Hackers use malware tags to deploy and attach to the device.

The hacking group APT-C-56, also known as Transparent Tribe, ProjectM and C-Major, has reactivated its activities, this time using Linux, a free and open source operating system developed by Linus Torvalds in 1991. Since then, Linux has become one of the most popular alternative commercial operating systems.

The main advantage of Linux is its open source code, which allows users to freely modify and distribute the system under the GNU GPL license.

Linux provides a stable, reliable and flexible platform for working with a computer or server. Most Linux distributions (eg, Ubuntu, Fedora, Debian) come with a variety of software and tools to work with, including office applications, Internet browsers, multimedia tools, and more.

Linux is also widely used in the server industry and embedded systems, such as routers and mobile devices.” data-html=”true” data-original-title=”Linux” >Linux-system.

The group of cybercriminals based in South Asia usually focuses its efforts on the countries of this region, including frequent attacks on India. APT-C-56 is known for its sophisticated phishing attack methods and multi-platform malware, including the notorious CrimsonRAT Windows Trojan.

Recently, experts from the 360 Advanced Threat Research Institute documented an attack in which APT-C-56 used a Linux c file with the “.desktop” extension to distribute malware. The malicious program, named Poseidon, is an infostealer and is designed to steal data. The method of attack with Linux-labels was used quite rarely before, which makes it especially dangerous.

To carry out the attack, the group created an archive file containing a desktop file, which in Linux systems acts as a shortcut. A user running this file activates a chain of events: a fake document is downloaded and opened, and malicious ELF files are simultaneously downloaded and launched. Poseidon, written in Golang, then establishes a constant presence on the system to collect confidential information.

The archive file, reviewed by the researchers, has the name “Agenda_of_Meeting.zip” and the desktop file “approved_copy.desktop”. This file uses the symbol “#” to increase its size and bypass anti-virus systems. After removing these characters, a script appears that downloads and opens a PDF document, then creates hidden directories and launches

malware. However, the program performs the function of collecting data and sending it to the malicious server.

Research has shown that Poseidon is capable of performing multiple tasks: capture keystrokes, upload and download files, scan ports, take screenshots, execute commands, and perform remote control. These features make it a powerful tool for espionage.

In August last year, a similar attack method was used against targets in India. Then APT-C-56 also used the archive with desktop files to distribute malware, which confirms the long-term strategy of criminals and their persistent interest in the countries of South Asia.

The analysis showed that the recent activity of APT-C-56 corresponds to its typical working methods. The use of Poseidon, disguised as legitimate software, and sophisticated methods of deceiving victims are characteristic features of this group. APT-C-56 continues to attack government and military structures in India, including Linux systems that are widely used in government institutions.

Experts strongly recommend increasing your security level and not running unknown files or clicking on suspicious links, regardless of the operating system you are using. Such actions may lead to compromise of the system and important data on the device.