UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Digital Forensics

Semester II (2022 – 2023)

**REGISTRY SPY AND OPEN EDR**

Student 1: Võ Anh Kiệt - 20520605

Student 2: Nguyễn Bùi Kim Ngân - 20520648

Student 3: Nguyễn Bình Thục Trâm - 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

**Hồ Chí Minh City, June 2023**

UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Digital Forensics

Semester II (2022 – 2023)

**REGISTRY SPY AND OPEN EDR**

Student 1: Võ Anh Kiệt - 20520605

Student 2: Nguyễn Bùi Kim Ngân - 20520648

Student 3: Nguyễn Bình Thục Trâm - 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

**Hồ Chí Minh City, June 2023**

Acknowledgement

To begin, we would like to thank our advisor, PhD Nguyễn Tấn Cầm, for his direction and consistent monitoring, as well as for providing important project information and for their help in finishing the research.

My gratitude and appreciation also extend to our colleagues and lecturers who assisted us in the development of the project, as well as to those who have volunteered their time and skills to assist us.

Võ Anh Kiệt – 20520605 – ANTN.2020

Nguyễn Bùi Kim Ngân – 20520648 – ANTN.2020

Nguyễn Bình Thục Trâm – 20520815 – ANTN.2020

Contents

[Acknowledgement 3](#_Toc136372206)

[Part 1: Introduction 5](#_Toc136372207)

[1.1. Overview Registry Spy 5](#_Toc136372208)

[1.2. Overview EDR 6](#_Toc136372209)

[1.3. Problem Statement 7](#_Toc136372210)

[1.4. Scope 9](#_Toc136372211)

[1.5. Objective 9](#_Toc136372212)

[Part 2: Background 10](#_Toc136372213)

[2.1. Registry spy 10](#_Toc136372214)

[2.2. EDR – OpenEDR 10](#_Toc136372215)

[Part 3: Requirement and Installation 12](#_Toc136372216)

[3.1. Requirement 12](#_Toc136372217)

[3.1.1. Registry Spy 12](#_Toc136372218)

[3.1.2. OpenEDR 12](#_Toc136372219)

[3.2. Installation 14](#_Toc136372220)

[3.2.1. Registry spy 14](#_Toc136372221)

[3.2.2. OpenEDR 14](#_Toc136372222)

[Part 4: Implementation 17](#_Toc136372223)

[4.1. Registry Spy 17](#_Toc136372224)

[4.2. OpenEDR 19](#_Toc136372225)

[Part 5: Conclusion and Future Work 25](#_Toc136372226)

[5.1. Conclusion 25](#_Toc136372227)

[5.2. Future work 26](#_Toc136372228)

[Reference 27](#_Toc136372229)

Part 1: Introduction

* 1. Overview Registry Spy

The management and organization of information have become crucial in today's digital environment, where enormous amounts of data are generated and saved. Utilizing registry technologies, which act as centralized repositories for storing and accessing critical information, is a key component of data management. These technologies are essential in a number of industries, including logistics, finance, and healthcare.

The Registry Tool Analysis is a comprehensive analysis of the features, advantages, and difficulties related to registry tools. An thorough review of these tools, their importance, and the effects they have on enterprises and organizations are all part of this in-depth report's goal.

The examination will delve into the fundamental ideas that underlie registry tools, illuminating how they support the effective management of data through hierarchical hierarchies and defined formats. Registry technologies provide unmatched simplicity and accessibility by collecting, organizing, and preserving crucial information in a single location, expediting crucial business operations.

The report will also examine the various industrial applications of registry tools. It will dig into the healthcare industry, where patient registries make it possible to gather and analyze data for epidemiological studies, medical research, and individualized patient care. Additionally, financial institutions use registry technologies extensively for customer relationship management, compliance monitoring, and fraud detection, offering an integrated method of managing client data.

Although registry technologies provide many advantages, the examination will also cover the difficulties that businesses encounter in setting up and maintaining them. This covers things like data security, privacy issues, scalability, and interoperability, which call for careful attention to guarantee registry systems perform at their best and maintain their integrity.

In the end, the goal of this Registry Tool Analysis is to provide businesses, decision-makers, and professionals with a thorough grasp of the function and potential of registry tools in contemporary data management. This paper will be an invaluable resource for anyone looking to harness the potential of registry technologies to improve their data management processes and boost operational efficiency by examining their capabilities, advantages, and limitations.

