Harrowing Experience of a Midwestern Town Hit by Ryuk Ransomware

RANSOMWARE RECOVERY STORY

This Midwestern town may not have heard about Ryuk ransomware, but in January 2020, they learned about the malware firsthand. In a recent blog post by Crowdstrike, *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*, they defined Ryuk ransomware. WIZARD SPIDER, a sophisticated Russian-based eCrime group, created it. They've been targeting large organizations for high ransomware payments. But in January, Ryuk ransomware also struck this small town.

The Attack

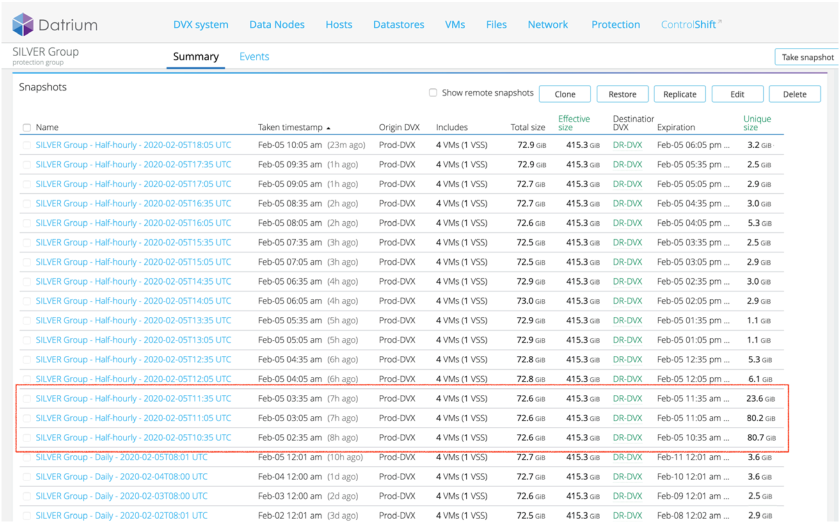
Staff members may have clicked on a link in an email, causing the infection. No one knows for sure how they first got infected, or how long the malware was dormant while the criminals waited to strike. What the IT team discovered was that one of their Azure shares was compromised. A hacker was able to access one of the domain controllers and edited a host profile to include a script installing the ransomware across the network. With the new policy in place, upon login, a startup script automatically executed, which began to encrypt all the system files. This policy was automatically pushed out to all Windows machines, both physical and VMs.

Employees were locked out of their systems – unable to access any of their files. Users received a message instructing them to send an email to a particular email address to learn how they could recover their data. The entire town was shut down, and the Governor contemplated declaring a state of emergency.

IT, Datrium, and the FBI Join Forces

The IT team quickly sprang into action to work on recovery. They built a war room, called in Datrium Support, and contacted the FBI. The FBI instructed the team to shut down everything, including the Datrium DVX system, so nothing new could be infected. This recommendation was part of the cautious approach the team took, but it isn't actually required when a customer is using Datrium DVX to recover.

The Datrium Support team quickly got involved. With built-in backup and immutable snapshots, they searched for a clean snapshot. The team looked at the change rate of data and were able to spot an anomaly in the unique snapshot size starting Monday afternoon. It looked something like the following image:



