DCIG

HYCU | Customer Validation

An Anatomy of Responding to and Surviving a Ransomware Attack

By Jerome M Wendt, DCIG President & Founder

A COO for a large, professional services firm found out just how insidious ransomware has become. The firm did backups. It had a viable DR strategy. Still ransomware infested his firm and almost crippled it. Only through his firm's use of HYCU and the efforts of HYCU's support team did his firm recover from this nearly devastating ransomware attack.

COMPANY

Professional Services Firm

CHALLENGES

- Ransomware attack took place in two stages.
- Data on all PCs, servers, and network filers was encrypted.
- Encrypted data was replicated to DR site preventing remote recovery.
- Backup files stored on network filers was also encrypted.

SOLUTION

HYCU for Nutanix

DIFFERENTIATORS

- HYCU hosted on Linux CentOS VM makes it less susceptible to ransomware.
- HYCU created local file on its VM that was immune from ransomware attack.
- HYCU's worldwide support team supports issues such as ransomware attacks.
- HYCU worked with firm to recover firm's VM in less than 36 hours.

The Setup

The Chief Operating Officer (COO) thought his large professional services firm was prepared to respond to any type of attack, including a ransomware attack. He had worked at the firm for 20+ years and had a solid grasp on its IT environment, including its backup strategy and disaster preparedness.

Based in the southeastern United States, the firm ran on Nutanix Enterprise Cloud platform. It hosted most of its applications on Nutanix and supported more than 50 servers, 10+ million files, and 30+ TB of data. Focused on the medical field, it also stored many records subject to HIPAA regulations.

To protect these data and applications, the firm took a two-fold approach. On the front end, it used cybersecurity software to detect and prevent ransomware attacks. For backups, it used HYCU for Nutanix doing daily, incremental backups and full weekly backups.

The firm also replicated all its data to a second data center located more than 100 miles away. This architecture ensured the firm could quickly failover and recover both locally and remotely. Little did the COO realize how well ransomware could penetrate these defenses and even use them against him.

The Warning Signs

The ransomware attack on the firm displayed few early warning signs until it detonated. Alerts first showed up in its logs the Friday before the attack started. The cybersecurity software the firm had in place showed signs of suspicious activity. However, none of these alerts were raised to the level that it caught anyone's attention or prompted a response.

Later investigations later revealed the attack's root cause. A Word file attached to an email entered the firm. Embedded in it was a macro. This Word file, when opened, introduced the RYUK malware virus into the environment that started a two-pronged attack.

The first phase of the attack spread the malware throughout the company's network by infesting file and Windows servers. This infestation planted an executable that detonated during the second phase. The original virus then deleted itself. This made it difficult to later diagnose the source of the attack and helped hide the virus' origins and identity.

All Hell Breaks Loose … on a Sunday

The COO's world began to become undone around 11 a.m. on a Sunday morning as the RYUK virus sprung to life. While no one was in the office it executed assuming the same security permissions as the user on each device. This gave the virus broad access to that system's resources as well as the network.

> ***"The ransomware attack left only one readable file. This included a link to the hacker's email address to negotiate a ransom payment."***

The attack continued by detecting and encrypting the network-attached and locally attached drives that it could access. It then encrypted all the files and data on the local server or PC. On each infected device, that ransomware only left one readable file: an HTML file. This file included a link to the hacker's email address that the victim could contact to negotiate a ransom payment.

No Good Path Forward

By the time the COO's pager went off, it already appeared too late. All the Windows PCs, laptops, servers and network files were encrypted. Aggravating the situation, the processes the firm had in place replicated encrypted data to its DR site. This prevented the firm from performing a remote recovery.

Then, to add insult to injury, the ransomware encrypted all the backup files stored on shared network drives. Despite feeling increasingly hopeless, the COO explored the only four paths available to him.

"Further investigation revealed the contractor who bid to help decrypt the data may well be a front for the hackers who encrypted his data."

1. He contacted the hacker's email address with his own anonymous email address to ascertain the requested ransom amount.
2. He checked his backup tapes to determine what, if any, data he could recover.
3. He engaged a contractor that claimed to assist companies recover from ransomware by helping to decrypt their data.
4. He contacted his backup provider, HYCU, to see if it could help his firm recover its data.

Paths to Nowhere

The feedback on the first three paths confirmed his worst fears. The hackers responded to his email with a ransom request of 92 bitcoins (approximately $1M US dollars.) While the COO was almost prepared to pay something, $1M was not an option.

The backup tapes offered some hope, but not much. The firm only kept about 60% of its data backed up to tape, which it only did monthly. Further, it would take weeks to recover the data from tape and reconstruct the applications. The COO viewed using tape as a source for recovery only as a last resort with little confidence it would work if used.

The decryption contractor provided no comfort and raised some red flags. Minimally it charged $10,000 to decrypt the data assuming its decryption software worked. However, further investigation revealed the contractor may well be a front for the hackers who encrypted his data. So, he dismissed this as an option.

HYCU: The First Glimmer of Hope

The first glimmer of hope came late Sunday when his team found an unencrypted file on the HYCU VM. The ransomware had encrypted all the backups stored on the network filers. However, HYCU kept a single system-generated file residing on its host VM that the ransomware had neither infected nor encrypted.

The COO and his team contacted HYCU shortly after detecting this unencrypted file. They wanted to find out if there was any way they could use this file for recovery.

A Hard Day's Night

Once contacted, the HYCU support team prioritized the issue. The challenge was the file stored on the HYCU VM was not initially intended nor formatted for recovery.

The HYCU backup software used this file to cache data prior to creating the backup files stored on the network server. Though unencrypted, it was unclear initially if HYCU could access and use this file for recovery.

As the HYCU support staff worked the issue, minutes turned into hours. In the background, HYCU passed the issue from support team to support team around the globe. In this way, fresh eyes always worked the problem. HYCU also pulled in members of its engineering group to diagnose the issue.

"The COO never saw the HYCU support team admit defeat. Rather, he witnessed their determination to work the problem with his team until it was resolved."

By the time Monday came around, HYCU had diagnosed and resolved the issue. HYCU managed to unpack this file, access the data in it, and restore all the firm's VMs.

Eternally Grateful

The COO could not begin to express how eternally grateful he was. HYCU had pulled the proverbial rabbit out of the hat and helped to recover his firm's data. He acknowledged how vital it was that HYCU had made that file available to him for recovery. Otherwise, it would have taken months for his firm to completely recover and rebuild its IT environment.

While the firm would have survived, it would have been a significant setback. He could not even begin to put numbers to the firm's potential losses in terms of money and time.

The COO never saw the HYCU support team admit defeat. Rather, he witnessed their determination to work and live the problem with his team until it was resolved. By the time HYCU finished, the COO acknowledged, *"It was a miracle to have all our systems and data back."* ■