NMC2S Technical Report

ANDREI CIRLIG(20049583)

16/12/2024

7COM1069-0901-2024 - Cyber Operations

Table of Contents

Executive Summary

A suspected cyberattack targeted the **National Military Command and Control System (NMC2S)**, a critical component of the nation's **Critical National Infrastructure (CNI)**. The abnormal traffic detected disrupted the operations of the NMC2S, raising concerns about potential adversarial intent. While the attacker's ultimate objective remains uncertain, it is believed they may aim to steal sensitive data, disrupt critical functions, or sabotage military operations through lateral movement within the network.
This report provides a detailed analysis of the captured **PCAP file**, which was obtained post-attack. The analysis seeks to uncover the methods employed by the adversary, assess the extent of the impact, and evaluate the security posture of the NMC2S.

Introduction

The **National Military Command and Control System (NMC2S)** is a vital infrastructure supporting national defense. It plays a critical role in facilitating secure military communications, managing highly classified information, and coordinating logistics for effective operational readiness. The integrity and availability of this system are essential for maintaining the nation's military effectiveness.
This investigation aims to:

1. Identify the techniques and methods used during the cyberattack.
2. Assess the overall impact of the attack on the NMC2S.
3. Determine the intentions of the adversary to provide insight into the threat landscape.
4. Propose robust mitigation strategies to prevent future incidents.

By analyzing the attack and strengthening the system's defenses, this report contributes to safeguarding the nation's CNI from evolving cyber threats. The findings and recommendations aim to improve the security posture of the NMC2S and create a resilient framework against future risks.

Attack and Threat analysis

Reconnaissance Activity

The PCAP file provided has a total of 129772 of packets displayed. To analyse the PCAP file for evidence of suspicious activity and potential threats or exploitations, I used different filters to sort the protocols and note the IP addresses that have an unusual activity.

1.HTTP

HTTP is an application-layer protocol used to exchange information between clients (e.g., web browsers) and servers. I started looking for POST or GET methods that have unusual web addresses. The analysed packets look legitimate apart from the ones exchanged between the IP 10.1.30.101 and the IPs 94.131.101.186 and 5.252.178.193. Further investigation is needed to see if this behaviour is an indicative of exfiltration of data.

2.TCP

The TCP protocol operates as a transport layer and establishes a connection between the sender and receiver before data transmission via the three-way handshake.
There are isolated connections to various destination which seem to be legitimate connection patterns(Figure 2), but TCP is vulnerable to SYN Floods and we can check for suspicious behaviour by using the filter tcp.flags.syn == 1 && tcp.flags.ack == 0.

The main source IP address for this suspicious behaviour is 192.168.3.112, targeting destination 192.168.1.158(Figure 3)

The main focused target was port 80 (HTTP) and 443 (HTTPS) and shows that most likely an automated tool was used by the attacker because source ports were incremented sequentially.
The attack occurred in a flood which could mean that the attack was being planned, but further investigation of the source IP address behaviour is needed in order to conclude if it was indeed an attack or a malfunction.

3.TLS

TLS is a cryptographic protocol that operates above **TCP** to provide **secure communication** over a network. When combined with TCP, TLS ensures that data is encrypted, authenticated, and maintains its integrity during transmission.

We can use the TLS SNI hostname to check for suspicious behaviour by using the filter ssl.handshake.extensions_server_name (Figure 4) and then checking the hostnames on virustotal.com

4.SMTP

SMTP (Simple Mail Transfer Protocol) is a protocol used for **sending emails** between servers and from clients to mail servers. Using the Tools > Credentials inside the Wireshark , we can observe that 2 authentication processes have been started(Figure 5) by the same IP address of 10.9.16.101. Furthermore, if we follow the TCP Stream of the first credentials we

will observe a possible exfiltration of private data and further investigation is needed. (Figure 6)

Exploitation attempts

DoS Attack

Following up on the suspicious activity of the IP 192168.3.112(PEC-PJ21AAC-LT) I decided to use the “Conversations” sub-menu from Wireshark to get an accurate number of connection request packets(SYN) sent without an ACK packet , thus creating a SYN flood attack to IP 19.168.1.158.

As seen in Figure 7 , there are 77,309 packets that received no response. This activity took almost 35 minutes and targeted the port 80 (HTTP) , from 12:02 until 12:37. This action resulted in a loss of availability of that service as it can be seen in Figure 8.

Analysing the packets further I’ve discovered that 192.168.3.112 sent 1344 packets using the CLDAP protocol through the UDP port 389 to different IP addresses: 147.197.131.130, 147.197.131.222, 147.197.131.193, 147.197.131.48 and 147.197.131.118.

These packets were sent almost in the same time with the TCP packets , from 12:07 until 12:34 indicating a possible CLDAP exploitation , but they didn’t received any response indicating a failure of amplification or a possible attempt to reconnaissance activity.

Malware Injection

The IP address of 10.1.30.101 demonstrates a multi-stage cyberattack leveraging malvertising and Command and Control (C2) communication. In the time span of 1 second a DNS request is made to adclick.g.doubleclick.net followed by two other intermediary domains projetodegente.com and www.verxy.me before connecting to a suspicious IP address hosted by a cloud provider , http://5.252.178.193/ . After verifying these 3 domains on virustotal.com I discovered they’ve been flagged as malicious as it can be seen in Figure 9 ,10,110.

Using a WebDAV client (Microsoft-WebDAV-MiniRedir/10.0.19045), the system made multiple OPTIONS and PROPFIND requests, ultimately retrieving a ZIP file (independert.zip, ~2 MB) containing an .msi file. Following the successful download, the system initiated multiple HTTP POST requests to mainsercheronlinehostingbot.com:8094, indicative of C2 communication. These requests suggest the ZIP file contained malware, which, upon execution, registered with the C2 server, potentially exfiltrated data, or retrieved additional

payloads. The use of non-standard HTTP port 8094 highlights an attempt to evade detection.

Going further with the investigation I downloaded the .zip file through Wireshark and uploaded it on virustotal.com. The file was flagged as being a Trojan(Figure 12) and being related to **DarkGate** malware. This offers more insight about the threats posed by this breach as **DarkGate** is a known sophisticated malware that operates as a **multi-purpose Trojan**, often used for data theft, ransomware deployment, remote access, and other malicious activities.

Infostealer keylogger over SMTP protocol

The IP address of 10.9.16.101 connects to a malicious domain (Figure 13) smtp.inhousepick.com through DNS then connects to the SMTP server us2.outbound.mailhostbox.com by providing a username and a password(Figure 14). The username and password are in Base64 format but by decoding them we can see that the credentials used are password : #(P%eO^#J0 and username: sender@inhousepick.com .

Studying one of the emails sent by 10.9.16.101 I observed an unusual pattern where the words " / VIP Recovery \ " were repeating . After further research I discovered that this is a common pattern of a infostealer named VIPKeyLogger and it shares a lot in common with the subscription-based Snake Keylogger, which is also known as 404 Keylogger.
The common way it spreads it's through phishing campaigns as an attachment that takes the form of an archive or Microsoft 365 files. The archive contains executable content in Microsoft Office files spread via C2.

Exfiltration or Sabotage

1. The malware that infested the IP 10.1.30.101 managed to send 25 HTTP POST requests as we can see in the Figure 15. All these requests happened in 33 seconds and all of them have been successful.

The success of these requests indicates that the receiving server acknowledged the data transmission and the presence of multiple POST requests suggests an iterative or bulk exfiltration process.

Even if HTTP is used (unencrypted), the malware seems to encrypt the payload itself making the exfiltrated data difficult to be analysed.

2. The keylogger that infested the IP 10.9.16.101 managed to exfiltrate 18 Accounts and Passwords from different websites and Outlook alongside the Client IP address , Country Name , Country Code , Time Zone , Longitude and Latitude. (Figure 16)

Attribution and Motive Analysis

The incidents involving the DoS attack, Trojan malware, and keylogger that exfiltrated accounts and passwords point to several possible motives behind the malicious activities:

1. **Espionage**:
   The attackers may have been gathering sensitive information for surveillance or competitive advantage. The exfiltration of accounts and passwords suggests a deliberate focus on credential theft, possibly targeting personal, organizational, or financial systems.
2. **Financial Gain**:
   Cybercriminals often exploit stolen credentials for monetary benefits. The exfiltrated data could be sold on the dark web, used for fraudulent transactions, or employed in ransomware attacks.
3. **Strategic Advantage or Disruption**:
   The attackers might aim to destabilize operations or critical systems for political, competitive, or ideological reasons. The DoS attack could be intended to render key services unavailable, while the Trojan and keylogger activities may serve to degrade operational capacity or sow confusion.
4. **Botnet Expansion**:
   The Trojan and keylogger may also aim to infect systems for inclusion in a botnet, enabling larger-scale future attacks like DDoS campaigns or spam distribution.

