the GORILLA GUIDE® to...

Real-Time Ransomware Detection and Recovery

Rethinking Your Disaster Recovery Strategies

JAMES PANETTI

Zerto
a Hewlett Packard
Enterprise company

POWERED BY ActualTech MEDIA

Real-Time Ransomware Detection and Recovery

By James Panetti

TABLE OF CONTENTS

Copyright © 2023 by Future US LLC
Full 7th Floor, 130 West 42nd Street, New York, NY 10036

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

www.actualtechmedia.com

Publisher's Acknowledgements

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

PARTNER AND VP OF CONTENT
James Green

WITH SPECIAL CONTRIBUTIONS FROM ZERTO
Kevin Cole, Global Director, Technical Product Marketing
David Paquette, Product Marketing Manager
Caroline Seymour, Vice President, Product Marketing

ABOUT THE AUTHOR

James Panetti is a techie by hobby and profession and loves writing about it via his company, Panetti Tech Insights. James has nearly two decades of tech industry experience spanning tech support, consulting, performance testing, release automation, cloud technology, and corporate policy writing.

Welcome to The Gorilla Guide® To... Real-Time Ransomware Detection and Recovery. Not only does ransomware threaten the very way we do business in the modern world, but it also forces us to adapt as rapidly as it grows in variety.

This adaptation includes rethinking our disaster recovery strategies to ensure we do not rely entirely on backups. Any potential threat to any piece of data must be detected the moment it appears, but if all else fails, then we must be able to recover any and all data from any point of time—*fast*—if we are to keep up with the pace of our attackers.

The Growing Threat of Ransomware

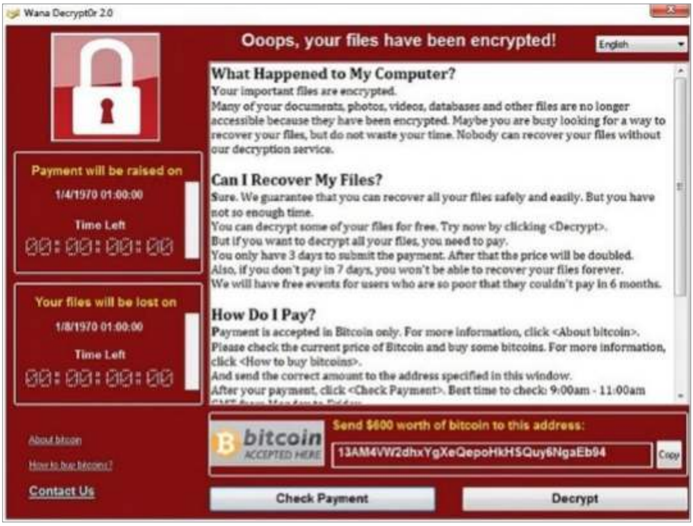
The era of viruses, trojans, rootkits, and the like has largely come and gone, now eclipsed by the modern king of malware, ransomware.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that locks access to data until a ransom is paid. The victim's data is typically encrypted while the attacker holds the secret decryption key.

WHAT DANGERS DOES IT POSE?

Ransomware can cripple an entire organization's operations for hours, days, or in the worst cases, even longer.



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Figure 1: Ransom note left on systems infected by WannaCry ransomware

The most common method is via hard drive encryption. Once a system is infected, ransomware may encrypt specific data or entire hard drives, then spread from system to system. Other variants lock users out of their workstations or servers while a lock screen with a ransom message fills the monitor (see **Figure 1**). In all scenarios, the data or system is unusable until the attacker's ransom is paid in full.

A ransomware attack can require a mountain of funds to resolve.

This can paralyze an entire production environment because ransomware tends to spread like wildfire, quickly locking swaths of data and systems throughout a network.

A ransomware attack can require a mountain of funds to resolve. Any possibility of recovering data will usually require significant downtime as unencrypted data is restored from backup—assuming backups haven't been compromised as well. Worse yet, in the event the data is beyond recovery, the only option left is to pay the attacker's exorbitant ransom and hope you can recover some of your data.

VARIETIES AND DELIVERY METHODS

Ransomware attacks come in a wide variety. The most common variants employ phishing or scareware to instill targeted users with a sense of urgency and trick them into voluntarily downloading and installing the ransomware package.

Other variants target enterprises via remote desktop protocol (RDP) running on Windows servers, exploiting service vulnerabilities that first compromise the server, then all users who remote into it. Yet others target Active Directory (AD), finding exploits in its structure and services via which it can steal passwords or even push more ransomware throughout the internal network.

