Mphasis

The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 25-06-2024, 06:00 IST

Title	**Unveiling_SpiceRAT**
Summary	• SneakyChef's continuing campaign targeting government agencies across several countries in EMEA and Asia, delivering the SugarGh0st malware (read the corresponding research here). However, we found a new malware we dubbed "SpiceRAT" was also delivered in this campaign. • SneakyChef is using a name "ala de Emissão do Edifício B Mutamba" and the email address "dtti.edb@[redated]" to send several phishing emails with at least 28 different RAR file attachments to deliver either SugarGh0st or SpiceRAT. • One of the decoy PDFs that was dropped by a RAR archive, delivered as an attachment in the emails likely targeted Angolan government agencies. The decoy PDF contained lures from the Turkmenistan state-owned news media "ТУРКМЕНСКАЯ ГОСУДАРСТВЕННАЯ ИЗДАТЕЛЬСКАЯ СЛУЖБА" (Neytralnyy Turkmenistan), indicating that the actor has likely downloaded the PDF from their official website.
Severity	Medium
Attack Vectors	• SpiceRAT, for its part, employs two different infection chains for propagation, one of which uses an LNK file present inside a RAR archive that deploys the malware using DLL side-loading techniques. • When the victim extracts the RAR file, it drops the LNK and a hidden folder on their machine. "After a victim opens the shortcut file, which masqueraded as a PDF document, it executes an embedded command to run the malicious launcher executable from the dropped hidden folder." • The launcher then proceeds to display the decoy document to the victim and run a legitimate binary ("dxcap.exe"), which subsequently sideloads a malicious DLL responsible for loading SpiceRAT. • The second variant entails the use of an HTML Application (HTA) that drops a Windows batch script and a Base64-encoded downloader binary, with the former launching the executable by means of a scheduled task every five minutes. • The batch script is also engineered to run another legitimate executable "ChromeDriver.exe" every 10 minutes, which then sideloads a rogue DLL that, in turn, loads SpiceRAT. Each of these components – ChromeDriver.exe, the DLL, and the RAT payload – are extracted from a ZIP archive retrieved by the downloader binary from a remote server. • With the capability to download and run executable binaries and arbitrary commands, SpiceRAT significantly increases the attack surface on the victim's network, paving the way for further attacks

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• 6ca2415aabb806a871889c2ab48ad05b1ba444b5867ceadbcea3ab7f23de72f4 • b84ebbe57151844ac7ac9fc5d488e4696f37f98779d13dceafe6c5a7f2219a4c • 0374a9812c7e43db1bde605cc3decff3d77c8b041b959a5422e4da0b60e0f6dc • 48c65bb99ce954df0ee492b92e634d602d621295be2ff87e57fcb07c8b33db8b • e2330f64c92a49927098f8a07de9da8fc54c87a89dc549f6ebdcf3bc78732db2 • 9d4283c05417c0b49a00c6e5159eb5bcb52142036f94fcdfb9712b231d020955
	Domain	• http://stock.adobe-service.net/homepage/index[.]aspx/ • http://app.turkmensk.org/homepage/index[.]aspx/ • http://94.198.40[.]4/homepage/index.aspx// • app[.]turkmensk[.]org/ • stock[.]adobe-service[.]net/
	IP	• 45[.]144[.]31[.]57 • 94[.]198[.]40[.]4

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Never trust or open links and attachments received from unknown sources/senders. • Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. **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://blog.talosintelligence.com/new-spicerat-sneakychef/ • https://thehackernews.com/2024/06/chinese-hackers-deploy-spicerat-and.html