IstroSec

Data Sheet

Digital Forensics

Digital forensic analysis is systematical investigation of device, system, network communication or memory image. In the context of solving cybersecurity incidents its purpose is to answer questions depending on type of analysis.

Digital forensic analysis consists of multiple phases:

- Obtaining digital evidence
- Analysis of digital evidence
- Creating report/briefing or expert's report for judicial proceedings

When capturing digital evidence, it is important to ensure:

- Precision - acquired evidence is identical with data from original media
- Integrity - acquired evidence must not be changed in time (their change must be discoverable)
- Authenticity - acquired evidence come from analyzed device/system/source in set time period
- Confidentiality and accessibility

IstroSec Methodology:

In **Istro**Sec, we have our own methodology that ensures that all the points above are met when acquiring digital evidence from workstations, servers, external media, mobile phones, cloud and network or security technologies.

During acquisition our specialists use up-to-date best practices, recognized in US, EU and Slovak court of law.

Why IstroSec?

Combined experience of more than 70 years

Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Certified experts to ensure compliance with security standards and legislation - IstroSec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)

Types of Digital Forensics:

- Forensic Triage
- Standard Digital Forensics
- Special Digital Forensics

European Cybersecurity Company.
Threat Intelligence. Incident Response. Cyber Advisory.

www.istrosec.com

Forensic triage

Description

During forensic triage, we focus on identifying the basic indicators of compromise, usually using automated tools. Forensic triage is especially important in cases where multiple devices are potentially compromised and in the scope of incident response. In this case, it is important to determine which of the devices are compromised, which device was infected first, or which was used by the attackers to compromise other systems.

Prerequisites:

- Provision of a drive or forensic image of a drive from the device under investigation or acquisition of digital evidence
- Provision of local system logs (Windows event logs), webserver access logs
- Provision of logs from the central logging system in case the logs are centralized in the log management solution

The service includes:

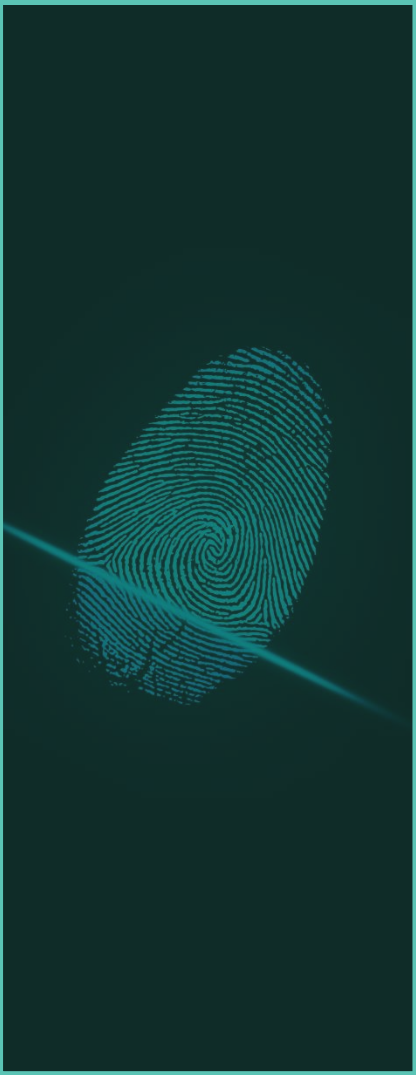
- Scan of provided devices and data for known malware
- Scanning for relevant indicators of compromise (IoCs) when a specific attacker or hacking group is suspected using knowledge of its tactics, techniques, and procedures (TTPs)
- Searching for indicators of persistence (approx. more then 100 different sources of persistence)
- Searching for evidence indicating program execution
- Searching for evidence indicating opening or viewing files and folders
- Searching for evidence indicating lateral movement (movement between devices)
- Searching for evidence of encryption
- Automated and partially manual log analysis

Deliverable:

- Summary of results from the analysis with actionable information to aid security incident response in the containment, eradication, and recovery phase.

Forensic triage typically answers questions like:

- Is the device being analyzed compromised?
- Does the system contain any IOCs with relation to case being investigated?
- Which systems were attacked from the analyzed system?
- Which devices accessed the analyzed system?
- Which accounts were compromised?
- What method did the attacker use to access C2 (Command and control)?
- Which persistence mechanisms were used?
- Were there attempts to get rid of evidence?
- Are the security mechanisms on system uncompromised?
- Does the system contain malware?



Case Study 1

Company type: Private healthcare provider

Service provided: Digital forensics

Solution: Forensic triage

A security incident is taking place in the organization and the REvil ransomware is spreading in it. The **Istro**Sec forensic team was delivered a forensic image of the workstation attacked by the ransomware.

The task of the team is to perform a forensic triage and obtain indicators of compromise, verify the existence of persistence and identify the way in which the ransomware is spread.