Critical Infrastructure and Risk Assessment

Critical ICT Assets in NMC2S

1. **Communication Servers**:
   - **Role**: Facilitate secure, real-time communication between military personnel, strategic operations centres, and field units.
   - **Examples**:
     - Secure Voice over IP (VoIP) servers.
     - Encrypted email servers.
     - Messaging platforms with end-to-end encryption.
   - **Importance**: Interruption or compromise can lead to miscommunication or complete loss of coordination during military operations.
2. **Data Repositories**:
   - **Role**: Store sensitive military data such as operational plans, logistics details, and intelligence reports.
   - **Examples**:

        - Centralized databases (e.g., PostgreSQL, Oracle DB) with classified information.
        - Data lakes for intelligence analysis.
        - Redundant backup systems to prevent data loss.
    - **Importance**: Breaches could expose sensitive data, leading to significant strategic disadvantages.
3. **Network Gateways and Firewalls**:
    - **Role**: Control traffic flow in and out of the NMC2S network, ensuring only authorized access.
    - **Examples**:
        - Intrusion Prevention Systems (IPS).
        - Virtual Private Network (VPN) gateways.
        - Next-generation firewalls with Deep Packet Inspection (DPI).
    - **Importance**: Exploitation could allow unauthorized access or data exfiltration.
4. **Control Systems**:
    - **Role**: Oversee and coordinate logistical and operational systems such as supply chain management, troop deployments, and strategic asset allocation.
    - **Examples**:
        - Logistics Management Systems (LMS).
        - Command and Control (C2) software platforms.
        - Automated tasking and deployment systems.
    - **Importance**: Disruption can cripple operational capabilities, causing delays or failures in military responses.
5. **Authentication and Identity Management Systems**:
    - **Role**: Manage secure access to NMC2S resources and prevent unauthorized use.
    - **Examples**:
        - Multi-Factor Authentication (MFA) servers.
        - Public Key Infrastructure (PKI) for certificate-based authentication.
        - Active Directory (AD) or similar directory services.
    - **Importance**: Compromising this system could allow adversaries to impersonate authorized personnel.
6. **Monitoring and Logging Systems**:
    - **Role**: Collect and analyse network activity data to detect anomalies and breaches.
    - **Examples**:
        - Security Information and Event Management (SIEM) tools (e.g., Splunk).
        - Packet capture and analysis tools (e.g., Wireshark, Zeek).
        - Endpoint Detection and Response (EDR) systems.
    - **Importance**: Disabling these systems would hinder the ability to detect and respond to intrusions.

Risk Assesment

Asset	Vulnerability	Vulnerability code from ISO/IEC 2005:2022(E)	Threat to IS properties CIA	Threat code from ISO/IEC 2005:2022	Consequence (C) Rating	Likelihood (L) Rating	Risk Rating (R = C x L)	Risk Treatment category (Accept/Reduce/Transfer/Avoid)
Monitoring and Logging System	Failure to encrypt log data during storage or transmission	VS01, VS02	Disabling detection tools	TH05 , TH07, TH10, TO04	4	3	12	Avoid
Data Backup System	Missing encryption of sensitive data	VS14, VS06	Ransomware or destruction of data	TH08, TH10, TH15, TO04, TO02	3	3	9	Avoid
Firewall	DDoS attacks	VN05, VN08	DoS attacks on gateways	TH25, TC01, TI03	3	3	9	Reduce
Laptops /Desktops	Unauthorized access due to lack of access control policy	VO26,VS13,VP06	Potential to data leakage	TH04,TH06,TH08, TH10	3	2	6	Reduce
Human Resources	Intentional/deliberate information leakage attempt	VP06,V018	Organizations CIA will be compromised	TC02,TO04,TH24	4	2	8	Avoid
Communication Server	Weak encryption protocols	VS02, VS13	Interception of sensitive data	TH08, TH10, TH15, TO04	3	3	9	Reduce
Centralized database	Unsecured access points/Insider threats	VS02 , VS14	Malware stealing endpoint data	TH10 , TH15, TH25	3	4	12	Avoid

	with privileged access							

Counterintelligence and Attribution

Tracing Threat Actors and TTPs

1. DoS Attack

- Attacker TTPs:
  - Tactic: Denial of Service (DoS).
  - Technique:
    - A SYN flood attack was launched from 192.168.3.112 targeting 192.168.1.158, overwhelming port 80 (HTTP) with 77,309 SYN packets without receiving corresponding ACK responses.
    - Simultaneous use of the CLDAP protocol (UDP port 389) suggests an attempt to exploit CLDAP amplification, which is a known method for reflection and amplification DoS attacks.
  - Procedure:
    - The attack spanned 35 minutes, causing a loss of service availability for port 80.
    - CLDAP requests to multiple IPs did not receive responses, indicating a reconnaissance attempt or failed amplification.
- Attribution Clues:
  - The coordinated use of TCP (SYN flood) and UDP (CLDAP) suggests a well-organized attacker leveraging a botnet or automated tools.
  - Specific IPs for the CLDAP traffic can be cross-referenced against threat intelligence databases to identify potential botnet command and control infrastructure.

2. Malware Injection

- Attacker TTPs:
  - Tactic: Malware Injection and C2 Communication.
  - Technique:
    - The attack leveraged malvertising to initiate a DNS request to adclick.g.doubleclick.net, redirecting through intermediary malicious domains (projetodegente.com and www.verxy.me) before connecting to the suspicious IP 5.252.178.193.
    - A WebDAV client (Microsoft-WebDAV-MiniRedir/10.0.19045) was used to issue OPTIONS and PROPFIND requests, ultimately retrieving a ZIP file (independert.zip).

        - Post-download, multiple HTTP POST requests were sent to mainsercheronlinehostingbot.com:8094, indicating C2 communication for data exfiltration or payload retrieval.
    - Procedure:
        - The ZIP file contained a Trojan related to DarkGate malware, as confirmed by VirusTotal.
        - DarkGate is a sophisticated multi-purpose Trojan used for data theft, ransomware delivery, and remote access.
- Attribution Clues:
    - The use of known malicious domains and IPs flagged by VirusTotal suggests the involvement of a threat actor with access to a well-maintained C2 infrastructure.
    - The use of non-standard ports (8094) and WebDAV exploitation indicates an attempt to evade typical security measures.

3. Infostealer Keylogger Over SMTP

- Attacker TTPs:
    - Tactic: Credential Harvesting and Data Exfiltration.
    - Technique:
        - The attacker connected to the malicious domain smtp.inhousepick.com via DNS, followed by an SMTP connection to us2.outbound.mailhostbox.com.
        - Base64-encoded credentials were used to authenticate, revealing the username sender@inhousepick.com and password #(P%eO^#J0 upon decoding.
        - Emails sent by the IP 10.9.16.101 contained repetitive patterns like / VIP Recovery \, a signature of the VIPKeyLogger malware, which is associated with the subscription-based Snake Keylogger.
    - Procedure:
        - Most probably the keylogger likely originated from a phishing campaign, delivered as a malicious Microsoft Office file or archive.
        - Data exfiltrated via SMTP includes credentials and possibly other sensitive system information.
- Attribution Clues:
    - Patterns resembling Snake Keylogger (404 Keylogger) suggest a commercially available malware tool often used by cybercriminals for espionage or financial theft.
    - Links to malicious domains (smtp.inhousepick.com) and SMTP servers could reveal C2 networks.

Threat Prediction

1. Future DoS Attacks:
    - Likelihood of a shift toward more sophisticated volumetric attacks leveraging additional reflection/amplification protocols like DNS or NTP.
    - Potential pivot to multi-vector attacks targeting critical systems.

2. Malware Campaigns:
    - Increased use of WebDAV exploitation for delivering additional payloads.
    - DarkGate malware might evolve to include enhanced obfuscation techniques, targeting not just individuals but enterprise systems.
3. Keylogger Campaigns:
    - Phishing campaigns may become more targeted, using legitimate-looking files or links to bypass security measures.
    - The stolen credentials could be used in credential-stuffing attacks on other systems.

Mitigation and Defensive Strategies

1. DoS Attack Mitigation

- **Technical Solutions**:
    - Implement rate limiting on port 80 and block unusual UDP traffic to port 389.
    - Deploy anti-DoS services such as Cloudflare or AWS Shield to absorb malicious traffic.
    - Monitor for SYN floods and configure firewalls to drop excessive SYN requests from a single source.
- **Proactive Strategies**:
    - Cross-reference involved IPs with threat intelligence to block related botnet infrastructure.
    - Conduct penetration tests to identify vulnerabilities in exposed services.

2. Malware Injection Mitigation

- **Technical Solutions**:
    - Block malicious domains (projetodegente.com, verxy.me, and 5.252.178.193) and similar flagged IPs.
    - Disable unused protocols like WebDAV if not required or limit it to internal use only.
    - Regularly scan endpoint devices with updated antivirus software to detect Trojan payloads.
- **Proactive Strategies**:
    - Conduct security awareness training for users to recognize malvertising attempts.
    - Enhance network segmentation to limit lateral movement if a Trojan infection occurs.

