

Digital Forensics Investigation

Investigation of a Cyber Attack on OSion Corporation

Darsh | January 26 2024

# Overview:

The results of a digital forensics study that was carried out to examine a cyberattack that was directed against OSION Corporation's network infrastructure are presented in this report. The investigation attempted to determine the attack's origin, the perpetrators' tactics, and the degree of damage done. The investigation carefully examined disk images, memory dumps, network traffic captures, log files, and other data to recreate the sequence of events that preceded and occurred during the attack. The study offers thorough insights into the attack routes, the attackers' behavior, and suggestions for reducing such risks in the future.



Table of Contents:

1. Introduction
2. Scope of Investigation
3. Methodology
4. Findings

* Initial Assessment
* Evidence Collection
* Analysis
* Timeline Reconstruction
* Attribution
* Damage Assessment

1. Recommendations
2. Conclusion
3. References

# Introduction:

The beginning of this digital forensics’ inquiry was caused by a cyber assault that OSION Corporation encountered on 2/22/2021. This study aims to identify the offenders, understand their tactics, methods, and procedures (TTPs), and offer suggestions for improving the security posture of OSION Corporation.

# Scope of Investigation:

The investigation's main goal was to examine OSION Corporation's network infrastructure, which included workstations, servers, and network devices among other things. The time frame when the cyberattack took place, from 2/22/2021 7:22:38 PM to 2/22/2021 7:35:38 PM, was included in the scope.

# Methodology:

The inquiry was conducted in a methodical manner, which includes:

* Initial investigation to compile data on the assault.
* Gathering of evidence from several sources, including memory dumps, disk pictures, network traffic captures, and log files.
* Analysis of gathered data utilizing methods and instruments from digital forensics.
* Reconstruction of a timeline to arrange the attack's events in order of occurrence.
* The goal of attribution is to pinpoint the threat actors in charge of the assault.
* Damage assessment to determine how the incident affected the data and systems of OSION Corporation.

# Findings:

Initial Assessment:

* On 2/22/2021, OSION Corporation came under ransomware assault.  
  Workstations and servers were among the systems that were impacted by the assault.
* Users complained that the ransomware was preventing them from accessing their encrypted data.

Evidence Collection:

* The servers and network devices of OSION Corporation's log files were gathered, offering insights into the attack pathways and initial breach.   
  Suspicious interactions with recognized command and control (C2) servers were discovered through network traffic captures.
* For offline investigation, disk images and memory dumps were taken from the impacted computers.

Analysis:

* A phishing email with a malicious attachment is most likely how the ransomware was distributed, according to an analysis of log files and network activity.  
  The existence of ransomware executables and accompanying artifacts was found through examination of disk images and memory dumps, confirming the infestation.

Timeline Reconstruction:

* The reconstruction of the timeline showed that the first breach happened when a user clicked on a malicious attachment in a phishing email.
* The malware encrypted files on linked systems as it moved horizontally throughout the network.

Attribution:

* Although it is difficult to pinpoint a single threat actor for the assault, the TTPs that were detected are consistent with well-known ransomware operations that target businesses to make money.

Damage Assessment:

* The OSION Corporation's activities were severely disrupted by the ransomware assault since users were unable to access vital data and systems.
* Downtime and possible data loss resulted in financial losses.

# Recommendations:

The investigation's conclusions led to the suggestions that follow, which are meant to improve OSION Corporation's security position:

* To stop unwanted access, use multi-factor authentication (MFA).
* Boost the capacity of network monitoring to identify and address unusual activity.
* Provide staff with frequent security awareness training to help reduce the impact of social engineering assaults.
* To guarantee a prompt and efficient reaction to security issues in the future, update your incident response protocols.

# Conclusion:

The cyberattack on OSION Corporation was better understood thanks to the digital forensics’ investigation. OSION Corporation may take proactive steps to fortify its security defenses and reduce potential threats by comprehending the attack pathways, locating the attackers, and evaluating the damage.

# References:

Magnet Forensics. (2019, March 19). *Magnet AXIOM Examine Overview - Magnet Forensics*. <https://www.magnetforensics.com/resources/magnet-axiom-examine-overview/>