The **Istro**Sec forensic team performed a forensic triage and identified:

- Malware sample with MD5 544900a52XXXXf2e4fe7598985bc688f is located in the C:\Users\Public\ directory with a random name.
- Ransomware is run through a scheduled task in the C:\Windows\System32\Tasks directory named WindowsUpdate.job
- The ransomware is distributed from the domain controller MAINDC01.organization.local through a domain policy called "ServerHardening"
- The account organization.local\BackupAdmin is used to run the task
- There is also TrickBot malware on the workstation in the C:\Windows\SysWow64\ directory named wmicmain.exe
- Malware persistence is secured through the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run registry key named WindowsTelemetry.

The information obtained from the forensic triage was used to prevent the spread of malicious code by disconnecting the domain controller MAINDC01.organizacia.local from the network. The incident team wrote an extension for EDR used in the organization that removed the infection from the organization.

Standard digital forensics

Description

In standard forensic analysis, one or more potentially compromised systems are examined. We analyze forensic artifacts that remain on the system after you install or run programs, Windows registers, or event logs. We find out how users interacted with the system, when they logged in and out, what programs they used and when, what files they accessed, and so on.

Standard forensic analysis covers a wide range of cases, such as investigating incidents involving malicious code or ransomware, as well as investigating data breaches up to complete compromises of systems and identification of suspicious transactions.

Prerequisites:

- Provide a drive or forensic image of the device under investigation or acquisition of digital evidence by IstroSec experts
- Provide additional data, such as backups of local system logs containing data beyond the data already present on the drive/forensic image, webserver access logs, and more
- Device RAM image

The service includes:

- System data collection
- Search for clues indicating the persistence of the attacker
- Automated scan of provided evidence for the presence of known threats (AV, Loki)
- Search for evidence indicating program execution
- Search for evidence indicating that files and folders have been opened or viewed
- Search for evidence indicating lateral movement (movement between devices)
- Search for evidence of encryption
- Comprehensive log analysis
- Timeline analysis
- Analysis of user activity, history of Internet activity
- Automated and manual analysis of Microsoft Event Logs and other logs located on the device
- RAM analysis

Deliverables:

- Report with detailed analysis results for each provided digital evidence (drive, forensic image, log export, etc.)
- Executive summary of the analysis outputs in a separate document
- Timeline of the attack and the most significant events during the incident
- If necessary, it is also possible to prepare an expert witness opinion in the following sectors:
    - Criminalistic informatics
    - Security and protection of information systems

Standard digital forensics typically answer questions like:

- Which device was infected first? (Patient 0)
- How did the attacker breach the first device? (Patient 0)
- What activity did the attacker perform on the device?
- What vulnerability did the attacker use to compromise the original device?
- What files did the attacker open or view?
- Did the user click on the spearphishing email?
- Was the data exfiltered?
- Did the attacker access any specific database?
- Did the attacker modify the documents on the device?
- Did the attacker modify the database?

Case Study 2

Company type: Private healthcare provider

Service provided: Digital forensics

Solution: Standard digital forensics

A security incident is taking place in the organization. REvil ransomware is spreading in the organization. The **Istro**Sec forensic team received a forensic image of a workstation compromised by a ransomware. The team's task is to perform forensic analysis and identify the attack vector and identify the device that was attacked first. The forensic team performed a forensic analysis of the submitted image and identified that the ransomware had been distributed from the MAINDC01.organization.local domain controller as a scheduled task through a domain policy called "ServerHardening". Apart from REvil, malicious code TrickBot has been also distributed. No other attacker access has been identified on the device. Malware analysis showed that the TrickBot malware on this device did not receive any commands from the control server.

After obtaining the forensic image of the memory and drives of the domain controller MAINDC01.organization.local, a forensic analysis was performed on this device and it was identified that:

- The attacker was present on the device 6 months before the ransomware has been launched in the organization
- The attacker accessed the domain controller from the IP address 10.10.15.29
- The attacker accessed the file server File01.organization.local and the database server Database05.organization.local from the domain device, downloaded the file x.zip and sent it via the WinSCP tool to the address of the control server attacker.example

Based on the above findings, digital evidence was acquired from the workstation 10.10.15.29 and the servers File01.organization.local and Database05.organizacia.local. A standard forensic analysis is to be performed for 10.10.15.29. For the devices File01.organization.local and Database05.organization.local, it was recommended to perform a complete analysis of data exfiltration from the above mentioned servers to identify leaked documents - see below.

A forensic analysis of the device on 10.10.15.29 was performed and it was identified that:

- The device on 10.10.15.29 is the Patient 0 of the infection.
- On January 10, 2021, the user john.smith clicked on the spearphishing email from anna.bell@partnerOrganisati0n.com with the subject “Measures during the Covid19 pandemic in the PartnerOrganization building”. The email contained an infected attachment that, when opened, executed malicious TrickBot code with the attacker.example control server.
- The attacker gained local administrator privileges through the obfuscated Mimikatz tool.
- The attacker obtained a domain administrator's NTLM hash from memory using Mimikatz.

