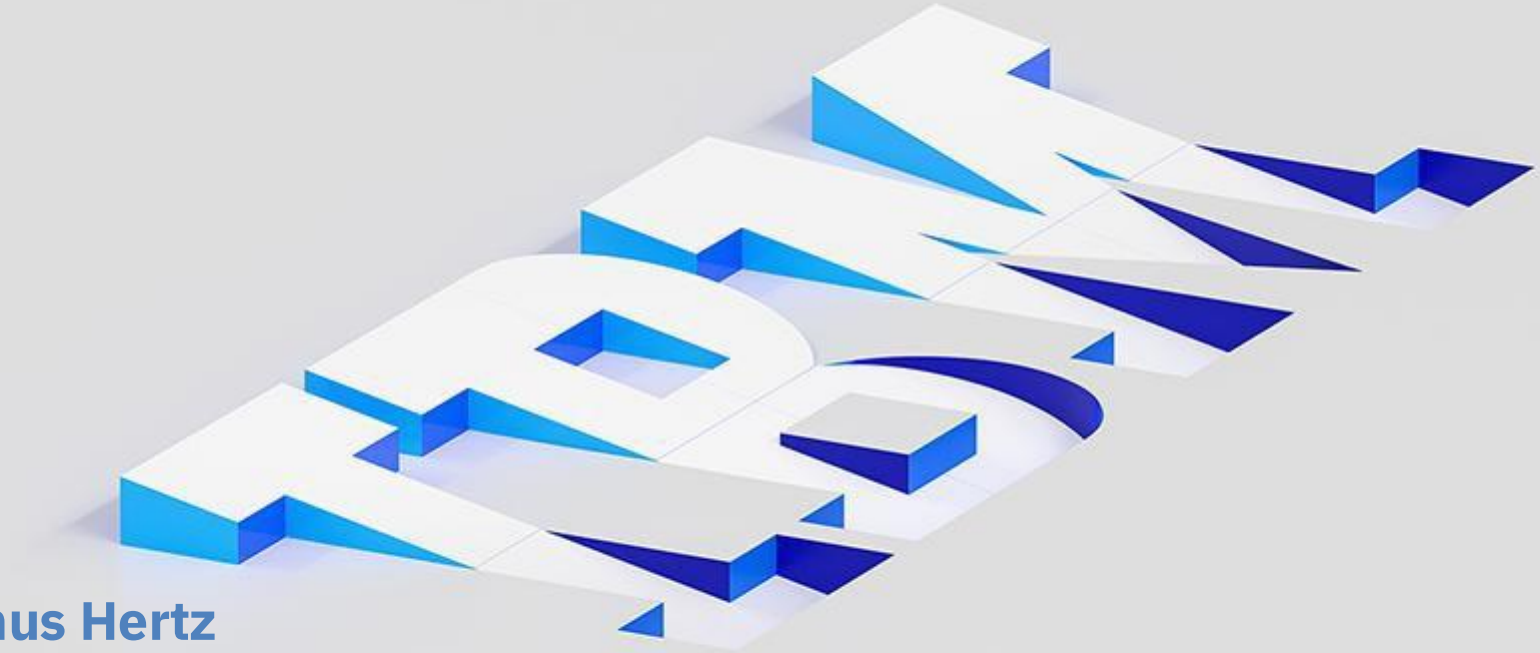
Welcome to Lyon, France and the 2026 Common Europe Congress

Session: Ransomware and IBM i

Ransomware and IBM i



Janus Hertz
Senior Consultant – IBM Power / IBM i - Security, HA/DR, Virtualization
IBM Expert Labs – Northern Europe
Janus.Hertz@dk.ibm.com

Acknowledgement to: Robert D. Andrews, IBM Expert Labs US

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. **No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.** IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

What is Ransomware?

Ransomware is malware (virus) that infects PCs and encrypts files to block access without paying a ransom

- When paid, attacker provides decryption program and key (maybe?)
  - IBM, as well as others, do NOT recommend paying ransom!
  - Encourages future attacks (since you paid!) and may be illegal in certain countries
- Double extortion not only encrypts but exfiltrates and then threatens to release data publicly if not paid
- Triple extortion threatens to DDoS (Distributed Denial of Service) attack your internet connections if not paid

Most infections come from opening email attachments or social engineering employees

Will not only encrypt local PC files but any connected network storage (file shares) - **This is the risk to the IBM i**

Quickly isolating and disconnecting infected PCs will help save IT resources

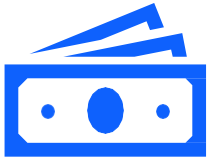
- Need XDR (eXtended Detection and Response) on end user devices - Auto Quarantine infected systems

Ransomware Over Time

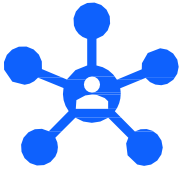
Data Encryption

Data Theft

Extortion / Blackmail



DDoS

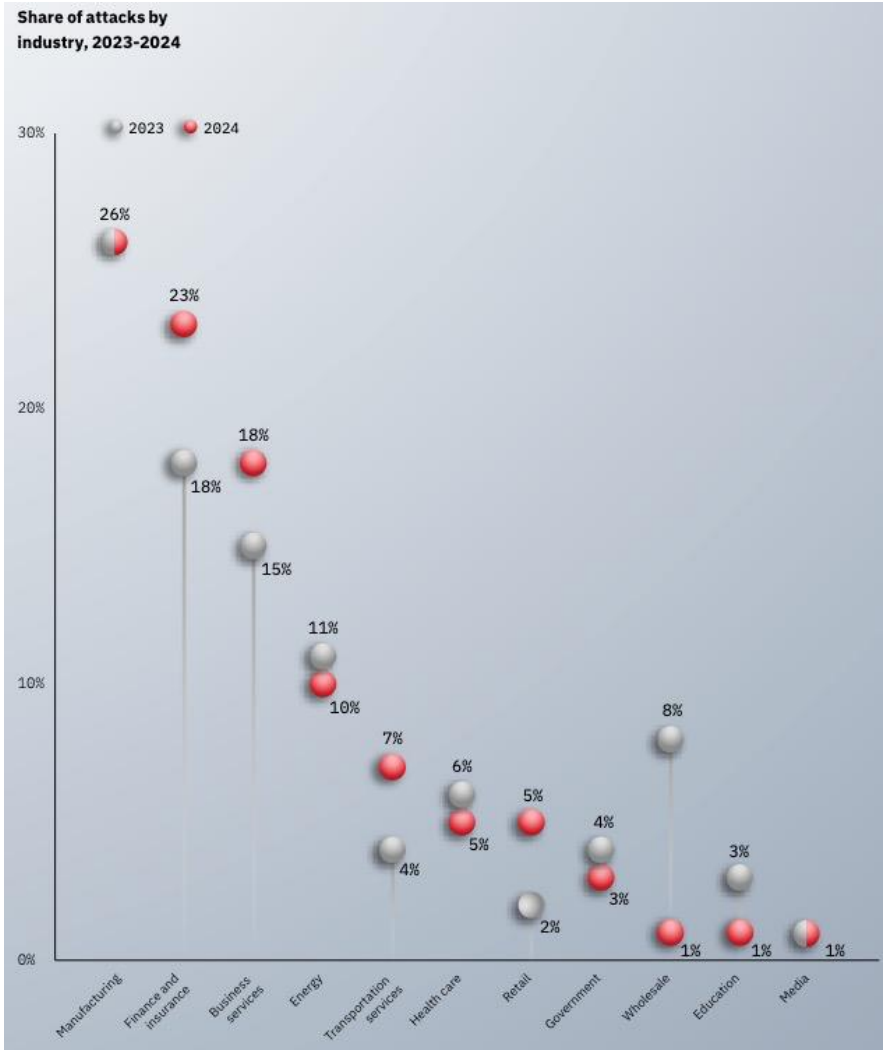


RaaS

Extortion has become the top cybersecurity impact

More than a quarter of incidents involved **extortion**, making it the **top impact** observed from cyberattacks. Cybercriminals are adopting techniques with high psychological impact to force victims to pay, and often target the most vulnerable industries, businesses and regions.

Extortion cases were most frequently achieved through **ransomware** or **business email compromise** attacks. This typically involves threatening to publish a victim's personal data—or permanently block access to it—coupled with a demand for money or some other response in return for stopping or remediating the attack.



Source: X-Force Threat Intelligence Index 2025

More attackers stole data (18%) than encrypted and, in most cases, extorted victim organizations (12%) last year as advanced detection technologies, recovery options, and increased law enforcement efforts pressure attackers to pivot to faster exit options

Source: X-Force Threat Intelligence Index 2025

Recovering from Ransomware

Have a complete and tested backup methodology on all storage systems!

- Easiest way to recover from ransomware is to wipe and restore data
  - Do not pay – no guarantee the attacker will actually provide a working decryption mechanism
  - Some decrypters have been so slow even if paid that recovery time is too long
  - Need to wipe entire system to remove any hiding copies of future malware
- Use a network-based file storage with versioning
  - Multiple prior copies of files – need more than one version – multiple versions may be encrypted
- Consider using immutable backup technology, such as IBM Safeguarded Copy
  - Backups that can not be altered, changed, or deleted after they are taken

Average cost of a data breach in the US:

USD 9.48 M

Average cost of a ransomware attack – not including the ransom itself:

USD 5.13 M

Time to detect and contain ransomware:

273 days

Source: Cost of a Data Breach Report 2023, IBM

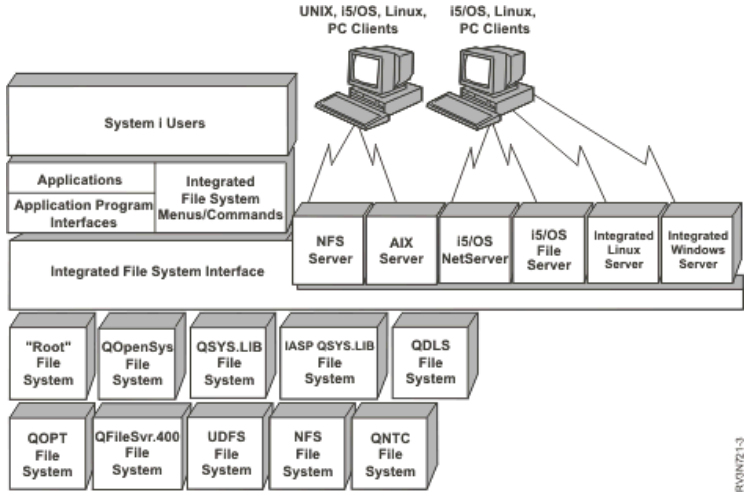
IFS Refresher

All storage segments accessible to the IBM i are part of one “Integrated File System” or IFS

- IBM i supports many different types of file systems, each with their own rules and properties and exist off of the “root” of the IFS

These file systems include:

- The “root” file system (folders and files off ‘/’ like ‘/www’)
- Library file system (QSYS.LIB) and IASP QSYS.LIB(s)
- Open systems file system (QOpenSys)
- Document library services file system (QDLS)
- Optical file system (QOPT)
- IBM i NetClient file system (QNTC) – points to Windows Shares
- IBM i file server file system (QFileSvr.400) – points to other IBM i’s
- Network File System (NFS) mounts – points to external NFS exports
- User-defined file systems (UDFSs)



Security Refresher

All file/storage objects have a set of permissions – five object level and five data level authorities

“Shortcuts” exist for common combinations – different names if dealing with QSYS objects or IFS files

	Authority	*ALL	*CHANGE	*USE	*EXCLUDE	*RWX	*RW	*RX	*R	*WX	*W	*X
Object Authorities	*OBJOPR	X	X	X		X	X	X	X	X	X	X
	*OBJMGT	X										
	*OBJEXIST	X										
	*OBJALTER	X										
	*OBJREF	X										
Data Authorities	*READ	X	X	X		X	X	X	X			
	*ADD	X	X			X	X			X	X	
	*UPD	X	X			X	X			X	X	
	*DLT	X	X			X	X			X	X	
	*EXECUTE	X	X	X		X		X		X		X
		QSYS Objects			Both	IFS Directories and Files						

Authority Flow Chart

There is a common flow in which authority is checked

Continues down flow using short circuit logic exiting if:

