KPMG

KPMG Cyber Threat Intelligence Platform

Muddled Libra – Embracing Helpdesk Impersonation

Muddled Libra (aka Oktapus, Scattered Spider, Scatter Swine, UNC3944), is a cyber espionage group that has been active since 2022. They steal information for financial gain and seem to not shy away from engaging with targets on call, SMS and various other ways. Muddled Libra has been linked to more than six related incidents from mid 2022 to early 2023 and remains undetected within targeted organizations until they achieve their goals. They pose a significant danger to industries like software automation, telecommunications, BPO, & technology.

Primary initial access tactic includes social engineering techniques like smishing & helpdesk impersonation. They use spoofed & truncated lookalike corporate domains to phish for credentials. Once they gain access, they install multiple legitimate commercial RMM tools to maintain access. They capture credentials by either requesting for immediate MFA codes or bombarding users with continuous MFA prompts. If unsuccessful, they pretend to be a victim & contact the organization's help desk to enroll their own MFA device. They disable all defenses, including host antivirus & firewall & are known to exploit CVE-2015-2291 to deploy malicious drivers into kernel to bypass EDR. They Re-enable existing AD accounts & gains access to EDR consoles, to thrive stealthily within the environment. They utilize a mix of pen-testing & admin tools for network discovery & attack automation. Captured credentials are used to escalate privileges & pivot laterally using RDP. Sensitive data from local machines & enterprise data management tools are collected & archived. Establishes a reverse proxy/ssh to C2 or uses file transfer sites to exfiltrate the same.

Muddled Libra is highly goal-motivated & adapts its techniques as per the scenario. Extensive employee awareness & vigilant monitoring are indispensable to defend against such threats.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Muddled Libra – Embracing Helpdesk Impersonation

Indicators of Compromise: IP Addresses	
138.68.27[.]0	149.28.125[.]96
207.148.0[.]54	105.101.56[.]49
185.56.80[.]28	172.96.11[.]245
64.227.30[.]114	45.156.85[.]140
45.32.221[.]250	146.190.44[.]66
167.99.221[.]10	105.158.12[.]236
165.22.201[.]77	193.149.129[.]177
157.245.4[.]113	213.226.123[.]104

Indicators of Compromise: Domains	
ttec-vpn[.]com	okta-hubspot[.]com
box-okta[.]org	twitter-okta[.]com
msauthsso[.]com	shoplfy-okta[.]com
msauthsso[.]com	transcom-sso[.]com
twiiio-sso[.]com	jonas71.bushiko[.]ru
kucoin-pin[.]com	mailchimp-okta[.]com
infosys-vpn[.]com	slack-mailchimp[.]com
qualfon-sso[.]com	internai-customer[.]io

Indicators of Compromise: Hashes
6639433341fd787762826b2f5a9cb202
56fd7145224989b92494a32e8fc6f6b6
828699b4133acb69d34216dcd0a8376e
1e5ad5c2ffffac9d3ab7d179566a7844
f5271a6d909091527ed9f30eafa0ded6
fe9cdcc94fcc545cea3b966cbae5bba3
591f3a3918b764ffe71222932df075d2
eb98d1afb26be96d0bdf72294394745a
0d8e404a11190b65f0990c318ef6baea
2c2f1014102a5db6c32caf056a5fdb33
dc1381abca1a09f8f773c32e9254a4bb
414701c85f830e0256d29a9f02be25f0

Indicators of Compromise: Hashes
0e0968031f43ad9d0d5f654e2d896833
5925785db5f3649e5869f6a79094d88d
f4e199703cccba46e29c784e532d0149
227dc025fb770ff0dd22cac0982f2dbf
0272b018518fef86767b01a73213716708acbb80
d8cb0d5bbeb20e08df8d2e75d7f4e326961f1bf5
10b9da621a7f38a02fea26256db60364d600df85
ec37d483c3c880fadc8d048c05777a91654e41d3
9ec4c38394ea2048ca81d48b1bd66de48d8bd4e8
f13c4795fa96e0ab188f5778c2349bf7d8e47ac2
5630b78b50eccf991530ba09e2a589c6d456a1b9
8e2db48be15e09769e76f827517f545600f9433b
4c5b0635ab062386c7116eea4b824dfe0026324b
062c8ab4948f4b22e04c3b412ef371cfdbfcd01a
4e3bcc7f2d2a03f92c4ae0c0088b8d5660d0f68c
cbfad11adb3380383a5353c8c7d148c35c0c4015
06cdd853490239f9bcc6667e69f18c7830865fe8
08d8f77f897b0a57e483df9de355bb30c543e658
bf16ffea12ac563c9bc96f4ad113c665dc33d6cb
08feed47ddb63ab0d7f4f9c8d351c277e9cdcb9f
3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08
acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918
982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e
443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58
53b7d5769d87ce6946efcba00805ddce65714a0d8045aeee532db4542c958b9f
4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93
cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005
648c2067ef3d59eb94b54c43e798707b030e0383b3651bcc6840dae41808d3a9
eaf18110b1cad729d8ab40ede52928be54aa997b7c58b7cb271a95009087a824
8b15d0ba041cbb5486f23e46b8d54930d531937c9a0a8fb06d3e307d1fcfacca
6fbbaf1a3e3431ff57d639b670fd1eea3dd45345b35784520b3269d1aa96e96a
ff6cb577a82b9998bed894b5bf41655b5e73e75f88f703ac2f42921cf50d5abe
9815e19e8e3aa29010e15cf422ea88a365fa5d4391821d6f192a0322fbd45e6d
7e673ccfc5038bff16a9878dd77f89fa39762543730eef67820226fc38a94f3c

KPMG

KPMG Cyber Threat Intelligence Platform

Muddled Libra – Embracing Helpdesk Impersonation

Indicators of Compromise: Hashes
7e3418019b7697def9d8de819d08e26059b1e9357a23054ea23fe700207efe4f
59443fd0525aafaabba1cbb96807e4de6365a3cea6407ed35df06dbd9b27852e
48c4f35fa5ab1be0a4feb438d41937523f885c5c81a601d5229dae627f911934
376e2c6abd92a7811f5fce0f0bb9bbc40c4b139e4112533ed09586df2df25733
1df89993681f461126bfd4e1c78cf8ebdc101af7b97932261d3b5b70d29ae1e1