


Mphasis SOC – Information Security News Date & Time Issued: 03-JUL-2024, 21:00 IST		
Title	Kematian Stealer forked from PowerShell Token Grabber	
Summary	<ul style="list-style-type: none"> • Kematian Stealer, a PowerShell-based malware that developed from a PowerShell Token-Grabber. The C++ loader hides an obfuscated script that decrypts and runs a batch file with advanced privileges to execute the PowerShell script. This script checks for admin rights and creates persistence via the Windows Task Scheduler. • Collects system and network information, such as public IP, UUID, MAC addresses, and username, storing this data in the temp directory. To evade detection, it removes files related to Discord Token Protector and attempts to download a payload, redirecting to the Kematian stealer GitHub page. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> • Stealers are a widespread threat providing threat actors with access to a wealth of sensitive data which is then exfiltrated to them for further abuse. Kematian Stealer, a PowerShell based tool is one such sophisticated malware. • The grub function contains the main stealer code that's mainly focused on system configuration and network environment information. It begins with obtaining the system's public IP by invoking the web request "Invoke-Web Request URL" after obtaining the IP it stores it in a text file located in the users local application data directory. • Then collects system information using the Windows command-line. PowerShell executes the Systeminfo.exe which retrieves the system information like OS Version, Host Name, System Model and more. • PowerShell-Token-Grabber; it was built by author KDot227 and now changed to Somali-Devs. In their recent updates they also mentioned about the author change in their source code and the GitHub page also redirects to the Kematian stealer GitHub page. • We got the main.exe from Virus total which was a python based executable. While decompiling the python executable, we came to know that this is where the browser stealer code is present. It focuses mainly on browser cookies, passwords, history details and the desktop screenshot • Also targets Discord tokens; it tries to inject code into various discord clients to capture discord tokens, for that it tries to download JavaScript by the author KDot227 in the name of injection.js. Discord , DiscordCanary ,DiscordPTB ,DiscordDevelopment. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> • 02F3B7596CFF59B0A04FD2B0676BC395 • D2EA85153D712CCE3EA2ABD1A593A028 • A3619B0A3EE7B7138CEFB9F7E896F168 • E06F672815B89458C03D297DB99E9F6B • 1CBBFBC69BD8FA712B037EBE37E87709

Recommendations	<ul style="list-style-type: none">• Block all identified IOCs at your security controls.• Application Whitelisting: Implement application control or whitelisting to allow only authorized applications to run. This prevents unauthorized scripts or executables from executing.• Network Segmentation: Segment your network to limit lateral movement. Isolate critical systems from less secure ones to prevent the spread of malware.• Privilege Management: Limit user privileges to the minimum necessary. Avoid running applications with administrative rights. Implement just-in-time (JIT) privilege escalation to grant elevated permissions only when needed.• Secure PowerShell Execution: Restrict PowerShell execution policies to prevent unauthorized scripts. Use constrained language mode or script block logging. Monitor PowerShell activity for signs of abuse.• Fileless Malware Detection: Invest in security tools that can detect fileless malware techniques, such as memory-based attacks and PowerShell-based threats.
References	<ul style="list-style-type: none">• https://labs.k7computing.com/index.php/kematian-stealer-forked-from-powershell-token-grabber/

The information contained in this message is proprietary. It is for Mphasis and its customers only.
Copyright © 2024. All rights reserved by Mphasis.