- Authority needed it found
- User/group is explicitly *EXCLUDEd

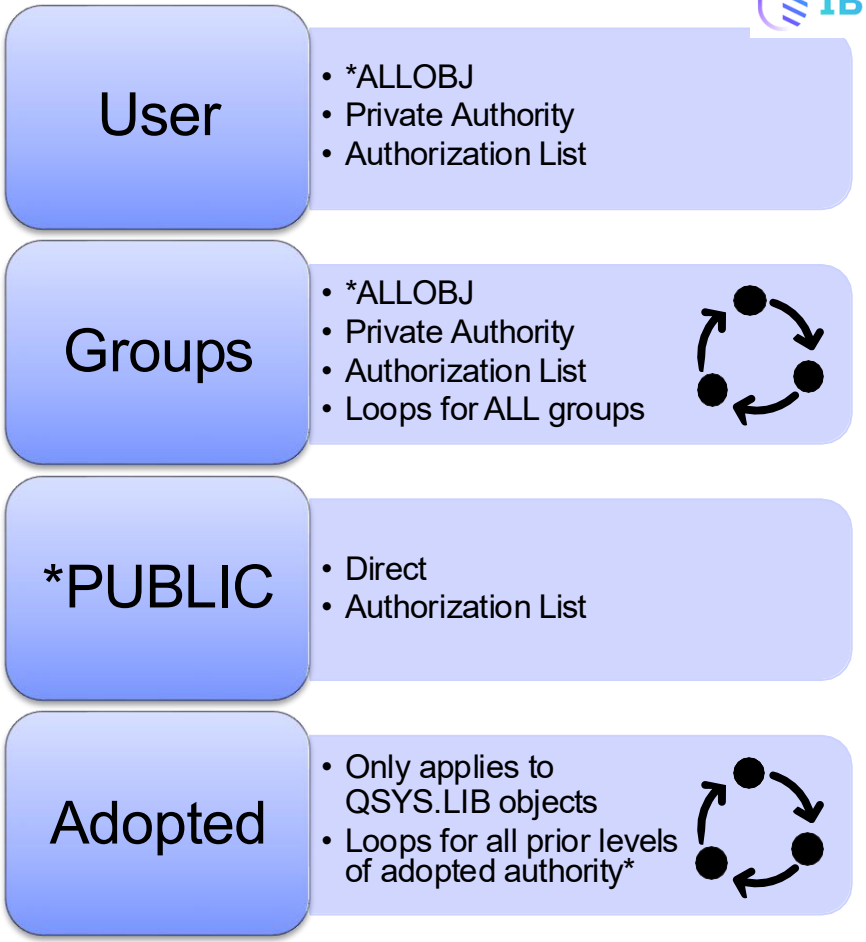
First checks user/private authority

Next checks each groups' authority

Then checks *PUBLIC's authority

Finally checks adopted authority

- Only applies to QSYS.LIB



*Unless *Use Adopted Authority* is set to *NO to prevent previous levels of adoption to be honored – current level is still honored based on *User Profile* parameter of *USER or *OWNER

Ransomware and IBM i

No currently known ransomware runs directly on the IBM i

However, the IBM i can host file storage for other network accessible PCs and Servers

- This includes byte stream files (IFS) and IBM i Library Objects

If a PC is infected and has access to IBM i, it can both exfiltrate and encrypt files stored on the IBM i

- This includes anything accessible from the network, even QSYS.LIB objects!

The risk to the IBM i is proportional to the number of objects accessible from the PC via the network

- Network access is most often done via NetServer/SMB (Server Message Block) or NFS (Network File System)

Objects should be secured at the OS layer – provides protection across ALL interfaces of IBM i

Further, limit network access (SMB and NFS) to only expose required items to PCs and network.

Limit Access to Data

IBM fully recommends following the **Principal of Least Privilege** (PoLP) – limiting users to only what they need for business purposes and denying everything else by default

- Limit *CHANGE (add/update/delete) ability and *USE (read) ability to specific users or groups
- Or use adopted authority/swapped profiles so end users have no direct authority to objects
- *PUBLIC should be *EXCLUDE – should not get access just because account exists

Removing *CHANGE/*W from libraries, objects, directories, and files prevents changes – including **encryption**

Removing *USE/*R from libraries, objects, directories, and files prevents reading – including **exfiltration**

Removing Object Operational/*X from libraries, objects, directories, and files prevents listing – leaking knowledge

These efforts will provide protection across all of IBM i and is a core “**best practice of security**”

Risks from SMB

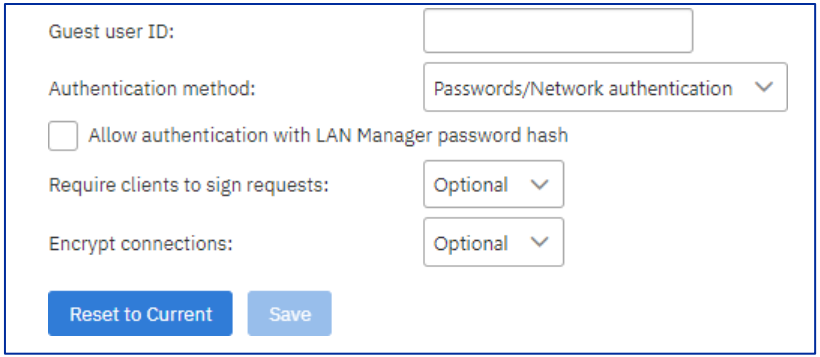
The most common form of network access to IBM i is *NetServer*, which uses SMB under the covers

- Allows shares to be mapped from the IBM i to Windows PC drive letters (“I:\ drive”)

