Forensic Examination of Digital Storage Media

When Security Tools Are Unavailable



Yuri Alekseevich Pavensky
Independent Expert

Security tools are deployed, but normal access is restricted

SECURITY ENVIRONMENT

Security tools deployed

SIEM, EDR, DLP, WAF, NGFW, SOAR and other solutions

Penetration tests and practical exercises

Improving incident response processes

Regular audits

DATA NETWORK

No connectivity

The corporate network is not functioning properly

ACCESS TO SECURITY TOOLS

Restricted

Normal access through the corporate network is unavailable. Access to individual security tools may still be possible

DIGITAL EVIDENCE

Remains on local systems

And continues to change every second

Having security tools does not guarantee that their data will be accessible during an incident

A leaked password exposed personal accounts

01 / SOURCE

Online store database

Customer personal data became publicly available, including email addresses and passwords for customer accounts

02 / USER

Employee of an IdM software developer

A personal email address was used to register with the online store

03 / PASSWORD

Password reuse

The same password was used for several of the employee's personal accounts

04 / ACCESS

Personal accounts compromised

Personal mailbox

Public cloud storage

At this stage, only the employee's personal accounts and resources had been compromised

Email correspondence revealed information about customers

01 / OSINT

Employee profile

Additional personal mailboxes

Corporate email address

Contact details

Organization and job title

02 / PERSONAL RESOURCES

Personal mailbox and cloud storage

Work correspondence was discovered

03 / CUSTOMERS

Organizations and IT infrastructure

List of organizations

Jump hosts

Remote access methods

04 / ACTIVE DIRECTORY

Accounts

Service accounts

Privileged accounts

The information obtained enabled the attackers to prepare an attack on one of the customers

Impersonating a contractor enabled access to a jump host

01 CORRESPONDENCE The conversation with a customer continued through the contractor employee's personal email account

02 PRETEXT Additional work was presented as a continuation of legitimate cooperation

03 ACCESS Remote access to the customer's jump host was obtained

04 RECONNAISSANCE The attackers studied remote access methods, the domain environment, accounts and privileges, critical servers, databases and network architecture

Access to the jump host was used for reconnaissance over the following week

Compromising AD established a persistent presence

AD

DOMAIN ENVIRONMENT

The pivot point from the jump host into the IT infrastructure

01 ACCOUNTS

Active Directory accounts were compromised

02 PRIVILEGES

Credentials were obtained for privileged and service accounts

03 PERSISTENCE

A persistent presence was established in the IT infrastructure

After AD was compromised, the attack extended beyond a single jump host

Databases and a backup of an IT employee's personal mobile device were exfiltrated

01 / DISCOVERY AND EXFILTRATION

DATABASES

CONTAINED INFORMATION ABOUT

Finances
Employees
Customers
Logistics processes

02 / DISCOVERY AND EXFILTRATION

UNENCRYPTED MOBILE DEVICE BACKUP

A personal Apple mobile device
The backup was found on an IT employee's corporate workstation

BACKUP CONTENTS

Conversations in messaging apps
Various credentials
Communication network diagrams
Photos of documents containing confidential information

The unencrypted personal mobile device backup became another source of confidential information

Server backups were destroyed and corporate network connectivity was disrupted

01 IT SERVER BACKUPS DESTROYED

02 NETWORK DEVICE CONFIGURATION FILES DELETED

03 CORE SWITCH CONFIGURATIONS MODIFIED



RESULT

CORPORATE DATA NETWORK CONNECTIVITY DISRUPTED

01 DOMAIN ENVIRONMENT DEGRADED
02 NORMAL ACCESS TO MOST SECURITY TOOLS LOST
03 CENTRALIZED ACCESS TO TELEMETRY RESTRICTED

Database encryption escalated into extortion

01 PASSWORDS Passwords for corporate databases were changed

02 ENCRYPTION Databases in the organization's IT infrastructure were encrypted

03 RANSOM An IT employee received a ransom demand via Telegram in exchange for restoring access to the data

04 DATA PUBLICATION The attackers threatened to publish all information from the personal Apple device backup that could damage the employee's honor, dignity and professional reputation. To demonstrate that the threat was real, they posted some of this information in a Telegram channel

The extortion combined denial of data access with threats to publish sensitive information

Three risk factors and the role of digital forensics

01 / PERSONAL ACCOUNT

START OF THE CHAIN

Compromising a single personal account can lead to a large-scale incident

02 / CONTRACTOR

TRUSTED ACCESS

Trusted access for contractors without adequate oversight creates significant risk

