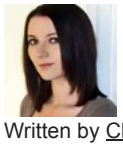
This new ransomware targets data visualization tool Jupyter Notebook

zdnet.com/article/this-new-ransomware-targets-data-visualization-tool-jupyter-notebook/

Home Innovation Security
Misconfigured environments are the entry point for the ransomware strain.



Written by Charlie Osborne, Contributor on March 30, 2022

-
-
-
-
-

A new strain of Python ransomware is targeting environments using Jupyter Notebook.

See also


ar Customer:

is time to pay for your software lease from PC Cyborg Corporation.
mplete the INVOICE and attach payment for the lease option of your choice.
you don't use the printed INVOICE, then be sure to refer to the important
ference numbers below in all correspondence. In return you will receive:

a renewal software package with easy-to-follow, complete instructions;
an automatic, self-installing diskette that anyone can apply in minutes.

portant reference numbers: A5599796-2695577-

e price of 365 user applications is US$189. The price of a lease for the
fetime of your hard disk is US$378. You must enclose a bankers draft,
shier's check or international money order payable to PC CYBORG CORPORATIO
r the full amount of $189 or $378 with your order. Include your name,
mpany, address, city, state, country, zip or postal code. Mail your order
PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Ransomware: An executive guide to one of the biggest menaces on the web

Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC is infected.

Read now

Jupyter Notebook is an open source web environment for data visualization. The modular software is used to model data in data science, computing, and machine learning. The project supports over 40 programming languages and is used by companies including Microsoft, IBM, and Google, alongside numerous universities.

Aqua Security's Team Nautilus recently discovered malware that has honed in on this popular data tool.

While Jupyter Notebook allows users to share their content with trusted contacts, access to the app is secured through account credentials or tokens. However, in the same way, that businesses sometimes do not secure their AWS buckets, leaving them open for anyone to view, Notebook misconfigurations have also been found.

The Python ransomware targets those that have accidentally left their environments vulnerable.

The researchers set up a honeypot containing an exposed Jupyter notebook application to observe the malware's behavior. The ransomware operator accessed the server, opened a terminal, downloaded a set of malicious tools -- including encryptors -- and then manually generated a Python script that executed ransomware.

While the assault stopped without finishing the job, Team Nautilus was able to grab enough data to simulate the rest of the attack in a lab environment. The encryptor would copy and then encrypt files, delete any unencrypted content, and delete itself.

Aqua Security

It should be noted that no ransom note was included as part of the package, which the team suspects indicate one of two things: either the attacker was experimenting with their creation on the honeypot, or the honeypot timed out before the ransomware attack was completed.

While attribution isn't concrete, the cybersecurity researchers say they might be "familiar" with the miscreant due to their trademark checks before an attack begins.

Clues indicate the individual could be from Russia, and if it is the same attacker, they have been linked to cryptojacking attacks on Jupyter environments in the past.

A Shodan search reveals several hundred internet-facing Jupyter Notebook environments are open and accessible (although some may also be honeypots.)

"The attackers gained initial access via misconfigured environments, then ran a ransomware script that encrypts every file on a given path on the server and deletes itself after execution to conceal the attack," the researchers said. "Since Jupyter notebooks are used to analyze data and build data models, this attack can lead to significant damage to organizations if these environments aren't properly backed up."

See also

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0
