Snake Malware Analysis from ANY.RUN

DUBAI, DUBAI, UAE, May 11, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the Snake infostealer.
Here are some highlights from the inner workings of Snake:

What is Snake

Snake is a modular infostealer and keylogger that was initially discovered in November 2020. Developed using the .Net programming language, it exhibits similarities with the AgentTesla, Formbook, and Matiex malware families, particularly in its staging mechanism.

Snake poses a significant risk to privacy due to its ability to exfiltrate a broad range of data. Its capabilities include:
• Keyboard capturing
• Clipboard hijacking
• Credential theft
• Screen recording

Snake is capable of stealing credentials from over 50 applications, including popular web browsers and file transfer clients, such as FileZilla. Notably, this malware is also able to steal wireless network profiles.

Snake keylogger execution process

As a typical stealer, Snake keylogger doesn't produce a lot of noticeable activity, which makes its detection potentially tricky. However, once it's established on an infected machine, it may increase its activity — capturing more data and sending it to the command-and-control server.

The Snake malware uses a variety of tactics and techniques. Key strategies include:
• exploiting client vulnerabilities for initial access
• extracting credentials from files and password stores
• querying the system registry
• and collecting local emails.

Distribution of Snake malware

As is common with Malware-as-a-Service families, Snake is distributed through mass email phishing campaigns and targeted spearphishing. It is known to arrive via infected Microsoft Office documents or PDFs, typically embedded in payment-related messages.

Upon the user extracting the executable, it proceeds to decode and decrypt the base-64 payload, which is contained within a string variable.

Snake malware conclusions

Snake is a powerful infostealer and keylogger that targets various industries and platforms, capable of extracting a wide range of data. Its sandbox evasion capabilities only add to the challenge of detection and analysis.

Read more with the code & scripts examples in the article at ANY.RUN.

Vlada Belousova
ANYRUN FZCO
2027889264
email us here
Visit us on social media:
Twitter
YouTube