INCIDENT RESPONSE CONSULTING
POWERED BY CHRONOS

CASE STUDY

Leveraging its proprietary Chronos platform, CSIS delivers best-in-class Incident Response services and minimizes damage caused by a major ransomware attack.

Executive Summary

A large multinational IT company, headquartered in Denmark, was hit by a ransomware attack that generated costs of DKK 20 million (c. EUR 2.7 million).

This case study explains how the CSIS Incident Response (IR) team ran an investigation and remediation process lasting a mere 4 weeks, resulting in the complete restoration of our customer's business-critical services, by leveraging Chronos, the most powerful incident response and cyber investigations platform.

The Attack

CSIS was contacted through our 24/7 emergency assistance line and the IT company reported that none of its systems were responsive. Understanding the gravity of the situation, a team of CSIS IR consultants was dispatched for on-site intervention immediately.

An initial 'situation meeting' led to the conclusion that, in order to stem the mounting financial losses, top management should instruct all non-essential activities to be halted, so that most employees and consultants could be sent home.

Immediately, the IR team turned its attention to the investigation and the three key questions that must be answered in any incident to ensure a thorough remediation process that will also minimize the probability of a repeat of the same incident:

1. How did the incident happen? This is about finding the infection vector and tracing the attacker's every action.

2. What data was stolen? Answering this question helps take appropriate and well-informed GDPR actions, including necessary notifications and public statements.

3. When did the attack happen? It is often found that attackers have had access to the network for longer than originally thought; an oversight of this type can end up leaving back-doors open, can cause unforeseen complications and can increase the response timeline.

"An incident leaves no choice. We must find out how it happened. The main reason why Chronos exists is to fill a gap where security monitoring is insufficient."

- Ian Qvist
Principal Consultant &
Incident Response Techlead
CSIS Security Group

"Chronos has the capability to analyze data for different purposes. It can be used as an investigation tool for incidents, which is its primary function. But it can also be configured to, for example, identify missing security policies and the state of security solutions, which gives a compliance-friendly view of the network."

- Ian Qvist
Principal Consultant &
Incident Response Techlead
CSIS Security Group

Chronos Deployment

Chronos is a crucial part of our IR team's methodology.

"Chronos has an unparalleled attention to detail and provides insight into an attacker's actions faster than any other platform. Case search, intelligence, timeline and a full featured analysis at my fingertips help to quickly provide answers to our customers' questions."

- Michael Bisbjerg
Senior Consultant & Incident Responder
CSIS Security Group

Once deployed, Chronos provided a total overview of the attacker's malicious activity on all machines in the network. Chronos is a very fast and easy to deploy application that collects up to 350 artefacts, those being the tiny remnants from malicious actions that provide essential hints of what happened during the breach. Such breadth and depth of visibility permits rapid detection and surgical yet comprehensive removal of the malware from the network. Moreover, a key benefit of using Chronos is that, while commonly-used security monitoring tools will miss any indicators of compromise that predate the tool's installation, Chronos does not suffer this blind spot, as it will gather all historical data related to activities on the computer.

Data collected and put through Chronos' automated analyzers allowed the IR team to discover that the attacker had compromised a machine on one of our customer's networks through a remote desktop vulnerability, enabling remote code execution on a server. The criminal escalated its privileges to first become a domain administrator on a local system and, subsequently, to global domain administrator, ultimately aiming to gain access to our customer's financial database.

Moreover, it was detected that shortly after the breach, the attacker initiated the deployment of ransomware across the backup server, afterwards logging into a domain controller and deploying the ransomware to all servers and all clients.

"Since Chronos gives us a complete insight into a computer's security configuration, we can use it to design a good security baseline that will protect the customer against future attacks."

- Ian Qvist
Principal Consultant & Incident Response Techlead
CSIS Security Group

Speed and effectiveness were, therefore, the most critical challenges in this investigation. Based on insights generated by Chronos, the IR team was able to start targeting and patching affected systems to stop the infection permanently. As part of the investigation, the team looked for stolen data, signs of backdoors and any exploited vulnerabilities. As soon as the infection was stopped, our customer could initiate the recovery process.

Once our customer's business-critical services were up and running again, they proceeded to harden their security level to prevent similar attacks in the future. Following our IR team's recommendations, our customer deployed various security solutions and installed an EDR system on all machines.

The Result

Normally, a case like this one could take around 8 weeks. The combined strengths of our IR team's investigation expertise and the capabilities of the Chronos platform enabled a much faster turnaround time.

Notably, though our team set out to answer the three core questions of an investigation, namely the how, what and when, they were also able to ascertain the who, i.e.: the identity of the threat actor. With this insight, we were able to enrich our understanding of the attacker's tactics and methods, which further strengthened the incident handling process.