot projects.	SE CONOPS Team	

1. Introduction

Purpose

Currently, remote malware attacks, also known as Command and Control for short, C2, happen very often at state agencies and businesses in Vietnam. The purpose of this topic will be to provide safe solutions to avoid the potential risks of malicious code. At the same time, increasing vigilance makes the equipment at the enterprise safer.

Meaning

In the field of security-network security, an extremely popular method often used by cybercriminals to distribute and control malware on target systems is to use a "Command and Control" server, also known as C2 or C&C for short. This is when the bad guys use a central server to surreptitiously distribute malware to the target computer, execute malicious commands. necessary commands to the malicious program and thereby take control of the device.

C&C is a particularly sophisticated attack method, because just one infected computer can become a bridge that allows hackers to take down the entire internal network. After malware successfully infiltrates an infected computer, the C&C server can instruct it to replicate and self-distribute to other computers on the network — this can easily happen because the malicious code has basically bypassed the network's firewall.

1.1 Research subjects

- Research languages that support the project building process: C/C++, Python, Java...
- Research tools to support the project construction process: Visual Studio Code, Draw.io, VMware Workstation Pro…
- Researching Vulnerability Exploit Tools in the project: Cobalt Strike, Metasploit's…
- Researching monitoring systems in the project: Splunk…

1.2 Research scope

- Realistic attack cases.
- Processes, log analysis of windows process.

- The integrated technology of the monitoring system.
- How to write reports and offer solutions.

2. Problem Definition

2.1 project request:

- A C2 or C&C attack consists of a set of tools and techniques that hackers use to communicate with compromised devices to give instructions to spread the infection. In a Command and Control Cyberattack, one or more communication channels may exist between the victim's PC or an organization and the platform the hacker controls. Attackers use these communication channels to pass instructions to compromised devices. DNS is a widely used communication channel for a C2 attack.
- Before we discuss Command and Control Cyberattacks further, there are some terms related to C&C attacks that you should know.

Zombie

- A zombie is a computer or device that has been infected with some form of virus or malware by an attacker. After turning a healthy computer into a zombie, an attacker can remotely control it without its owner's knowledge or consent. In a C2 infrastructure, the malware or virus that a hacker uses to infect a particular computer opens an avenue for the hacker to send instructions to the infected computer. This is a two-way street, which means that an attacker can send instructions to the infected computer and download content from the infected computer. Infected devices in a C2 or C&C infrastructure are called zombies because these devices are used by attackers to infect other healthy computers on a particular network. Once infected, these computers act like zombies appearing in Hollywood sci-fi or horror movies.

Botnet

- A botnet is an army of infected computers. In a C2 infrastructure, when one computer is infected, the infection is transferred to another computer connected to the network. The same process is repeated to infect other computers in the same network to create an army of bots. This army of bots (virus-infected computers) is called a botnet. A hacker can use a botnet for various cyber attacks,

such as a DDoS attack. Alternatively, a hacker can also sell botnets to other cybercriminals.

Beaconing

- Signaling is the process by which malware in an infected computer communicates with a C&C server to receive instructions from the hacker and send data from the infected device to the hacker.

2.2 Project solution:

You can define Command and Control Cyber Attack with the help of log files.

DNS log files: As described above, DNS is the most commonly used communication channel in Command and Control Cyberattacks. As a result, DNS log files can provide you with important information about C&C attacks. As we said, most C&C attacks are done through DNS servers. But if the C&C attack is not done through the DNS server, the DNS log files will not give you any information about the attack.

Proxy log files: Most organizations use filtering proxies. User traffic must go through this proxy for security reasons. Web proxy log files can be an important source of information regarding Command and Control Cyber Attacks.

Firewall logs: Firewall logs can also be a good source for a C&C attack investigation.

After gathering information from various log files, you can look for the following in the log file to confirm whether a C&C attack has taken place. Repeat pattern of HTTP requests,

Connect to an HTTP server especially outside of normal business hours,

Ask social networking sites, especially outside office hours,

DNS response with low TTL,

Repeated requests for URL shortener domains,

Outgoing IRC or P2P traffic, etc.

2.3 Technical constraints:

Reverse Engineering:

To reverse engineer malware, the researcher will analyze the actual malware binary, and attempt to recover the source code. This can give valuable insights into the

operation of the malware, and can even give vital information such as hardcoded C&C server addresses and encryption keys.

Honeynets/Malware Traps:

A honeynet is typically made up of a number of honeypot nodes, which are machines that run vulnerable (un-patched) software with a goal of becoming infected with malware. The infected machines can then be used to profile malware through wither automatic or human means.

