National College of Ireland

The Impact of Conti Ransomware on a Modern Virtualized Environment

MSc Research Project
MSc in Cybersecurity

Alessandro Gentili
Student ID: x19176546

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Alessandro Gentili…………………………………………………………………………		
Student ID:	x19176546		
Programme:	MSc in Cybersecurity	**Year:**	2021/2022
Module:	Internship		
Supervisor:	Ross Spelman		
Submission Due Date:	15/08/2022		
Project Title:	The Impact of Conti Ransomware on a Modern Virtualized Environment		
Word Count:	5900 **Page Count** 23		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………………………………………………………………………………………………………

Date: 15/08/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

The Impact of Conti Ransomware on a Modern Virtualized Environment

Alessandro Gentili
Student ID x19176546

Abstract

The recent attack on the Irish Health Service Executive (H.S.E.) system by the Conti ransomware has underlined the danger of this kind of threat in the international panorama. Unfortunately, technical knowledge about the Conti ransomware and the overall understanding of how this group operates is still in part unknown. As such, there is an opportunity to increase knowledge in this area, especially from an academic point of view. In order to study the Conti ransomware safely, one main requirement is to have the virtual laboratory as secure as possible. Therefore, it has been designed with all CIA principles. In addition, the researcher can benefit from the VPN and the Tor network to achieve anonymity, hidden geolocation, and data encryption. The overall implementation uses virtualization technology and automation. The experiments have been performed with static and dynamic analysis to check both source code and behavioral aspects. The findings show that the virtual lab is safe for experimenting without fear of being tracked back. The results also show that the impact of the Conti ransomware varies if this is carried out online or offline. In addition, a minimum layer of security can stop Ransomware from spreading through the network. Other researchers can reuse the proposed architecture and the conclusions to study the impact of the Conti ransomware and its variants for future experiments.

Keywords: Conti ransomware, Virtualized Environment

1 Introduction

"What is the impact of the recent Conti Ransomware attack on a Modern Virtualized Environment?" is the research question of this paper that falls within the Cybersecurity realm and, more specifically, in the malware analysis area. The word malware means "malicious software," a program written by a developer to damage one or all the CIA (Confidentiality, Integrity, Availability) aspects of a particular computer system/network.

Ransomware is malware that blocks access to specific data residing on an IT system. It demands the data owner for a ransom, usually in non-traceable cryptocurrencies, to reinstate user access to the data. Ransomware [1] consists of two subcategories, lockers and crypto. Lockers restrict the entry to the victim's data by locking the system. Crypto ransomware restricts entrance to the victim's data by encrypting it. It uses the latest state-of-the-art cryptographic algorithms by "creating insecurity by using security."

The latest state-of-the-art cryptographic algorithms are tough to decrypt, primarily if long passwords or passphrases are used. The use of encryption makes crypto-ransomware attacks extremely harmful, dangerous, and without a "cure" when they are successfully delivered. The best-known solution is to have an offline verified backup [2] of the data secured in an external physical location. Unfortunately, this is not always possible in modern environments where high availability is required, so prevention remains the best option to counter this threat. A modern Information Technology infrastructure environment nowadays often employs massive virtualization to reduce costs, optimize resources, provide business continuity, and enhance cybersecurity. Virtualization is achieved by creating an abstract layer on top of the hardware layer. It involves having multiple virtual servers on top of a single physical server. The de-facto standard used in most installations for modern virtualized environments consists of three main components: computational servers, networking devices, and storage area networks.

Computational servers are attained by using the Hypervisor. This core component enables virtualization, which can be either software (type 2) or an operating system (type 1 and the most common in the enterprise world). In order to keep simplicity in this research paper, containerization and nested virtualization will be included under the same term: virtualization. Furthermore, the Hypervisor layer is typically believed to be immune to viruses; however, recent techniques of virtual machine escape must be considered either in a virtual environment or in the virtual lab where this experiment is conducted.

The most common virtualized environment setup used by a company "in production" (to operate its core business) tends to be composed of a mixture of Windows and Linux operating systems. The first is often used for Active Directory services directly related to Windows clients, and the second is to deliver LAN services such as DNS, FTP, NAS, VPN, and WEB services. For this reason, it is not surprising that the main target of Conti ransomware is the Windows Operating system. Therefore, the virtual experiment will include client and server, both Windows and Linux virtual machines, to avoid excluding potential Conti Ransomware evolutions.

As detailed in the SonicWall cyber threat report, ransomware attacks increased by 105% in 2022[1] to total 622.3 million incidents worldwide. Two reasons explain this considerable growth. One reason is the availability of Ransomware as a Service (RaaS) on the dark web [3], allowing technical and non-technical people to buy an attack and seek out multiple targets.

[1] https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

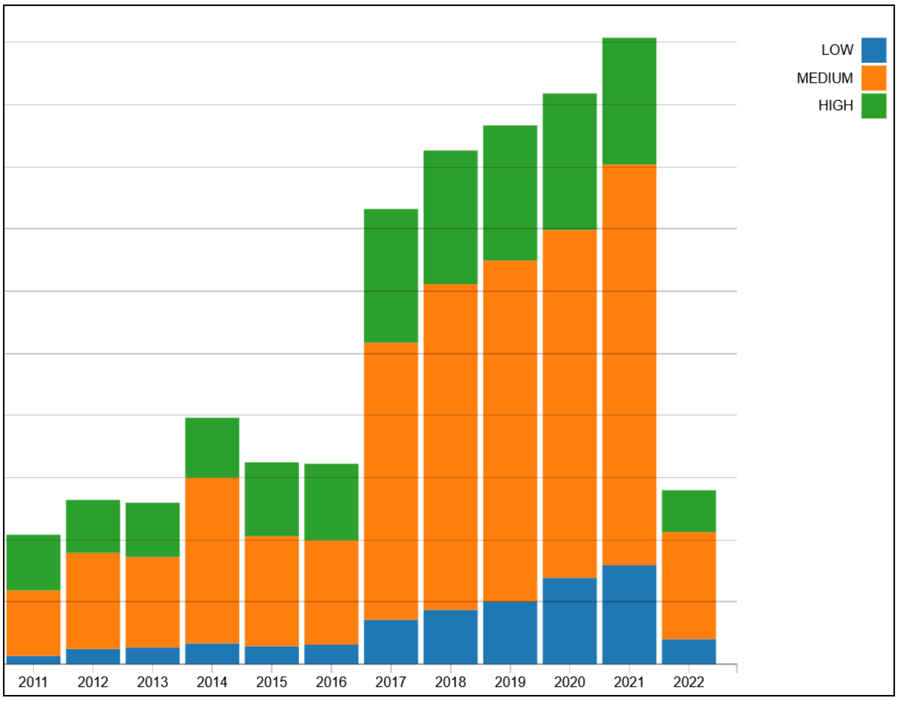


Figure 1 NIST CVSS Severity Distribution over time[2]

Another reason is the massive increase of vulnerabilities, with more than 20,000 in 2021 alone, as shown in the diagram above provided by NIST. These new vulnerabilities allow the refurbishing of old Ransomware. For instance, old Ransomware [4] using the EternalBlue vulnerability is considered obsolete because it can have its code changed to exploit the recent Log4j vulnerability to become very dangerous again.

The Conti ransomware, the subject of this research paper, utilizes multiple ways to breach an IT infrastructure[3], including known and zero-day vulnerabilities, 'spearphishing' campaigns, weak RDP sessions, phone calls, and fake software. The Conti Group, an international group with headquarters believed to be located in Saint Petersburg (Russia), developed the Conti ransomware.

