Welcome to Lyon, France and the 2026 Common Europe Congress

Bienvenue à Lyon, en France, et au Congrès de Common Europe 2026

FORTRA

Today's Presenter

Mike Davison

Support Manager

EMEA Power Systems Support

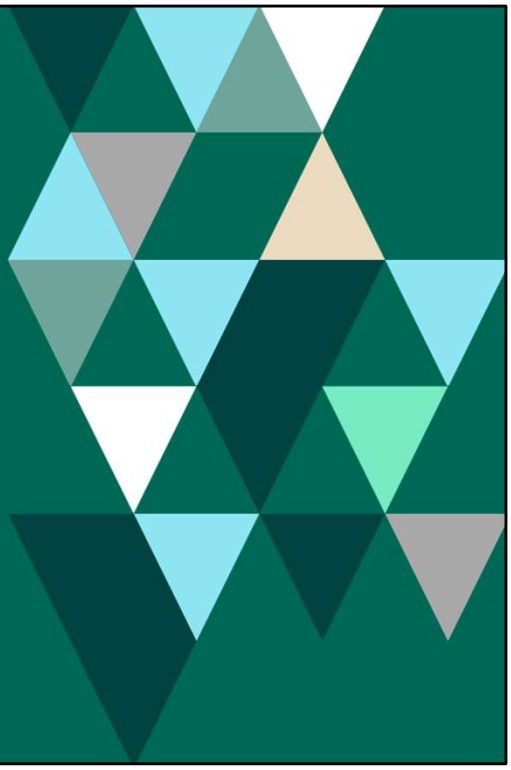
Fortra

Mike Davison has worked on IBM equipment in IT Operations since starting on the 4381 running VM/VSE as a trainee Operator in 1987. He's worked for blue-chip companies in global data centres and has a varied 30+ years' experience of IBMi, AIX, VIOS, UNIX, Linux, storage and disaster recovery. Currently a Senior Technical Consultant and the EMEA Power Systems Support Team Lead for Fortra, Mikes main role is to manage his team to provide consultancy and support for customers seeking to secure, monitor and automate their Power System operations.

FORTRA

Security Zero to Security Hero in <=30 minutes.

Protect your IBM Power i, AIX and Linux systems



FORTRA

Topics for this session

1. What are the threats?
2. Why bother?
3. Power systems can’t be infected right?
4. How to combat this?


What are the threats?

All data has value

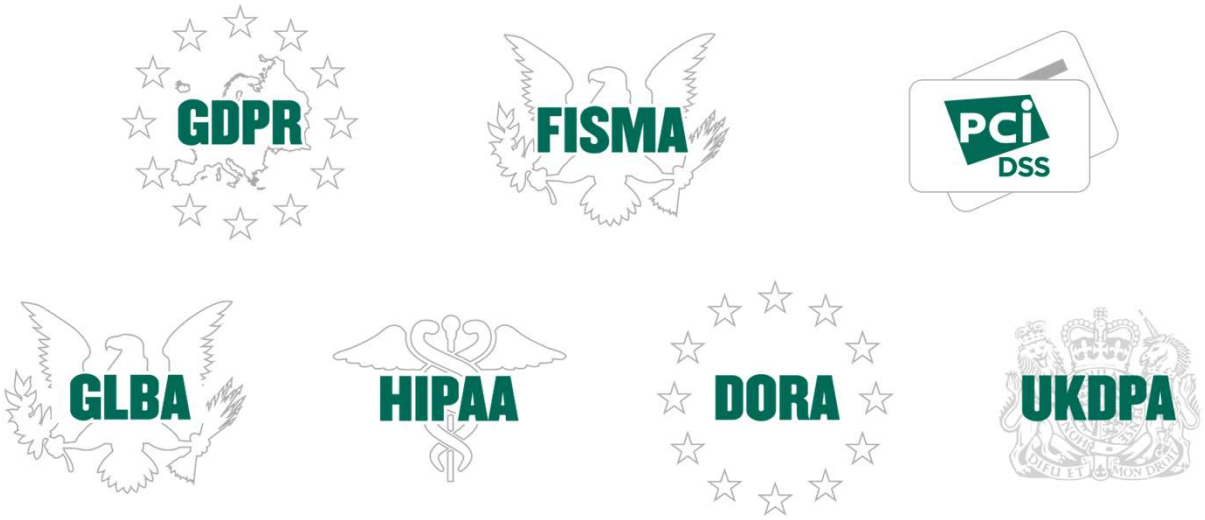
Organizations paid at least $457 million to ransomware gangs in 2022, a drop of $300 million showing an sharp decline in payments, which is reassuring that organisations are maturing in their recovery plans.

Source: https://www.techtarget.com/searchsecurity/news/252529391/Chainalysis-Ransomware-payments-down-fewer-victims-paying


Why bother?

FORTRA

Regulatory requirements



Source: https://www.ibm.com/security/data-breach

UK Data Protection Act

European Union General Data Protection Regulation (GDPR)

EU Digital Operational Resilience Act (DORA)

Payment Card Industry Data Security Standard (PCI-DSS)

Health Insurance Portability and Accountability Act (HIPAA)

Federal Information Security Management Act (FISMA)

Gramm-Leach-Bliley Act (GLBA)

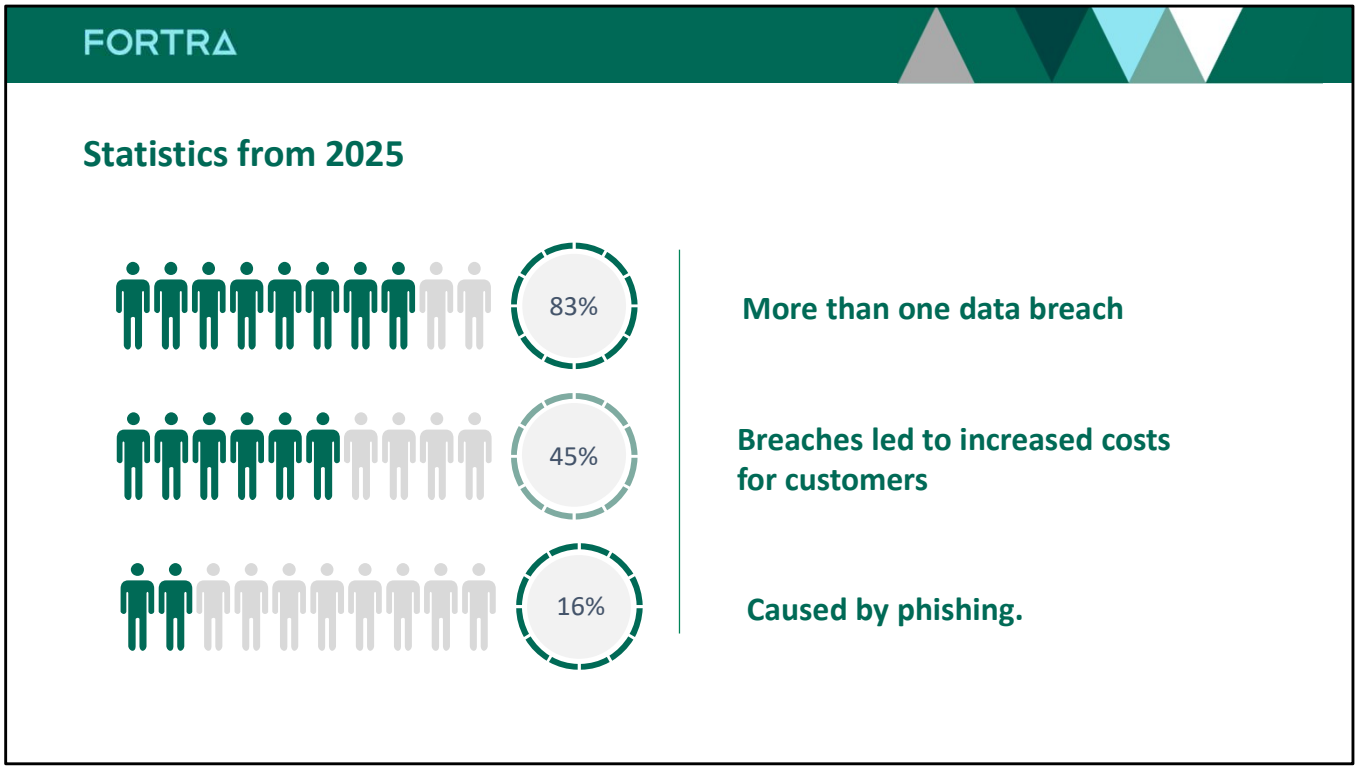
FORTRA

The penalties can be severe.

Vodafone, Greece	550,000 €
LastPass UK Ltd, UK	1,400,000 €
Nexpublica, France	1,700,000 €
S-Pankki Oyj, Finland	1,800,000 €
ING Bank Śląski, Poland	4,323,250 €
Telecoms Operator, Croatia	4,500,000 €
Capita PLC, UK	9,180,000 €
Aena, S.M.E., S.A., Spain	10,043,002 €
British Airways, UK	20,000,000 €

Not only loss of revenue, loss of reputation, loss of stock value, etc….

Source: https://www.enforcementtracker.com/



In 2022 83% of organisations reporting have had more than one data breach

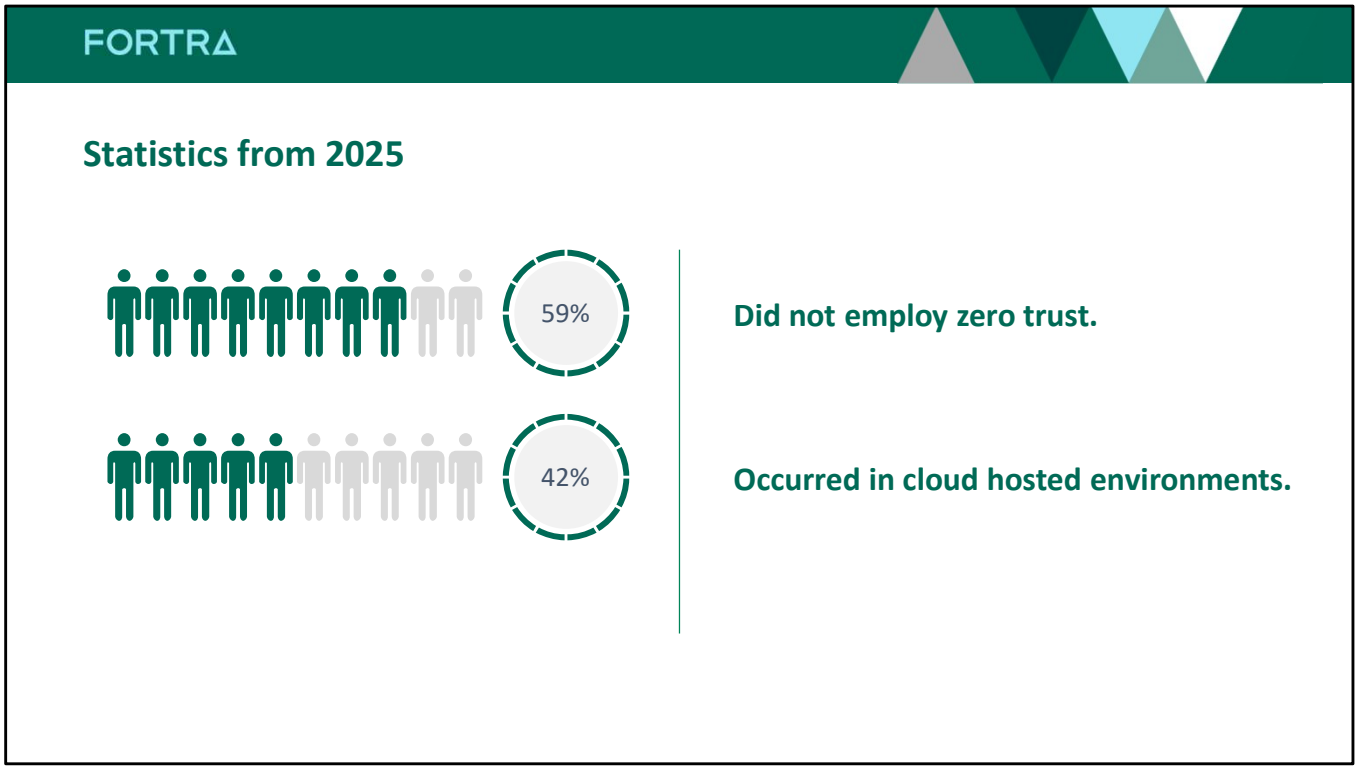
Of these, 45% led to increases in prices passed on to customers.

19% of breaches occurred due to stolen or compromised credentials.

Credential breaches have the longest lifecycle because threat actors will linger in the system so they can gain the maximum value.

