Internet platform for analyzing computer memory of Windows operating systems for conducting information security investigations

Michael Tretyak, Larisa Cherckesova, Denis Korochentsev, Elena Revyakina, and Alexey Popov

1 DonState Technical University, 344002 Rostov-on-Don, Russia
2 Institute of Service and Entrepreneurship (branch) DSTU, 346500 Shakhty, Rostov region, Russia

Abstract. Within the framework of this article, an analysis of the dynamics of the growth of information security incidents identified in companies by specialists of the department of monitoring and responding to information security threats was carried out. The study examined the problems faced by information security specialists in companies, and what tools they use to perform their tasks. Countering cyberattacks requires timely response to a recorded incident and accuracy in its investigation. As part of this scientific work, an automated digital platform was developed for analyzing RAM dumps of Windows operating systems for conducting investigations in the field of information security. This tool will provide a digital forensics specialist with additional time to investigate information security incidents by minimizing routine tasks and a centralized information processing location.

1 Introduction

The rapid growth of informatization indicators at enterprises, and the introduction of new digital technologies in the spheres of life of modern society and public administration, testify to the increased importance and value of information as a strategically important resource of any state, a valuable commodity, as well as an information advantage, the possession and retention of which is becoming one of priority tasks in ensuring the national security of the country.

The claims of competing countries, rival companies, a large number of groups of different levels of training and individual citizens for this advantage become the cause of attacks of many degrees of complexity, the inability to resist which can result in negative consequences for the status and economy of the country. Today, the issue of protecting the information infrastructure of a business has a high priority and requires a rapid response from the Security Operation Center (SOC) specialists from different departments, who counter attacks by hacker groups around the clock. It is important for an information security expert to be able to interpret events logged by a computer system in order to detect potentially dangerous activity of an intruder during an investigation.
2 Materials and methods

2.1 Analysis of information security threats

The idea of the analysis of information security threats by forensics experts consists of data collected as a result of the conducted investigations of attacks, on the basis of which recommendations for investigations are created, new attack scenarios are created for which correlation rules, playbooks are created, as well as reports with detected indicators of compromise noticed during the attacks [5].

The main task of the SOC is to monitor and respond to information security incidents within the framework of the Service Level Agreement (SLA) agreed in advance with the company [6]. Incident monitoring and response is the basis of any SOC, they represent the so-called active protection. In addition, it is necessary to be able to build hypotheses and find opportunities to detect the criminal and prevent the attack, avoiding the moment when the situation becomes critical.

This approach is called proactive. The key roles of such threat protection are played by Threat Hunting and Threat Intelligence, which are one of the areas of work of the Solar Security research laboratory Solar JSOC CERT. As part of Threat Hunting and Threat Intelligence, specialists continuously study the potentially dangerous activity of intruders in the open information space, identify profiles of their behavior, and as a result of the research, a database is collected on the basis of which Solar JSOC services are improved, taking into account the discovery of new techniques and tactics for conducting attacks.

Attackers can hide their presence in a company's infrastructure for weeks or even months before they are discovered. They patiently wait for the right moment to download enough confidential company information or credentials to gain enhanced access, setting the stage for a major attack.

According to the "How much does a data breach cost in 2022" report, a data breach costs a company an average of approximately $4 million [7] and the disruptive effects of disruption to a company can linger for years, and in the US, the average cost was $9.44 million, the highest of any nation. The less timely work is done to eliminate system malfunctions, the more it can cost the organization [8]. At the same time, in the Russian financial sector, cases of bringing to justice employees who provoked the leakage of confidential information continue to be recorded. 36% of survey participants estimated the potential cost savings from prevented leaks at more than RUB 10 million over the past year. At the same time, in 2 cases, the real damage from the incidents that occurred amounted to more than 100 million rubles. In light of this, the response measures taken by the management of financial institutions look more than adequate [9].

The investigation of a new attack and the collection of data about it, which will be transferred to specialists in monitoring and responding to information security incidents, are carried out by specialists in expert areas such as:

- Reverse engineering
- Forensics

---

2 Materials and methods

2.1 Analysis of information security threats
Analysts

Reverse engineers study by bytes how the malicious code works; Analysts analyze the received data, put forward new hypotheses, check whether the Security information and Event Management (SIEM) system has a rule for detecting a detected threat; if not, create and add new rules[10], while forensics specialists investigate information security incidents, studying the chronology of the attack and events, and if a new malware is discovered, they pass it on to reverse engineering specialists for investigation [11].

The term forensics is revealed as an applied science of solving crimes related to computer information, the study of digital evidence, methods of searching, obtaining and fixing such evidence [12].

As part of the investigations, digital forensics experts need to use tools that allow them to implement a comprehensive analysis to identify certain threats to information security. At the same time, to master each tool, you have to allocate not only the effort and time to achieve the appropriate level of proficiency in them, but also to deploy them on virtual hosts [13].