In conclusion, this research paper aims to fill the knowledge gap in the current academic literature about the Conti ransomware by studying its interaction with an IT infrastructure, reverse-engineering the code, and looking for a kill switch and other relevant content in the source code. The data is collected by experimenting in a virtual laboratory ad-hoc designed and tailored to be as anonymous and secure as possible. The main goal of this study is to provide other academic researchers with a secure lab to conduct experiments and more information about the Conti ransomware to develop tools to stop this severe threat.

[2] https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
[3] https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

2 Related Work

2.1 Introduction

The academic literature about the Conti ransomware should be more extensive, considering the amount of damage it caused during 2021 and 2022. The total ransomware cost in losses reached $20 billion[4] US dollars in 2022 and is estimated to grow to $265 billion by 2031. Thus, it is not surprising that the cybersecurity industry focuses mainly on this threat, with thousands of new web articles regularly written globally. However, there is a lack of academic papers about Conti.

In paragraphs 2.2 and 2.3, academic papers published concerning the Conti ransomware are compared and contrasted with the emphasis on the background and entry point aspects. Next, paragraphs 2.4 and 2.5 focus on literature related to the "target" of the Conti ransomware, the virtual environment, and the best experimental design for the virtual lab. Finally, paragraphs 2.6 - 2.9 critically assess the literature about "how" to test and the existing studies.

2.2 Conti ransomware background

According to the website Cloudwards, the "debut" of the Conti ransomware into the malware scene was around 2020[5] when it was provided as RaaS [3] on the dark web by an international group, most likely Russian mother tongue. The tactics used by the ransomware group consists of two stages. The first one is where the Ransomware is loaded through an entry point into the victim's network/system, usually via spam emails that trick the victim into installing the Cobalt Strike Beacon penetration testing tool (in this case, it is used as a trojan horse). Next, access is persisted using remote connection agents (e.g., Anydesk), allowing the second stage to occur, which is represented by the execution of the malware itself.

The Computer Fraud and Security article [5] underlines that the Conti Group is specialized in targeting organizations that offer emergency and critical services to centralize their enterprise around business continuity, such as healthcare. The Conti ransomware actors have also developed a sophisticated technique to remove backups of the victim (especially Veeam, one of the leaders in the backup software market), increasing the restoring time or blocking it completely. The Conti ransomware, even if still very "young," is already deemed one of the most severe malware on the internet that does not leave any opportunity to recover data.

[4] https://www.cloudwards.net/ransomware-statistics/

[5] https://cyware.com/research-and-analysis/a-detailed-look-into-conti-ransomwares-tactics-5dd5

2.3 Conti initial access

The initial access of Conti Ransomware can leverage everything available to gather access to the organization's internal network. Three phases of the Cyber Kill chain have been identified by Mirza, Brown, Halling, Shand, and Alam [6]: Reconnaissance, Weaponization, and Delivery. Conti uses vulnerabilities to exploit the target that can comprehend recent, old, and even zero-day vulnerabilities in addition to all other classical methods such as spam, social engineering, and phishing.

Keshavarzi & Ghaffary's research paper [7] outlines that there is a lack of information about Ransomware and that it should be treated as a separate category from all the other malware. A public database should be created with all the ransomware signatures to take advantage of artificial intelligence and deep learning tools. A potential work claimed by this analysis is the need for more information about the installation phase of Ransomware. This present research study can be seen as a complement to this future research section.

In the academic literature, the Cyber Kill Chain is generic and not tailored explicitly for Ransomware, so here there is an opportunity to modify it or create a different one to make it more suitable for studying Ransomware. For example, the Conti ransomware combines multiple top threats [8] altogether (malware, web-based attacks, phishing, denial of service, spam, botnets structure, data breach, insider threat, physical damages and loss, information leakage). Therefore, identifying the Conti ransomware in an early stage of the Kill Chain can make a difference in preventing the infection.

2.4 Virtualized environments and Conti threat

A virtualized environment [9] on-premises or on the Cloud [10] represents the typical IT infrastructure used by most organizations to provide internal and external services. The ability to deliver a hybrid environment of different operating systems (Windows, Linux) explains the global adoption of this model. A virtualized environment's other essential features are redundancy and hardware resource optimization, enabling security and cost reduction. For Compastié, Badonnel, Festor, and He [11], in a virtual environment, security is vital to deliver business continuity and avoid downtime that would cost a massive amount of money and credibility that will affect the company's reputation and stock market valucations. Technically this is achieved by adding a further layer of abstraction on top of the traditional physical and operating system layers. A Hypervisor type 1 is an operating system that allows other operating systems (virtual machines) to run on top of the same hardware, sharing and optimizing resources. Multiple Hypervisors can be joined together to form a cluster that is connected through a dedicated data switch to the same storage resource, typically a SAN (Storage Area Network). In this scenario, all connections and resources are redundant. Moreover, in case of a hardware or software failure, a virtual machine providing a service can be migrated, even live, from one Hypervisor to another. This setup ensures business continuity, and it is the main reason why most companies adopt it. The business continuity and the data represent the targets of the Conti ransomware to demand a ransom from the victim. This Ransomware has been designed to spread across a virtualized environment through all its network components. In the academic literature, attempts have been made by Arabo, Dijoux, Poulain, and Chevalier about behavioral analysis [12]. However, the fact that the system has to be exposed to a risk, even for just five seconds, before the malware is detected, might not be an appropriate option for a company.

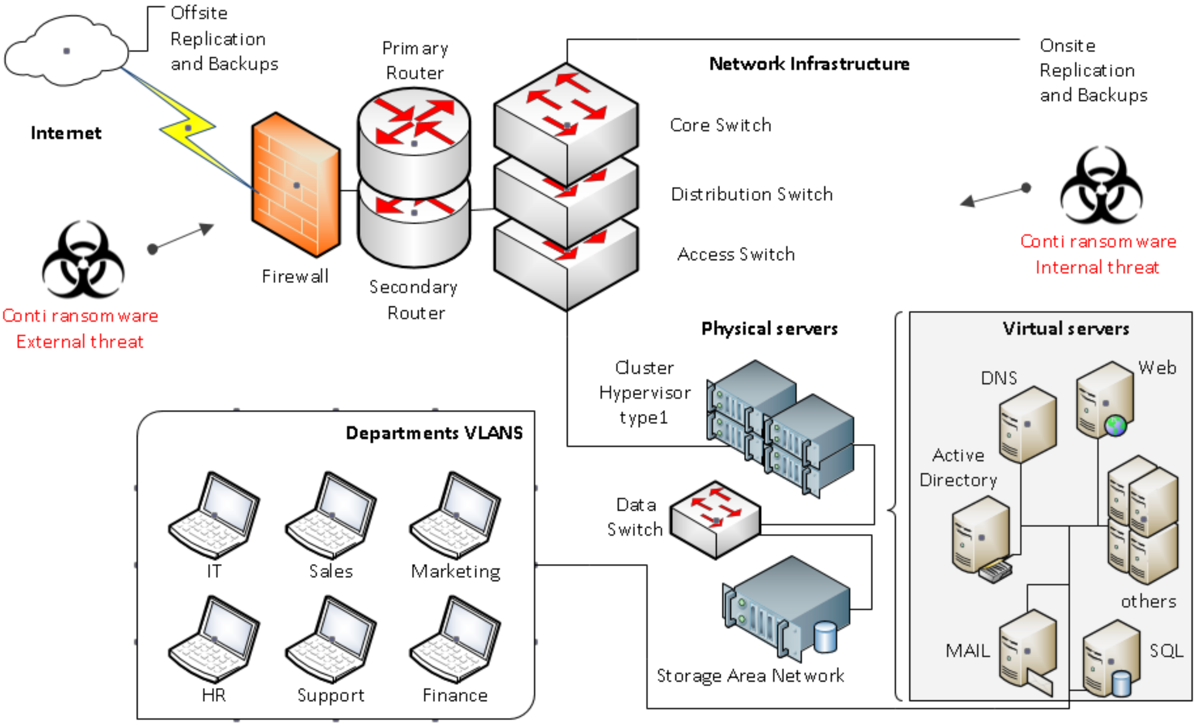


Figure 2 Conceptual Diagram - Virtualized Environment and Conti threats

As found by the senior security research engineer Radu Emanuel Chiscariu, the Conti ransomware uses the NtDelayExecution[6] windows native API to avoid running in a Virtual Machine or a Sandbox. For the successful study of the Conti ransomware, a behavioral-based approach [13] should be taken. However, the implementation could be very complex, employing even an SDN system [14]. Therefore, the challenge of designing a virtual lab has

[6] https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/09/29/conti_ransomwarebehaviorandtechniques-cImV.html

also been taken into consideration as part of this project since there is the opportunity to architect it to be more anonymous and secure.

