Tech Talk

ONE CLICK FIX

Jan. 2024 | Issue No. 13

Hackers Hacked Microsoft - for their own data!

Microsoft was hacked last Friday by the hacking group Midnight Blizzard. What was interesting about this attack, was that the attackers didn't go for customer data. They instead enumerated through files for data on themselves!

To be more specific, the hacking group wanted to know what Microsoft knew about them. They targeted email accounts for information related to their own group. The group gained access using a technique called password spraying, which is where an attacker tries millions of passwords to see what will work.

In 2024, several emerging technologies are expected to gain significant traction and have a considerable impact on various industries. Some of these technologies include:

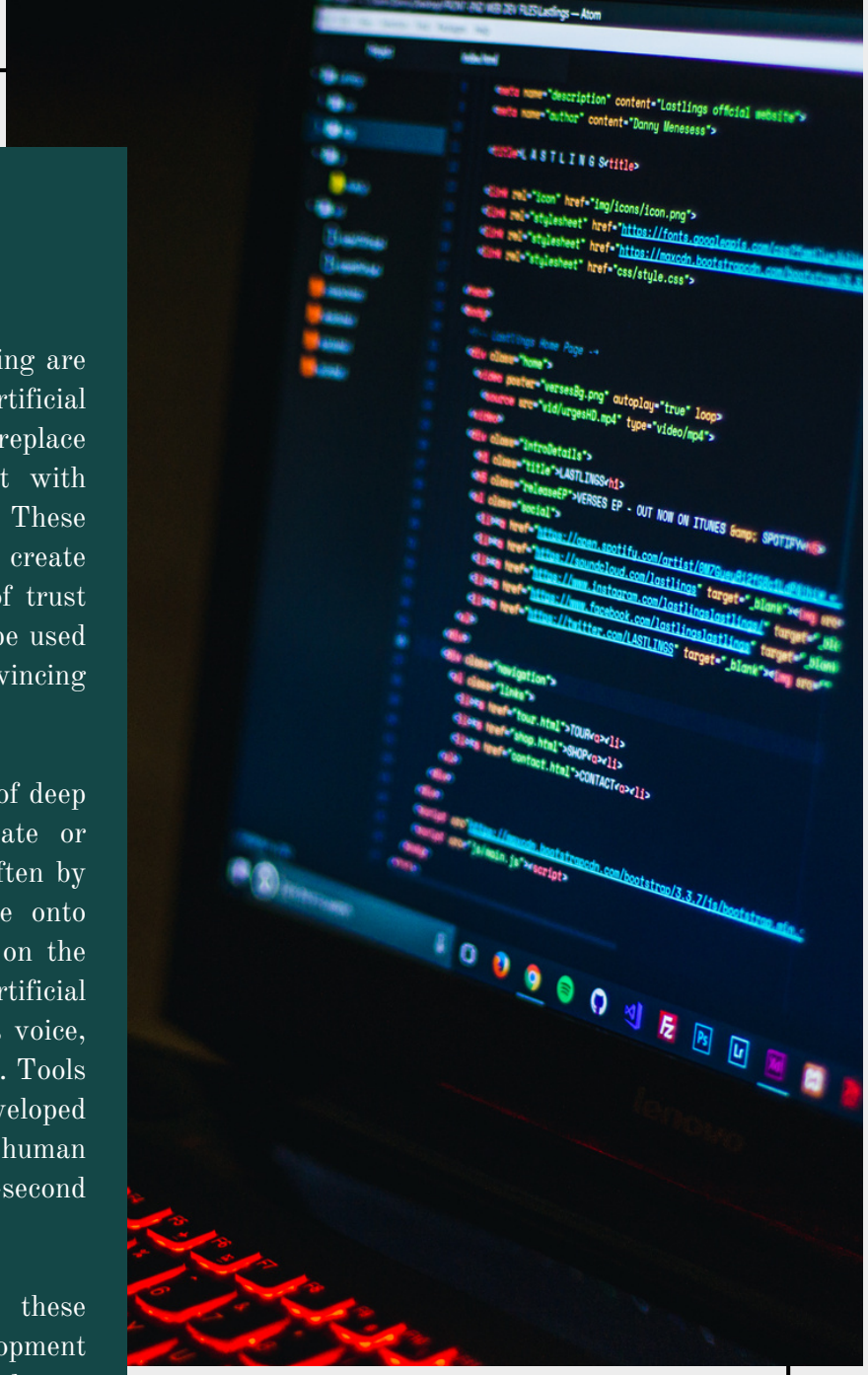
1. Quantum computing: The development of quantum computers is expected to continue, with companies like IBM, Google, and Intel working towards creating viable quantum systems.
2. Electric vehicles: The market for electric vehicles will continue to expand, with new personal eVTOLs, electric trucks, electric boats, and electric scooters being introduced.
3. Brain-computer interfaces: Companies like Synchron are working on brain-computer interfaces, such as the stentrode, which can be inserted via catheter, bypassing the need for open brain surgery.
4. Deepfake detection: As deepfake technology becomes more sophisticated, the development of methods to detect and counter deepfake media will become increasingly important.

Fun Facts

1. If you were born before 1998, you are older than Google!
2. Email predated the World Wide Web and the World Wide Web actually started out as a series of separate intranets that were later connected together.
3. 'Google' is actually a misspelling of the intended name; it was supposed to be 'Googol'.

ONECLICKFIX

Amy's Corner: Deepfakes



Deepfake videos and voice spoofing are emerging technologies that use artificial intelligence to manipulate or replace existing audio or video content with synthesized, often fake, content. These technologies have the potential to create significant challenges in terms of trust and authentication, as they can be used to create highly realistic and convincing fake content.

Deepfake videos involve the use of deep learning techniques to manipulate or replace existing video content, often by superimposing one person's face onto another's body. Voice spoofing, on the other hand, focuses on creating artificial voices that can mimic a person's voice, often using just a short recording. Tools like VALL-E, an AI model developed by Microsoft, can replicate the human voice with only a three-second recording.

The rapid advancement of these technologies has led to the development of detection methods aimed at identifying fake content. However, the constant evolution of deepfake techniques makes detection a challenging task. As these technologies continue to develop, it is crucial for individuals and businesses to be aware of their potential risks and to stay informed about the latest detection methods and best practices for protecting themselves from potential misuse.

ONECLICKFIX

If you post a high quality photo online, a print out can be used as facial recognition..

ONECLICKFIX

WE DO ONSITES OR REMOTES 24/7 / 365

We're there when you need us - onsite or by remote - highly skilled, friendly service that gets it done. We take care of your servers, desktops, laptops, network, internet, and more. Addressing small problems before they become issues. And if your internet goes down, we address it immediately.

ENTERPRISE CIO SERVICES

Have an issue? Let us know, instantly, through our email ticketing system or helpdesk phone. We can also receive alerts regarding your various systems in real time. Not only can you treat us just like an internal IT department, but we can act as your CIO. We provide vision and oversight for your IT - making sure you're using it as a competitive advantage, ensuring your projects stay on budget, and helping you become compliant with industry regulations.

CYBER SECURITY CAN SAVE YOU $$$

Cyber security controls don't have to be expensive, and they can actually save you money. When we implement security controls, not only is your data safer, but so are your employees' actions. Having proper controls can help prevent a breach, which shuts most businesses down as they cannot pay the fines or cannot recover from the client-trust impact. Additionally, security controls can lower cyber security insurance costs!