KPMG Cyber Threat Intelligence Platform

Lazarus Group – The Most Notorious Group

Lazarus Group (a.k.a HIDDEN COBRA or Zinc) is a North Korean state-sponsored Advanced Persistent Threat(APT) group. This group is known to be involved in a wide range of threats from cyber espionage to disruption of financial services. The group has been active since 2010, and have been involved in multiple attacks like Operation Troy(2009), Darkseoul(2013), Sony Breach(2014), Operation Blockbuster(2016), Bank Cyber Heist(2016), Wannacry (2017), Cyptocurrency attack(2017). The recent 2021 attack was deployed with novel methodologies and specialized toolkits.

In January 2022, the group initiated a spear-phishing campaign weaponized with malicious document using its good old 'job opportunity' theme and a slick use of windows update to execute malicious payload while using GitHub as a C&C server. Initially, the persistence in the target system is achieved by malicious macros followed by series of injections. Once the file is accessed by the user, the macros drops "WindowsUpdateConf.lnk" file in the startup folder along with a hidden DLL file into the "Windows/System32" folder. The ".LNK" file then launches the Windows update service, which of course is a genuine file on the windows file system. It works on delivering automatic updates in windows system where it is used to run the malicious DLL file. This way, the malicious code is executed using following arguments: "/UpateDeploymentProvider", Path to malicious the DLL and "/RunHandlerComserver". Once the malicious code is executed on the system, a connection to Github C2 server is created for further communication attack co-ordination. Though Lazarus Group is one of the oldest and widely tracked APT groups known, it keeps updating its toolset and employs several new techniques to remain effective and create havoc among its target.

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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Lazarus Group – The Most Notorious Group

Indicators of Compromise: IP Addresses	
103.95.99[.]3	66.181.166[.]15
103.5.124[.]94	114.113.63[.]130
95.0.200[.]212	75.146.197[.]161

Indicators of Compromise: Domains	
gsachshr[.]com	datacentre[.]center
lm-career[.]com	dubbedfinally[.]link
ilesaves[.]cloud	digitalguarder[.]com
onedocshare[.]com	trollinguneaten[.]org
docusign[.]agency	pavestonecorset[.]com
fsdriveshare[.]org	doc.filesaves[.]cloud
onlinedocpage[.]org	markettrendingcenter[.]com

Indicators of Compromise: Hashes
85fe6affdb218b2d09a59e08e80eb1fa
de097c5ab5e31ac16b4466cd56e9bd2d
e87b575b2ddfb9d4d692e3b8627e3921
A27a9324d282d920e495832933d486ee
3f326da2affb0f7f2a4c5c95ffc660cc
490c885dc7ba0f32c07ddfe02a04bbb9
f2a0e9034d67f8200993c4fa8e4f5d15
a0e9f5d64349fb13191bc781f81f42e1
dec25c57bdc8c945ba975d0f693243cb
e0d2e5a8cafdc137d4006a21a80d7c8e
d0a5e14ce27abc2fa22a6bd7f4269e88
c44d866adf8c6845b7dda742c59c6b59
bed99a09a68eb8f8b53d2a9d0ccc085a
b139bb873c275a61730fbcb0145aed30
adefa310e925fcbd6f8aeea3bfb68afd
a0c1ca01548be7690f2976742f068e67
934c7b7c31d84728f0086be9b80ee1e4
8ce07870c4633f40d4f53d978b0a4334
8b9fee7600633e4017337d5b56613a59

KPMG

KPMG Cyber Threat Intelligence Platform

Lazarus Group – The Most Notorious Group

Indicators of Compromise: Hashes
1af33e1657631357c73119488045302c
84dd7ccb69d0010c97c1fc336650d5e2
791e527a2082e6207d1ac9b9b4550fdf
75733ee381ee80a07cfeddc6bddd91de
4b9366f2dcab60d56d09e69e21d77d91
42e6310ffbdd24cf9a2b5d200190359e
3c324706e3bae0b7187b134a813011cb
724cda52f18c86272eb82444644e6ebf0a8d4123
59882261d10983842e855d9d969881980565a5e5
21d230bcc2f38fbd01ddfceb5315fc12e40b712d
28a4f1155b0980c4a05505bb60ef805699a4f3e0
ed94bef7f2d99ee150bf38d263a902586672c7d8
e8226dfbb2c055843dbd11547ed8697a1e1ae825
cdfce1f630239655285963 75bdbc64c8ffacc3ca
cab6dcec5bd77f8e59b1caa330ad58f0f8280f39
c38a63dc92db5c80e7198eecce5cd23db948b3c2
b4a20a7d4bccc0d2e2c8445de0383b015968ea84
88a5a6d55becf367a666d5538a2683a9d4c8c3fe
8197b6f95fb3c84c61a919644caeddcccc4a84a4
72fdea3122085a14065b6feac23e755f29c04213
5d93026501eb6f6fd844eaa5f0db3d7cc9c96986
2cd776c976b89dc5551c7d5b5817f708528c9560
2bc090dded3f325e969a0bbac4aa62d3f1e918a1
18e4203dab96fefd1b2c0c7e653b354fb3d27add
b19e3b0ea216eea3c3cdfae490b0929b8d0ca40d
a46318a25582c2616f33f49f7af986137637ba1d
8c5a0b975a1c585e6edcbeff4a0995b299c858b0
23d10901395b484f57492fb40ec590254aedb1dc
c6bda6161acdce21c9b356c26a41e79fa73d6cf6
a9a7c77df16fab16faf4d6ebf43d27a9134f2815
a23bc8f13e10ef3fee5102cd018e79b5303083d2
97515b70184f4553e5ae6b51d06a148b30d0a6632c077b98ad320e3c27cfd96f
4216f63870e2cdfe499d09fce9caa301f9546f60a69c4032cb5fb6d5ceb9af32
660e60cc1fd3e155017848a1f6befc4a335825a6ae04f3416b9b148ff156d143

