



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

19 Feb 25

## Cyber Threat Roundup

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

### Contents

Articles .....	2
WinRAR 7.10 Boosts Windows Privacy by Stripping MoTW Data .....	2
Snake Keylogger Slithers into Windows, Evades Detection with AutoIt-Compiled Payload .....	2
Why Rebooting Your Phone Daily Is your Best Defense Against Zero-Click Attacks .....	2
New FrigidStealer macOS Malware Distributed as Fake Browser Update .....	2

## Articles

### WinRAR 7.10 Boosts Windows Privacy by Stripping MoTW Data

WinRAR 7.10 was released yesterday with numerous features, such as larger memory pages, a dark mode, and the ability to fine-tune how Windows Mark-of-the-Web (MoTW) flags are propagated when extracting files. These new features include enabling larger memory pages for increased performance, a reworked settings interface, and a long-awaited dark mode. A "Zone.Identifier" tells Windows and supported applications that the file was downloaded from another computer or the Internet and, therefore, could be risky to open. If the file contains a MoTW, you will see a message at the bottom stating, "This file came from another computer and might be blocked to help protect this computer." MoTW is a powerful security feature that is commonly targeted by threat actors who attempt to find zero-day flaws that allow their malicious files to bypass Windows' security warnings.

<https://www.bleepingcomputer.com/news/security/winrar-710-boosts-windows-privacy-by-stripping-motw-data/>

### Snake Keylogger Slithers into Windows, Evades Detection with Autolt-Compiled Payload

A new variant of Snake Keylogger is making the rounds, primarily hitting Windows users across Asia and Europe. This strain also uses the BASIC-like scripting language Autolt to deploy itself, adding an extra layer of obfuscation to help it slip past detection. Snake Keylogger is a Microsoft .NET-based data stealer. As with earlier versions of the malware, once this software nasty gets onto a victim's PC, typically as an attachment to a spam email, this variant logs keystrokes, captures screenshots of the desktop, and collects clipboard data to steal credentials, credit card details, and other sensitive data. The keystrokes can include usernames and passwords typed into browsers Chrome, Edge, and Firefox.

[https://www.theregister.com/2025/02/18/new\\_snake\\_keylogger\\_infects\\_windows/](https://www.theregister.com/2025/02/18/new_snake_keylogger_infects_windows/)

### Why Rebooting Your Phone Daily Is your Best Defense Against Zero-Click Attacks

In the last decade, spyware tools have been repeatedly found on the phones of journalists, activists, and politicians, including US officials, raising concerns over the unprecedented proliferation of spyware technologies and, subsequently, the lack of protections within the tech space amid growing threats. Once a phone is infected with a zero-click capability, the operator of the attack can secretly gain total access to the phone by exploiting a security vulnerability. While the WhatsApp attack was predominantly launched against members of civil society, mobile spyware is an emerging threat against everyone because mobile exploitation is more widespread than one might think.

<https://www.zdnet.com/article/why-rebooting-your-phone-daily-is-your-best-defense-against-zero-click-attacks/>

### New FrigidStealer macOS Malware Distributed as Fake Browser Update

The malware, dubbed FrigidStealer, is written in the Go programming language and was built with the WailsIO project, to render content in the victim's browser and hide its malicious intent. Upon execution, it prompts the user for their password, and proceeds to harvest browser cookies and files associated with passwords and cryptocurrency, as well as Apple Notes, and exfiltrates them to its command-and-control (C&C) server. TA2727 was seen employing the same tactics, techniques, and procedures (TTPs) in other campaigns targeting Windows users with Lumma Stealer and DeerStealer, and Android users with the Marcher banking trojan. Active since at least September 2022, TA2726 is likely responsible for webserver and website compromises that are then shared with other cybercrime groups. Since the beginning of the year, the threat actor has used the TDS to redirect traffic

to TA569 and TA2727 web injects.

<https://www.securityweek.com/new-frigidstealer-macos-malware-distributed-as-fake-browser-update/>