2.5 Virtual lab design for ransomware analysis

Virtualization technology can be beneficial in creating a virtual environment to study the malware impact because it can be designed to be secure and reproduce the same type of environments that are usually the target of the Conti ransomware. For example, in his study [15], Nasir Alsagoff proposed a safe solution based on the Acronis True Image software, making a bootable rescue disk (read-only). However, this is more suitable for production than a virtual laboratory because it requires a massive effort from the infrastructure administration. The typical steps[7] to building a malware analysis laboratory[16] usually consist of: Resource allocation, software, and hardware; Isolation of the lab from the production environment; The tools for analysis (behavioral-dynamic, code-static, and automated); Install the nested network infrastructure, including targets and attack vectors. It is important to underline that enhanced anonymity is essential in the study of Ransomware as the researcher can be exposed to retaliation[8] by the Conti group. To implement anonymity at a sufficient level is possible to use an approach that combines virtualization, a proxy server, a VPN server, and the Tor [17] network. This design will ensure the network traffic is encrypted and the service provider's real IP is hidden. However, there is an opportunity to implement it locally in the lab so that the servers are hosted internally without disclosing logs.

2.6 Impact analysis approach: static and dynamic

In his research paper [18], Mohammad examines the different methods used to study Ransomware. He concludes that all these malware are so complex that finding a unique methodology is impossible. Still, it is advisable to find the best for each specific ransomware/variant each time. This assumption enforces the research question to find a better-tailored approach to analyze the impact of the Conti ransomware. In the thesis "*Ransomware analysis based on the surface, runtime and static code method*" [19], Usman, Prayudi, and Riadi, have compared the different analysis methods. The static analysis is the approach that can be performed without running Ransomware. This methodology can reveal valuable information such as kill switches and firewall countermeasures. In this research

[7] https://zeltser.com/build-malware-analysis-toolkit/#next-steps

[8] https://www.cnet.com/news/politics/conti-ransomware-group-warns-retaliation-if-west-launches-cyberattack-on-russia/

project, the static method is the one that is prioritized due to its "a-priori" intrinsic nature. On the other hand, the dynamic analysis of Ransomware, such as the one made for the WannaCry [20] by Kao and Hsiao study, suggests the proper tools be used to assess the process, registry, file system, and network activities. More specifically, regarding network traffic analysis, the article "Ransomware Network Traffic Analysis for Pre-encryption Alert" [21] by Moussaileb, Cuppens, Lanet, and Le Bouder states that most Ransomware have the same behavior. However, the dynamic analysis's limitation is that it is only suitable for lab activity but is not helpful as a prevention system because the network has already been infected.

2.7 Existing impact studies about Conti ransomware

The recent study "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method" [22] shows that the Conti ransomware can spread through a network without connection to the C2 server (command and control). The research uses a live forensic methodology and canonical static and dynamic tools, identifying four key stages: preservation, collection, examination, and analysis. However, live forensic is a post-incident approach unsuitable for high availability scenarios, even where the threat is executed for just a few seconds. Other non-academic studies such as "Conti unpacked: understanding ransomware development as a response to detection – a detailed technical analysis"[9] and "Conti Ransomware - How it Works and 4 Ways to Protect Yourself"[10] show the rapid evolution of the Conti ransomware. Here there is the opportunity to augment this knowledge by researching the latest Conti variants that leverage the Log4j and Spring4Shell vulnerabilities.

2.8 Conclusion

The Conti malware academic literature is underdeveloped because this threat is still relatively recent. The high obfuscation effort made by the Conti group has hidden valuable information from researchers. Furthermore, the ability of the Conti ransomware to change and evolve into multiple variants leveraging new vulnerabilities such the Log4j and the Spring4Shell has made the research landscape vast and complex. There is an excellent opportunity to fill the gap in this research project by doing a substantial study of the Conti ransomware and its interaction with a modern virtual environment.

[9] https://assets.sentinelone.com/sentinellabs/conti-ransomware-unpacked

[10] https://www.datto.com/blog/conti-ransomware-how-it-works-and-4-ways-to-protect-yourself

3 Research Methodology

This research has been conducted after an extensive literature review on primary academic resources such as IEEE, Springer, ACM, ScienceDirect, and Google Scholar. The approach followed in the research is the empirical one, where an experiment is performed to produce specific evidence. This evidence, in this case, the impact as the consequence of the Conti malware infection, is subsequently analysed. Finally, the analysis shows the effects of Ransomware on the virtual environment, designed to re-create a real production environment. The research methodology follows a scientific process to generate the required data through appropriate tools that will be underlined in subsequent paragraphs. This process aims to produce tangible scientific results that can be useful for future academic research. The overall process aims to develop correct technical countermeasures and ways to predict malware infection. Increasing the overall knowledge and awareness about the Conti ransomware makes production environments more secure. In this research project a lab architecture has been proposed to recreate a realistic virtual environment maintaining security and anonymity for the researcher. The aim is to study the Conti ransomware impact by simulating the infection. The process observed for the creation of this project is composed of the following steps: the literature review, the design of the virtual lab, the implementation of the virtual lab, including the download of the Conti sample, the experiment (infection of the Conti virus), the data collection (through static, dynamic, and forensic tools), the analysis of the data and its report.

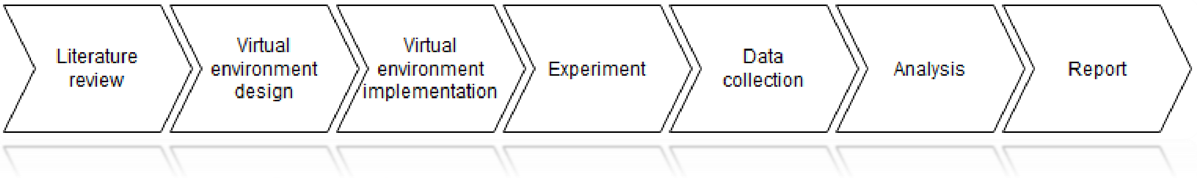

Literature review
Virtual environment design
Virtual environment implementation
Experiment
Data collection
Analysis
Report

Figure 3 Methodology for the Proposed System

This methodology follows a waterfall[11] approach where each stage is completed fully before moving to the next stage. During and at the end of the literature review, the requirements and the analysis have been conducted around the Conti interaction with a modern virtual environment. The virtual environment design represents the next stage, where the system's inception with all the required logical components is created. Finally, the environment implementation includes all the details about the system's final configuration, including

[11] https://en.wikipedia.org/wiki/Waterfall_model

downloading the Conti ransomware sample (for all the steps required during the configuration and entire process, please consult the separate Configuration Manual file). The experiment stage assesses the interaction between the Conti ransomware and the proposed system tailored to be as realistic as possible and at the same time safe for the researcher. First, the data collection is performed using appropriate tools listed in paragraph 3.2 for the static, dynamic, and forensic [23] analysis. Once collected, the data is analysed and evaluated against the research question (paragraph 3.1) to see if the hypothesis is verified or not.

