SAFETECH INNOVATIONS

Critical Incident Response Case Study: STI CERT ® Response to a Ransomware Attack

Critical Incident Response Case Study: STI CERT ® Response to a Ransomware Attack

In a context where cyberattacks are becoming more sophisticated and frequent, a recent incident at a Romanian company demonstrated the importance of a quick and coordinated reaction to a ransomware threat. The prompt intervention of the emergency-activated Safetech Innovations Computer Emergency Response Team (STI CERT ®) played a key role in limiting the impact and quickly restoring the organization's critical operations, highlighting the importance of partnering with an advanced cybersecurity service provider and using modern detection and response mechanisms.

Introduction – Why Ransomware Protection Should Be a Priority in 2025

In 2025, ransomware attacks remain one of the biggest threats to organizations, regardless of size. According to the report of the European Union Agency for Cybersecurity **"ENISA Threat Landscape 2024",** at European level, the most targeted sectors are manufacturing, retail, digital service providers, services, financial-banking, education, transport, public administration and energy. Attackers are using increasingly sophisticated tactics, including exploiting zero-day vulnerabilities, manipulating the software supply chain, and fileless techniques to circumvent traditional security solutions. The same ENISA report shows that LockBit, Cl0p and PLAY are among the most used ransomware variants in RaaS (Ransomware-as-a-Service) and extortion attacks, with LockBit responsible for almost half of the incidents reported in 2024.

This year also saw the largest ransom payment in the history of ransomware attacks: $75 million was extorted from a single Fortune 50 company, setting a new global record. But the costs associated with a ransomware incident aren't just financial. Disruption of critical operations, data loss, reputational damage, and regulatory sanctions can jeopardize a company's long-term viability. Therefore, anti-ransomware protection must be an integral part of a proactive cybersecurity strategy, supported by modern technologies and rapid incident response capabilities.

Context of the attack and initial causes

In a cyber incident in 2025, Safetech Innovations' CERT team was activated as a matter of urgency to manage an ongoing ransomware attack. The target was a Romanian company, with about 500 employees, whose IT systems were compromised.
Primary investigations and traffic packet analysis revealed that the initial access vector involved downloading a first-stage payload from a previously compromised .ro domain. The domain in question had a positive reputation in VirusTotal, which made it possible to avoid detection in the early stages of the attack through the reputation solutions implemented at the gateway level.

Alerting & Reaction

The company, which did not have a contract with Safetech Innovations, asked for emergency help while the ransomware attack was ongoing. The full activation of the STI CERT response team took place in less than 45 minutes from the incident being reported, with the immediate involvement of security analysts, both remote and onsite.

Benefiting from standardized internal procedures and experience in similar incidents, the CERT STI team carried out the preliminary analysis in less than four hours. At the same time, triage, containment and emergency implementation of an EDR (Endpoint Detection and Response) solution were immediately started. The attack in question had failed to compromise the entire IT infrastructure of the client and, in this case, STI CERT applied the Cynet EDR platform on the functional endpoints, in order to use its unified coverage capabilities (endpoint, network, user) and automated remediation mechanisms. The implementation on critical equipment was completed in a few hours, thus ensuring rapid operational coverage.

Cynet EDR 360 for proactive security and automated response

Cynet EDR 360 is an advanced Endpoint Detection and Response / Extended Detection and Response platform that offers extensive threat detection capabilities and alerting, investigation and response functions, organized in automated flows. The platform integrates Next Generation Antivirus (NGAV) technologies for the automatic prevention, detection and blocking of malware, exploits, macros, malicious scripts, fileless attacks or ransomware. It also includes User Behavioral Analytics (UBA) functionalities, essential for detecting and preventing attacks involving the use of compromised credentials.

Cynet 360 also integrates advanced security breach simulation technologies, as well as powerful investigation and validation tools, which allow the filtering and analysis of the historical data collected, based on multiple search criteria. At the same time, it ensures the orchestration and automation of response actions, through configurable playbooks with predefined remedial measures.

Immediately after installation, Cynet agents quickly gave us visibility into the environment, helped us identify the infection vector and block the spread – suspicious files and malicious scripts were detected running on one of the already affected stations. These include an obfuscated PowerShell script, responsible for executing a fileless payload that activates the ransomware. This information was critical for conducting the forensic analysis and completing the post-incident investigation.

Technical analysis and operational response

Security analysts from STI CERT conducted a comprehensive forensic analysis, identifying how attackers exploited Group Policy Object (GPO) policies for lateral propagation and implementation of a persistence mechanism. They introduced a registry key that ensured the automatic, continuous execution of malicious code when rebooting the affected systems. Relevant digital artifacts were collected and analysed and Indicators of Compromise (IoCs) of major importance were extracted. Based on this data, customized containment and remediation measures could be applied, stopping the spread of ransomware at an early stage and protecting the rest of the infrastructure.

Following the analysis of the observed behavior of the attacks and the tactics, techniques and procedures (TTPs) used, correlated with the MITRE ATT&CK matrix, the team made a probable attribution of the attack to a cyber group known for ransomware attacks in this region. The operational patterns detected, including the use of specific tools, were documented as part of a final incident report, delivered by the STI CERT team.

