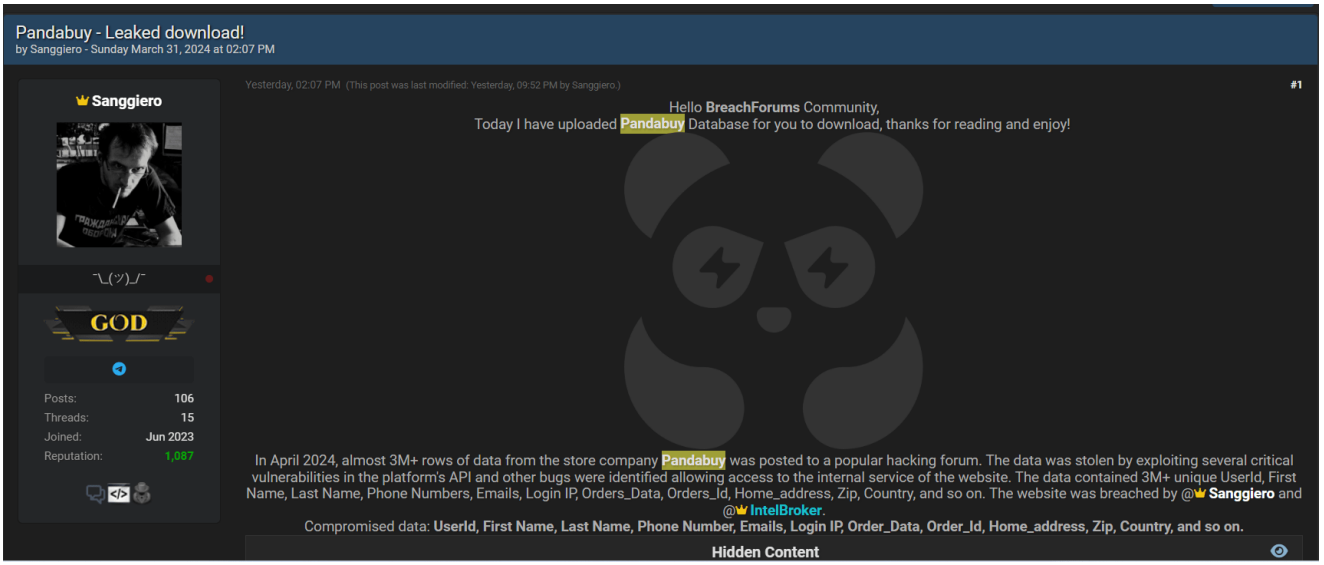
Pandabuy was extorted twice by the same threat actor

securityaffairs.com/164263/cyber-crime/pandabuy-extorted-again.html

June 7, 2024

Pierluigi Paganini June 07, 2024



Chinese shopping platform Pandabuy previously paid a ransom demand to an extortion group that extorted the company again this week.

The story of the attack against the Chinese shopping platform Pandabuy demonstrates that paying a ransom to an extortion group is risky to the victims.

BleepingComputer **first reported** that Pandabuy had previously paid a ransom to an extortion group to prevent stolen data from being published, but the same threat actor extorted the company again this week.