Communication Detection

As we have seen, many malware variants have very particular protocols when it comes to communication. These are often noticeably different to legitimate traffic, both in packet contents and in the behavior of the communications. This makes signature-based detection methods very good for detecting known variants of malware. Many different pieces of malware may also be based upon a common component, meaning that a single signature can be used to detect multiple pieces of similar malware. One possibility for this kind of detection is to produce signatures based upon the contents of packets.

Sandboxes

A slight variant on a honeynet is a malware sandbox. In this instance, malware is directly installed on a machine and the activities analyzed. The main difference with a honeynet, however, is that the owner will also interact with the malware (for example, by mimicking command and control servers). This allows the researcher to gain a much bigger picture of the malware's operation under different situations.

Fast Flux

As we recall, in a fast flux network the command-and-control server is hidden behind a proxy of numerous compromised hosts. Performing DNS queries on the domain of the server will return a large, and constantly changing, set of IP addresses. As you may expect, this type of behavior is relatively easy to detect.

3. Current Status of Art

3.1. Summarize the search and research results

In the wake of the ongoing war between Russia and Ukraine, many Russia-linked APT groups used a new data-delete malware known as Hermetic Wiper by the IT security community. A corresponding list of known indicators can be found in our IOC list. Here we will look at attack chain #1.

The attack sequence begins with the victim receiving a malicious archive via email (mostly .zip archives and .7zip archives have also been detected). The archive contains a document file themed after the currently ongoing war between Russia and Ukraine, however this topic is subject to change in the future. The document contains macro code that reduces and executes VBScript while the victim is opening the document, VBScript has been identified as a piece of malware called gamma load.

Table : List IOC

T09.1	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d	Compressed SHA256 of X86 Driver for Windows XP used in Attack
T09.2	2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d	Decompressed SHA256 of X86 Driver for Windows XP used in Attack
T10	HKLM\SYSTEM\CurrentControlSet\Control\CrashControl	Modified Registry Value (to 0) to disable crash dumps
T11	EPMNTDRV	Device Name of the Malicious Driver that is installed
T12	74ce360565fa23d9730fe0c5227c22e0	MD5 of DLL used in 2nd Attack Chain
T12.1	ypagjgfyy.dll	Name of a DLL used in 2nd Attack Chain
T13	coagula[.]online	C2 Domain 1st Attack Chain
T13.1	deer.dentist.coagula[.]online	C2 Domain 1st Attack Chain
T13.2	declaration.deed.coagula[.]online	C2 Domain 1st Attack Chain
T13.3	surname192.temp.swtest[.]ru	C2 Domain 1st Attack Chain
T14	http://surname192.temp.swtest[.]ru/prapor/su/ino.gif	Document Template URL for 1st Attack Chain
T14.1	http://surname192.temp.swtest[.]ru/prapor/su/derg.gif	Document Template URL for 1st Attack Chain
T14.2	http://surname192.temp.swtest[.]ru/prapor/su/flagua.gif	Document Template URL for 1st Attack Chain
T14.3	http://surname192.temp.swtest[.]ru/prapor/su/flages.gif	Document Template URL for 1st Attack Chain
T15	94.158.244[.]27/absolute.ace	Download IP for Payload of the 1st Attack Chain
T15.1	94.158.244[.]27/distant.cdr	Download IP for Payload of the 1st Attack Chain
T16	kfctm[.]online	C2 Domain 2nd Attack Chain
T16.1	my.cloud-file[.]online	C2 Domain 2nd Attack Chain
T16.2	my.mondeychamp[.]xyz	C2 Domain 2nd Attack Chain
T16.3	files-download.infousa[.]xyz	C2 Domain 2nd Attack Chain
T16.4	download.logins[.]online	C2 Domain 2nd Attack Chain
T17	http://kfctm[.]online/0802adqeczoL7.msi	Download IP for Payload of the 2nd Attack Chain
T17.1	http://my.cloud-file[.]online/Microsoft_VieweR_2012.msi	Download IP for Payload of the 2nd Attack Chain
T17.2	http://my.mondeychamp[.]xyz/uUi1rV.msi	Download IP for Payload of the 2nd Attack Chain
T17.3	http://my.mondeychamp[.]xyz/ReadMe.msi	Download IP for Payload of the 2nd Attack Chain
T17.4	http://files-download.infousa[.]xyz/Windows_photo_viewers.msi	Download IP for Payload of the 2nd Attack Chain
T17.5	http://files-download.infousa[.]xyz/Windows_photo_viewer.msi	Download IP for Payload of the 2nd Attack Chain
T17.6	http://download.logins[.]online/exe/LinK13112020.msi	Download IP for Payload of the 2nd Attack Chain

This script starts by collecting information about the user and the system on which it is executed and prepares them for the C2 server. The IP address of domain C2 {T13} is then obtained, which the attacker has configured through the WMI script {T01}. Then the {T15.x} payload snippet for the next step is downloaded and the collected data is being uploaded to the configured C2 server. This connection can be identified through a user-specific string {T02} hard-coded in the malware.

