Ransomware – Defense in Layers

Organizations need backup software that ensures top-level backup and recovery and limits the number of entry points for ransomware.

Infosecurity magazine reported that weekly cyberattacks have increased worldwide by 7 percent in Q1 2023 compared to the same period last year, with each firm facing an average of 1248 attacks per week.[1] Cybersecurity ventures reported that the frequency of ransomware attacks on governments, businesses, consumers and devices will continue to rise over the next five years and is expected to rise to every two seconds by 2031. They expect ransomware damage costs to exceed $265 billion USD annually by 2031.[2] And when all is said and done, most companies can only recover about 65 percent of their data.[4] These startling statistics highlight the dire need for stronger data protection.

Furthermore, there's also the cost of not being able to fully recover all the data after a ransomware attack. An April 2022 study queried 1,456 cybersecurity professionals from organizations with 700 or more employees.[5] They found 73 percent of organizations have suffered at least one ransomware attack – up 33 percent from last year.[5] Sixty percent of those companies admitted ransomware gangs had been in their network from one to six months before they were discovered. However, only 42 percent said the payment resulted in the restoration of all systems and data (down from 51 percent last year).[5] Consequently, nearly 40 percent of companies laid off staff as a direct result of the attack.[5]

The threats and costs of ransomware are as high as they've ever been, and the challenge for IT and backup admins is to constantly re-evaluate the defensive layers needed to lessen the risk of ransomware.

Ransomware damage costs are expected to exceed $265 billion USD annually by 2031.

[1] Infosecurity Magazine
[2] CybersecurityVentures
[3] The Cost of IT Downtime
[4] Ransomware.org
[5] Ransomware the True Cost

RANSOMWARE USES VARYING METHODS TO GAIN ACCESS

There are various methods ransomware uses to gain access. Some could be classified as "spray attacks," which cast a wide net to reach as many victims as possible. More recently, others have become very targeted towards particular types of businesses. Let's explore a few of the more well-known examples.

THE NEXT PHASE

Ransomware is changing into a new phase, with a more considered and targeted approach. Some tool sets are now being looked upon as Ransomware-as-a-Service, or RaaS. These openings and compromised credentials are being sold to criminals who only want to make money via ransom.

73 percent of organizations have suffered at least one ransomware attack – up 33 percent from last year.

Even the financial models are changing. The days of hackers asking for $300 worth of Bitcoin to decrypt data are gone. Nowadays, ransom demands commonly range anywhere between $1M-$10M. In addition, perpetrators are using new tactics to collect ransom, like threatening to publish the organization's data openly if it doesn't pay the ransom.

This often presents as a data breach, opening the organization to compliance violations from legislation like GDPR, CCPA or the new Washington state HB1071 bill changing its rules on Personal Identifiable Information (PII) data and breach notification.

These attacks are also changing. Human activity in prolonging the attack is also becoming a growing trend. Let's look at one possible ransomware scenario.

EXAMPLE SCENARIO

In this section, we'll explore a potential Group Policy Object (GPO) attack. Group policy is Microsoft's core infrastructure for managing the configuration of both users and computers in an enterprise windows forest.

According to Microsoft: "Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory. GPO settings are evaluated by clients using the hierarchical nature of Active Directory."

You probably spotted the importance of file systems and Active Directory. A successful attack on your Active Directory is like handing over the keys to the castle to your worst enemy.

These attacks are sometimes called Group Policy Hijacking and will use known exploits to gain control of an entire organization. However, this type of attack also has the added twist of being updated by human interaction, to keep changing things and retain an entry point into the organization under attack.

A LAYERED DEFENSE

To minimize the threat of ransomware, organizations must establish a layered defense. While the list presented here is not exhaustive, and offers no guarantees against ransomware attacks, it should start you on the path to considering what to cover, or perhaps even provide a confirmation for things already in place.

End-user training

Educating and training your user base is imperative, and letting them know the risks. Educate them on how ransomware enters an organization (i.e. downloads, files, fake websites, file sharing sites, phishing attacks to gain user details and credentials).

End users should also be made aware of physical opportunities for ransomware to enter the organization. For example, there are known cases of infected USB keys being left in car parks, office lobbies, etc. that are picked up by unsuspecting users who plug them into a laptop.

Patching

Keep your systems up to date. Don't rely on remembering, or spreadsheets. Automate the process and patch all machines, clients and servers.

Not just Windows

Don't assume that this is just a "Windows thing." Linux still has threats, so updating Linux servers is just as important.

Network monitoring

Make sure you monitor anything that looks like traffic interception. Re-routing, spoof apps and traffic re-direction are the starting point to gaining access to the broader organizational infrastructure with 'Man in the Middle' (MITM) attacks.

Data protection

Backing up your data seems obvious, right? Well, these are still servers, and they're still running an operating system, making them just as vulnerable. Moreover, backup products that use network shares to store backup data are at a higher risk, since network shares are a target for most ransomware.

DATA PROTECTION ONLY GOES SO FAR

All things considered, creating a layered defense is the only reasonable outcome that must be employed. Simply relying on a data protection solution as a prevention measure is not enough.

Data protection is a reactive technology. You react to a need that requires data to be recovered. Data protection is carried out on a regular basis, or should be, to mitigate against data loss. But this is only effective if the solution provides methods to prevent the loss of the backup data itself.

Consider the situation where a backup solution is using a network share. While it has permissions and user accounts associated with that share, the network share is still available on the network. A GPO attack that allows elevated domain access to servers and client machines will make it easy for a ransomware perpetrator to encrypt a network share that contains any backup data.

Data protection solutions are a safety net in most instances. But with the rise in ransomware attacks, their role in an organization has been highlighted to be critical in terms of recovering quickly after a ransomware attack. To achieve this effectively, the backup solution must be able to be as resilient as possible, without compromising its usefulness.

Consider for a moment what a backup solution must achieve: It must move all your data from point A to point B as fast as physics will allow. At least that's what most people will look for. This necessitates that it has access to all of the organization's important data, applications, network, production storage, etc. In fact, it has more access than most corporate users, except for domain administrators!

Yet, we still see data protection solutions that are poorly secured with default usernames and passwords. Or these data protection solutions use open shares that are just that: wide open. We've all done it. Selecting 'Everyone' as a permissions option is the easy way to make something work, but that also creates one of the easiest entry points for ransomware.

HOW QUEST CAN HELP

To effectively minimize the ransomware risk, organizations need a backup solution that provides additional strength in combatting the ransomware impact on backup solutions. Quest NetVault Plus does exactly this.

NetVault Plus is a comprehensive enterprise data protection solution optimized for most modern data center applications and infrastructure, as well as cloud solutions. It has a heterogenous capability, not only in what it protects, but also how it can be deployed from a server architecture point of view. NetVault Plus also comes with an integrated software-defined storage solution that allows for deduplication, compression, encryption, replication and cloud integration.

Consider how NetVault Plus stores data. It uses an integrated storage technology called QoreStor. t uses an integrated storage technology that relies on an unpublished protocol called Rapid Data Access (RDA) that protects backup data. NetVault Plus also provides data encryption to ensure data is well protected.

Unlike Server Message Block (SMB), used for Windows shares, RDA is not an open protocol. It is not accessible directly by an operating system and has an authentication requirement that sits outside the local server or domain-controlled constructs. When using NetVault Plus, backup data flows directly from source to destination. There is no need to have traditional media servers. While this helps to reduce complexity it also

Cybercriminals target your backups too, so protecting your backup data is as important as protecting your production data.

A layered defense is the only reasonable approach to ransomware protection and recovery.

reduces risk by having fewer core components that could be attacked.

NetVault Plus strengthens your ransomware protection with immutable secondary storage, both on-premises and in the cloud. Backup jobs can be assigned as "immutable" such that backup data cannot be overwritten, changed, deleted or encrypted during the backup retention policy. It also supports object locking when using object storage on-prem and in the cloud.

NetVault Plus also provides a backup recycle bin that can be set to keep a copy of any deleted backup data for a specified period of time. The recycle bin is also immutable during the recycle bin retention policy.[1]

Additionally, NetVault Plus uses source-side deduplication to reduce the amount of data being sent over a network, from a client machine to storage. This further reduces exposure to data capture techniques.

On top of that, NetVault Plus employs Secure Connect technology that wraps the data transfer and control commands in a TLS 2.0 secure layer. This is a great step to restrict access to your backup data from ransomware. Of course, NetVault Plus can still have backup data access, so we also need to consider that.

You may have noticed so far that ransomware has been known to predominately target Windows-based systems, partly due to popularity, but also due to the number of existing user client/user endpoints that ransomware perpetrators can take advantage of. NetVault Plus minimizes that threat by installing the server and its infrastructure components on Linux. While not completely invulnerable, installing the server on Linux reduces the number of potential threats. Because NetVault Plus is a completely heterogeneous solution, with core components running on Linux, NetVault Plus continues to protect Windows, Unix, Linux, application data and virtualization platforms in the same way.

Another consideration is how access is granted. NetVault Plus has two main methods for granting access: Integration with a directory service or its own role-based access mechanism. Given the potential issues we've already discussed about GPO attacks, we must consider that this level of compromise could allow access to the backup application where systemic data deletion could be achieved.

But NetVault Plus has the ability to provide robust role-based access without the need to integrate with a service such as Active Directory. While this might

Operational improvements using NetVault Plus

Item	Remarks
Backup Immutability	NetVault backup jobs can be assigned as "immutable," preventing any changes, deletions or encryption during the specified backup retention policy.
Access Protocol	Data written by RDA cannot be accessed via CIFS/SMB, NFS or other protocols.
Data Access	Data stored using the RDA protocol is accessible only from the original (backup) server. An alternative backup server cannot access the data without the correct credentials and unique identification number.
Data Deduplication	There is no readable file system with visible files representing files or parts of files in a backup stream.
Operating System	NetVault Plus runs on Linux and can run on a minimal installation. It supports the use of a Linux firewall adding the rules during installation. It also supports the use of SELINUX.

be less convenient for user and group control, it does offer another degree of separation from the production environment and potential access by an undesired third party.

CONCLUSION

In the end, even the most prepared organization can't completely protect itself against ransomware attacks. But you can limit the risks when you have a backup solution that not only allows you to restore all your data quickly and fully, but also:

- Mitigates the risks of ransomware impacting your business
- Reduces the number of core components that can be attacked
- Limits exposure to data capture techniques
- Restricts your backup data from ransomware

For more information about NetVault Plus visit www.quest.com/products/netvault-plus

NetVault Plus provides a wide range of ransomware protection and recovery capabilities.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.