NetServer needs to be properly secured – setup via Navigator

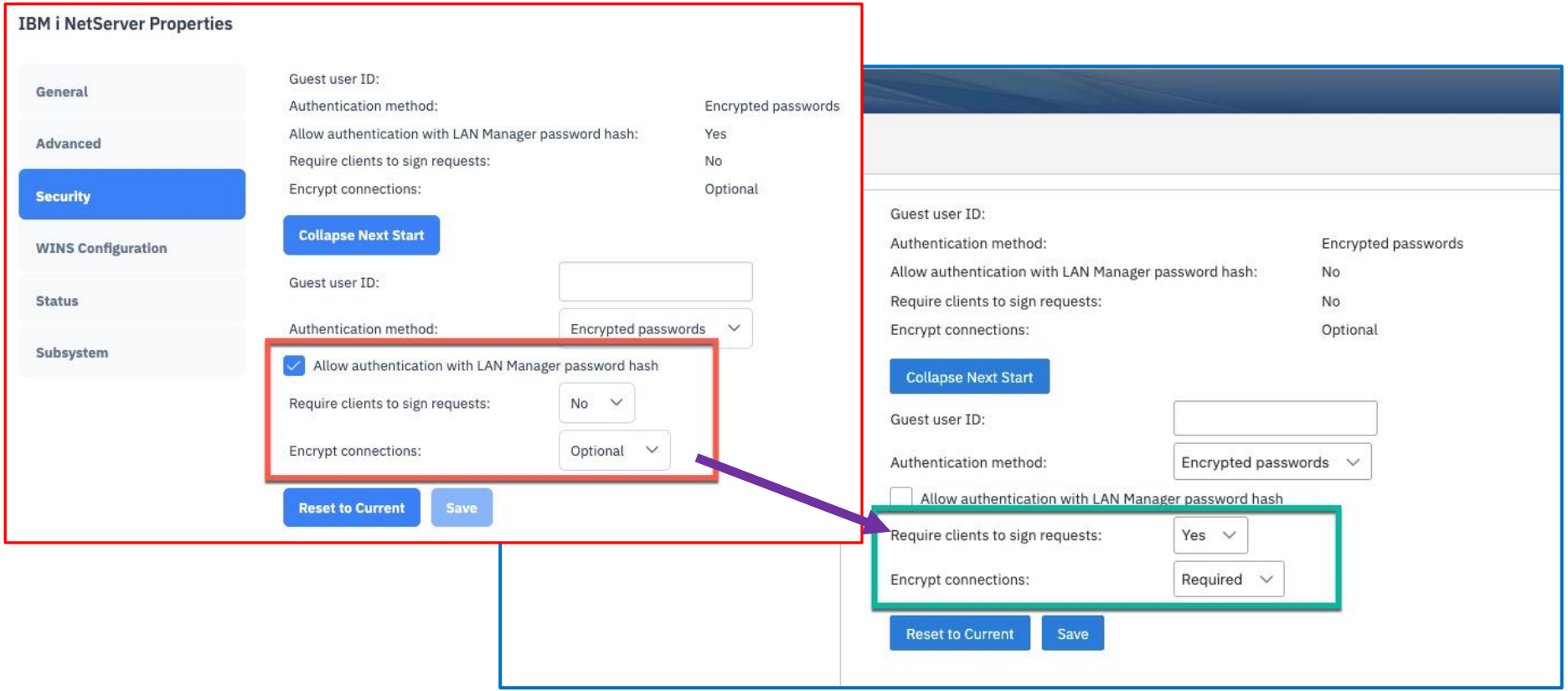
NetServer allows a GUEST account – access is provided as the GUEST user if no credentials are provided.

- This is a major risk – allows **anonymous** access to data with no user profile or password, not traceable
- Do NOT enable GUEST Support on NetServer!
- Remove the account and make it blank!
- Restart NetServer to activate changes



IBM i NetServer Access & Microsoft SMB protocol

- How to configure require encrypted connections and signed requests via IBM i Navigator:



 Technote on SMB v.1,2 & 3: https://www.ibm.com/support/pages/ibm-i-netserver-smb-protocol-version-control-guide

Eliminate Shares and Files Exposed

Look at the list of current file shares from NetServer from Navigator – remove any old or unused shares

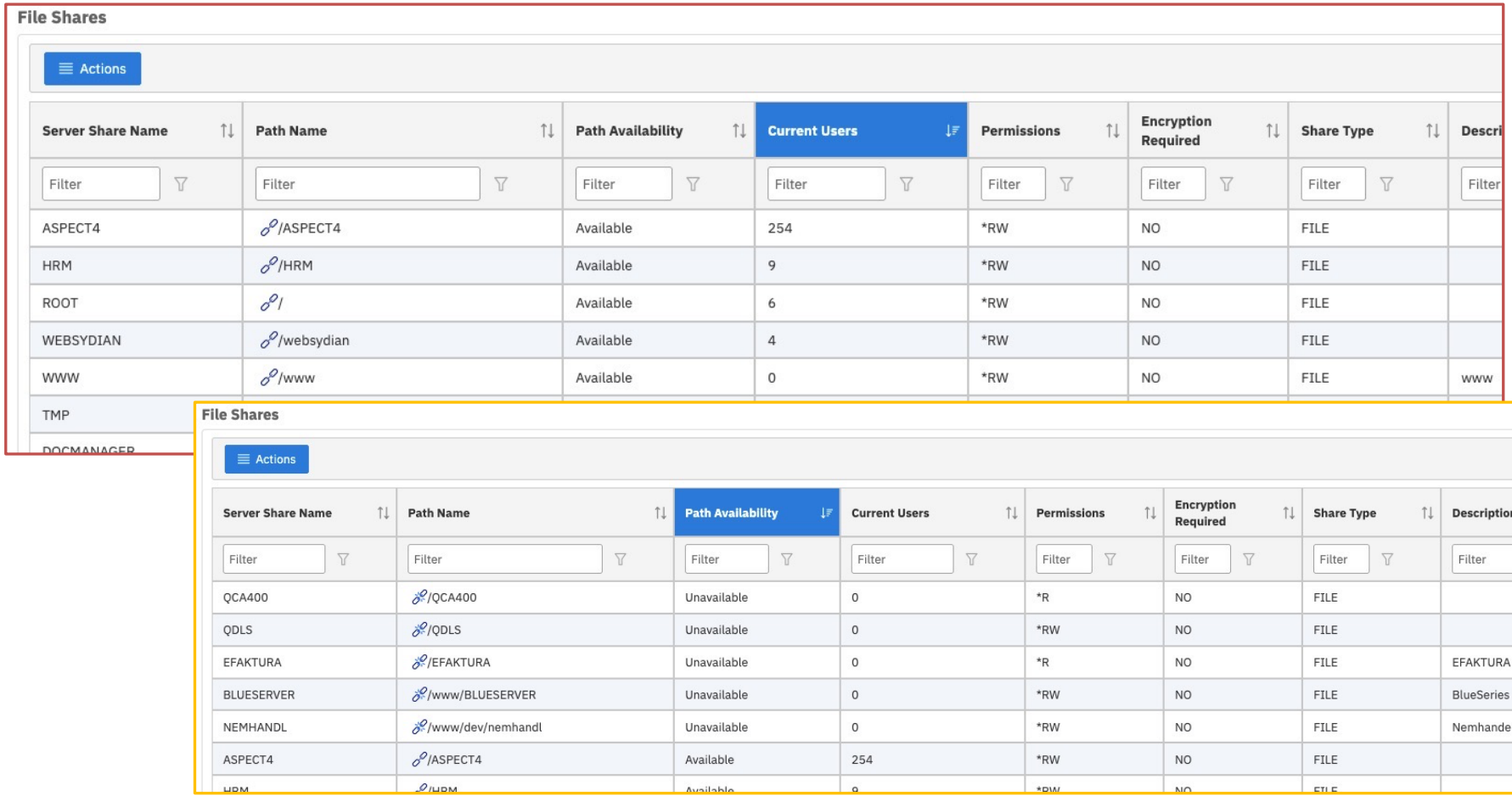
Look at remaining shares and see if they are at the “lowest” level possible path