Ransomware has grown so popular that some attackers even hire third-party "hacker" services, referred to as Ransomware as a Service (RaaS), often procured via the dark web.

NO OS IS SAFE

Though 91% of ransomware attacks targeted Windows as of 2020, the variety of targets is steadily growing to include MacOS, Linux, iOS, and Android.

The tried-and-true backup strategies of old are unable to keep up with the speed of modern attackers.

No OS or even hypervisor is safe. Ransomware variants such as 2022's Cheerscrypt and Black Basta target virtual machines (VMs), the latter specifically targeting Linux hosts.

What systems have you seen infected by ransomware?

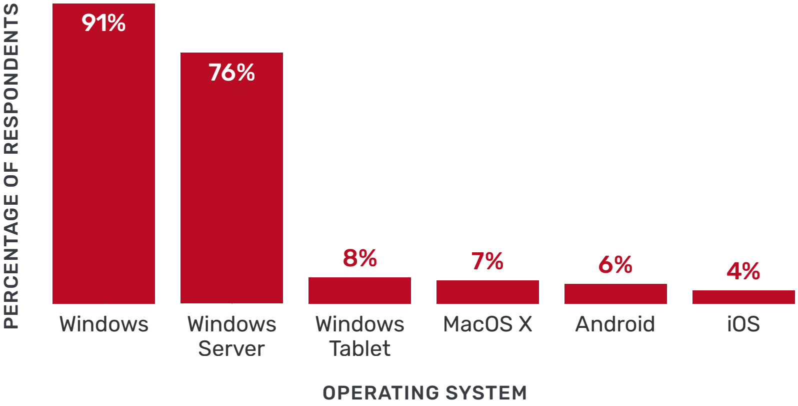


Figure 2: 2020 OS survey from Statista

RANSOMWARE IS ON THE RISE

The growth in the number and variety of ransomware show no signs of slowing down; rather attacks continue to escalate. Though 2022 studies showed that the median dwell time for various types of network intrusions was down, possibly suggesting an improvement in responsiveness, ransomware was a significant factor in driving it down as it achieved a median dwell time of four days.

Challenges of Traditional Data Protection Solutions

The tried-and-true backup strategies of old are unable to keep up with the speed of modern attackers. Once upon a time, the last line of defense was the always reliable last resort of "simply wipe and restore from backup." This is no longer foolproof.

TRADITIONAL BACKUP STRATEGIES ARE OUTDATED

Backups were always an assured final fallback because their data was clean and safe. This is no longer true. Many ransomware variants specifically target backup data.

For example, some ransomware variants target a backup solution's software agent, either compromising it to serve its purposes or disabling it to ensure no backup processes can execute before the attack. Others prove to be so pervasive that any backup or restore process will trigger a second attack, immediately re-compromising the data.

Traditional backup methods cannot account for this because incremental backups only restore data from the point of time in which the backup executed. Ransomware can easily compromise an entire organization's critical data within that time window so that the most recent backup will be too old to fully restore all the data lost and any backups that follow will back up compromised, unusable data.

Comparing Solutions

Each backup solution possesses its own strengths and weaknesses. None can offer a perfect, impervious defense, though they can be combined to complement each other for increased resiliency.

OFFLINE & OFFSITE BACKUPS

Offline and—better yet—offsite backups, be they in the form of tapes, detached NAS, or on a cloud, make for a strong line of defense, simply because ransomware cannot reach it; it can only spread over the network.

Offline storage is sadly not a guarantee. The biggest risk is that any data backed up during the undetected attack window is already compromised, rendering the backup useless. Second, long-term backups have the largest gaps of time between incremental backups, therefore an attack can cost entire days' worth of productivity. Any data compromised since those backups were taken is forever lost unless the ransom is paid.

A well-designed disaster recovery network will be walled off from the rest of the organization's networks.

The process of restoring data from an offline or offsite backup is by far the slowest of recovery options. It trades speed for capacity and reliability, therefore the time it takes to restore any data—to say nothing of an entire organization's data—can take days or even weeks to complete.

⚠ **Tape media is among the oldest but most reliable and popular of offline options**, but their use is usually in the interest of fulfilling compliance use cases that demand very long data retention and very infrequent access, thus rendering them insufficient for cyber resiliency.