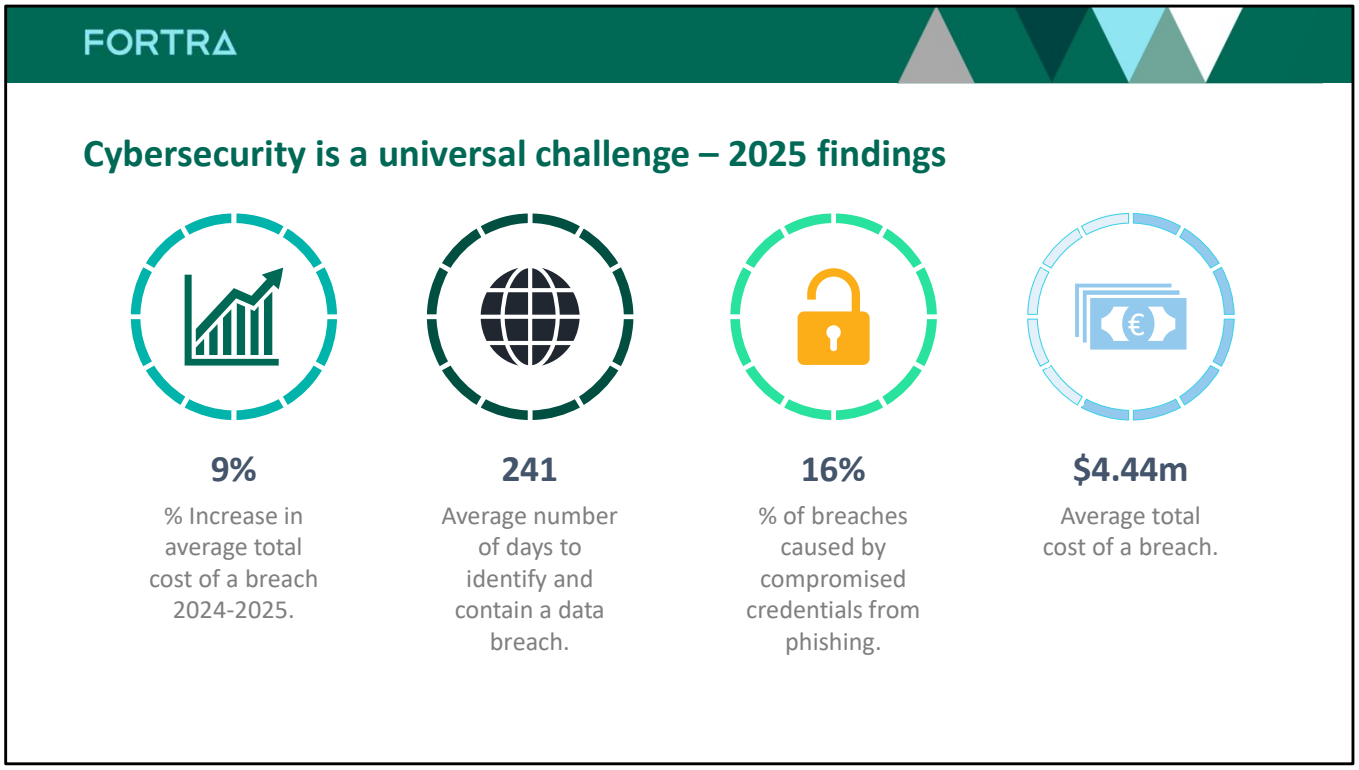
Phishing came a close second at 16%

Source: https://www.ibm.com/reports/data-breach



59% don’t deploy zero trust and it costs an additional $1 million USD per breach in costs.

42% occurred in public cloud based environments (private, public and hybrid)



Source: https://www.ibm.com/security/data-breach

9% increase in 2024 costs.

Average days to identify and contain, down from 292 in 2024 to 241

Credential breaches down by 1%

Average cost is down from 4.88 Million USD to 4.44 Million USD


Power systems can’t be infected right?

FORTRA

IBM i

A traditional x86 virus will **not infect** an IBM i native object,

for example; an RPG Program, Physical File, Query Definition.

We **mistakenly** read that as “no virus possible!”

IBM has **never** claimed that the IBM i IFS was **immune**.

As proof, IBM i received **integrated anti-virus** controls in V5R3 (2004)

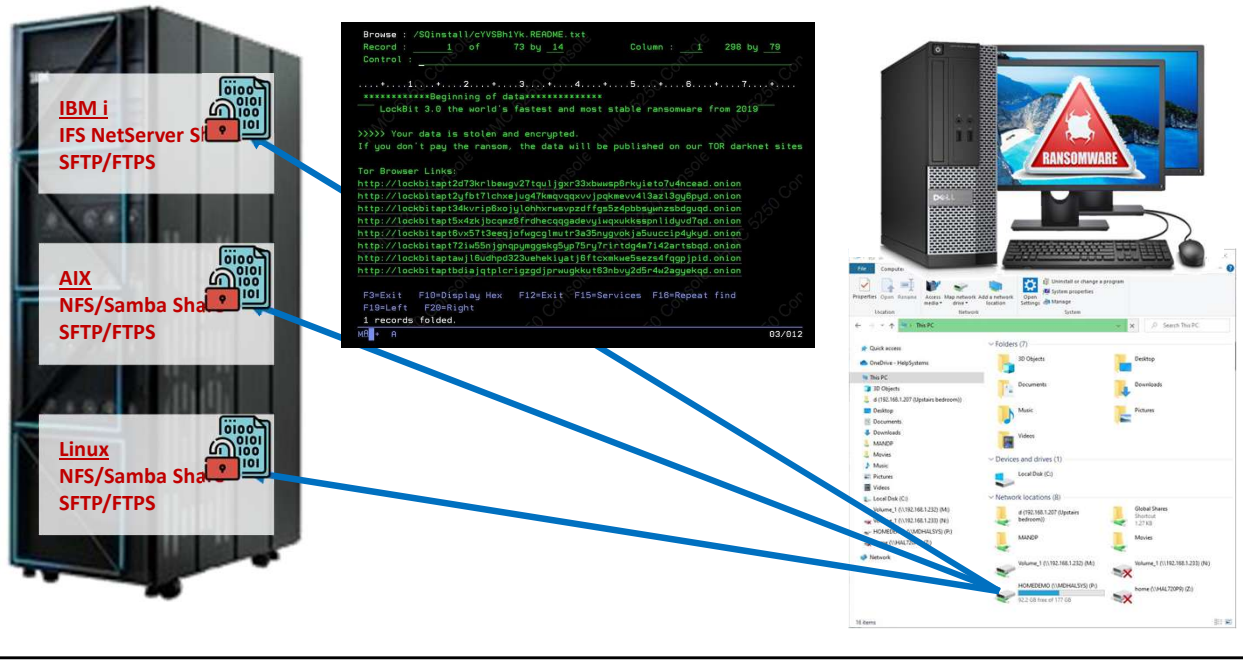
Look at:

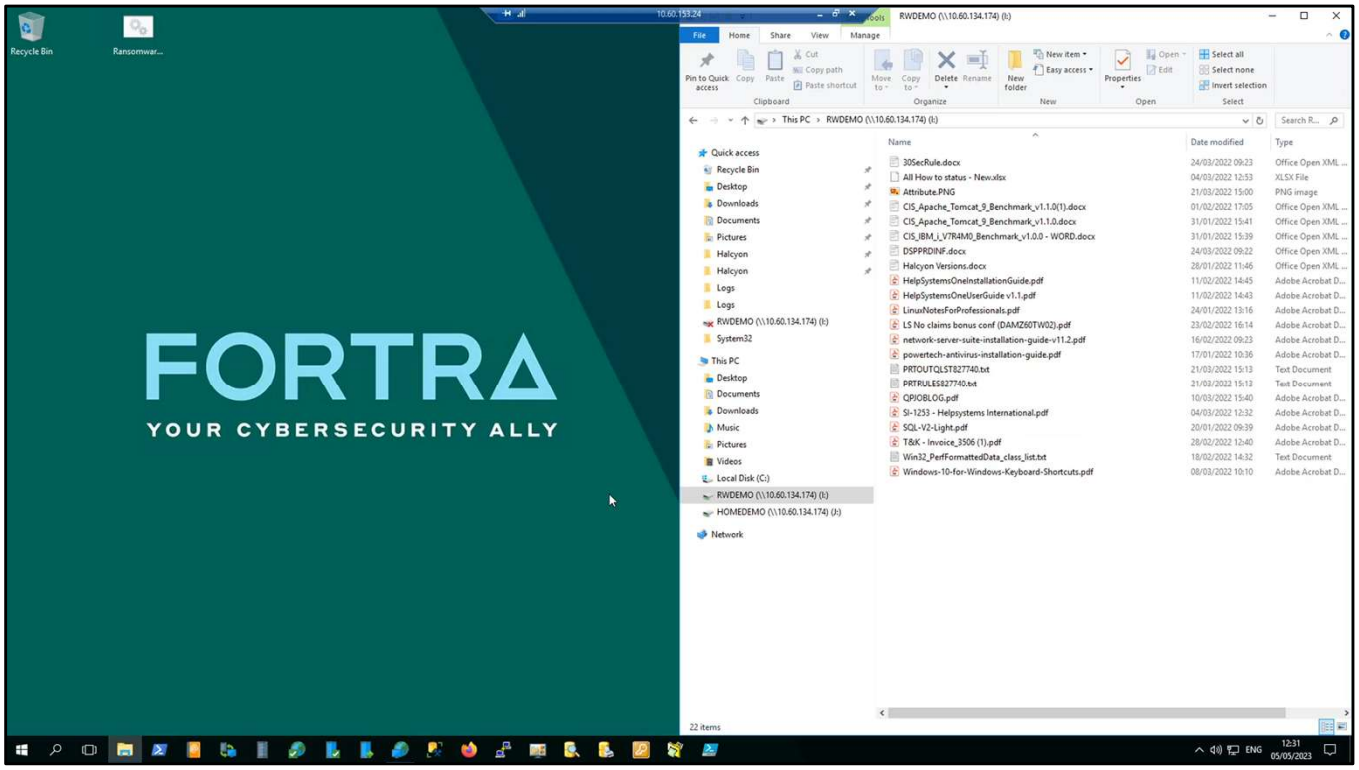
System values:
QSCANFS controls if virus scanning is enabled (default is ON).
QSCANFSCTL provides options to tune scanning performance.

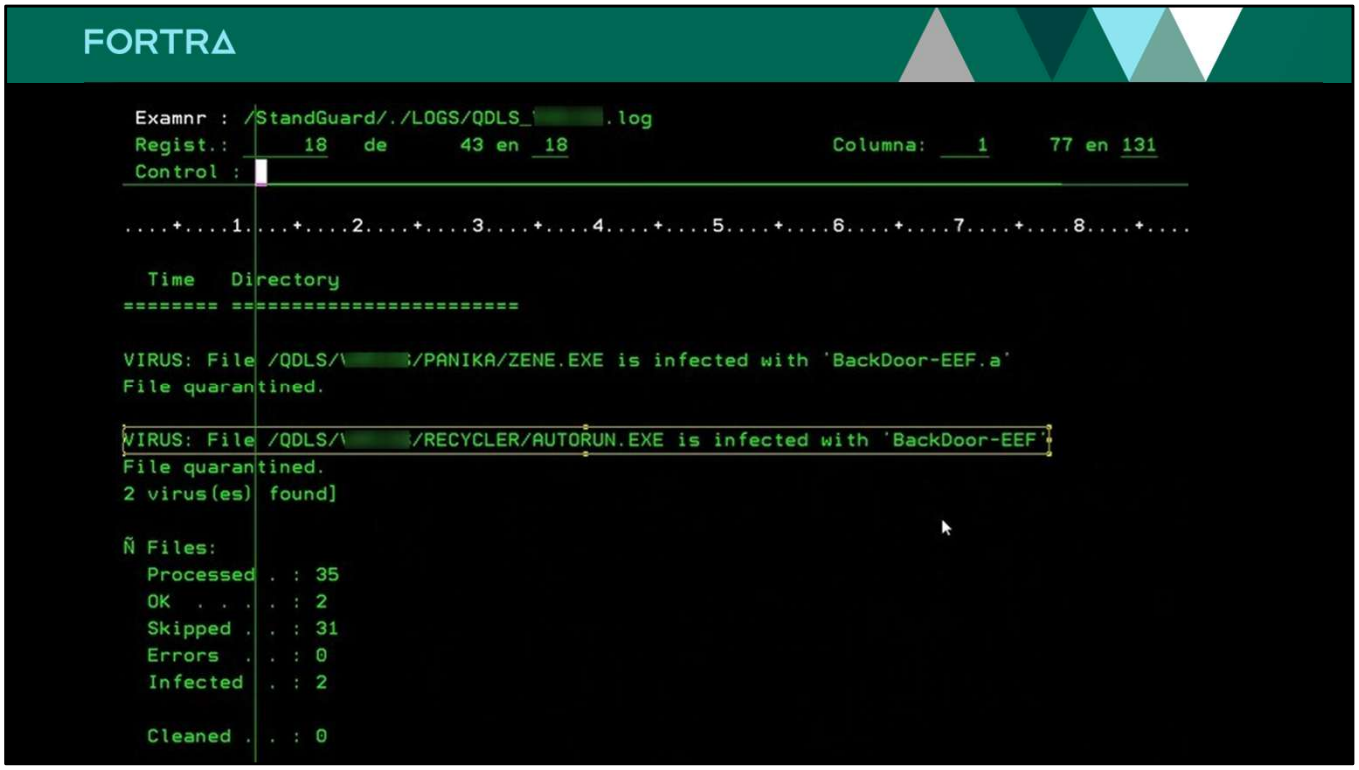
Object scanning attributes for IFS objects.

