Utilizing Capa in Kali Linux for Wannacry Malware Identification and Analysis

Pritiy Singgam¹ Afifah Naila Nasution² Pedro Stella Mario Meyar Waruwu³

Computer Science Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Medan, Indonesia¹

Mathematic Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Medan, Indonesia^{2,3}

Email: pritymirota@gmail.com1

Abstract

Purpose: This study aims to analyze the WannaCry ransomware using Kali Linux and the Common Access Platform Assistant (CAPA) method to provide a deeper understanding of the malware's attack tactics, capabilities, and behaviors. Methods/Study design/approach: The research was conducted by installing CAPA version 7.4.0 downloaded from GitHub, followed by file extraction and access permission configuration. The WannaCry malware was obtained from the "thezoo" repository on GitHub, extracted, and analyzed using CAPA commands in the Linux terminal. The analysis results were presented in tables showing the malware's tactics, techniques, and behaviors. Result/Findings: The analysis revealed that CAPA effectively identified various tactics and techniques used by WannaCry, confirming its classification as malware. Validation through antivirus services indicated that 68 out of 72 services flagged the file as malicious, emphasizing the importance of robust cybersecurity measures. Novelty/Originality/Value: This study offers new insights into the working mechanisms of WannaCry ransomware and highlights the effectiveness of the CAPA method in malware analysis. The findings contribute to a better understanding of cybersecurity threats and provide valuable information for professionals in the field to enhance defense strategies against malware.

Keywords: WannaCry Ransomware, Malware Analysis, Kali Linux, Common Access Platform Assistant (CAPA), Cybersecurity



This work is licensed under a <u>Creative Commons Attribution-NonCommercial 4.0 International License</u>.

INTRODUCTION

Kali Linux is the world's most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. The advancement of computer and Internet technology has changed our lives, and it has revolutionized the way organizations conduct businesses. However, technological evolution and digitization have given rise to cybercriminal activities. The growing threat of cyberat tacks on critical infrastructure, data centers, private/public, defense, energy, government, and financial sectors pose a unique challenge for everyone from an individual to large corporations. These cyberat tacks use malicious software (also known as Malware) for financial theft, espionage, sabotage, intellectual property theft, and political motives. Symantec's Internet Security Theart Report on the infection of malicious software attacks that use cryptographic techniques that threaten to publish a victim's data or permanently block access with a ransom or so-called ransomware continues to increase, and in May 2017 a new ransomware was identified that encrypts data, as well as makes copies of itself and gives time to pay, warning that the victim's files will be deleted. This type of ransomware is known as wannacry.

RESEARCH METHODS

In this research we use kali linux which kali linux functions as an operating system that analyzes malware such as wannacry ransomware with the CAPA (Common Access Platform Assistant) method. The first step is the installation of capa which is downloaded via github, then we use the v7.4.0 release. We extract it first then After extracting we open the terminal then to give access we use the command "chmod += capa". then enter capa with the command "./capa" then the capa version will come out. To add malware we take it on "thezoo github", then we can download the desired malware. We took the WannaCry Ransomware. After downloading, we open the file manager and then extract the file, when extracted there will be a password request where the password is "infected". We enter the command "./capa then drop the malware file that we have extracted. The result that comes out is the WannaCry Ransomware table which contains attack tactics, capabilities and behavior.

RESEARCH RESULT AND DISCUSSION

Picture 1 and Picutre 2 are the results of testing malware in linux times using capa. The capa is in accordance with what is suggested by the CAPA documentation where the capa we use supports python 3.8 and python 3.9.



Picture 1. (Table of Ransomware WannaCry)

Capability	Nanespace		
high-dats with CHC2 (2 matches) encrypt data using AGK (3 matches) entrate directory (3 matches) extrate directory (3 matches) eth classes (4 matches) eth file attributes (5 matc	data-manipulation/ceckum/cccl2 data-manipulation/ceckum/cccl2 data-manipulation/exccppino/as data-manipulation/exccppino/2es data-manipulation/exccppino/2es data-manipulation/exccption/cc data-manipulation/exccption/cc data-manipulation/exccption/cc bost-interaction/file-system host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/crast host-interaction/file-system/read host-interaction/file-system/read host-interaction/file-system/read host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste host-interaction/registry/craste		
[pritysinggam@pritys)-[-/Documents] [(pritysinggam@pritys)-[-/Documents]			

Picture 2. (Table of Ransomware WannaCry)

In both tables from Picture 1 and Picture 2 we can see that there are attack tactics and techniques, then MBC Objective and MBC Behavior tables and finally Capabilities and namespaces. The next table of Picture 1.3 is to prove whether the wannacry ransomware is really malware. the results show that 68 out of 72 antivirus services mark this file as malicious or containing a virus.

