Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

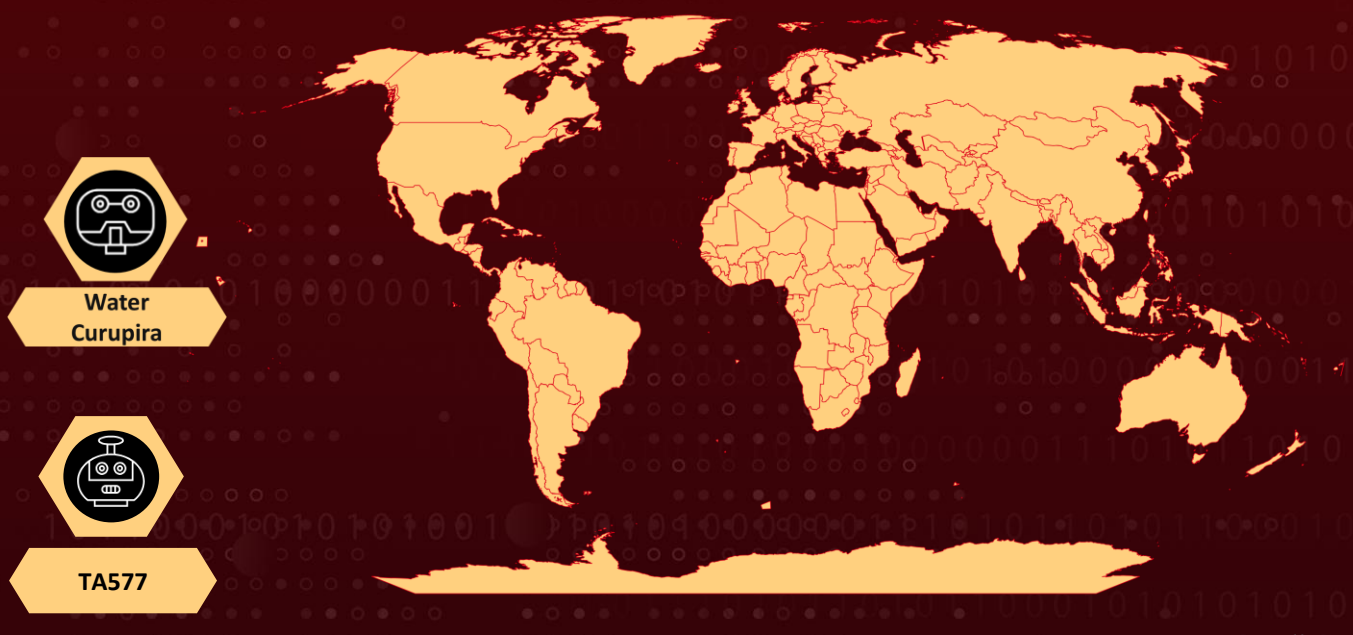
PikaBot Malware Unleashes Threat via Malvertising

Date of Publication	Last Update Date	Admiralty Code	TA Number
December 20, 2023	January 11, 2024	A1	TA2023513

Summary

Attack Discovered: February 2023
Attack Region: Worldwide
Actor: Water Curupira, TA577
Malware: PikaBot, Black Basta
Attack: PikaBot, a recently identified malware family, has become a prominent threat in malvertising campaigns, particularly through search engine ads. Associated with the TA577 threat actor and linked to ransomware distribution, PikaBot employs advanced tactics, such as decoy websites and fingerprinting, highlighting the evolving landscape of cyber threats. Threat actor, Water Curupira has also been actively spreading the PikaBot loader malware through spam campaigns.

Attack Regions



Attack Details

#1 In the past year, there has been a rise in malicious advertising (malvertising) targeting businesses, particularly through search engine ads. Browser-based attacks, including those involving social engineering, have become more common. Criminals are using specialized services to bypass Google's security measures and set up decoy infrastructures. A new malware family called PikaBot has emerged in 2023, distributed via malvertising and associated with the threat actor TA577.

#2 PikaBot was initially identified in malspam campaigns and later linked to TA577, known for distributing various payloads, including QakBot and ransomware. After the takedown of the QakBot botnet, malspam campaigns delivering PikaBot and DarkGate increased. The typical distribution chain for PikaBot involves emails with links to external websites, tricking users into downloading a malicious JavaScript that fetches the payload from another site.

#3 PikaBot's core module is injected into the legitimate SearchProtocolHost.exe process, using stealthy techniques like indirect syscalls. The malware targets Google searches related to the remote application AnyDesk. The distribution involves malvertising, with threat actors using tracking URLs and fingerprinting via JavaScript to evade security checks. Similarities with previous malvertising campaigns, such as FakeBat, suggest a common process used by different threat actors.

#4 In another campaign, Water Curupira, a threat actor linked to Black Basta ransomware attacks, has employed thread-hijacking to disseminate PikaBot. Cobalt beacons linked to Water Curupira were observed on more than 70 domains.