Useful URL:
https://www.ibm.com/docs/en/i/7.2?topic=concepts-scanning-support

FORTRA


IBM i
IFS NetServer Sh
SFTP/FTPS
AIX
NFS/Samba Sha
SFTP/FTPS
Linux
NFS/Samba Sha
SFTP/FTPS
Browse : /SQinstall/cYVSBhlYk.README.txt
Record : 1 of 73 by 14 Column : 1 298 by 70
Control :
LockBit 3.0 the world's fastest and most stable ransomware from 2019
>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites
Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp8rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevylwqxukkspnlidyvd7qd.onion
http://lockbitapt6vx57t3eqqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
F3=Exit F10=Display Hex F12=Exit F15=Services F18=Repeat find
F19=Left F20=Right
1 records folded.
MRI A
03/012
RANSOMWARE


Recycle Bin
Ransomwar...
FORTRA
YOUR CYBERSECURITY ALLY
RWDEMO (\\10.60.134.174) (I:)
File
Home
Share
View
Manage
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Copy to
Delete
Rename
New folder
New item
Easy access
Properties
Open
Edit
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
This PC › RWDEMO (\\10.60.134.174) (I:)
Search R...
Quick access
Recycle Bin
Desktop
Downloads
Documents
Pictures
Halcyon
Halcyon
Logs
Logs
RWDEMO (\\10.60.134.174) (I:)
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
RWDEMO (\\10.60.134.174) (I:)
HOMEDEMO (\\10.60.134.174) (J:)
Network
Name
Date modified
Type
30SecRule.docx
All How to status - New.xlsx
Attribute.PNG
CIS_Apache_Tomcat_9_Benchmark_v1.1.0(1).docx
CIS_Apache_Tomcat_9_Benchmark_v1.1.0.docx
CIS_IBM_i_V7R4M0_Benchmark_v1.0.0 - WORD.docx
DSPPRDINF.docx
Halcyon Versions.docx
HelpSystemsOneInstallationGuide.pdf
HelpSystemsOneUserGuide v1.1.pdf
LinuxNotesForProfessionals.pdf
LS No claims bonus conf (DAMZ60TW02).pdf
network-server-suite-installation-guide-v11.2.pdf
powertech-antivirus-installation-guide.pdf
PRTOUTQLST827740.txt
PRTRULES827740.txt
QPJOBLOG.pdf
SI-1253 - Helpsystems International.pdf
SQL-V2-Light.pdf
T&K - Invoice_3506 (1).pdf
Win32_PerfFormattedData_class_list.txt
Windows-10-for-Windows-Keyboard-Shortcuts.pdf
22 items
ENG
12:31
05/05/2023



Recent infection in QDLS of one of our customers.

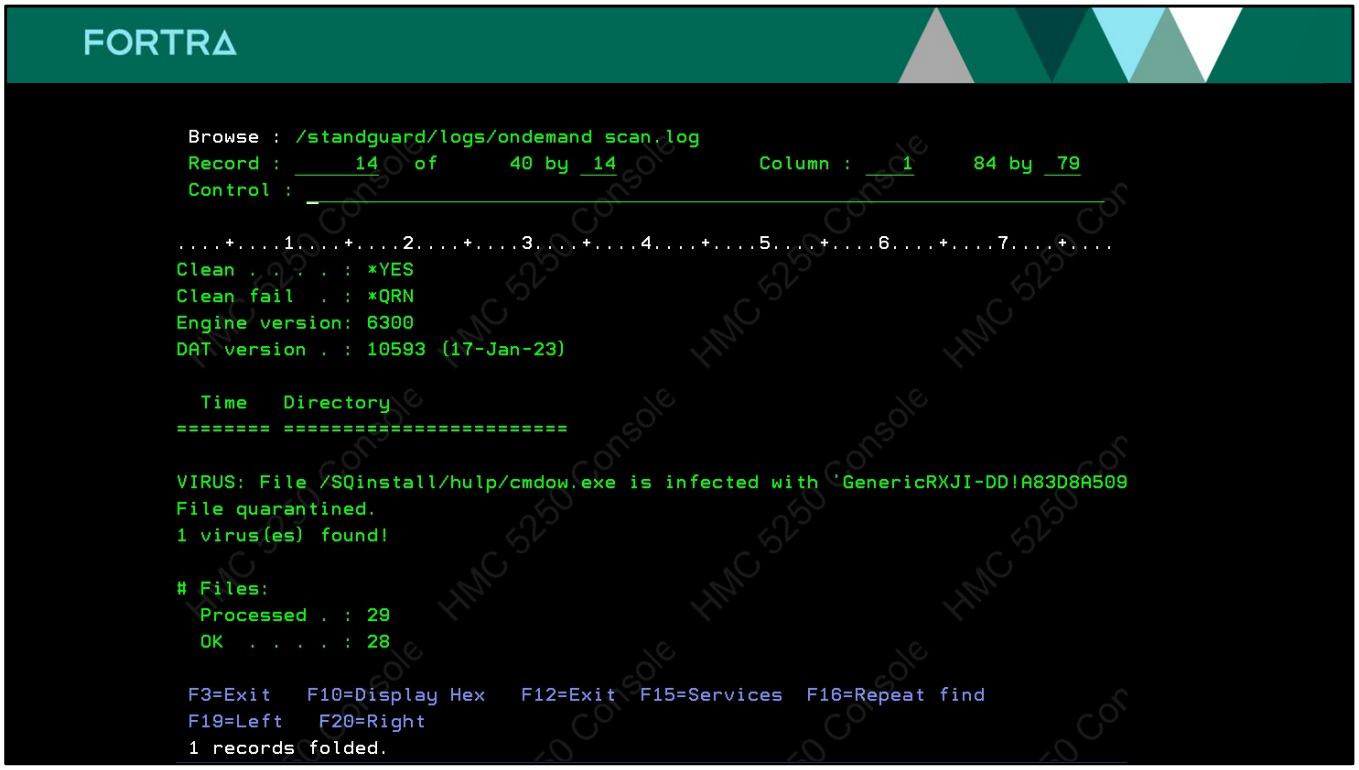
Another of our customers was hit with Russian Ransomware in their open Netserver Share from an infected laptop.

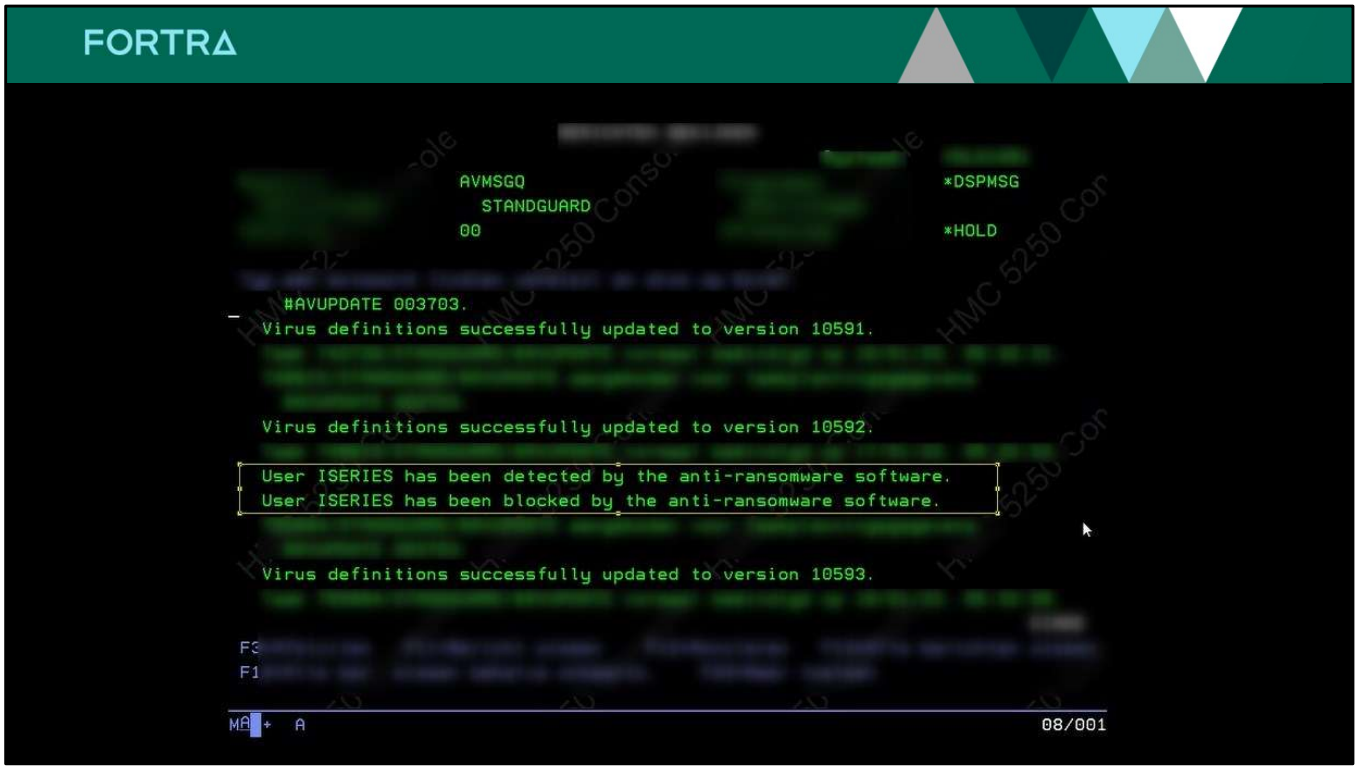
1000's of IFS files were encrypted before the plug was pulled.

They are now a Powertech Anti-Virus and Ransomware customer.

The Anti-Ransomware module of PTAV works brilliantly.

FORTRA


Browse : /standguard/logs/ondemand scan.log
Record : 14 of 40 by 14 Column : 1 84 by 79
Control :
....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
Clean . . . . : *YES
Clean fail . : *QRN
Engine version: 6300
DAT version . : 10593 (17-Jan-23)
Time Directory
======== ========================
VIRUS: File /SQinstall/hulp/cmdow.exe is infected with 'GenericRXJI-DD!A83D8A509
File quarantined.
1 virus(es) found!
Files:
Processed . : 29
OK . . . . : 28
F3=Exit F10=Display Hex F12=Exit F15=Services F16=Repeat find
F19=Left F20=Right
1 records folded.


FORTRA
AVMSGQ *DSPMSG
STANDGUARD
00 *HOLD
#AVUPDATE 003703.
Virus definitions successfully updated to version 10591.
Virus definitions successfully updated to version 10592.
User ISERIES has been detected by the anti-ransomware software.
User ISERIES has been blocked by the anti-ransomware software.
Virus definitions successfully updated to version 10593.
08/001

FORTRA

AIX/Linux

- **Ebury SSH Malware** – OpenSSH backdoor.
- **Cdorked** – HTTP backdoor.
- **Calfbot** – Perl script used to send spam.
- **Onimiki** – DNS redirection.
- Do you have “Typhoid Mary” syndrome? Should we now call it “Covid Colin”?

Ebury SSH Malware – OpenSSH backdoor used to keep control of servers and steal credentials.
Out in the wild for over 10 years!

Cdorked
Runs in memory, single modified httpd binary. HTTP backdoor used to redirect web traffic.

In 2014 it was found, 25,000 Linux servers joined in a massive botnet sending out spam and malware using Ebury and Cdorked.

Calfbot – Perl script used to send spam

Onimiki – DNS redirection.

Sources:
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

https://www.eweek.com/security/malware-turns-25k-linux-servers-into-spam-distribution-botnet/

Read about the FASTCash heist:
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

FORTRA

RECENT LINUX THREATS

- CVE-2022-0492 flaw in Linux Kernel cgroups feature allows container escape.
- B1txor20 Linux botnet use DNS Tunnel and Log4J exploit.
- CVE-2022-0847 Dirty Pipe Linux flaw allows gaining root privileges on major distros.