- If /app has /app/PDFs and only the PDFs are needed on PCs, make the share at /app/PDFs and not /app
- If the share is at /app because there are multiple subfolders that need to be access, but some files should not, then it is better to create multiple “smaller” shares than one “larger” one that exposes too much to PCs
    - Given folder /app with sub-folders /app/PDFs, /app/Export, and /app/HelpDocs, if only PDFs and Export need to be accessed on PCs, do not share /app but rather create two shares – one for /app/PDFs and a second for /app/Exports – protects the /app/HelpDocs folder from being exposed to the network

Shares can be set to Read Only access – overrides object level Write authority

- Does NOT provide Read access if the OS is blocking - *EXCLUDE
- Only adds restrictions to higher levels of authority – prevents **encryption!**

IBM i NetServer shares: Used and unavailable shares



File Shares

Actions

Server Share Name	Path Name	Path Availability	Current Users	Permissions	Encryption Required	Share Type	Descri
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
ASPECT4	/ASPECT4	Available	254	*RW	NO	FILE	
HRM	/HRM	Available	9	*RW	NO	FILE	
ROOT	/	Available	6	*RW	NO	FILE	
WEBSYDIAN	/websydian	Available	4	*RW	NO	FILE	
WWW	/www	Available	0	*RW	NO	FILE	www
TMP							
DOCMANAGER							

File Shares

Actions

Server Share Name	Path Name	Path Availability	Current Users	Permissions	Encryption Required	Share Type	Description
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
QCA400	/QCA400	Unavailable	0	*R	NO	FILE	
QDLS	/QDLS	Unavailable	0	*RW	NO	FILE	
EFAKTURA	/EFAKTURA	Unavailable	0	*R	NO	FILE	EFAKTURA
BLUESERVER	/www/BLUESERVER	Unavailable	0	*RW	NO	FILE	BlueSeries PC Client server po
NEMHANDL	/www/dev/nemhandl	Unavailable	0	*RW	NO	FILE	Nemhandel - Webservices
ASPECT4	/ASPECT4	Available	254	*RW	NO	FILE	
HRM	/HRM	Available	9	*RW	NO	FILE	

IBM i NetServer – Root share usage

- Root share MUST be removed!
- Replace with more target shares - only share as little as possible and in “read only” mode if possible!

ROOT Properties

Actions

Workstation Name	Session ID	User Name	Time Active	Time Idle	Number of connections	Number of files opened	Used guest user for logon
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
::ffff:192.1[redacted]	20647612	EX[redacted]	8134	313	1	2	No
::ffff:172.2[redacted]	17778874	W[redacted]	6056745	9	2	2	No
::ffff:172.2[redacted]	20636309	ED[redacted]	27738	550	2	4	No
::ffff:172.2[redacted]	20510349	ED[redacted]	283315	0	3	93	No
::ffff:10.10[redacted]	20651882	AS[redacted]	11	11	1	1	No
::ffff:172.2[redacted]	20651873	AS[redacted]	15	14	1	1	No
::ffff:10.10[redacted]	20651881	AS[redacted]	11	11	1	2	No
::ffff:10.10[redacted]	20651876	AS[redacted]	15	14	1	2	No
::ffff:172.2[redacted]	20651878	m[redacted]	14	8	1	1	No
::ffff:10.10[redacted]	20651880	AS[redacted]	11	9	1	1	No

« ‹ 1 › » 100

Never Share the IFS Root - /

NO. STOP. DON'T DO IT.

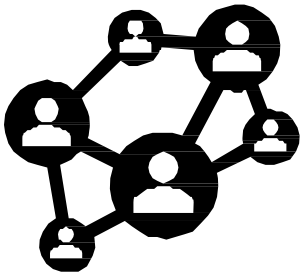
You would never share an entire OS drive on a Windows Server…

– Don't share your entire IBM i (OS, Data, files, etc.)!

- Exposes the IBM i Operating System and critical objects that have no value in being shared and **creates risk**
- Can cascade the **risks to other IBM i** or **Windows Servers** by exposing them too
- Sharing the root shares /QFileSvr.400/ (links to other IBM i) and /QNTC/ (links to Windows Server)
  It seems like a quick and easy solution, but the risk is **monumental**

DO NOT SHARE THE IFS ROOT /

Seriously. Don't. Okay?



QPWFSERVER Authorization List

/QSYS.LIB contains the IBM i OS, all Libraries, and Library objects…. and can be shared to the network

- Objects can be read, but also changed, corrupted, and encrypted

The QPWFSERVER authorization list secures access to the QSYS.LIB file system via NetServer

- Acts as a gatekeeper at the /QSYS.LIB directory in file server and IBM i NetServer jobs
- Prevents IBM i Access, IBM i NetServer, Java Toolbox, File Server and others from entering /QSYS.LIB
- Does NOT prevent access by other mechanisms (e.g. FTP, SSH, etc.)
  Default is *PUBLIC *USE but can be changed to *PUBLIC *EXCLUDE via EDTAUTL
- Requires explicit permission if need to access QSYS.LIB via shares (or *ALLOBJ Special Authority)

Also secures access to the independent ASP (iASP) QSYS.LIB file systems

Does NOT grant object level access if the user profile does not already have it – this is one additional check

NetServer and Share Level Authorization Lists

IBM i 7.5 (and later) now allows a server-level and share-level authorization list to be defined

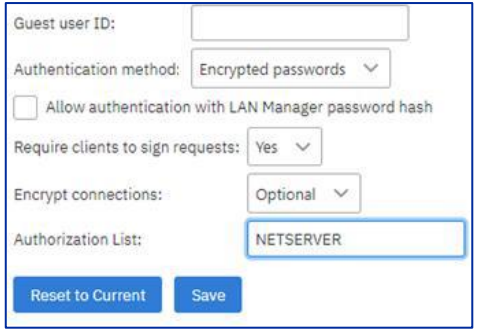
First, can create an optional Authorization List at the Server level – needed if accessing ANY share

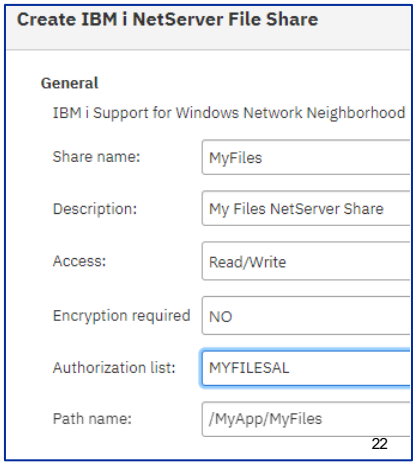
- Need *USE or higher to server-level authorization list to use any NetServer share
- Need to restart NetServer to pick changes made to the auth list name (not the contents of the auth list)

Second, can create an optional Authorization List at the Share level – needed if accessing that specific share

- Need *CHANGE or higher to share-level auth list for read/write access to share
- Need *USE for read only access to the share
- Again, does not grant additional authority
  - Need access at OS object level as well

These are optional – can run without, which is the default





IBM i NetServer *AUTL Server and Share Security

- Extra layer of security for either the server or on a share.
  - Does NOT replace normal security of using permissions on objects.