When analyzing RAM dumps of compromised systems, information security experts form hypotheses, the refutation or confirmation of which is achievable through a complete analysis of the chains of events recorded in RAM [14], defining goals and identifying attacker tactics and strategies [15].

It is important for a monitoring expert to understand what events are written to the event log by the system during attacks; reading and correctly interpreting these events leads us to the root cause of the attack. This allows you to minimize the risks of its recurrence, which is important, as well as to understand the causes and eliminate the consequences[16].

The main tools that help specialists in the investigation are, of course, system logs. These can be system logs, security logs, application logs, kernel logs, and many others. In addition, different devices have their own standards for logging certain events, for example, Windows security logs, event logs for Unix-like operating systems and Kaspersky are very different from each other [17]. In order to interpret raw events, it takes a lot of time, in addition, the number of events that occur can tend to a point at which the study of one activity can take a long time [18].

Information security professionals use data from Managed Detection and Response (MDR), SIEM, and information security threat intelligence tools as the basis for their search [19]. Other tools, such as packer parsers, are also often used to search for information on the Internet [20]. It should be noted that the use of SIEM and MDR tools requires the integration of the main event sources and tools in the environment [21]. After the events are captured on the final source hosts, they are normalized and centrally collected by the SmartConnector on the connector server. In the process of normalization, events acquire a clear and readable form, in other words, they are brought to a certain standard [22]. On connectors, events go through an aggregation process, as a result of which many duplicated events are replaced by one. Figure 1 shows an example of aggregating several similar events into one.

The next step after aggregation is to pass events through enrichment rules. Enrichment rules are applied to events to supplement the "enrichment" of information that is already present in the event [23]. At the same time, the data that supplements the information can be taken from other events, or their tabular lists stored in the SIEM system.
In addition, enrichment rules can complement the lists used in the investigation, for example, if we need to add a user account to the stop list, when authentication on the host is unsuccessful.

The next important step in event processing is correlation, events. In the case of correlation and enrichment, the rules can be triggered several times, after which an incident event occurs, which is sent to the SIEM operator for investigation.

After the generation of the incident, the monitoring engineer began to investigate the activity, he describes in detail all the potentially dangerous activity, after the described activity gets to the customer, who determines whether this activity is dangerous cause by an attacker, or illegitimate actions of the employees of the customer's Company [24]. If an attack is detected and a more detailed and in-depth study of the system that has been compromised is carried out, the investigation of the incident continues by experts from the Forensic Department.

To analyze RAM dumps of various operating systems, experts often use utilities similar in their functionality to the Volatility Framework, but often the functionality of many of them is already provided in this framework, which allows you to analyze the activity of a system fixed in RAM at the time of its snapshot creation:

- Autopsy Forensic Browser is a graphical interface for the digital exploration tools in the Sleuth suite. Together they allow you to explore the computer's file system and volumes [25]
- CAINE is a GNU/Linux distribution created as a project by Digital Forensics. CAINE offers a feature-rich environment that is designed to integrate existing software tools into software modules and provide a user-friendly graphical interface. The main design objectives are an interoperable environment that supports the digital investigator during the four phases of the investigation, a user-friendly graphical interface, semi-automated compilation of the final report.
- The Rekall Framework is a fully open source set of tools implemented in Python under the Apache license and the GNU General Public License for extracting and analyzing computer systems of digital artifacts [26]

Based on the information collected, response rules are formed for more complex attack scenarios, such as Threat Hunting and Threat Intelligence, the investigation of which requires a certain level of competence and skills from a specialist.

2.2 Related works

Fig. 1. Aggregation of events coming to SIEM

![Aggregation](image)

IP address source: 65.65.55.65
Source Port: 1355
Ip address destination: 20.30.30.30
Destination Port: 80
Number of events: 10
for analyzing RAM dumps of operating systems of the Windows family during information security investigations by digital forensics specialists. This tool allows forensic experts to rationally spend the time allocated for investigating information security incidents, minimizing routine tasks and processing computer memory snapshots in a centralized place for information processing[27].

Since investigations involve the analysis of unique activity, full automation of this process at the current stage is a time-consuming task, since in the presence of routine tasks, the level of occurrence of anomalous events remains high, for the understanding of which human participation is extremely necessary. The best solution to this problem is the partial automation of human investigation processes.

To achieve the goal and fulfill the requirements set as part of the analysis, the architecture of the digital platform should consist of the following components:

1) An automated dump analysis service capable of performing a basic scan of the dump when requested in the normal mode and generating a report with the information received, as well as uploading the received information in a user-readable form to the server and back to the client upon request.

2) The main services of the platform provide for the interaction of the components with each other, as well as the interaction of the system with services that have an open Application Programming Interface (API), which allows integrating third-party services, providing mechanisms for using the developed tool as a cloud service for analysis.