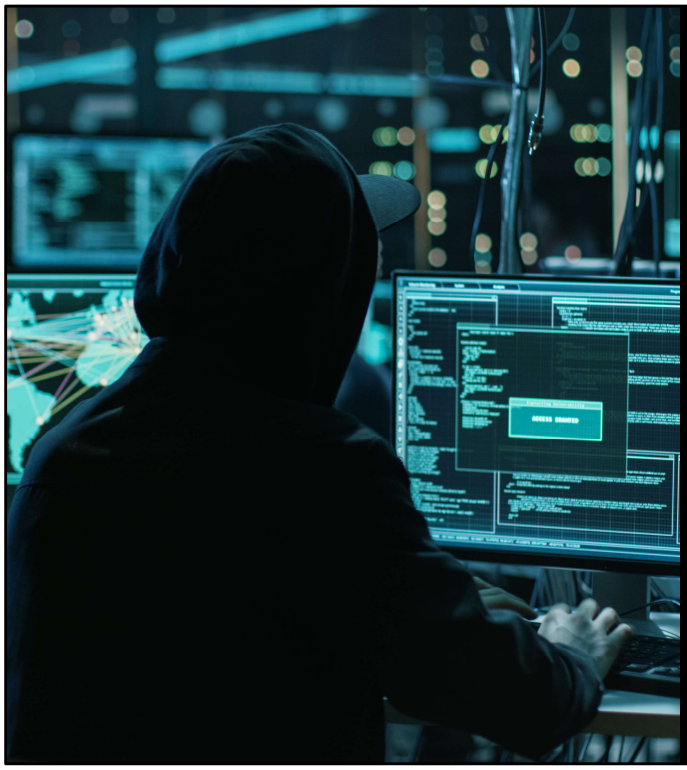
RECENT IBM i THREATS

- CVE-2022-22365 IBM WebSphere Application Server vulnerable to spoofing.
- CVE-2021-45046, CVE-2021-45105
  Multiple vulnerabilities in Apache Log4j affects some features of IBM® Db2

CVE-2022-0492 easily remediated by standard security hardenings.

AIX Vulnerabilities

https://www.cybersecurity-help.cz/vdb/ibm_corporation/ibm_aix/



Real world study: 隱藏的黃蜂

- Chinese based Linux Trojan.
- Used for targeted remote control.
- Fully developed suite including trojan, rootkit and deployment script.
- Second stage payload.
- Reason unknown at present.

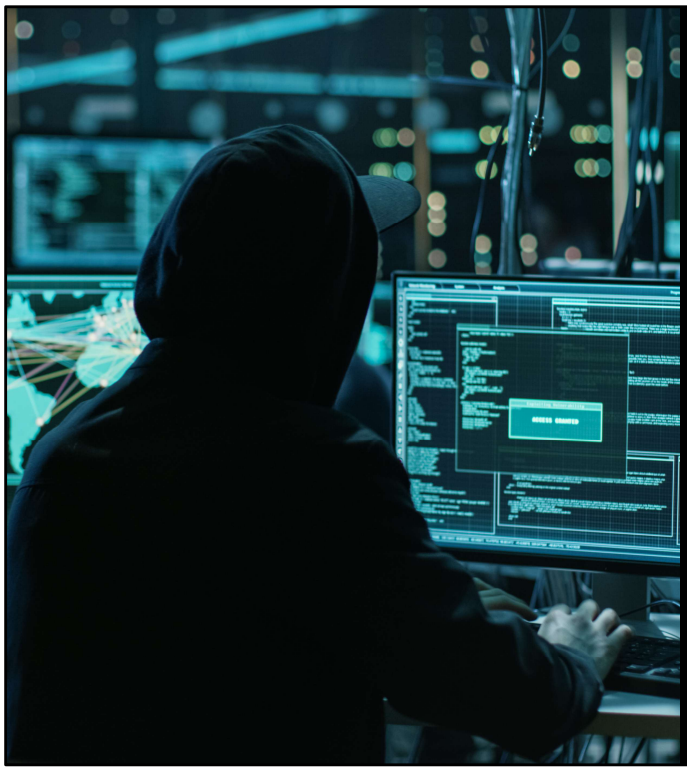
Hidden Wasp

HiddenWasp can interact with the local filesystem; upload, download, and run files; run terminal commands; and more.

Development reason unknown, it is not the usual DDOS or mining malware.

Evidence shows in high probability that the malware is used in targeted attacks for victims who are already under the attacker's control, or have gone through a heavy reconnaissance

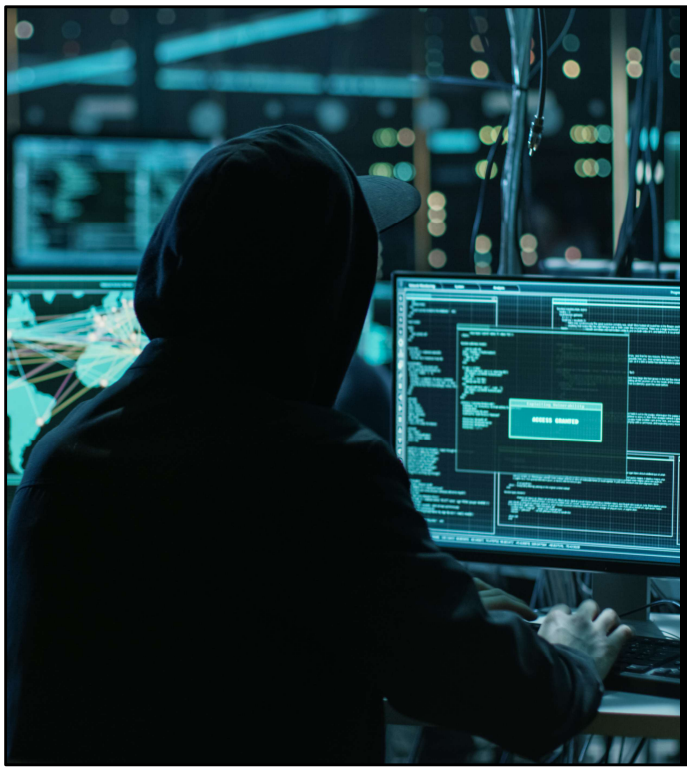
DDoS Distributed Denial of Service



Real world study: Drovorub

- Russian based Linux Malware.
- Used for targeted remote control.
- Fully developed suite including implant, rootkit, C&C server, FTP and port forwarding tool.
- Persists through reboot.

Source: NSA FBI
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF



Real world study: LemonDuck

- Cryptocurrency mining process.
- Uses older vulnerabilities.
- Uses a brute force attack on port 22.
- Installs cryptomining malware.

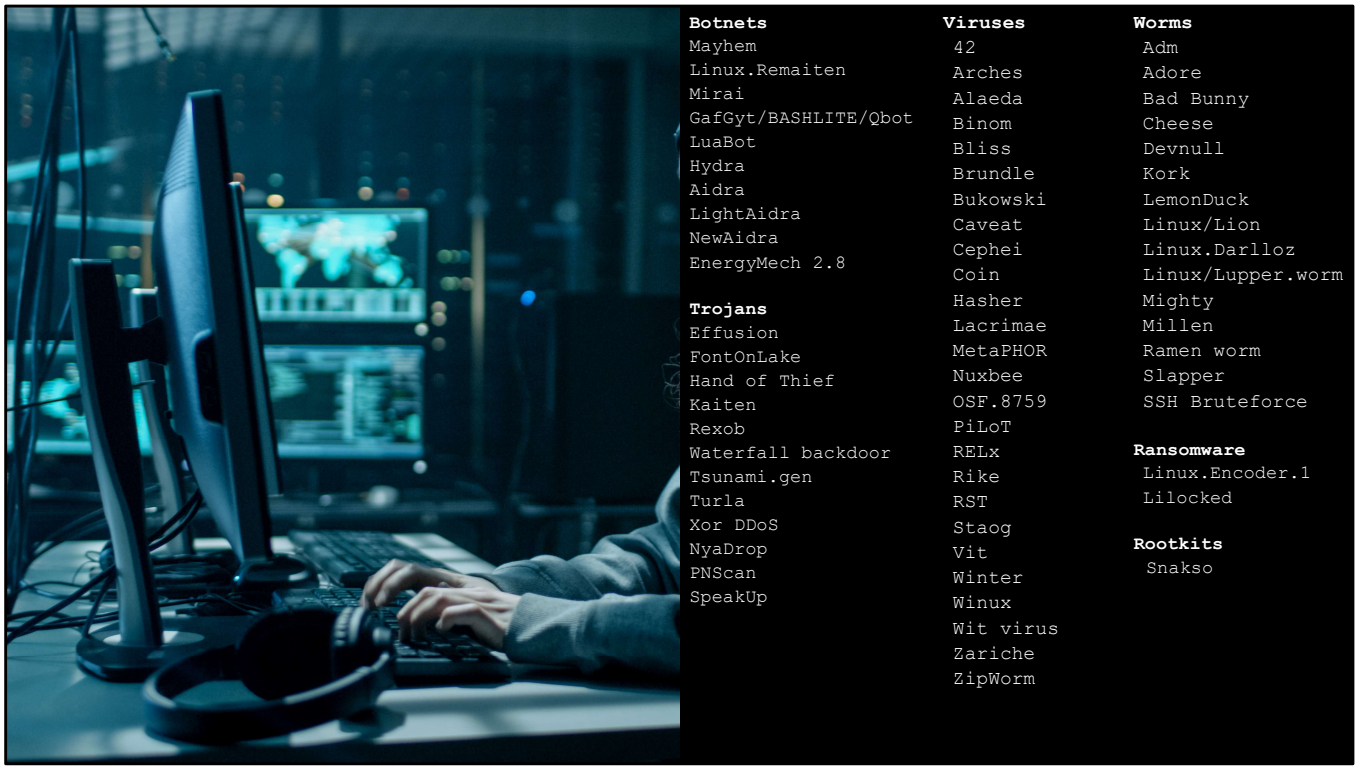
Source: https://linuxiac.com/lemonduck/

LemonDuck makes use of a port scanning module that searches for Internet-connected Linux systems listening on the 22 TCP port used for SSH.

When it finds them, it launches an SSH brute force attack on these machines, with the username root and a hardcoded list of passwords.

If the attack is successful, the attackers download and execute malicious shell code.

Ironically, LemonDuck removes other attackers from a compromised device by getting rid of competing malware and preventing any new infections by patching the same vulnerabilities it used to gain access.



All of these UNIX Botnets, Trojans, Viruses, Worms, Ransomware and rootkits are out in the wild.

Botnet: a network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

Trojan: malware hidden within what appears to be a normal file.

Virus: A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Worm: A computer worm is a malicious program that reproduces itself as it spreads to as many computers as possible over networks.

Ransomware: Malware that employs encryption to hold a victim's information at ransom.

Rootkit: A clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence


How to I combat this?

FORTRA

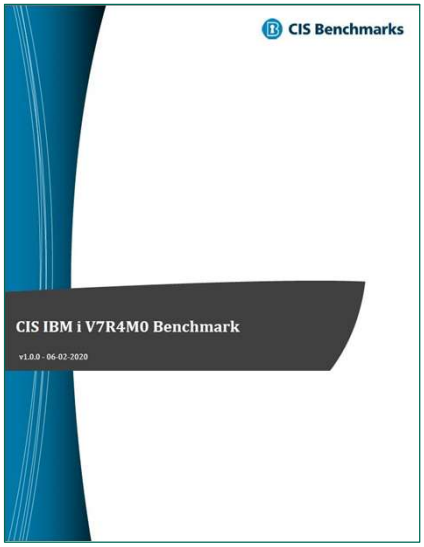
CIS Benchmarks – IBM i / IBM AIX / Linux

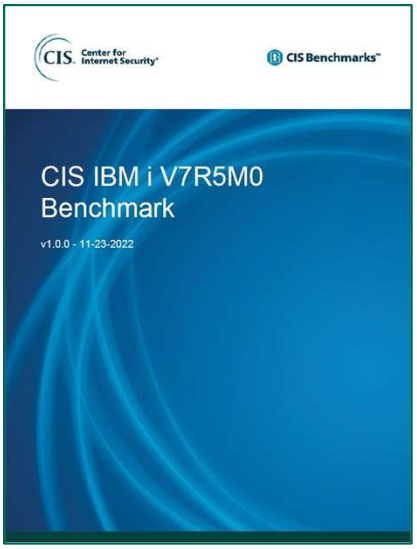
Level 1: Corporate/Enterprise Environment (General use)

- ✓ Practical and prudent.
- ✓ Provide a clear security benefit.
- ✓ Not negatively inhibit the utility of the technology beyond acceptable means.

