www.HackersMo.com

The op-ed follows this introduction.

The FBI is worried about rising Chinese hacking activity. However, I feel the intelligence apparatus does not want to stop hackers. Hackers can attack the grid, pipelines, financial systems, military systems, and more. But if we stop the hackers then we can't retaliate by hacking enemy critical systems. However, with strategic corrections only the enemy hackers would be stopped.

The modus operandi of hackers, have been in several newspapers. Reuters 05/15/24 "China's rising cyber threat." News-Press 04/14/24, "Health info of 144M exposed. News-Press 03/24/14, "Why operating systems are perfect for data theft." News-Press 07/16/16, "Mainframe systems could have stopped hackers." New York Post Letters@NYPost.com 09/16/17, "Equifax's Security Fail: Putting Our Data at Risk." News-Press & Naples News 07/08/21, "Methods to stop hacking."

All the articles stress that hacking of **mainframe systems** is unheard of. Yet, **PC and servers** are hacked. Mainframes are large computers with a mainframe operating system, OS, 100 times more secure than a PC or server type OS. FBI Discourages Ransomware Payments AP, 06/12/21. What to do if a business is down? Logically, a decision is made which is less costly. Pay the ransom or bide time, stop business, and rebuild the ransomed data base. Assuming there's a **non-effected** backup. That will go on until the root cause of Ransomware's or hacker's success is identified and corrected.

Some noteworthy hacks, a meat supplier cyberattacked AP, 06/02/21. Time to protect American cybersecurity USA TODAY, 06/01/21. US pipeline cyberattacked AP news, 05/08/21. South Florida School records exposed Naples Daily News, 04/21/21. Florida school ransomware attack Naples Daily News, 04/02/21. US Agencies Hacked USA TODAY, 12/15/20. Federal Agencies Hacked NY Times, 12/14/20. Cloud Company Hacked Fort Myers News-Press, 09/18/20. The articles missed the root cause of cyber hacking, flaws in the operating system, OS, code running the PC or servers.

Before reading **Hackers Modus Operandi note,** Ransomware and hackers do not require stolen IDs or PWs.

HACKER'S MODUS OPERANDI (OP-ED)

US Agencies, pipe lines, and cloud companies hacked. Cloud, isn't that where are we supposed to keep our data safe from hackers? Is the grid next? **NOTE, ransomware does not need stolen IDs or PWs.** What intelligent operating system, OS, e.g. Windows, controlling a server or PC, would allow a single user to download a complete customer database, a cloud, or Federal database? Why would that OS allow spontaneous changes to its program code by a user half way around the world, e.g., Ransomware?

Where are we supposed to store our data to avoid Ransomware or viruses? What are the ramifications of a major pipeline or electric grid shutdown? How do we protect ourselves if the Federal Government can't protect itself? Why ***doesn't*** this happen in mainframe computer systems running a **mainframe** OS?

As a 30 year IBM Consulting Systems Engineer, I worked with the design, programming, and support of large interactive database systems housed in mainframes. For those unfamiliar with the term ***mainframe***, they are large **non-PC or server type** computers with massive databases. The OS controlling a mainframe is ***much more secure*** than PC or server type OS.

All mainframe program changes are previously authorized, monitored, journalized, documented, tested, and accomplished by designated personnel. This assures that no one, anywhere in the world, can write program code to be spontaneously downloaded and executed as allowed in PC or Servers.

Mainframe programs cannot access files for which they ***were not authorized or designed for***. In other words, an email program, processing mail will not have access to a financial database, power plant infrastructure, or other critical systems. Moreover, the imputing device, could not send program code to the mainframe for execution.

Customer service programs can only access portions of a customer's data. Moreover, only after identifying specifics such as name, address, or SS number are input to retrieve a **synopsis** of a single customer record. Terminals ***cannot automate that process.*** Hence, it would be virtually impossible, or **undetectable**, to download a complete database, ***one record at a time.***

This emphasizes the impossibility that a hacker would have to know some specifics of ***every customer*** before gaining a copy of each record. Personal computers and their operating systems have increased productivity a thousand-fold, but that functionality has been abused and high-jacked. As an example, a program, in a PC or Server, activated by an email message, gets control from the OS until it relinquishes it. While in that mode, a hacked program can access data for which it was not designed or intended for, modify programming code, or it can even download, ransom, or destroy a database.

The Internet, originally designed for communication between scientists, engineers, and researchers was rushed into financial systems and infrastructure controlling systems like power plants. The ability to hack into power grids, pipelines, financial systems, military systems, and much more, is worrisome. Virus protection software may not prevent hacking. Most Viruses are designed to destroy. Hackers want to gain control or collect data.

Virus protection software is updated after a new de jour virus has manifested and maligned multiple computers. Thus, the constant updates required by virus protection software. The updates only protect computers that have not already been attacked by the de jour virus.

Hacker code and viruses are usually unleashed by clicking on Internet links, viewing photos, or opening attachments that contain malicious code. Stolen IDs or PWs are not needed. Now, review the questions at the top of this document. Hacking into today's **mainframe systems is virtually unheard of.** There are preventive measures that can be used before PC and server operating systems are improved. The solutions to prevent hacking are **obvious and readily available.**

Inexperienced reporters or techies will say "Mainframes can be hacked." This is only true if the mainframe is running a PC or Server type OS. Mainframe manufacturers, to be competitive, allow customers to run PC or Server type systems on their mainframes. That type of OS running on any mainframe has the same exposure as a PC or Server. Thus, mainframes running a normal mainframe OS are not susceptible to hacking.

John Piccolo
John@Piccolo.US