3.1 Research Objectives

The research objectives are obtained from the research question and subquestions: *"What is the impact of the recent Conti Ransomware attack on a Modern Virtualized Environment?"* and the other sub-questions: *"Does the Conti ransomware contain a kill-switch in its source code?", "What is the best virtual environment to test the Conti ransomware, to be as realistic as possible and at the same time secure and anonymous?".*

Research objectives:

- Implement a virtual lab to re-create a realistic architecture to study the Conti ransomware that is at the same time safe and anonymous for the researcher
- Study the interaction of the Conti ransomware with a modern virtual environment
- Scan the Conti ransomware source code to find evidence of hidden mechanisms/functions

3.2 Data and Tools

The data is collected during the experiment by reverse-engineering the source code of the Conti ransomware, recording the changes in the processes, registers, and volatile and persistent memory with dynamic and forensic tools. Static malware analysis is the most secure way to gather data because it works without the need to run the malware itself. A disassembler tool is used to reverse engineer the compiled code. Dynamic analysis or behavioral analysis is used to study the Conti ransomware when running. It is performed with a debugger that runs each instruction in sequence. The information is collected with the tools that record the changes made by the Conti ransomware to the underlying Operating system. The data is also collected by intercepting the network traffic when it is in clear text and not yet encrypted to facilitate the analysis process. The network tool used is Wireshark. Other useful tools in this research are the forensic tools used post-incident and virtualisation features such as snapshots to revert quickly to a safe configuration.

4 Design Specification

4.1 Requirements

The functional and non-functional requirements addressed in the literature review:

- Study the impact of Conti ransomware
- Security Lab for the researcher (Conti group threat) and Hypervisor
- Hardware capable of virtualization
- Re-create a virtual environment as close to reality to minimize malware recognition of sandbox/VM.

4.2 Proposed Architecture

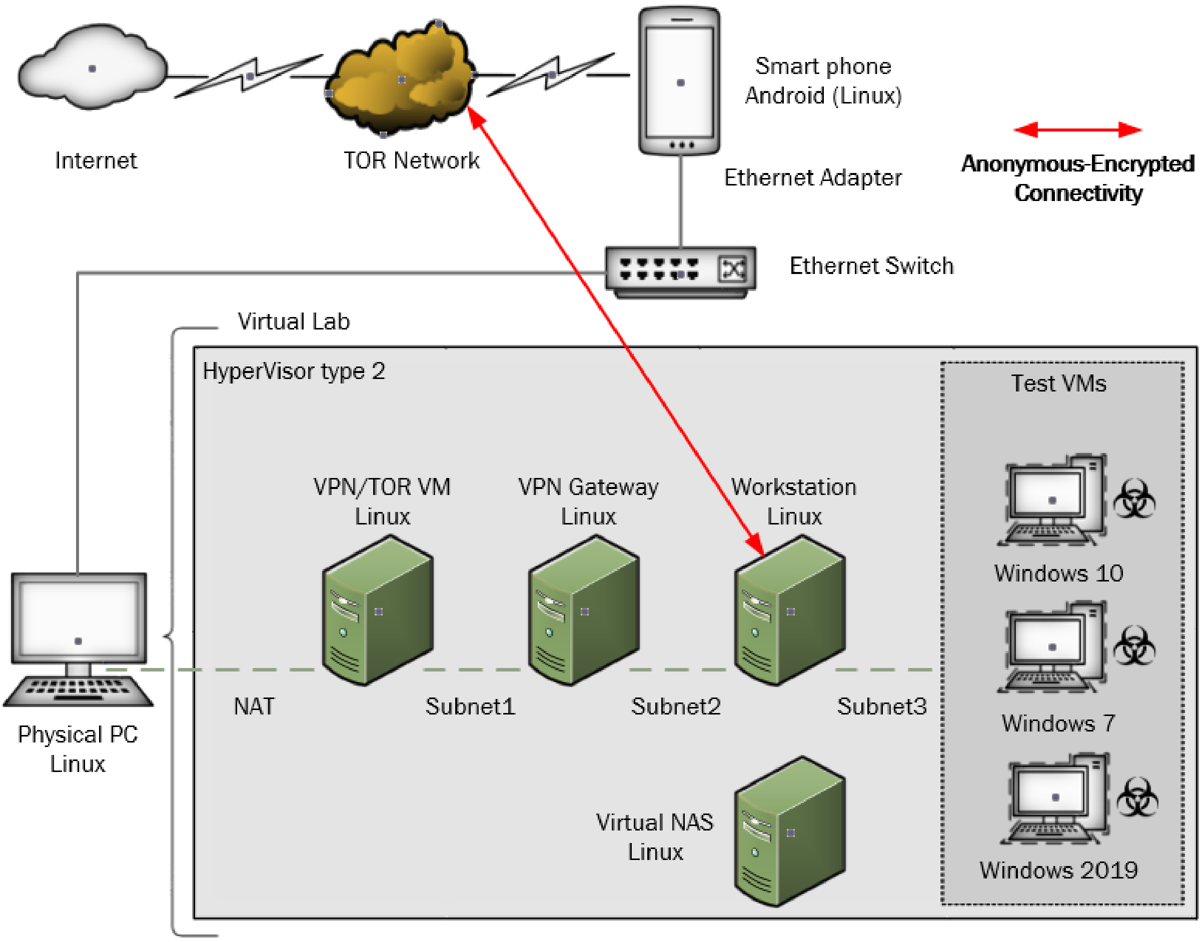


Figure 4 Proposed Architecture

The proposed architecture satisfies the above requirements and the security concerns raised in the literature review for the virtual lab. First, the network and the systems are fully physically isolated from other networks, so there is no risk of infecting any home/organization device.

The internet connection is provided by a mobile device, an Android smartphone, through the ethernet switch to the physical Linux workstation. This host system contains a type 2 Hypervisor capable of virtualizing systems and networks. The network is segmented into different subnets interconnected with Linux gateways. These machines act as routers, sending and receiving packets, and firewalls to have control of the network traffic. Furthermore, each machine can be shut down to isolate the virtual lab part of interest.

A VPN/Tor VM is connected to the physical machine through a NAT (Network Address Translation) that does not allow potential attackers to browse the internal resources of the lab from the outside. The physical machine is detached from the virtual NIC card participating in the NAT itself. A Linux gateway VM will create a VPN connection with the VPN/Tor VM automatically routed to the underlying subnet2 and shared through a DHCP server to Linux Workstation. The Linux workstation is used to download the ransomware sample and intercept the traffic between itself and the test virtual machines populating subnet3 because the traffic is purposely in clear text to facilitate analysis. The test virtual machines are all Microsoft Windows [24] because the Conti ransomware is a malware that affects these operating systems (the recent VMware ESXi Linux variant has not been considered). In addition, a Linux virtual NAS VM is used to share findings and screenshots.

4.3 Security and Anonymity

The security and anonymity aspects of the virtual lab are of fundamental importance for the experiment. It enables a researcher to analyse the ransomware sample minimising the risk of device infection and personal exposure.