Level 2: High Security/Sensitive Data Environment (Limited functionality)

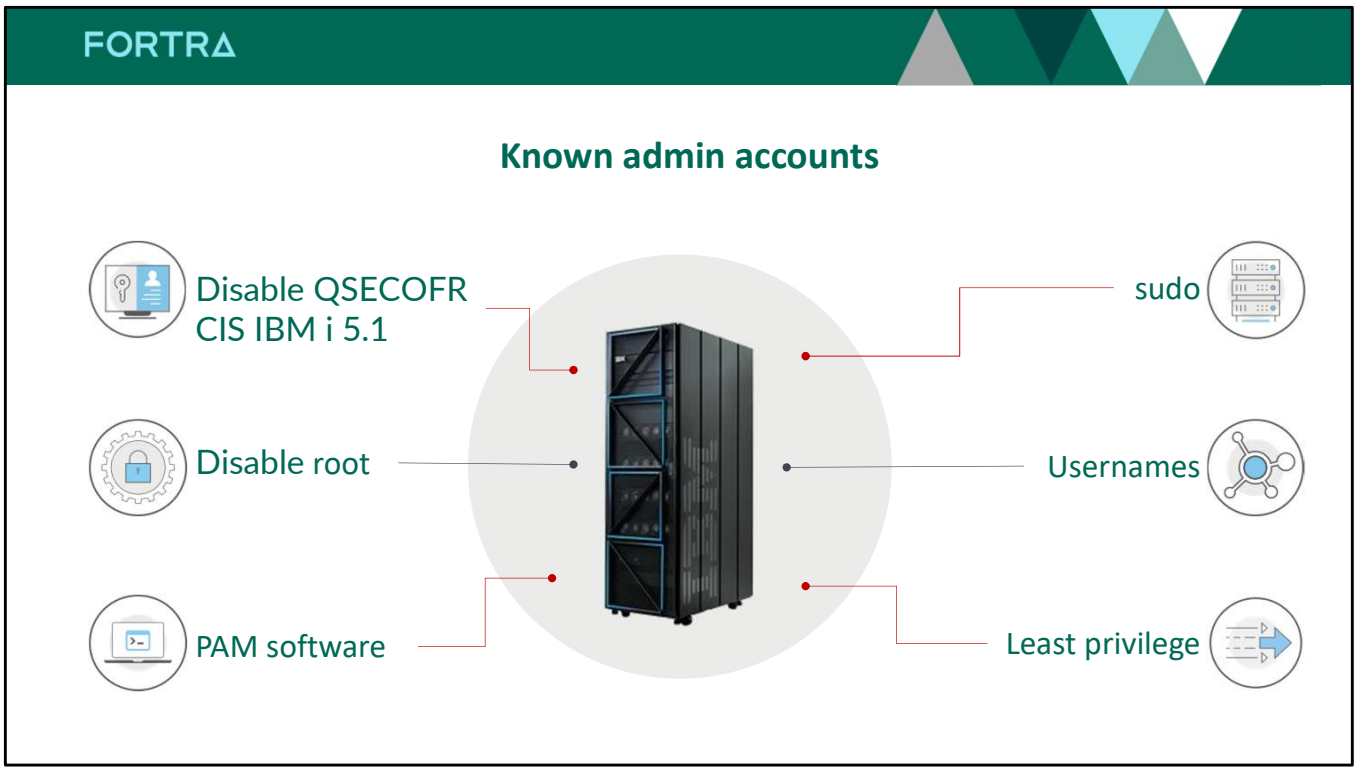
- ✓ Intended for environments or use cases where security is paramount.
- ✓ Acts as defense in depth measure.
- ✓ May negatively inhibit the utility or performance of the technology.





IBM i 7.2 through 7.5 are available

7.6 is in draft



Disable QSECOFR and root.

Get some PAM software for IBMi. (Eg: Powertech Authority Broker)

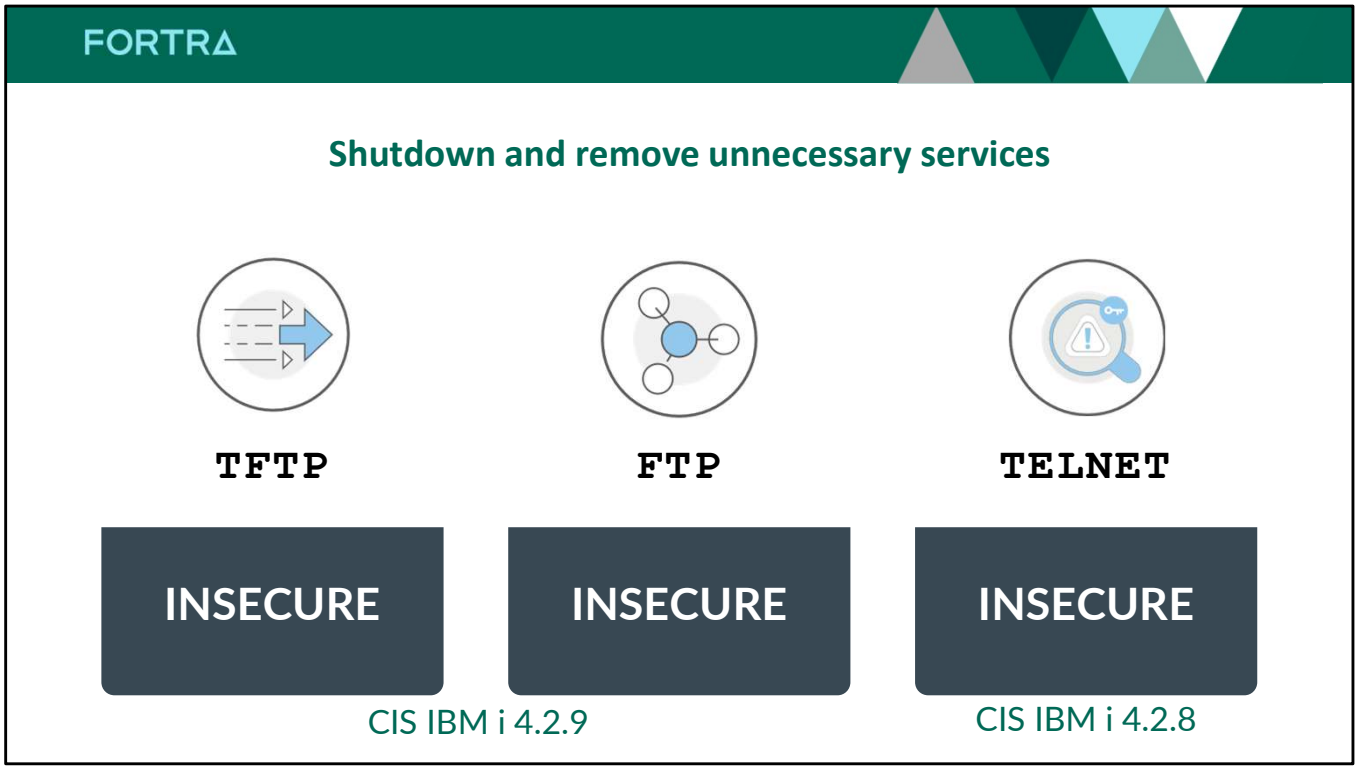
Use sudo for Linux and AIX (It's free to use and implement. Alternatively for large installations you can use Core Privileged Access Manager (BoKS)

Don't use obvious usernames (eg: JSMITH)

Work on the principle of least privilege for everyone.

Developers DO NOT NEED QSECOFR/ROOT access.

PAM: Privileged Access Management

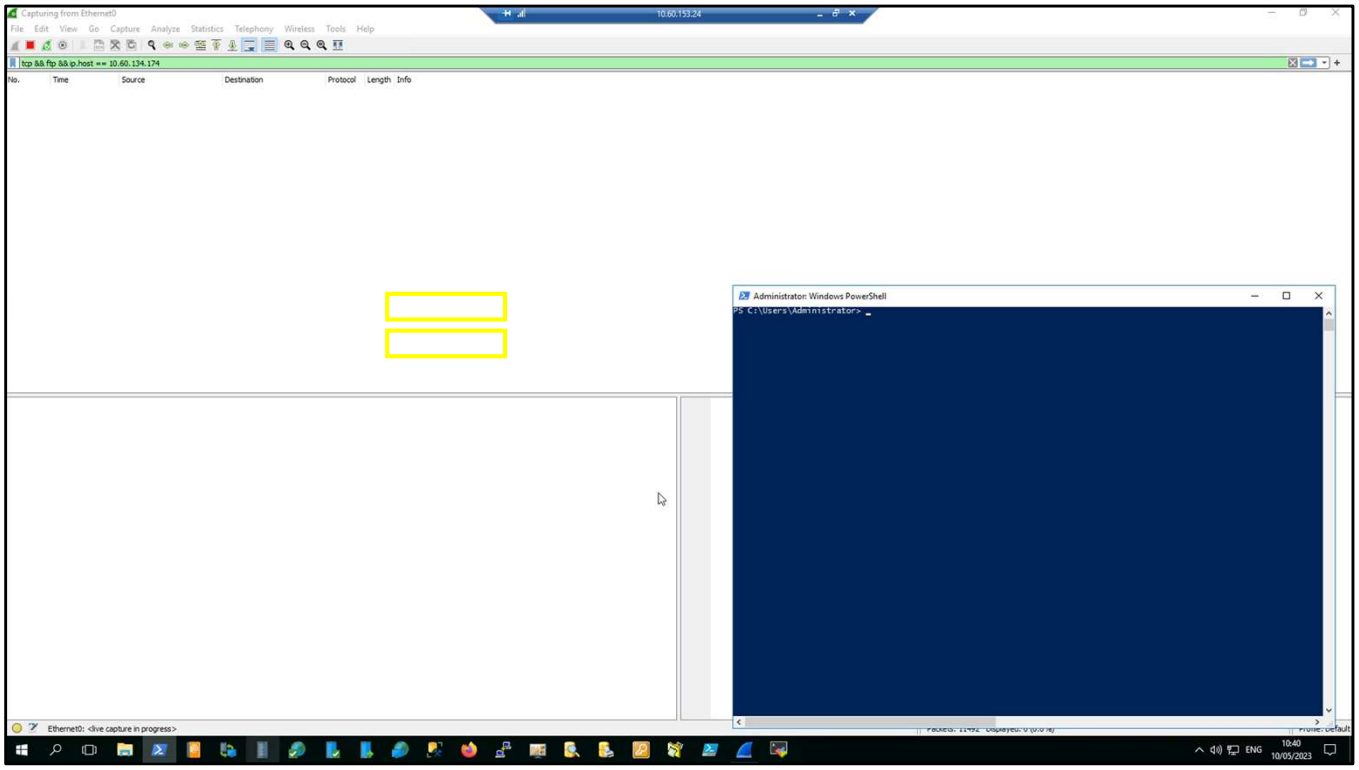


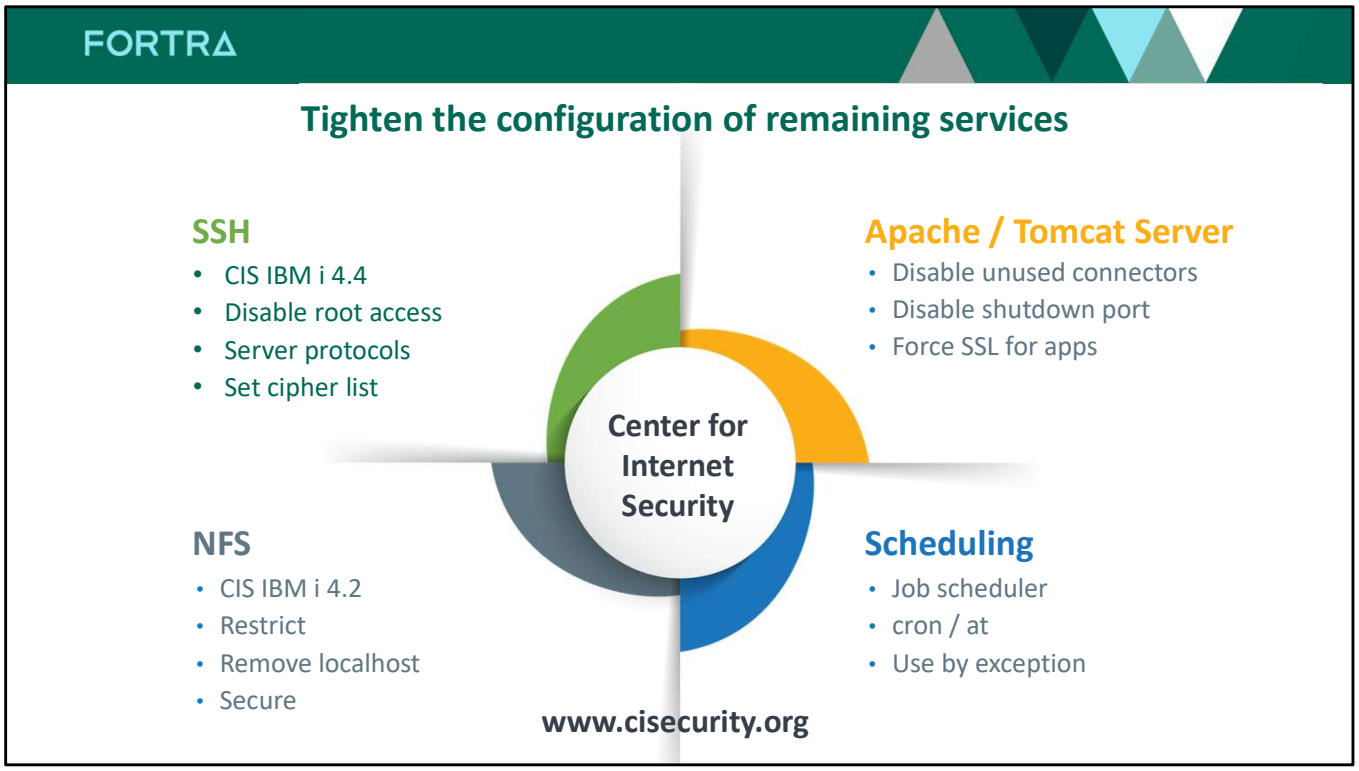
There are a multitude of services that are still shipped with IBM i, AIX and Linux that are inherently insecure.