* 1. Overview EDR

The dynamic threat environment in the field of cybersecurity necessitates new strategies to safeguard digital assets. EDR, or endpoint detection and response, has become an essential part of the protection against sophisticated cyberthreats. Organizations can identify, look into, and react to dangerous actions at the endpoint level thanks to EDR technologies.

This piece tries to offer a comprehensive analysis of EDR, its features, and the importance it bears in protecting contemporary digital environments. The convergence of endpoint security, threat detection, and incident response will be the subject of this report, which will clarify the crucial part that EDR plays in reducing cyber risks.

The investigation will go into the underlying ideas of EDR, examining how it uses cutting-edge technologies like behavioral analytics, machine learning, and artificial intelligence to spot malware, flag suspicious activity, and react to security issues. EDR solutions give security teams real-time endpoint visibility, allowing them to proactively fight against sophisticated threats like fileless assaults, zero-day exploits, and advanced persistent threats (APTs).

The paper will also go through the primary attributes and functions of EDR solutions, such as continuous monitoring, forensic analysis, integration of threat intelligence, and automated reaction. EDR gives companies the ability to quickly recognize and neutralize threats, reducing the potential effect of cyber disasters. It does this by supplying granular visibility into endpoint actions and developing thorough defense systems.

The analysis will include the difficulties in installing and managing EDR solutions in addition to the advantages. This includes things like system complexity, resource needs, false positives, and making sure the system is compatible with the current security architecture. To make the most of their EDR initiatives, organizations must carefully assess these factors.

In the end, the purpose of this EDR research is to give decision-makers, security experts, and businesses a thorough knowledge of the value and potential of EDR in the face of changing cyberthreats. This research will be an invaluable resource for anyone looking to improve their cybersecurity posture and secure their digital assets through the deployment of effective EDR solutions by examining its functions, advantages, and problems.

* 1. Problem Statement

The potential of malware penetration is a huge concern in today's linked society, as digital gadgets are omnipresent and play a critical part in both our personal and professional life. Malicious software, also referred to as malware, is constantly evolving and adapting, coming up with new and creative ways to get past the security measures put in place by devices like computers, smartphones, tablets, and Internet of Things (IoT) devices.

The issue is that malware is becoming more sophisticated and diverse all the time. It may infect devices using a variety of attack routes, including phishing emails, compromised websites, software flaws, social engineering tricks, and illegal app downloads. Malware can cause chaos once it has gained access to a device by stealing confidential data, jeopardizing user privacy, engaging in unwanted actions, and even making the device unusable.

The effects of malware infestation are extensive and significant. Financial loss, identity theft, data breaches, system outages, and reputational harm are risks that both individuals and corporations must contend with. In addition, as technology develops and the Internet of Things connects more gadgets, there is an urgent need to be concerned about the possibility of broad malware outbreaks and their potential cascade repercussions.

Malware infiltration must be addressed using a multifaceted strategy that includes strong cybersecurity controls, user education, proactive threat detection, and efficient incident response. Individuals, businesses, and security experts must maintain vigilance, regularly upgrade their defenses, and use security technologies that can identify and counter new malware threats.

The issue also gets more complicated as the lines between personal and professional gadget usage blur. The difficulty of securing a wide variety of devices, including employee-owned devices (Bring Your Own Device, or BYOD), is one that businesses must address because it increases the risks and potential weaknesses of corporate networks.

In conclusion, the issue of malware gaining access to devices is a persistent and constantly changing difficulty in today's digital environment. In order to protect themselves from malware infection and its effects on devices, people, companies, and the security community as a whole must always be on watch, react to new threats, and put strong security measures in place.

Malware, malificious file,…

Users The endpoint device

* 1. Scope

Deploy the EDR

Deploy the Registry Spy

Analysis the endpoint device

Detect malware

* 1. Objective

Using the EDR sponsor by OpenEDR to analysis the machine and detect malware.

Using the Registry spy to detect the DAT file

Part 2: Background

* 1. Registry spy

Registry Spy is a free, open-source cross-platform Windows Registry viewer. It is a fast, modern, and versatile explorer for raw registry files.