and round forming	ng] - Oracle VM	/irtualBox				-		×
File Machine	View Inp	ut Devices	Help					
🛛 📼 🖬 💊 🍪	• 1 2	3 4 🛛 📰 💇	0 -	to more and	•	A 0	23:44	≙ ¢
0 Release v7.4.0	-mandian: ×	/irusTotal - File - ed0	Oleb 🛪 🔣 Eile an	d Directory Permis				
	O A https:/	/www.virustotal.com	m/gui/file/ed01eb1b	c9eb5bb 999%	ជ	0 3		
Kali Linux 🧟 Kali To	ols 🚊 Kali Docs 🐒	Kali Forums 🛛 式 Ka	li NetHunter 💊 Exp	oloit-DB 💊 Goog				
a, un, master								Carlos
68	est01ebft	c9eb5bbea545a44d01b45f	1071661840490439c6e5.				28.	
	diskport			3.35 MB	3 minutes ag		EXE	
Comments	alation of the later	vister detect debug and okspace safe were per	institute the shape	checks notwork adapters	evertay) in			
					 1980 (Fig. 1) 			
	thethics			minare	an chain			
	(distant			Indexe				
	DETAILS RELATIO	ne legat (mecane despe NS BEHAVIOR	community 30-	Hulaure				
DETECTION Juin our Commun	thesis BETAILS RELATIO	er legat (encodes despected IS BEHAVIOR permutity insight and co	of the somework allow COMMUNITY (3)=)	instant	sate checks.			
DETECTION	(thester DETAILS RELATIO	er land executed disponents NS BEHAVIOR Demonstry insights and on	d Ris Statements alone COMMUNITY (20)- own/bourced detections, p	nutrane tian an API key to autor	sate checks,			
DETECTION Join out Commun Popular threat	Cohestion DETAILS RELATIO By and enjoy additional of chronomeant wathformy waterstarygeter	en region Venticies despon NS BEHAVIOR Demoustry insights and co Threat categories	d file () set somewiskers COMMUNITY (201) Investoranced detections, p S () someway () () space)	mulmum flat an API key to autoor Family label	sate checks.			
DETECTION Join our Commun Popular threat Isaet Security venders' a	Example and enjoy additional of an example additional of an example additional of a second range additi	en tiget () electrics despen NS BEHAVIOR permussity insights and on Threat categories	d Rie (194 sommers also COMMUNITY (202) Sweltssurced detections, p 8 (secondarie) (togae)	walken kar an API key to autom Family labet	sate checks, B. warracry Do you wa	Teamacopal Into actors	ter autor	
DETECTION Jain our Commun Propular threat Intel Security vendors' a Arelab V3	ettessis BETANIS RELATION BETANIS RELATION BETANIS RELATION SETESSIS BETANIS B	en kiget en sons e en sons en	effic (university) COMMUNITY (35-) Invertionment (single) Communities (single) Communities (single) Communities (single)	malaum han an API key In aidean Family labet	safe.shecks, Is warrany Do you wa	(mercecce) nt to actors	iei (warn are checks: 20010	
DetTECTION Join and Common Index With Common Security wenders' of Arelub-V3 Arelub-V3	disease d	en light encodes depart AS BEMANIOS Demonstry integrits and co Thread categories 2. Waterood copyright R200571 1	COMMUNETY 2021 communed detections, p s teammak angle database Althout	nusionan Alla on All key to andere Family label O Record	sate checks, Is wannary Do you wa pro: Win22 Wiat	Summer of the Surface out to Surface marking at (1) marking at (1)	ter ann ate checks 20010	
BETECTION Jain sur Commun Index Security vendors' a Security vendors' Articute V3 Articute V3 Articute V3	DetAils ReLATIO DetAils ReLATIO Reg and anyor solidional of anomalies solidional anomalies and another anomalies another another anom	en Inpert en Characteristen Annuel en Contemporative International Contemporative Thread Categories Contemporative Internative Contemporative Internative Contemporative Co	COMMUNETY 2021	mainen Art key te anfast Family label O Ross O Tealis O Tealis	nate shecks, B - annany Do you ao une Win 12 W at In Remont Wat	into actors ni to actors naCryster anCryster	ter (ware are checks 20010	
DETECTION Jain sur Commun Index Security vendors' of Articute's Articute's Articute's Articute's Articute's Articute's	DETAILS RELATION DETAILS RELATION RECARD CALLER AND CALLER CONTRACTOR AND CALLER CONTRA	er layor events descent descent vis BESMVIDB Descents integers and con Threat categories 2 Warens-Cryster #200271 a con_WHC22 Warens Cryster #2(1)	COMMUNETY 201 COMMUNETY 201 Communed detections, p Althouse Althous Althous Althous Althous Althous	numbers Alexan and API key to addeet Farmity label O Rosse O Tropie O Tropie	sate shecks, It wantery Do you wa per Win22 Wait in Remon War in Remon War 2 Ward Cry A [1	into sutor nt to sutor nuCryptor suCryptor (i)	ner (waren ate checks) bitoto 4	

Picture 3. (VirusTotal of Ransomware WannaCry)



CONCLUSION

This research demonstrates the use of Kali Linux and the Common Access Platform Assistant (CAPA) method to analyze the WannaCry ransomware. Through the installation and implementation of CAPA, the analysis revealed detailed insights into the attack tactics, capabilities, and behaviors associated with WannaCry, and confirmed its classification as malware. In addition, the validation of WannaCry as malware, was reinforced by external evaluations. Of the 72 antivirus services that reported the ransomware as a threat. The majority of them highlighted the malicious nature of the malware and emphasized the importance of strong cybersecurity measures to counter the threat. In summary, this analysis not only provides a deeper understanding of the working mechanism of the WannaCry ransomware, but also highlights the effectiveness of the CAPA technique in malware analysis and provides valuable insights in the field of cybersecurity.

BIBLIOGRAPHY

- Asaad, R. R. (2021). Penetration testing: Wireless network attacks method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12.
- Konecka, S., Bentyn, Z. (2024). Cyberattacks as Threats in Supply Chains. European Research Studies Journal. (27) 3 : 778-796
- Pandey, A. K., et al. (2020). Trends in malware attacks: Identification and mitigation strategies. In Critical Concepts, Standards, and Techniques in Cyber Forensics (pp. 47–60). IGI Global.
- Wijaya, A. H., & Fitrani, A. S. (2019). Wannacry identification for computer data security. JICTE (Journal of Information and Computer Technology Education), 3(1), 22–28.