3) The user interface of the platform, which provides access to tools for analyzing the RAM dump, receiving information through the API interface.

To implement the implementation of this task, as well as taking into account the architectural principles of building a service, it is required to use software tools that have high performance indicators [28], and also demonstrate themselves well when working with a large amount of data, which can later prove to be good in scalability and stability.

Also, for the correct operation of the service, it is necessary to place the target server in the Demilitarized Zone (DMZ) of the company's infrastructure and restrict access to it by irrelevant data, namely the user account and the IP address added to the white list [29].

Figure 2 shows the layout of the web service in the DMZ network.

As the main tool for analyzing snapshots of computer memory, the Volatility Framework is used, which is an open source non-commercial project, which is a package of expertise consisting of various analysis modules [30]. This plugin is the most popular solution among digital forensic experts due to the volume of useful plugins, cross-platform, detailed documentation.

The expertise package starts scanning immediately after the dump of the computer's RAM is uploaded to the platform server.

Fig. 2. Placement of the service in the architecture of the company's network
3 Results and discussion

3.1 Development of a RAM dump analysis service

In order to fulfill the tasks set during the implementation of the service, a list of technologies used in the development of a digital platform for analyzing RAM dumps was determined, a brief description of the currently defined technologies and its main advantages are presented below.

The main programming language is C# [31], which is an object-oriented programming language that has adopted much from Java and C++. The C# language supports polymorphism, inheritance, operator overloading, static typing. .NET was used as the main framework [32]. The development of the user interface was carried out using the programming methods provided by the React framework.

To carry out the implementation of the task, as well as considering the architectural principles of building a service, it is required to use software tools that have high performance indicators, and also demonstrate themselves well when working with a large amount of data, which can later prove to be good in scalability and stability. Figure 3 shows a logical diagram of the interaction between the components of the service being developed.

Fig. 3. Logical model of platform components interaction

Note that the services implemented in the architecture are located in Docker containers isolated from each other, the interaction between which is carried out by Rabbit MQ mechanisms. This solution ensures the independence of the configured tools inside the containers and from each other, and thus avoids the conflict of dependencies used by the tools.

Also, to set up the processes of supplying correctly configured software to the server, it was decided to use continuous integration and continuous delivery of Continuous Integration Continuous Deployment (CI/CD) [33].

3.2 Implementation

The owner of the compromised system sends the dump to the service's user interface for processing. After a successful upload to the server via the protocol, the dump is sent for scanning. In the meantime, the information security specialist who will be investigating...
begins to download the dump from the digital platform's storage to his local computer. At the same time, the analysis service returns a ready-made report to the user and the digital forensics expert with the results of performing routine tasks.

This solution will allow the information security specialist to rationally use the time allocated for the investigation by 11% of the investigation time without the use of automation tools by the specialist.

After reviewing the report, the information security specialist begins the main investigation, considering the information obtained from the report. Figure 4 shows the user interface designed to work with the service.

Fig. 4. Main page of the computer version of the web service

Figure 5 shows the main page of the mobile version of the web service.

Fig. 5. Main page of the mobile version of the web service

Figure 6 shows a fragment from the report containing information about a Trojan disguised as a software component of the vendor VMware Inc.
Fig. 6. Disguised Trojan disguised as a legitimate file

The user can refresh the page when uploading a file through the web interface without fear that the progress of loading a snapshot of RAM will be reset.

The download speed of the dump depends on the average load on the network and the speed of the data transmitted in it. Big data delivery assurance is provided by the TUS protocol as an add-on over HTTP.

The service was tested by analyzing a 4 GB RAM dump belonging to the Windows operating system. The dump was analyzed with manual testing and using a digital platform. The test results are presented in Table 1.

Table 1. Comparison of testing time by manual and automated method

<table>
<thead>
<tr>
<th>Method</th>
<th>Average execution time of the standard algorithm, seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human</td>
<td>570</td>
</tr>
<tr>
<td>Digital platform</td>
<td>508</td>
</tr>
</tbody>
</table>

According to the test results, it can be concluded that the use of the developed digital platform will reduce the time for analyzing RAM dumps.

4 Discussion

When choosing the sets of plug-ins used during testing, the greatest performance increase for a snapshot of computer memory was recorded without using methods for analyzing computer network activity.

5 Conclusion

The main result obtained as a result of the study is the developed digital platform for analyzing RAM dumps of operating systems of the Windows family, which allows you to partially automate the study of the dump and compile a detailed report containing the collected information. This solution allowed information experts to rationally spend the time allocated for analysis, minimizing routine tasks. The operability of the service was checked on a previously taken snapshot of the RAM of a computer running the Windows operating system. This test confirmed the effectiveness of the developed platform.
References


13. J. Turnbull, Containerization is the new virtualization Kindle Edition (July 12, 2014)


