Isolated Backups on Dell EMC Data Domain

A last line of defense against ransomware attacks

Introduction

According to the August 2016 report from Osterman Research, *Understanding the Depth of the Global Ransomware Problem*, 39% of organizations surveyed had been negatively impacted by a ransomware attack in the previous 12 months. Companies faced with a ransomware attack find their critical data surreptitiously encrypted or discover they are locked out of their own computers with no access to the affected system. The goal of the attack is to cripple an individual’s or organization’s ability to carry on operations to an extent where the cost of paying the ransom is more viable than any alternatives. The scope of a ransomware attack can range from one computer compromising locally attached data to thousands of systems and petabytes of data on enterprise storage arrays. According to the Osterman report, decision makers in the United States are not confident in their ability to effectively stop ransomware attacks.

Further evidence of the scope of the ransomware problem comes from a recent Symantec Corporation report, *The evolution of ransomware*:

>“Never before in the history of human kind have people across the world been subjected to extortion on such a massive scale as they are today.”

Ransomware is rapidly gaining popularity with cybercriminals because of the opportunity to extort small sums of money from a vast number of individuals and large sums of money from mid-size and enterprise-size organizations, all while staying under the radar of the authorities. Attackers set the ransom amount at a level where individual users find it easier and faster to pay the ransom rather than seek professional assistance or remediate the problem themselves. Large organizations, faced with locked systems, idle workers, and a lack of viable recovery options also find it faster and easier to pay the ransom.

Attacker’s currency of choice is Bitcoin. The international cryptocurrency has no limitations on borders and is difficult to track. Attackers charge individual users a fraction of one Bitcoin (about $200–$300) and charge large organizations as much as 20 to 100 Bitcoin (about $18,000–$100,000). And, just because an individual or organization pays to regain control of their systems from one attacker, it doesn’t preclude another attack from the same, or different, attacker in the future. The cycle can go on indefinitely until appropriate action is taken to prevent or remediate future attacks.

Three widely accepted strategies for protecting a business from ransomware attacks include prevention, containment, and recovery. Dell EMC, a leader in backup and recovery, shows in this paper how protecting backups and executing fast restoration can safeguard the business from extortion.
Ransomware—cost and payment statistics

According to US government statistics, shown in Figure 1, more than 4,000 ransomware attacks are attempted every day. Cyber criminals stole $209 million in the first quarter of 2016 alone, putting ransomware on course to be a $1 billion business by the end of 2016, with predictions of $2 billion by the end of 2017.

Several complex business questions must be answered before a decision can be made about paying or declining to pay a ransom. The majority of ransomware victims choose not to pay. The overall worldwide average of organizations that pay is 37%. In the United States, the average is only 3% (roughly 850,000). Many victims of ransomware attacks also elect not to report the incident so actual numbers of attacks might not be accurate. The logic for not paying is as follows:

- Paying a ransom funds both more attacks and more sophisticated attack strategies.
- Paying a ransom emboldens cybercriminals and can lead to more attacks.
- There is no guarantee that the business will recover any data or system access after paying a ransom.

The worst-case scenario when deciding not to pay a ransom is that the encrypted data or locked systems cannot be recovered and the business impact is permanent. The best-case scenario depends on the capability of the business to quickly recover lost data. Defeating ransomware requires a comprehensive approach to training IT professionals and investing in prevention and recovery technology. Recovering from an attack is dependent on the organization’s investment in backup processes and the safeguards put in place to protect backups as well as the core systems and data.

Types of infection vectors and ransomware

Ransomware can infect a computer and spread to other accessible systems in many ways. Email is a very common infection vector. Opening a malicious email or email attachment, or clicking a link inside an email are some ways that ransomware can infect the business. Links that lead to nefarious websites are also a popular ransomware infection vector. And many ransomware emails fake an appearance of importance by impersonating a well-respected organization.
Other infection vectors include:

- Downloaded exploits are malicious programs disguised as anti-virus or other useful tools available for free. After it is downloaded, the fake program appears to be scanning and removing viruses from the computer but in reality is encrypting files.