The payload contains several types of remote desktop applications, most observed so far being Ultravnc (see {T03.x} for other possible options). This allows the attacker to perform various tasks on the affected system including deleting data and destroying the system. See a diagram of the attack.

HermeticWiper – Attack Chain Number 1

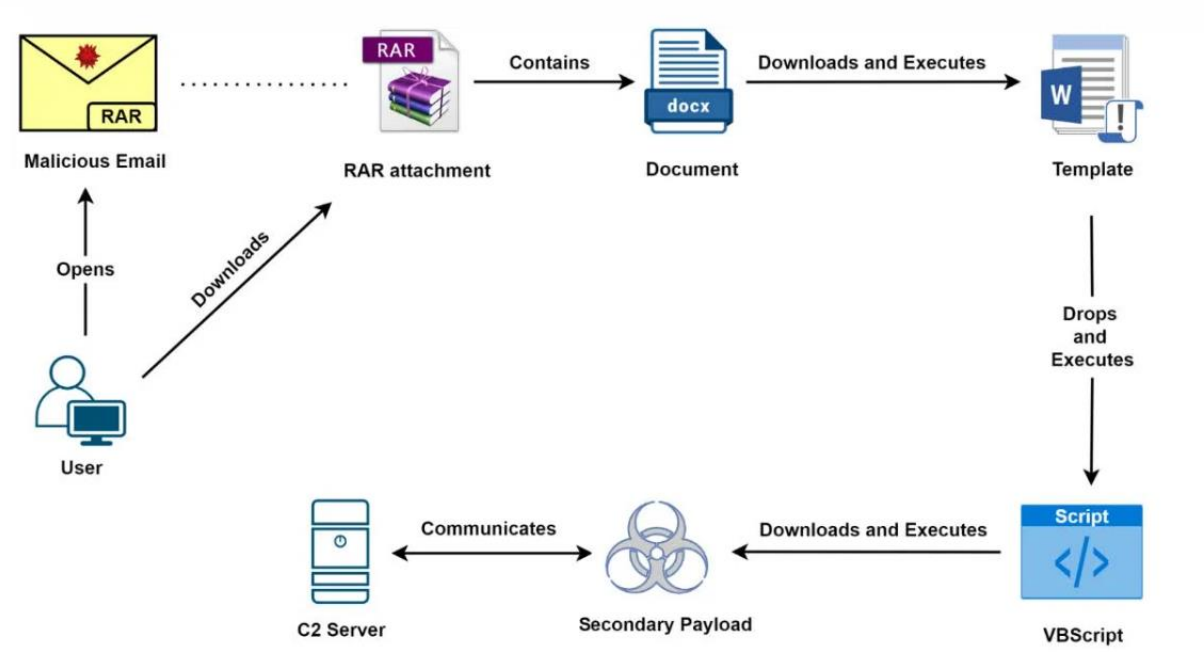


Figure 1: Visualization of the 1st attack chain(source:[3])

Currently, malware-operating cybercriminals use the popular Cobalt Strike engine to reduce multiple payloads after profiling a compromised network. Cobalt Strike is a commercially available and popular command and control (C2) framework used by the security community as well as a wide range of threat actors. The powerful use of Cobalt Strike allows threat actors to execute incursions with precision.

Based on the model of mining steps using the Cobalt Strike tool.