- Individual Users Can Be Restricted From Server Access.
  - User can be:
    - Allowed to access the server (*USE or greater).
    - Not allowed to access to the server (*less than *USE or *EXCLUDE).
  - Configured:
    - New Navigator IBM i NetServer properties.
    - GO NETS tool – server configuration.
    - IBM i NetServer APIs.

- Individual Users Can Be Restricted From Share Access.
  - User can be:
    - Allowed full access (*CHANGE or greater).
    - Restricted to read-only access for a share defined as read/write (*USE).
    - Not allowed any access to the share (less than *USE or *EXCLUDE).
  - Configured:
    - New Navigator IBM i NetServer share properties.
    - GO NETS tool – share properties.
    - IBM i NetServer APIs.

IBM i NetServer *AUTL Server and Share Security

- **ALLOBJ special authority overrides *AUTL permission.*
- Most restrictive permission is used permission.
  - Example: User A has *RW authorization to the *AUTL, but only *R to actual object.
    - User A will have *R authority to object.
- [New in 7.6] Authority Requirements Change for Shares
  - Additional authority is required to create, modify, or remove IBM i NetServer shares.
  - Need either *IOSYSCFG special authority OR authorization to the QIBM_QZLS_NETSVR_SHARE function usage identifier and ownership.
  - Just being object owner is no longer authority sufficient.

[New in 7.6] NetServer Audit Records

- **New NetServer Audit Records**
  - VP-U for guest / invalid user attempts.
  - VP-C and VP-E for start / end of session and share connections.
  - VP-S to log share changes.

- **Enabling New NetServer Audit Records**
  - *NETFAIL – A(uthorization list failure), D(isabled profile), P(assword invalid), and U
  - *NETBAS – S
  - *NETSMBSVR – C and E

- IBM i Documentation for more information
  https://www.ibm.com/docs/en/i/7.6.0?topic=netserver-using-i-auditing

NetServer File Exit Point

QIBM_QPWFS_FILE_SERV can be used to log or restrict what clients are allowed to do over the File Host Server

Two different formats – triggered by file open, create, delete, move, copy, rename, change file attributes, list file attributes, or allocate a conversation

Exit program is passed the User, Operation requested, Access requested, and File name for the operation

- Exit program can reject the request – can create very fine grain control over sensitive files
- Exit program called for IBM i Access, IBM i NetServer, Java Toolbox, and QFileSvr.400 accesses

IBM provides the hook (exit point), client must provide or purchase the program that provides the logic and protection

Network File System - NFS

The concepts for NFS are the same as NetServer/SMB, but the execution of them is slightly different

Do not allow anonymous (guest) access to NFS

- Set per NFS export (share), not at server level as it is in NetServer, by using the **ANON=-1** option for each export

Limit exposed files: remove old/unused exports, export the farthest down the path as possible, limit files exported, make sure only files/folders to be exposed are exported and nothing more.

Set the export to Read Only, if the business needs allow, by using the **RO** option for each export

Do not export the IFS Root / – see prior conversation

There are no authorization lists or exit points to help limit NFS access like there are for NetServer

Filtering Network (SMB and NFS) Access

Setting a share/export to Read Only (*R/-RO) **FILTERS** the end user's underlying authority to the object when accessed via NetServer (SMB) or NFS – has no effect on access via any other method

This **NEVER** grants any user additional authority – only **RESTRICTS** the authority they already have

- Sets the highest-level access – removes the ability to write or even read via NetServer (SMB) or NFS only

Same concept with QPWFSERVER

- **FILTERS** access to /QSYS.LIB/ when accessed via NetServer (SMB) only

Setting a share/export as Read/Write or adding a user in QPWDSERVER does NOT grant users access the objects

- Just does not apply any additional filters beyond normal IBM i authority checking (see Authority Flow Chart)

Protect the IFS Root - /

IFS root (/) shipped with *PUBLIC *ALL – done to make everything work for everyone by default...

- *RX – allows applications to navigate, *W – allows objects to get created, *OBJMGT, *OBJEXIST – needed for UNIX apps, *ALTER, *REF – unused but without is ‘user-defined’
- Folders created off the root inherit *PUBLIC *RWX rights, then files created in those folders also inherit *PUBLIC *RWX rights, can quickly open a large amount of data to be *PUBLIC *RWX

Secure the IFS root (/) Directory by setting *PUBLIC to *RX after system and initial applications are installed

- Prevents creating, deleting (unlink), or renaming objects in the root (/)
- Do not set *PUBLIC *EXCLUDE on the root (/)
- This does NOT affect any existing folders or files, just newly created ones after the change
  - Can use CHGAUT with SUBTREE(*ALL) to change existing folders and files – USE CAUTION!!
- Please check with your third-party apps to see how they would be affected by this change

This is NOT specific to NetServer (SMB) or NFS access – this is a general IBM i Security recommendation!