□ Name	Taken timestamp ▲	Origin DVX	Includes	Total size	Effective size	Destinatior DVX	Expiration	Unique size
□ SILVER Group - Half-hourly - 2020-02-05T18:05 UTC	Feb-05 10:05 am (23m ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 06:05 pm ...	3.2 GiB
□ SILVER Group - Half-hourly - 2020-02-05T17:35 UTC	Feb-05 09:35 am (1h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 05:35 pm ...	2.5 GiB
□ SILVER Group - Half-hourly - 2020-02-05T17:05 UTC	Feb-05 09:05 am (1h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-05 05:05 pm ...	2.9 GiB
□ SILVER Group - Half-hourly - 2020-02-05T16:35 UTC	Feb-05 08:35 am (2h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-05 04:35 pm ...	3.0 GiB
□ SILVER Group - Half-hourly - 2020-02-05T16:05 UTC	Feb-05 08:05 am (2h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 04:05 pm ...	5.3 GiB
□ SILVER Group - Half-hourly - 2020-02-05T15:35 UTC	Feb-05 07:35 am (3h ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-05 03:35 pm ...	2.5 GiB
□ SILVER Group - Half-hourly - 2020-02-05T15:05 UTC	Feb-05 07:05 am (3h ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-05 03:05 pm ...	2.9 GiB
□ SILVER Group - Half-hourly - 2020-02-05T14:35 UTC	Feb-05 06:35 am (4h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 02:35 pm ...	3.0 GiB
□ SILVER Group - Half-hourly - 2020-02-05T14:05 UTC	Feb-05 06:05 am (4h ago)	Prod-DVX	4 VMs (1 VSS)	73.0 GiB	415.3 GiB	DR-DVX	Feb-05 02:05 pm ...	2.9 GiB
□ SILVER Group - Half-hourly - 2020-02-05T13:35 UTC	Feb-05 05:35 am (5h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 01:35 pm ...	1.1 GiB
□ SILVER Group - Half-hourly - 2020-02-05T13:05 UTC	Feb-05 05:05 am (5h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 01:05 pm ...	1.1 GiB
□ SILVER Group - Half-hourly - 2020-02-05T12:35 UTC	Feb-05 04:35 am (6h ago)	Prod-DVX	4 VMs (1 VSS)	72.8 GiB	415.3 GiB	DR-DVX	Feb-05 12:35 pm ...	5.3 GiB
□ SILVER Group - Half-hourly - 2020-02-05T12:05 UTC	Feb-05 04:05 am (6h ago)	Prod-DVX	4 VMs (1 VSS)	72.8 GiB	415.3 GiB	DR-DVX	Feb-05 12:05 pm ...	6.1 GiB
□ SILVER Group - Half-hourly - 2020-02-05T11:35 UTC	Feb-05 03:35 am (7h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 11:35 am ...	23.6 GiB
□ SILVER Group - Half-hourly - 2020-02-05T11:05 UTC	Feb-05 03:05 am (7h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 11:05 am ...	80.2 GiB
□ SILVER Group - Half-hourly - 2020-02-05T10:35 UTC	Feb-05 02:35 am (8h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 10:35 am ...	80.7 GiB
□ SILVER Group - Daily - 2020-02-05T08:01 UTC	Feb-05 12:01 am (10h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-11 12:01 am ...	3.6 GiB
□ SILVER Group - Daily - 2020-02-04T08:00 UTC	Feb-04 12:00 am (1d ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-10 12:01 am ...	3.6 GiB
□ SILVER Group - Daily - 2020-02-03T08:00 UTC	Feb-03 12:00 am (2d ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-09 12:01 am ...	2.5 GiB
□ SILVER Group - Daily - 2020-02-02T08:01 UTC	Feb-02 12:01 am (3d ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-08 12:02 am ...	2.9 GiB

Ransomware Caused an Anomaly in Unique Snapshot Size

They were able to see unusually large amounts of data being created, which was caused by the Ryuk ransomware encrypting the data.

The Golden Image

The team decided to analyze the snapshots that were created on Sunday at midnight. They picked a random timestamp and powered up the system on a quarantined network. A security team verified that this snapshot did not contain the malware. The team could have continued to look at the snapshots to identify the last clear version, but they decided it was more important to begin the restoration process. This clean immutable snapshot that was taken at midnight on Sunday became the golden image.

Restoring the Environment

With Datrium DVX, the team could have done a mass update of all of their VMs to restore to this golden image, but the IT team decided to take a more cautious approach. Working with Datrium Support, they prioritized and began restoring individual VMs, each time running an antivirus scanner to confirm the ransomware had not infected them.

Within two days, they were able to restore any VM they wanted and quickly resume normal operations without paying the Ryuk ransomware criminals – thanks to the Datrium Support Team and the DVX built-in immutable snapshots.

Learn More

To learn more about how Datrium can help you recover from ransomware, visit www.datrium.com, and contact us for a demo.