3. Keylogger Mitigation

- **Technical Solutions**:

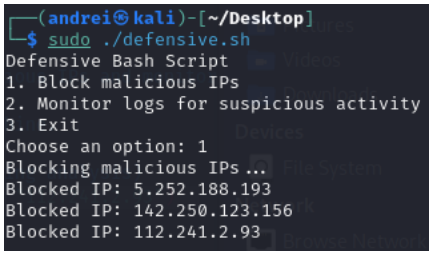
    - Block access to known malicious domains (smtp.inhousepick.com) and restrict outbound SMTP traffic.
    - Deploy endpoint detection tools to identify unauthorized keylogging activities.
    - Implement email filtering and sandboxing to prevent phishing payload delivery.
- **Proactive Strategies**:
    - Enable multi-factor authentication (MFA) for all systems to minimize the impact of stolen credentials.
    - Conduct phishing simulations to educate users about suspicious email attachments.

Defensive Bash Script

How the Script Addresses Defensive Tasks

1. **Blocking Malicious IPs**:
    - The script leverages iptables to block inbound and outbound traffic for known malicious IPs.
    - It prevents redundant rules by checking if the IP is already blocked before adding a rule.
    - Logs the actions taken for tracking and auditing purposes.
2. **Monitoring Suspicious Activity**:
    - Continuously monitors system logs (/var/log/syslog) for activity involving malicious IPs.
    - Alerts the user in real-time if suspicious activity is detected, allowing immediate action.
3. **Graceful Exit**:
    - Includes a trap mechanism to handle user interruptions (e.g., Ctrl+C), ensuring the script exits cleanly without leaving processes running.

Sample Output:



Conclusion

The analysis of the suspected cyberattack on the **National Military Command and Control System (NMC2S)** revealed a multi-faceted threat targeting the nation's **Critical National Infrastructure (CNI)**. Key findings include evidence of abnormal traffic indicative of a **DoS attack**, malware injection linked to **DarkGate Trojan**, and **keylogger-based credential theft**. These activities demonstrate sophisticated tactics aimed at disrupting operations, exfiltrating sensitive data, and potentially compromising military readiness.

The implications of such an attack are severe, including the risk of operational paralysis, loss of classified information, and weakened national security. These threats underscore the urgency of reinforcing the security of the NMC2S.

To mitigate future risks, it is recommended to:

1. Deploy **intrusion prevention systems (IPS)** and rate-limiting mechanisms to counter DoS attacks.
2. Strengthen endpoint security by restricting unused protocols, implementing anti-malware solutions, and conducting regular system audits.
3. Enforce **multi-factor authentication (MFA)** and improve email filtering to prevent phishing-based credential theft.

By addressing these vulnerabilities and enhancing the defensive capabilities of the NMC2S, the nation can build a more resilient infrastructure to withstand evolving cyber threats.

Appendices

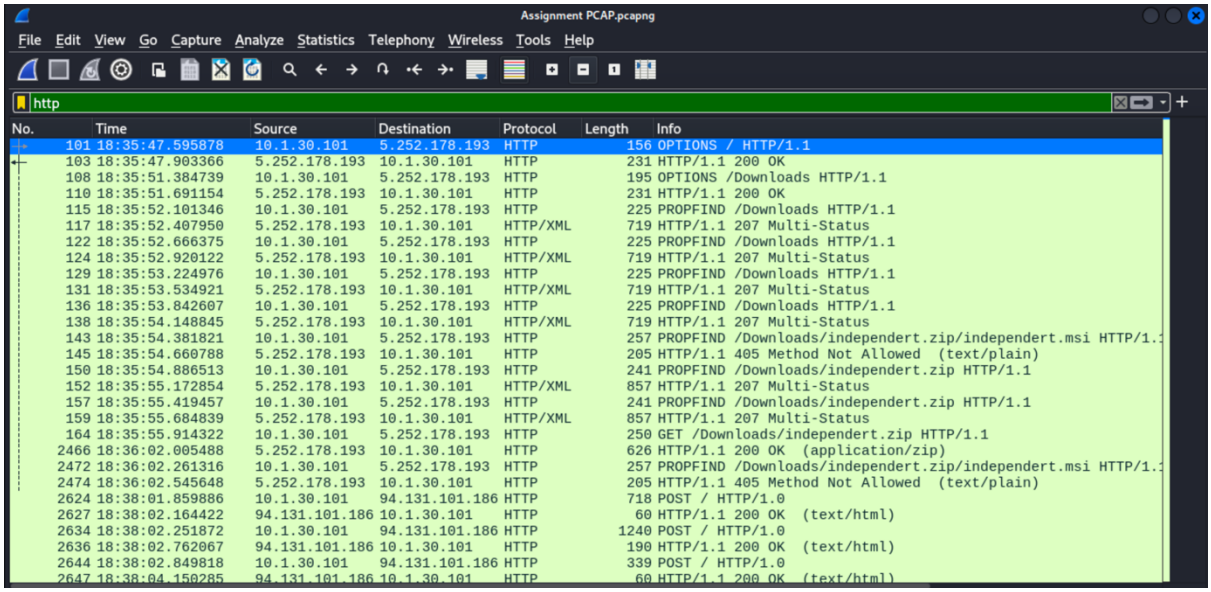


Figure 1

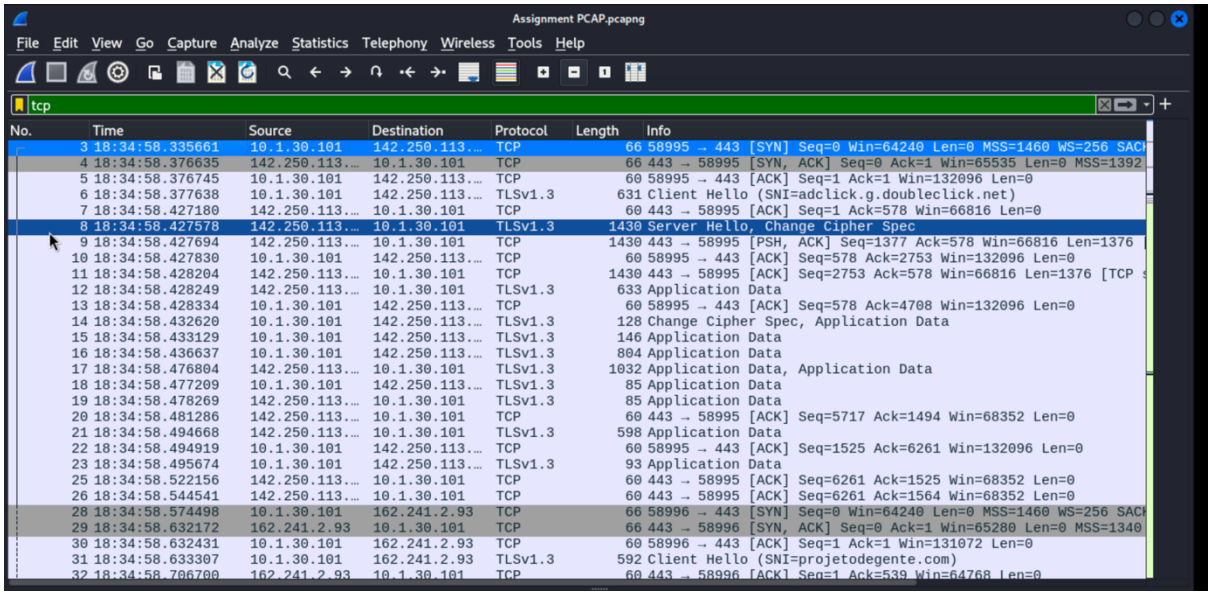


Figure 2

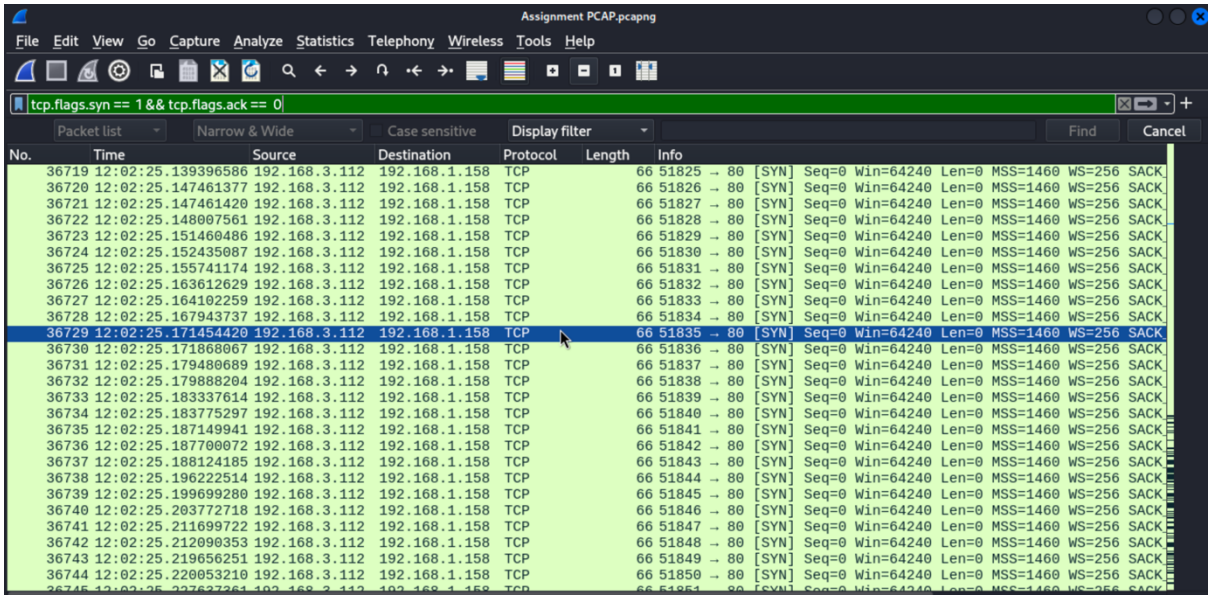


Figure 3