KPMG

KPMG Cyber Threat Intelligence Platform

Lazarus Group – The Most Notorious Group

Indicators of Compromise: Hashes
11b5944715da95e4a57ea54968439d955114088222fd2032d4e0282d12a58abb
9d18defe7390c59a1473f79a2407d072a3f365de9834b8d8be25f7e35a76d818
c677a79b853d3858f8c8b86ccd8c76ebbd1508cc9550f1da2d30be491625b744
5098ec21c88e14d9039d232106560b3c87487b51b40d6fef28254c37e4865182
2d9d95bed6a6108802fa7c750cb66f2acce7b124f790ba552ec009c4d1d20744
cda63761c4305452ae097b31f01704d4bfd4fd9c88c5c44ff2ddb58c70485fe1
a6c9e9a9a4a05249502dee5d21dc92b3cdd44a0d0f044678715a6ecd907a938c
f70d826eba98bd0965341dfa05d7f9be233bdb57198a3d46e01a6606c6004c80
dcdfb1abc8dce78d6c2e0096a00c9cfef7223f4db78b02d108a251b42f95e1e2
bbf1a328f2d705201c1e4db7634ad1c503b96738285452b4f4be9f46364c1905
ac7b6ca73207db6ec6d4af2632a7c842c32af6658e3214753e589b567d809125
a6d614ec8d8135a7250d76d6c575da0de69efd862ea936af66a3cabb50e50789
a488b6bc2f4674c3a8fada86cc2794888713e61278c7c47d27f9706be0d18f4d
a3a1968fefab3c9d11976f8c00a9f726e0729f8e21761247f41790b4669bfde8
a042bfeee49345d514c274e5f44da374eb0875da4a5671e8bf67005078c076fd
9d6fdb5344f64e059043980c5bb80e9c8986f1a5a62d7d7871144b388df65262
928e92a0d08fab2e19bb07601f4904f60ed265a9f030d938c5a5454b4ed69af7
6cc98355f46b057b50bbf45cb9ad20408942f88cc12bb20293e5650936a1c925
6b0a93826b47e2b96fd79f19d02d9be1034958b30ef246ae57612b84c2ff5041
829eceee720b0a3e505efbd3262c387b92abdf46183d51a50489e2b157dac3b1
f14b1a91ed1ecd365088ba6de5846788f86689c6c2f2182855d5e0954d62af3b
689ea0e58022b86655596c946591a5b99b051f96e5cb0b0fd60dea302bbf91d2
52e9361cfec3bc643f5ac715709e1818766e1790c7f83e93e3ee7cc96fd1a473
51eaf8af57211f8d9e534f98413e71f4ddf5abcce806a111fc49a30d3bcec696
44759678842d930ca4251413f185d0a009b2da52dcdd45decf0daed5c78a97e9
4228efa547d22dcf38c44243e1e468a2ded17d4997b728ebf88c79d12346fca4
413c8b5d9156c4b399a180bc395d90a4bb8aa78df35b75241d33e186ea120f0f
3979b2d47cec119a9a22a80b1e5cdda7c59e97f9fc144918c20eeec5e27a6549
38ed248501bd35cd140f8376ac42e2c5a46ed4ec71cff0cec290fbc93678f323
353f82475fcfad5b3f06ed85a931bda46ec34279793b5d70085aa8c603e8ebec
1b9224a950584f736c81d5a803132cd99a422d7a1651d9e2ece52466cedda4d3
10d83ed487de6ddbd99011f405006efbd415e24037cfd9c724628decffd5aadd
0b8d7a851920d4584777505f9fb484b226a8457d4049885a87c847f7d3532d28
031e65bbf779b019e331fd1d0fd986e46db18681c5cd0102950b4d775f68aed1

KPMG

KPMG Cyber Threat Intelligence Platform

Lazarus Group – The Most Notorious Group

Indicators of Compromise: Hashes
f5563f0e63d9deed90b683a15ebd2a1fda6b72987742afb40a1202ddb9e867d0
8e1746829851d28c555c143ce62283bc011bbd2acfa60909566339118c9c5c97
294acafed42c6a4f546486636b4859c074e53d74be049df99932804be048f42c
65f7211c3d7fde25154b4226a7bef0712579e0093020510f6a4bb4912a674695
ebd6663d1df8228684a0b2146b68ce10169fc41c5e91c443fdf6f844f5ffeb62