KPMG Cyber Threat Intelligence Platform

Pikabot Malware – The Multilayer Trojan Spreading Through Malspam

Pikabot is a newly discovered Trojan malware that emerged in early 2023. It employs malvertising to distribute itself, transitioning from malspam after the successful takedown of the Qakbot malware. Comprised of a loader and a core module, Pikabot enables unauthorized remote access, allowing attackers to execute arbitrary commands from a C&C server. This sophisticated multistage malware integrates multiple components within a single file, utilizing decrypted shellcode for DLL decryption. Pikabot's malicious activities include distributing CobaltStrike, ransomware, and other harmful software.

Infiltrates via crafted spam emails containing ZIP or PDF attachments using email thread-hijacking. Once opened, the ZIP file contains an IMG file, with a disguised LNK file (word document) along with a DLL file, triggering the malware through rundll32.exe or it could be a PDF file with JavaScript attempting command execution via cmd.exe. If unsuccessful, it fetches malware from an external server using Curl.exe. To evade analysis, it employs anti-analysis techniques such as debugger checks, string obfuscation, fake DLL loading, and indirect system calls. It controls single instances with a hard-coded mutex and checks for debugging processes with shellcode. Encrypted process information is sent to C&C servers via a named pipe, while system details are forwarded in JSON format. Communicates using specific IP addresses and URLs for C&C operations, sending encrypted victim system information by appending it to designated URLs. It also deploys backdoors, often leading to other ransomware attacks.

Defenders must enhance cybersecurity measures to counter Pikabot's anti-analysis techniques and multistage approach. This includes advanced threat detection, strict access controls, network monitoring, and collaboration with threat intelligence.

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

KPMG Cyber Threat Intelligence Platform

Pikabot Malware – The Multilayer Trojan Spreading Through Malspam

Indicators of Compromise: IP Addresses	
65.20.78[.]68	15.235.47[.]206
45.154.24[.]57	51.79.143[.]215
45.85.235[.]39	210.243.8[.]247
94.199.173[.]6	154.92.19[.]139
15.235.47[.]80	154.61.75[.]156
188.26.127[.]4	129.153.135[.]83
64.176.5[.]228	15.235.202[.]109
70.34.209[.]101	154.221.30[.]136
64.176.67[.]194	137.220.55[.]190
15.235.44[.]231	158.247.253[.]155
15.235.45[.]155	

Indicators of Compromise: Domains
brouweres[.]com

Indicators of Compromise: Hashes
de387211ce4d850475df9c828ebd5cb6
6c88a65f17b9d3c26b15b62fc9f66dcb
b9a7f2cc9283df19c763c6dd8c2ff3fe
57d788f3ba753769ac17f3c323df0a18
e191ac95111778ea0c609aec54fcb5c5
4deb812eeae3c499530e1bd4f0e108ba
5be9d3aa133d23c439e5181da7450323
de2cab21e6342cf20535b0734d5ca3c0
222b1793938f507877ee194ba0acd86b
7d6a6233a8792ea216a529836c13e923
22be88cf8f57d9412eaa40c541f08eb2
c28f33fee92fd7396fdb5792dea90365
2430e3a9d5c97d0184f8af59abda4abb
905cab370e0422d96da8aa51b023b4be
7204144dbed504187136592d8b18e9f9
5ea07b4293ad10317cb27ca2de5f68b4

KPMG

KPMG Cyber Threat Intelligence Platform

Pikabot Malware – The Multilayer Trojan Spreading Through Malspam

Indicators of Compromise: Hashes
1e26ae07589794225c37134a7cd9d3fd
6f206f8bd2edf6127c665728ca66d77d
83a2653afd8537c46ea7e5256532d305
7c3773311edb63631225bb03ff318714
491de488716811cf6c432a435a413688
fb2729cb59a5bc0420425ea693d26190
527774acc9e68d3274e0806873b5c88d
a2090749675827cd029c5564ee9816b1
6fe4f35e2d2b2aacf64b19e60529ab05
dcd03d771e347e34ccde8e5be5bdda78
8a69cbede14352596b97d5dd57dbeed6
1b8361e2f1b058a9791047dce0df57c4
fc263f70e9457b31a651d25b0c94cf77
bcd23166402f089f7e82853b0300a7ca
1be0957d4bc3dee90f43ef6b2c4a6045a6511dfc
e0d6e092f81438e882423416e0fb59c4ed1dcf23
698473f1c86fe7dc9dfe5075b535af95aa57fda5
7f1979b33dccf26cb68c764769ccb8e64e86da29
73f759759831dbd591e0c64b69c691167e251b5f
3f380fd41bbd1118e4452532487ed3d2c5cf1c7c
3b37517ced041d764872696df2ab8d05a8a702a9
82cefca402664fc2b7fec7565d77af0a650da2e8
b20ad80d950b0954c17e8cc2cd0a1925edf0e6e6
fbddcd3b38f2658f38bf3c28773ecc79692f63a0
43ce1d0a7189994c253c3d0004f383d0d15fcd78
dbf14b1eee8908137c75fc41f53fa7f2713f936d
469567c2bf172c4e0d270b085ae9acaf0559c066
a94c4cb94baa8985a38202e8d654119dbaf1580a
8abe153f385a93bd0ff5097297455d36be2fca10
66153c61804457797a5dcbb62cf413109ce21cac
172118934b4827f791df810998c366a0a9e92864
6d0f9be4ca3d1262fde3c6e185753cb41858f5de
457acffaed6586e5e391f6d74238808a5a718649
3cd3750507971e8f9eef55249e5b2646855652c6

KPMG

KPMG Cyber Threat Intelligence Platform

Pikabot Malware – The Multilayer Trojan Spreading Through Malspam

Indicators of Compromise: Hashes
381f60c89aa59b04ba0b576bae0d11a5609a3e55
21cf7b20454f18a6b676620d626c0c5358d11683
dffd520c04bf2b1f87aef81e1514267a733c24d1
92153e88db630163346255148 02d0d1019363989d7b3f6863947ce0e490c1006
a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821
8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365
a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc
347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944
1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469
6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e
7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3
2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe
8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df
79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21
1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a
eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a
7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7
46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66
fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de
6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8
6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193
3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624
4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b
7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2
07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632
2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8
33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34
29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8
ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d
1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b
b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7
980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753
8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004
ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21