Setting Root to *RX vs. Sharing the Root

Setting Root (/) to *RX	Sharing or Exporting the Root (/)
Applies to **ALL** access on IBM i regardless of interface (Telnet, FTP, etc.)	**ONLY** applies to NetServer or NFS access from PC if share/export exists
Applies to everyone since the IFS root always exists – to be done after general system bring up and application installation	IF you must have the IFS Root shared/exported, then it is HIGHLY recommended you set it **Read Only**
Only applies to the **root (/) itself** – no other directories, folders, files, or objects	Applies to **ALL objects** accessed via that particular share or export
IS **ALWAYS** RECOMMENDED	IS **NEVER** RECOMMENDED

Antivirus and IBM i

Since the IBM i can hold any type of binary files, those files may contain malware

- The IBM i is just file storage at this point, like a USB flash drive
- Files can get on to the IBM i storage in many ways: mapped drive, FTP, SFTP, removable media (tape, CD)

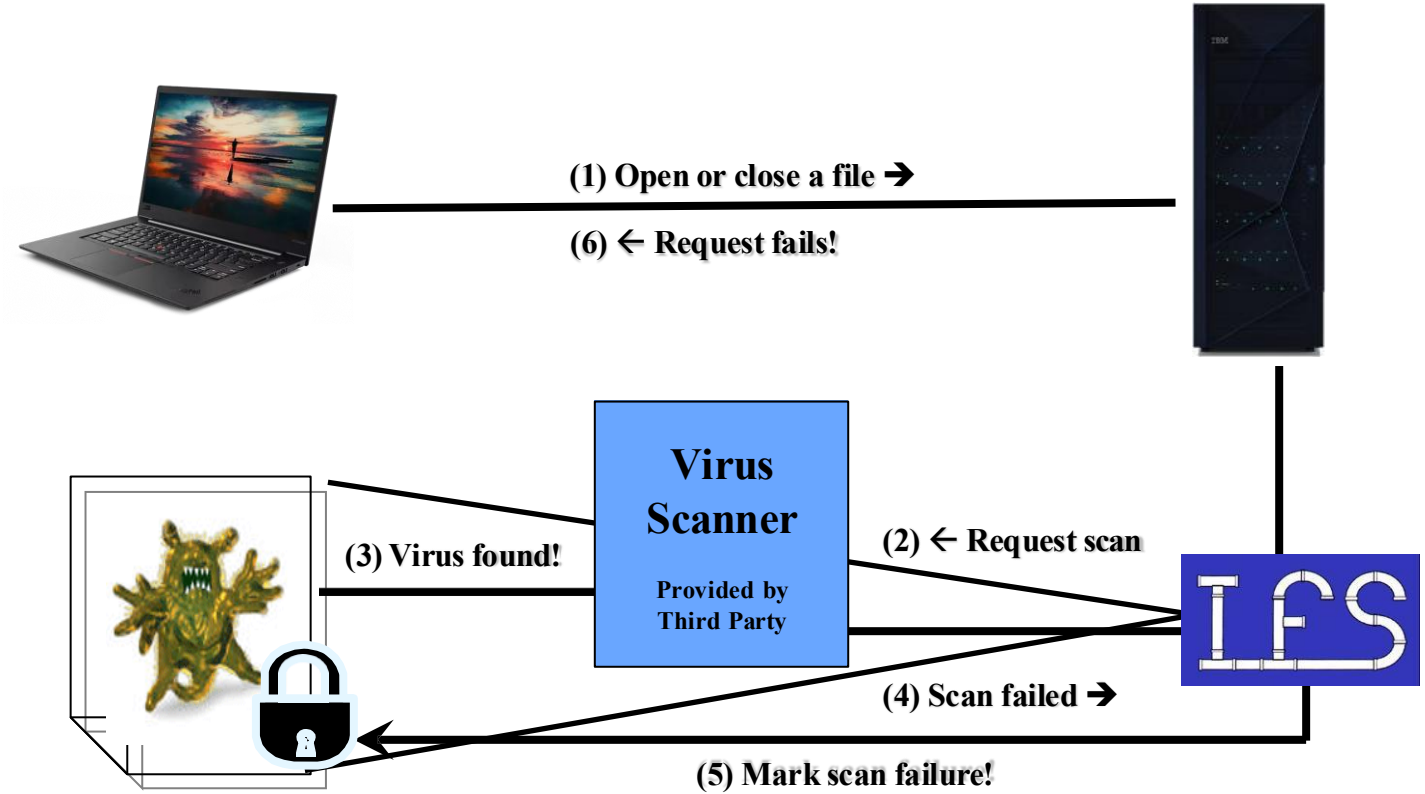
Some companies choose to run Antivirus software on the IBM i

- IBM i provides exit points to enable software to scan files on open (QIBM_QP0L_SCAN_OPEN) or close (QIBM_QP0L_SCAN_CLOSE)
- Need to provide third party scanning engine and virus definitions/signatures
- Controlled by Scan file systems (QSCANFS) and Scan file systems control (QSCANFSCTL) system values
- IBM i “remembers” scan history and only re-scans if needed (file changed, different CCSID, new scan signatures)

IBM recommends NOT using a PC based Antivirus scanner and scanning mapped drives over the network

- Slow, moves all files over the network in the clear, uses bandwidth, may go into infinite loops (symbolic links)

Antivirus and IBM i: How it Works



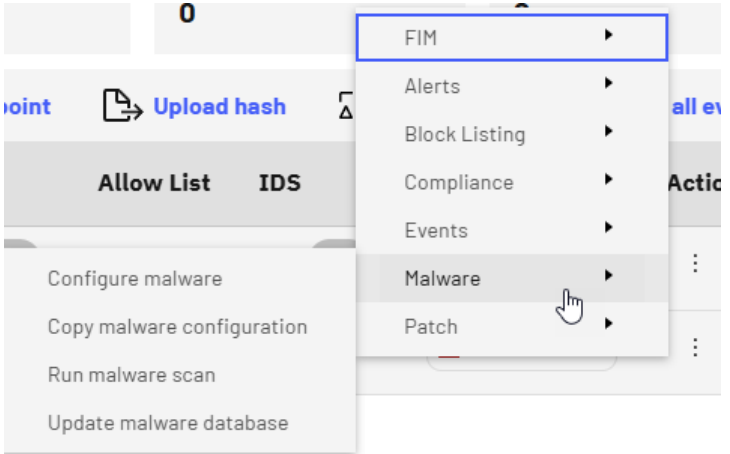
Antivirus and IBM i – Another Option

PowerSC for IBM i provides and supports a port of ClamAV for AV and AM scanning

- Needs to be installed separately from the PowerSC media
- Check Docs website for pre-req packages that must be there first

This is a scheduled based scanner that can check the IFS for malarious files

- Reports can be scheduled and emailed for security team for review
  - This is not on-demand scanner as files are accessed
- Need to use the freshclam to update signatures on a regular basis
  - Can be scheduled from PowerSC GUI



Object open and close exit points

Two new exit points are supplied in 7.5 release: QIBM_QP0L_OBJ_CLOSE & QIBM_QP0L_OBJ_OPEN

New file system attributes:

- Run exit program: Controls whether exit programs will run during open/close
- Create run exit program: Directory attribute controls value of “run exit program” for new objects

Exit program can perform application-specific processing when the object is opened or closed, such as verification, conversion, or removal of temporary objects, security logging, prevent opening, etc.

