CASE STUDY

INCIDENT FORENSICS FOR A SOFTWARE DEVELOPMENT COMPANY

Client Background

Our client helps companies ranging from startups to the Fortune 100 improve quality, timeliness, and predictability of their software throughout the entire development cycle. The company offers software services to facilitate development work at all stages of the process as well as improve their customers` overall processes, increase quality, reduce time to delivery, and provide higher levels of predictability and stability.

Business Challenge

Our client experienced three security attacks within a short period of time. Taking into account the severity of the risks and their possible consequences, after the third attack, drastic measures needed to be put into place. The company decided to conduct an independent 3rd-party incident investigation and discover how far the hackers got into the network and what sensitive data they might have accessed.

softserve

Project Description

In order to conduct a proper Incident investigation, SoftServe worked closely with the client's team. The investigation was carried out according to the internationally recognized guides and methodologies:

- NIST SP 800-86 "Guide to Integrating Forensic Techniques into Incident Response"
- NIST SP800-61rev2 Computer Security Incident Handling Guide
- CERT® Coordination Center Steps for Recovering from a UNIX or Windows System Compromise.

The project was executed by a certified SoftServe Security Consultant and was completed within 2 weeks. All of the evidence including logs, command history, attacker malware, and memory state were carefully collected, structured and analyzed. All suspicious records were marked and attached to the report. An incident roadmap was created and recommendations for immediate actions were provided. The project was executed in four phases:

1. **Preparation phase:**

- Interviewing stakeholders

2. **Evidence collecting phase:**

- Logs
- Network data
- Processes information and memory dumping
- Configuration file dumping

3. **Analysis phase:**

- Emails between stakeholders
- Logs
- Memory and processes
- Configuration files
- File modification, access, and creation time
- Sources of data leakage
- Malicious activity sources
- User data
- System checks for rootkits
- Chain of events
- Vulnerability scanning of the target system

4. **Analysis phase:**

- Documenting the complete results of the investigation
- Creating and presenting final report

Value Delivered

As a result of the Incident forensics process, our client received comprehensive information on the vulnerabilities in their system that allowed unauthorized access that could be exploited by a malefactor. The project calculated the business impact and provided a course of action to prevent future attacks. It also protected our client`s assets through proper information security management implementation. Additional benefits provided the client with:

- Detailed information on the malefactor's activities on the compromised server
- Sensitive information that may have been extracted by the malefactor or automated malware
- Analysis of employees` and applications' behavior to identify the cause of the data loss
- A new focus on security-awareness.

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience are built on a foundation of empathetic, human-focused design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy—No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

USA HQ

201 W 5th Street, Suite 1550
Austin, TX 75703
+1 866 687 3588

EUROPEAN HQ

One Canada Square
Canary Wharf
London E14 5AB
+44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com

softserve