#5 The phishing emails involve a malicious JavaScript and were sent from compromised email addresses. The obfuscated JavaScript file executes conditional commands, downloads the PikaBot payload, and runs it. The JavaScript file can also download password-protected attachments, disguise PDF files as Microsoft OneDrive files, and use array manipulation to obfuscate the code's structure.

#6 The association between PikaBot campaigns and the deployment of the ransomware along with involvement of multiple TAs adds an extra layer of danger to these campaigns. Further, malvertising has also emerged as a potent tool for malware delivery, allowing threat actors to target businesses without users visiting compromised websites directly. Defending against malvertising is challenging, especially with the presence of malicious ads in search engine results.

Recommendations

Update Security Software: Ensure that all security software, including antivirus and anti-malware tools, is up-to-date. Regularly check for updates and patches to enhance protection against evolving threats like PikaBot.

Email Security Measures: Employ advanced email filtering solutions to detect and block malicious emails. Implement DKIM and DMARC to authenticate emails and reduce email spoofing.

Web Filtering: Utilize web filtering tools to block access to known malicious websites and domains. Regularly update and maintain blacklists to include new threats as they emerge.

Browser Security Settings: Configure browsers to block pop-ups, disable unnecessary plugins, and limit the execution of scripts. Keep browsers and plugins up-to-date to patch any known vulnerabilities.

Endpoint Protection: Deploy robust endpoint protection solutions that include antivirus, anti-malware, and anti-ransomware features. Regularly update and patch operating systems and software to address security vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0042 Resource Development
TA0007 Discovery	TA0011 Command and Control	TA0009 Collection	TA0010 Exfiltration
TA0040 Impact	T1082 System Information Discovery	T1057 Process Discovery	T1219 Remote Access Software
T1583 Acquire Infrastructure	T1583.008 Malvertising	T1566 Phishing	T1566.002 Spearphishing Link
T1204.002 Malicious File	T1204 User Execution	T1036 Masquerading	T1059.007 JavaScript

T1059 Command and Scripting Interpreter	**T1218.011** Rundll32	**T1218** System Binary Proxy Execution	**T1218.007** Msiexec
T1041 Exfiltration Over C2 Channel	**T1140** Deobfuscate/Decode Files or Information	**T1560** Archive Collected Data	**T1102** Web Service
T1574 Hijack Execution Flow			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5, da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff, 69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320, 4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8, 6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8, ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d, 1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b, b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7, 980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753, 6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193, 3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624, 8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004, 7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a,

TYPE	VALUE
SHA256	ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21, 07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632, 2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34, 1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469, 6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e, 7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3, 2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe, 8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df, 79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21, eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a, 7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7, 46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66
URLs	hxxps://sindicaturadetecate[.]gob[.]mx/pe/?IDbHJCMofpEIzDQjrcwNcDqHoiQRnSKZQcA, hxxps://lsn[.]edu[.]dz/pqis/?aWDzZBatBsyv, hxxp:188[.]34[.]192[.]184/76DKN6/Wheez, hxxps://brouweres[.]com:443/vvs49/0.6515179055030298.dat, hxxps://brouweres[.]com:443/vvs49/0.8450027286577588.dat, hxxps://brouweres[.]com:443/vvs49/0.15313287608559223.dat, hxxps://brouweres[.]com:443/vvs49/0.9900618798908114.dat
MD5	4deb812eeae3c499530e1bd4f0e108ba, 5be9d3aa133d23c439e5181da7450323, de2cab21e6342cf20535b0734d5ca3c0, 222b1793938f507877ee194ba0acd86b, 7d6a6233a8792ea216a529836c13e923, 22be88cf8f57d9412eaa40c541f08eb2, c28f33fee92fd7396fdb5792dea90365, 2430e3a9d5c97d0184f8af59abda4abb
IP	172[.]232[.]186[.]251, 57[.]128[.]83[.]129, 57[.]128[.]164[.]11, 57[.]128[.]108[.]132, 139[.]99[.]222[.]29, 172[.]232[.]164[.]77, 54[.]37[.]79[.]82,

TYPE	VALUE
IP	172[.]232[.]162[.]198, 57[.]128[.]109[.]221, 15[.]235[.]202[.]109:2226, 15[.]235[.]44[.]231:5938, 15[.]235[.]45[.]155:2221, 15[.]235[.]47[.]206:13783, 15[.]235[.]47[.]80:23399, 154[.]221[.]30[.]136:13724, 154[.]61[.]75[.]156:2078, 154[.]92[.]19[.]139:2222, 188[.]26[.]127[.]4:13785, 210[.]243[.]8[.]247:23399, 51[.]195[.]232[.]97:13782, 51[.]68[.]147[.]114:2083, 51[.]79[.]143[.]215:13783, 64[.]176[.]5[.]228:13783, 154[.]221[.]30[.]136:13724, 137[.]220[.]55[.]190:2223, 210[.]243[.]8[.]247:23399, 65[.]20[.]78[.]68:13721, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 154[.]92[.]19[.]139:2222, 172[.]233[.]156[.]100:13721, 154[.]61[.]75[.]156:2078, 64[.]176[.]67[.]194:2967, 158[.]247[.]253[.]155:2225, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 172[.]233[.]156[.]100:13721, 154[.]92[.]19[.]139:2222, 154[.]61[.]75[.]156:2078, 137[.]220[.]55[.]190:2223
Domains	anadesky[.]ovmv[.]net, cxtensones[.]top, startupbusiness24[.]net, seohomee[.]com, softradar[.]net, investsystemus[.]net, blocknowtech[.]net, mytrailinvest[.]net, realeinvestment[.]net, cloudwebstart[.]net, monitor-websystem[.]net, karmafisker[.]com, airbusco[.]net, trailgroupl[.]net, monitorsystem[.]net,

