Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Water Hydra Exploits CVE-2024-21412 to Target Financial Traders

Date of Publication	Admiralty Code	TA Number
February 15, 2024	A1	TA2024060

Summary

Attack Began: December 2023
Targeted Countries: Worldwide
Threat Actor: Water Hydra (aka DarkCasino)
Targeted Industries: Finance, Cryptocurrency, Forex and Stock trading, Banking, Gambling sites and Casinos
Malware: DarkMe RAT
Affected Platform: Windows
Attack: Water Hydra exploited CVE-2024-21412 to bypass Microsoft Defender SmartScreen, targeting financial traders with DarkMe malware through sophisticated spearphishing tactics. This underscores the persistent threat of APT groups and highlights the challenge of defending against evolving attack methods.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21412	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows Internet Shortcut Files	✓	✓	✓
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1 Water Hydra, an advanced persistent threat (APT) group, active since 2021 and recently exploited a zero-day vulnerability in Microsoft Defender SmartScreen, designated as CVE-2024-21412, to target financial market traders. This vulnerability, now patched by Microsoft, was disclosed by the Trend Micro Zero Day Initiative.

#2 The attack involved spearphishing campaigns on forex and stock trading forums, luring victims into executing malicious .url files disguised as JPEG files. These .url files exploited the CVE-2024-21412 vulnerability to bypass Microsoft Defender SmartScreen and infect victims with DarkMe malware. CVE-2024-21412 appears to be bypass of CVE-2023-36025 which also enabled specially crafted .url files to bypass SmartScreen.

#3 Water Hydra's attack patterns demonstrate high technical proficiency, including the ability to exploit undisclosed zero-day vulnerabilities. The group has previously targeted the financial industry and has been linked to campaigns using other vulnerabilities like CVE-2023-38831.

#4 The attack chain evolved over time, with Water Hydra updating its methods to streamline the infection process. They utilized techniques like abusing the search protocol and crafted Advanced Query Syntax (AQS) queries to customize Windows Explorer views, further deceiving victims.

#5 Once the SmartScreen protection was bypassed, the malware executed a series of commands, ultimately establishing communication with a command-and-control (C&C) server. The malware, known as DarkMe, gathered system information and awaited commands from the attacker, enabling a wide range of malicious functionalities. This incident underscores the persistent threat posed by APT groups and the challenges in defending against zero-day exploits, highlighting the need for robust security measures and timely patching.

Recommendations

Email Filtering and Web Filtering: Implement robust email filtering solutions to detect and block phishing emails before they reach users' inboxes. Additionally, deploy web filtering tools to block access to known malicious websites and URLs.

Patch Management: Maintain a rigorous patch management process to ensure that all software, including operating systems, web browsers, and security applications, is up-to-date with the latest security patches. Promptly apply patches released by software vendors to mitigate known vulnerabilities.

Endpoint Protection: Deploy advanced endpoint protection solutions that include anti-malware, anti-phishing, and behavior-based detection capabilities. Ensure that endpoint security software is configured to detect and block malicious activities, including attempts to exploit vulnerabilities like CVE-2024-21412 and CVE-2023-36025.

Network Segmentation: Implement network segmentation to restrict the lateral movement of attackers within the network. Segment critical systems and sensitive data from less secure areas of the network to minimize the impact of a successful breach.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0005 Defense Evasion
TA0004 Privilege Escalation	TA0011 Command and Control	TA0042 Resource Development	TA0003 Persistence
T1566.002 Spearphishing Link	T1566 Phishing	T1204 User Execution	T1204.001 Malicious Link
T1105 Ingress Tool Transfer	T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1588.006 Vulnerabilities
T1588 Obtain Capabilities	T1588.005 Exploits	T1559 Inter-Process Communication	T1559.001 Component Object Model