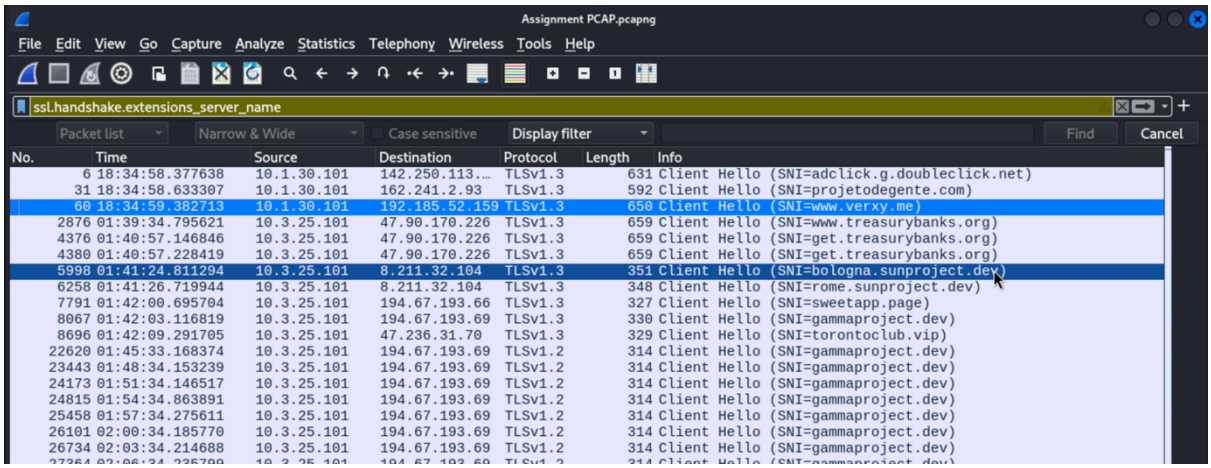


Figure 4

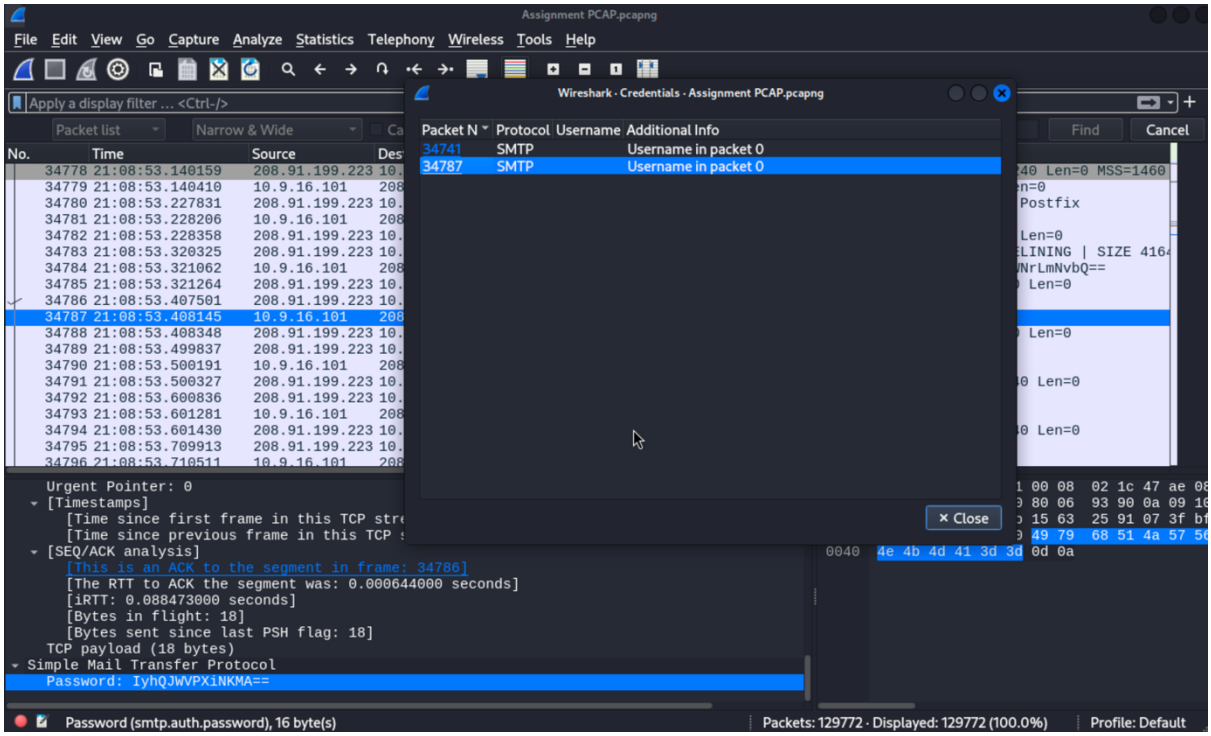


Figure 5

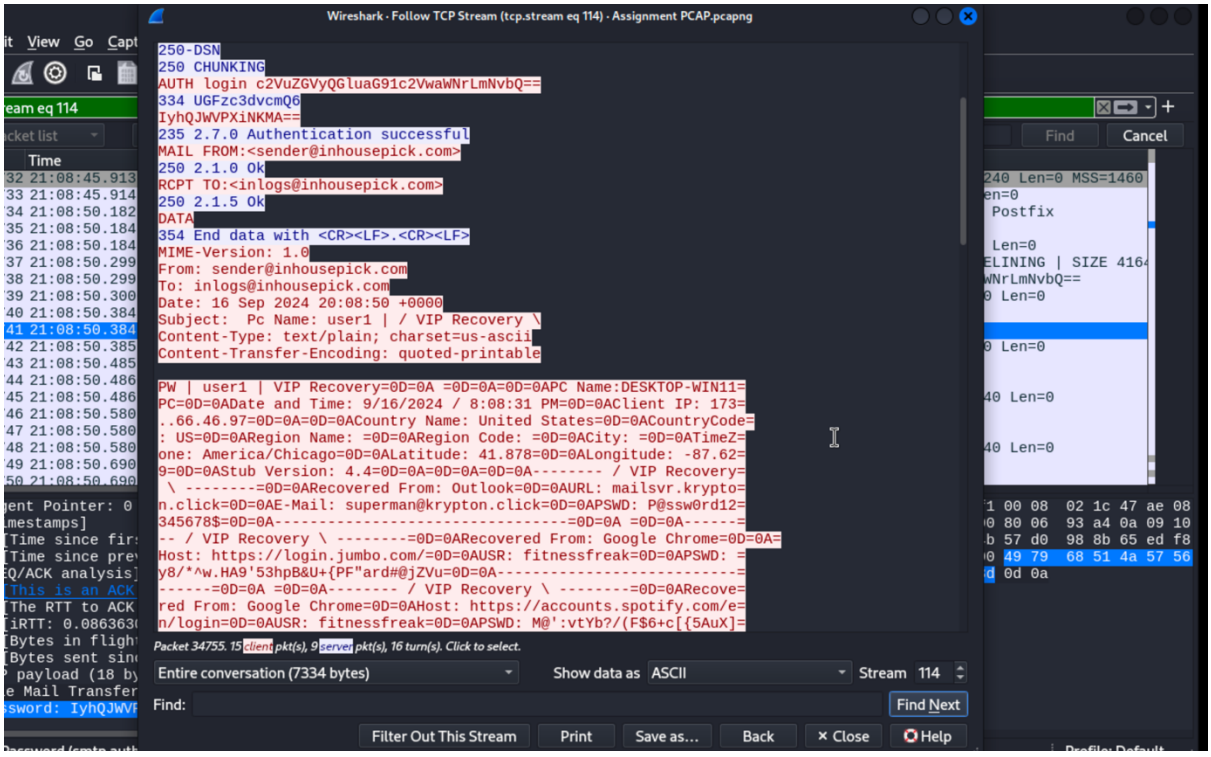
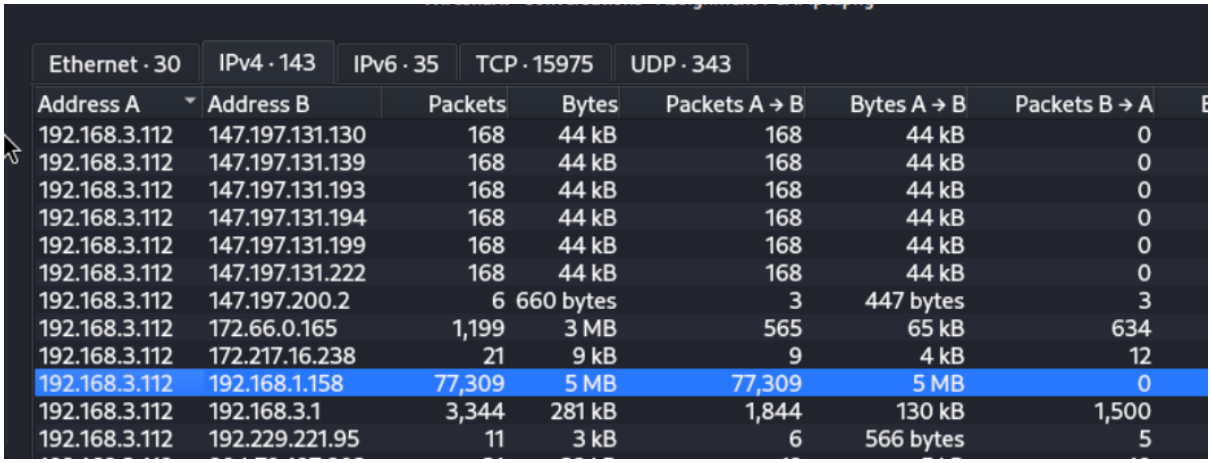


