# XWorm Technical Analysis: New Malware Version

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 29, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the XWorm Malware Analysis. Here are some highlights from the latest version of a XWorm sample:

□□□□ □□ □□□□□

XWorm is a malware that targets Windows operating systems. It is known for its stealth and persistence, and a wide range of malicious activities, spanning from remote desktop control to ransomware and information theft. Adversaries employ this threat widely —it's not uncommon to see it in ANY.RUN's top 10 most used malware by uploads.

□□□□□ □□□□□□□ □□□□□□□ □□□□□□□□

While searching for new threats, ANY.RUN discovered an interesting sample, uploaded by users to Public submissions. It was downloaded from the file hosting "Mediafire" in a RAR archive with a password.

□□□□□ □□□□□□ □□□□□□□□

The investigation shows how researchers:
• Bypassed XWorm's virtualization detection.
• Decrypted the malware's C2 communication.
• Detailed the full range of evasion techniques used by XWorm.

• Identified an off-by-one error in its code.
• Obtained the complete set of the sample's IOCs.

□□□□□□□□ □□□□□□□□□□□□: □□□□□□ □□□□□□□ □□□□□□□□□□□

After a brief review of the methods' contents, a constructor was found that bears a striking resemblance to a block containing settings.
ANY.RUN's final AES key looks like this:
"01d31d5e811fce422987107f962c4001d31d5e811fce422987107f962c406600."

ANY.RUN efficiently extracts configurations for malware like XWorm, ultimately saving security researchers precious time and resources.

Read the article to see how ANY.RUN successfully analyzed the functionality of XWorm sample, as well as extracted its configuration.

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