Features include:

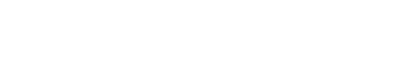
* Windows, macOS, and Linux support
* Fast, on-the-fly parsing means no upfront overhead
* Open multiple hives at a time
* Searching
* Hex viewer
* Modification timestamps

A green text on a black background

Description automatically generated with medium confidence

* 1. EDR – OpenEDR

Open EDR is a sophisticated, free, open-source endpoint detection and response solution. It provides analytic detection with Mitre ATT&CK visibility for event correlation and root cause analysis of adversarial threat activity and behaviors in real time. This world-class endpoint telemetry platform is available to all cyber-security professionals, and every sized organization, to defend against threat actors and cyber criminals.



Capability:

* Visibility and coverage: Open EDR solutions provide visibility into all activity and can cover both physical and virtualized environments.
* Detection: It provides an effective solution on detecting potential threats.
* Response: It reacts quickly and helps you contain and remediate incidents.
* Management and reporting: It is easy to manage and provide comprehensive reports that can help you improve your security posture.

There are many benefits of using Open EDR solutions, including:

* Improved Detection: It can help organizations to detect malicious activity that would otherwise go unnoticed. By collecting data from multiple sources and applying advanced analytics, Endpoint detection response software can provide visibility into suspicious activity and help security teams to immediately identify potential threats.
* Faster Investigation and Response: With all the data collected by an EDR solution in one place, security teams can quickly investigate incidents and take appropriate action to mitigate the threat. In addition, it often includes features such as automatic file quarantine that can help to contain an incident while it is being investigated.
* Damage from Attacks: By identifying attacks early and taking immediate action to block or contain them, EDR solutions can help organizations to reduce the damage caused by malicious actors. This can help organizations to minimize the impact of an attack and reduce the amount of time needed for recovery.
* Improved Compliance: It can also help organizations to meet compliance requirements, as many regulations require organizations to have effective security measures in place to protect data and systems. By deploying an EDR solution, organizations can demonstrate that they are taking appropriate steps to protect their systems from malicious activity.