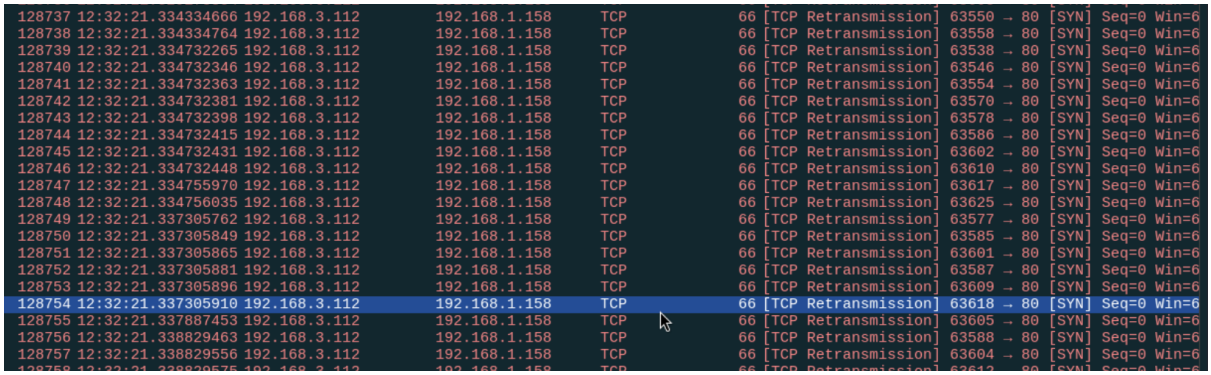
Figure 6



Ethernet · 30 | IPv4 · 143 | IPv6 · 35 | TCP · 15975 | UDP · 343

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
192.168.3.112	147.197.131.130	168	44 kB	168	44 kB	0
192.168.3.112	147.197.131.139	168	44 kB	168	44 kB	0
192.168.3.112	147.197.131.193	168	44 kB	168	44 kB	0
192.168.3.112	147.197.131.194	168	44 kB	168	44 kB	0
192.168.3.112	147.197.131.199	168	44 kB	168	44 kB	0
192.168.3.112	147.197.131.222	168	44 kB	168	44 kB	0
192.168.3.112	147.197.200.2	6	660 bytes	3	447 bytes	3
192.168.3.112	172.66.0.165	1,199	3 MB	565	65 kB	634
192.168.3.112	172.217.16.238	21	9 kB	9	4 kB	12
192.168.3.112	192.168.1.158	77,309	5 MB	77,309	5 MB	0
192.168.3.112	192.168.3.1	3,344	281 kB	1,844	130 kB	1,500
192.168.3.112	192.229.221.95	11	3 kB	6	566 bytes	5

Figure 7



```
128737 12:32:21.334334666 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63550 → 80 [SYN] Seq=0 Win=6
128738 12:32:21.334334764 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63558 → 80 [SYN] Seq=0 Win=6
128739 12:32:21.334732265 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63538 → 80 [SYN] Seq=0 Win=6
128740 12:32:21.334732346 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63546 → 80 [SYN] Seq=0 Win=6
128741 12:32:21.334732363 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63554 → 80 [SYN] Seq=0 Win=6
128742 12:32:21.334732381 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63570 → 80 [SYN] Seq=0 Win=6
128743 12:32:21.334732398 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63578 → 80 [SYN] Seq=0 Win=6
128744 12:32:21.334732415 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63586 → 80 [SYN] Seq=0 Win=6
128745 12:32:21.334732431 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63602 → 80 [SYN] Seq=0 Win=6
128746 12:32:21.334732448 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63610 → 80 [SYN] Seq=0 Win=6
128747 12:32:21.334755970 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63617 → 80 [SYN] Seq=0 Win=6
128748 12:32:21.334756035 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63625 → 80 [SYN] Seq=0 Win=6
128749 12:32:21.337305762 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63577 → 80 [SYN] Seq=0 Win=6
128750 12:32:21.337305849 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63585 → 80 [SYN] Seq=0 Win=6
128751 12:32:21.337305865 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63601 → 80 [SYN] Seq=0 Win=6
128752 12:32:21.337305881 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63587 → 80 [SYN] Seq=0 Win=6
128753 12:32:21.337305896 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63609 → 80 [SYN] Seq=0 Win=6
128754 12:32:21.337305910 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63618 → 80 [SYN] Seq=0 Win=6
128755 12:32:21.337887453 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63605 → 80 [SYN] Seq=0 Win=6
128756 12:32:21.338829463 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63588 → 80 [SYN] Seq=0 Win=6
128757 12:32:21.338829556 192.168.3.112  192.168.1.158  TCP  66 [TCP Retransmission] 63604 → 80 [SYN] Seq=0 Win=6
```

