ANY.RUN Shares Technical Analysis on HawkEye Keylogger Malware and Its Attacks

DUBAI, DUBAI, UNITED ARAB EMIRATES, November 13, 2024 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, released a detailed report on the HawkEye malware, also known as PredatorPain. The research provides critical insights into the malware's evolution, delivery methods, technical behavior, and advanced functionalities.

□□□□□ □□□□□□□ □□□□□□□□□

HawkEye emerged before 2010 and gained significant popularity through spearphishing campaigns starting in 2013. The malware has been widely distributed on dark web sites and has been cracked, allowing widespread use by various actors. It saw a resurgence during the COVID-19 pandemic.

HawkEye has evolved from a simple keylogger into a sophisticated stealer with capabilities such as credential and wallet theft, screenshot capture, and security software detection.

HawkEye is also commonly used in conjunction with other malware like Remcos and Pony.

□□□□ □□□□□□□□ □□□□□□□□

The report goes in-depth on the technical aspects of HawkEye attacks which mostly follow the same pattern:

· The malware drops multiple copies of itself in temporary directories and injects code into

legitimate software processes to avoid detection.

· It establishes persistence through registry keys and task scheduling, using obfuscation techniques to hide its persistence mechanisms.

· HawkEye collects a wide range of data, including keystrokes, clipboard data, system information, and credentials.

· It uses various methods for information exfiltration, including FTP, HTTP, and SMTP.

Read the full report on ANY.RUN's blog.

About ANY.RUN

ANY.RUN serves over 500,000 cybersecurity professionals globally, offering an interactive platform for malware analysis targeting Windows and Linux environments. With advanced threat intelligence tools such as TI Lookup, YARA Search, and Feeds, ANY.RUN enhances incident response and provides analysts with essential data to counter cyber threats effectively.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
LinkedIn