- Social media and mobile applications are another way that cybercriminals can infect computers and devices. Clicking a link in a social media site can install ransomware and download an app that can lock the device.

- Brute-forcing password discovery can sometimes result in rapid guessing of the login credentials for computers and servers.

![Infection Vectors](image)

**Figure 2. Infection vectors and ransomware**

Of the three types of ransomware—fake anti-virus, locker ransomware, and crypto ransomware—crypto is currently the most popular with cybercriminals. When established, it can use remote protocols such as Remote Desktop Protocol (RDP) to infect other systems. Crypto ransomware encrypts valuable data on systems without alerting the user or administrator—the files are then inaccessible. A crypto program will run undercover on a computer system to encrypt as many files as possible without unduly impacting the operating system. Most users will continue to use the computer, without realizing that the ransomware is running, until they are presented with an extortion message requesting payment to decrypt the files.

Fake anti-virus is a common delivery vector for crypto ransomware. The ransomware is disguised as a useful program that removes viruses or malware. The fake program appears to be scanning the system for viruses but instead it is encrypting data files.

Locker ransomware denies access to the computer by locking the systems and allowing users to interact only with the malware. Locker ransomware typically leaves the files on the computer unmodified so that users can access the files again after the malware has been removed. IT organizations and advanced users have a better chance of recovering a computer from locker ransomware infections than from other forms of attack.

Understanding the various types of ransomware and the current state of infection vectors enables an organization to use the best preventative measures to reduce the chance of being compromised. For a thorough understanding of the challenges of ransomware, refer to the ISTR special report [Ransomware and Businesses 2016](#).
Data security best practices

Experts encourage everyone—from law enforcement to corporations to individuals—to always follow best security practices. Most importantly, ensure that you have a verified gold copy of your data securely stored and available at any time from a backup and restore solution. New variants of ransomware not only encrypt local drives and file systems, but also attack network-attached drives and enterprise storage arrays. Because of these new attack vectors, having an isolated (offline), tested disaster recovery process is the number one line of defense against ransomware attacks.

Best practices for preventing ransomware attacks

- Back up your files, devices, and images often and keep a copy offline
- Disable macros in Microsoft Office documents
- Keep applications and your operating system patched and up to date
- Enable the **Show file extensions** option in the Windows settings on your computer
- Do not give users higher credentials than they need
- Enable VLANs and segment your traffic
- Train and educate your employees

Your backups are at risk

Modern backup architectures use the network to provide access to backup systems. The advantage of a centralized backup system that is accessible over the network is the capability to consolidate operations, reduce complexity, and streamline management. However, crypto ransomware is becoming increasingly sophisticated and can infect the contents of shared or networked systems, even those used for backup. Ransomware such as CryptoFortress attempts to enumerate all open network SMB-enabled systems and, if successful, encrypts files on any unmapped network drives. Organizations are now at risk of network resources being encrypted whether the drives are mapped or unmapped.

Figure 3 shows how the chain of infection can impact many network accessible resources including the backup system. Depending on the crypto ransomware used and the backup system in place, damage and disruption varies greatly but can include:

- Loss of backups or backup data
- Inability to restore or recover any systems
- Inability to backup any systems
Protecting the backup system is critical to an organization’s ability to recover from a ransomware attack without having to pay a ransom. The cornerstone of this approach is using a secure and isolated area in the data center for the backup systems—that is, an area to which only authorized personnel have access. Isolation demands that all equipment is off the network and that access to the equipment requires special passwords. Dell EMC has created an isolated recovery solution using Data Domain to protect the backup environment and enable an organization to quickly restore infected systems.

