Mphasis SOC – Information Security News
Date & Time Issued: 25-Jun-2024, 12:00 IST

Title	Ducktail Malware
Summary	• Ducktail Malware is a malicious program designed by hackers to infiltrate computers and networks globally. Ducktail malware is typically delivered through a spear-phishing email that contains a malicious attachment or a link to a malicious website. Once the malware infects a system, it establishes a persistent presence and begins to gather information about the system and the network it is connected to. • This info-stealer is being disseminated through Facebook URLs, employing a technique that redirects users to suspicious websites or pages. Once redirected, users are prompted to manually click on a download button, which initiates the download of malicious files onto their devices. This method of distribution capitalizes on user interaction and engagement to deceive them into downloading the malware. The malicious files obtained through this process pose a significant threat to the security and privacy of the affected users, potentially leading to various harmful consequences such as unauthorized access to sensitive information, system compromise, or further malware infections.
Severity	Medium
Attack Vectors	• The threat actors have shifted their focus from targeting specific employees with administrative or financial access to Facebook Business accounts to a broader audience. The malicious executable files are typically in .ZIP format and are hosted on file-sharing platforms, posing as cracked or free versions of popular applications like Office, games, subtitles, and explicit content files. Compared to previous campaigns, changes have been made in the execution of the malicious code. The threat actors now employ a scripting version where the main stealer code is a PHP script instead of a .NET binary. • The execution flow begins with a fake installer that generates a temporary file, which then re-initiates the installer with a "/Silent" parameter. Another temporary file is created, which drops all the supporting files and malicious files at a specific location on the victim's machine. To achieve persistence, a series of events take place, scheduling tasks to execute the malicious payload, named "libbridged.exe," daily and at regular intervals. • The PHP script creates PHP associative arrays to prepare for data transmission to the C&C server. The CURL command is used for sending and receiving files over HTTP, and specific switches are employed during communication. • After completing the data-stealing activities, the PHP script connects to the C&C server to obtain a list of targeted folders and URLs stored in JSON format, which are then used to gather further information. The stolen data is sent to the C&C server in JSON format.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hashs	• f3015c46ff2103431b383514591e1c1bf348119475c6a183066d3b8f6a896bca • 9f8e5f98f6ed3f63fb9266fde5f36b3bff242e8ebedbe6130558c65fde8addf7 • 221bbb95675d605597b278756a04acaa66f884f3c570717cb1025cbc7d62130a • facf9cf0e986ba43f6317457ccb711e45c06e279c08ed4bbafc77c6a5e6d0b60
	Domains	• slmg[.]online • roberthalfchro[.]online • strongeagle[.]online • cakoi2[.]online • strongeaglehr[.]online • qrispokaslotnew[.]xyz • cakoi3[.]online • flashbots[.]online • roberthalfhr[.]online • recruitmentb2c[.]online • roberthalfhr[.]site • roberthalfjob[.]site

Recommendations	• Block all threat indicators at your respective controls. Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Enabling two-factor authentication (2FA) on your accounts adds an extra layer of security and can help prevent unauthorized access even if your login credentials have been stolen. • Regularly backing up your important data can help ensure that you don't lose any critical information in the event of a malware infection or other data loss event. • Be wary of emails, attachments, and links from unknown sources. Also, avoid downloading software from untrusted sources or clicking on suspicious ads or pop-ups. • Make sure all of your software, including your operating system and applications, is up to date with the latest security patches. This can help prevent vulnerabilities that could be exploited by info-stealers and other types of malwares. • Promptly apply security patches and updates for operating systems, software applications, and browsers. This helps to address vulnerabilities that threat actors may exploit to deliver malware. • Maintain regular backups of critical data, including Facebook Business account information, and ensure they are stored securely offline. This enables quick recovery in case of a successful attack or data loss. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**
References	• https://www.rewterz.com/threat-advisory/an-emerging-ducktail-infostealer-active-iocs-9