TYPE	VALUE
Domains	cloudworldst[.]net, neobeelab[.]net, stockinvestlab[.]net, prettyanimals[.]net, gift4animals[.]com, ionoslaba[.]com, buyadvisershop[.]net, blockcentersys[.]net, startuptechnologyw[.]net, investmentrealtyhp[.]net, mynewbee[.]net, buzzybeet[.]net, wellsystemte[.]net, investmendvisor[.]net, reelsysmoona[.]net, startupbizaud[.]net, building4business[.]net, steamteamdev[.]net, audsystemecll[.]net, welausystem[.]net, treeauwin[.]net, clearsystemwo[.]net, lindacolor[.]com, withclier[.]com, unougn[.]com, bluenetworking[.]net, getfnewsolutions[.]com, conitreid[.]com, allcompanycenter[.]com, sandelias[.]com, getfnewssolutions[.]com, erihudeg[.]com, reganter[.]com, masterunis[.]net, masterunis[.]net, taskthebox[.]net, taskthebox[.]net, settingfir[.]com, magementfair[.]com, businesforhome[.]com, ruggioil[.]com, gertefin[.]com, gartenlofti[.]com, garbagemoval[.]com, constrtionfirst[.]com, animalsfast[.]net, schumacherbar[.]com, maluisepaul[.]com, masterunix[.]net,

TYPE	VALUE
Domains	wardeli[.]com, nutiensel[.]com, jessvisser[.]com, caspercan[.]com, kolinileas[.]com, unitedfrom[.]com, brendonline[.]com, septcntr[.]com, auuditoe[.]com, conectmeto[.]net

References

https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads

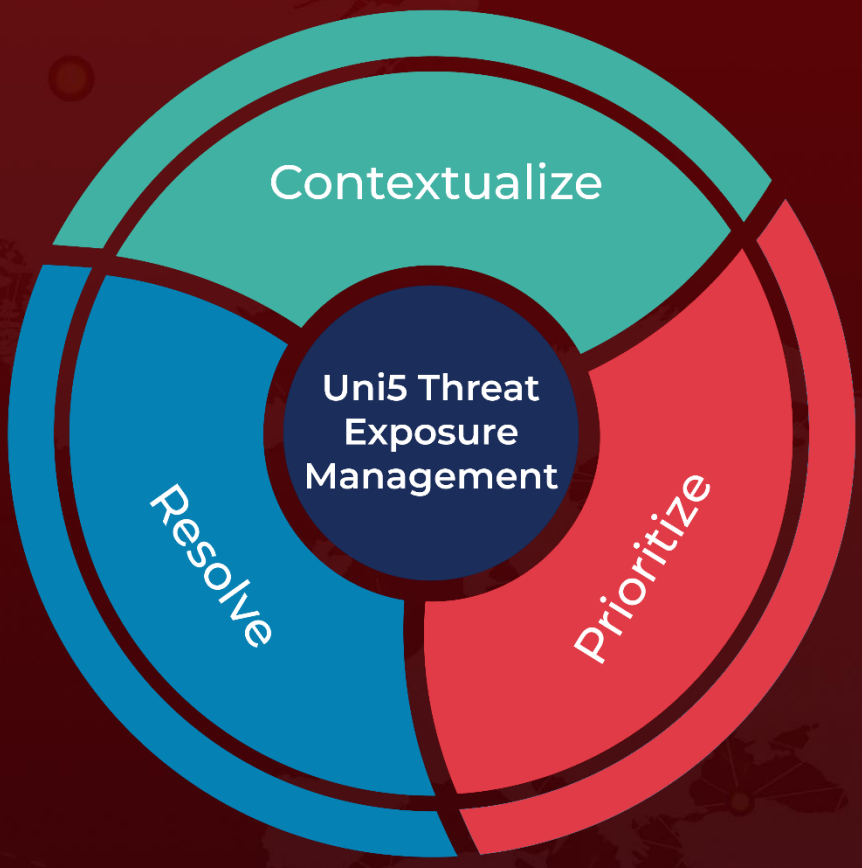
https://www.hivepro.com/threat-advisory/pikabot-a-stealthy-backdoor-with-ingenious-evasion-tactics/

https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

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

December 20, 2023 . 5:30 AM

More at www.hivepro.com