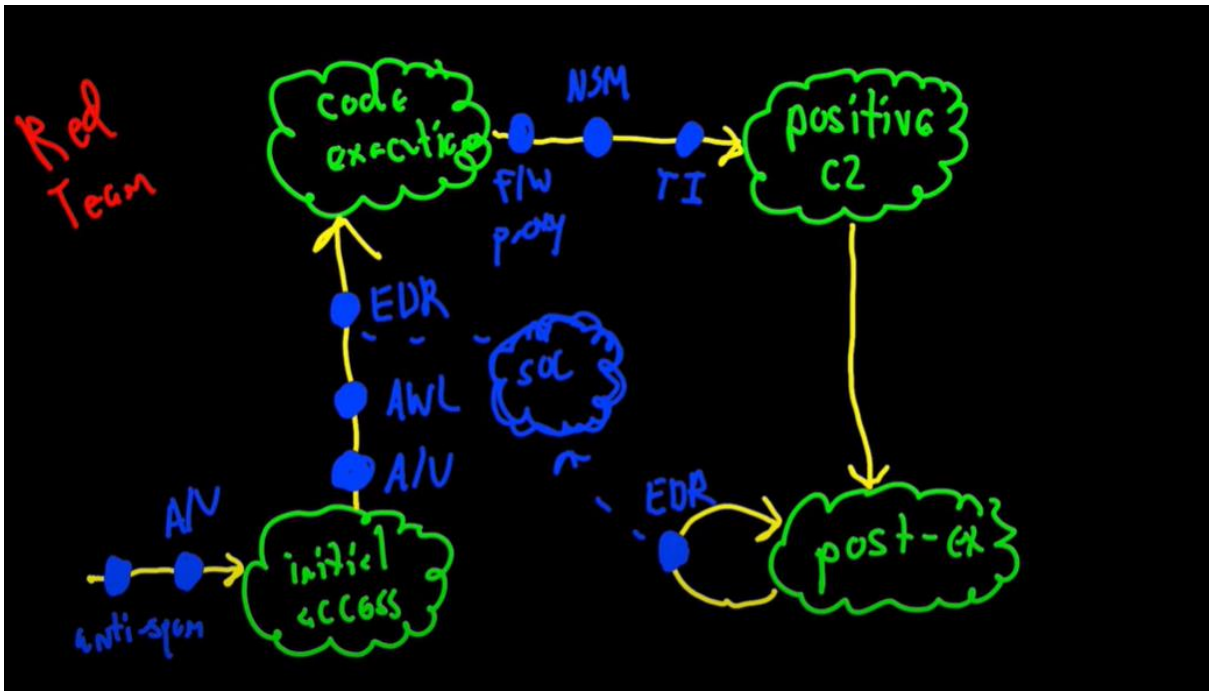


Figure 2 : Operation Command and Control

Initial Access Stage

- This is considered the initial stage to get the first access to the enterprise's system using different mining techniques on MITER ATT&CK.
- This is the stage of the Mail Anti-Virus attack type
- Cons: Bypass Anti virus, Access Whitelist, EDR (Endpoint Detection and Response)

Code Executing Stage

- The stage for malicious code to execute on this active user environment to bypass the firewall.

- Cons: Firewalls, Proxies, Network Security Monitoring, ...

Positive Control Phase (c2)

- Successful c2 deployment stage on victim's machine.