There are three that are common to all platforms.

If you have TFTP, FTP or TELNET running, implement SSH and then shut them down and disable or remove them.

Check what services are running and what are actually required.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp && ftp && ip.host == 10.60.134.174
No. Time Source Destination Protocol Length Info
10.60.153.24
Administrator: Windows PowerShell
PS C:\Users\Administrator>
Ethernet0: <live capture in progress>
ENG
10:40
10/05/2023



CIS 4.2, 4.3, 4.4

If you are running SSH, NFS, Apache server, etc then ensure you are following CIS Standards. They have good free benchmarks.

Monitor your configuration with something like Powertech Policy Minder for IBMi and Powertech Security Auditor for everything else.

Badly configured databases and http servers are common entry points for data breaches.

https://www.cisecurity.org/

CIS 4

Passwords.

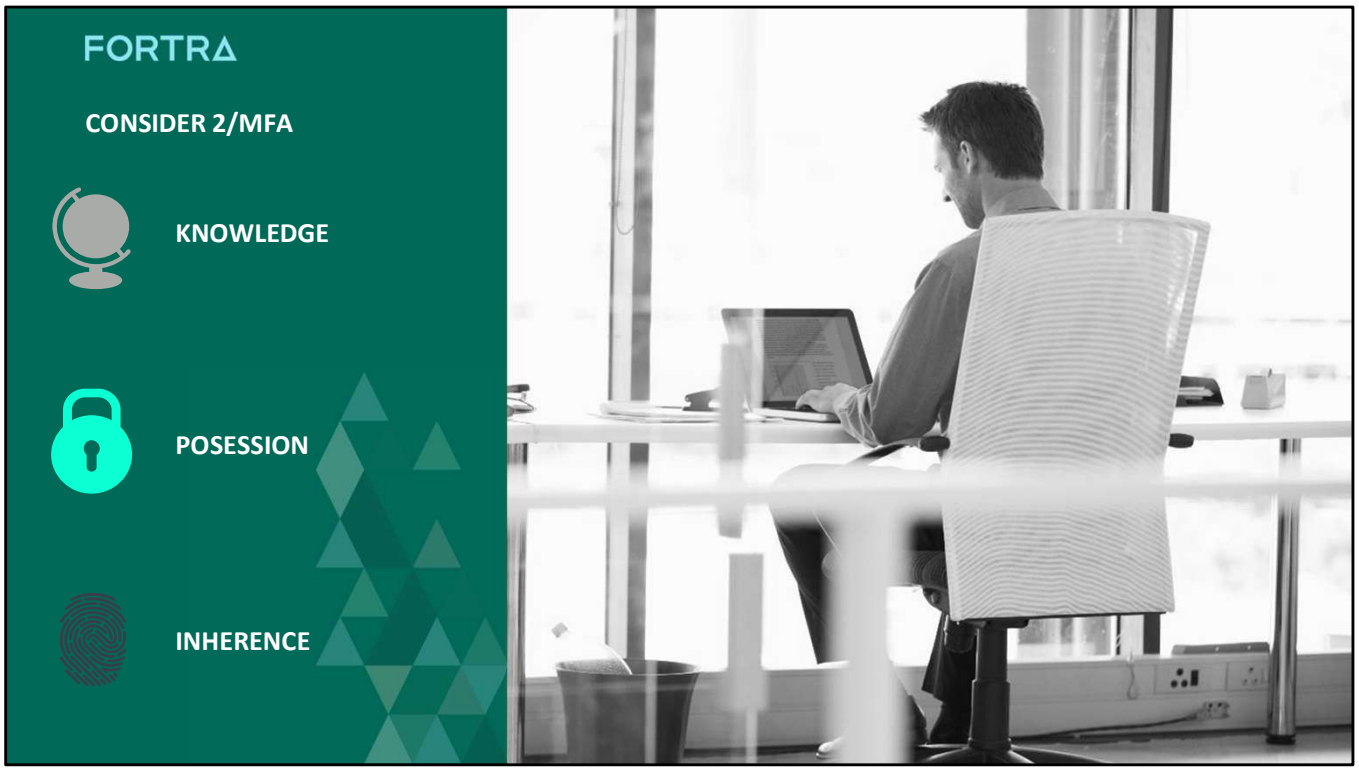
Define a strong password policy

- Reuse options
- Differences between old and new passwords
- Minimum number of lowercase, uppercase, special, etc

QPWDLVL 2 or 3 (IBM i 7.6 now defaults to 3)

Better still, start using “pass phrases” which can’t be cracked using a brute force dictionary attack.

Even better, start using a SSH key which only allows access to a system on exchange of an encrypted key.



IBM i 7.6 – Includes basic MFA.

Knowledge: Something only the user knows - Password, passphrase, PIN.

Possession: Something only the user has - Security token, software token, QR code.

Inherence: Something only the user is – Biometrics, fingerprint, face, voice or iris recognition.

Review user and group accounts regularly.

Automatically lock those that have not been used for a while.

Check object ownership regularly.

CIS 7

Monitor everything, report by exception

Look at a SIEM solution.

At the very minimum use a SYSLOG aggregator.

The days of "If it isn't broken, don't fix it – are GONE!" – STAY CURRENT – OS Releases and PTF updates.

Sept 29th 2021 IBM issues three security bulletins for IBM i depicting security vulnerabilities in OpenSSL, HTTP Server and Websphere liberty components.

April 2022
https://www.itjungle.com/2022/04/20/ibm-i-ptf-guide-volume-24-number-16/

IBM WebSphere Application Server Liberty for IBM i is vulnerable to spoofing and clickjacking attacks due to swagger-ui (CVE-2018-25031, CVE-2021-46708), which you can read more about here. The IBM i PTF numbers containing the fix for the CVEs:

OpenSSL for IBM i is vulnerable to a denial of service due to a flaw in the BN_mod_sqrt() function (CVE-2022-0778), which you can find out more about at this link.

CIS 11

We can’t stress the importance of backups and testing that you can recover.

Only 54% of organisations have a disaster recovery plan in place.

7% of companies have never tested their plan

Source: https://invenioit.com/continuity/disaster-recovery-statistics/

It's worth remembering that the core reason for having a disaster recovery plan and to test it regularly, is to arm you and your team with the confidence that digital continuity can be provided, minimizing disruption to the business.

Regular testing proves the plan and ensures that agreed recovery points and times continue to be achievable.

Confidence, comes from experience, which comes from practice.

FORTRA

Also consider…

- Review permissions to folders/directories/shares.
- Do NOT share the *root* "/" folder. **EVER**.
- Make Netserver / NFS shares read-only whenever possible.
- Monitor your configuration for changes.
- Use QPWFSERVER authorization list to limit access to /Qsys.lib.
- Implement IBM AIX Trusted Execution (TE).
- Implement SELinux.

If it is too big a task – start with Netserver, NFS and Samba shares

IBM i ships the IFS root filesystems "/" with *PUBLIC *RWX access – have you changed yours?

IBM i 7.5+ includes security features for Netserver and shares - *AUTL for both.

Once configuration is reviewed and set, monitor it.

Trusted Execution (TE) refers to a collection of features that are used to verify the integrity of the system and implement advance security policies, which together can be used to enhance the trust level of the complete system.
https://www.ibm.com/docs/en/aix/7.3?topic=configuration-trusted-execution

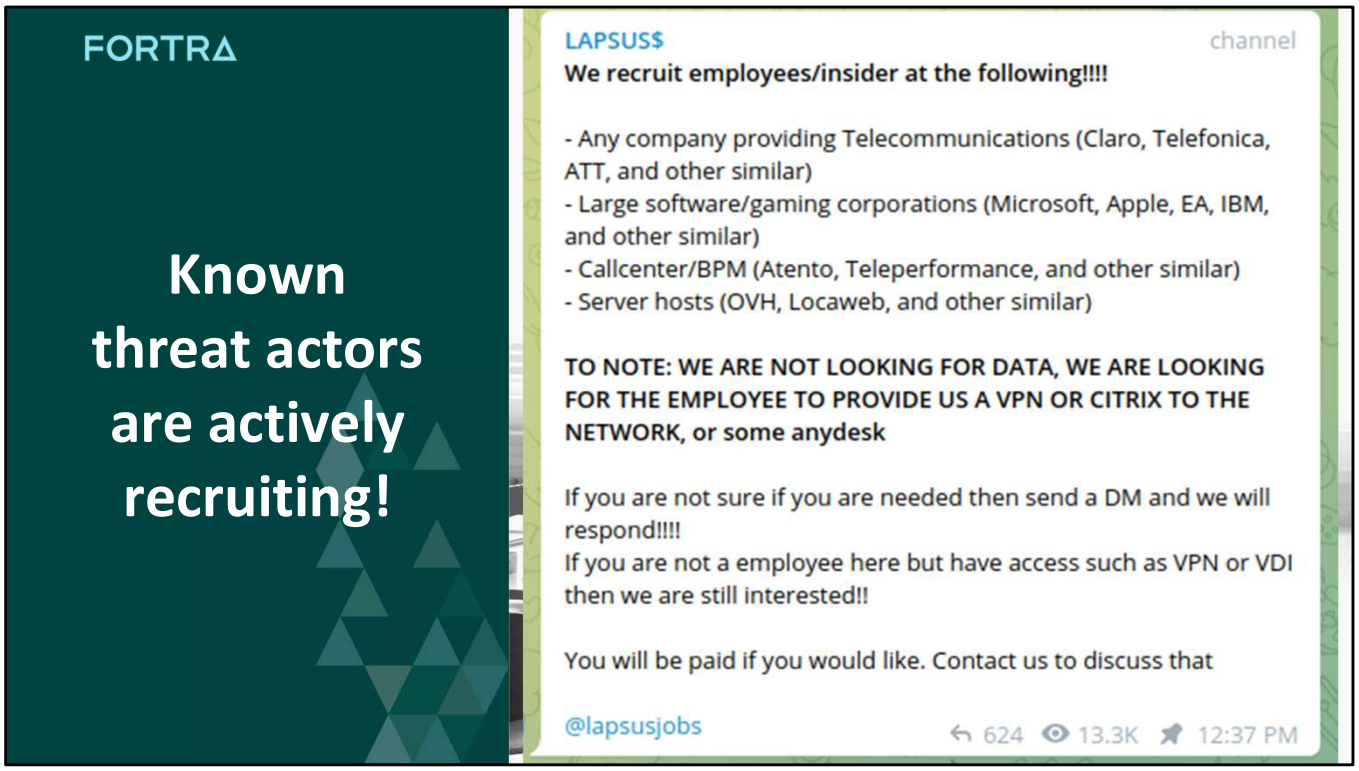
SELinux stands for **S**ecurity **E**nhanced **Linux**, which is an access control system that is built into the Linux kernel. It is used to enforce the resource policies that define what level of access users, programs, and services have on a system.

In its default enforcing mode, SELinux will deny and log any unauthorized attempts to access any resource. This approach, usually referred to as the principle of least privilege, means that explicit permission must be given to a user or program to access files, directories, sockets, and other services.