- Network isolation: All the setup is built with dedicated hardware and logically separated through subnetting and internal routing. This segmentation easily enables blocking and segregating resources from the internal to the external and vice versa.
- Network entry point: The network connection is made with a cellular phone so that a mobile IP address would be shared in the worst-case scenario, using wired tethering and an ethernet adapter (DHCP server-client)
- Non-vulnerable OS: As the Conti ransomware is a malware that affects the MS Windows OS, all the systems that compose the virtual lab environment are Linux-based, both physical and virtual (Except of course for the Test VMs).
- Anonymity: a VPN is used to encrypt the system traffic, Tor network to hide the real IP, and Proxy to transparently redirect traffic without knowledge of the upper line layer by the machine where the sample is downloaded, executed, and analysed.

5 Implementation

5.1 Software

Hypervisor (type 2)	VMware Workstation 16 Pro (Linux vers.)

Table 1 - Software

5.2 Hardware

Platform	Intel NUC
CPU	i5 (8 threads)
RAM	64 GB.
Drives	1TB NVME SSD + 1TB SATA SSD
Network	1Gbit ethernet adapter
Mobile Device	Samsung Note 10 Lite
Network Adapter	USB-C Ethernet Adapter

Table 2 - Hardware

5.3 Deployment

For the implementation of the lab, all the nodes, both physical and virtual, have been installed with Ubuntu Linux 18.04 LTS (long-term support) because Conti is Ransomware that affects Microsoft Windows OS. Therefore, even in the worst-case scenario of a leak, it would not affect the operational layer and block any malware propagation. The Ubuntu Physical machine runs the software VMware Workstation 16 (Hypervisor type 2), purposely chosen for its ability to create virtual networks (up to 20). The JanusVM[12] is the most external virtual machine of the lab. Its external VNIC (virtual network card) is connected to the internet through the NAT (subnet 172.16.247.0/24) of the Ubuntu 18.04 physical machine.

The NAT ensures from a security perspective that it can not be browseable from the outside (physical machines network layer). The internal VNIC instead is the subnet 192.168.10.0/24 shared only with the Ubuntu Linux Gateway VM. The JanusVM provides a VPN and Tor server. The Ubuntu Linux Gateway V.M. is a client for the JanusVM on its external VNIC

[12] https://blog.malwarebytes.com/threat-analysis/2012/04/anonymizing-traffic-for-your-vm-and-capturing-traffic/

and a firewall/router in its internal VNIC subnet 192.168.20.0/24. So all the VMs that will automatically obtain an IP address from the DHCP server of the Ubuntu Linux Gateway will be connected transparently with VPN encrypted traffic to the Tor network without any knowledge of the underlying network infrastructure.

Remnux Linux, a specific Ubuntu 18.04 VM with added tools for malware analysis, is the client of the Ubuntu Linux Gateway VM and is connected with its internal VNIC, subnet 192.168.30.0/24, to the test VMs. These VMs have Microsoft Windows Operating Systems installed to reproduce a modern virtual environment and study the impact of the Conti ransomware. The OpenMediaVault Linux is a NAS (Network-Attached Storage) to facilitate data sharing (screenshots, data sharing, and malware samples) in the test VMs subnet.

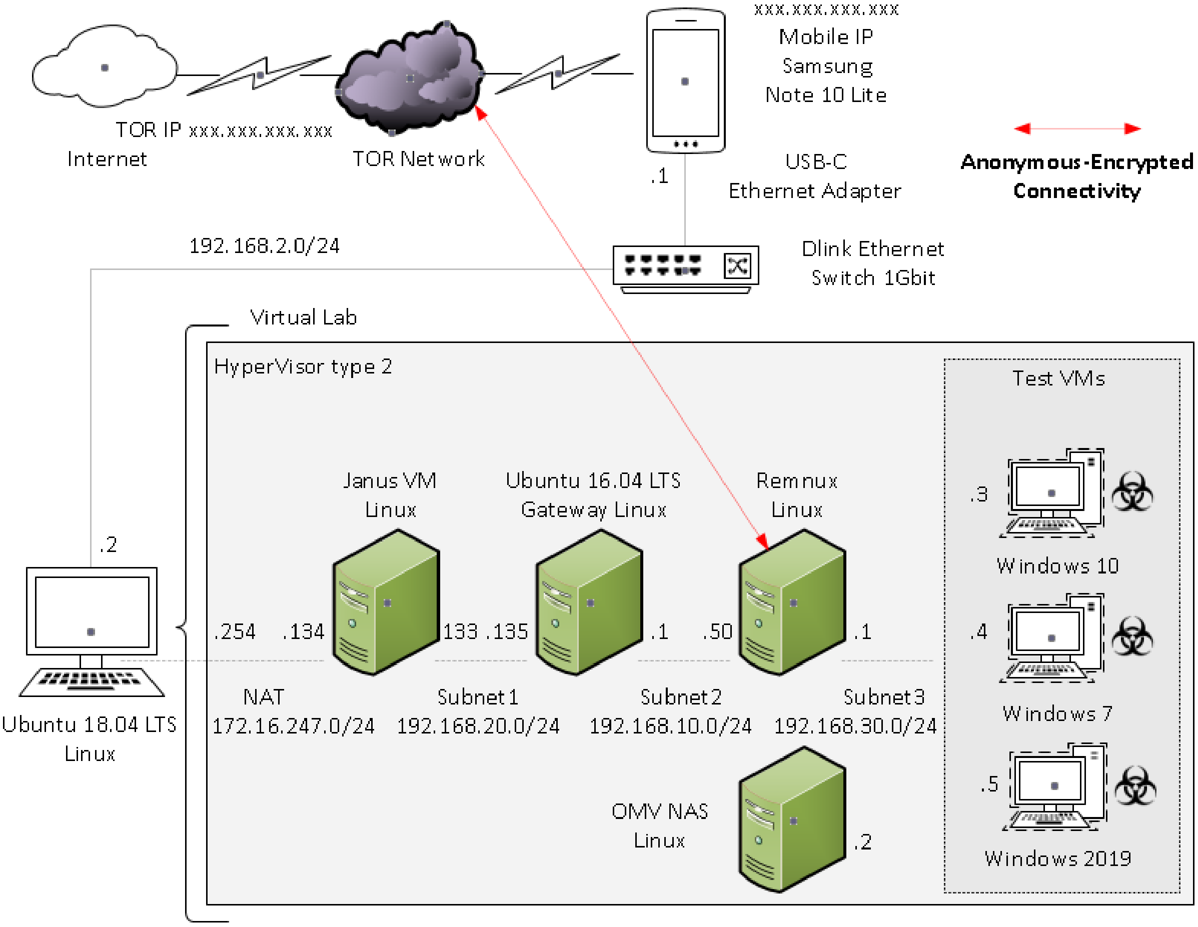


Figure 5 Implemented Architecture

5.3.1 Model implemented features

The implemented architecture has the flexibility of isolating each node of the chain by shutting down the systems that are no longer needed. For example, to block any connectivity with the "outside world" it is sufficient to power off the JanusVM, Ubuntu Linux Gateway, or both. Another good feature of this implementation is that on all the subnet3, the traffic is not yet encrypted with the VPN so this facilitates traffic capture and analysis. At the same time, the researcher can be safe because the traffic going external is automatically encrypted and anonymized with the Tor network when it reaches subnet1 and subnet2.