Part 3: Requirement and Installation

3.1. Requirement

3.1.1. Registry Spy

Operation System

Table

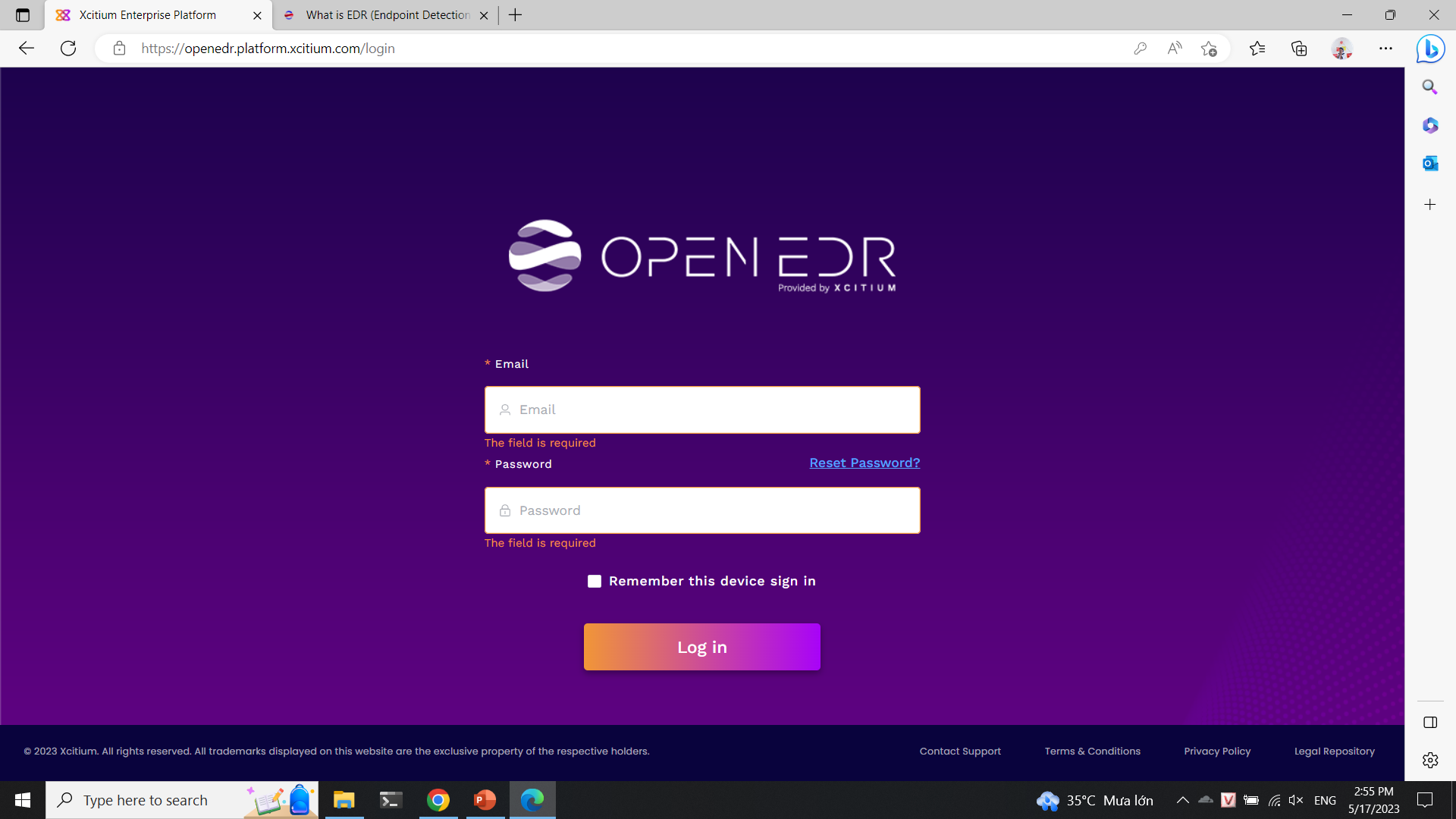
Description automatically generated

3.1.2. OpenEDR

This system require:

* The main system to get the annoucement from agent
* The machine installed agent

The main system:



The machine with agent:

A screenshot of a computer

Description automatically generated

3.2. Installation

3.2.1. Registry spy

The newest version 1.1.0:

Graphical user interface, text, application, email

Description automatically generated

There are 2 method to install it:

Install with pip:

Pip 🡪 pip install registryspy 🡪 registryspy

Install manually:

Clone the reposity/standalone 🡪 pip install –r requirements.txt 🡪 python setup.py install 🡪 registryspy

3.2.2. OpenEDR

Register and install the main system:

A screenshot of a computer

Description automatically generated

Install the agent to the machine:

A screenshot of a computer

Description automatically generated

Install the packages:

A screenshot of a computer

Description automatically generated

Part 4: Implementation

4.1. Registry Spy

Check the information of the machine:

Computer name:

A screenshot of a computer

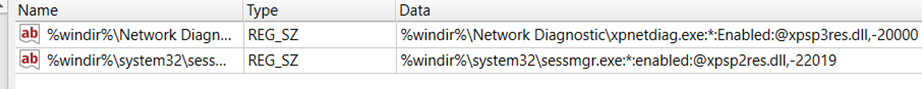
Description automatically generated

Firewall:

A screenshot of a computer

Description automatically generated with medium confidence

List application in Firewall list;



Operation System:

A screenshot of a computer

Description automatically generated with medium confidence

Enviroment:

A screenshot of a computer

Description automatically generated

Mount Device:

A screenshot of a computer

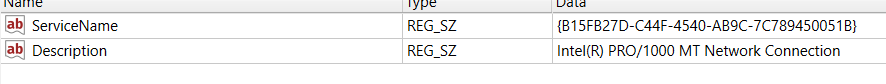
Description automatically generated

Time Zone:

A screenshot of a computer

Description automatically generated

Network card:



Memory management:

A screenshot of a computer

Description automatically generated

4.2. OpenEDR

Scan the information of the endpoint:

A screenshot of a computer

Description automatically generated

Scan the software of the endpoint:

A screenshot of a computer

Description automatically generated

Scan the patch of the endpoint:

A screenshot of a computer

Description automatically generated

Detect the process of the endpoint:

A screenshot of a computer

Description automatically generated

Process of detect and respone the malware of OpenEDR:

