Crypto24 ransomware hits large orgs with custom EDR evasion tool - Agai

Data: 2025-08-14 19:02:57

Autor: Inteligência Against Invaders

The Crypto24 ransomware group has been usingcustom utilities to evade security solutions on

breached networks,exfiltrate data, and encrypt files.

The threat group'searliest activity was reported on BleepingComputer forums in September 2024, though it never reached notable levels of notoriety.

According to Trend Micro researchers tracking Crypto24's operations, the hackers havehit several large organizations in the United States, Europe, and Asia, focusing on high-value targets in the finance, manufacturing, entertainment, and tech sectors.

The security researchers report that Crypto24 appears to be knowledgeable and well-versed, suggesting a high likelihood that it was formed by former core members of now-defunct ransomware operations.

Post-compromise activity

After gaining initial access, Crypto24 hackers activate default administrative accounts on Windows systems within enterprise environmentsor create new local user accounts for stealthy, persistent access.

Following a reconnaissance phase using a custom batch file and commands that enumerate accounts, profile system hardware, and the disk layout, the attackercreatesmalicious Windows services and scheduled tasks for persistence.

The first is WinMainSvc, a keylogger service, and the second is MSRuntime, a ransomware loader.

[IMAGEM REMOVIDA]Trend Micro researchers say.

“The file in question is a legitimate tool provided by Trend Micro for troubleshooting, specifically to resolve issues such as fixing inconsistent agents within Trend Vision One deployments.”

“Its intended use is to cleanly uninstall Endpoint BaseCamp when required for maintenance or support.”

This tool essentially prevents the detection of follow-on payloads like the keylogger (WinMainSvc.dll) and the ransomware (MSRuntime.dll), both custom tools.

The keylogger, which masquerades as “Microsoft Help Manager,” logs both active window titles and keypresses, including control keys (Ctrl, Alt, Shift, function keys).

The attackers also use SMB shares for lateral movement and staging files for extraction.

All stolen data is exfiltrated to Google Drive using a custom tool that leverages the WinINET API to interact with Google’s service.

The ransomware payload executes after deleting volume shadow copies on Windows systems to prevent easy recovery.

[IMAGEM REMOVIDA]indicators of compromise that other defenders can use to detect and block Crypto24 ransomware attacks before they reach the ultimate stages.

Bill Toulas

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

You may also like: