KPMG

Threat Intelligence Research

The Lapsus$ Group: Brazen, notorious and chaotic extortionists

Suspected to be based out of Brazil, Lapsus$ has done what others feared : actually leveraging insider access as a viable, fast initial access tactic. They have optimized and compressed the killchain model to mere hours with a take-no-prisoner's approach. Currently the poster child of infosec buzz, Lapsus$ has successfully targeted big names such as Microsoft, Okta, LG, Nvidia, Samsung, Vodafone to name a few. Notorious and brazen, they are known for their showmanship and a penchant for gaining street cred.

Lapsus$ made headlines in December 2021 by extorting Brazil's Ministry of Health and quickly began recruiting insiders via social media platforms. They maintain an active Telegram presence wherein host polls on whom to target next, recruit for remote insider access and share trophies by leaking victim's data. Even recent law enforcement action has not slowed group down.

Initial attack vector includes social engineering campaigns to recruit insiders, phishing campaigns, SIM-swapping, session token replay and MFA bypass. This is followed up with lateral movement, privilege escalation and exfiltration tactics. They are known to leverage creative TTPs to target organizations and their TTPs evolve as per defensive endeavors taken by victims, for instance, in one of their campaigns, they intentionally disrupted the network to learn the victim's incident response workflow. Unlike other groups, they do not ransom data through ransomware tactics, they instead extort through name & shame tactics.

Lapsus$ has cemented insider access as a viable tactic to target trusted environments, which has given organizations an opportunity to relook at their authentication and access workflows.

What should you do?

- Relook your authentication and access mechanisms and keep a close eye on anomalies.
- Monitor Indicators of Compromise (IoCs) to identify anomalies.
- Ensure your environment is patched to the brim.

What is KPMG Cyber Threat Intelligence Platform (CTIP)?

The KPMG Threat Intelligence Platform (CTIP) is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree 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.

Range of services
Strategic Threat Intelligence Report
Machine Ingestible Threat Intelligence feeds
Threat Intelligence driven pre-emptive Threat Hunting Exercise
Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

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

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

KPMG

Threat Intelligence Research

The Lapsus$ Group: Brazen, notorious and chaotic extortionists

Indicators of Compromise (IoCs)

IP Addresses	
93.95.98[.]5	45.146.166[.]38
37.0.10[.]214	198.244.205[.]12
185.56.83[.]40	108.61.173[.]214
51.89.208[.]22	103.195.100[.]11
185.56.83[.]40	188.124.36[.]242
81.4.105[.]174	173.239.198[.]46
45.32.137[.]94	108.61.207[.]100
185.56.83[.]40	104.238.222[.]243
78.24.222[.]162	104.238.222[.]158
62.182.159[.]86	

Domains	
2no[.]co	lalindustries[.]com
chrisro[.]fun	windows-upgraded[.]com
lapsusgroup[.]tk	advanceorthocenter[.]com
discrodappp[.]com	hockeybruinsteamshop[.]com
cothdesigns[.]com	privacytoolz123foryou[.]xyz
a.goatagame[.]com	fsstoragecloudservice[.]com
rdp.chrisro[.]fun	

Hashes
54ef1804c22f6b24a930552cd51a4ae2
521ceeb7f28d79041f7a40211b9d449b
4dfae4ff7570aa9877b3cd7cfe16d281
4bd0da68ae035e5d91b3a9961d8f8a83
4ba089b88198d0a07813e84c7d53acfb
49a5353d5f6975e302b612bdc02c287a
489547521e5657f050995a5dab008575
47506e81a931712c01a53405ab8b8378
41084089d5432ebcd2433d5a3bccc497
3e87597e474483fe8658b76c22c5c4f6
ca12e39b1914f04adf984b0be948d145d672cb9d
c1dca912e6c63e3730f261a3b4ba86dec0acd5f3

KPMG

Threat Intelligence Research

The Lapsus$ Group: Brazen, notorious and chaotic extortionists

Indicators of Compromise (IoCs)