Detect the suspicious file 🡪 Quarantine 🡪 Detect 🡪 Delete 🡪 Find the same file again 🡪 Delete automaticly 🡪 Annoucement

A picture containing text, font, number, line

Description automatically generated

Quarantine file:

A screenshot of a computer

Description automatically generated with medium confidence

Quarantine room:

A screenshot of a computer

Description automatically generated

Detect malware:

A screenshot of a computer

Description automatically generated with medium confidence

Delete malware:

A screenshot of a computer

Description automatically generated with medium confidence

Delete malware automaticly (2nd times):

A screenshot of a computer

Description automatically generated with medium confidence

Top 10 OWASP:

A screenshot of a computer

Description automatically generated

**Pygoat - No announcement on OpenEDR:**

**A screenshot of a computer

Description automatically generated**

**Webgoat - No announcement on OpenEDR:**

A screenshot of a computer

Description automatically generated

**Weakness – detect and ban wrong process:**

A screenshot of a computer

Description automatically generated

Part 5: Conclusion and Future Work

5.1. Conclusion

In conclusion, the registry tool and Endpoint Detection and Response (EDR) play vital roles in enhancing the security and overall management of computer systems. The registry, as a core component of the operation system, acts as a centralized database that stores essential configuration settings and options. By utilizing the registry tool effectively, administrators and users can modify settings, troubleshoot issues, and optimize system performance.

EDR, on the other hand, provides advanced threat detection, prevention, and response capabilities to safeguard endpoints against malicious activities. It continuously monitors and analyzes system events, network traffic, and user behavior to identify and respond to potential threats promptly. EDR solutions offer real-time visibility into endpoint activities, enabling security teams to detect and mitigate sophisticated attacks, such as fileless malware, advanced persistent threats, and zero-day exploits.

When used in conjunction, the registry tool and EDR form a robust defense mechanism against cyber threats. The registry tool allows for fine-grained control over system settings, ensuring secure configurations that align with organizational security policies. EDR solutions provide additional layers of defense by actively monitoring the system, detecting anomalies, and responding swiftly to potential threats, minimizing the risk of data breaches, system compromise, and unauthorized access.

Moreover, the integration of the registry tool and EDR enhances incident response capabilities. In the event of a security incident, the registry tool can be leveraged to analyze system changes, track suspicious registry modifications, and restore critical settings. EDR solutions, with their comprehensive visibility and incident investigation capabilities, provide valuable insights into the attack vector, its impact, and potential lateral movement within the network. This information empowers security teams to conduct thorough forensic investigations, facilitate timely incident response, and implement appropriate remediation measures.

In conclusion, the effective utilization of the registry tool and EDR strengthens the security posture of computer systems by enabling secure configurations, proactive threat detection, and efficient incident response. As the threat landscape continues to evolve, organizations must embrace these tools, alongside other security measures, to safeguard their digital assets and maintain a resilient cybersecurity posture. By prioritizing the implementation and integration of the registry tool and EDR, organizations can enhance their ability to mitigate risks, detect and respond to threats, and protect sensitive information, ultimately safeguarding the integrity and availability of their systems.

5.2. Future work

In the future, there are several areas that can be explored and expanded upon regarding the registry tool and Endpoint Detection and Response (EDR) to further enhance their effectiveness and impact on computer system security. Here are some potential avenues for future work:

* Advanced Registry Analysis
* Registry Integrity Monitoring
* Enhanced Registry Remediation
* Integration with Threat Intelligence
* Registry Auditing and Compliance
* Cross-Platform Support

In conclusion, the future work of the project surrounding the registry tool and EDR presents exciting opportunities for further research and development. By focusing on advanced analysis techniques, integrity monitoring, automated remediation, threat intelligence integration, auditing, compliance, and cross-platform support, we can continue to enhance the security posture of computer systems, detect and respond to emerging threats effectively, and ensure the resilience and protection of critical assets in the face of evolving cyber risks.

Reference

OpenEDR: [What is EDR (Endpoint Detection & Response)? Open source EDR® (openedr.com)](https://www.openedr.com/)

Registry Spy: [GitHub - andyjsmith/Registry-Spy: Cross-platform registry browser for raw Windows registry files](https://github.com/andyjsmith/registry-spy)