DISASTER RECOVERY NETWORKS

Disaster recovery networks, often set up as VLANs, are a particularly strong option. A well-designed disaster recovery network will be walled off from the rest of the organization's networks. An isolated network is much harder to compromise.

The biggest problem is in its complexity. An isolated network replicating large swaths of production data necessitates constant diligence and maintenance. The network itself is only as secure as the perimeter defenses built around it. If any one of those defenses suffers any vulnerability, the entire disaster recovery network can be at risk.

For example, recall that many ransomware variants specifically target RDP and AD services. In order to be truly isolated from the rest of your organization's networks, your disaster recovery network must not be joined to AD nor any component accessible via RDP.

THE 3-2-1 RULE

The 3-2-1 Rule is by far the most resilient of disaster recovery strategies because it combines multiple data protection methods, each method's strengths accounting for the others' weaknesses.

The 3-2-1 Rule, a one-to-many replication model, is simple in concept: 3 copies, 2 types of media, 1 offsite.

To elaborate, your organization must have a minimum of three copies of your data. Those three copies should include two different types of media. Finally, one of the three must be offline and offsite. This strategy greatly reduces the probability of a ransomware attack compromising all your backups at once.

A 3-2-1-1 or 4-3-2-1 method is even superior.

The 3-2-1-1 version consists of the same criteria but adds one air-gapped or immutable copy. Air-gapped media is deactivated and inaccessible. It can only be accessed when powered on. Immutable storage is designed in a Write Once, Read Many (WORM) format, meaning that once backup data is written to it, it cannot be deleted or modified for a specified period; it can only be read.

The 4-3-2-1 rule requires four copies across three locations, two of which must be external. One of the four must be immutable. In other words, two of the four copies may be kept in proximity, the remaining two must each be stored far away from each other and the organization's environment, and one must be in WORM format.

Real-Time Ransomware Detection & Recovery

Now that disaster recovery infrastructure itself is a target of attack, real-time detection is a must-have for any modern disaster recovery strategy.

REAL-TIME DETECTION

Any solution protecting your data and recovery mechanisms should include real-time behavioral analysis and real-time threat analytics.

Known ransomware variants share commonalities in behavior, therefore effective real-time detection should not only detect ransomware explicitly, but should also detect suspicious behavior that implicitly suggests ransomware activity. Behavioral analytics can leverage machine learning to watch for behaviors that resemble ransomware triggers, unexpected data encryption, obfuscation techniques, and so on.

Now that disaster recovery infrastructure itself is a target of attack, real-time detection is a must-have for any modern disaster recovery strategy.

Similarly, real-time threat analytics serve to mitigate threats by constantly monitoring network perimeters and intercepting traffic, testing activity against known ransomware variants, and strategically isolating and removing suspected threats.

A solution including these features is superior to those that only detect a threat at the time a backup is executed. Ransomware can easily wreak havoc within hours, crippling entire production environments and ensuring all data generated since the last daily backup is beyond restoration.

CONTINUOUS DATA PROTECTION

While threats must be detected in real time, data must be protected continuously—that is to say, around the clock.

Continuous data protection (CDP) models grant organizations the ability to continuously track and replicate all data modifications, regardless of granularity. In other words, *every* time *any* piece of data is altered in any way, a copy of that data is immediately replicated for safe keeping. Data written to one location is immediately and asynchronously written to a journal. This finely granular, always-immediate replication means that any data may be restored at any time regardless of what point in time it may have been compromised by an attacker.

One need not labor the point that CDP is therefore far more resilient than traditional incremental backup processes. CDP minimizes any loss of data to literally *seconds*, given there's no longer any snapshot tied to a limited window of time.

Once data is initially synced, only alterations to that data are replicated from that point forward. CDP can thus restore any data to any point in time. Within the context of a ransomware attack, this means compromised data can be easily and swiftly restored to its clean state right before the attack, rendering the attacker's encryption efforts useless.

Zerto as an All-in-One CDP Solution

Zerto, a Hewlett Packard Enterprise company, provides a single, comprehensive solution that addresses the shortcomings of traditional disaster recovery methods and infrastructure.

Zerto is built upon a CDP foundation to protect enterprise infrastructure across on-premises, hybrid, and multi-cloud environments. It features innovative methods of detecting encryption anomalies, and it can interoperate with your existing tech stack, including both cross-hypervisor and cross-cloud functionality.

