# How Yuba County Survived a Ransomware Attack and Lived to Tell the Tale

### INDUSTRY

Local Government

### RESULTS

- $0 paid in ransom
- 100% of backups recovered within 7 days
- 90%+ management time savings
- Near-zero RTOs

### CHALLENGES

- Attack initiated through infected PC
- Kerberos issues behind AD servers
- ~50 PCs and 100 servers encrypted

### BUSINESS TRANSFORMATION

Yuba County not only strengthened their DR strategy with Rubrik, they survived a ransomware attack and lived to tell the tale. With Rubrik, Yuba County had peace of mind knowing that 100% of their backups were able to be recovered and they did not have to pay the ransom for their data.

### PARTNER

ePlus

Yuba County is a rural county in Northern California. Within it are various departments concerned with health and public safety including the Sheriff's office consisting of 911 dispatch for fire and ambulance. Another critical area is the health department which manages testing, contact tracing and vaccinations for COVID-19. All are vital services for the citizens of Yuba County.

Paul LaValley, former CIO for Yuba County, oversees a team of 16 people who are responsible for providing a dependable, always-on infrastructure for the community's safety and livelihood. Due in large part to the pandemic and an increased prevalence in remote work, ransomware attacks are on the rise and have become a lucrative business for cybercriminals.

"When we were hit by ransomware in February 2021, it could have been a debilitating disaster for the county; however, one of the few moments of satisfaction during weeks of discomfort was knowing that Rubrik was backing up our data and that we wouldn't have to pay the ransom for data recovery," LaValley remarked.

## DoppelPaymer, Dridex, IceID, Oh My!

Yuba County confirmed they were hit with ransomware when a DoppelPaymer ransomware note showed up on several servers and PCs. "By the time we got to it, it had encrypted roughly 50 PCs and 100 servers," LaValley described. Prior to this, there were several indications that they were compromised.

"First, we noticed there were Kerberos issues behind our active directory (AD) servers, which prevented them from communicating. Later that evening, a GPO push occurred and an enterprise AD admin account was created. We knew through forensic analysis that Dridex, Cobalt Strike, IcedID, as well as PowerShell scripts were all used for portions of the attack. Based on that, we realized our compromise was a Kerberos attack, traditionally called a Golden Ticket attack, which was used to compromise AD and enable and deploy ransomware encryption on multiple machines," added LaValley.

## Ransomware Survival Kit Fit for the County

How did Yuba County respond? In multiple phases: "In the initial 24 hours, we disconnected all servers, backed up files, disabled admin accounts, and reset passwords," LaValley explained. "The next step was restarting the department and user notifications. We communicated to department heads, county management, and users what was going on. This included the FBI, various CA State Agencies, in particular the California Office of Emergency Services. Additionally, we blocked all inbound and outbound network traffic outside of the US."

With Rubrik, Yuba County was able to accelerate its ransomware recovery with just a few clicks and restore to the most recent clean slate. "Backups are one of the most, if not the most, important defenses against ransomware. Rubrik's file system was built to be immutable, meaning backups cannot be encrypted or deleted by ransomware. I am very fortunate to say that 100% of what we had on Rubrik we were able to recover with LiveMount since 90% of our servers are virtualized," LaValley stated.

What initially drove Yuba County to adopt Rubrik was the need for a different type of DR. The DR strategy they had in place was for the typical flood or earthquake, unfit for modern-day threats, especially ransomware. "Rubrik saved our data during this sensitive time thanks to its immutability, MFA, and retention lock. Understanding the hackers were in control of AD, Rubrik ensured we cleared AD of anything tied to Rubrik, building an immutable protected vault," explained LaValley.

"Needless to say, I learned a lot through this process. I can sleep better at night knowing we have systems in place to impede either a recurrence or another ransomware attack." LaValley remarked. Additional benefits:

- **$0 paid in ransom**: "One of the few moments of satisfaction in weeks of discomfort was knowing Rubrik was backing up our data and that we wouldn't have to pay the ransom for data recovery. This saved the county potentially hundreds, if not millions, of dollars."
- **100% of backups recovered within 7 days**: "We were able to recover 100% of what we had on Rubrik thanks to its native immutability and avoided paying any ransom."
- **90%+ management time savings (26 days of productivity back)**: "Previously, we were spending between four to five hours per week managing our backups. This has now been reduced to 30 minutes per week with Rubrik. As a result, our team has gained 26 days of productivity. As a small shop, we don't have a dedicated backup administrator, so any time savings that we can devote to other projects is critical."
- **World-class support**: "As soon as we were notified of the attack, Rubrik's support team engaged us and prioritized our recovery efforts. They worked around the clock to help maintain continuity and were always available to help. I couldn't be more thankful to the Rubrik team."
- **Recoverable isolated backups**: "Having recoverable isolated backups that attackers cannot get to is the key component in protecting against ransomware. You cannot prevent someone from attacking you but at least you have recoverable data with Rubrik. The peace of mind we have is priceless."
- **Near-zero RTOs**: "With our legacy solution, we were unable to perform granular restores. We were tasked with recovering an on-prem file server for legal discovery purposes but ended up having to recover a complete backup to restore a single file server image. This entire process took one week and even worse, our backups came to a halt. With Rubrik, the difference is night and day—it takes minutes to recover our data from on-prem and the cloud. We also have the granularity to recover exactly what we need."

rubrik

**Global HQ**
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter.