AL2025_40 New YiBackdoor Malware Shares Major Code Overlaps with IcedID and Latrodectus (September 24th, 2025)

Description

In June 2025, Zscaler ThreatLabz discovered a new malware family named YiBackdoor, which shows significant source code overlap with IcedID and Latrodectus. Researchers assess with medium-to-high confidence that the malware is linked to the same developers behind those loaders. YiBackdoor enables attackers to execute arbitrary commands, collect system information, capture screenshots, and deploy additional plugins to expand functionality. Current detections indicate limited deployment, suggesting YiBackdoor is still under development or undergoing testing.

Attack Details

YiBackdoor infection begins by copying itself (a DLL) into a randomly named directory and establishing persistence through a Windows Run registry key entry using regsvr32.exe. To hinder forensic analysis, the malware self-deletes after setup. It then injects into svchost.exe to blend in with legitimate processes.

The malware contains an embedded encrypted configuration that extracts the command-and-control (C2) server. It communicates via HTTP, receiving instructions and encrypted plugin payloads. Supported commands include:

- systeminfo – collect host metadata
- screen – capture screenshots
- CMD – execute shell commands via cmd.exe
- PWS – execute commands via PowerShell
- plugin – interact with existing plugins and return results
- task – initialize and execute a new Base64-encoded, encrypted plugin

YiBackdoor employs rudimentary anti-analysis techniques to evade sandboxed or virtual environments. Code overlap has been confirmed in its injection methods, configuration decryption routines, and plugin handling compared to IcedID and Latrodectus. Researchers note that Latrodectus itself is believed to be a successor of IcedID, placing YiBackdoor within the same malware lineage.

Remediation

- Deploy EDR/AV signatures and YARA/Sigma rules to catch YiBackdoor's decryption routines, injection, and plugin behavior.

- Monitor for svchost.exe with unusual child threads, injected modules, or outbound connections to suspicious endpoints.
- Enable PowerShell logging (ScriptBlock, Module, transcription) to detect misuse.
- Inspect HTTP/HTTPS traffic for encoded payloads (X-tag header, small, encrypted POST/GET) and DNS anomalies that may indicate tunneling.
- Block or restrict usage of regsvr32.exe via AppLocker or Windows Defender Application Control.
- Enforce least privilege; remove local administrator rights where it's not necessary.
- Limit outbound HTTP and DNS to trusted channels; segment internal networks.
- Maintain resilient backups and a tested IR playbook.
- Train users on phishing tactics and monitor for loader malware delivery patterns.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News, New YiBackdoor Malware Shares Major Code Overlaps with IcedID and Latrodectus (September 24th, 2025).The Hacker News. https://thehackernews.com/2025/09/new-yibackdoor-malware-shares-major.html

- Zscaler ThreatLabz, YiBackdoor: New Malware Family Links to IcedID and Latrodectus. Zscaler. (September, 2025). Retrieved from Zscaler ThreatLabz. https://www.secureblink.com/cyber-security-news/py-pi-shuts-down-stolen-tokens-after-massive-ghost-action-supply-chain-attack