A SOFTWARE-ONLY SOLUTION

Most traditional backup solutions of old require one install of a software agent on each server and workstation to manage and execute regular backups, which, as noted previously, can be hijacked by ransomware. Many such solutions also require specific types of complex or costly backup infrastructure and media.

While threats must be detected in real time, data must be protected continuously—that is to say, around the clock.

Zerto has no such restrictions. As a software-only solution that doesn't rely on any type of agent component whatsoever, Zerto can save your organization backup and infrastructure costs, given its small footprint and low overhead. Better yet, Zerto allows your organization to use the hardware infrastructure and storage media types of its own choosing.

CONTINUOUS DETECTION

Zerto's real-time ransomware detection delivers continuous detection—every minute of every hour of every day—that provides both the fastest ransomware warning and data recovery.

Most competing solutions come in the form of backup solutions whose detection capability is limited to comparing differences between periodic backups, which are typically hours apart. This means a malicious attack that may have begun hours earlier will not be detected until the *next* backup is checked.

Zerto automatically detects unusual encryption behavior in real time as writes stream in and immediately alerts incident response teams. Zerto can pinpoint anomalous behavior and mitigate a would-be ransomware attack during its earliest stages of encryption. Zerto can also track data in third-party monitoring solutions via APIs.

Detection is based on Zerto's near-synchronous replication and journaling. Zerto reports on every encryption activity, down to the number of blocks encrypted, as it observes data in real time. It automatically identifies encryption activities that pass a certain behavioral threshold as anomalous. Zerto meanwhile tags recovery checkpoints in the journal to identify when an attack likely began (when encryption began). That journal then ensures the data affected may be immediately restored to the clean state it had been in within seconds prior to the attack.

This early warning system empowers incident response teams to swiftly investigate and verify an attack, then immediately mitigate damage and recover data.

CONTINUOUS PROTECTION

As a lightweight, software-only replication solution, Zerto includes all the CDP functionality detailed earlier, adding critically needed modern protection against modern threats.

Zerto is always on and provides near-synchronous replication of all an enterprise's data, but with no impact on production processes, given that Zerto doesn't install any agents, nor does it perform computationally expensive snapshot processes. It also provides the functionality to isolate, air-gap, and vault data so that it will be safe from an attacker's reach.

Zerto's CDP model also means there's no longer any need for administrators to micromanage backup windows. Admins need not schedule downtime or stay after-hours to ensure a daily backup goes smoothly.

SWIFT RECOVERY

Zerto's CDP approach overcomes traditional capacity limitations and ensures a swiftness in recovery that cannot be matched by traditional methods. Old disaster recovery strategies can easily consume hours, days, or more during a crisis, while Zerto can restore any data to any specific point in time prior to an attack within mere minutes.

Zerto is well suited for leveraging production-grade storage instead of requiring secondary storage, purpose-built backup appliances (PBBAs), or tape media. This means that in the middle of a crisis, there's no need to move from lower-tier storage up to production-grade storage in order get a production environment up and running again. In fact, Zerto can provide your organization with a recovery point objective (RPO) in terms of seconds, and a recovery time objective (RTO) of minutes, both of which equate a dramatically lower loss of data and shorter period of downtime.

HYBRID & MULTI-CLOUD AGILITY

Zerto is ideal for building your 3-2-1, 3-2-1-1, or 4-3-2-1 disaster recovery strategy because it can leverage both your onsite and offsite cloud architectures, including multiple clouds via a one-to-many replication model. Zerto can simultaneously replicate up to three different targets, all on disparate platforms or infrastructures (if so desired) in order to minimize risk.

When it comes to cloud architecture specifically, Zerto's scale-out architecture is designed to protect entire petabytes of data, containers, and all the VMs you could possibly need, no matter how many thousands upon thousands you may have. It can also protect your various Software-as-a-Service applications, such as Microsoft 365, Salesforce, and Google Workspaces.

You can easily get started with Zerto today. Simply go to Zerto's website to review a free whitepaper, request a demo, or try a free hands-on lab.

About Zerto

Zerto

a Hewlett Packard Enterprise company

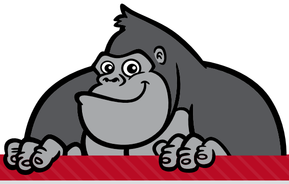
Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto eliminates the risk and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only solution uses continuous data protection at scale to solve for ransomware resilience, disaster recovery, and multi-cloud mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Amazon, Google, IBM, Microsoft, and Oracle and more than 350 managed service providers.

About ActualTech Media

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/