Figure 8

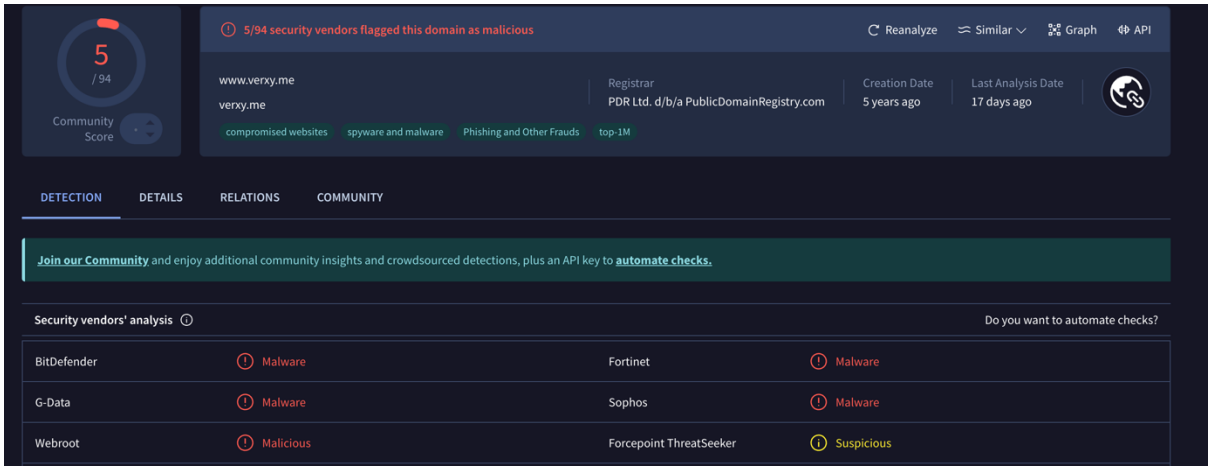


Figure 9

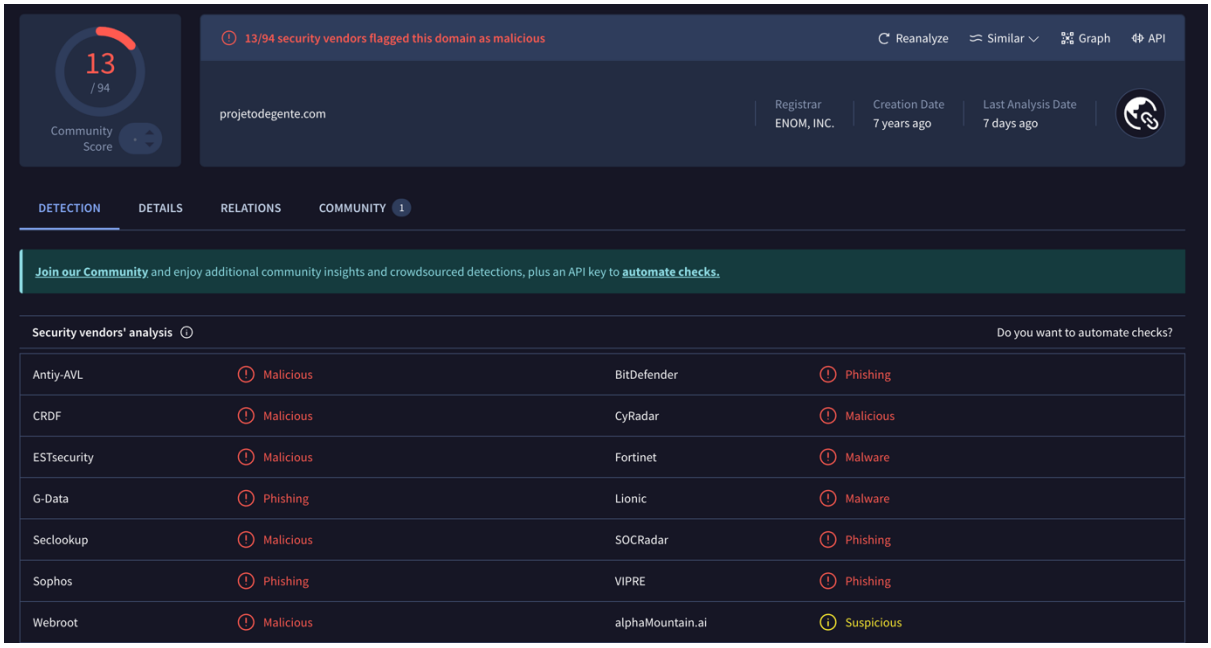


Figure 10

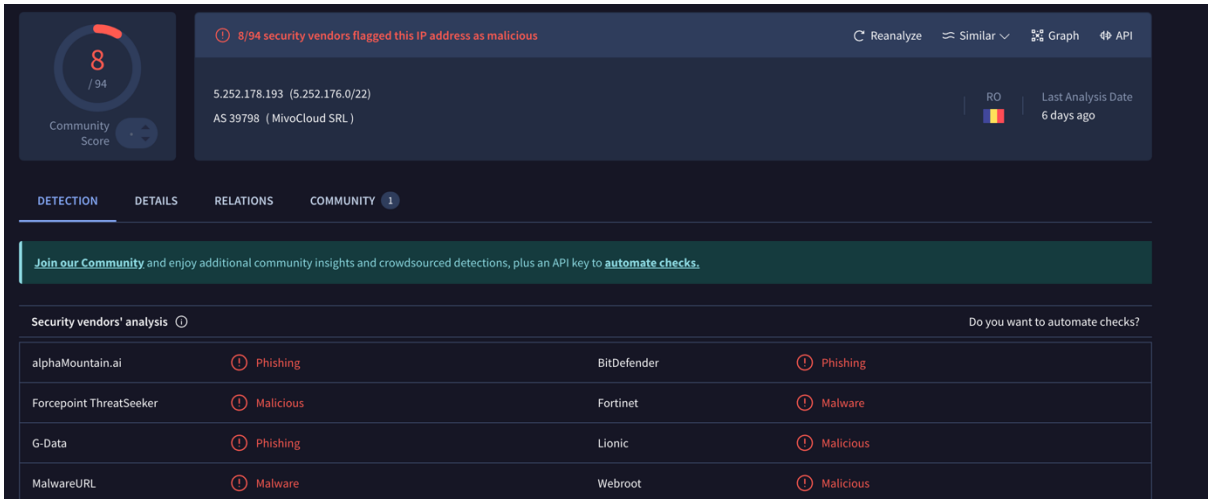


Figure 11

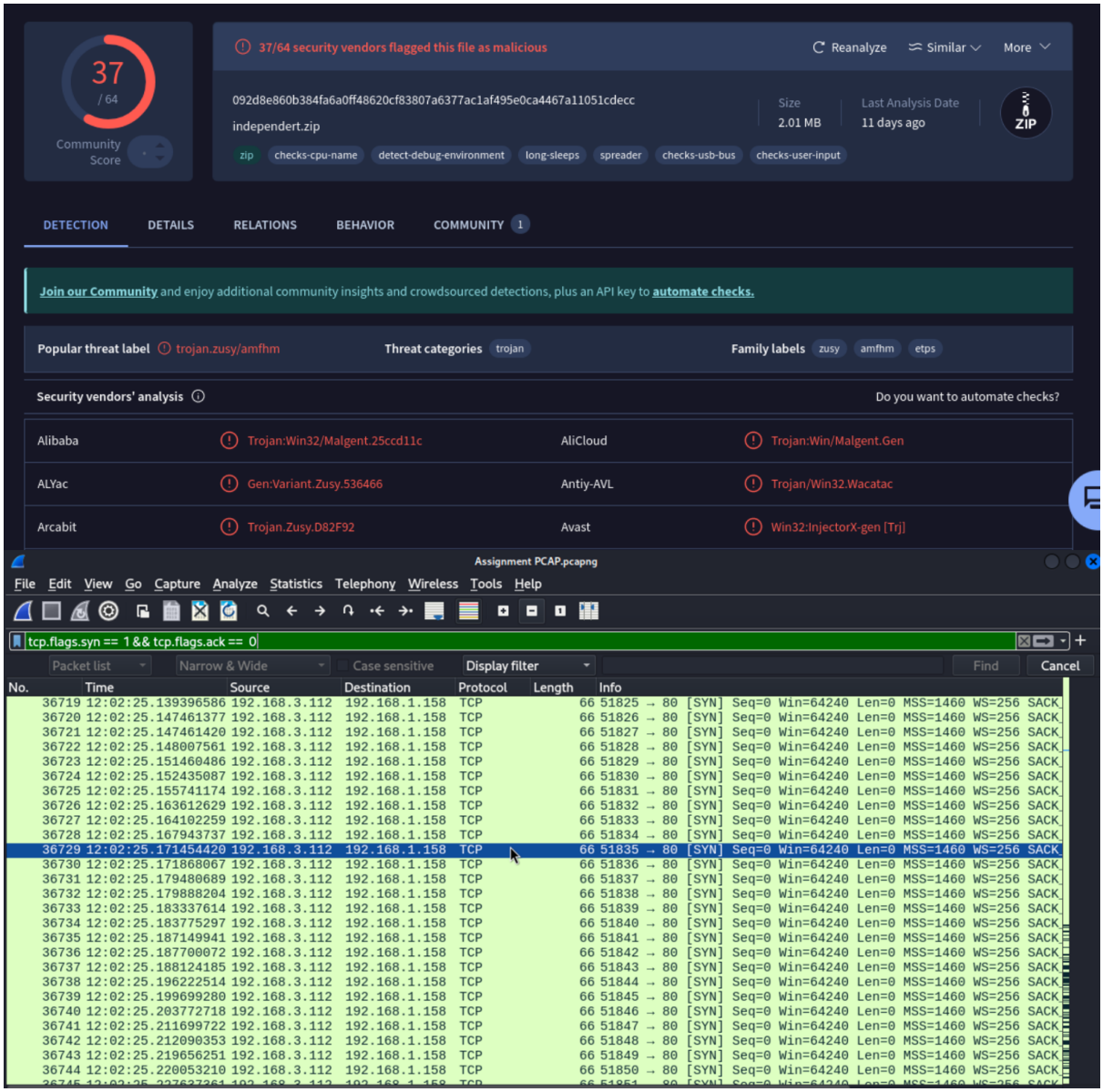


Figure 12

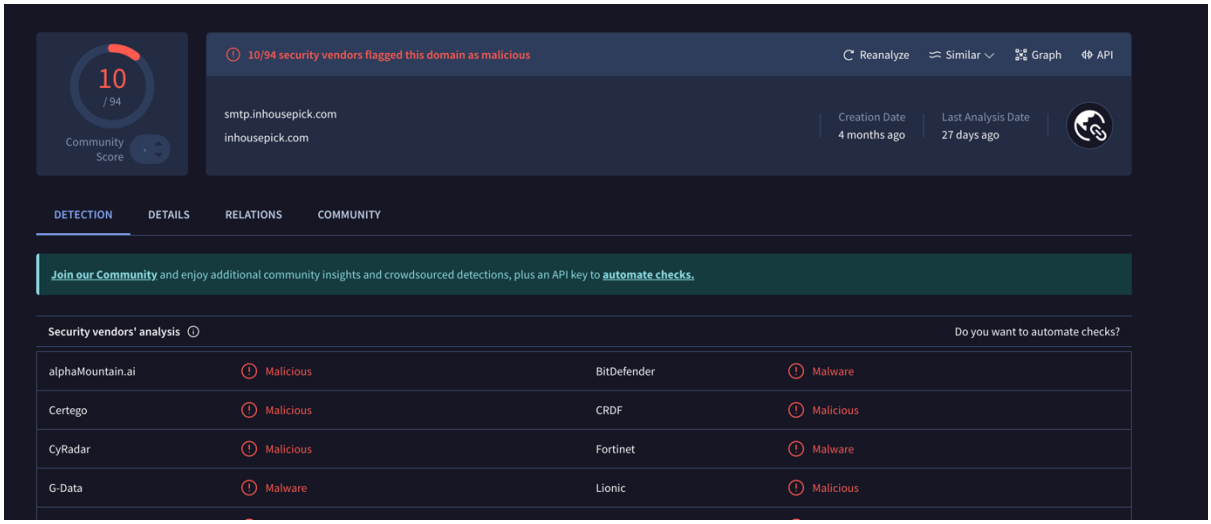
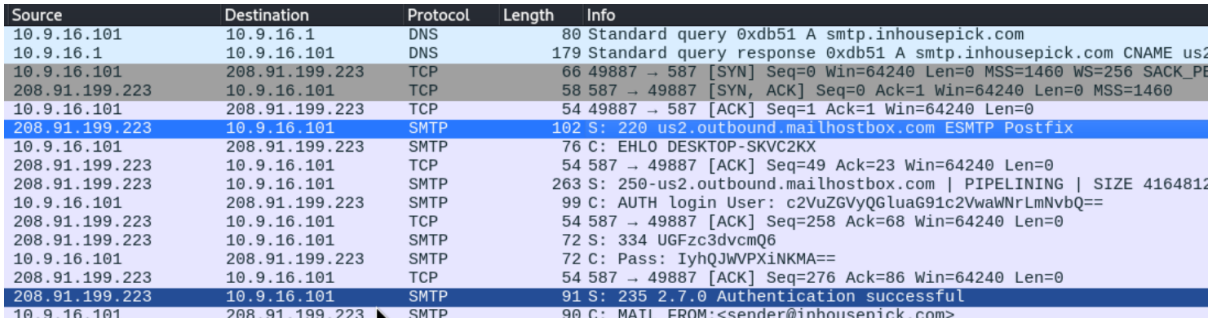


Figure 13



Source	Destination	Protocol	Length	Info
10.9.16.101	10.9.16.1	DNS	80	Standard query 0xdb51 A smtp.inhousepick.com
10.9.16.1	10.9.16.101	DNS	179	Standard query response 0xdb51 A smtp.inhousepick.com CNAME us2
10.9.16.101	208.91.199.223	TCP	66	49887 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
208.91.199.223	10.9.16.101	TCP	58	587 → 49887 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10.9.16.101	208.91.199.223	TCP	54	49887 → 587 [ACK] Seq=1 Ack=1 Win=64240 Len=0
208.91.199.223	10.9.16.101	SMTP	102	S: 220 us2.outbound.mailhostbox.com ESMTP Postfix
10.9.16.101	208.91.199.223	SMTP	76	C: EHLO DESKTOP-SKVC2KX
208.91.199.223	10.9.16.101	TCP	54	587 → 49887 [ACK] Seq=49 Ack=23 Win=64240 Len=0
208.91.199.223	10.9.16.101	SMTP	263	S: 250-us2.outbound.mailhostbox.com | PIPELINING | SIZE 416481
10.9.16.101	208.91.199.223	SMTP	99	C: AUTH login User: c2VuZGVyQGluaG91c2VwaWNrLmNvbQ==
208.91.199.223	10.9.16.101	TCP	54	587 → 49887 [ACK] Seq=258 Ack=68 Win=64240 Len=0
208.91.199.223	10.9.16.101	SMTP	72	S: 334 UGFzc3dvcmQ6
10.9.16.101	208.91.199.223	SMTP	72	C: Pass: IyhQJWVPXiNKMA==
208.91.199.223	10.9.16.101	TCP	54	587 → 49887 [ACK] Seq=276 Ack=86 Win=64240 Len=0
208.91.199.223	10.9.16.101	SMTP	91	S: 235 2.7.0 Authentication successful
10.9.16.101	208.91.199.223	SMTP	90	C: MAIL FROM:<sender@inhousepick.com>