T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1585 Establish Accounts	T1585.001 Social Media Accounts
T1586 Compromise Accounts	T1586.001 Social Media Accounts	T1584 Compromise Infrastructure	T1584.004 Server
T1211 Exploitation for Defense Evasion	T1218.007 Msiexec	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1458a762332676f7807ab45f8f236c22a1a7bb0c21fcd8c779f972f2446a11d0, 758c6364ab560fbeff2bfa8712a2e09132d85d0bf6918e6acc79fe12f5b71ec3, 77d685e29c3dbe75fa8a82c69c68c731a09904020a76145ca27aeaf0058455cd, b36dc329a5dc766c2645d5f5b6cdaa9542ec3b0aa1bc13dc1f899ce6d95d59fb, d895fff3c909ea2eb6624fc5f154c924fe0af51c6c899fd9093dc3cd27a5dad2, 008e57d62caa8cfa991f5519eabe3f15d79799b81ba8cc6b67cde6da0dbffdab, 087878208755420d5d7ae2eb6a84482768cb8972732911ac16096cd0c95fa0f7, 1115e4bed3949493d8ab184e5c42f047355f13b9bf91c1621acb7971a148bea2, 18b1dc2e00245cb017ebdedfe63881929d7542eeffa8f42ee0ad20cc2ebf181a, 1956bcd3df47e76b2e9f396514f072311563d092ae02509f817c488567749998, 1fbc621a71578cb22d4e3a0feec68735321358a3aeb18adbe4a20630c7f788b8, 39fb9fb06910f1133f3b23c523a5139f61d243380802b0670a664473d00e1fa9, 3e420ce1dc1a8503f48815b880381dd23206e08be2474d151f1353df7df2d796,

TYPE	VALUE
SHA256	4201ab8c0c4cf0f01f5a25d8e4e7221634776b5bad8c3faad5ad819ec58619ad, 58b0f5da4a53e956b35e77f55ced641291a596e16067b1dab6ac54d9cb6a52a5, 5b16ac1edb747053ee5a085ab826c61218c5b471eaa04f2471dc2e80b5621023, 5c85a0fe230d351b35da364c797cc95557f5dcceec034eb648e1805237c7203b, 5f4ef55201080ef3a62b0fbdc4c27e0ccdf4041f41c04471f35b127ff6515405, 61de01bc154b1118caacfed3839c996a795d6c21c2efbf1da6b926414f5d182d, 65cc5594b307c2ac4e3c251aeae68dedf7d1f24ba3b0d7ab5ad3623e8a9fc865, 6793e0fbc2def9173bf8e2a6c1aa357ba7fc3e32dc1cf81107677166f175c890, 6bec457f83d0d98f6f6ea1243c2327e012db38fb61680f6bd68dbab0dc07170a, 7058ae0f02e116b38536ee1ec20f47645aecf761361b5a5e85de2961f3cc88c6, 70b4c2d696a24a5ae2f5e5095dc44e68b4605e4690c8a49930194ee87eb80252, 73922ab0d048b45a01f13ba967f1423bc6cd6cc711f8e7d00a4cf2b1d3646f4e, 761fa42bc4cc5332a640c7389240324242981176ca1626e4267cc8a00cf9545f, 88bb1df99e02021801b08beeff87ec3ceb9e16c42f62904c5ac04c1a26213a48, 941cf63028bf8314bc7114a088f4d1f1dd995bec4a4b7c51fda34fbb3528667f, a45e0ea5a17ba6f3a2ce7258f6cc81c6f93f37873b49218a25ec638987da6f96, a5096c4624a523a660242e3451c2f4d644431a35098e36b724fab9f7d88d145d, a9633da58719f07159702101474b6ba78f2ffee28b3f7ebda3feb36db4e2d0e9, b0ab19986ab1297870854980f1287f1a4b8d003c540773a6c04fb3565e5701ee, b350a787c19a756c0824e14eec7e9d746450d1aafb28a5d15209ec9f34c58129, b738e92afc95cba819aa7aebfad459de38743c478e9e8b8f29f9919697b495b0, b8b6b6d98b7ea689f0c33d55a06afcf20482b25c51929ca9a1b302374290b337, babbd9c94dedb94be8baac2ddc5b4714c44a8d0c60d49c0dc91708784bc0d57f, bbdf52481bd1a15710d75b89240c7a360450e2f4f00ba2cb140affba79ebec94,

