YiBackdoor Arrives: What You Need to Know and How to Protect Your Net

Data: 2025-09-26 15:57:03

Autor: Inteligência Against Invaders

Redazione RHC**:26 September 2025 16:01**

In a new report, Zscaler ThreatLabz has revealed details of a new malware family called **YiBackdoor** , first observed in June 2025.

From the outset, *the analysis highlighted significant source code matches with the IcedID* and *Latrodectus* downloaders, and it is this connection that Zscaler points to as crucial to understanding the new sample's possible origin and role in the attacks.

The malware is a **modular DLL library** with a basic set of host remote control functions and a plugin-based extension mechanism. By default, its functionality is limited, *but attackers can load additional modules to expand its capabilities.*

The program copies itself to a newly created folder with a random name, gains persistence via the Windows Run key, and launches regsvr32.exe with a malicious path.

The registry entry name is generated using a pseudorandom algorithm. The primary module self-destructs, complicating response measures and forensic analysis. The malicious logic is executed via an **embedded encrypted configuration** , from which the command and control server address is extracted, and communication with the C2 occurs via HTTP responses containing commands.

YiBackdoor's capabilities include *collecting system metadata, taking screenshots, and executing shell commands via cmd.exe and PowerShell, as well as loading and initializing Base64-encrypted plugins.* Key commands identified in the control mechanism are listed below: **Systeminfo, screen, CMD, PWS, plugin, and task** . Code injection involves injecting code into the svchost.exe process, and built-in anti-analysis techniques focus on detecting virtual machines and sandboxes, reducing the likelihood of detection when analyzing in a protected environment.

Zscaler analysts **note several similarities with IcedID and Latrodectus** : a similar injection method, identical format and length of the configuration decryption key, and similar algorithms for decrypting configuration blocks and plugins. Given these similarities and the observed architecture, *the company's employees assess YiBackdoor with a moderate to high level of confidence.* However, current implementations are limited, indicating a development or testing phase and **the potential role of the sample as a precursor to subsequent exploitation stages** , including preparing initial access for the ransomware.

The organization emphasizes *the importance of monitoring outgoing HTTP requests and registry changes, as well as implementing detection rules that focus on behavioral indicators of svchost.exe* *injections and anomalies associated with regsvr32.exe launches from random locations.* These indicators enable early detection of YiBackdoor injection attempts and prevent further attacker activity.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli