Ransomware – Defense in Layers

Organizations need backup software that not only ensures top-level backup and recovery, but also limits the number of entry points for ransomware.

Ransomware isn't new. It's been around a long time, and as long as ransomware perpetrators see the opportunity for financial gain, it's here to stay.

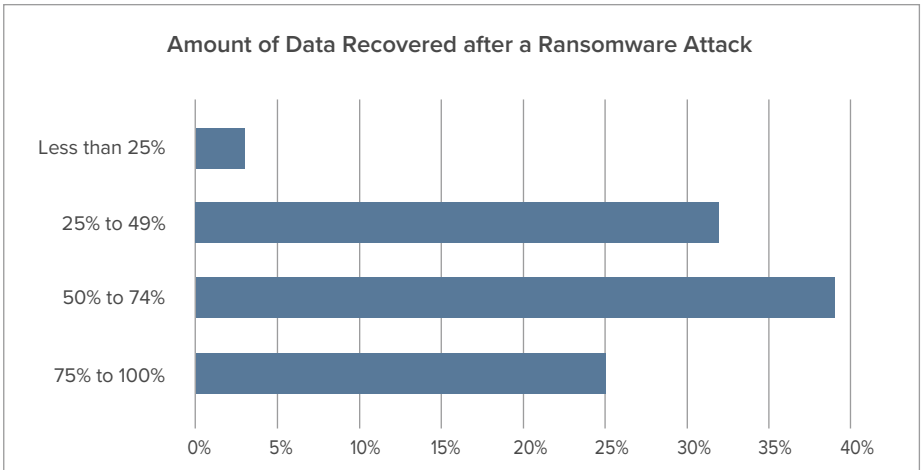
In fact, according to a 2019 report from Forrester Research[1], the number of ransomware attacks on enterprises is up 500% over the previous year. Furthermore, Forrester projects that these attacks will cost businesses $11.5 billion – and that's not even considering the intangible costs of losing trust from your customers and partners.

Furthermore, there's also the cost of not being able to fully recover all the data after a ransomware attack. In fact, a 2019 Forrester survey[2] showed that following a ransomware attack, only 25% of survey respondents said they were able to recover between 75% and 100% of their data. Conversely, 39% of survey respondents said they could only recover between 50% and 74% of their data.

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

Ransomware attacks on enterprises are up 500%, and will cost businesses $11.5 billion.

[1] "Forrester's Guide to Paying Ransomware," Forrester Research, Inc., June 5, 2019
[2] "Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans," Forrester Research, Inc., October 2019.



A 2019 Forrester survey showed that only 25% of survey respondents said they were able to recover between 75% and 100% of their data following a ransomware attack.

Just three pieces of ransomware caused upwards of $1 billion worth of damages in more than 65 countries.

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.

WannaCry

It's famous, well known and sprang into life by knocking out many organizations around the globe. WannaCry exploited a known vulnerability – Eternal Blue – and used this vulnerability to attack un-patched and older systems to gain a foothold in the IT environment.

This attack was introduced via a spray method: Mass email with attachments or links to websites, document links to file-share sites, etc. Most instances came as the result of an end user downloading a document or payload that was then executed on the end user's hardware.

Then the ransomware would encrypt data and hackers would then request payment via cryptocurrency to decrypt the data. This, of course, came with no guarantee that the data will be de-crypted even if companies paid the ransom.

NotPetya

Unlike WannaCry, NotPetya differed in that it was not about collecting ransom, but rather, it was about wreaking havoc and causing destruction. Spreading fast was its game. Again, this ransomware required someone to get the tools into an organization before it become effective. It used a modified version of Eternal Blue and a leaked Eternal Romance SMB exploit.

BadRabbit

According to WIRED magazine, BadRabbit spread via "drive-by attacks" on legitimate websites. End users would visit a legitimate website, while the threat actor would drop malware disguised as an Adobe Flash installer. This malware would immediately begin locking the infected hardware. Ransom notes would follow, typically asking for around $280 in Bitcoin.

Just these three pieces of ransomware alone caused upwards of US$1 billion worth of damages in more than 65 countries!

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.

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 itself 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, just 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 offer a confirmation of things already in place.

End-user training

It's imperative to educate and train your userbase and let them know the risks. Educate them on the ways that 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. and being 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 with a trusted solution, like Quest KACE Unified Endpoint Management solutions. Don't leave it to chance. Patch all machines, clients and servers.

Not just Windows

Don't assume that this is just a "Windows thing." Linux still has its threats, so keeping Linux servers updated 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 wider organizational infrastructure with 'Man in the Middle' (MITM) attacks.

A successful attack on your Active Directory is like handing over the keys to the castle to your worst enemy.

A layered defense is the only reasonable outcome. Simply relying on a data protection solution as a prevention measure is not enough.

Data protection

Backing up your data seems obvious, right? Well, these are still servers, and they're still running an operating system, and it makes 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 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 broad 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. This software-defined secondary storage solution is purpose-built for backup solutions. NetVault has a tight integration with QoreStor and leverages a protocol called Rapid Data Access (RDA).

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 of the local server or domain-controlled constructs. When using NetVault Plus, backup data flows directly from source to destination, in this case QoreStor. There is no need to have traditional media servers. While this helps to reduce complexity it also reduces risk by having fewer core components that could be attacked.

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 of your backup data from ransomware. Of course, NetVault Plus itself can still have access to the backup data, so we also need to consider that too.

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.

NetVault Plus uses source-side deduplication to reduce the amount of data being sent over a network … further reducing exposure to data capture techniques.

Operational improvements using NetVault Plus.

Item	Content	Remarks
NetVault Plus data on QoreStor	WORM	NetVault writes backups as data streams to QoreStor. This data stream cannot be modified by NetVault. NetVault can remove the entire data stream (backup) from QoreStor, not parts of it.
QoreStor Access (protocol)	RDA	NetVault only has access to QoreStor via the RDA protocol. This protocol has different versions. NetVault uses version 2.0, which allows writing, reading and replication of data only. Change is not possible. Data written by RDA on QoreStor cannot be accessed via CIFS/SMB, NFS or other protocols.
QoreStor Access (authentication)	Username/ Password	Access to QoreStor always takes place via a user account and password combination. Passwords are encrypted (AES) and exchanged via encryption (AES). Access to QoreStor on a management level does not allow access to data, only to configuration settings.
Data Access	RDA	Data stored by using the RDA protocol is accessible only from the original (backup) server. An alternative backup server has no access to the data without the correct credentials and unique identification number.
QoreStor Access	SSH	It is possible to access QoreStor via SSH, however, this does not allow access to the data, only to a menu of configuration settings. SSH access requires a password login.
Type of storage	Dedupe	All data on QoreStor is stored in its own format. There is no readable file system with visible files representing files or parts of files in a backup stream.
Used OS	Linux	QoreStor 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 support the use of SELINUX.
Patching	OS	It is recommended that OS patching is maintained to ensure secure operation of the OS against known vulnerabilities.
Protocol	RDA	RDA is a protocol created and owned by Quest. There is no public description of this protocol available. RDA is only used in Quest products. Currently NetVault, vRanger.

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 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: https://www.quest.com/products/netvault/netvaultplus.aspx

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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.