Recovery and reinforcement of the security posture

After removing the threat, the CERT STI team conducted a full compromise assessment to determine how extensive the impact was, clearly define the vulnerable surface, and check if there were any other hidden backdoors or control mechanisms.

Based on the findings, multiple customized remediation measures were implemented, which made it possible to quickly restore the affected equipment and resume business activities in a minimum amount of time, significantly reducing the operational impact of the incident. Simultaneously, in accordance with the current regulations, the customer notified the competent authorities.

By correlating and analyzing the evidence collected during the investigation, Safetech highlighted an operational pattern specific to the identified actor, which reinforced the conclusions and allowed the outlining of protection mechanisms. Also, the extracted Indicators of Compromise (IoCs) have been integrated into a proactive alerting playbook, which allows monitoring the customer's infrastructure and blocking other subsequent intrusion attempts.

Comprehensive protection and rapid response through Safetech SOC as a Service (SOCaaS)

- Safetech Innovations offers **Security Operations Center (SOC) outsourcing services** through its STI CERT center – the first private Computer Emergency Response Team in Romania, accredited as a Trusted Introducer. It provides onboarding, proactive asset discovery, vulnerability assessment, event monitoring, incident detection, advanced analytics, and 24-hour incident response.

- Currently, STI CERT receives, on average, 100 billion events per month, analyzes 25,000 security alerts per month and handles 180 security incidents per month, serving customers in various sectors, such as financial-banking, utilities, healthcare, technology, retail, distribution, consulting and gaming.

Conclusion

The global climate marked by increasingly sophisticated cyberattacks is also reflected in Romania, where more and more companies are recording significant financial and image damage as a result of ransomware attacks. Incidents generate the exfiltration of tens of gigabytes of data: email addresses, contracts, invoices, source code, and even personal information about customers and employees.
In this context, the incident presented validates the importance of a coordinated, rapid and technologically supported response in the management of cyberattacks. The success of the intervention was possible thanks to a combination of:

- prompt intervention,
- strong forensic investigation capabilities,
- the use of a high-performance EDR solution,
- operational experience in similar incidents.

The incident also demonstrates the importance of a partnership with an advanced cybersecurity service provider, capable of ensuring not only rapid detection and real-time response, but also effective remediation and continuous hardening of the security infrastructure.

With the rapid involvement of the STI CERT team, damage was limited, extensive data loss was prevented, and the customer's IT infrastructure was significantly strengthened to cope with future threats. Such interventions validate the need for continuous investments in modern EDR/XDR solutions, specialized services and practice-tested response procedures.

In 2025, cyber resilience is based on anticipation, integrated technology, and teams ready to react professionally at all times. The response of the STI CERT team limited the spread of ransomware and allowed the organization to avoid a major crisis.

For technical and commercial information regarding Safetech Innovations services, we invite you to visit **the services section of the company's website**. For any details, do not hesitate to contact us at email sales@safetech.ro.

Since 2011, Safetech Innovations S.A. has been providing cybersecurity services and solutions tailored to the needs of each organization. Throughout its history, the company has specialized in the integration of complex cybersecurity projects and critical infrastructure security services. The company's main areas of expertise are:

- Outsourcing operations for monitoring and responding to cybersecurity incidents,
- Providing and implementing technical solutions for cybersecurity risk management,
- Consultancy for risk management and compliance with applicable security regulations,
- Securing critical IT and OT infrastructures,
- Cybersecurity training,
- Security testing and auditing,
- Information security and risk management.

Safetech Innovations holds a market leader position in Romania in the segment of cybersecurity services provided by local companies. Safetech has also been included in the prestigious Top 250 MSSP 2024 and 2025, which recognizes the top 250 Managed Security Service Providers globally.

Safetech Innovations has partnerships with a number of companies with a decisive role in the field of cybersecurity, such as CheckPoint, Cynet, DarkTrace, HID, Microsoft, Splunk, Stellar Cyber, Palo Alto, Picus Security.

Currently having over 70 employees, the company has dedicated teams for the research and development of cybersecurity software products, the implementation and support of security solutions and the Computer Emergency Response Team (CERT). Safetech's Security Operations Center has been serving customers since 2015 and provides them with a mature and efficient cyber threat detection, response and remediation capability, with 24/7/365 coverage. Currently, STI CERT investigates an average of 25,000 security alerts/month and contributes to the security of more than 80,000 employees.

The company has customers in the fields of utilities, healthcare, insurance, industrial manufacturing, retail and the public sector. Also, seven of the ten largest banks in Romania have chosen Safetech as a cybersecurity service provider. Safetech Innovations has been involved in more than a hundred critical infrastructure security projects in the United States, Canada, Brazil, Morocco, the European Union, Singapore, the Philippines, India, China, and New Zealand. Safetech Innovations S.A. is listed on BVB (BSE: SAFE) and has points of presence in the UK and the United Arab Emirates.

SAFETECH INNOVATIONS

APPLIED CYBER INTELLIGENCE

12-14 Frunzei Street, Floors 1-3, District 2, 021533 Bucharest, Romania
+40 21 3160565 | sales@safetech.ro
www.safetech.ro