KPMG Cyber Threat Intelligence Platform

Water Hydra APT – Infiltrating the Financial Sector

Water Hydra, aka Dark Casino, emerged in 2021, utilizing phishing techniques and zero-day exploits like the WinRAR vulnerability. Initially mistaken for Evilnum, it later emerged as a distinct cybercrime group focusing on financial institutions. In 2022, researchers discovered DarkMe, a VisualBasic RAT used in the DarkCasino campaign targeting European traders and gambling platforms. The group continues to target financial institutions, banks, cryptocurrency platforms, forex, stock trading platforms, as well as gambling sites and casinos worldwide.

Water Hydra gains initial access via spearphishing, targeting forex and stock trading forums and Telegram channels. Victims are enticed with disguised malicious links, often posing as JPEG images or PDF files, or messages offering trading advice, leading to a trojan horse stock chart on a compromised Russian trading and cryptocurrency site (fxbulls[.]ru). Victims execute the malicious links, leading to the exploitation of CVE-2024-21412, bypassing Microsoft Defender SmartScreen and allowing the execution of code from an untrusted source. Persistent execution is ensured through copying and running a DLL loader from the attacker's WebDAV share. Communication with the attacker's C2 server is established over TCP using a custom protocol, enabling command execution and data retrieval. Sensitive information, including system details and active window titles, is exfiltrated to the attacker's C2 server. Obfuscation techniques are employed to hinder detection and reverse engineering. Water Hydra's operations can disrupt services on compromised systems by halting critical processes, potentially leading to denial of service.

Water Hydra's capability to exploit zero-day vulnerabilities, which remain undisclosed to software vendors, underscores the necessity for organizations to implement robust cybersecurity measures.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Water Hydra APT – Infiltrating the Financial Sector

Indicators of Compromise: IP Addresses	
64.31.63[.]70	179.43.172[.]191
64.31.63[.]194	179.43.172[.]127
84.32.189[.]74	

Indicators of Compromise: Domains	
87iavv[.]com	p2oaviwt39ui[.]com
fxbulls[.]ru	unfawjelesst322[.]com

Indicators of Compromise: Hashes
f87b1582be230f1335a84b6607a8ea76
86c846fc810843ba525c5ba488bdf1ed
6edb0405d8d700f8de037879d89711dd
dc05d20891ce3a106bcc8a36cca7a2cb
4ca43d817fbbe6544544a532bf41fe3a
b39eb1379b8c6c6dc1da8494091feca2
807a38f402f646093d4614c2059a7e5b
7fa805b3c23ef7a4a47ddfc4e51d1231
4b700f00322e72ae41372d8e79ea6a15
734dbd553a34faed038537cc2e128a6a
999765df60217e9011fe76b5335f3cf0
586edd642827ac6094a24e220a64e99e
dc1ab9f3939ceb5014c379d28b0a184f
bde19eeb32ffaa59315293656847158f
858db46a94638e9ac17c21cf359be373
dbc3136002a0ad813166debccc697e79
5b415de6fb57e8a1d86ac3ac7f1ee48d
6193d8262954a260cead37caa926b7d0
366e3a52218fef463c765c629b45f433
8141f076e3fdbd3302de8f1534be5ef3
6ae5dc5449d356b8d4637505ed3c4010
2d871792b8bd645af79b70a744623938
4cf4a9928f98d091e9280041d8733638