TYPE	VALUE
SHA256	c86ba0da732e1fa1f06549d3ebc5ae6ae091199e95930681ac2a9152a8834184, d6000a19198b8b9719fc17f7c06366e542802a8e7e232ba731b72c31226cc890, d81e7d95004441ea4f5344215232db57f48579bf335c7ba4ed7f6ec6f9136ed0, db1bc70c0d0c7121f1d4422a6fcd0e0668d9da786affb52dd77852641e425710, ddda5737b2c3207d72d728bf40709a7296c31e7c50951dcad441f4707581ccb1, e1b903eba88b920909876442306e1160eed9b69c69a05ea370cba2121e305ba1, e49a7d9083b2e448274d117405c39b0c1b2c0c20ab5195bdf94aaeda7cc113d7, f44964c8fdf6dbdb21c141df61b45467bba5a4482f7ab19fd6f1841fdb791f2a, f6b01df60d526f1de530230724d41b482adfff81084a1872bb97c316b76e45e3, f701f500d348b63f3250239cd8305a8b38230e67d74456f3333c6efeeef85bbb, fb67be10a5a8b26ca86f8f79935ddd4a5b40379bb6d0af21d23f56af14bb2a90, 4307a067db6b6abd852441e6d70de29c3bd0e4d6a68f0449b403401518b7e037, 69fc5bed55acf559035f2c5550bf8807236b580f8e2db88966b3fc80c83914d3, 4c43b4575063d50ca5668e45a434aaf288970c89e8a4414812560ee787307f58, 135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc, b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb, bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c, dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54,

TYPE	VALUE
File Paths	/fxbulls, /fxbulls/pictures, /fxbulls/pictures/photo_2023-12-29[.]jpg[.]url, /fxbulls/pictures/Thumbs[.]db , /fxbulls/pictures/2[.]url , /fxbulls/pictures/a2[.]zip , /fxbulls/pictures/a2[.]zip/a2[.]cmd, /fxbulls/pictures/a2[.]zip, /fxbulls/pictures/b3[.]dll, /fxbulls/pictures/7z[.]dll, /fxbulls/pictures/7z[.]exe, /fxbulls/pictures/photo_2023-12-29s[.]jpg, /fxbulls/pictures/My2[.]zip, /fxbulls, /fxbulls/images, /fxbulls/images/photo_2023-12-29[.]jpg[.]url, /fxbulls/images/Thumbs[.]db , /fxbulls/images/2[.]url , /fxbulls/images/a2[.]zip , /fxbulls/images/a2[.]zip/a2[.]cmd, /fxbulls/images/a2[.]zip, /fxbulls/images/b3[.]dll, /fxbulls/images/7z[.]dll, /fxbulls/images/7z[.]exe, /fxbulls/images/photo_2023-12-29s[.]jpg, /fxbulls/images/My2[.]zip, /fxbulls/net, /fxbulls/net/photo_2023-12-29[.]jpg[.]url, /fxbulls/net/Thumbs[.]db , /fxbulls/net/2[.]url , /fxbulls/net/a2[.]zip , /fxbulls/net/a2[.]zip/a2[.]cmd, /fxbulls/net/a2[.]zip, /fxbulls/net/b3[.]dll, /fxbulls/net/7z[.]dll, /fxbulls/net/7z[.]exe, /fxbulls/net/photo_2023-12-29s[.]jpg, /fxbulls/net/My2[.]zip, /underwall/docs, /underwall/docs/7z.zip, /underwall/docs/passport.jpg.url, /underwall/docs/warop.url, /underwall/expand, /underwall/expand/7z.zip, /underwall/expand/photo_2023-12-26.jpg.url, /underwall/expand/warop.url, /underwall/society, /underwall/society/7z.zip, /underwall/society/photo_2023-12-26.jpg.url, /underwall/society/warop.url

TYPE	VALUE
Domains	fxbulls[.]ru, 87iavv[.]com, unfawjelesst322[.]com, p2oaviwt39ui[.]com
IPv4	84[.]32[.]189[.]74, 179[.]43[.]172[.]127, 179[.]43[.]172[.]191, 64[.]31[.]63[.]70, 64[.]31[.]63[.]194
URLs	hxxp[://]84[.]32[.]189[.]74, hxxp[://]84[.]32[.]189[.]74/xampp/, hxxp[://]84[.]32[.]189[.]74/webdav/, hxxps[://]fxbulls[.]ru, hxxps[://]fxbulls[.]ru/wp-content/uploads, hxxps[://]fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]htm, hxxps[://]fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]html, hxxps[://]84[.]32[.]189[.]74@0[.]0[.]0[.]80/fxbulls/net/2[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29[.]jpg[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls, hxxp[://]84[.]32[.]189[.]74/fxbulls/images, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29[.]jpg[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/net, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29[.]jpg[.]url,