5.4 Tools

5.4.1 Static analysis tools

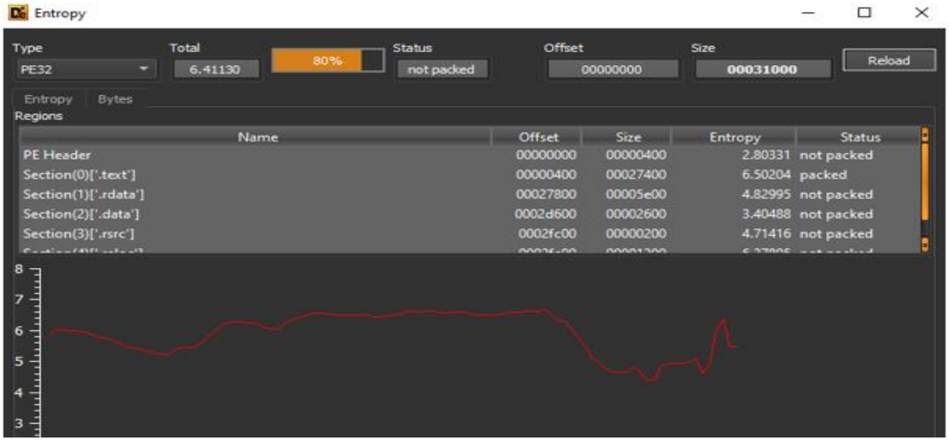
Identifiers: PeID, PeSudio, Olly. Debuggers: Ida Pro. Disassemblers: Ghidra.

5.4.2 Dynamic analysis tools

Network emulators: FakeNet-NG. Network analyzers: Wireshark.

5.4.3 Conti Sample

The sample has been downloaded from the website MalwareBazaar[13] dated 2021-05-26 the same period when the Conti virus was used to attack the Irish H.S.E. (Health Service Executive).



Type: PE32
Total: 6.41130 80%
Status: not packed
Offset: 00000000
Size: 00031000

Regions

Name	Offset	Size	Entropy	Status
PE Header	00000000	00000400	2.80331	not packed
Section(0)['.text']	00000400	00027400	6.50204	packed
Section(1)['.rdata']	00027800	00005e00	4.82995	not packed
Section(2)['.data']	0002d600	00002600	3.40488	not packed
Section(3)['.rsrc']	0002fc00	00000200	4.71416	not packed

Figure 6 – Conti Sample Entropy

The entropy value found with the utility Detects It Easy is 80%, indicating a high probability that the sample is not packed. The file has been renamed conti.exe to efficiently locate it during experiments and analysis.

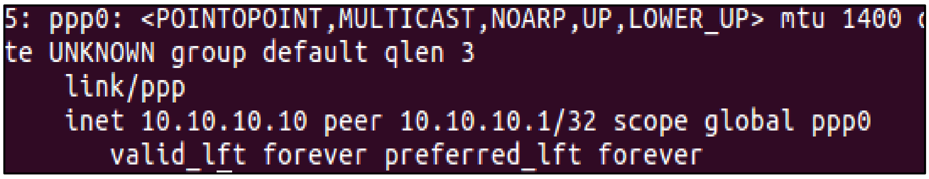
Hash SHA256 58ca4e482db7cf5c924256e53d8516d422e76cf4b85b43dc2b9ba0c7cb471ff7 verified (more details in the configuration manual).

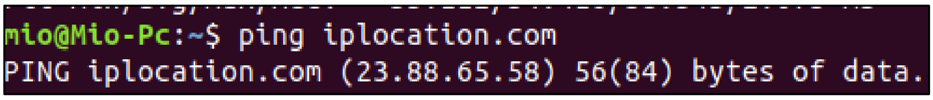
[13] https://bazaar.abuse.ch/

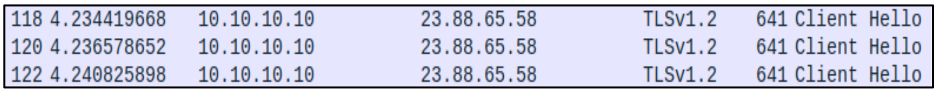
6 Evaluation

6.1 Experiment 1 - Virtual Lab Security Testing

The network capture shows encrypted packets and IP 185.220.100.255 Latitude 49.5985 Longitude 10.997 Country Germany instead of Ireland's actual location. The real IP is replaced by the one acquired when joining the Tor network. The Onion router is a network of nested routers where the connection bounces from one node to another with encrypted communications that do not track activities in their logs. This technology can be used for malevolente purposes (dark web) or security reasons like in this project.

Lab VM Ip
VPN tunnel
	
	`5: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1400`
	`te UNKNOWN group default qlen 3`
	`    link/ppp`
	`    inet 10.10.10.10 peer 10.10.10.1/32 scope global ppp0`
	`       valid_lft forever preferred_lft forever`

Ip location
website url
	
	`mio@Mio-Pc:~$ ping iplocation.com`
	`PING iplocation.com (23.88.65.58) 56(84) bytes of data.`

Encrypted packets captured	
	`118 4.234419668   10.10.10.10   23.88.65.58   TLSv1.2   641 Client Hello`
	`120 4.236578652   10.10.10.10   23.88.65.58   TLSv1.2   641 Client Hello`
	`122 4.240825898   10.10.10.10   23.88.65.58   TLSv1.2   641 Client Hello`

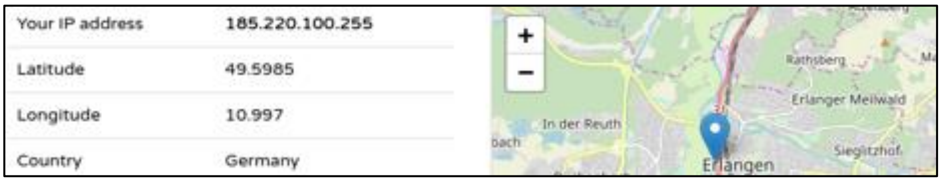
Hidden Ip of VM transparently joined Tor.	 Your IP address 185.220.100.255 Latitude 49.5985 Longitude 10.997 Country Germany + − Rathsberg Erlanger Meilwald In der Reuth bach Sieglitzhof Erlangen

Table 3 – Virtual Lab Security Testing and Findings

Evidence shows that precise information is not disclosed, the underlying virtualization layer is fully transparent, and the traffic from the Linux Gateway to the external is not sent in clear text. These features secure the research activities when studying the communication between the Conti ransomware and the CNC server.

6.2 Experiment 2 - Static Analysis

6.2.1 Kill Switches

A kill switch is essentially a sort of "if" statement in the malware source that, if a condition is met, it would not trigger an action; otherwise, it will stop. Furthermore, a kill switch can be used by a hacker as an anti-sandbox mechanism or as a private function to terminate malware operations and erase logs and the virus itself. For instance, in regards to the Wannacry

Ransomware, the encryption process started if a specific internet domain was unavailable. This experiment looked at the Conti source code for evidence of kill switches.

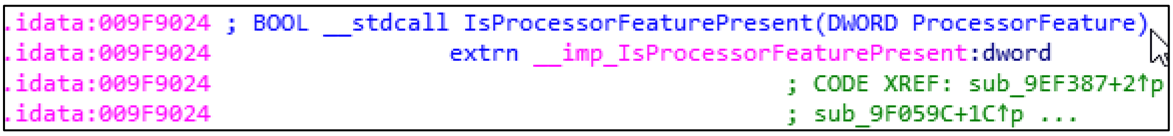
The "pestr" command utility in Remnux Linux workstation run against the sample conti.exe has not shown any string related to a potential domain address that could be used as a kill switch for the Ransomware.

```
# pestr conti.exe | grep -ie “http” -ie “www” > killswitchcheck.txt
```

Figure 7 – Killswitch code snippet

6.2.2 Encryption Mechanism

The sample conti.exe has been analyzed with the disassembler Ida to check the source code for functions/APIs used during the encryption process. In the imports, the function __imp_IsProcessorFeaturePresent is used to determine whether or not the CPU has AES dedicated instructions. In this second case, the algorithm ChaCha20 [25] will be used in place of AES for the encryption. The reason is that ChaCha20[14] generally can run on any 32-bit CPU faster than AES, making it more suitable for blind attacks.



```
.idata:009F9024 ; BOOL __stdcall IsProcessorFeaturePresent(DWORD ProcessorFeature)
.idata:009F9024                 extrn __imp_IsProcessorFeaturePresent:dword
.idata:009F9024                                         ; CODE XREF: sub_9EF387+2↑p
.idata:009F9024                                         ; sub_9F059C+1C↑p ...
```

Figure 8 – Ida Pro Imports detail

6.3 Experiment 3 - Dynamic Analysis

6.3.1 Offline vs. Online Execution

Conti has been executed offline, the virtual machine wholly isolated from the external, and online, the virtual machine connected to the internet through the designed architecture. Results have shown that the encryption process is accomplished in both scenarios; however, in the offline one, the message is false (that the Conti hacker group claims to own the victim's data). This is not true because there is no interaction between the offline virtual machine and the Conti group CNC server.