**Building a last line of defense—what you need**

<table>
<thead>
<tr>
<th><strong>Isolation</strong></th>
<th>An isolated data center environment that is normally disconnected from the network and restricted to personnel with the proper clearance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data copy and scheduled air gap</strong></td>
<td>Software to perform data copies to a secondary set of infrastructure and backup targets, together with scheduled air gap maintenance between the production environment and the isolated recovery zone. Automation is an essential component of managing the air gap and data movement.</td>
</tr>
<tr>
<td><strong>Integrity checking and alerting</strong></td>
<td>Integrity checks to verify that a system is unaffected by malware, and mechanisms to trigger alerts in the event of a breach.</td>
</tr>
<tr>
<td><strong>Recovery and remediation</strong></td>
<td>Validated procedures to perform recovery and remediation processes after an incident. Regular restore procedures.</td>
</tr>
</tbody>
</table>
Data Domain isolated recovery solution

Dell EMC has decades of experience in securing data for customers. Our solutions meet the most stringent requirements and use the most robust and secure technology set in the market. Dell EMC is helping customers thwart ransomware threats by designing and implementing isolated recovery solutions that lock out hackers from the most critical data sets and ensure a path to quick business recovery.

At Dell EMC, we are dedicated to helping our customers:

• Identify strategies for designing isolated recovery solutions.

• Procure the components required to implement a comprehensive solution to the ransomware threat.

• Define the process and operational steps required to ensure key applications can be quickly returned to an operational state.

We are applying existing technology and products in new, creative ways to build a trusted last line of defense against ransomware data loss and system outages. For most customers, these solutions are an extension of current infrastructures and can be rapidly deployed to accelerate time to protection. Simply put, there are practical steps any customer can take across people, process, and products to mitigate risk.

Data Domain offers the capability to replicate data securely and asynchronously between systems with a connection air gap implemented during replication idle times. This isolates the replica Data Domain system, safeguarding a no-access vault copy of your critical data for the purposes of recovery.

A key component of the solution is a secure and isolated area in the data center. Only authorized personnel should have access to this area. All equipment should be off the network. Special passwords should be required for equipment access and equipment should be accessible by authorized personnel only. Management, validation, and recovery hosts should be staged in the isolated area to enable system management, data integrity validation, and quick recovery of business applications.

Figure 4. Data Domain isolated recovery system
Isolated backup best practices

- The workstation for the isolated Data Domain system must have no connection to the data center network and must be used only for root access and management of the Data Domain system.

- Dedicate a physical network port on the primary Data Domain for the private, isolated replication connection to the isolated recovery system. Implement network hardening best practices.

- Implement and schedule (in concert with Backup Software replication policies) the physical and logical connection of the transmission links at the infrastructure layer between your backup system and the isolated recovery system.

- Perform validation checks to ensure that the replication link is online and can be made at the Data Domain OS level.

- Data Domain replication offers the capability to encrypt data (256bit AES) in flight and at rest, ensuring that data cannot be read either while it is being transferred (man-in-the-middle attacks) or when it is at its final resting place for secure retention.

- After replication has completed, make the relevant logical and physical disconnections to ensure that the isolated Data Domain system has no external access points available. In this way, the data is kept isolated and inaccessible from any external or internal network attack.

Summary

As the threat and capability of ransomware increases, there might be only two categories of computer users, those who have been attacked and those who will be attacked.

Data Domain uniquely offers the ability to address ransomware threats in environments where business critical systems reside on both Dell EMC and non-Dell EMC systems.

Dell EMC has a portfolio of options for providing a flexible set of security solutions to meet the specific needs of our customers in all industries, including the financial, healthcare, and federal sectors.

References

Understanding the Depth of the Global Ransomware Problem (Malwarebytes, 2016)
The evolution of ransomware (Symantec, 2015)
An ISTR Special Report: Ransomware and Businesses 2016 (Symantec, 2016)
EMC Data Domain Isolated Backup White Paper (EMC, 2015)
Dell EMC Data Domain home page

Contact us
To learn more, contact your local representative or authorized reseller.

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA February 2017 Solution Brief H15740.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Authors: Dave Simmons CISSP, Judith Cuppage.

This document is not intended for audiences in China, Hong Kong, and Taiwan.