CASE STUDY

Kroll Ontrack helps global pharmaceutical restore 400 virtual disks following cyberattack by disgruntled employee.

Major drug company faced hacked IT systems that threatened supply of vital medication and prescriptions.

THE CLIENT

A leading pharmaceutical lost access to all of its data following a malicious cyber-attack by an ex-employee.

THE SITUATION

The customer was in the process of acquiring another company, which had most of its systems virtualised. When the company's users left the office on Friday all of the systems were operational and when they came in Monday morning the users were not able to access the virtual machines.

The client contacted the HP and VMware support teams and after an initial investigation discovered that the virtual machines and their snapshots had been deleted from the source volumes. The volumes containing the backups had been initialised - overwriting the backup files.

The customer was then referred to Kroll Ontrack for data recovery.

THE SOLUTION

The company suspected foul play so the Kroll security team was dispatched to the customer location to begin an investigation during the data recovery. The security team locked down the data centre and installed monitoring systems, then started a full investigation into the suspected breach. Kroll Background Screening was also brought in to do a background check on suspected individuals.

The team soon determined that an individual had logged into a system from outside the company and then connected to a series of systems. Once the individual reached the VMware server, the individual intentionally and maliciously deleted the virtual disks and backups. This individual was able to access 27 out of the 28 logical unit numbers (LUNs).

The customer had an initial consultation with Kroll Ontrack and was offered a Remote Data Recovery solution. They connected multiple machines and upon connection, Kroll Ontrack teams were assigned to perform an evaluation of the LUNs provided. The Kroll Ontrack engineers confirmed that the data had been deleted from the volume. They then proceeded to identify all of the recoverable data on each LUN and provided the customer with reports detailing the data.

The evaluation was very challenging as the client had limited documentation, unknown virtual machine names, unknown content on the virtual disks and unknown operating systems. They also did not have a disaster recovery plan in place for this system, so it had changing priorities during the evaluation.

Having identified the sheer scale of the problem, which meant that the company was prevented from delivering vital prescriptions and other medical supplies, Kroll Ontrack constructed a virtual team based on resources from eight data recovery centres around the world. Upon review of the provided reports and approval from the customer, the Kroll Ontrack teams extracted the deleted data and as needed extracted the contents of corrupted virtual disks to new storage provided by the customer.

THE OUTCOME

The lead system administrator from the smaller company left his employment before talks of the merger happened – taking all of the system information with him. The company was forced to rehire him as a contractor to perform a knowledge share with the remaining employees.

During the time he was a contract employee, the lead administrator set up a rogue vCenter on the company's network without the knowledge of any of the other employees. He then finished his contract and left the company without incident. Shortly after he left the company for the second time, the business went through a merger with a larger pharmaceutical. During the merger, some employees were laid off including the lead administrator's friend.

During the Kroll security investigation, investigators found an unauthorised entry from outside the network in one of the router logs. The entry led them to the rogue vCenter and from there, after working with VMware support, they determined that it was the system used to delete all of the virtual disks and their snapshots.

The Kroll team then contacted the FBI and working with their team, they were able to determine that the external IP address belonged to AT&T. The FBI contacted AT&T and learned that the IP address was registered to a McDonalds. The FBI sent field agents to the McDonalds and found evidence that one of their suspects had been there the day the incident occurred. Once the field agents had the evidence, they confronted the suspect and he confessed to the crime.

From written accounts and court records, the team learned that the lead administrator decided to get revenge for the layoff of his friend and teach the smaller company a lesson. One Sunday morning, he got in his car, drove to the McDonalds in question, purchased breakfast with his credit card and then logged into the public WiFi. From there he made a connection to the rogue vCenter and proceeded to delete all of the virtual machines as well as the backups.

THE RESOLUTION

Kroll Ontrack was able to successfully recover all of the critical virtual machines and provided that data to the customer in a timely fashion. Total recovery time was approximately three weeks.

The defendant (lead engineer) was sentenced to 41 months in federal prison and fined $812,000.

CONTACT

For more information, call or visit us online:
+44 (0)20 3627 2118 | krollontrack.co.uk
+353 (0)1 960 9265 | ontrackdatarecovery.ie

Kroll Ontrack®

Copyright © 2016 Kroll Ontrack LLC. All Rights Reserved. Kroll Ontrack, Ontrack and other Kroll Ontrack brand and product names referred to herein are trade marks or registered trade marks of Kroll Ontrack LLC. and/or its parent company, Kroll LLC., in the United States and/or other countries. All other brand and product names are trade marks or registered trade marks of their respective owners.