- Cons: EDR

Post-Exploitation Stage

- This phase is to end the attacker's exploit and return to safety undetected

- Cons: EDR

So, we can imagine the attack scheme of the cybercriminals who take advantage of a simple file to build up infrastructure in order to want to take away sensitive data and put it up for sale. outside for their own benefit. So based on these research results, we can see the fact that external attacks always take place every day. Visual representations of attacks are viewed on CHECKPOINT THREATCLOUD.

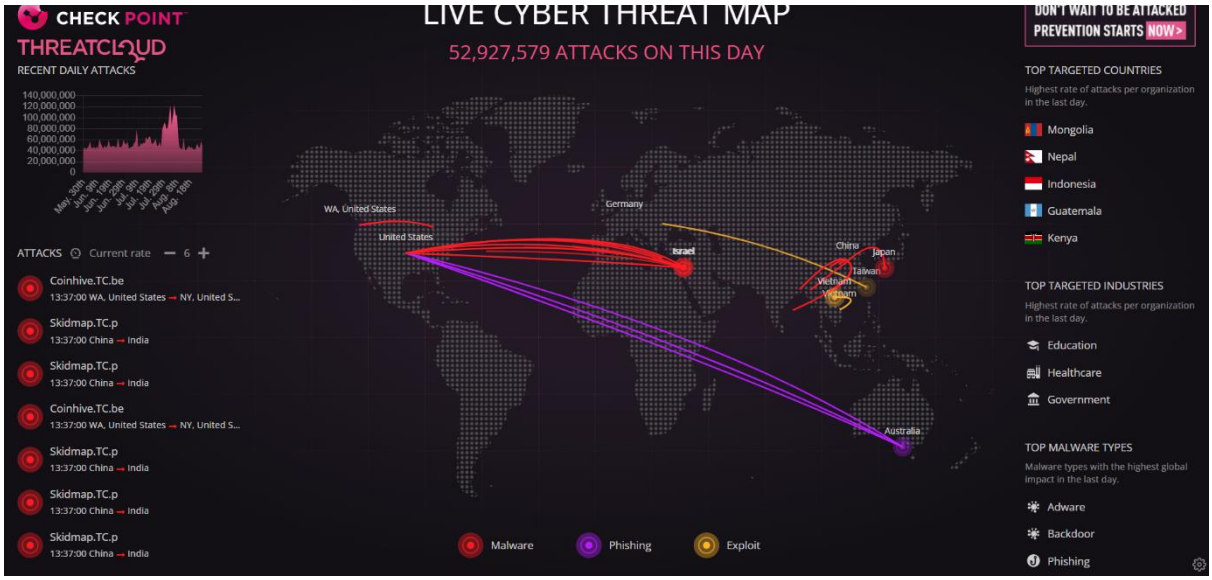
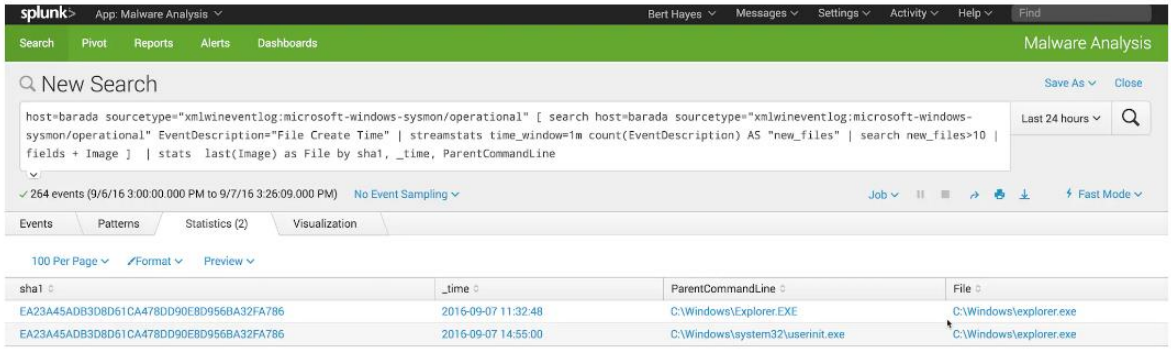


