

How to Recover From Ransomware Using Code42

Ransomware threatens to hurt your bottom line and tie up valuable resources. Restoring your data to the moment of the attack can be completed in a few simple steps.

“After deploying Code42, two of the same executives were hit again with ransomware. What might have been a repeat nightmare proved no issue thanks to automatic backups and extensive versioning.”

Situation

When ransomware strikes, business productivity and yield suffer. Businesses estimate time-to-respond to ransomware is anywhere from several hours to several days per device. Without reliable backup, there is no certainty of data recovery no matter how much time is spent trying.

Analysts and industry experts recommend frequent backups to mitigate risk of data loss and eliminate ransom payments; but not all backups are created equal. The highest quality backups are those that happen automatically and continuously and offer versioning that supports reliable file restore.

Solution

After a ransomware event, IT admins can initiate a full device restore to a new or reimaged device by following these steps:

1. Identify the time of the infection. If unknown, restore several versions of an individual file to determine the correct timeframe or analyze file timestamps to identify the timeframe of recent file modifications.
2. Select the root folder from which you would like to restore.
3. Select the date and time from which you would like to restore.
4. Initiate the restore. If specific files are needed to resume work immediately, select and download these files first before initiating a full device restore. Files will be restored to original folder structures and locations.
5. Tell users they can get back to work while files download in the background.
6. When restoring files to a new or reimaged device, you can save time, storage and bandwidth by adopting the original backup archive rather than re-starting a new backup.

Intel Security predicts ransomware incidents will continue to rise in 2016, and begin heavily targeting Mac OS X users and the financial industry.¹

QUICK FACTS

Financial technology company

Prior to Code42, the company experienced a ransomware attack on six executives

Restoring from legacy backup proved unreliable

Incident became a fire drill for the IT support specialist and resulted in full data loss

After deploying Code42, two of the same executives were once again hit with ransomware

All end-user data was quickly recovered

CUSTOMER SPOTLIGHT:

A financial technology company of more than 5,000 employees uses Code42 to protect the critical end-user data on its laptops and desktops.

Team

IT support specialist

6 VP-level executives

Customer pre-condition

Prior to Code42, the company relied on Syncplicity and SOS Online Backup for data protection. When six of its executives were hit with ransomware, Syncplicity synced the infection to its saved files as well. SOS Online Backup also proved unreliable—it had not successfully completed a backup for six months. The end result: complete data loss.

Customer post-condition

After deploying Code42, two of the same executives were hit again with ransomware.

What might have been a repeat nightmare proved no issue thanks to automatic backups and extensive versioning. The IT support specialist was able to restore all data and garner the ultimate praise from an executive who said, “Thank God for this software and good job bringing it in.”

Conclusion

This data recovery story is one of many. In fact, one-third of Code42 customers have already used Code42 to recover from ransomware.² The threat of ransomware and the cost to recover continues to grow. In the last year, organizations represented 43 percent of all ransomware victims and the average ransom doubled from nearly \$300 to \$679.³

Code42 offers a full year of end-user data protection for just one-sixth the cost of a single ransom payment. With Code42, IT has the ability to view, analyze and restore employee files and remediate and recover from any data incident. When ransomware inevitably hits, you'll restore devices in less time, with less effort—all without paying a ransom.

¹ <http://intel.ly/2brWXj8>

² <http://bit.ly/2btsRdX>

³ <http://bit.ly/2blmFz7>



FOR MORE INFORMATION: CODE42.COM/CONTACT

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM