EINPRESSWIRE

Employees exposed to rogue apps & BOTS daily

i2Chain's patent secures sharing of information across untrusted applications securely and confidently

SAN FRANCISCO, CALIFORNIA, USA, September 18, 2022 / EINPresswire.com/ -- Cybercriminals deploy rogue applications and BOTS that look and feel like corporate applications to steal employee credentials and gain access to sensitive classified information stores and their backups. The fraudulent apps impersonate legitimate programs by copying the names, logos, and other details to direct people to malicious portals and websites that look and feel like original brands. One unsuspecting employee can make way for the loss of sensitive, classified, or personally identifiable information. In several cases, the criminals succeed in ransomware and seek to damage the reputation of the brands.

December 2021 study by Positive Technologies stated, "hackers can successfully penetrate 93% of corporate networks." Veeam's 2022 research "Ransomeware Trends," says that 95% of attacks attempt infecting backups, 41% of data was encrypted in ransomware, and 31% of the enterprises who paid the ransom still could not recover their data.

i2Chain is delighted to obtain its third patent from USPTO #US11374912B2 to perform the exchange of documents with third-party applications securely.

"i2Chain's patent helps to share information across untrusted applications securely & with confidence", says Ajay Jotwani, Co-founder & CEO i2Chain. Ajay adds that the silver bullet of information security is to be a step ahead of cybercriminals, and the i2Chain IP provides ammunition to take a giant leap forward."

Dr. Mark Manasse, the lead researcher of the patent, adds, "the patent considers running untrusted viewers and editors in containerized environments with short-lived encrypted virtual file systems so that efforts to save unencrypted copies of the document can be prevented, preserving the security of the chain. We also virtualize paste operations to fail outside the container and to wipe the cut buffer and storage used in the virtual file system on exit."

> The silver bullet is to stay a step ahead of cybercriminals, and i2Chain provides ammunition to take a giant infosec leap forward - now, share information across untrusted applications with confidence”
>
> *Ajay Jotwani, Co-founder & CEO, i2Chain.*

In the last ten years, venture funds and enterprise CISOs missions funding initiatives to battle the ever-changing landscape of detection and response. Lately, enterprises are seeking strategies to prevent cyber crimes in active coordination with law enforcement agencies. The number of daily cyber crimes is on a reducing graph, albeit slowly.

Mainak Trivedi, the global head of engineering & operations at i2Chain, adds, "The patent ensures secure data exchange between the user device and the server. The application component(s) are further isolated by containerizing on the user device to form a virtual digital space unreachable to other entities and applications. Mainak adds, "enterprises can use the i2Chain APIs to create non-fungible, rights-enforced, & traceable information artifacts that are tamper-proof and hack-proof so you can retain control of information shared with untrusted applications.

Mainak Trivedi
i2Chain, Inc.
Press@i2Chain.com
Visit us on social media:
Facebook
Twitter
LinkedIn