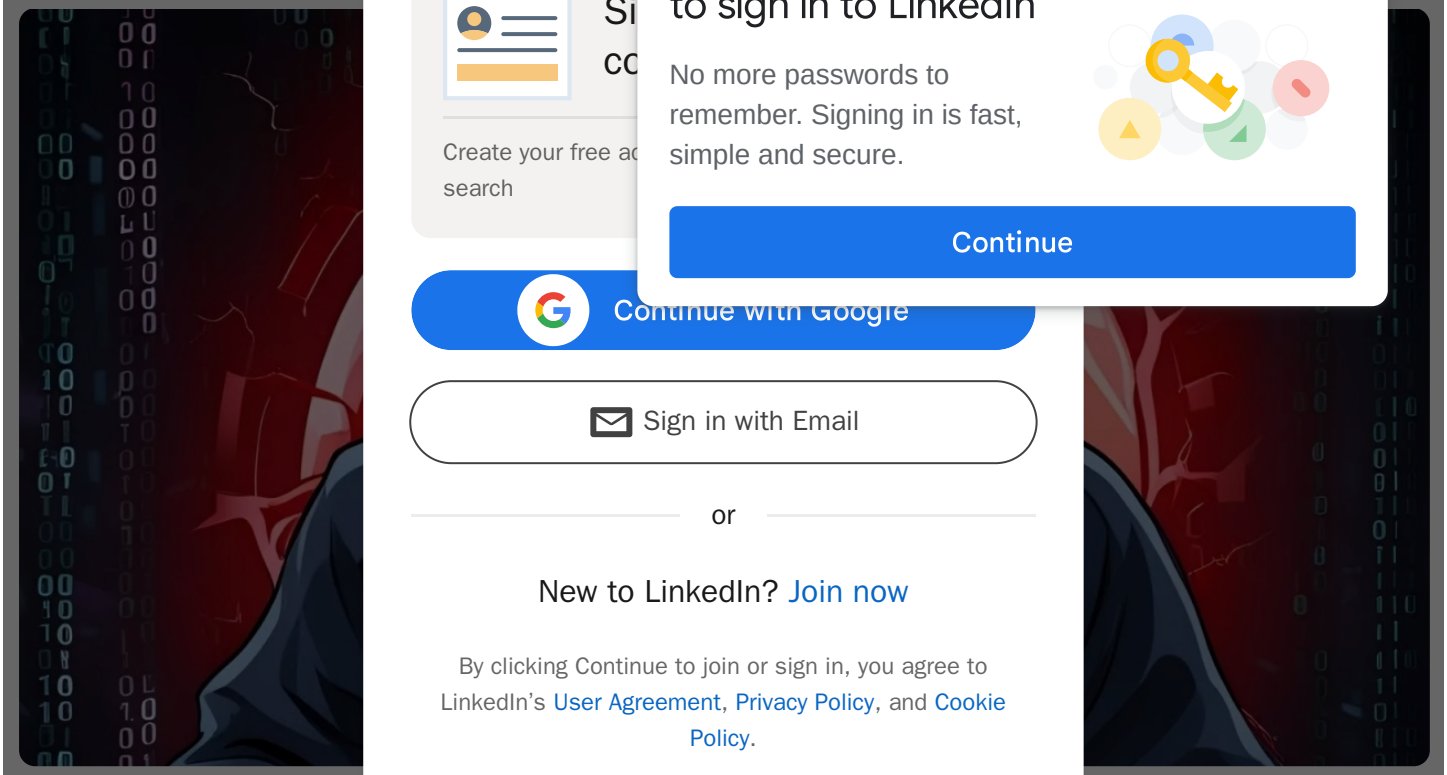
Top Content



RansomHub Ransomware Deploys Malware to Breach Corporate Networks

Ethical Hackers Academy ®

Ethical Hackers Academy is the #1 most trusted e-Learning portal with 100+ advanced cyber security courses.

Published Apr 29, 2025

SocGholish Malware as Initial Vec

RansomHub market MP (Russian Anonymous Market ion.

The infection chain l a malicious file named "Update.zip."

This file contained a mmunication with a SocGholish Comma oods[.]com" to fetch and execute s

Technical Depth: M sion Tactics

The SocGholish scri , harvesting critical system information and processor architecture, which v erver via HTTP POST requests.

Utilizing Living Off the Land Binaries (LOLBins) like net.exe and systeminfo, the malware gathered network and system details, while PowerShell commands enumerated servers in Active Directory and extracted browser credentials from Microsoft Edge and Google Chrome, including encryption keys for stored sensitive data.

Within roughly 6.5 minutes of initial contact, a Python-based backdoor was retrieved, renamed to "python3.12.zip," unpacked, and executed via a scheduled task.

complex layered defense against ana

The final stage reve 38.146.28[.]93," enabling SOCKS pro movement within compromised netwo reports on similar TTPs.

According to eSentir c patience of RansomHub affiliate gets post-discovery, bypassing ers.

The deployment of S ed with a Python backdoor for persist payloads designed for stealth and impa

Organizations must DR) solutions to identify anomalous l ks or network traffic to suspicious domai

Regular patching of ing on phishing and social engineering ta anisms are critical to mitigate such thr

eSentire's 24/7 Security Operations Centers (SOCs), backed by Elite Threat Hunters and the TRU team, continue to track and respond to such incidents, reinforcing the need for proactive cybersecurity in an era where adversaries operate beyond conventional schedules.

Source: https://gbhackers.com/ransomhub-ransomware-deploys-malware/

for Windows 11, version

56 · 1 Comment

Apr 3, 2

New P

Secur

in the

emote Takeover

critical exploit chain

Apr 3, 2

CISA I

The U

Show more

Explore content

Career

Productivity

Project Management

Show more