Hashes
bab615526528b498a09d76decbf86691807e7822
7bfaa385f1833ed35f08b81ecd2f10c12e490345
76ab68f1517d039d9ea6d7ab3bca9aed456e4466
71d8398652a891d09492db64bc1458349ba4cdbc
6ce25829ac6404025d51006cfc10ffbe69333152
6199b33c52351cdc5d6cd1b61bb9f3602c9eb799
5819d925377d38d921f6952add575a6ca19f213b
5438628759dc6347f8988cdcf5bc68ca67d9acc6
d7a024e5a65adc579ca49638c4e542da4b1c073c7c972b39bbd4ac269acfbfec
e940ec4a396fa3dfcedfb308412049892dda2f34d92ec625cbc6005279c33615
e9f66d914970a0508757f2c88e06ab96796db8aa1d48cb7ebcc29c2a1686a637
eab9ac84f23f1a78871de1035d5b8c058c54f2934114dd818f509a47f4c8e259
a0aa66f6639e2b54a908115571c85285598845d3e52888fe27c6b35f6900fe56
04dde2489d2d2e6846d42250d813ab90b5ca847d527f8f2c022e6c327dc6db53
255a65d30841ab4082bd9d0eea79d49c5ee88f56136157d8d6156aef11c12309
79dc8659dc41b718793abf3cd28513e01202513ffb2d47d052368acaa52b8032
d968a966ef474068e41256321f77807a042f1965744633d37a203a705662ec25
0e1638b37df11845253ee8b2188fdb199abe06bb768220c25c30e6a8ef4f9dee
d569c6cede1c9248349eba10f2fab21d24ef73417ef94dd0f1e5ad673e1f3568
f4ec629473fbe96fa82fe1c1e30e6784144163d662e1c977acf5bc1d62b20c0b
eec05dc9ade2a7ee74ea5fb115bdd687b457d1f81841238a61e9775d6cc4bfa6
e1cbebc0c9a675ca172e7de1908991f7b0bd0866c1bea9404ae10bc201de0fe6
dde32911345a4c9d54355c6d57a72c5177d2a46cb0c507121e3709cadfcc9b44
dbd9cfa3d9b4e482ee79e7726e95168a5e27bb0482a0e4744a1e1c56d75f1c32
dab2a18df66f2e74d0831a8b118de6b9df2642ac939cbad0552e30696d644193
cb54b6471597a9417bcc042d0f0d6404518b647bd3757035a01e9de6aa109490
ca46080e121408d9624322e505dc2178ba99e15871c90e101b54e42ea7b54a96
b483fe7d29ce8eedcb3e1ec061e0f45bc44d0b48e4f21eaaf67a063388314ff7
98c781b3fd15d6c7c7624aa1a0c93910dd5d19722a1d9b8cb1c7b9673d311090
963989f4b4d6e2d7c2281992ae5d62966726e81b5070b792399c7fd2017ca5ca
9460ffe580332fe64bb4f35bb63dc6a4302f3613718a04dc0986cea989160039
8cfa7e9bc6cbd458cec18a25e6f763a3776802490e6b3d451d864c4dba50c437
8b57cd06470e93abf9ea61e86839a3f7eb3b13fbb37c5fec34888652a65185c3
857dd46102aea53f0cb7934b96410ebbc3e7988d38dcafdc8c0988f436533b98
6d4b28002fc36b27dfdca0fbd886c73704950ee88b14b805512a938f423d7e1c

Threat Intelligence Research

The Lapsus$ Group: Brazen, notorious and chaotic extortionists

Indicators of Compromise (IoCs)

Hashes
57fb96b12db08b18906ce22c7e55b81a214ede326166e772ae87412281044497
57381b4de751f07c4537e2becbb0f5c93a23897aa1bf1f0274e05f3ff4fd62f5
4b95ff6312411ed2eec0dc2fdb251d985b6e9892e1b2f61aadb94dea1b3eeb13
3593247c384586966e5a0e28eb4c4174b31e93c78c7a9e8fef96ec42a152e509
15ad913c094cd58fffa2067d86b75cf08fbcac95c16c2d68bab5b3498f059e31
1583fceeae47160fd37427a55f1d2122f3654e528e29c55d64df145122515a55
f088dac66ed4630d674073125c7562aa3eb283a30bc4bcc162abf0d47458ce8f
d2e03bb72a530d14de71be2c7d4aa2275887113aa2ff6d57f53c57f4a8516365
c33defdd2c60f2d74ebaabbe82805a7a36fa2428cda8c42fd202396b4eda28f6
ae9e7613eb86358cf0c50eb2753c82c605f170fcae1ada510506d037d2987e66
9a305e8a3616def77c4c7f18c0c91a7b67544fd4473c209d95b8b614c31a5790
927965d51c202140e974ea473ed143e701e1ed3b6b34583200d5a8935457a36f
a7c3ce181e5c3956bb6b9b92e862b6fea6d6d3be1a38321ebb84428dde127677
1928a6969812987501e58d7ee640d1215f00c00ca3eed7565a527b4739e5c3ba
065077fa74c211adf9563f00e57b5daf9594e72cea15b1c470d41b756c3b87e1
9d123f8ca1a24ba215deb9968483d40b5d7a69feee7342562407c42ed4e09cf7
2f578cb0d97498b3482876c2f356035e3365e2c492e10513ff4e4159eebc44b8
77a1efb6136f52dd2372987b13bf486aa75baeacb93bad009aa3e284c57b8694
32528efb1c2d7710b98d42eeee0be369e3a15646d7f78fc4e4548b58b97c99e6
391349270769647f0bee670795f0d1f08ce545a62c849442b26b10600d6518f5
3e58db1b5a90a4352124914d3be7bfa293910e8f8027478c92dc97b361d10c63
41b2a9030ef324ee810fe4c41126403f4c1e6c77d1f88faaeb8ccdb12fda5168
4e805799145aa3b3ced6468c1f2b1dd90645cc0c045105a2da104664f7e3cab9
506a7d48fafc1f069d465c5a4f2899273e1ed6f36524e270d26fd4003836d9fc
58583f42a747fff8b8cd7e2f8ce991a28ccfe8111acd077993b50af9bea95d2d
5cd6dec4a0a0ffef0484c4e12c2dbdfd5558774187fe6ecca5f75e2a60d91147
6cff4fba23cd2253a9e5081cf38bb639643e08918f47c6843a848cdfd4b1f977
81f56a85a42fec9dc6cc4bb0c7d852f4500053640336e06a035bdde9e7166d40
88baa2a228807126dd2ee835ba305dd2c56e14e39b8af36504e6d41144b915e8

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.