KPMG

KPMG Cyber Threat Intelligence Platform

Water Hydra APT – Infiltrating the Financial Sector

Indicators of Compromise: Hashes
01422dedb39670cebbc2ed9614aeea17
fd47b4dd7ccfcef3f12c49ed5872d8c6
893e63b7364a6aa0b732db6bfdb3ce83
f1f9d3e5b08370f82a8009144675bec3
aac35a0f3a7d58c39494d9879a9ec2d9
26d60eb679870d00a653f28f400e4039
e93a48506b56a548974c1eac0cadf554dd06ee33
31b635fb96bbaa56e07c5b0727abc66599635cac
9b28f37acef0fd2a4bbc85e411f97f0d577920fb
de2cb8f07c0393c0b8eefd084eb2df6567680e6b
efcbe62a2b8b80909a378b5daf5de9fa260a64d0
f210ba7fe2b0ad928648da78b72e151e45dbc76f
dbff7e0a63074d134bfe04868f8610291c3c245e
afc31c89455b3a630b4ae760669c5841f3513c01
0fb64c439261634b967efb7c4c22f1c17dc6970f
f702fef88327c52d9da2f62b4cb8a1cce543ac35
07d731b8146ddf2573742ab89d8bb040e70a4f93
9b81591f6411e766ba3081413bad804c19dd9a32
477f5daea152db77f58619adc6938af67480265c
91c726b01f5e160a6f4bb25930890313ea46e276
dcd8c690094359e8cb49c4611ef32abda34d9b0d
0b9a82356134087c4bb62f78496b5461b9fcc572
86ec331da3b3ed7a6c0ee108cb3cc36130b9b43d
6993dfa54b56475938e66d5caeab92639bdbadd3
d16b7a028f2af54d24ea72cd5f2733b848e28436
5f11dd1b4e20bcfb7cabd502488667b23e4281db
d41c5a3c7a96e7a542a71b8cc537b4a5b7b0cae7
9682a044b93e02f31b6c2c579e10a508ab9bf7ef
4898c97014c87e4c13f1b61b1760f43381627fed
783eb04dc4cba6b197ce8831c1da4bd1443057a9
1b2307e7e5c3c2f656f9a821bc4b0e31f90d2a1b
4ab5cfcac151b30844a9b7cd8b16fd06a487cef8
af0722881b58e097c713ba3167092beed90127b4
8280299d3f6d4e2dc27b9abb74241b11a1dabc4b

KPMG

KPMG Cyber Threat Intelligence Platform

Water Hydra APT – Infiltrating the Financial Sector

Indicators of Compromise: Hashes
00029ab0f337b08b068d6483fc979bef783f4719
2b46491f444761d268022433cdd2905d9566fc25
1458a762332676f7807ab45f8f236c22a1a7bb0c21fcd8c779f972f2446a11d0
758c6364ab560fbeff2bfa8712a2e09132d85d0bf6918e6acc79fe12f5b71ec3
77d685e29c3dbe75fa8a82c69c68c731a09904020a76145ca27aeaf0058455cd
b36dc329a5dc766c2645d5f5b6cdaa9542ec3b0aa1bc13dc1f899ce6d95d59fb
d895fff3c909ea2eb6624fc5f154c924fe0af51c6c899fd9093dc3cd27a5dad2
008e57d62caa8cfa991f5519eabe3f15d79799b81ba8cc6b67cde6da0dbffdab
087878208755420d5d7ae2eb6a84482768cb8972732911ac16096cd0c95fa0f7
1115e4bed3949493d8ab184e5c42f047355f13b9bf91c1621acb7971a148bea2
18b1dc2e00245cb017ebdedfe63881929d7542eeffa8f42ee0ad20cc2ebf181a
1956bcd3df47e76b2e9f396514f072311563d092ae02509f817c488567749998
1fbc621a71578cb22d4e3a0feec68735321358a3aeb18adbe4a20630c7f788b8
39fb9fb06910f1133f3b23c523a5139f61d243380802b0670a664473d00e1fa9
3e420ce1dc1a8503f48815b880381dd23206e08be2474d151f1353df7df2d796
4201ab8c0c4cf0f01f5a25d8e4e7221634776b5bad8c3faad5ad819ec58619ad
58b0f5da4a53e956b35e77f55ced641291a596e16067b1dab6ac54d9cb6a52a5
5b16ac1edb747053ee5a085ab826c61218c5b471eaa04f2471dc2e80b5621023
5c85a0fe230d351b35da364c797cc95557f5dceec034eb648e1805237c7203b
5f4ef55201080ef3a62b0fbdc4c27e0ccdf4041f41c04471f35b127ff6515405
61de01bc154b1118caacfed3839c996a795d6c21c2efbf1da6b926414f5d182d
65cc5594b307c2ac4e3c251aeae68dedf7d1f24ba3b0d7ab5ad3623e8a9fc865
6793e0fbc2def9173bf8e2a6c1aa357ba7fc3e32dc1cf81107677166f175c890
6bec457f83d0d98f6f6ea1243c2327e012db38fb61680f6bd68dbab0dc07170a
7058ae0f02e116b38536ee1ec20f47645aecf761361b5a5e85de2961f3cc88c6
70b4c2d696a24a5ae2f5e5095dc44e68b4605e4690c8a49930194ee87eb80252
73922ab0d048b45a01f13ba967f1423bc6cd6cc711f8e7d00a4cf2b1d3646f4e
761fa42bc4cc5332a640c7389240324242981176ca1626e4267cc8a00cf9545f
88bb1df99e02021801b08beeff87ec3ceb9e16c42f62904c5ac04c1a26213a48
941cf63028bf8314bc7114a088f4d1f1dd995bec4a4b7c51fda34fbb3528667f
a45e0ea5a17ba6f3a2ce7258f6cc81c6f93f37873b49218a25ec638987da6f96
a5096c4624a523a660242e3451c2f4d644431a35098e36b724fab9f7d88d145d
a9633da58719f07159702101474b6ba78f2ffee28b3f7ebda3feb36db4e2d0e9
b0ab19986ab1297870854980f1287f1a4b8d003c540773a6c04fb3565e5701ee

KPMG

KPMG Cyber Threat Intelligence Platform

Water Hydra APT – Infiltrating the Financial Sector

Indicators of Compromise: Hashes
b350a787c19a756c0824e14eec7e9d746450d1aafb28a5d15209ec9f34c58129
b738e92afc95cba819aa7aebfad459de38743c478e9e8b8f29f9919697b495b0
b8b6b6d98b7ea689f0c33d55a06afcf20482b25c51929ca9a1b302374290b337
babbd9c94dedb94be8baac2ddc5b4714c44a8d0c60d49c0dc91708784bc0d57f
bbdf52481bd1a15710d75b89240c7a360450e2f4f00ba2cb140affba79ebec94
c86ba0da732e1fa1f06549d3ebc5ae6ae091199e95930681ac2a9152a8834184
d6000a19198b8b9719fc17f7c06366e542802a8e7e232ba731b72c31226cc890
d81e7d95004441ea4f5344215232db57f48579bf335c7ba4ed7f6ec6f9136ed0
db1bc70c0d0c7121f1d4422a6fcd0e0668d9da786affb52dd77852641e425710
ddda5737b2c3207d72d728bf40709a7296c31e7c50951dcad441f4707581ccb1
e1b903eba88b92090987644 2306e1160eed9b69c69a05ea370cba2121e305ba1
e49a7d9083b2e448274d117405c39b0c1b2c0c20ab5195bdf94aaeda7cc113d7
f44964c8fdf6dbdb21c141df61b45467bba5a4482f7ab19fd6f1841fdb791f2a
f6b01df60d526f1de530230724d41b482adfff81084a1872bb97c316b76e45e3
f701f500d348b63f3250239cd8305a8b38230e67d74456f3333c6efeeef85bbb
fb67be10a5a8b26ca86f8f79935ddd4a5b40379bb6d0af21d23f56af14bb2a90
4307a067db6b6abd852441e6d70de29c3bd0e4d6a68f0449b403401518b7e037
69fc5bed55acf559035f2c5550bf8807236b580f8e2db88966b3fc80c83914d3
4c43b4575063d50ca5668e45a434aaf288970c89e8a4414812560ee787307f58
135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c
252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146
594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978
6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49
71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc
b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb
bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c
dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54