2025

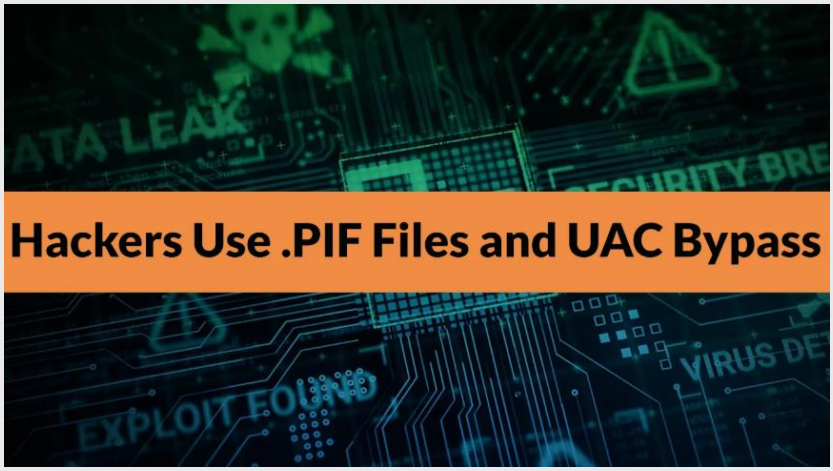
Cyber Threat and Intelligence Awareness Report

CryptoGen

the security focus company

CryptoGen | the security focus company

Hackers Use .PIF Files and UAC Bypass to Drop Remcos Malware on Windows



ID : **0142**

Severity : **High**

CTIA Type : General

Date : **07 July 2025**

Time: **22.00 pm**

Executive Summary

A newly identified multitarget phishing campaign has been identified that delivers the infamous **Remcos Remote Access Trojan (RAT)** via the usage of outdated file formats and evasion methods in Windows files. The attack chain originates with phishing emails with malicious archives. These archives contain an executable file labeled as "**FAKTURA,**" which facilitates the deployment of the **DBatLoader** malware into the target computer. This multi-step campaigns exploit attackers capitalizes on the legitimate windows functionalities and outdated file formats to bypass modern security solutions. Determined by **Any.Run** using sandbox analysis, the attack uses Program Information Files **(.pif)** which were originally designed to be used with **DOS applications** to hide malicious executables. It was more dangerous because other hackers might use the attacks methods. Task abuse creates a robust infection framework that challenges traditional detection methodologies and requires advanced behavioral analysis for identification.

Infection Mechanism and UAC Bypass Techniques

The campaign exploits .pif files and Windows folder name vulnerabilities allowing the malware to gain elevated privileges without triggering standard **UAC (User Account Control)** prompts. It uses **PING.EXE** to create delays for evasion. Persistence is maintained via scheduled tasks triggering a **Cmwdnsyn.url** file that launches the **.pif** dropper. **BatCloak** obfuscates **.cmd** files, and **extrac32.exe** manipulates Windows Defender exclusions. **Remcos** are injected into trusted processes like **SndVol.exe** and **colorcpl.exe** to evade detection.

Mitigation Strategies

- Block or monitor use of **.pif files** like alpha.pif.
- Prevent or detect the creation of directories with **trailing spaces**.
- Monitor and control use of **PING.EXE** for repeated pings to 127.0.0.1.
- Train users to recognize and avoid **phishing emails** containing malicious archives like those with the "FAKTURA" executable.
- Conduct effective cyber security awareness training for the organization's employees.

References

- https://cybersecuritynews.com/hackers-use-pif-files-and-uac-bypass/#google_vignette