Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 21-06-2024, 20:00 IST

Title	**Oyster Backdoor Spreading via Trojanized Popular Software Downloads**
Summary	• A malvertising campaign is leveraging trojanized installers for popular software such as Google Chrome and Microsoft Teams to drop a backdoor called Oyster (aka Broomstick and CleanUpLoader). • The threat actors are luring unsuspecting users to fake websites purporting to contain legitimate software. But attempting to download the setup binary launches a malware infection chain instead. • Specifically, the executable serves as a pathway for a backdoor called Oyster, which is capable of gathering information about the compromised host, communicating with a hard-coded command-and-control (C2) address, and supporting remote code execution.
Severity	Medium
Attack Vectors	• The execution of the malware is followed by the installation of the legitimate Microsoft Teams software in an attempt to keep up the ruse and avoid raising red flags. It also observed the malware being used to spawn a PowerShell script responsible for setting up persistence on the system. • The disclosure comes as a cybercrime group known as Rogue Raticate (aka RATicate) has been attributed as behind an email phishing campaign that employs PDF decoys to entice users into clicking on a malicious URL and deliver NetSupport RAT. • If a user is successfully tricked into clicking on the URL, they will be led via a Traffic Distribution System (TDS) into the rest of the chain and in the end, have the NetSupport Remote Access Tool deployed on their machine. • It also coincides with the emergence of a new phishing-as-a-service (PhaaS) platform called the ONNX Store that allows customers to orchestrate phishing campaigns using embedded QR codes in PDF attachments that lead victims to credential harvesting pages. • Besides using Cloudflare's anti-bot mechanisms to evade detection by phishing website scanners, the URLs distributed via the quishing campaigns come embedded with encrypted JavaScript that's decoded during page load in order to collect victims' network metadata and relay 2FA tokens.

Indicators of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• 9601f3921c2cd270b6da0ba265c06bae94fd7d4dc512e8cb82718eaa24accc43 • 574C70E84ECDAD901385A1EBF38F2EE74C446034E97C33949B52F3A2FDDCD822 • CFC2FE7236DA1609B0DB1B2981CA318BFD5FBBB65C945B5F26DF26D9F948CBB4 • 82B246D8E6FFBA1ABAFFBD386470C45CEF8383AD19394C7C0622C9E62128CB94
	Domain	• prodfindfeatures[.]com/ • micrsoft-teams-download[.]com/ • impresoralaser[.]pro/ • whereverhomebe[.]com/ • supfoundrysettlers[.]us/ • retdirectyourman[.]eu/
	IP	• 149.248.79[.]62 • 64.95.10[.]243 • 206.166.251[.]114

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://thehackernews.com/2024/06/oyster-backdoor-spreading-via.html • https://www.rapid7.com/blog/post/2024/06/17/malvertising-campaign-leads-to-execution-of-oyster-backdoor/