EINPRESSWIRE

Cybersecurity Firm ANY.RUN Releases Reports on Four Active Malware Families

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 13, 2024 /EINPresswire.com/ -- ANY.RUN, a leader in interactive malware analysis, has published detailed reports on four significant and active malware families: BlackBasta, DarkTortilla, SSLoad, and WarmCookie. These reports, now available on ANY.RUN's Malware Trends Tracker page, allow cybersecurity professionals to collect necessary information to detect, analyze, and develop effective protection strategies against these evolving threats.

□□□□□□□□ □□ □□□□□□□ □□□□□□□□

1. □□□□□□□□□□: A ransomware-as-a-service (RaaS) run by Storm-1811, known for double extortion: encrypting and stealing data for ransom. First identified in 2022, it often infiltrates systems via spear-phishing, using tools like QakBot and Cobalt Strike, making it a highly sophisticated threat.

ANY.RUN's sandbox analysis has provided a detailed breakdown of BlackBasta's infection process, from initial access to the final encryption stages.

2. □□□□□□□□□□□□: A multi-stage crypter used by attackers to spread a variety of harmful payloads, including RATs and information stealers. Active since 2015, DarkTortilla is known for its ability to evade detection by running payloads directly in memory and using social engineering tactics to remain hidden.

ANY.RUN has revealed how DarkTortilla operates, from its initial loading to injecting the main malicious payload into the system through the core processor.

3. □□□□□□: A sophisticated malware loader that downloads and executes additional payloads on compromised systems. It evades detection using encryption and in-memory execution, often spread through phishing emails as part of a broader Malware-as-a-Service (MaaS) operation. ANY.RUN’s analysis highlights SSLoad’s complex methods, including its use of MSI installers and DLL side-loading to bypass security measures.

4. □□□□□□□□□□: Also known as BadSpace, this two-stage backdoor malware spreads via phishing emails mimicking job sites, granting attackers remote access to steal data, deploy malware, and maintain control over infected systems.

ANY.RUN’s sandbox analysis demonstrates how WarmCookie establishes its foothold on targeted systems and communicates with its C2 servers.

□□□ □□ □□□□□□□□ □□□□□□ □□□□□□□□ □□□□□ □□□.□□□

ANY.RUN’s interactive sandbox offers cybersecurity professionals the tools to deeply analyze these malware families. By uploading samples to the sandbox, users can observe real-time malware behavior, monitor network traffic, and extract valuable Indicators of Compromise (IOCs) to strengthen their defenses.

For a comprehensive look at how these malware operate and to explore the full reports, visit the ANY.RUN’s blog.

□□□□□ □□□.□□□

ANY.RUN supports over 400,000 cybersecurity professionals worldwide with its innovative sandbox and threat intelligence tools. Specializing in both Windows and Linux malware analysis, ANY.RUN’s platform provides fast and detailed insights, enabling users to detect, analyze, and respond to emerging threats effectively.

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