FORTRA

Hire and retain top talent.

Be kind to them.

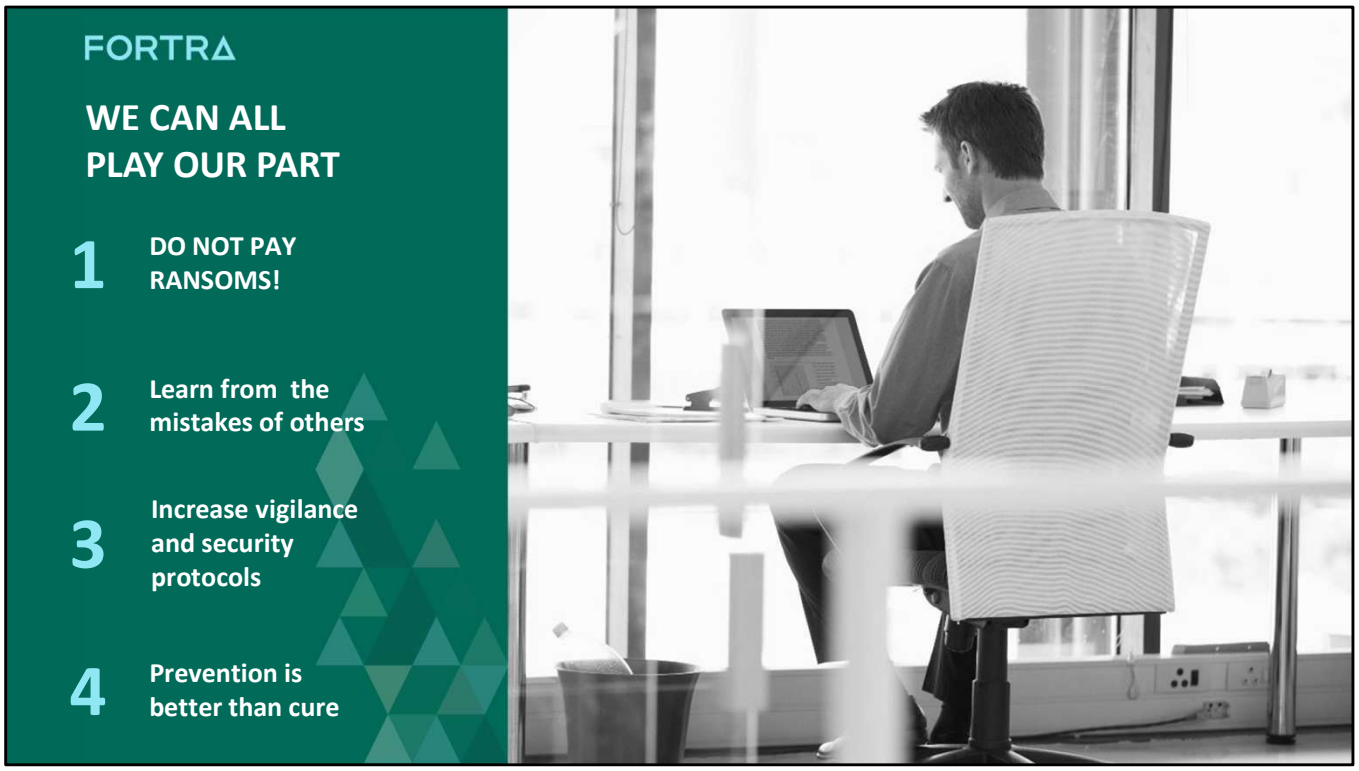


LAPSUS$ group are actively recruiting

Source: https://securityaffairs.co/wordpress/128912/cyber-crime/lapsus-ransomware-is-hiring.html

35% of breaches involve internal actors (malicious or accidental)

https://invenioit.com/continuity/disaster-recovery-statistics/



It is far better to avert a ransomware attack by hardening your attack surfaces than to have to deal with the aftermath.

You don’t need to pay ransom’s, right?

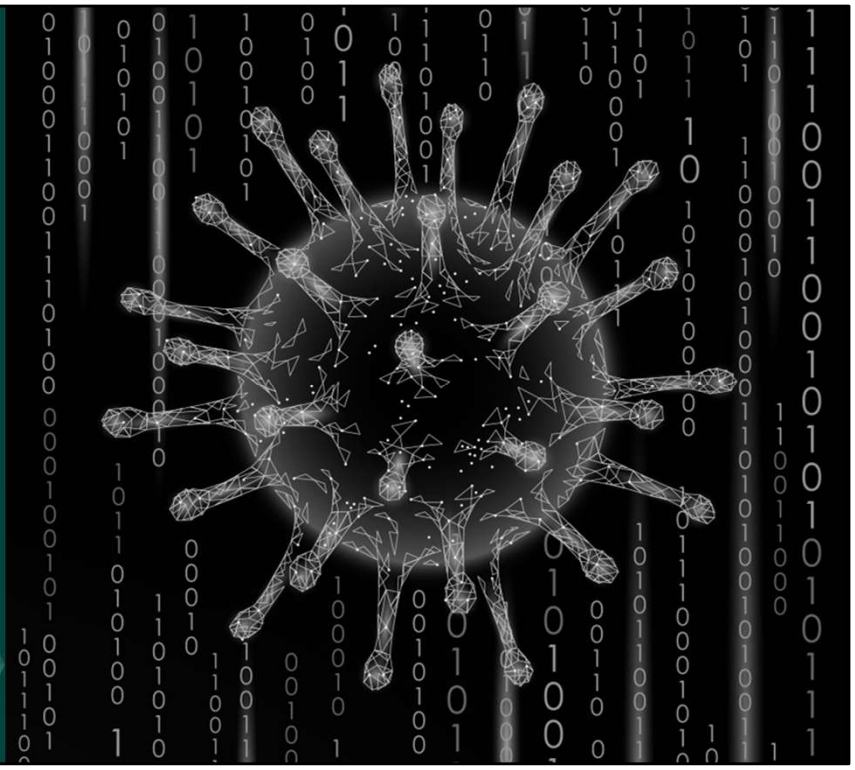
Because you have a backup and DR plan that you have tested right?

The Japanese have a saying, "Fix the problem, not the blame." Find out what’s broken and fix it. Nobody gets blamed. We're always after who screwed up. Their way is better.

If we start playing the blame game, our collaborators will no longer want to report a security incident. It also applies to the outside: There are still organizations that already do not handle external reports well and go so far as to accuse those who report vulnerabilities as external crackers.

FORTRA

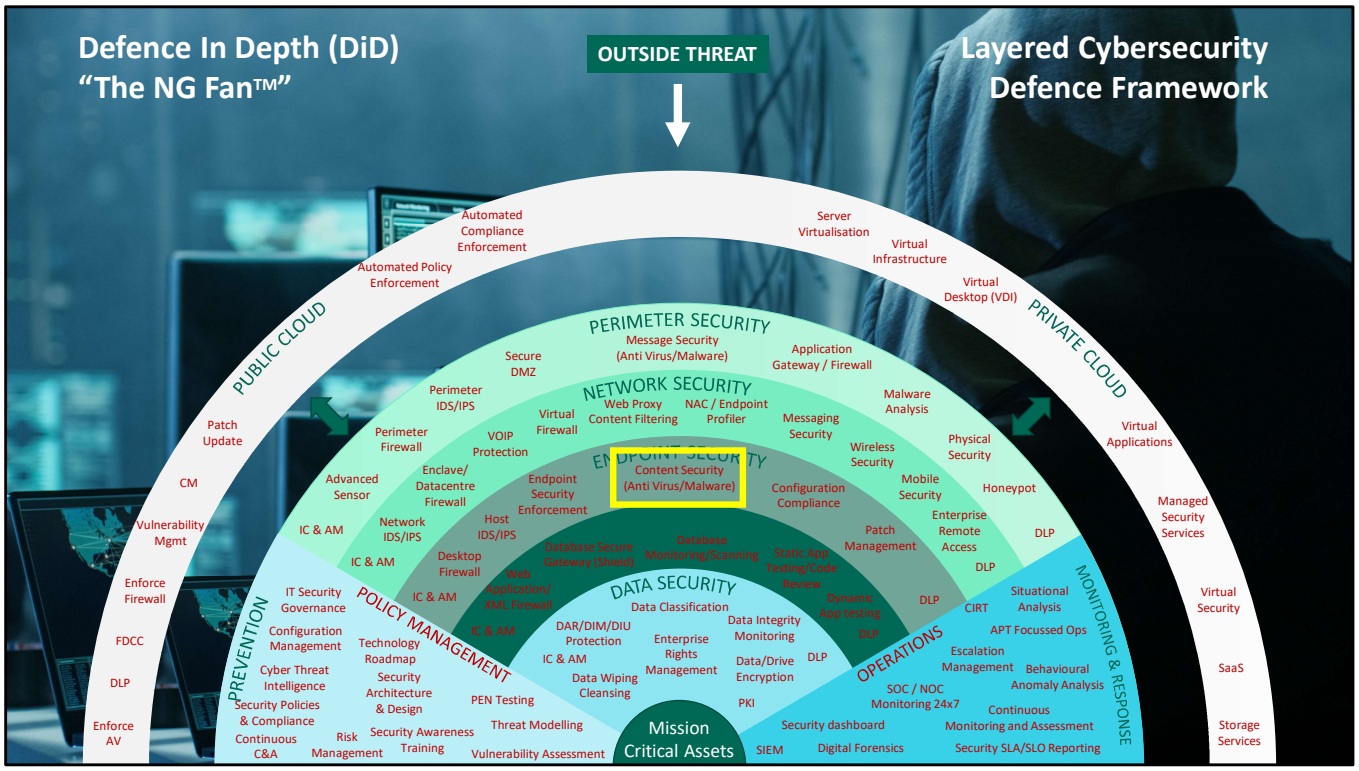
Why use native anti-virus?



All data has value

Organizations paid at least $813.5 million to ransomware gangs in 2024

Source: https://www.varonis.com/blog/ransomware-statistics#top

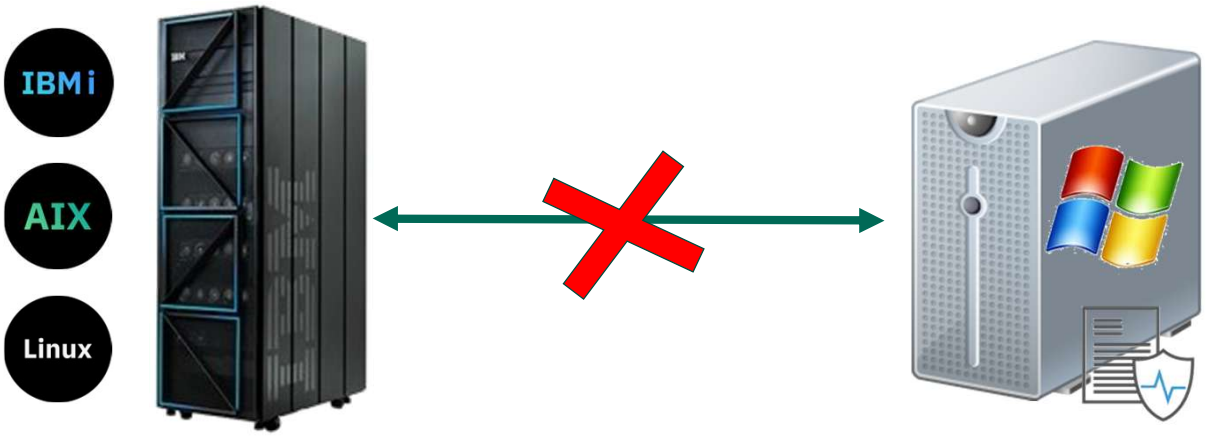


The Northrop Grumman "Defence in Depth" (DiD) FanTM
A holistic view of a layered cybersecurity defence framework.
Anti-Virus / Malware is central to the Endpoint Security layer.

SaaS	Software as a Service
DLP	Data Loss Prevention
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLO	Service Level Objective
SOC	Systems Operation Centre
NOC	Network Operations centre
CIRT	Computer Incident Response Team
APT	Advanced Persistent threat
PKI	Public Key Infrastructure
VOIP	Voice Over IP
C&A	Certification and Accreditation
ICAM	Identity, Credential and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	De-Militarlised Zone
AV	Anti-Virus
CM	Continuous Monitoring
FDCC	Federal Desktop Core Configuration
DAR	Data At Rest
DIM	Data In Motion
DIU	Data In Use
NAC	Network Access Control
PAM	Privileged Access Management

FORTRA

Why use Native Antivirus?