03 / DATA STORAGE

DATA OUTSIDE CONTROL

Unauthorized storage of restricted work information on personal mobile devices and in their backups can harm both the organization and the employee

When normal access to security tools is unavailable, digital forensics helps reconstruct the incident

10 response stages when normal access to security tools is unavailable

01-05 / INITIAL ACTIONS AND DECISIONS

01 Document, register and perform initial escalation

02 Organize the response

03 Make a preliminary assessment of incident scope

04 Issue mandatory notifications and coordinate externally

05 Decide on further actions for the systems and devices under investigation

06-10 / COLLECTION, RECONSTRUCTION AND CLOSURE

06 Preserve volatile artifacts and data at high risk of loss

07 Acquire verifiable copies of storage devices, virtual machines and persistent digital data for subsequent examination

08 Reconstruct the attack sequence and test hypotheses

09 Remediate the impact and restore the IT infrastructure

10 Close the security incident and implement corrective actions

Preserve volatile artifacts or isolate the host?

01 / PRESERVE VOLATILE ARTIFACTS BEFORE ISOLATION

Conditions:

- A link to the incident has been established;
- damage is no longer occurring;
- there are no suspicious network connections or attacker-accessible paths to other systems and resources.

KEEP THE HOST POWERED ON UNTIL STAGE 6 IS COMPLETE

Take further actions in accordance with the documented decision.

02 / PRIORITIZE CONTAINMENT

Conditions:

- Encryption, deletion or modification of data continues;
- a suspicious network connection exists;
- an attacker-accessible path to other systems and resources remains.

CONTAINMENT TAKES PRIORITY

Perform automated data collection if acceptable. Then isolate the host, preferably without powering it off. If any delay is unacceptable, isolate it immediately and preserve the available data afterward.

SPECIAL CASES (FULL PROCEDURE AVAILABLE VIA THE QR CODE):

- No established link to the incident: do not collect data (reconsider if new information becomes available).
- Host powered off: do not power it on or boot its operating system.
- Running VM: take a snapshot including RAM, if supported and if this does not delay containment.

There is no universal rule to "collect everything first" or "isolate everything immediately."
Make a separate decision for each host.

Start with the data most likely to be lost



01 BASIC HOST INFORMATION

Host name, operating system or loaded kernel version, uptime, current account, system date, time and time zone; simultaneously record the time from an independent source and its offset from the host's system time

02 SESSIONS AND ACTIVITY

Active users and sessions, processes and services with their startup parameters, cached authentication data for current sessions, and open files

03 LOGS AND MODULES

Local logs at risk of being overwritten, loaded drivers and modules, kernel extensions, and active interprocess communication mechanisms

04 NETWORK STATE

Network interfaces, active connections and listening ports, network routes, and information about neighboring hosts (ARP/NDP)

Capture a RAM dump after collecting the data listed above*

*** If a compatible, tested tool is available and the operation does not create unacceptable risk.**

Capture the state before restoring the network

CLI

LOCAL ACCESS

Connect through the local console port from a standalone workstation that is not joined to the domain

01 BEFORE THE FIRST COMMAND

Enable terminal session logging and record the time from an independent source

02 FIRST COMMAND

Capture the available command history: new commands may displace earlier entries from the limited buffer

03 THEN CAPTURE THE STATE

Record system time, device version and uptime, administrative sessions, logs, running and startup configurations, interface status, network routes and key operational tables

Use only pre-tested display commands with minimal and predictable impact

A verifiable copy: provenance and integrity

VERIFIABILITY - data source, acquisition method, tool and version, operation time, output location and calculated checksums.

01 / PHYSICAL DRIVE

WRITE PROTECTION

Do not boot the operating system from the drive under examination.

A hardware write blocker is preferred.

If none is available, use pre-tested software write protection.

Acquire a sector-by-sector (bit-for-bit) copy when technically feasible and justified.

02 / RAID ARRAY

NO UNNECESSARY DISASSEMBLY

Record the controller model, RAID level and state, disk count, physical bay (slot) numbers, serial numbers and the state of each disk.

If the logical volume is accessible through the existing controller, acquire it without disassembling the array; prevent writes and automatic rebuilds.

Otherwise, reconstruct it from copies of the physical drives.

03 / VIRTUAL MACHINE

SELF-CONTAINED SET

Export the configuration, platform logs, base virtual disk and the full chain of linked differencing disks.

Export the memory state file if available.

If a sector-by-sector (bit-for-bit) copy is technically impossible, perform documented, targeted collection