LevelBlue - Open Threat Exchange

By ChrisTan0

Archived: 2026-04-02 10:45:29 UTC

- 41 Subscribers

Unauthorized RDP Connections For Cyberespionage Operations

CVE: 5 | **FileHash-MD5:** 4 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 9 | **URL:** 7

Cyble Research and Intelligence Labs uncovered an ongoing cyberattack campaign utilizing malicious LNK files to gain unauthorized Remote Desktop access on compromised systems. The sophisticated multi-stage attack chain employs PowerShell and BAT scripts to evade detection, create administrative accounts, and alter Remote Desktop settings. The campaign, named 'HeptaX', has been active since 2023, targeting various sectors with consistent techniques. It involves the deployment of ChromePass, a tool for stealing saved passwords from Chromium-based browsers. The attack begins with a ZIP file containing a malicious shortcut, likely distributed via phishing emails, and progresses through multiple stages of payload downloads and executions, ultimately enabling the threat actors to establish remote access for further malicious activities.

- 373,183 Subscribers

Space Pirates: Explore the tools and connections of a new hacker group

CVE: 1 | **FileHash-MD5:** 156 | **FileHash-SHA1:** 150 | **FileHash-SHA256:** 150 | **URL:** 1 | **Domain:** 5 | **Email:** 1 | **Hostname:** 56

At the end of 2019, specialists from the Positive Technologies security expert center (PT Expert Security Center , PT ESC) discovered a phishing email targeting one of the enterprises in the Russian aerospace industry. It contained a link to previously unknown malware. Our experts discovered the same malware in 2020 while investigating an information security incident in one of the Russian government organizations. In the course of this work, several new malware families were also discovered using a common network infrastructure, while some of them were not previously mentioned in open sources.

- 354 Subscribers

- 840 Subscribers

Cycldek: Bridging the (air) gap | Securelist

A Chinese threat actor has developed new capabilities to target air-gapped systems in an attempt to exfiltrate sensitive data for espionage, according to a newly published research by Kaspersky

- 65 Subscribers

Indicators Search

Show expired indicators

We've found 39 indicators

Source: https://otx.alienvault.com/browse/pulses?q=tag:chromepass