



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

26 Feb 25

## Cyber Threat Roundup

*A collection of recent open-source items of interest to the Defense Industrial Base*

### Contents

Articles .....	2
New Auto-Color Linux Backdoor Targets North American Govts, Universities .....	2
GitVenom Attacks Abuse Hundreds of GitHub Repos to Steal Crypto.....	2
Belarus-Linked Ghostwriter Uses Macropack-Obfuscated Excel Macros to Deploy Malware .....	2
New LightSpy Spyware Variant Comes with Enhanced Data Collection Features Targeting Social Media Platforms.....	2

## Articles

### **New Auto-Color Linux Backdoor Targets North American Govts, Universities**

A previously undocumented Linux backdoor dubbed 'Auto-Color' was observed in attacks between November and December 2024, targeting universities and government organizations in North America and Asia. According to Palo Alto Networks' Unit 42 researchers who discovered the malware, it is highly evasive and difficult to remove from infected systems, capable of maintaining access for extended periods. Given its stealth, modular design, and remote control features, Auto-Color is a serious threat to Linux systems, particularly those in government and academic environments targeted in the observed attacks.

<https://www.bleepingcomputer.com/news/security/new-auto-color-linux-backdoor-targets-north-american-govts-universities/>

### **GitVenom Attacks Abuse Hundreds of GitHub Repos to Steal Crypto**

A malware campaign dubbed GitVenom uses hundreds of GitHub repositories to trick users into downloading info-stealers, remote access trojans (RATs), and clipboard hijackers to steal crypto and credentials. According to Kaspersky, GitVenom has been active for at least two years, targeting users globally but with an elevated focus on Russia, Brazil, and Turkey. The researcher explains that the fake repositories are crafted with care, featuring details and appropriately written readme files, likely with the help of AI tools. Moreover, the threat actors employ tricks to artificially inflate the number of commits submitted to those repositories, creating a fake image of high activity and increasing credibility.

<https://www.bleepingcomputer.com/news/security/gitvenom-attacks-abuse-hundreds-of-github-repos-to-steal-crypto/>

### **Belarus-Linked Ghostwriter Uses Macropack-Obfuscated Excel Macros to Deploy Malware**

Opposition activists in Belarus as well as Ukrainian military and government organizations are the target of a new campaign that employs malware-laced Microsoft Excel documents as lures to deliver a new variant of PicassoLoader. The threat cluster has been assessed to be an extension of a long-running campaign mounted by a Belarus-aligned threat actor dubbed Ghostwriter (aka Moonscape, TA445, UAC-0057, and UNC1151) since 2016. It's known to align with Russian security interests and promote narratives critical of NATO.

<https://thehackernews.com/2025/02/belarus-linked-ghostwriter-uses.html>

### **New LightSpy Spyware Variant Comes with Enhanced Data Collection Features Targeting Social Media Platforms**

Cybersecurity researchers at Hunt.io have found an updated version of the LightSpy spyware that supports an expanded set of data collection features to target social media platforms like Facebook and Instagram. ThreatFabric researchers first discovered a macOS version of LightSpy spyware in May 2024, the threat has been active in the wild since at least January 2024. ThreatFabric observed threat actors using two publicly available exploits (CVE-2018-4233, CVE-2018-4404) to deliver macOS implants. The experts noticed that a portion of the

CVE-2018-4404 exploit is likely borrowed from the Metasploit framework.

<https://securityaffairs.com/174674/malware/new-lightspy-spyware-variant-data-collection-targets-social-media-platforms.html>