Figure 3 : CheckPoint ThreatCloud

As observed on the left, Malware attacks are always taking place the most in the world. To provide solutions to prevent these malicious attacks, the application of this Splunk monitoring system in log analysis will help businesses avoid the risk of minimizing this attack.



	Search, Analyze	Monitor, Alert and Report	Collect and Index Data
Advantages	- Intuitive interface for log analysis. - Support data analyst to search faster. - Analysis of optimal events.	- Monitor events recorded on the spelunk system. - Tracking alerts and event-specific responses are available. - Save more specific and intuitive search actions.	- Collect machine-based data securely. - Secure safe data retrieval. - Can be collected on many different operating systems.
Disadvantages	- Search will be difficult for non-analysts. - The commands will be more complicated. - Event log analysis will take more time.	- View event tracking number of many, so time consuming.	- Use manual configuration on the machine to get data. - Use manual configuration on the machine to get data.

Figure 4 : Show search results on Splunk

4. Engineering Approach (including solution alternatives)

4.1. Idea

- The first idea builds on the C2 infrastructure design, which simulates a C2 attack and the exchange of information between the attacker machine and how it works to perpetuate the malware on the victim machine. The ways the attacker will perform on the diagram.

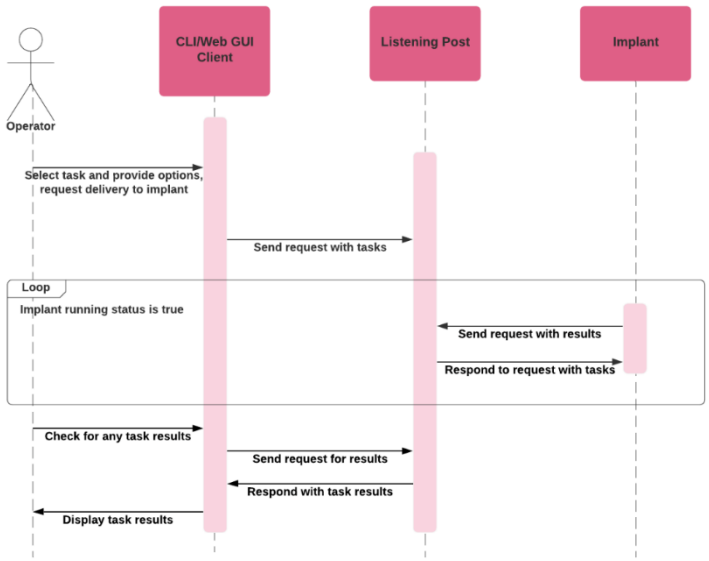


Figure 5 : Basic C2 Setup

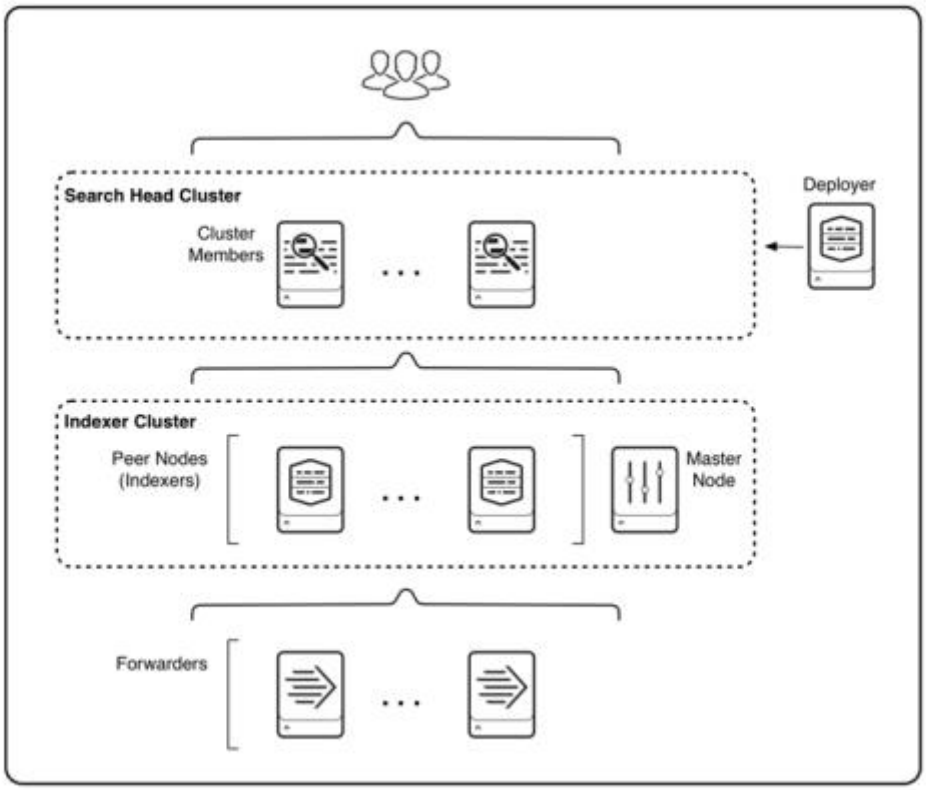


Figure 6 : Monitoring System

- The second idea to troubleshoot and promptly respond to an attack, will include a monitoring system in this project to reduce the risk of network attacks and also provide a way to analyze the log before the attack. attack to respond promptly. Structural diagram overview system.

4.2 Explanation

- First the attacker will use CLI (Command Line) to execute C2 (Command and Control), now the attacker needs a server to listen securely to avoid detection this will need some TCP, SMB, DNS protocols will generate the payload to perform listening on the server (Server). So, from the form of communication from the listening server to the exchange from the Server to the malicious software that supports that software implanted on the machine continuously to facilitate the

exchange of data to the victim's machine. Any results will be returned to the server that listens last to the attacker's machine.

- Splunk provides a distributed search architecture that allows scaling to handle large volumes of data and better handling of access control and distributed data. In a distributed search scenario, the search head sends search requests to an index group, also known as search peers.
- About the monitoring system by rough diagram is divided into 3 main parts:

§ Forwarders: Installed on servers (except network devices) to collect log data and send it to the monitoring system.

§ Indexer Cluster: These stored indexes are all from Forwarders data from pre-installed operating systems on the victim machine.

§ Search Head: The purpose will be used to create ways to search and view log data.

4.3 Approaching some knowledge

- Network Knowledge:

  - The main purpose of applied network knowledge is to understand the operation of the infrastructures and protocols that are important in the application of the C2 infrastructure in the project.

- Hacking Exploits:

  - Apply step-by-step processes to perform an enterprise system security assessment.

- Implementing Splunk:

  - Apply distributed data system for fast search analysis by MAP-Reduce technology.

4.4 Contents of knowledge would be learned to pursue the solution approaches

– Because the requirement is to simulate a C2 attack and also implement event data analysis processes and will follow a clear step-by-step in the log analysis.

5. Tasks and Deliverable

5.1. Tasks and Scope of your expected work:

Phase 1: Analysis

We searched for relevant documents on C2 malware attack. Then research and install the monitoring system in a deployment project. Then learn to assess these levels of harm through the monitoring system.

Phase 2: Design

We build monitoring systems that integrate functions and build C2 attack models for our project, all the core of this project is based on the platforms we learn and research like Splunk and C2 infrastructure.

Set up a collection of applications, in order to support the monitoring and analysis of the attack sequence of malicious code samples.

Phase 3: Code

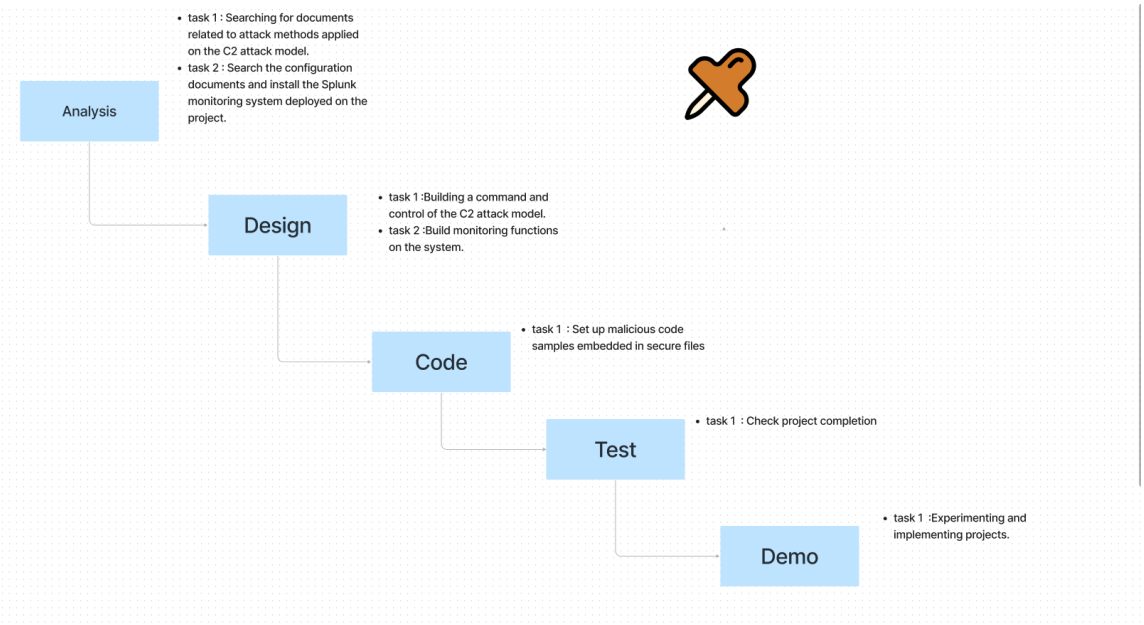
Set up secure malware patterns to bypass antivirus software.

Phase 4: Test

Check project completion. Test everything from implementation to experimentation. Then we come up with a solution

Phase 5: Demo

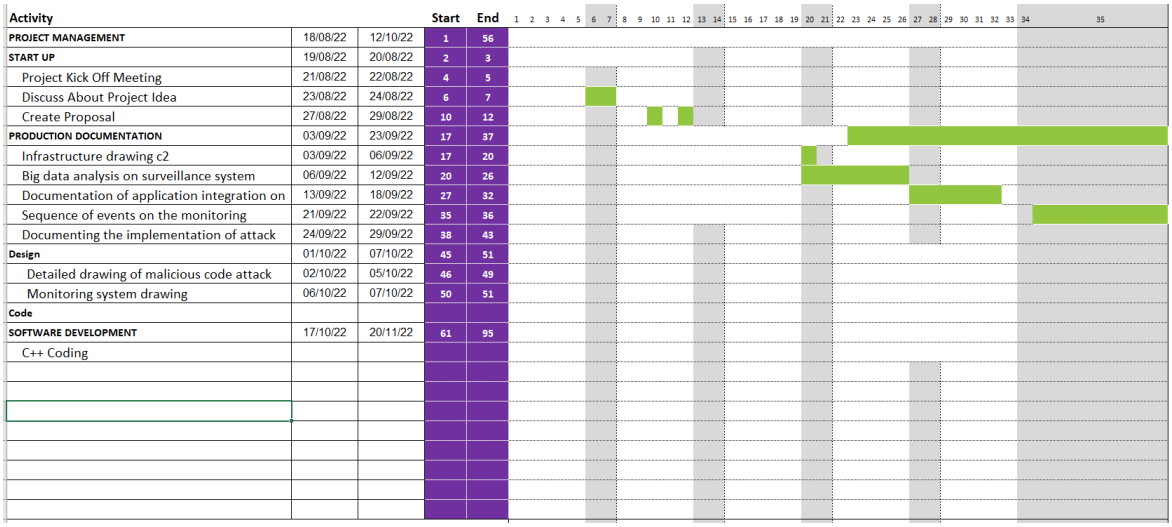
Offer products for testing and evaluation, final result



