PERFORMANTA

Case study

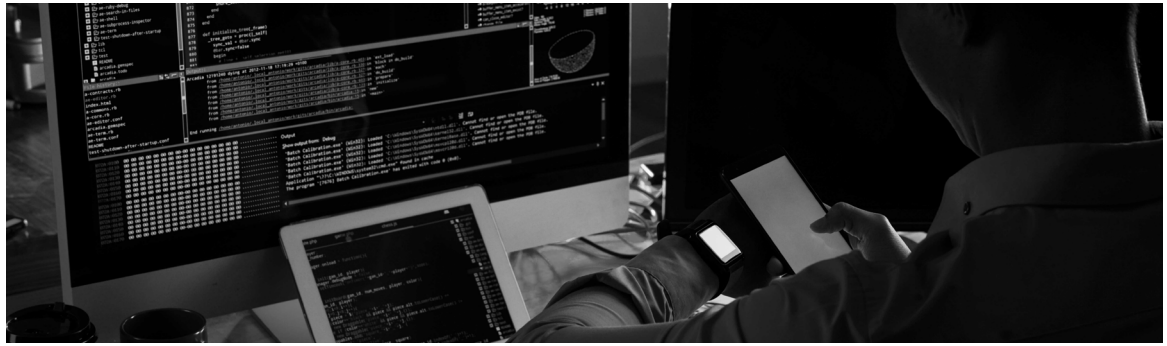
Recovering from a Ransomware Attack

Leading Regional Telecoms company

Incident Response (IR)

Overview

- A large regional telecoms company detected an advanced ransomware attack crippling its systems.
- They needed to contain the attack and enlisted Performanta's incident response (IR) experts.
- Our IR team worked with our client to contain and investigate the attack, then set actions in motion without alerting the attackers and giving them a chance to react.
- Using best practices tailored to our client's unique environment, we contain and investigate, audit systems, harden detection and response, systematically remove the attackers, and take back the environment.
- The Performanta Safe Platform improved our client's controls to achieve 98.5 percent coverage and 98.6 percent compliance, and we transitioned them into a continuous 24x7 managed detection & response (MDR) service.
- Performanta and our client developed improved response plans to manage potential future incidents. Our client has not experienced any further attacks of this magnitude since.



Executive Summary

Ransomware are blunt but highly effective attacks that encrypt a company's data and demand payment to reverse the encryption. Criminals use tactics such as phishing to fool key employees into deploying malware that rapidly encrypts important data, causing big system outages and stopping operations. Ransomware attacks are covert and can spread very quickly. This was the experience of our client, a large regional telecommunications company. Even though their security operations centre (SOC) detected the attack, it was too late, and they needed help to contain and recover.

This help arrived in the form of Incident Response (IR), a specialised skill set that contains and investigates breaches, then sets countermeasures and cleanups into action. IR is a deeply technical capability that forensically scours data such as alerts and incident reports, then plans and executes how to contain the attack without alerting the attackers and giving them time to change tact. Once contained, the attack is nullified, and the attackers are removed as part of the 'take back' phase.

While companies can mitigate ransomware attacks through disaster recovery, these are not foolproof, nor do they remove the attack. In this case, the disaster recovery was partially successful, but the attackers had compromised key systems such as Exchange and Postillion, not to mention numerous infected mailboxes. Performanta's IR experts contained these attacks and squeezed the criminals out of the systems.

Within 12 weeks, the attack was contained and nullified, and we handed the systems back to our client. Performanta implemented robust security measures, including Endpoint Detection and Response (EDR) and Privileged Access Management (PAM). Performanta Safe Platform improved our client's controls to achieve 98.5 percent coverage and 98.6 percent compliance. We additionally developed improved response plans to manage potential future incidents and transitioned our client into a continuous 24x7 managed detection & response (MDR) service. Since then, they have detected and stopped such attacks and have not suffered a major breach event.

The Challenge

Our client, a large telecommunications enterprise, detected a fast-spreading ransomware attack in progress. Ransomware can bring operations to a halt, and the client was experiencing major outages across key systems. Specifically, the attackers had infiltrated the client's Exchange and Postillion systems.

Our client had disaster recovery (DR) sites and could create limited operational recovery. But the DR sites' security also fell short. It was critical to contain the attack, limit its damage, and start to remove the attackers before they could deploy countermeasures. To achieve these goals, our client needed access to incident response professionals.

This situation is very delicate: the attack must be stopped and reversed without prematurely alerting the attackers.

The Solution

Incident response is a niche ability that involves extensive forensics, data inspection, and response planning. Performanta specialises in IR; our IR specialists jumped into action when the client recruited our help. Though every IR scenario is unique, we activated best practices to contain such an attack: contain and investigate, audit systems, harden detection and response, systematically remove the attackers, and take back the environment for handover to the client.

Over twelve weeks, Performanta's IR teams worked with our client to contain the attack without alerting the attackers and quickly restore operations. We implemented robust security measures, including Endpoint Detection and Response (EDR), Privileged Access Management (PAM), Firewalls, Intrusion Prevention Systems (IPS) and Managed Detection and Response. We additionally developed improved response plans to manage potential future incidents.

The Results

Late detection of an attack is better than not discovering it at all. Even though this ransomware attack caused extensive problems, including downed systems, reputational damage and financial losses, it could have been much worse. Without an effective incident response, the damage can linger, making ongoing and future attacks much more likely. Yet, since IR skills are considerably rare and expensive, most large companies don't have them in-house.

Our client could rely on our quick and focused response. Within twelve weeks, Performanta contained the attack, removed the attackers, took back the environment and put our client back in control. Using the Performanta Safe Platform, we improved our client's controls to achieve 98.5 percent coverage and 98.6 percent compliance. We also helped harden the security of their disaster recovery sites, develop new incident response plans, and transition them into a continuous 24x7 managed detection & response (MDR) service. They have not experienced any further attacks of this magnitude since.

PERFORMANTA

www.performanta.com