Figure 14

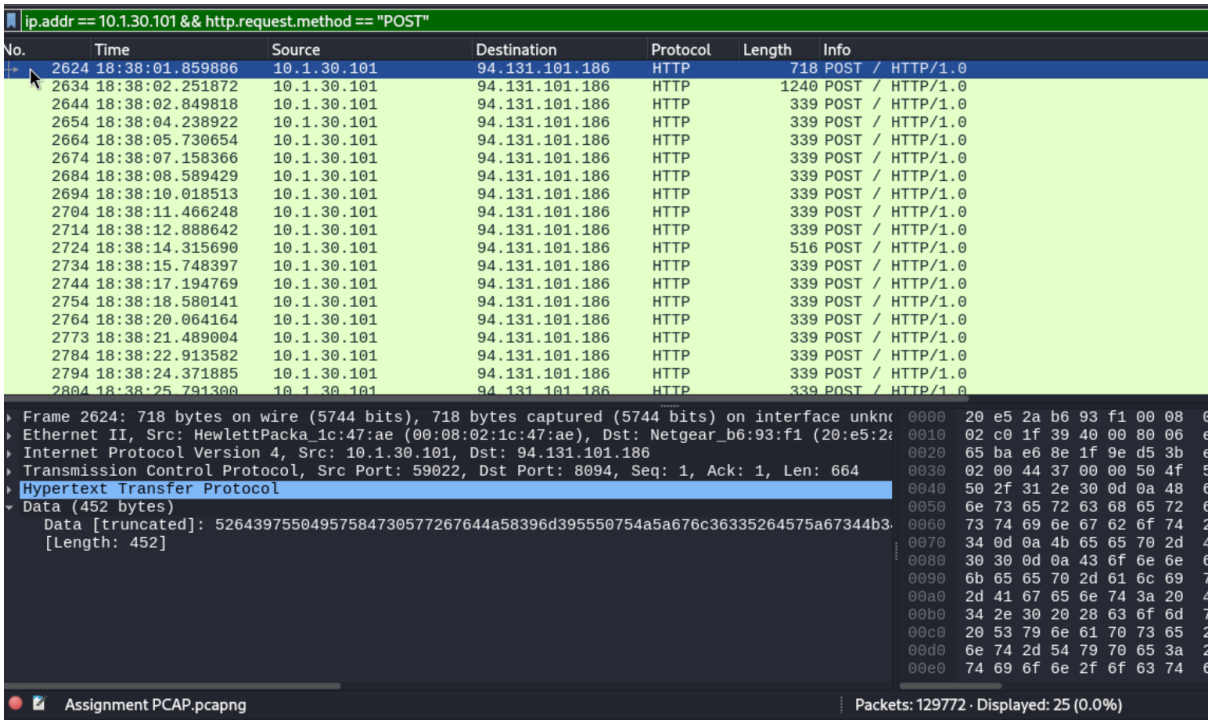


Figure 15

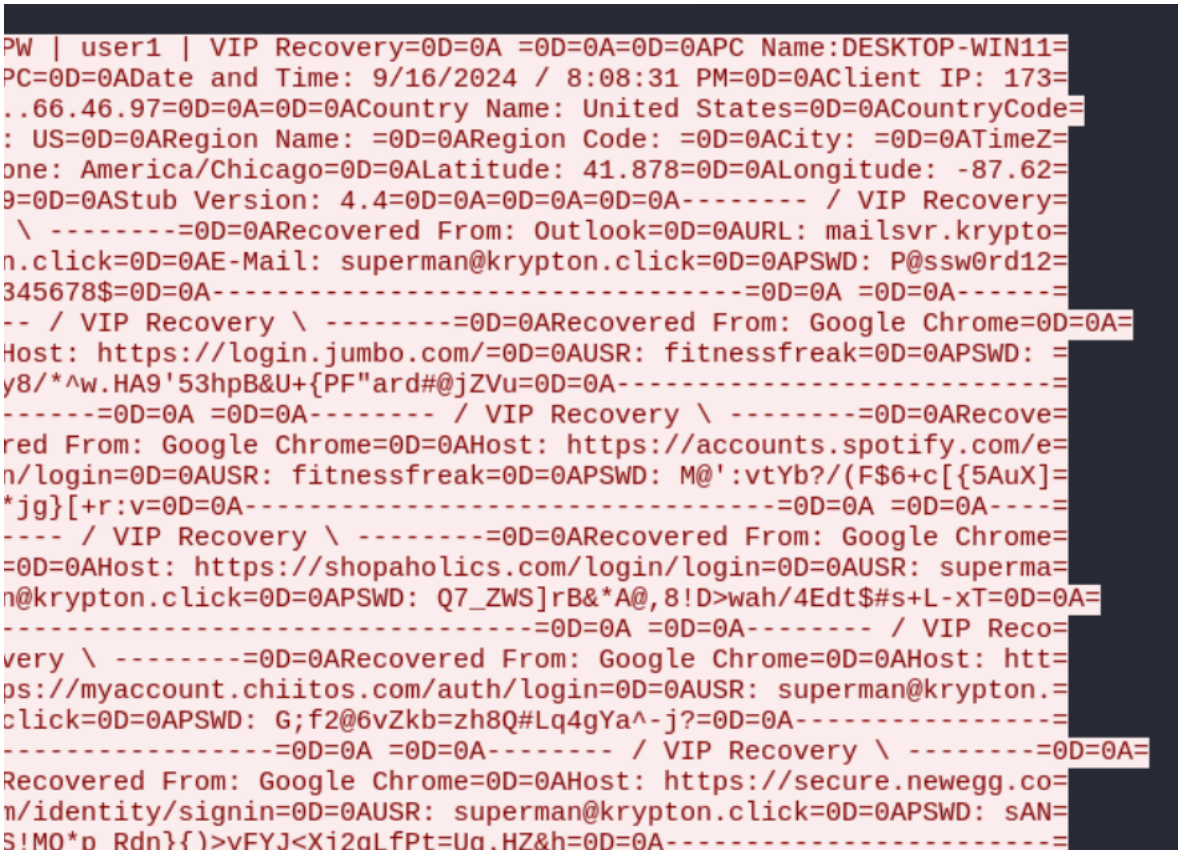
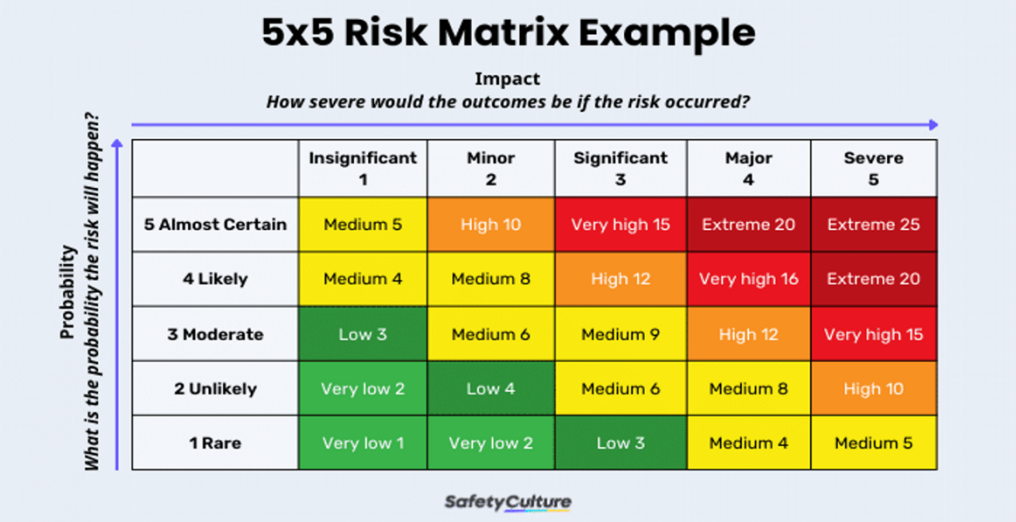


Figure 16

Appendices - Risk Assessment tables and matrices

Table A.1 — Example of consequence scale

Consequences	Description
5 – Catastrophic	**Sector or regulatory consequences beyond the organization** Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	**Disastrous consequences for the organization** Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	**Substantial consequences for the organization** High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	**Significant but limited consequences for the organization** Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).



Level of risk	Risk evaluation	Description
Low (green)	Acceptable as is	The risk can be accepted without further action.
Moderate (amber)	Tolerable under control	A follow-up in terms of risk management should be conducted and actions should be set up in the framework of continuous improvement over the medium and long term.
High (red)	Unacceptable	Measures for reducing the risk should absolutely be taken in the short-term. Otherwise, all or a portion of the activity should be refused.

Table A.10 — Examples of typical threats

Category	No.	Threat description	Type of risk source [a]
Physical threats	TP01	Fire	A, D, E
	TP02	Water	A, D, E
	TP03	Pollution, harmful radiation	A, D, E
	TP04	Major accident	A, D, E
	TP05	Explosion	A, D, E
	TP06	Dust, corrosion, freezing	A, D, E
Natural threats	TN01	Climatic phenomenon	E
	TN02	Seismic phenomenon	E
	TN03	Volcanic phenomenon	E
	TN04	Meteorological phenomenon	E
	TN05	Flood	E
	TN06	Pandemic/epidemic phenomenon	E
Infrastructure failures	TI01	Failure of a supply system	A, D
	TI02	Failure of cooling or ventilation system	A, D
	TI03	Loss of power supply	A, D, E
	TI04	Failure of a telecommunications network	A, D, E
	TI05	Failure of telecommunication equipment	A, D
	TI06	Electromagnetic radiation	A, D, E
	TI07	Thermal radiation	A, D, E
	TI08	Electromagnetic pulses	A, D, E
Technical failures	TT01	Failure of device or system	A
	TT02	Saturation of the information system	A, D
	TT03	Violation of information system maintainability	A, D
	TH01	Terror. attack, sabotage	D
	TH02	Social Engineering	D
	TH03	Interception of radiation of a device	D

[a] D = deliberate; A = accidental; E = environmental.

Table A.10 *(continued)*

Category	No.	Threat description	Type of risk source [a]
Human actions	TH04	Remote spying	D
	TH05	Eavesdropping	D
	TH06	Theft of media or documents	D
	TH07	Theft of equipment	D
	TH08	Theft of digital identity or credentials	D
	TH09	Retrieval of recycled or discarded media	D
	TH10	Disclosure of information	A, D
	TH11	Data input from untrustworthy sources	A, D
	TH12	Tampering with hardware	D
	TH13	Tampering with software	A, D
	TH14	Drive-by-exploits using web-based communication	D
	TH15	Replay attack, man-in-the-middle attack	D
	TH16	Unauthorized processing of personal data	A, D
	TH17	Unauthorized entry to facilities	D
	TH18	Unauthorized use of devices	D
	TH19	Incorrect use of devices	A, D
	TH20	Damaging devices or media	A, D
	TH21	Fraudulent copying of software	D
	TH22	Use of counterfeit or copied software	A, D
	TH23	Corruption of data	D
	TH24	Illegal processing of data	D
	TH25	Sending or distributing of malware	A, D, R
	TH26	Position detection	D
Compromise of functions or services	TC01	Error in use	A
	TC02	Abuse of rights or permissions	A, D
	TC03	Forging of rights or permissions	D
	TC04	Denial of actions	D
Organizational threats	TO01	Lack of staff	A, E
	TO02	Lack of resources	A, E
	TO03	Failure of service providers	A, E
	TO04	Violation of laws or regulations	A, D

[a] D = deliberate; A = accidental; E = environmental.

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
Personnel	VP01	Absence of personnel
	VP02	Inadequate recruitment procedures
	VP03	Insufficient security training
	VP04	Incorrect use of software and hardware
	VP05	Poor security awareness
	VP06	Insufficient or lack of monitoring mechanisms
	VP07	Unsupervised work by outside or cleaning staff
	VP08	Ineffective or lack of policies for the correct use of telecommunications media and messaging
Site	VS01	Inadequate or careless use of physical access control to buildings and rooms
	VS02	Location in an area susceptible to flood
	VS03	Unstable power grid
	VS04	Insufficient physical protection of the building, doors and windows
Organization	VO01	Formal procedure for user registration and de-registration not developed, or its implementation is ineffective
	VO02	Formal process for access right review (supervision) not developed, or its implementation is ineffective
	VO03	Insufficient provisions (concerning security) in contracts with customers and/or third parties
	VO04	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
	VO05	Audits (supervision) not conducted on a regular basis
	VO06	Procedures of risk identification and assessment not developed, or its implementation is ineffective
	VO07	Insufficient or lack of fault reports recorded in administrator and operator logs
	VO08	Inadequate service maintenance response
	VO09	Insufficient or lack of Service Level Agreement
	VO10	Change control procedure not developed, or its implementation is ineffective
	VO11	Formal procedure for ISMS documentation control not developed, or its implementation is ineffective
	VO12	Formal procedure for ISMS record supervision not developed, or its implementation is ineffective
	VO13	Formal process for authorization of publicly available information not developed, or its implementation is ineffective
	VO14	Improper allocation of information security responsibilities
	VO15	Continuity plans do not exist, or are incomplete, or are outdated
	VO16	E-mail usage policy not developed, or its implementation is ineffective
	VO17	Procedures for introducing software into operational systems not developed, or their implementation is ineffective
	VO18	Procedures for classified information handling not developed, or their implementation is ineffective
	VO19	Information security responsibilities are not present in job descriptions
	VO20	Insufficient or lack of provisions (concerning information security) in contracts with employees
	VO21	Disciplinary process in case of information security incident not defined, or not functioning properly
	VO22	Formal policy on mobile computer usage not developed, or its implementation is ineffective

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
	V023	Insufficient control of off-premise assets
	V034	Insufficient or lack of "clear desk and clear screen" policy
	V025	information processing facilities authorization not implemented or not functioning properly
	V026	Monitoring mechanisms for security breaches not properly implemented
	V027	Procedures for reporting security weaknesses not developed, or their implementation is ineffective
	V028	Procedures of provisions compliance with intellectual rights not developed, or their implementation is ineffective

Table A.2 — Example of likelihood scale

Likelihood	Description
5 – Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.