Native antivirus scanning avoids numerous pitfalls inherent with scanning from a remote server:

- Opening the door wider with a Read-Write share to *ROOT
- A persistent network connection with *ALLOBJ / root profile to run scans
- No real-time (live) scanning
- No intelligence of when and what to scan
- Requirement to monitor scanning (in case of error messages)
- Heavy network bandwidth consumption
- Movement of stream files in clear text
- No OS acknowledgement of infection

FORTRA

Why native Antivirus protection is important for all systems

- Studies have shown that Linux malware alone accounts for more than 35% of all malware
- The number of Linux malware variants have tripled over the past three years
- Linux organization finds malware on their system and pays over $1,000,000 in bitcoin to get their servers back online
- An AIX organization is compromised by malware sending public safety data to servers in Russia
- Linux and Unix servers can host and spread Windows viruses like Typhoid Mary
- Linux and Unix servers can be directly infected by ransomware, crypto-lockers, scripts, trojans, worms and many other types of malware

FORTRA

Your call to action

Audit your systems.
    Before the auditors arrive.
Check your Disaster Recovery Plan
    Before the disaster happens.
Do not use QSECOFR or root.
    Change NOW.
Investigate and utilise CIS benchmarks.
    They are a free and fantastic resource.
Ask Fortra for a FREE security scan.
    No obligation.

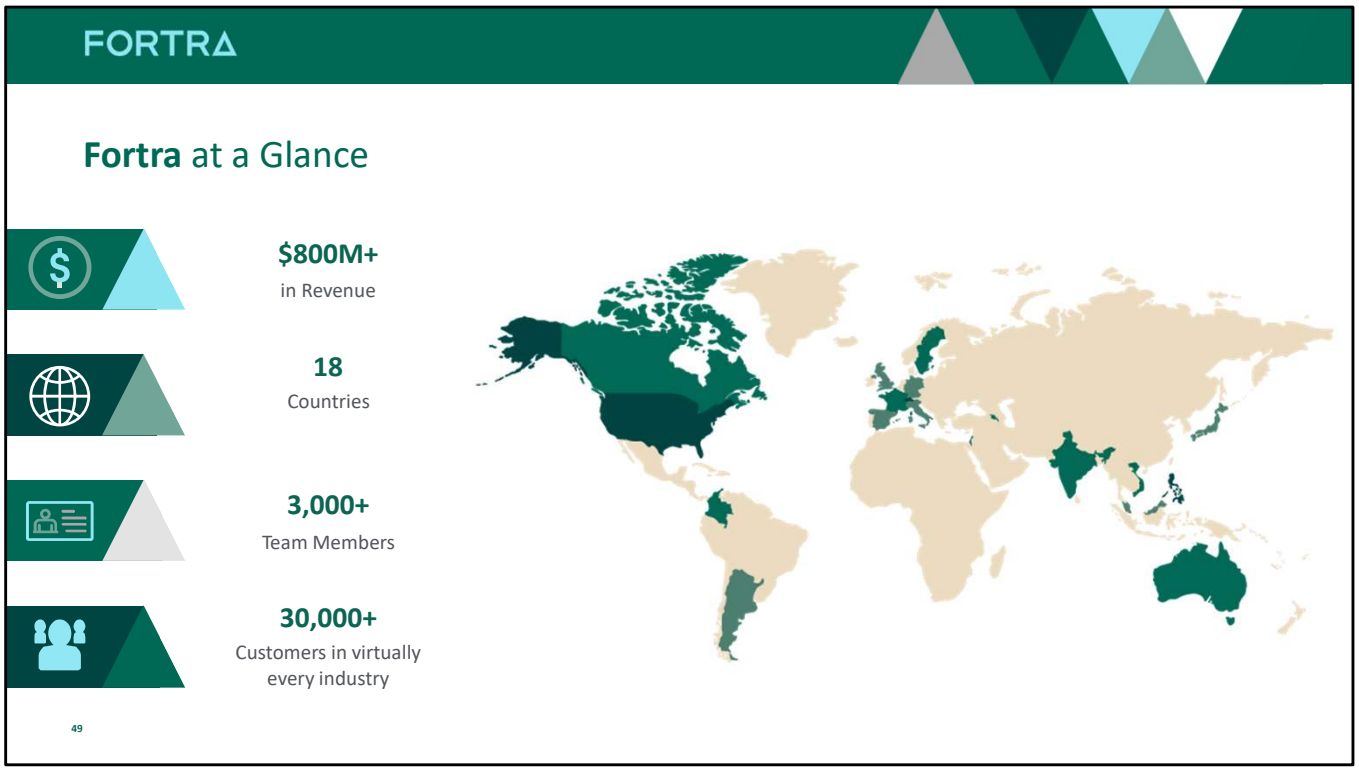
www.cisecurity.org

www.ibm.com/security/data-breach

www.ncsc.gov.uk

www.power.fortra.com


FORTRA
IBM i Solutions - Fortra
48



A Global Perspective

While our headquarters is located just outside of Minneapolis, MN in Eden Prairie, we have offices located across the United States for sales, support and development and strategically located offices in Australia, England, Germany, Spain, Sweden, Switzerland, Canada and Argentina.

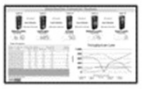
FORTRA

Legendary Software For IBM i

Backup and HA

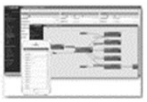
Document Management

Monitoring and Alerting



Business Intelligence

Capacity Planning



Automation

… including, of course, cybersecurity

Cybersecurity

FORTRA

The 60 second elevator pitch: We can help.

Security Product	Use	IBMi	AIX	Linux
Antivirus	Antivirus/malware/ransomware protection	✓	✓	✓
Event Manager	SIEM solution	✓	✓	✓
Tripwire	Configuration management and monitoring		✓	✓
Compliance Monitor	Configuration management and monitoring	✓		
Core PAM (BoKS)	Privileged Access Management		✓	✓
Authority Broker	Privileged Access Management	✓		
Exit Point Manager	Exit point management and monitoring	✓		
RSA SecurID	2FA	✓		
Encryption	Encryption of database fields, backups and IFS	✓		

FORTRA

Best of Breed Security Products

Compliance Reporting
Compliance Monitor for IBM i

Privileged Access Management
Authority Broker for IBM i

Self-Service Password Reset
Password Self Help for IBM i

Database Monitoring
Database Monitor for IBM i

User Provisioning
Identity Manager for IBM i

Multi-Factor Authentication
Multi-Factor Authentication for IBM i
SecurID Agent for IBM i

Native Encryption
Encryption for IBM i

Free Security Snapshot
Powertech Security Scan

Solution View

Perimeter Access Control
Exit Point Manager for IBM i

Command Monitoring
Command Security for IBM i

Automated Risk Audit
Risk Assessor for IBM i

Security Information and Event Management
SIEM Agent for IBM i
Event Manager

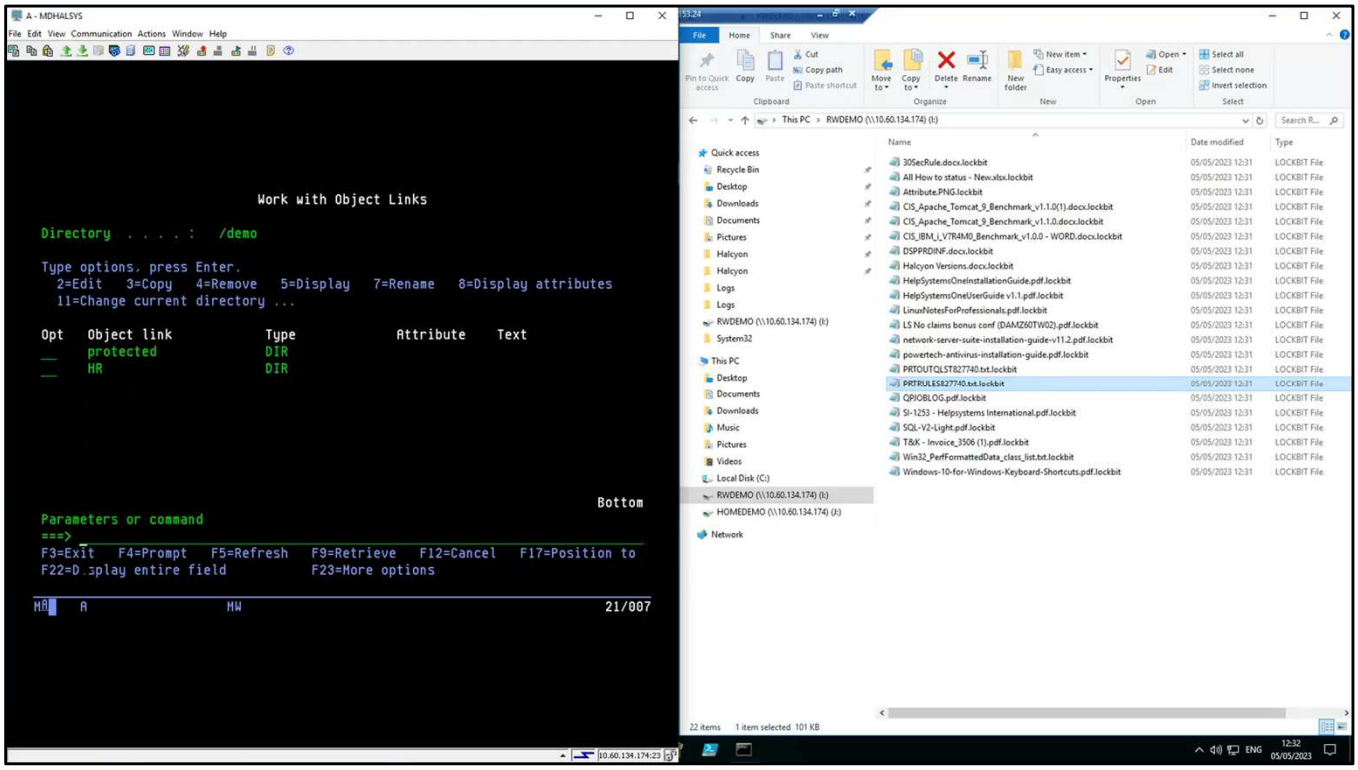
Native Virus Protection
Antivirus for IBM i, AIX, Linux, Linux on Z and LinuxONE

InfoSec Policy Control
Policy Minder for IBM i

Risk & Pen Testing Services

Fortra Security Services

52


A - MDHALSYS
File Edit View Communication Actions Window Help
Work with Object Links
Directory . . . . : /demo
Type options, press Enter.
2=Edit 3=Copy 4=Remove 5=Display 7=Rename 8=Display attributes
11=Change current directory ...
Opt Object link Type Attribute Text
protected DIR
HR DIR
Bottom
Parameters or command
===>
F3=Exit F4=Prompt F5=Refresh F9=Retrieve F12=Cancel F17=Position to
F22=Display entire field F23=More options
MA A MW 21/007
10.60.134.174:23
File Home Share View
Clipboard
Organize
New
Open
Select
This PC › RWDEMO (\\10.60.134.174) (I:)
Search R...
Quick access
Recycle Bin
Desktop
Downloads
Documents
Pictures
Halcyon
Halcyon
Logs
Logs
RWDEMO (\\10.60.134.174) (I:)
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
RWDEMO (\\10.60.134.174) (I:)
HOMEDEMO (\\10.60.134.174) (J:)
Network
Name
Date modified
Type
30SecRule.docx.lockbit
All How to status - New.xlsx.lockbit
Attribute.PNG.lockbit
CIS_Apache_Tomcat_9_Benchmark_v1.1.0(1).docx.lockbit
CIS_Apache_Tomcat_9_Benchmark_v1.1.0.docx.lockbit
CIS_IBM_i_V7R4M0_Benchmark_v1.0.0 - WORD.docx.lockbit
DSPPRDINF.docx.lockbit
Halcyon Versions.docx.lockbit
HelpSystemsOneInstallationGuide.pdf.lockbit
HelpSystemsOneUserGuide v1.1.pdf.lockbit
LinuxNotesForProfessionals.pdf.lockbit
LS No claims bonus conf (DAMZ60TW02).pdf.lockbit
network-server-suite-installation-guide-v11.2.pdf.lockbit
powertech-antivirus-installation-guide.pdf.lockbit
PRTOUTQLST827740.txt.lockbit
PRTRULES827740.txt.lockbit
QPJOBLOG.pdf.lockbit
SI-1253 - Helpsystems International.pdf.lockbit
SQL-V2-Light.pdf.lockbit
T&K - Invoice_3506 (1).pdf.lockbit
Win32_PerfFormattedData_class_list.txt.lockbit
Windows-10-for-Windows-Keyboard-Shortcuts.pdf.lockbit
LOCKBIT File
22 items 1 item selected 101 KB
ENG
12:32
05/05/2023

FORTRA

IT Transformation is
A Journey
Not a Destination.
Let's Move Forward.