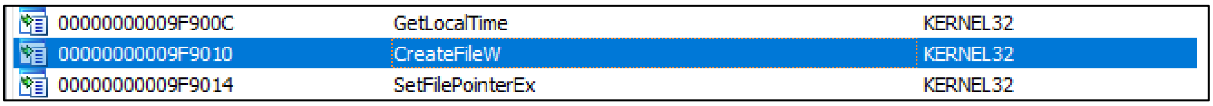
The Conti ransomware scans the local network using the Windows API GetIpNetTable and starts ARP requests to all the potential IP addresses inside the subnet. It has a multi-thread option with the parameter -m that will enable running up to 32 parallel processes to perform all the malicious operations quicker. Conti will attempt to spread throught all the networks as it is possible to see in the network capture attached zip file.

[14] https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html

6.3.2 Open Shares vs. Protected Shares

Conti executed with the -all parameters will attempt to propagate over the network, checking the configuration in use and pinging all the devices within the same subnet.

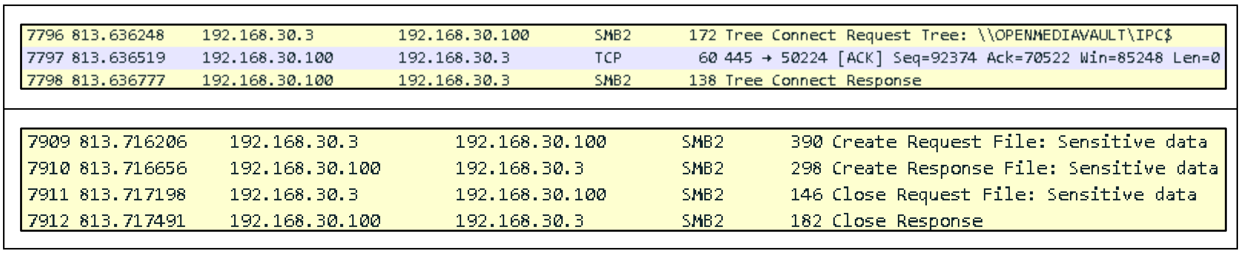
Once a suitable target is found, it will connect and request to scan folders and subfolders to encrypt all the data. Each folder will leave a copy of the readme.txt file with ransom instructions.



```
00000000009F900C    GetLocalTime       KERNEL32
00000000009F9010    CreateFileW        KERNEL32
00000000009F9014    SetFilePointerEx   KERNEL32
```

Figure 9 -Function used to write the encrypted file

The results show that the Ransomware has encrypted the open share in the OpenMediaVault server with reading and write rights.

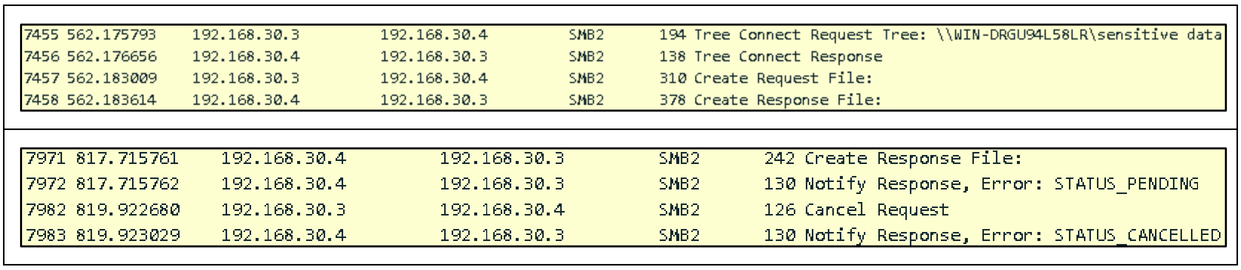


```
7796 813.636248    192.168.30.3      192.168.30.100    SMB2    172 Tree Connect Request Tree: \\OPENMEDIAVAULT\IPC$
7797 813.636519    192.168.30.100    192.168.30.3      TCP      60 445 → 50224 [ACK] Seq=92374 Ack=70522 Win=85248 Len=0
7798 813.636777    192.168.30.100    192.168.30.3      SMB2    138 Tree Connect Response

7909 813.716206    192.168.30.3      192.168.30.100    SMB2    390 Create Request File: Sensitive data
7910 813.716656    192.168.30.100    192.168.30.3      SMB2    298 Create Response File: Sensitive data
7911 813.717198    192.168.30.3      192.168.30.100    SMB2    146 Close Request File: Sensitive data
7912 813.717491    192.168.30.100    192.168.30.3      SMB2    182 Close Response
```

Figure 10 – Network Capture of Conti File Encryption on an open share

Instead, the SMB file share on the Windows Server has not been encrypted. From the network, capture is possible to see that attempts have been made; however, that malware doesn’t have the capability to exploit vulnerabilities or make brute force/dictionary attacks. This result clearly shows that the Conti ransomware needs a human component to be effective and dangerous, otherwise, it will only be able to perform simple attacks that are easily stoppable by implementing a minimum layer of security.



```
7455 562.175793    192.168.30.3    192.168.30.4    SMB2    194 Tree Connect Request Tree: \\WIN-DRGU94L58LR\sensitive data
7456 562.176656    192.168.30.4    192.168.30.3    SMB2    138 Tree Connect Response
7457 562.183009    192.168.30.3    192.168.30.4    SMB2    310 Create Request File:
7458 562.183614    192.168.30.4    192.168.30.3    SMB2    378 Create Response File:

7971 817.715761    192.168.30.4    192.168.30.3    SMB2    242 Create Response File:
7972 817.715762    192.168.30.4    192.168.30.3    SMB2    130 Notify Response, Error: STATUS_PENDING
7982 819.922680    192.168.30.3    192.168.30.4    SMB2    126 Cancel Request
7983 819.923029    192.168.30.4    192.168.30.3    SMB2    130 Notify Response, Error: STATUS_CANCELLED
```

Figure 10 – Network Capture of Conti File Encryption on a protected share

6.4 Discussion

The findings show that the implementation of the virtual lab has been successful. The researcher can conduct his experiments without the fear of being tracked because the IP address and the network packets are protected. The analysis of the source code has not revealed any kill switch mechanism. The Conti group most likely wanted to reduce the probability of stopping the Ransomware and avoid what happened with the Ransomware Wannacry. Regarding the encryption mechanism has been observed that a function checks if the CPU has AES features. Otherwise the Chacha8 algorithm will be utilize because it is more general purpose and will work faster on any CPU architecture. The dynamic analysis shows that running the Conti in an offline environment reduces its capabilities, and the readme.txt claims to own the user data when it is actually not true. Conti can spread inside the network but, without human supervision, can not leverage exploits to gain access to third resources. Findings also underline that implementing minimum security, such as simple authentication to a network share, prevents Conti from encrypting the victim's data.

