ANY.RUN Exposes Malicious Methods for Bypassing Windows 11 User Account Control

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 21, 2024 /EINPresswire.com/ -- Cybersecurity experts at ANY.RUN have published new research on the top User Account Control (UAC) bypass methods employed by modern malware. The piece provides valuable insights into the tactics used by malicious actors to exploit Windows 11 systems and includes real-world examples from threats such as FormBook, LockBit, and BlankGrabber.

□□□□□ □□□□ □□□□□□□ □□□□□□□ (□□□) User Account Control (UAC) is a security feature in Windows operating systems that helps prevent unauthorized changes to the system. UAC prompts users for permission or credentials when an application or task requires administrative-level access, ensuring that users are aware of the potential risks before proceeding.

ANY.RUN covers the three primary methods used to bypass UAC in Windows 11:

□□□□□□□□□□□□ □□ □□□ □□□□□□□□□□ □□□□ □□□ □□□□-□□□□□□□ □□□□□□□□

Malware families, such as FormBook and LockBit, abuse the Component Object Model (COM) interfaces, gaining elevated privileges without triggering the UAC prompt. Some of the examples of COM objects include cmstplua and colorui.

□□□□□□□□□□□□ □□ □□□ □□-□□□□□□□□ □□□□□□□□ □□□□□□

Malicious actors can manipulate the ms-settings registry branch to bypass UAC and execute unauthorized actions. BlankGrabber is one of the prominent examples of malware with such capabilities.

□□□□□□□□□ □□□ □□□□□□ □□□□
This technique bombards users with an endless loop of UAC prompts, relying on their actions to gain access. The experts at ANY.RUN have uncovered DCrat and PureMiner samples using this method.

Learn more about UAC bypass methods and discover real-world examples on ANY.RUN's blog.

About ANY.RUN

ANY.RUN is a provider of cybersecurity products. Its sandbox enables malware analysts to quickly and accurately analyze malicious files and links, gaining a complete view of advanced cyber attacks. The platform's threat intelligence services, including TI Lookup, Yara Search, and TI Feeds, present users with up-to-date data on the latest malware currently active across the globe. The company is currently celebrating its 8th birthday with special offers that include six months of free service and extra licenses for enterprises.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
Twitter
YouTube
