CASE STUDY

Briskinfosec Did Digital forensic service for **A Major Technological company in The Europe Region**

INDUSTRY	STANDARDS	PRIMARY SECTOR
Software Sector	NIST	Software

LOCATION	OFFERED SERVICE
EUROPE	Digital Forensic Service

TYPE OF SERVICES: **Digital Forensics Service**
for a Leading Software Firm

ABOUT CUSTOMER

Our Stakeholder is a global leader in information technology, cloud communications software, and services for managing business-to-business customer interactions at scale. This company provides software and services that enable businesses and organizations to stay in constant contact with their customers via enhanced interactive channels such as social, messaging, and voice. After the acquisition is completed, will be able to provide customer-facing businesses with an end-to-end customer interaction management solution and rich customer experiences, as well as the ability to drive faster and smarter interactions and collaboration throughout the customer's lifecycle journey.

ASSESSMENT SCOPE

Under the investigation, Our Stakeholder wanted us to conduct a Digital Forensics service to find out what is the inbound and outbound data in the respective systems. During the assessment, we got the systems but not connected to internet / Active directory so we conducted Dead laptop forensic investigation to fulfil the scope.

THE SOLUTION

Briskinfosec followed NIST standards (National Institute of Standards and Technology) Digital Forensic methodologies to identify all evidences in the system.

Key highlights of the Evidence Findings are as follows:

- We could able to get all the Browser History, Passwords and Top sites searched from the system's start date.
- We found a suspicious application running in the background which is not displayed in the antivirus program.
- We found a Ransomware application in the system
- In the system, we discovered malicious crypto generator code.
- We were able to get all Third-party applications installed and uninstalled, as well as their activity.
- we were able to see the devices connected to the systems. (Both wired and wireless devices)

DIGITAL FORENSICS ASSESSMENT REPORT

Complete Digital Forensic Assessment was carried out. All the Investigation findings and the proof of concept (POC) will be covered with detailed steps in a PDF format.

DATABACK UP

Every possible finding will be submitted for the stakeholder's reference and for the legal proceedings.

CHALLENGES

During a Digital Forensics assessment, there were certain complications that were faced by our Forensics team.Those challenges are elucidated below:

- While this investigation was conducted from the Blackbox perspective, a large amount of data was discovered during the Data Recovery, and we sent a large number of findings as a result.
- Since every system had a large number of users, a large amount of browser history data was collected.

THE DELIVERABLE

The reports and the data backup provided for stakeholder's reference and legal proceedings. The following reports were submitted to the customer.

Key highlights of the bug fix are cited below:

DAILY STATUS REPORT

This Digital Forensic assessment consumed around 1-2 weeks of time. During the investigation were identified and we shared all Findings with corresponding recommendation Fix. Our prospect looked at the given valid report and started working from Day 1 as they need not work laboriously on the last day when the entire report is given by the security team thus making their final assessment report easier for preparation.

CONCLUSION

We advised our Stakeholder on the measures they should take for rectifying the various vulnerabilities in their systems.
For remediation, we educated them about the mandatory processes such as:

- Implementing a strong DLP and AD for stronger security.
- Recommending regular monitoring of the systems.
- Disabling the USB and wireless device connectivity to ensure the integrity of the data is unchanged in the systems.
- Removing cloud-based data sharing applications such as (OneDrive).

We also worked closely with our Stakeholder for improving policies, procedures and employee awareness programs for increasing security maturity.

BRISKINFOSEC
TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com