Enabled for the root, QOpenSys, user-defined, and QDLS file systems

Good Security Practices

Make sure to have an up to date and test backup and recovery methodology for all storage devices

- Consider using multiple snapshot immutable volumes

Stay current on IBM i OS release levels, PTF Groups, Technology Refreshes and other patches

Have a planned, documented, and rehearsed incident response and communication plan

Get an annual IBM i Security Assessment from an outside organization

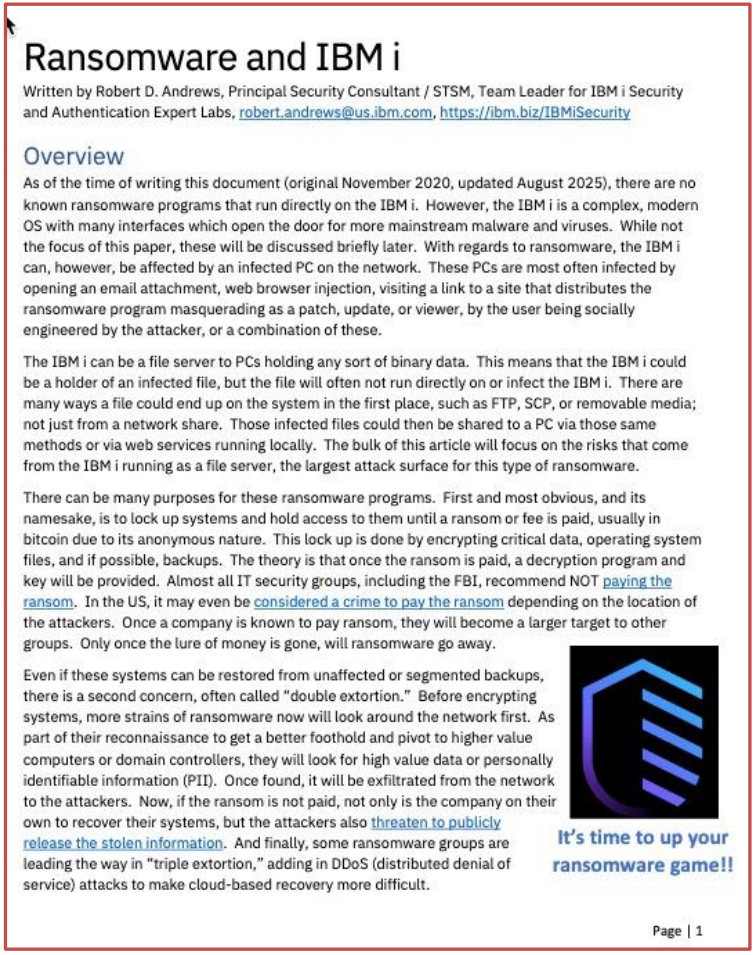
- A set of “fresh eyes” to see things the IT org may have overlooked
- Take the remediation recommendations seriously and protect the system

IT security is ultimately about the **reputation of your company**, and if your clients want to continue trusting you with their business!

Ransomware and IBM i – whitepaper

Written by:
Robert D. Andrews, IBM Expert Labs US

Download latest version:
https://ibm.biz/Ransomware-and-IBMi



Ransomware and IBM i

Written by Robert D. Andrews, Principal Security Consultant / STSM, Team Leader for IBM i Security and Authentication Expert Labs, robert.andrews@us.ibm.com, https://ibm.biz/IBMiSecurity

Overview

As of the time of writing this document (original November 2020, updated August 2025), there are no known ransomware programs that run directly on the IBM i. However, the IBM i is a complex, modern OS with many interfaces which open the door for more mainstream malware and viruses. While not the focus of this paper, these will be discussed briefly later. With regards to ransomware, the IBM i can, however, be affected by an infected PC on the network. These PCs are most often infected by opening an email attachment, web browser injection, visiting a link to a site that distributes the ransomware program masquerading as a patch, update, or viewer, by the user being socially engineered by the attacker, or a combination of these.

The IBM i can be a file server to PCs holding any sort of binary data. This means that the IBM i could be a holder of an infected file, but the file will often not run directly on or infect the IBM i. There are many ways a file could end up on the system in the first place, such as FTP, SCP, or removable media; not just from a network share. Those infected files could then be shared to a PC via those same methods or via web services running locally. The bulk of this article will focus on the risks that come from the IBM i running as a file server, the largest attack surface for this type of ransomware.

There can be many purposes for these ransomware programs. First and most obvious, and its namesake, is to lock up systems and hold access to them until a ransom or fee is paid, usually in bitcoin due to its anonymous nature. This lock up is done by encrypting critical data, operating system files, and if possible, backups. The theory is that once the ransom is paid, a decryption program and key will be provided. Almost all IT security groups, including the FBI, recommend NOT paying the ransom. In the US, it may even be considered a crime to pay the ransom depending on the location of the attackers. Once a company is known to pay ransom, they will become a larger target to other groups. Only once the lure of money is gone, will ransomware go away.

Even if these systems can be restored from unaffected or segmented backups, there is a second concern, often called "double extortion." Before encrypting systems, more strains of ransomware now will look around the network first. As part of their reconnaissance to get a better foothold and pivot to higher value computers or domain controllers, they will look for high value data or personally identifiable information (PII). Once found, it will be exfiltrated from the network to the attackers. Now, if the ransom is not paid, not only is the company on their own to recover their systems, but the attackers also threaten to publicly release the stolen information. And finally, some ransomware groups are leading the way in "triple extortion," adding in DDoS (distributed denial of service) attacks to make cloud-based recovery more difficult.

It's time to up your ransomware game!!

Page | 1

IBM i Security Technology Expert Labs

Security Services for IBM i include:

- Security Assessment
- Single Sign On Implementation
- Security Remediation
- Encryption Assistance
- Security Mentoring

IBM Technology Expert Labs:

- Simplify management and measurement of security & compliance
- Reduce the cost of security & compliance
- Improve detection and reporting of security exposures
- Improve auditing/monitoring to satisfy reporting requirements
- Guide your business toward a more secure operational model

Thank you

Janus Hertz
Senior Consultant – IBM Power / IBM i - Security, HA/DR, Virtualization
IBM Technology Expert Labs – Northern Europe

Janus.Hertz@dk.ibm.com
+45 28804749

https://ibm.biz/IBMiSecurity

Find details about all these items as well as the **Ransomware and IBM i** Security Checklist at:

https://ibm.biz/IBMiSecurity