

HiveForce Labs

THREAT ADVISORY

**ACTOR REPORT**

The Rise of DarkCasino APT Group Exploiting WinRAR 0-Day

Date of Publication

November 27, 2023

Admiralty code

A1

TA Number

TA2023477

Summary

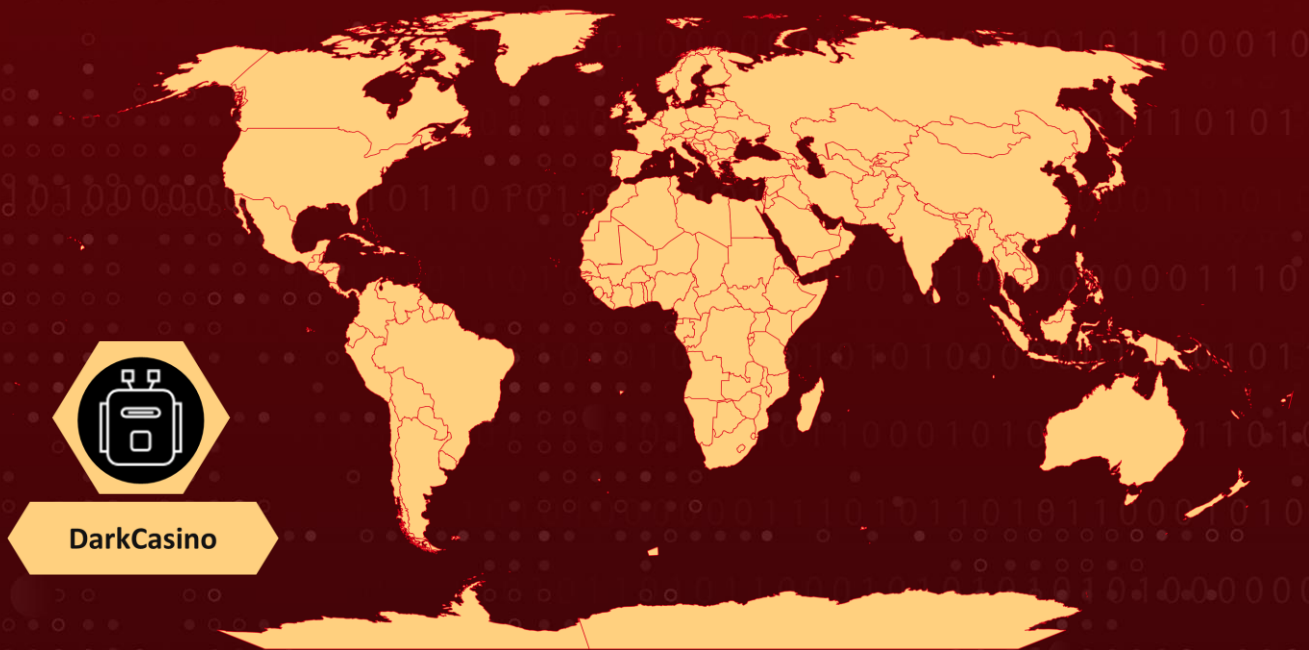
First Discovered: 2021

Actor Name: DarkCasino

Target Industries: Cryptocurrency trading platforms, online casinos and network banks worldwide




Target Region: Worldwide

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR			

Actor Details

#1

DarkCasino, an APT group with economic motivations, was first identified in 2021. The name "DarkCasino" is associated with a significant APT attack of the same name that was observed in 2022. The group primarily focuses on targeting various online trading platforms across Europe, Asia, the Middle East, and other regions. Its scope extends to industries such as cryptocurrencies, online casinos, network banks, and online credit platforms.

#2

DarkCasino is adept at collecting passwords from target hosts, enabling them to access assets deposited in online accounts by victims. The group consistently launches attacks with a notable focus on stealing online property. Technically and linguistically proficient, DarkCasino stands out as an APT threat actor capable of incorporating a variety of popular APT attack technologies into its methodologies.

#3

DarkCasino has crafted a diverse set of multi-level loading patterns, leveraging various Visual Basic components to execute sophisticated network attacks. In 2021, the APT group introduced DarkMe, a Trojan Horse program based on Visual Basic. This malware possesses capabilities such as gathering host information, capturing screenshots, manipulating files and the Windows Registry, executing arbitrary commands, and autonomously updating on the compromised host.

#4

DarkCasino has been recently associated with the zero-day exploitation of [CVE-2023-38831](#), an arbitrary execution vulnerability found in WinRAR software. DarkCasino leverages this vulnerability in phishing attacks, launching malicious payloads and engaged in pilferage activities. Their go-to tool, the DarkMe Trojan, is extensively utilized in this attack campaign.

