eSentire vs. Phantom: Unveiling the Cyber Spook's Dance of Darkness

By Ddos

Published: 2023-12-26 · Archived: 2026-04-05 17:57:43 UTC

An example of the traffic for the SwaetRAT | Image: Esentire

In the shadowy realms of cyber threats, a formidable entity known as PhantomControl has emerged, marking its presence with intricate and sophisticated cyberattacks. First observed by eSentire's Threat Response Unit in November 2023, PhantomControl's modus operandi is as stealthy as it is effective, utilizing phishing emails as its initial infection vector. The sinister dance begins with a malicious redirection to a compromised website, cleverly concealing a ScreenConnect client. This client, when run, establishes a connection to a controlled instance, laying the groundwork for the actor's nefarious activities.

The ingenuity of PhantomControl doesn't end there. Their arsenal includes a VBS script that fetches and executes content from an external domain, cleverly hiding its true intentions with garbled strings and reversed sequences. This script, once deobfuscated, reveals a complex mechanism involving PowerShell scripts, image-based data retrieval, and .NET binary payloads, aptly named Ande Loader.

An example of the traffic for the SwaetRAT | Image: Esentire

PhantomControl, a chameleon in the digital world, has previously been associated with the Blind Eagle threat actors, known for their focus on delivering RATs (Remote Access Trojans) to Latin American countries. This association underscores the threat actor's versatility and reach.

A deep dive into their toolkit unveils SwaetRAT, a potent 32-bit RAT developed in .NET, boasting capabilities like keylogging and system information harvesting. This RAT, constantly on the prowl for sensitive data, diligently records keystrokes and searches for specific strings, sending valuable information back to the command-and-control center.

The sophistication of PhantomControl lies not just in its attack vectors but in its ability to seamlessly blend into the digital environment. By creating mutexes for self-checks and employing intricate command parsing techniques, PhantomControl ensures its persistence and evasion from detection.

As cyber threats evolve, PhantomControl stands as a testament to the ever-increasing complexity and stealthiness of modern cyber adversaries, posing significant challenges to cybersecurity defenses worldwide.

Support Our Threat Intelligence

If you find our CVE report and cybersecurity news helpful, consider supporting our work.

Post navigation