7 Conclusion and Future Work

In conclusion, the Conti ransomware represents one of the most dangerous pieces of malware that has targeted many big companies and governments, such as the HSE (Irish Health Service Executive) in recent times. The Conti gang is an international criminal organisation composed of multiple dangerous skilled members - thus having a safe environment to study the malware is of vital importance for the researcher himself and to study the state of art ransomware behaviour. The aim of this research was to increase the overall knowledge about Conti ransomware and its impact on a virtualized environment. This research proposes a secure architecture that allows the researcher to study safely the Conti ransomware by implementing the CIA principles. Furthermore, the malware analyst can focus his efforts on the ransomware itself because confidentiality is provided automatically by the virtual lab (VPN and Tor network).

To the best of my knowledge, I did not find evidence of kill switches inside the Conti ransomware code during this project. Mainly for two reasons; the first is that the authors wanted to maximise the threat danger, and secondly, being interactive (Conti accepts console parameters for its execution) the authors want to target specific files from another compromised PC used as a pivot. Offline backups are the best way of remediation against ransomware, so the Conti group targets environments where business continuity is vital such as healthcare, and restoration time is not an option. Results show that without a human 20 component, the malware can be stopped by enforcement of a simple and minimum layer of security like authentication.

Future researchers can benefit from this project to study all the ransomware features in more depth. Given a higher level of time and resources, I would have liked to explore more. This work can be improved by enhancing the number of experiments with several target virtual machines. Future research could utilize a more agile approach rather than a waterfall methodology to allow more flexibility in adapting the process methodology during the experiment. This research and the proposed architecture can be extended for future work to study Conti variants and other ransomware. This project infrastructure could also be potentially implemented in a cloud version by simply porting the virtual machines in AWS, Azure, or similar environments.

8 References

[1] P. R. Kumar and H. R. E. B. H. Ramlie, 'Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques', in *Computational Intelligence in Information Systems*, Cham, 2021, pp. 205–214. doi: 10.1007/978-3-030-68133-3_20.

[2] S. Young, 'When ransomware strikes, what's your recovery plan?', *Netw. Secur.*, vol. 2021, no. 7, pp. 16–19, Jul. 2021, doi: 10.1016/S1353-4858(21)00077-5.

[3] 'The Ransomware-as-a-Service economy within the darknet | Elsevier Enhanced Reader'. https://reader.elsevier.com/reader/sd/pii/S0167404820300468?token=273B136E5DF1D0FEF0C027C477DE4725275524E037FB776AECB70132689596A0C0FA5375CAC825258D135C7E87069F23&originRegion=eu-west-1&originCreation=20220403162624 (accessed Apr. 03, 2022).

[4] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, 'Ransomware: Recent advances, analysis, challenges and future research directions', *Comput. Secur.*, vol. 111, p. 102490, Dec. 2021, doi: 10.1016/j.cose.2021.102490.

[5] 'Major ransomware campaign targets healthcare facilities in US', *Comput. Fraud Secur.*, vol. 2020, no. 11, pp. 1–3, Nov. 2020, doi: 10.1016/S1361-3723(20)30112-3.

[6] Q. K. A. Mirza, M. Brown, O. Halling, L. Shand, and A. Alam, 'Ransomware Analysis using Cyber Kill Chain', in *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2021, pp. 58–65. doi: 10.1109/FiCloud49777.2021.00016.

[7] M. Keshavarzi and H. R. Ghaffary, 'I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion', *Comput. Sci. Rev.*, vol. 36, p. 100233, May 2020, doi: 10.1016/j.cosrev.2020.100233.

[8] H. Kettani and P. Wainwright, 'On the Top Threats to Cyber Systems', in *2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT)*, Mar. 2019, pp. 175–179. doi: 10.1109/INFOCT.2019.8711324.

[9] İ. Arslan and İ. G. Özbilgin, 'Virtualization and security: Examination of a virtualization platform structure', in *2017 International Conference on Computer Science and Engineering (UBMK)*, Oct. 2017, pp. 221–226. doi: 10.1109/UBMK.2017.8093379.

[10] N. Jain and S. Choudhary, 'Overview of virtualization in cloud computing', in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, Mar. 2016, pp. 1–4. doi: 10.1109/CDAN.2016.7570950.

[11] M. Compastié, R. Badonnel, O. Festor, and R. He, 'From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models', *Comput. Secur.*, vol. 97, p. 101905, Oct. 2020, doi: 10.1016/j.cose.2020.101905.

[12] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, 'Detecting Ransomware Using Process Behavior Analysis', *Procedia Comput. Sci.*, vol. 168, pp. 289–296, 2020, doi: 10.1016/j.procs.2020.02.249.

[13] M. Kim, T. J. Lee, Y. Shin, and H. Y. Youm, 'A study on behavior-based mobile malware analysis system against evasion techniques', in *2016 International Conference on Information Networking (ICOIN)*, Jan. 2016, pp. 455–457. doi: 10.1109/ICOIN.2016.7427158.

[14] M. A. S. Monge, J. M. Vidal, and L. J. G. Villalba, 'A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation', in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg Germany, Aug. 2018, pp. 1–10. doi: 10.1145/3230833.3233249.

[15] S. N. Alsagoff, 'Malware self protection mechanism issues in conducting malware behaviour analysis in a virtual environment as compared to a real environment', in *2010 International Symposium on Information Technology*, Jun. 2010, vol. 3, pp. 1326–1331. doi: 10.1109/ITSIM.2010.5561600.

[16] J. Peppers, 'Creating a Malware Analysis Lab and Basic Malware Analysis', p. 44.

[17] E. Ramadhani, 'Anonymity communication VPN and Tor: a comparative study', *J. Phys. Conf. Ser.*, vol. 983, p. 012060, Mar. 2018, doi: 10.1088/1742-6596/983/1/012060.

[18] A. Mohammad, 'Ransomware Evolution, Growth and Recommendation for Detection', *Mod. Appl. Sci.*, vol. 14, p. 68, Feb. 2020, doi: 10.5539/mas.v14n3p68.

[19] L. Usman, Y. Prayudi, and I. Riadi, 'Ransomware analysis based on the surface, runtime and static code method', *J. Theor. Appl. Inf. Technol.*, vol. 95, pp. 2426–2433, Jun. 2017.

[20] D.-Y. Kao and S.-C. Hsiao, 'The dynamic analysis of WannaCry ransomware', in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2018, pp. 159–166. doi: 10.23919/ICACT.2018.8323682.

[21] R. Moussaileb, N. Cuppens, J.-L. Lanet, and H. Le Bouder, 'Ransomware Network Traffic Analysis for Pre-encryption Alert', in *Foundations and Practice of Security*, Cham, 2020, pp. 20–38. doi: 10.1007/978-3-030-45371-8_2.

[22] R. Umar, I. Riadi, and R. S. Kusuma, 'Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method', *IJID Int. J. Inform. Dev.*, vol. 10, no. 1, pp. 53–61, Jun. 2021, doi: 10.14421/ijid.2021.2423.

[23] I. Kara and M. Aydos, 'The rise of ransomware: Forensic analysis for windows based ransomware attacks', *Expert Syst. Appl.*, vol. 190, p. 116198, Mar. 2022, doi: 10.1016/j.eswa.2021.116198.

[24] T. R. Reshmi, 'Information security breaches due to ransomware attacks - a systematic literature review', *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100013, Nov. 2021, doi: 10.1016/j.jjimei.2021.100013.

[25] P. McLaren, W. J. Buchanan, G. Russell, and Z. Tan, 'Deriving ChaCha20 key streams from targeted memory analysis', *J. Inf. Secur. Appl.*, vol. 48, p. 102372, Oct. 2019, doi: 10.1016/j.jisa.2019.102372.