#5

In recent months, [multiple threat actors](#), including APT28, APT29, APT40, Dark Pink, Ghostwriter, Konni, and Sandworm, have exploited the CVE-2023-38831 vulnerability. These APT groups have incorporated this vulnerability into their phishing attack methods, aiming to target critical entities. The exploitation of the flaw in various phishing attacks signals a potential increase in the number of victims in the future.

NAME	ORIGIN	TARGET REGIONS	TARGETED INDUSTRIES
DarkCasino	-	Worldwide	Cryptocurrency trading platforms, online casinos and network banks worldwide
	MOTIVE		
	Economic benefits		

Recommendations



Patch or Update WinRAR: Ensure that all instances of WinRAR in your organization are updated to versions 6.23 or higher to address the CVE-2023-38831 vulnerability. Regularly check for updates and automate the patching process where possible.



Remain vigilant: Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.



Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

🔬 Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access	<u>TA0011</u> Command and Control
<u>T1027</u> Obfuscated Files or Information	<u>T1055</u> Process Injection	<u>T1566</u> Phishing	<u>T1140</u> Deobfuscate/Decode Files or Information
<u>T1056</u> Input Capture	<u>T1059</u> Command and Scripting Interpreter	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities
<u>T1105</u> Ingress Tool Transfer	<u>T1204</u> User Execution	<u>T1204.002</u> Malicious File	<u>T1203</u> Exploitation for Client Execution

✂ Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	dd9146bf793ac34de3825bdabcd9f0f3, 5504799eb0e7c186afcb07f7f50775b2, c5331b30587dc94bfde94040d4fc89, ac28e93dbf337e8d1cc14a3e7352f061, fefe7fb2072d755b0bdf74aa7c9013e, 428a12518cea41ef7c57398c69458c52, 7bb106966f6f8733bb4cc5bf2ab2bab4, 2b02523231105ff17ea07b0a7768f3fd, 63085b0b7cc5bb00859aba105cbb40b1, 7195be63a58eaad9fc87760c40e8d59d, 129ccb333ff92269a8f3f0e95a0338ba, cd1f48df9712b984c6eee3056866209a, b05960a5e1c1a239b785f0a42178e1df, 6b5d5e73926696a6671c73437cedd23c

Patch Details

Update WinRAR version to 6.23 or later versions

Link:

https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

References

<https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/>

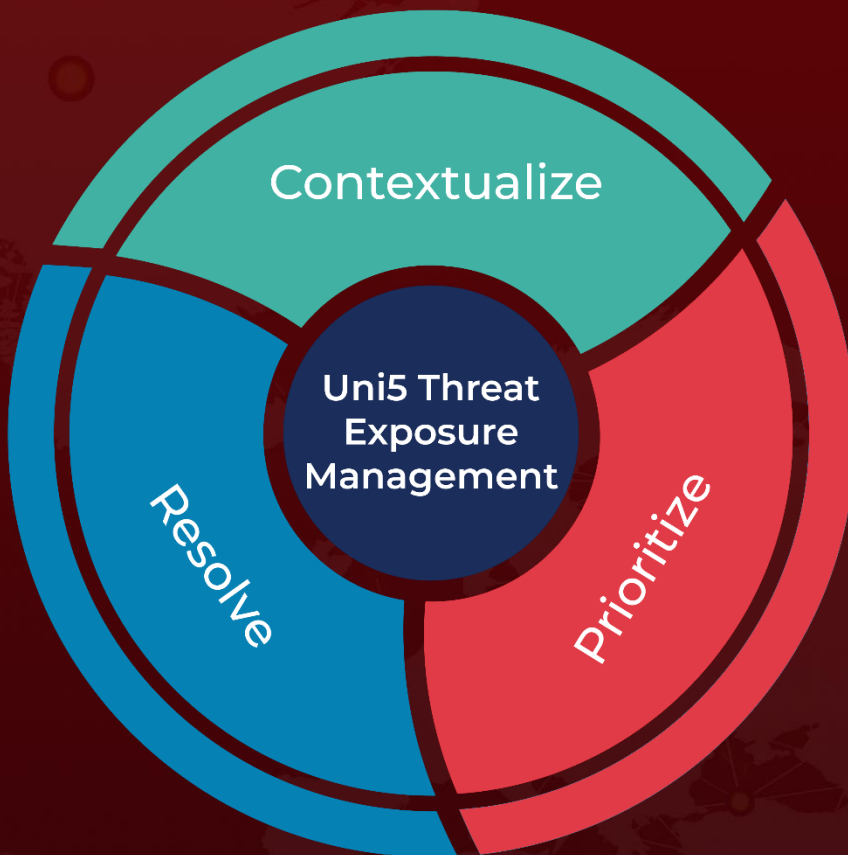
<https://www.hivepro.com/threat-advisory/winrar-zero-day-exploit-targeting-traders-since-april/>

<https://www.hivepro.com/threat-advisory/multiple-state-sponsored-groups-exploit-winrar-vulnerability-in-phishing-attacks/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

November 27, 2023 • 4:20 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com