Introduction to IT Security - Exercise sheet 2

Vianney HERVY

0. Use of generative AI

For this report, I used Google's Gemini[1] exclusively for halping translating certain sentences in the provided sources in german. Not only is it better at reformulating in a more english/french-native way, but is also able to simplify and sumarize the statements.

1. Current Attacks[2]

The Schweizerische Gesundheitsstiftung RADIX (Radix Foundation) is a non-profit organization in Switzerland that acts as a national competence center for the development and implementation of public health and sustainable development measures. As it provides services and handles sensitive data for various administrative units of the Swiss Federal Administration and public health initiatives, it represents a critical point in the nation's supply chain.

The attack was carried out by a known cybercrime organization: the Sarcoma ransomware group. Their primary goal was financial extortion: Demanding a ransom payment from Radix in exchange for a decryption key to restore encrypted data. The attackers also stole 1.3 TB of sensitive data before encryption. Their secondary goal was to threaten the company to leak this stolen data. Ultimately, Radix refused to meet the ransom demands, leading to the successful double extortion where the stolen 1.3 TB of sensitive data was leaked, resulting in significant reputational and legal damage.

Radix did not communicate precisely on its security mechanisms but we can assume that working closely with the Swiss Federal Administration offices and handling sensitive public health information requires high security standards. How the malware overcame the security mechanisms can also only be inferred.

Radix's major security mechanism is data backup. Backuping all data voids any random attack and prevents data losses. Radix's network is segmented in different infrastructures. This measure makes any attack less scalable because it may isolate the critical services from the compromised network. Concerning reactivity mechnisms, Radix's team immediately revoked access to the compromised systems and engaged the National Cyber Security Centre, Zurich Police and Data Protection Commissioner. Fast response is often what limits the damages.

Despite the presumed high standards, the Sarcoma group's success implies that the attackers effectively bypassed the initial perimeter and then moved laterally to the main network. While the specific exploit remains undisclosed, the initial access was likely achieved through a spear phishing campaign or by exploiting a vulnerability in a publicly accessible service (like a VPN). This initial foothold overcame the perimeter defense. Once inside, the attackers probably exploited poor credential hygiene to escalate privileges from a basic user account to a domain administrator. With elevated rights, the attackers disabled or avoided endpoint detection tools before initiating their large-scale data exfiltration—bypassing logging and internal network monitoring. Crucially, while network segmentation successfully protected the separate counseling services, it failed to fully isolate the main administrative and data storage networks, allowing the threat actors to spread widely enough to encrypt key systems and steal 1.3 TB of data before the IR team could fully contain the main breach.

[1] https://gemini.google.com/

[2] https://www.news.admin.ch/

2. Malware

2.1. Number of new Malwares reported daily[3]

Approximately 11.500 new mobile malware variants are registered daily, with Android devices being the primary target.

2.2. Botnets[4]

A botnet is a network of computers (roBOT-NETwork) that have been secretely infected with malware. These devices are controlled by command servers and are frequently used for DDoS attacks. Internet of Things is playing a large role as botnet component. Indeed, there is a growing number of devices to infect and control.

Android is the primary target for mobile malware, which is often used to establish or expand botnets for mobile devices. Most of the IoT devices run on Android, restating the point previously made.

2.3. Typical actions perfomed before executing ransomware[5]

The attack begins with an initial infection where a spam email with a malicious attachment compromises a victim's device. Once inside, the attackers perform lateral movement to navigate from the single infected machine into the broader corporate network. Finally, before locking any files, they steal sensitive data and exfiltrate it to an external server, ensuring they have leverage for extortion before the encryption phase begins.

2.4. Recommended mechanisms againts malware[6]

ID	Requirement Title	Protection Level
OPS1.1.4	Creating a Malware Protection Concept	Basic
OPS.1.1.4.A2	Using System-Specific Protection Mechanisms	Basic
OPS.1.1.4.A3	Selection of a Virus Protection Program	Basic
OPS.1.1.4.A5	Operation and Configuration of Virus Protection Programs	Basic
OPS.1.1.4.A6	Regular Updating of Virus Protection Programs and Signatures	Basic
OPS.1.1.4.A7	User Awareness and Obligations	Basic
OPS.1.1.4.A9	Reporting Malware Infections	Standard
OPS.1.1.4.A10	Using Special Analysis Environments	Increased
OPS.1.1.4.A11	Using Several Scan Engines	Increased
OPS.1.1.4.A12	Using Storage Media Locks	Increased
OPS.1.1.4.A13	Handling Untrusted Files	Increased
OPS.1.1.4.A14	Selecting and Using Cyber Security Products to Thwart Targeted Attacks	Increased

3. Vulnerability Management

For this part, the IDs and descriptions and CVSS scores come directly from the EUVD's public API.

[3] **Cybercrime Bundeslagebild**, 2019, p. 15

[4] **Cybercrime Bundeslagebild**, 2019, p. 3, 25, 39

[5] **Die Lage der IT-sicherheit in Deutschland**, 2022, p. 15, (figure 3)

[6] **IT-Grundschutz-Compendium**, 2022, p.

[7] https://nvd.nist.gov/vuln/detail/CVE-2025-26533

3.1. EUVD-2025-4270 (8.1)[7]

- **Description:** An SQL injection risk was identified in the module list filter within course search.
- **Assets:** The Moodle database (containing all user, grades and course data
- **Workarounds:** No official config workaround. The vulnerability lies deep in the core search logic. However, disabling the feature will prevent any attack.

3.2. EUVD-2025-4274 (8.3)[8]

- **Description:** Description information displayed in the site administration live log required additional sanitizing to prevent a stored XSS risk.
- **Assets:** Admin session/account (via cookie) and web server integrity
- **Workarounds:** Disabling Live log report

3.3. EUVD-2025-4275 (8.6)[9]

- **Description:** Insufficient sanitizing in the TeX notation filter resulted in an arbitrary file read risk on sites where pdfTeX is available (such as those with TeX Live installed).
- **Assets:** The server filesystem (LaTeX could read `/etc/passwd` or the Moodle config)
- **Workarounds:** Disabling the TeX notation filter

3.4. EUVD-2025-4271 (8.3)[10]

- **Description:** The question bank filter required additional sanitizing to prevent a reflected XSS risk.
- **Assets:** User accounts and session Tokens
- **Workarounds:** Raise awareness among teachers about not clicking on suspicious links

In most of the analyzed cases, the only effective workaround is to completely disable the affected feature. This highlights the critical importance of Security by Design. If a product is not built with security in mind from the start, IT operators are often left with no good options once it is shippedn ,forcing them to choose between keeping a service running insecurely or shutting it down entirely.

[8] https://nvd.nist.gov/vuln/detail/CVE-2025-26529

[9] https://nvd.nist.gov/vuln/detail/CVE-2025-26525

[10] https://nvd.nist.gov/vuln/detail/CVE-2025-26530