2024-02-29

HUNTER

EMERGING THREATS

DARKCASINO (WATER HYDRA) THREAT GROUP

The APT group, DarkCasino (also known as Water Hydra), has been in the wild since 2021 and has had operations observed targeting online trading platforms in Asia, the Middle East, and Europe. Examples of the specific targets are gambling websites, casinos, banks, cryptocurrency and stock trading platforms. Their modus operandi is to steal assets from the victims' and their online accounts by stealing passwords from victimized hosts. Their attack method(s) at first were similar to the TTP's used by another APT group named Evilnum, however they have since expanded their capabilities. In recent events, the evolving APT group has been observed exploiting their own developed Visual Basic-based malware named "DarkMe". It has been utilized to exploit CVE-2023-38831 (a WinRAR Zero-Day vulnerability discovered in mid-2023), and most recently deployed by the exploitation of CVE-2024-21412 (Windows Defender SmartScreen Zero-Day). With DarkCasino's evolution and therefore, sophisticated nature, as well as their ability to exploit new vulnerabilities as they are found - it is important to assess, understand and prepare for the actor's capabilities and operations.

CYBORG SECURITY

Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.

THREAT SUMMARY

The APT group, DarkCasino (also known as Water Hydra), has been in the wild since 2021 and has had operations observed targeting online trading platforms in Asia, the Middle East, and Europe. Examples of the specific targets are gambling websites, casinos, banks, cryptocurrency and stock trading platforms. Their modus operandi is to steal assets from the victims' and their online accounts by stealing passwords from victimized hosts. Their attack method(s) at first were similar to the TTP's used by another APT group named Evilnum, however they have since expanded their capabilities. In recent events, the evolving APT group has been observed exploiting their own developed Visual Basic-based malware named "DarkMe". It has been utilized to exploit CVE-2023-38831 (a WinRAR Zero-Day vulnerability discovered in mid-2023), and most recently deployed by the exploitation of CVE-2024-21412 (Windows Defender SmartScreen Zero-Day). With DarkCasino's evolution and therefore, sophisticated nature, as well as their ability to exploit new vulnerabilities as they are found - it is important to assess, understand and prepare for the actor's capabilities and operations.

CYBORG SECURITY
Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.

SYNOPSIS

DarkCasino (aka Water Hydra) is a significant threat actor since 2021, targeting financial institutions, cryptocurrency platforms, and online trading and gambling platforms as well. When first seen in the wild, the group employed tactics similar to the TTP's used by another APT group named Evilnum - which included the methods of how they delivered malware (Windows Shortcut files (LNK) being nested within .ZIP files). Fast forward a few years and DarkCasino has expanded their attack patterns and evolved to the use of Visual Basic components for example, in order to become a more sophisticated threat.

More specifically, they developed a malware family dubbed "DarkMe" (remote access trojan), which has been used in conjunction with the exploitation of various zero-day vulnerabilities since its inception. Most recently, it has been observed alongside DarkCasino attacks exploiting CVE-2024-21412 - a vulnerability in Microsoft Defender SmartScreen that could be exploited to bypass security measures. This was achieved by involving a shortcut within another shortcut, which was enough to circumvent the application of the Mark-of-the-Web (which allows it evade SmartScreen). This gave the capability of the threat actors to infect victim(s) machines with the DarkMe malware, handing them unauthorized remote access - which can be used to capture system information, monitor user activities, gather and exfiltrate sensitive information, execute commands and even drop more malware into the victim's system.

CYBORG SECURITY
Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.

HUNT PACKAGES

DIRECT TO IP ADDRESS IN EXECUTION OF WEBDAV DLL VIA RUNDLL32 - MALICIOUS LINK OR EXPLOITATION
https://hunter.cyborgsecurity.io/research/hunt-package/d020807d-8833-460f-ac88-b004b74ecea4

SUSPICIOUS FILE EXECUTED FROM INETCACHE - POTENTIAL MALICIOUS SCRIPT EXECUTED FROM REMOTE HOST
https://hunter.cyborgsecurity.io/research/hunt-package/b529a453-a0c1-49dc-beed-7990cb71b0ea

SUSPICIOUS FILE EXTENSION WRITTEN TO INETCACHE - POTENTIAL MALICIOUS FILE DOWNLOADED FROM REMOTE HOST
https://hunter.cyborgsecurity.io/research/hunt-package/44507f9d-d1bd-43bf-92cd-8f9dcbbf15cc

AUTORUN OR ASEP REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

SUSPICIOUS FILE EXTENSION EXECUTED FROM INETCACHE - POTENTIAL MALICIOUS FILE EXECUTED FROM REMOTE HOST
https://hunter.cyborgsecurity.io/research/hunt-package/43542c5b-f282-4834-8602-ab2d076359c2

SUSPICIOUS CMD PROXY EXECUTION IN APPDATA\LOCAL\TEMP - POTENTIAL MALICIOUS SCRIPT OR FILE EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/573e774e-2d22-48a1-a24d-b217ab8af8e4

WINDOWS CMD.EXE LAUNCHING SCRIPT INTERPRETER
https://hunter.cyborgsecurity.io/research/hunt-package/a5c2a987-f7cd-479f-a77e-f992f1be2ea6

ABNORMAL EXECUTION OF WEBDAV DLL VIA RUNDLL32 - POTENTIALLY MALICIOUS LINK OR EXPLOITATION
https://hunter.cyborgsecurity.io/research/hunt-package/062ae7c6-3e3d-401c-8797-1df3218f3e47

7Z PASSWORD PROTECTED ARCHIVE ACCESSED
https://hunter.cyborgsecurity.io/research/hunt-package/669cf97c-57c8-41fa-8162-005cdd998972

HTTP PROPFIND REQUEST FOR SUSPICIOUS FILE EXTENSIONS - POTENTIAL CVE-2024-21412 LINK
https://hunter.cyborgsecurity.io/research/hunt-package/

HTTP REQUEST FOR INTERNET SHORTCUT - POTENTIAL CVE-2024-21412 LINK
https://hunter.cyborgsecurity.io/research/hunt-package/

RELATED LINKS
Sign up for free HUNTER access
DarkCasino (Water Hydra) Threat Group Emerging Threat Collection

Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.

MITRE CONTEXT

- Tactic Names:
  - Privilege Escalation
  - Initial Access
  - Credential Access
  - Impact
  - Execution
  - Command and Control
  - Defense Evasion
  - Lateral Movement
  - Persistence
  - Exfiltration
- Technique Names:
  - Registry Run Keys / Startup Folder
  - Malicious File
  - Phishing
  - Remote Services
  - Rundll32
  - Exfiltration Over Physical Medium
  - Exploitation for Credential Access
  - Malicious Link
  - Web Protocols
  - Data Encrypted for Impact
  - Windows Command Shell
  - System Binary Proxy Execution
- Threat Names:
  - DarkMe

CYBORG SECURITY
Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.

REFERENCES

1. https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
2. https://twitter.com/Cybermaterial_/statuses/1762236157566349630
3. https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/

Cyborg Security Confidential. Unauthorized disclosure is strictly prohibited.