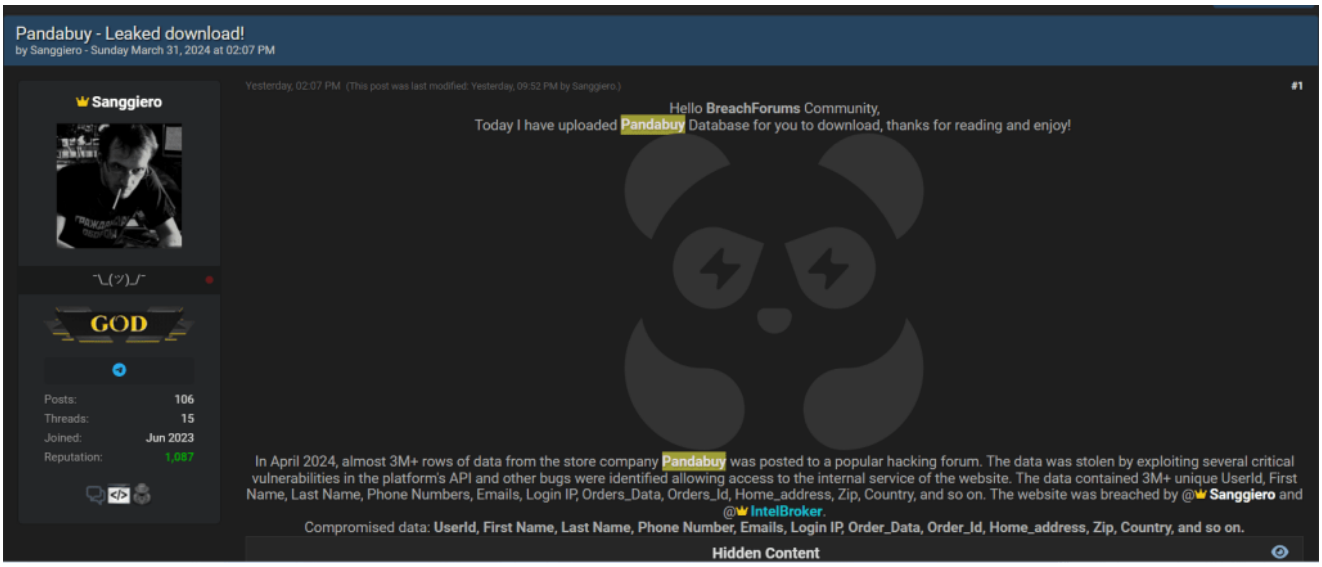
In April, at least two threat actors claimed the hack of the PandaBuy online shopping platform and leaked data of more than 1.3 million customers on a cybercrime forum.

The member of the BreachForums 'Sanggiero' announced the leak of data allegedly stolen by exploiting several critical vulnerabilities in Pandabuy's platform and API. Sanggiero said that he breached the platform with another threat actor named 'IntelBroker.'

> PandaBuy has been breached by Threat Actors operating under the names "Sanggiero" and "IntelBroker". Exfiltrated data includes:
>
> – UserId
> – First name
> – Last name
> – Phone number
> – Email
> – Login Ip
> – Full address
> – Order information
>
> Breach patrons are relatively excited pic.twitter.com/Gg0HLEMSj1
>
> — vx-underground (@vxunderground) April 1, 2024

Stolen data included UserId, First Name, Last Name, Phone Numbers, Emails, Login IP, Orders_Data, Orders_Id, Home_address, Zip, and Country.

*"In April 2024, almost 3M+ rows of data from the store company **Pandabuy** was posted to a popular hacking forum. The data was stolen by exploiting several critical vulnerabilities in the platform's API and other bugs were identified allowing access to the internal service of the website. The data contained 3M+ unique UserId, First Name, Last Name, Phone Numbers, Emails, Login IP, Orders_Data, Orders_Id, Home_address, Zip, Country, and so on. The website was breached by @Sanggiero and @IntelBroker." reads the announcement published by BreachForums.*



The data is available for sale on the cybercrime forum, Sanggiero published a sample as proof of the data breach.

HIBP founder Troy Hunt confirmed that 1.3 million email addresses are valid, the remaining addresses are duplicates. Hunt added the leaked addresses to HIBP, users can check if they have been impacted in the incident.

A company representative said on a Discord channel that the security breach took place in the past, he also added that the company security team said no data breach took place this year.

On June 3, 2024, Sanggiero offered the entire database he had previously stolen from Pandabuy for sale at $40,000. The actor claims the database contains more than 17 million lines, greater than the initial dataset offered in April, which included 1.3 million lines.

“A Pandabuy spokesperson admitted to BleepingComputer that they had paid the hacker an undisclosed amount to stop the data leak, adding that the threat actor may have shared the data with others, so they would no longer cooperate with him.” ***reported BleepingComputer****.*

The company attempted to downplay the incident saying that the data offered by Sanggiero is the same of the previous leak

Pandabuy added that they could not continue paying ransom due to frozen funds, anyway they addressed the vulnerabilities exploited in the original attack. The company speculates the threat actors had “secretly sold” their data to cybercriminals.

Pierluigi Paganini

(SecurityAffairs – hacking, cybercriminals)

you might also like

leave a comment