A comprehensive report was prepared from the digital forensics which included:

- Executive summary
- Timeline of the incident
- Attacker’s activity in the victim’s infrastructure
- Vulnerabilities identified in the infrastructure during the digital forensics analysis
- Recommendations for improving the security of the infrastructure.

Special digital forensics

Description:

In-depth investigation of the incident requires additional analytical steps beyond the basic forensic analysis. These are, for example, cases related to data exfiltration, cases of advanced targeted attacks, cases of insider threat attacks and the like.

Prerequisites:

- The same as for standard digital forensics
- Any other kind of digital evidence, depending on the type of incident

The service includes:

- The same as for standard digital forensics
- Specific steps needed for a specific case - heavily dependent on the circumstances of the case and on the client's requirements. It can be, for example:
  - Detailed analysis of user behavior; what resources were accessed and when, whether anonymization or encryption tools were used, and the like
  - Email analysis
  - File system analysis, reconstruction of deleted files where possible
  - Database access analysis
  - Exfiltration analysis

Deliverables:

- Report with detailed results from the analysis for each provided digital evidence (drive, forensic image, export of logs, etc.)
- Executive summary of analysis outputs in a separate document
- Timeline of the attack and the most significant events during the incident
- Answers to the questions set for the analysis, for example:
  - Determine if any data was exfiltrated and if so, which documents leaked
  - Determine if and what data was deleted from the system, which user account or which tool was used to delete it
- If necessary, it is also possible to prepare an expert witness opinion in the following sectors:
  - Criminalistic informatics
  - Security and protection of information systems

If needed, these types of digital forensics can be extended by:

- **Network forensics** – analysis of captured network communication (full packet capture) or netflow analysis.
- **Log analysis** - analysis of network and security devices logs, analysis of central log management solutions or analysis using SIEM solutions.
- **Memory forensics** - analysis of RAM captured from a device.

Why Us?

Experience and knowledge

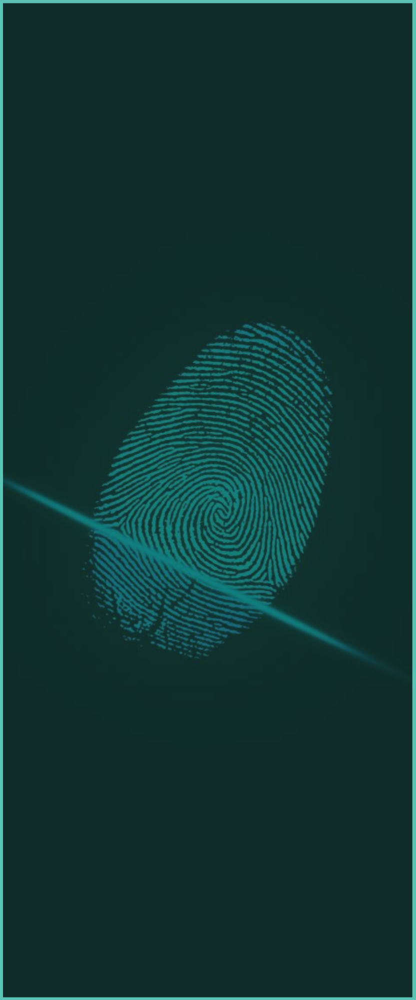
IstroSec specialists have experience in digital forensics analysis, according to internationally accepted frameworks. They know the tactics, techniques, and procedures of attackers and have the knowledge necessary to enable you to make decisions during incident response based on an analysis of the attackers' activities during in the attack.

Expertise in DFIR

Expertise in digital forensics and incident response and many other areas of information security, such as information security management, audit, or world-class malware analysis, which they have repeatedly demonstrated while dealing with state-sponsored cyber-attacks, attacks on Fortune 500 organizations, as well as the participation of four **Istro**Sec experts in the winning team of Locked Shields 2016 exercise.

Certified professionals

IstroSec experts are also holders of internationally recognized certificates in these areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and more.



Case Study 3

Company type: Private healthcare provider

Service provided: Digital forensics

Solution: Special digital forensics

We will follow up on the above-described case of the incident of REvil ransomware infection.

Based on the results of the forensic analysis of the compromised devices, the customer requested to perform a special forensic analysis. A complete data exfiltration analysis was performed for the File01.organization.local and Database05. organization.local devices to identify documents leaked from these servers. As part of the forensic analysis, an analysis of the files created, modified, or copied by the attacker was performed. At the same time, it was identified that the attacker also accessed local databases through the integrated SQL Server Management Studio. The analysis identified data within that database that was changed by the attacker.

A comprehensive report was prepared from the digital forensics which included:

- Executive summary
- Report with detailed results from the analysis for each provided digital evidence (drive, forensic image, exported logs, etc.)
- A list of most probably exfiltrated documents from the servers