6. Project Management

6.1. Tentative Schedule

Activity			Start	End
PROJECT MANAGEMENT	18/08/22	12/10/22	1	56
START UP	19/08/22	20/08/22	2	3
Project Kick Off Meeting	21/08/22	22/08/22	4	5
Discuss About Project Idea	23/08/22	24/08/22	6	7
Create Proposal	27/08/22	29/08/22	10	12
PRODUCTION DOCUMENTATION	03/09/22	23/09/22	17	37
Infrastructure drawing c2	03/09/22	06/09/22	17	20
Big data analysis on surveillance system	06/09/22	12/09/22	20	26
Documentation of application integration on	13/09/22	18/09/22	27	32
Sequence of events on the monitoring	21/09/22	22/09/22	35	36
Documenting the implementation of attack	24/09/22	29/09/22	38	43
Design	01/10/22	07/10/22	45	51
Detailed drawing of malicious code attack	02/10/22	05/10/22	46	49
Monitoring system drawing	06/10/22	07/10/22	50	51
Code				
SOFTWARE DEVELOPMENT	17/10/22	20/11/22	61	95
C++ Coding				



7. Project Constraints

Constraint	**Constraints Description**	**Guidelines for Acceptance**
Economic	In terms of the cost of deploying a complete defense system, a lot of money goes into the network of equipment, so it only applies to the main organizations that cover the businesses of VNPT, VNCERT.	Elements for consideration are design costs, production costs, maintenance costs, operating costs, and sales price
Environmental	Regarding the impact of external factors, it will be on the durability of the network path, it is necessary to ensure the sustainability of the system in the company.	The impact of the design on the environment as well as the impact of the environment (e.g., temperature range, humidity, vibration, electromagnetic interference immunity, and shock) on the design should be considered. Design for recycling and design to use recycled materials should also be considered

Ethical	The main area in this area will be the so-called SOC (Security Operations Center), where an information security team is responsible for monitoring and analyzing the security situation of the organization. continuous. The goal of the Security Operations Center team is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a robust set of processes. Security operations centers are typically staffed by analysts and engineers as well as by managers. Security Operations Center staff work closely with the organization's incident response teams to ensure security issues are resolved quickly when discovered. Security Operations Center monitors and analyzes activity across networks, servers, endpoints, databases, applications, websites, and other systems, looking for possible unusual activity.	Ethical considerations can be broad. Areas that are typically addressed include intellectual property, reverse- engineering, privacy, security, and the conflict between cost and safety

	This is a sign of a security problem or intrusion. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, protected, investigated and reported.	
Public health, safety, and welfare	This is a locally deployed system, so electrical hazards will be maintained and maintained by infrastructure teams.	Includes safety standards as well as the impact of the design on users (for example, electrical or physical hazards)
Social and Global	Regarding the benefits of this project, to help organizations grasp the risks that need to be avoided in the face of an attack, they will promptly provide a solution.	Addresses aspects such as benefits, risks, the human-machine interface, the acceptance of products by the intended user or by society at large, and global and socially responsible engineering.
Cultural		Which cultural characteristics could influence the approach? How do the design from different cultures differ?

Sustainability	To be sustainable as well as to help with surveillance in cyberspace will be a source of training more human resources. Including personnel who must have the expertise, skills as well as solid knowledge, when performing infrastructure maintenance and threat analysis. Infrastructures also need to strictly have someone operating and looking after the infrastructure at all times. The second thing is that the more funding, the higher the safety of infrastructure damage.	Refers to the sustainability of resources, including material, energy, supplies, manufacturing techniques, personnel, operation, and the need for additional infrastructure, as well as the sustainability of the design including reliability, lifetime, durability, reusability, maintainability.

8. Conclusion

This report has tried to make clear the current malware attacks based on c2 form and also the implementation of the monitoring system on the enterprise. First, we look at the case, especially when compared with traditional attack tools, and look at some of the modern tools used to implement attack simulation. If your organization is interested in applying log analysis processes to the monitoring system to provide accurate results. Finally, we surveyed information security forum sites and articles from cybersecurity experts. We hope that this overview helps businesses recognize problems and take timely action to prevent them.

To evaluate the integrity and safety of an enterprise, the Red team plays an important role in system testing.

9. References

https://dgc.org/en/hermeticwiper-malware/

https://socprime.com/blog/armageddon-apt-known-as-uac-0010-drops-gammaload-ps1_v2-espionage-malware-in-a-new-phishing-campaign-against-ukraine/

https://www.malwarebytes.com/cybersecurity/business/what-is-hermetic-wiper

https://xuanthulab.net/nguyen-ly-lap-trinh-ioc-inversion-of-control-ioc.html

https://blog.sekoia.io/hunting-and-detecting-cobalt-strike/

https://community.splunk.com/t5/Random/which-technology-Splunk-use/m-p/295515

https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/SQLtoSplunk?_gl=1*8kwqi7*_ga*MTY0NjkyNDEwOC4xNjYwMjg1NTg2*_gid*MTcxNjQyODQ1OS4xNjYxNjcxNDU4&_ga=2.127218253.1716428459.1661671458-1646924108.1660285586

https://www.bluevoyant.com/knowledge-center/splunk-enterprise-architecture-features-and-capabilities