TYPE	VALUE
URLs	hxxp[://]84[.]32[.]189[.]74/fxbulls/net/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/underwall/docs, hxxp[://]84[.]32[.]189[.]74/underwall/docs/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/docs/passport.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/docs/warop.url, hxxp[://]84[.]32[.]189[.]74/underwall/expand, hxxp[://]84[.]32[.]189[.]74/underwall/expand/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/expand/photo_2023-12-26.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/expand/warop.url, hxxp[://]84[.]32[.]189[.]74/underwall/society, hxxp[://]84[.]32[.]189[.]74/underwall/society/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/society/photo_2023-12-26.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/society/warop.url,

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

References

https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html

https://www.trendmicro.com/fr_fr/research/24/b/cve-2024-21412-facts-and-fixes.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-smartscreen-zero-day/ioc-list-water-hydra-cve-2024-21412.txt

https://www.hivepro.com/threat-advisory/microsofts-february-2024-patch-tuesday-addresses-two-zero-day-vulnerabilities/

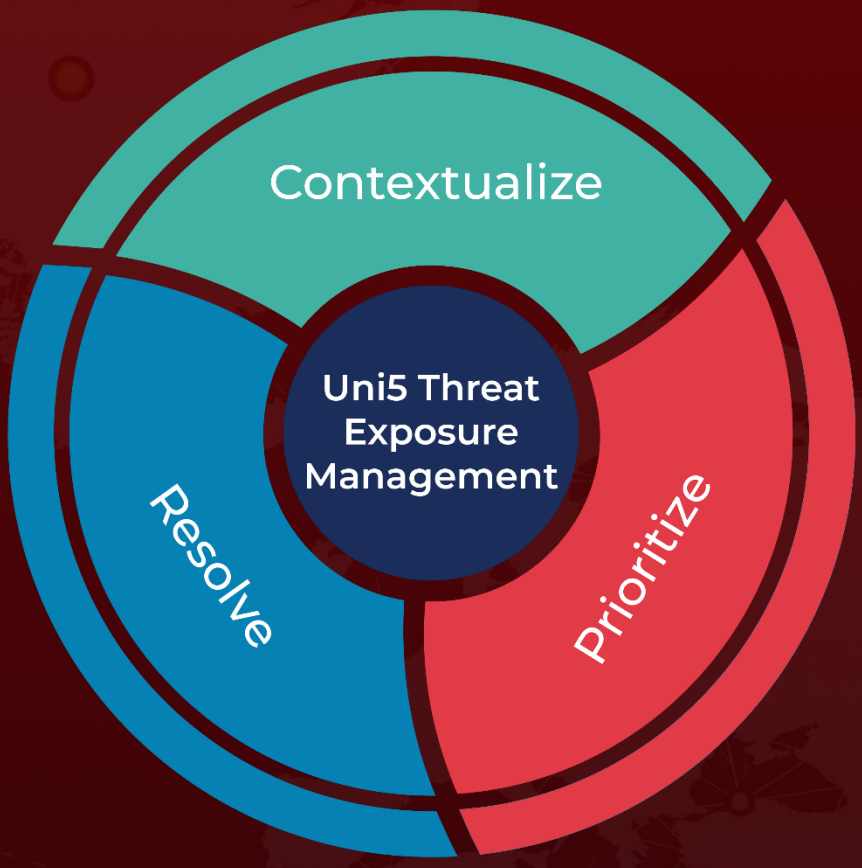
https://www.hivepro.com/threat-advisory/windows-smartscreen-exploit-paves-the-way-for-phemedrone-stealer/

https://www.hivepro.com/threat-advisory/the-rise-of-darkcasino-apt-group-exploiting-winrar-0-day/

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

February 15, 2024 • 11:30 PM

More at www.hivepro.com